Pulse Secure®

Pulse Secure iOS Client Administration Guide

Product Release	9.3.0
Published	November 2020
Document Version	1.0

Pulse Secure, LLC
2700 Zanker Road,
Suite 200 San Jose
CA 95134

www.pulsesecure.net

© 2020 by Pulse Secure, LLC. All rights reserved.

Pulse Secure and the Pulse Secure logo are trademarks of Pulse Secure, LLC in the United States. All other trademarks, service marks, registered trademarks, or registered service marks are the property of their respective owners.

Pulse Secure, LLC assumes no responsibility for any inaccuracies in this document. Pulse Secure, LLC reserves the right to change, modify, transfer, or otherwise revise this publication without notice.

END USER LICENSE AGREEMENT

The Pulse Secure product that is the subject of this technical documentation consists of (or is intended for use with) Pulse Secure software. Use of such software is subject to the terms and conditions of the End User License Agreement ("EULA") posted at http://www.pulsesecure.net/support/eula/. By downloading, installing or using such software, you agree to the terms and conditions of that EULA.

Revision History

The following table lists the revision history for this document

Document Version	Date	Description
1.0	November 2020	Initial Publication for Release 9.3.0

Contents

© 2020 Pulse Secure, LLC.

Pulse Mobile Client for Apple iOS

Pulse Mobile Client for Apple iOS Overview

Pulse Secure Client for Mobile Devices (Pulse Mobile Client) provides Layer 3 VPN connectivity based on SSL encryption and authentication between an Apple iOS device (iPhone, iPad, iPod Touch) and Pulse Connect Secure. Pulse Mobile Client enables secure connectivity to corporate applications and data based on identity, realm, and role. Pulse Mobile Client is designed to provide battery-friendly connectivity by automatically disconnecting from the VPN when the device is inactive while on Wi-Fi, automatically reestablishing VPN connectivity when the device reactivated, and maintaining connectivity when roaming from network to network. Pulse Mobile Client is available for download from the Apple App Store.

Note: Pulse Mobile Client features are updated frequently and each Pulse Mobile Client has a release number that is independent from the other clients and from the Pulse Mobile Client for Windows and the Pulse Mobile Client for Mac. We recommend that users upgrade their Pulse Mobile Client to the latest release to ensure that all features described in this guide are supported on the devices.

The *Pulse Secure Mobile Client Supported Platforms Guide*, available from the Pulse Secure website (www.pulsesecure.net), lists the mobile device OS versions supported by Pulse Mobile Client and the security features supported on each mobile device OS.

The Pulse Mobile Client app supports the following features:

- Full Layer 3 tunneling of packets
- UDP/ESP and NCP/SSL modes
- Authentication by all authentication options available on the Pulse Connect Secure server
- IPV6 mixed modes like IPv4 connections in IPV6 tunnels and vice versa
- IP based split tunneling and route monitoring

© 2020 Pulse Secure, LLC.

- Certificate authentication followed by any other form of authentication
- Layer 3 and Layer 4 Per-App VPN Connections
- Source IP enforcement through Pulse Policy Secure
- Multi-factor authentication (cascading two different types of authentication)
- Host Checker

Note: A Host Checker policy that is configured for a VPN tunnel is not triggered if the VPN is launched automatically by VPN on Demand on iOS. If the VPN session is started through Pulse Mobile Client, Host Checker policy is correctly applied.

- Apple VPN on Demand

  A VPN on Demand configuration enables an iOS device to automatically initiate a VPN connection when any application running on the phone initiates a connection to a host in a predefined set of hosts. A VPN on Demand connection uses client certificate-based authentication so the user does not have to provide credentials every time a VPN connection is initiated.

Note: When you configure VPN on Demand, you must create an exception for your Pulse Connect Secure server hostname. For example, if the hostname is sslvpn.example.com and you want Pulse Mobile Clients to automatically establish the VPN whenever requests are made for hosts in the example.com domain, the VPN on Demand configuration should contain the following rules:

- If domain name = sslvpn.example.com, then never initiate VPN connection.
- If domain name = example.com, then always initiate VPN connection.

  There are different methods for creating VPN on Demand connections:

  - Create and manage VPN on Demand configurations from within Pulse Mobile Client for iOS client.
  - Use the iPhone Configuration Utility. For complete information about how to create a VPN on Demand configuration using the iPhone Configuration utility, see the *iPhone OS Enterprise Deployment Guide*, available from the Apple website (www.apple.com).

- Secure Mail

  An ActiveSync proxy on the Pulse Connect Secure server provides secure email services to Pulse Mobile Client for iOS. The secure mail service encrypts email body content and attachments, supports email forwarding, and allows the Pulse Mobile Client administrator to quarantine the iOS device. Users view encrypted email body with any native iOS email client. Encrypted attachments are displayed by the secure viewer in the Pulse Mobile Client for iOS.

Before You Begin

Before you configure support for Apple iOS devices with Pulse Connect Secure, keep in mind the following client software behaviors:

- With Wi-Fi connectivity, Pulse Mobile Client reconnects the VPN tunnel automatically when the user wakes up the device. With 3G connectivity, the VPN reconnects when the user generates network traffic using an application like Safari or Mail.
- Establishing the VPN tunnel through a proxy is supported (regardless of the split tunnel mode), except for proxies that require authentication credentials.

© 2020 Pulse Secure, LLC.

- Static host mapping is not created for the Pulse server/proxy hostname.
- DNS considerations:
  - When split tunneling is set to Split tunneling disabled with access to local subnet, Pulse Mobile Client uses the DNS servers that are configured on the Pulse Secure server.
  - When split tunneling is set to Split tunneling enabled, DNS servers that are configured on the Pulse Secure server are used only for hostnames within the Pulse Connect Secure domains.
- Session scripts are not supported.
- Web-based installation from a Pulse Secure gateway is not supported.
- Session timeout reminders are not supported.
- When you use client certificate authentication, and the user is enabled to select from among assigned roles, the user is prompted to enter the role name instead of being presented with a list of roles.
- To ensure that users see consistent bookmarks in the Pulse Mobile Client UI no matter which server they are connected to, you can configure and enable user record synchronization, a feature of the Pulse Connect Secure platform.

Configuring a Role and Realm for Pulse Mobile Client for Apple iOS

To enable SSL/VPN access from an Apple iOS device to Pulse Connect Secure, the device user must download, install, and configure the Pulse Mobile Client app, and the Pulse Mobile Client administrator must configure specific realm and role settings on Pulse Connect Secure.

Note: Pulse Secure has created an App VPN SDK that enables app developers to integrate Pulse Mobile Client VPN connectivity within individual apps. Using an App VPN tunnel means that a mobile device user does not need to activate a Pulse Mobile Client connection and direct all traffic from the mobile device to the Pulse Secure gateway. Only traffic from the app goes through the tunnel. Configuration on the Pulse Secure server for App VPN is no different than the configuration for Pulse Mobile Client connections. For more information about Pulse Mobile Client SDK, contact Pulse Secure Technical Support (https://support.pulsesecure.net).

To configure Pulse Connect Secure for Apple iOS device access:

1. Log in to the Pulse Secure server admin console.
2. Select **User Roles > New User Role**.
3. On the New Role page, specify a name for the role and, optionally, a description. Make note of the name because later in this procedure, you create a realm and map realm users to this role.
4. In the "Access Features" section of the New Role page, select the **VPN Tunneling** check box.
5. Click **Save Changes** to create the role and to display the role configuration tabs.

   Specifying Host Checker policies is part of the role configuration. However, you must first create the policy you want to assign to the role, so that procedure is covered later.
6. Select **Web > Bookmarks** and then click **New Bookmark**.
7. Specify a name and description for the bookmark.

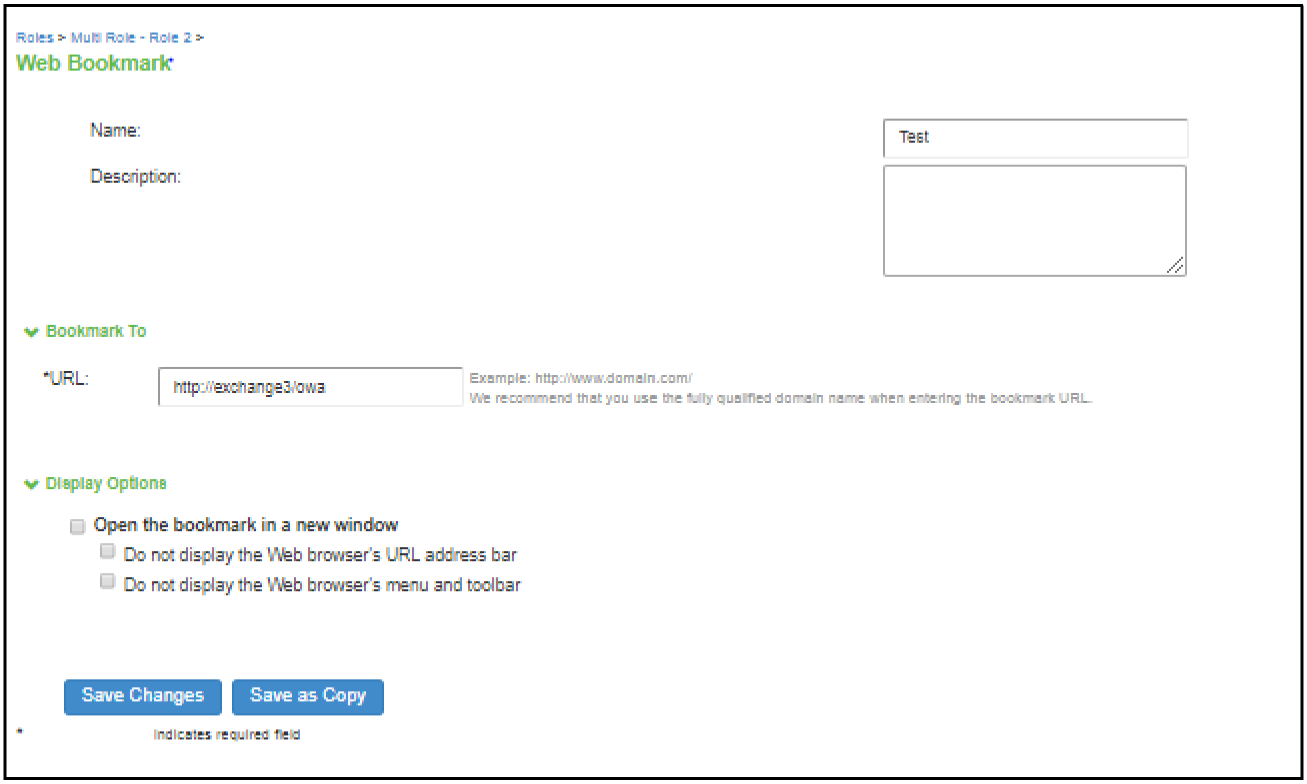
© 2020 Pulse Secure, LLC.

You must create bookmarks to enable the buttons that appear in the Pulse Mobile Client for iOS user interface. Typically, you create a bookmark for your company intranet and for Web e-mail.

Note: You must create an e-mail bookmark to enable the e-mail button within the Pulse Mobile Client interface on the iOS device, and that e-mail bookmark must be named Mobile Webmail.

8. In the URL box, specify the Web address for access to your organization's e-mail.

Figure 1 Creating the E-mail Bookmark for Pulse Mobile Client



Roles > Multi Role - Role 2 >

Web Bookmark

Name: Test

Description:

Bookmark To

*URL: http://exchange3/owa

Example: http://www.domain.com/
We recommend that you use the fully qualified domain name when entering the bookmark URL.

Display Options

□ Open the bookmark in a new window
□ Do not display the Web browser's URL address bar
□ Do not display the Web browser's menu and toolbar

* Indicates required field

Note: Alternatively, use Web resource policies to define the bookmarks.

9. On the **VPN Tunneling** tab, set the Split Tunneling options by selecting the following options:

   Split Tunneling

   - **Enable**: Split tunneling resource policies specify the traffic that passes through the VPN tunnel.
   - **Disable**: All network traffic goes through the VPN tunnel.

   Route Precedence

   - **Tunnel Routes**: The route table associated with the Pulse Mobile Client virtual adapter take precedence. Pulse Mobile Client overwrites the physical interface routes if there is conflict between the Pulse Mobile Client virtual adapter and the physical adapters. Pulse Mobile Client restores the original routes when the connection is ended.
   - **Tunnel Routes with local subnet access** (Pulse Mobile Client on Windows and macOS only)
   - **Endpoint Routes**: The route table associated with the endpoint's physical adapter take precedence.

10. To change default session time-outs, select **General > Session Options**.

© 2020 Pulse Secure, LLC.

11. In the Session lifetime section, specify **Max. Session Length** in minutes. The remaining session time appears in the Pulse Mobile Client user interface in the format days hours:minutes:seconds. The other session settings are not applied to Pulse Mobile Client.

12. Click **Save Changes**.

13. Select **Users > Resource Policies > VPN Tunneling > Connection Profiles**.

    A resource policy is a system rule that specifies resources and actions for a particular access feature. .

14. Click **New Profile**.

15. Specify a name and description for the connection profile.

    When you define the connection profile, note the following:

    - **IP Address Assignment options**: When Pulse Connect Secure receives a client request to start a session, it assigns an IP address to the client based on the IP address policies you define.
    - **Connection Settings**: ESP is the default transport. Pulse Mobile Client for iOS supports both ESP and SSL.
    - **DNS Settings**: Searching IVE DNS first with split tunneling enabled is not supported. With split tunneling enabled, Pulse Mobile Client uses the IVE DNS for queries for hosts in the IVE DNS search domains only. All other queries go to the client's DNS servers.
    - **Proxy Server Settings**: Pulse Mobile Client for iOS supports MDM remote proxy settings.

16. In the Roles area, select **Policy applies to SELECTED roles**. Then add the role you created for iOS devices to the Selected roles list.

17. Click **Save Changes**.

18. Select **Users > User Realms > New User Realm**.

19. Specify a name and description. Then click **Save Changes** to create the realm and to display the realm option tabs.

20. In the "Servers" section, specify the authentication settings.

21. On the **General** tab for the realm, select the **Session Migration and Sharing** check box.

22. On the **Role Mapping** tab for the realm, create a new rule that maps all users to the iOS device role you created earlier in this procedure.

Allowing Pulse Mobile Client for iOS Users to Save a Webmail Password

A Web bookmark on the role for iOS users allows users to access e-mail through a Web link. You can allow users of the Pulse Mobile Client for iOS app to save their e-mail password when they login to the e-mail system. After you have created a Mobile Webmail bookmark for the role used by iOS users, enable password the option for user to save their e-mail password by doing the following.

1. Open the role you created for iOS users.

2. Click **General > Session Options**.

3. In the section labeled “Persistent Password Caching”, select **Enabled**.
4. Click **Save Changes**.

Host Checker for Pulse Mobile Client for iOS

Host Checker is a component of Pulse Mobile Client that reports the integrity of iOS endpoints that are attempting to connect to Pulse Connect Secure. Host Checker runs as a Trusted Network Connect (TNC) client on the endpoint. The client evaluates the endpoint according to predefined criteria and reports to the Trusted Network Connect server, which is a part of Pulse Connect Secure. If the endpoint is not in compliance with the Host Checker policies, then the user might not get access to the network or might get limited access to the network depending upon the enforcement policies configured by the administrator.

Note: A Host Checker policy that is configured for a VPN tunnel is not triggered if the VPN is launched automatically by VPN on Demand.

For iOS clients, Host Checker can evaluate client compliance based on the following predefined criteria:

- **OS Checks**: You can specify the iOS version or minimal version that must be installed on the device.
- **Jail Breaking Detection**: Jail breaking is a process that allows Apple iPhone, iPad and iPod Touch users to gain root access to the iOS operating system and bypass usage and access limitations imposed by Apple. With a jail broken device, an iOS user can install applications that are not available through the Apple App Store. Jail broken devices expose the device to a greater risk of running malicious applications.

Configuring Host Checker for Pulse Mobile Client for iOS

Host Checker policies can be part of a larger Host Checker configuration that applies to many different types of clients or to iOS devices only. However, you might find it easiest to create a separate Host Checker policy specifically for iOS devices.

Note: A Host Checker policy that is configured for a VPN tunnel is not triggered if the VPN is launched automatically by VPN on Demand on iOS.

To create a Host Checker policy for iOS devices:

1. From the admin console, select **Authentication > Endpoint Security > Host Checker**.
2. In the Policies section, click **New** to open a New Host Checker Policy page.
3. Specify a name for the new policy and then click Continue to open the Host Checker Policy page.

   The name appears in lists when you implement the policy so be sure to use a descriptive name, such as iOS HC Policy.
4. Click the **Mobile** tab, and then click the **iOS** tab.
5. In the “Rule Settings” section, click **Select Rule Type** and select one of the following options and then click **Add**:
   - **OS Checks**: To specify the iOS version that must be installed on the device:

© 2020 Pulse Secure, LLC.

1. Specify a descriptive name for this rule. For example, "Must-Be-iOS-4.1-or-higher". Rule names cannot include spaces.
2. Specify the criteria. For example, to enforce iOS 4.1 or higher, create two conditions: "Equal to 4.1" and "Above 4.1".
3. Click **Save Changes**.

- **Jail Breaking Detection**: Jail breaking is a process that allows Apple iPhone, iPad and iPod Touch users to gain root access to the iOS operating system. and bypass usage and access limitations imposed by Apple. With a jail broken device, an iOS user can install applications that are not available through the Apple App Store. Jail broken devices possess a greater risk of running malicious applications.

    1. Specify a descriptive name for this rule. For example, "No-iOS-Jailbreak".
    2. The **Don't allow Jail Broken devices** check box is enabled by default.
    3. Click **Save Changes**.

6. After you have configured all of your rules, specify how you want to enforce them by choosing one of the following options:

    - All of the rules
    - Any of the rules
    - Custom

    For Custom requirements, you can specify a custom expression using Boolean operators AND and OR and also group and nest conditions using parenthesis.

7. Specify remediation options:

    - **Enable custom instructions**: If you enable this check box, a text box appears and allows you to type information that appears on the user's device if Host Checker discovers an issue. For example, if you enabled the MSS rule that terminates the VPN session of Host Checker discovers a virus, you can instruct the user to run a virus scan to clear the issue before trying to connect.
    - **Send reason strings**: Select this option to display a message to users (called a reason string) that explains why the client machine does not meet the Host Checker policy requirements. For example, if the jailbreak detection policy fails, Pulse Mobile Client displays A jailbroken device is not allowed to access the network. Please contact your network administrator.

8. When you are finished, click **Save Changes**.

Implementing Host Checker Policies for Pulse Mobile Client for iOS Devices

After you create one or more Host Checker policies for iOS devices, you must implement them. Pulse Connect Secure can use Host Checker policies at the realm or the role level.

© 2020 Pulse Secure, LLC.

Realm Authentication: You can configure a realm authentication policy to download and run Host Checker with a particular Host Checker policy. If the iOS device does not meet the Host Checker requirements, then Pulse Connect Secure can deny access. You can provide remediation information in the Host Checker policy to describe the requirement and help users take steps to solve the issue.

To enable a Host Checker policy for a realm:

1. From the admin console, select **Users > User Realms > SelectRealm > Authentication Policy > Host Checker**. The Host Checker page displays all of the available Host Checker policies.
2. Select the check box next to each policy you want to include. Select one or both of the following check boxes next to the policy:
   - **Evaluate Policies**: Evaluates without enforcing the policy on the iOS device and allows access.
   - **Require and Enforce**: Requires that the iOS device be in compliance with the Host Checker policy. Pulse Connect Secure downloads Host Checker to the iOS device after the user is authenticated and before the user is mapped to any roles in the system. Selecting this option automatically enables the Evaluate Policies option.
3. Optionally select **Allow access to realm if any ONE of the selected "Require and Enforce" policies is passed**. This check box is available if you selected more than one Host Checker policy. If you enable this check box, an iOS device is allowed access if it passes any of the Require and Enforce policies. The Cache Cleaner policy does not apply to iOS devices.
4. Click **Save Changes**.

Role: You can configure a role to download and run Host Checker with a particular Host Checker policy. If the iOS device does not meet the Host Checker requirements, then Pulse Connect Secure can deny access or assign the user to a remediation role that has limited access. You can provide remediation information in the Host Checker policy to help users take steps to solve the issue.

To enable a Host Checker policy for a role:

1. From the admin console, select **Users > User Roles > SelectRole > General > Restrictions > Host Checker**. The Host Checker page displays all of the available Host Checker policies.
2. Select **Allow users whose workstations meet the requirements specified by these Host Checker policies**.
3. In the Available Policies list, select the policies that you want to apply to select them, and then click **Add** to move them to the Selected Policies list. To select a policy click it. To select more than one policy, use CTRL+click.
4. Optionally select **Allow access to realm if any ONE of the selected "Require and Enforce" policies is passed**. This check box is available if you selected more than one Host Checker policy. If you enable this check box, an iOS device is allowed access if it passes any of the Require and Enforce policies. The Cache Cleaner policy does not apply to iOS devices.
5. Click **Save Changes**.

© 2020 Pulse Secure, LLC.

Installing Pulse Mobile Client for Apple iOS App

Pulse Mobile Client is available in the iTunes App Store. After installing the Pulse Mobile Client app, a user can manually configure it.

1. On the iOS device, launch Pulse Mobile Client.
2. Tap the Configuration item on the main status page to display Pulse Mobile Client configurations.
3. Create a new configuration with the URL. The URL for the connection is the Pulse Connect Secure sign-in URL that was created and defined for mobile devices. Then configure the certificate settings as required.

Note: For certificate authentication, the Pulse Connect Secure SSL certificate must be issued by a CA. It cannot be self-signed. If the CA is not one of the built-in trusted CAs on the iOS device, then the CA certificate must be imported into the iOS device. Also, the Pulse Connect Secure must be accessed using a hostname (not an IP address), and the hostname must match the Common Name of the Pulse Connect Secure SSL certificate.
For information on apple security standards to connect VPN, refer https://support.apple.com/en-in/HT210176#.

Using iPhone Configuration Utility Profiles for Pulse Mobile Client for iOS

One method of creating VPN configurations is to use a Configuration Profile to define Pulse Mobile Client configurations for the iOS device, and then distribute the configuration profiles by e-mail or by posting them on a Web page. When users open the e-mail attachment or download the profile using Safari on their iOS device, they are prompted to begin the installation process.

You use the iPhone Configuration Utility to create configuration profiles and specify Pulse Secure SSL as the Connection Type for the VPN Payload. You can download the iPhone Configuration Utility (3.0 or later) from the Apple support Web. For details about the utility and how to create Configuration Profiles, see the *iPhone OS Enterprise Deployment Guide*, available from the Apple website (www.apple.com).

Collecting Log Files from Pulse Mobile Client for iOS

The iOS device user can use the following procedure to e-mail the Pulse Mobile Client log files:

1. On the iOS device, start the Pulse Mobile Client app.
2. Navigate to support -> share email or share with other medium.
3. Enter an e-mail address, then tap **Send**.

© 2020 Pulse Secure, LLC.

Launching Pulse Mobile Client for iOS App with a Command

The Pulse Mobile Client launcher for iOS is a command that is registered with iOS when the mobile device user installs Pulse Mobile Client for iOS app. The Pulse Mobile Client launcher starts (or stops) Pulse Mobile Client and can establish a VPN connection using connection parameters specified in the command. The command can specify all login parameters. If the app generates or accesses an appropriate passcode, Pulse Mobile Client starts and establishes a VPN connection with no input from the user. You can use the Pulse Mobile Client launcher command in Web pages and external apps.

When a user taps a button that is tied to a Pulse Mobile Client launcher command, the command launches the Pulse Mobile Client app if it is not already running. If Pulse Mobile Client is not already installed on the iOS device, an error occurs. The next step depends on the current Pulse Mobile Client connection status and configuration. One of the following occurs:

- If Pulse Mobile Client does not already have an active connection to Pulse Connect Secure, it uses an existing configuration to establish the VPN connection.
- If Pulse Mobile Client does not already have an active connection, and it does not already have a configuration for the target Pulse Secure server, Pulse Mobile Client opens the Add Configuration screen. The target URL is already defined and the user just needs to specify a name for the connection.
- If the Pulse Mobile Client app is already connected to a Pulse Secure server, the Pulse Mobile Client app is brought to the foreground.

To employ the Pulse Mobile Client launcher in your Web pages or external applications, specify the link using the following format:

```
pulsesecure://<server-host>/<server-path> ?method={vpn} &action={start|stop} &DSID=<dsid-cookie> &SMSESSION=<smsession-cookie> &username=<username> &password=<password> &realm=<realm> &role=<role>
```

Usage notes:

- If the DSID cookie is given in the URL, the app does not use the "username", "password", "realm", or "role" parameters because no login is required.
- The values for username, realm, and role are URI-escaped values. Special characters are replaced with their hexidecimal equivalents preceded by '%'.
- If the user has specified the username, realm, and role when creating the VPN configurations in the Pulse Mobile Client app, those values are used to auto-fill the username, realm, and role for the login pages during a Web-based login. During login, if all fields are successfully auto-filled from fields in the VPN configuration or the pulsesecure:// launch URL, the login progresses without any user input. The username, realm, and role values need to already exist in the VPN configuration for them to be auto-filled during the login process. If the user manually specifies the username, realm, or role during login, the app will not add or update these values in the VPN configuration. The user needs to explicitly update the VPN configuration with these values.
- The Pulse Mobile Client app does not save the password in the Password field in VPN configurations. The Pulse Mobile Client app does not use values from Password fields in VPN configurations installed by the iPhone Configuration Utility. Pulse Mobile Client will only use passwords specified in pulsesecure:// URLs.

© 2020 Pulse Secure, LLC.

- If the user manually specifies the username, realm, or role during login, the app stores these values in the VPN configuration and they will be auto-filled the next time the user signs in. Passwords entered by the user are not saved in the VPN configuration.
- Realm and role fields in the VPN configuration format are supported in Apple iOS 4.2 and later. If the Pulse Mobile Client app is run on an iOS device running iOS 4.1, the realm and role fields will not be visible in Pulse Mobile Client Add/Edit configuration view.

Examples:

If the calling application has already obtained a DSID cookie from Pulse Connect Secure, the app can use the following command to start the VPN:

```
pulsesecure://<server-host>/<server-path> ?method=vpn &action=start &DSID=<dsid-cookie>
&SMSESSION=<smsession-cookie>
```

If the calling application does not already have a DSID, it can use the following command to start the VPN:

```
pulsesecure://<server-host>/<server-path> ?method=vpn&action=start &username=<username>
&password=<password> &realm=<realm> &role=<role>
```

If the calling application wants to stop the VPN, it can use the following command:

```
pulsesecure://<server-host>/<server-path> ?method=vpn &action=stop
```

Pulse Mobile Client for iOS Error Message Reference

The following error message summary for Pulse Mobile Client for iOS describes possible issues and suggests resolution actions where possible.

© 2020 Pulse Secure, LLC.

Table 1 Pulse Mobile Client for iOS Error Messages

Message	Possible Causes	Suggested Actions
Please provide values for all the fields	A required field was not provided.	Provide a value for all the required fields and then try the operation again. Contact your mobile security provider.
A configuration with the same name already exists. Please choose a different name.	Configuration names must be unique.	Choose a configuration name that is not in use by another configuration, and then try the operation again.
An internal error occurred while creating the configuration.	An undefined error occurred.	Verify all of the values you entered, and then try the operation again. If the error occurs again, contact the Pulse Mobile Client administrator.
Please contact your administrator.	Host Checker policy failed and the reason string is displayed for the failure.	Tap the **Cancel** button and then try again after performing the remediation actions.
Your device is running operating system version x.y.z.	The iOS version running on the device is not allowed to connect.	If prompted to continue, tap **Continue** to connect with limited connectivity or tap **Cancel** to cancel the connection and try again after upgrading iOS.
Your iOS device is jailbroken.	Jail broken iOS devices are not allowed to connect.	If prompted to continue, tap **Continue** to connect with limited connectivity or tap **Cancel** to cancel the connection.
Host Checker is not supported with this version of Pulse Mobile Client. Please upgrade Pulse Mobile Client or contact your administrator.	Unsupported Pulse Mobile Client - Pulse Mobile Client Host Checker is supported on Pulse Mobile Client 3.2 and later.	Check for the update of Pulse Mobile Client on the App store and upgrade Pulse Mobile Client to 3.2 or later, and then try again.
Session disconnected due to invalid certificate.	Pulse Mobile Client downloads session information from the Pulse Secure server and the certificate received from the server does not match the stored session certificate.	Click the **Close** button on the Alert dialog to return to home screen. The user can retry the connection.
Failed to connect to the server.	Sign-in process failed.	Check the network connection (for example, Wi-Fi, 3G, etc.), and then retry the connection.
Compliance Check couldn't be completed.	Host Checker compliance check couldn't be completed during sign-in process.	Try to connect again.

Configuring Secure Mail

For iOS devices, you can configure Secure Mail to:

- Use ActiveSync to synchronize e-mails with a Microsoft Exchange server
- Encrypt the e-mail body and attachments

© 2020 Pulse Secure, LLC.

- Block access to e-mail for lost or stolen devices, and erase all e-mails on the device
- Support back-end redirection, where an Exchange ActiveSync server redirects the client to another Exchange server

For other devices, an authorization-only sign-in policy can be defined that supports all of the Secure Mail features, except encryption.

Secure Mail is enabled in the user role, and requires a resource profile to specify the Exchange server and encryption options. In addition, an S/MIME certificate must be imported to Pulse Connect Secure.

For iOS devices that use Secure Mail, Pulse Mobile Client must be installed during onboarding. Onboarding downloads the ActiveSync profile to the device, along with any other profiles defined for enterprise onboarding. Profiles are signed by the Pulse Connect Secure device certificate, which must be trusted by the client device.

Enabling Secure Mail at the Role Level

To use Secure Mail for iOS devices, you must enable it at the user role level and then create a resource profile that specifies the mail server and encryption settings.

Note: Do not enable both Secure Mail and Email Client options in the same role. To disable Secure Mail for a role, you must first block e-mail access for all devices that are currently onboarded with this role (see Managing Onboarded and ActiveSync-Only Devices).

To enable Secure Mail for a user role:

1. In the admin console, choose **Users > User Roles > [RoleName] > General > Overview**.
2. In the "Enterprise Device Onboarding" section, select the **Secure Mail** check box.
3. Click **Save Changes**.
4. Click **Options** next to the **Secure Mail** check box to view or change the resource profile for Secure Mail (see “Defining the Secure Mail Resource Profile” on page 14).

Defining the Secure Mail Resource Profile

To use Secure Mail for iOS devices, you must enable it at the role level and then create a resource profile that specifies the Exchange server and encryption settings. You must also obtain and import an S/MIME certificate (see “Obtaining an S/MIME Certificate” on page 15).

To define the Secure Mail resource profile:

1. In the admin console, choose **Users > Resource Profiles > Mobile**.
2. Specify the information in the following table:

© 2020 Pulse Secure, LLC.

Table 2 Secure Mail Resource Profile settings

Setting	Description
Virtual Hostname	Enter a hostname alias for the Exchange server, and update your DNS server to map the alias to the IP address of Pulse Connect Secure. The name must be unique among all virtual hostnames. For example, if the virtual hostname is email.com, and the backend URL is https://mail.pulsesecure.net:8080, a client request to https://email.com/test1 via Pulse Connect Secure is converted to https://mail.pulsesecure.net:8080/test1. The response to the converted request is sent to the client web browser.
Exchange Server	Enter the URL and port number of the Microsoft Exchange server, such as https://mail.pulsesecure.net:379. If the port number is omitted, it defaults to 80.
Description	Description of the Exchange server (optional).
Username	Select one of the following to specify the e-mail account format used by the Exchange server: • **None**: Inserts the <USER> variable for the user's login name for Pulse Connect Secure (the default). • **Exchange 2007/2010/2013**: Inserts the <NTDOMAIN>\<USER> variables to include the user's domain before the login name. • **Office 365**: Inserts <USER>@domain.com, and you can enter the appropriate domain, such as <USER>@pulsesecure.net.
Secure Mail Options	Select one or more of the following encryption options: • **Encrypt Body**: Encrypts the body of the e-mail using an S/MIME certificate. The encrypted e-mail body can be viewed by any native e-mail client. Note: Graphics embedded in the encrypted e-mail body are displayed twice on iOS devices. • **Encrypt Attachments**: Encrypts the e-mail attachments using a key generated by Pulse Connect Secure. Encrypted attachments, which must be opened with Pulse Mobile Client, are identified by a pulsesecure file extension, such as report.pdf.pulsesecure. The encrypted file types are listed in the File Extensions text box, separated by semhicolons. You can add or delete file extensions from the list. Note: If you add .gif, .jpeg, .jpg, .png or .htm to the list of encrypted file types, graphics embedded in the e-mail body are not displayed correctly on iOS devices. • **Allow Outbound E-Mail Attachments**: Decrypts attachments before forwarding an e-mail to an external account. If this option is not selected, e-mails are forwarded without attachments and include a note indicating that attachments were removed. If you change the encryption settings, onboarded devices must be re-onboarded to obtain the new settings.

3. Click **Save Changes**.

Obtaining an S/MIME Certificate

If you enable Secure Mail, an S/MIME is required for each client device. You can generate an S/MIME certificate for each device or use a global certificate for all devices by requesting an S/MIME certificate from a Certificate Authority (CA) and importing the certificate and private key to Pulse Connect Secure.

© 2020 Pulse Secure, LLC.

To generate or import an S/MIME certificate:

1. In the admin console, choose **Users > Resource Profiles > Mobile > S/MIME Certificate**.
2. Specify one of the following options:

Table 3 S/MIME certificate options

Setting	Description
Generate per User Certificate	Select this option to use the SCEP server and a CSR template to generate a certificate for each client. Select a CSR template from the Use Certificate Template list. To create a CSR template, see Configuring Enterprise Onboarding.
Upload and Use Single Global Certificate	Select this option to use the same certificate for all client devices. Click **Import Certificate & Key**, click **Browse** in one of the following forms to locate the certificate file, enter the password key if the file is encrypted, and then click **Import**. • **If certificate file includes private key**: When the certificate and key are contained in one file. • **If certificate and private key are separate files**: When the certificate and key are in separate files. • **Import via System Configuration file**: When the certificate and key are contained in a system configuration file that has been exported from Pulse Connect Secure.

Note: The **Import Certificate & Key** button is disabled on FIPS hardware platforms because importing private keys is not allowed. On a FIPS hardware platform, you must create a CSR and then import a signed certificate from the CA.

Configuring an Authorization-Only Policy for ActiveSync

An authorization-only policy can be defined to allow almost any device to use ActiveSync to synchronize e-mails with a Microsoft Exchange server. Encryption is not supported, but if the option to allow only ActiveSync traffic is enabled, e-mail access can be blocked for devices that are lost or stolen, and back-end redirection is supported (the Exchange ActiveSync server can redirect the client to another Exchange server).

To configure an authorization-only access policy for ActiveSync:

1. In the admin console, choose **Authentication > Signing In > Sign-in Policies**.
2. To create a new authorization-only access policy, click **New URL** and select **Authorization Only Access** for the user type. Or, to edit an existing policy, click **Secure Mail** next to a URL in the "Virtual Hostname" column.

Note: If a resource profile for Secure Mail is defined, the virtual hostname is displayed with a link to the resource profile. The virtual hostname for the authorization-only policy must be different from the Secure Mail virtual hostname.

3. Specify the information in the following table:

Table 4

Setting	Description
Virtual Hostname	Enter a hostname alias for the Exchange server, such as email.com, and update your DNS server to map the alias to the IP address of Pulse Connect Secure. The name must be unique among all virtual hostnames. Do not include the http(s) protocol.For example, if the virtual hostname is email.com, and the backend URL is https://mail.pulsesecure.net:8080, a client request to https://email.com/test1 via Pulse Connect Secure is converted to https://mail.pulsesecure.net:8080/test1. The response to the converted request is sent to the client web browser.
Backend URL	Enter the URL and port number of the Microsoft Exchange server, such as https://mail.pulsesecure.net:8080. If the port is omitted, it defaults to 80.
Description	Description of the Exchange server (optional).
Authorization Server	Select the authorization server name or No Authorization. If you select a server, ensure that the front-end server provides the SMSESSION cookie otherwise you will receive an error.
Role Option	Select a user role. The role must have a Web Access policy, and only the following role options apply: • Allow browsing untrusted SSL web sites (**Users > User Roles > [RoleName] > Web > Options > View advanced options**) • HTTP Connection Timeout (**Users > User Roles > [RoleName] > Web > Options > View advanced options**) • Source IP restrictions (**Users > User Roles > [RoleName] > General > Restrictions**) • Browser restrictions (**Users > User Roles > [RoleName] > General > Restrictions**)
Protocol Option	Select the **Allow ActiveSync Traffic only** option to verify the request is consistent with the ActiveSync protocol, and to include the device on the Device Management page, which allows e-mail access on the device to be blocked if needed. If validation fails, a message is created in the user's event log. If you do not enable this option, both ActiveSync and non-ActiveSync requests are processed, but the device is not shown on the Device Management page.

4. Click **Save Changes** to save your edits.

   The "System Status Overview" page displays the number of current ActiveSync and authorization-only connections, and a histogram of the active concurrent connections ("Authorization Only Access Active Connections" plot in the Concurrent SSL Connections graph).

Using Pulse Client with PZTA

Pulse Secure provides a PZTA-ready version of the Pulse Client software required for end-user devices to be able to connect to your secure applications and resources.

Pulse Client connects to PZTA services, by default, through an on-demand connection basis and can handle multiple simultaneous PZTA and non-PZTA connections. To learn more, see On-Demand and Simultaneous Connection Handling.

© 2020 Pulse Secure, LLC.

Pulse Client maintains communication with the PZTA Controller to continuously-enable synchronization of policy and configuration updates. Through this mechanism, user requests to access resources and applications are subject to continuous assessment for risk and authorization. For more details, see Dynamic Policy Update and CARTA.

To learn more about enrolling user devices for use with PZTA, see Enrolling a User Device.

On-Demand and Simultaneous Connection Handling

While active, Pulse Client maintains two connection channels for PZTA services, a control channel to the PZTA Controller, and a data channel to your PZTA Gateways. For more details on networking considerations when deploying Gateways, see Working with Gateways.

The control channel connection to the PZTA Controller is activated when Pulse Client is started up and remains in an always-on state, silently in the background. If Pulse Client is able to locate a valid session cookie from an earlier session, the connection is re-established automatically. If no valid cookie is present, Pulse Client requests re-authentication from the user. The PZTA Controller connection is terminated when Pulse Client is shut down.

Pulse Client creates data channel connections to PZTA Gateways as an on-demand service. That is, connections to resources and applications controlled by PZTA Gateways become active only when required, and the connection is suspended after a period of inactivity. The user remains unaware of the connection state, unless re-authentication becomes necessary. As a user makes a request for a resource, Pulse Client transitions automatically from disconnected to connected. The connection remains in this state for the duration of the session, or until one of the following events occurs:

- An idle time-out occurs (after 5 minutes)
- The connection is actively placed in a disconnected state
- Pulse Client is shut down

To avoid the data channel being reconnected unnecessarily, non-PZTA DNS traffic is redirected to the device's physical network adapter.

Applicable Pulse Client versions can manage simultaneous connections with the PZTA Controller, and with other Pulse Secure services such as Pulse Connect Secure (PCS). While PCS connections must be activated and deactivated by the user, connections to PZTA are provided on-demand, as mentioned. Therefore, a PZTA connection in the Pulse Client does not provide the same **Connect** and **Disconnect** controls. Instead, PZTA connections include only a **ZTA** button to provide access to the PZTA Applications page. If this button is active, the connection to the Controller has been established. If the button is inactive, the connection to the Controller has not yet been established, or a communication problem has occurred. In this case, access to your applications is prevented.

When running active connections to both PZTA and PCS simultaneously, note that the following PCS features are not supported:

- Route Monitoring
- Traffic Enforcement
- Stealth Mode
- Always on VPN/LockDown
- Location awareness

© 2020 Pulse Secure, LLC.

- IPv6 support

Disabling the PZTA Connection

Pulse Client additionally provides the ability to actively disable the on-demand connection feature. Use of this facility disables the PZTA connection, avoiding the scenario where Pulse Client attempts to repeatedly request authentication even after the user might be unable to authenticate due to too many failed attempts, or where the user just does not require access to any PZTA-controlled resources during that session.

If a user attempts to request a PZTA-controlled resource during the period a PZTA connection is disabled, the request fails. Other Pulse Client connections are unaffected.

For Pulse Client on iOS devices, use the **Disconnect** option in the Pulse Client application. Open Pulse Client, locate the PZTA connection profile, and tap the **Disconnect** button.

By setting the PZTA connection to be disconnected, Pulse Client suspends both the control channel and the data channel (where either are active). If the control channel was previously logged-in to the PZTA Controller, this remains the case to facilitate session resumption through a subsequent reconnect.

The disconnect feature is not activated by clicking or tapping Cancel in the PZTA authentication dialog. Canceling an authentication request triggers a timeout interval, after which Pulse Client re-displays the authentication dialog. The disconnect feature instead disables the authentication request process until the user manually reinstates it.

To reinstate the PZTA connection on iOS devices, tap the ZTA button in the PZTA connection profile in the Pulse Client application:

If the existing session cookie is still valid, the control channel is re-established. If the session is now invalid, Pulse Client prompts the user for their PZTA credentials as normal. On successful re-establishment of the PZTA session, the user is presented with the PZTA End User Portal in the default browser.

When restarting Pulse Client, PZTA connections default to being on-demand services. That is, a previously disabled PZTA connection is re-enabled when Pulse Client starts.

Dynamic Policy Update and CARTA

To complement the zero-trust approach, PZTA supports dynamic policy updates and CARTA (Continuous Adaptive Risk and Trust Assessment) for your end user devices. This framework establishes an approach of continuous assessment and updating of secure access policies on the client, without the requirement to disconnect and reconnect to establish an updated authorization posture.

As your policies, applications, and authentication configuration are updated by the administrator on the PZTA Controller, changes are synchronized out to client devices dynamically and take effect immediately. Pulse Client ensures that any application updates are applied and any new authentication requirements are met before continuing the session, providing the end user with a seamlessly-updated experience. This method ensures that Pulse Client is always updated at the point of change, and not just when establishing a connection to a PZTA Gateway to access an affected resource.

© 2020 Pulse Secure, LLC.

The CARTA implementation in Pulse Client means that the security posture of the end user is continuously assessed in conjunction with policies configured in the Controller, with allow or deny decisions enforced through dynamic assessment and updating of the current policy set. Where application access is denied or restricted, Pulse Client informs the user of any access restrictions or policy contravention at the point of use. For example, the PZTA Desktop Client Home page updates to provide visual cues with applicable error messages whenever a specific application becomes unavailable:

By hovering your pointer over the warning symbol in the inactive application, PZTA provides an explanatory message.

Furthermore, user attempts to access a restricted web resource in a browser trigger a CARTA response with Pulse Client presenting a pop-up resource blocked message:

Pulse Client implements a no-repeat interval for resource blocked messages of 2 minutes, to avoid a user repeatedly seeing the same pop-up message for every browser request for the same restricted resource. While the resource remains blocked to further access attempts, no further messages are displayed by Pulse Client until after 2 minutes has elapsed. You can force Pulse Client to continue hiding blocked resource messages indefinitely by right-clicking the connection in the Pulse Client dialog and selecting Disable Block Messages. To re-enable showing blocked resource messages, select Enable Block Messages.

Enrolling First Time Users

When enrolling a new device, an authorized user contacts the PZTA Controller to activate an initial first-time enrollment of their client device. The Controller responds to a valid enrollment request by activating a download of Pulse Client along with a suitable client certificate.

After Pulse Client is installed, a secure connection request is attempted with the Controller. The request is validated against the designated authentication policy applicable to that combination of user and device and, where successful, a connection profile is downloaded to the client. This profile enables Pulse Client to set up a secure tunnel directly to the PZTA Gateway serving the resource set the client is authorized to view.

Enrolling Existing PZTA Users

After you have enrolled the new device, Pulse Client is installed and configured with the policies and settings relevant to the device type. Your application and resource access rights should be duplicated to the new device.

Note: If a user device is currently using a Beta version of the PZTA-ready Pulse Client, Pulse Secure advises to remove the PZTA connection from Pulse Client and to re-perform the enrollment procedure through a web browser. For more details, see your support representative.

© 2020 Pulse Secure, LLC.

© 2020 Pulse Secure, LLC.