



## Pulse Mobile

### Android for Work Guide

#### Pulse Secure Android application

Document Revision 2.0  
Published: 2016-04-15

Pulse Secure, LLC  
2700 Zanker Road, Suite 200  
San Jose, CA 95134  
<http://www.pulsesecure.net>

© 2016 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.

*Android for Work Guide*

The information in this document is current as of the date on the title page.

#### **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.

# Table of Contents

**Goal**----- 5

**Functionality** ----- 5

**Restrictions Schema**----- 5

*Description of Restrictions Entries* -----5

**Workflow** ----- 8

**Limitations** ----- 23

**Supported Devices** ----- 23

**Known Issues**----- 23

List of Figures

Figure 1 *Pulse Secure Android Application in Work profile* ----- 8

Figure 2 EULA – Pulse Secure Android Application ----- 9

Figure 3 VPN Connections ----- 10

Figure 4 View Connection – App VPN----- 11

Figure 5 Connections – VPN Profile----- 12

Figure 6 View Connection - Connection Name ----- 13

Figure 7 Select Connection ----- 14

Figure 8 Choose Certificate----- 15

## Goal

Goal of this document is to describe how Pulse Secure Android client functions in a Work profile created using Android for Work framework on a supporting Android device. It provides information about how a device policy client (DPC, also known as a Work Policy Controller) application can configure VPN profile. Pulse Secure Android application will be one of the managed applications within a Work profile. It defines and implements a restrictions schema that allows a DPC to configure VPN profile. Subsequent sections provide details on how this is done.

## Functionality

Use cases:

- Creating a VPN configuration using Android for Work restrictions framework.
- Authentication using username/password or dual auth or certificate in Android Keystore.
- Work profile VPN: Setting up VPN tunnel within the work profile. Only the applications within work profile sends data from VPN tunnel.
- Application VPN: Allowing select applications within the work profile to pass data from VPN tunnel.
- Split tunneling with Application VPN: Layer 3 routes on VPN interface functions the same way when application VPN is configured.
- Deleting a VPN configuration which was created using Android for Work restrictions framework.
- Setting a VPN configuration as default profile.

## Restrictions Schema

### Description of Restrictions Entries

- 1) `profile_name`  
It is VPN profile name. This is a mandatory field for supported actions on a VPN profile and must be unique for a particular VPN profile.  
Restriction type: string
- 2) `url`  
VPN server url. This is a mandatory field for “create” action.  
Restriction type: string
- 3) `action`  
Action required from Pulse Secure Android client when a restriction is applied by DPC.  
Restriction type: choice  
Possible values  
0: Create a VPN profile.  
1: Delete a VPN profile.  
2: Set a VPN profile as default
- 4) `authentication_type`  
Identifies the authentication type used in the VPN profile. This authentication type will be used while creating a connection with VPN server.  
Restriction type: choice  
Possible values

- 1: Certificate alias in certificate store. 2:  
User name, password authentication  
3: Dual authentication with two username/passwords or username/password and  
certificate
- 5) username  
Username when authentication\_type is set to username/password type. It is stored by Pulse Secure Android client and auto-filled during login process.  
Restriction type: string
  - 6) password  
Password when authentication\_type is set to username/password type. It will be auto-filled during login process.  
Restriction type: string
  - 7) username2  
Username2 when authentication\_type is dual auth. It is stored by Pulse Secure Android client and auto-filled during login process.  
Restriction type: string
  - 8) password2  
Password when authentication\_type is dual auth. It is stored by Pulse Secure Android client and auto-filled during login process.  
Restriction type: string
  - 9) cert\_alias  
Certificate alias for the certificate stored in Android keystore. DPC application is expected to store the certificate in the keystore for the work profile and pass the certificate alias to Pulse Secure Android client by setting restriction.  
Restriction type: string
  - 10) realm  
It's an optional parameter to specify the realm.  
Restriction type: string
  - 11) role  
It's an optional parameter to specify the role.  
Restriction type: string
  - 12) default  
Make a VPN configuration default  
Restriction type: bool
  - 13) route\_type  
VPN route type that is configured by Pulse Secure Android client.  
Restriction type: choice  
Possible values  
0: VPN tunnel is established for the work profile. Data for all applications within the work profile is routed from the VPN tunnel.  
1: VPN tunnel is established for the work profile but will only apply for certain applications. Pulse Secure Android client uses Android 5.0 Application VPN APIs to only allow certain applications to send data from the VPN tunnel. See the parameters to configure Application VPN.
  - 14) appvpn\_action  
Configure Application VPN action when establishing VPN interface.

This parameter is read only when route\_type is set for Application VPN.

Restriction type: choice

Possible values

0: Allow application packages configured using appvpn\_packages to use the VPN tunnel. Traffic for other application in the work profile goes outside the VPN tunnel, through WIFI or other interface.

1: Disallow application packages configured using appvpn\_packages to use the VPN tunnel.

15) appvpn\_packages

Android application package names that is allowed or disallowed for VPN tunnel access.

appvpn\_action parameter value provides the action taken for these application packages.

The parameter value needs to be a comm-separated string.

Example: "com.android.vending,com.android.chrome"

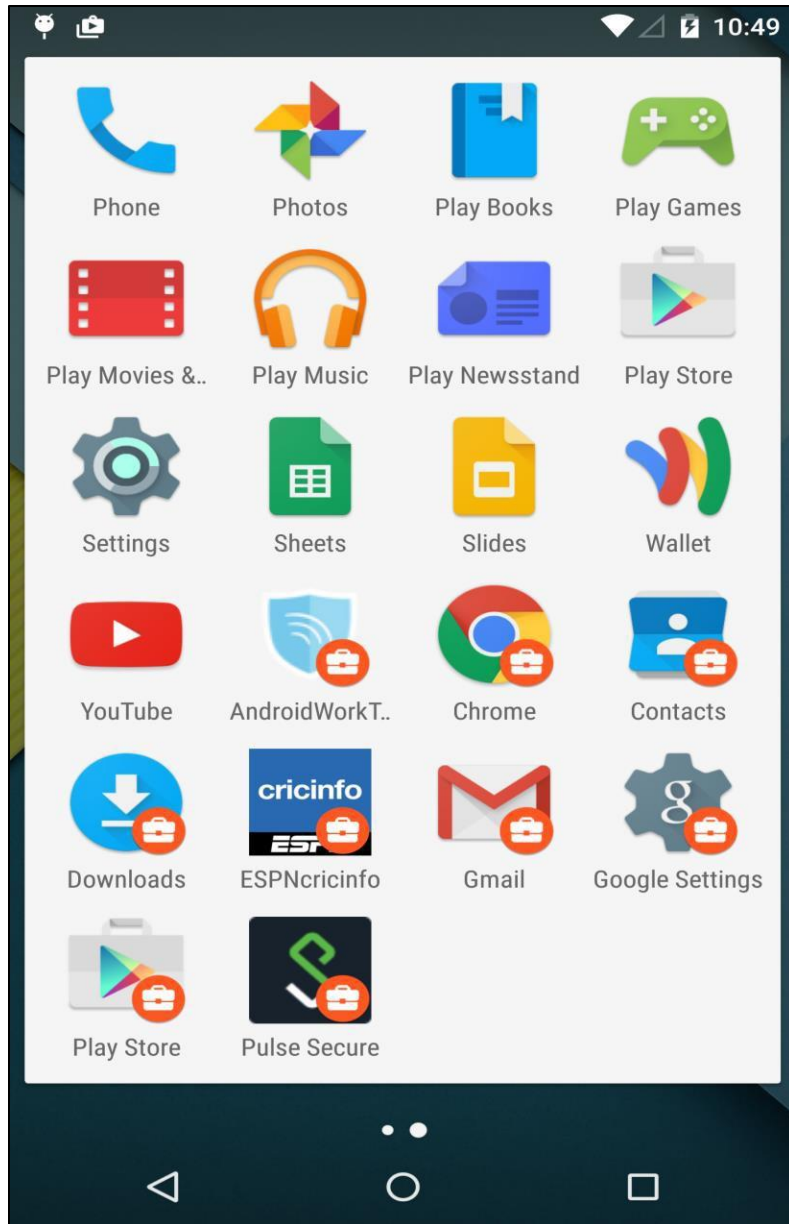
From this example, Google Play and Google Chrome applications are included. Google Play uses a separate Android package for downloading the applications and that will not be included.

Restriction type: string

## Workflow

1. Device Policy Client (DPC) application creates the work profile and installs Pulse Secure Android application as one of the managed applications within the work profile.

*Figure 1 Pulse Secure Android Application in Work profile*

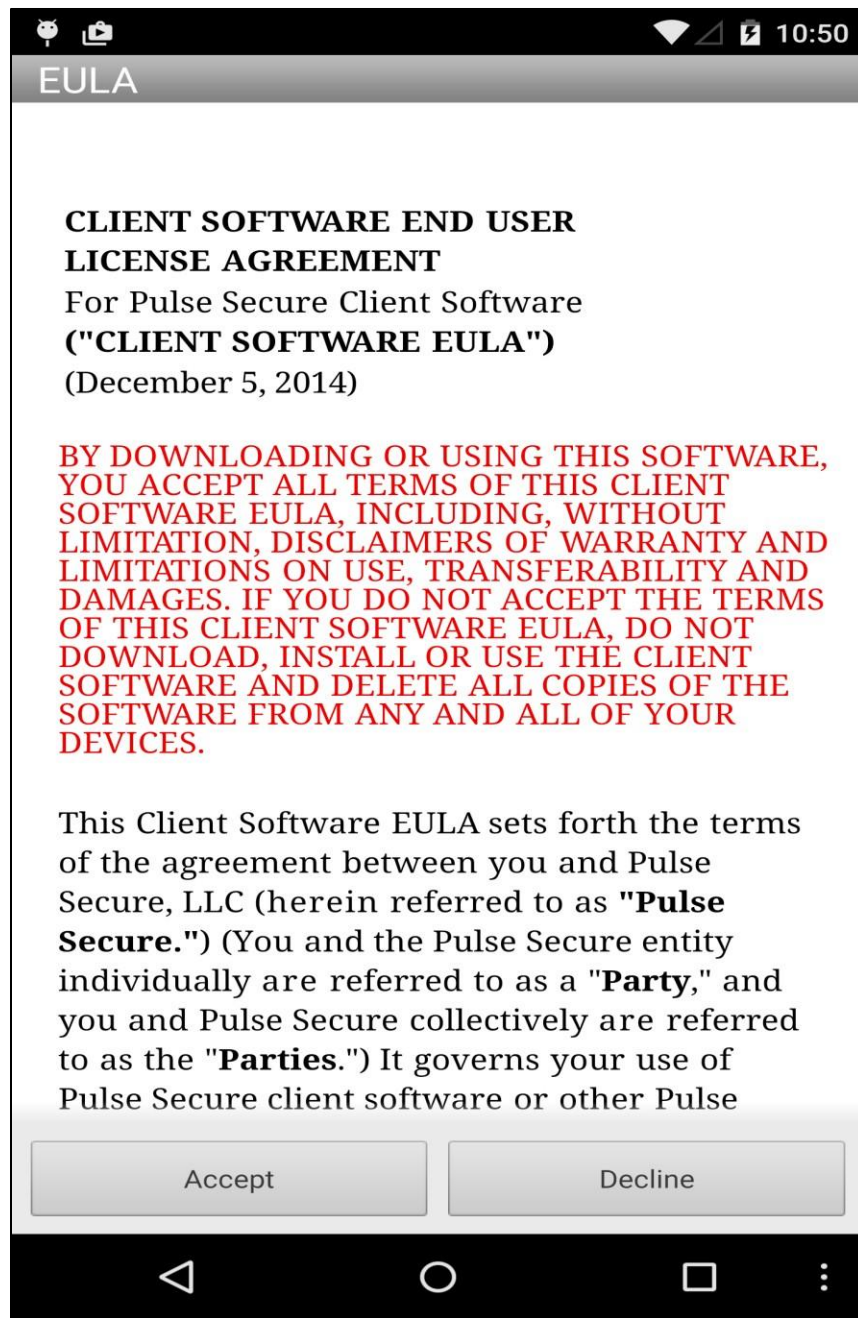


2. Pulse Secure Android application is launched.



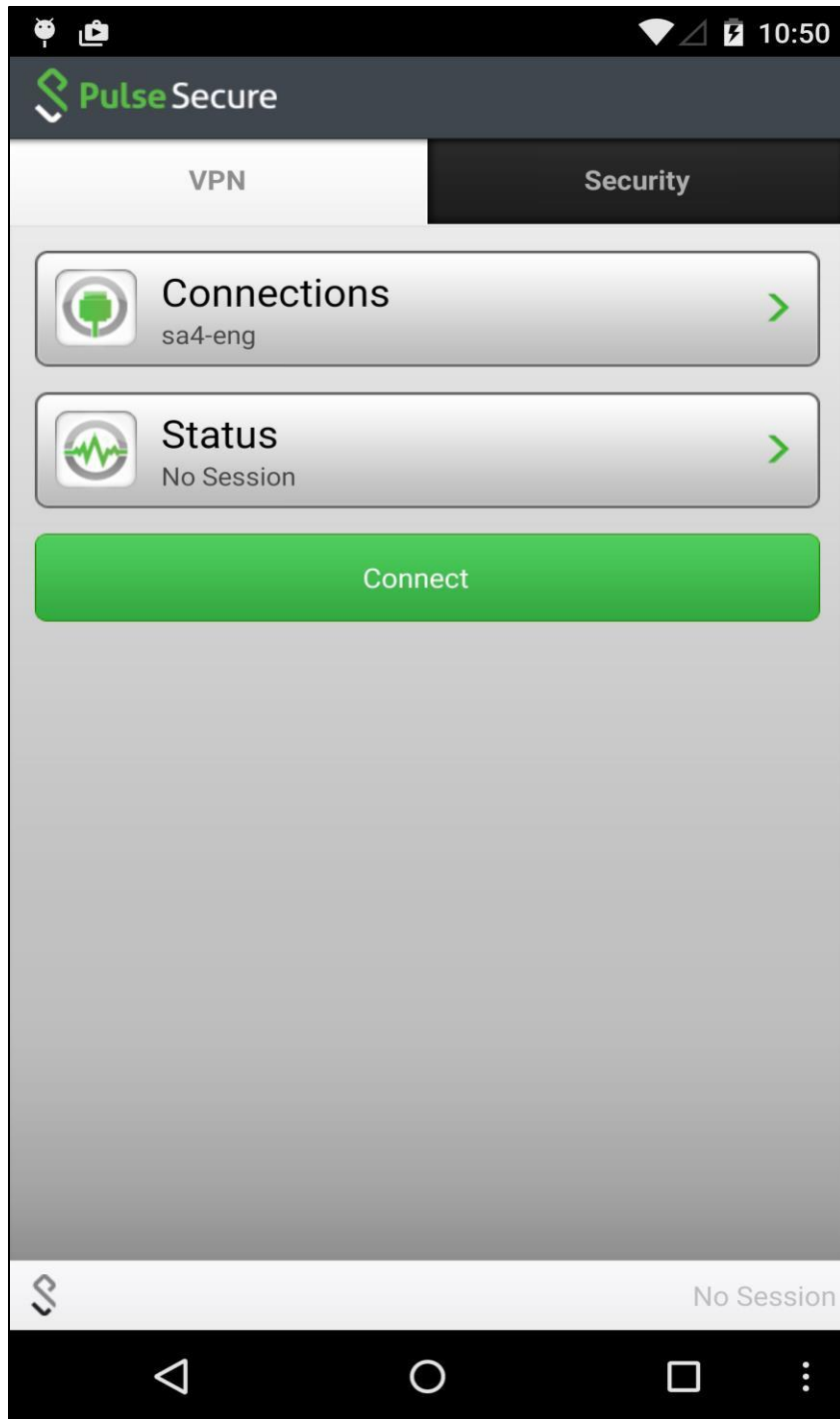
3. Pulse Secure Android application registers for a broadcast to listen for change in restrictions.
4. User accepts EULA in Pulse Secure Android application.

*Figure 2 EULA – Pulse Secure Android Application*



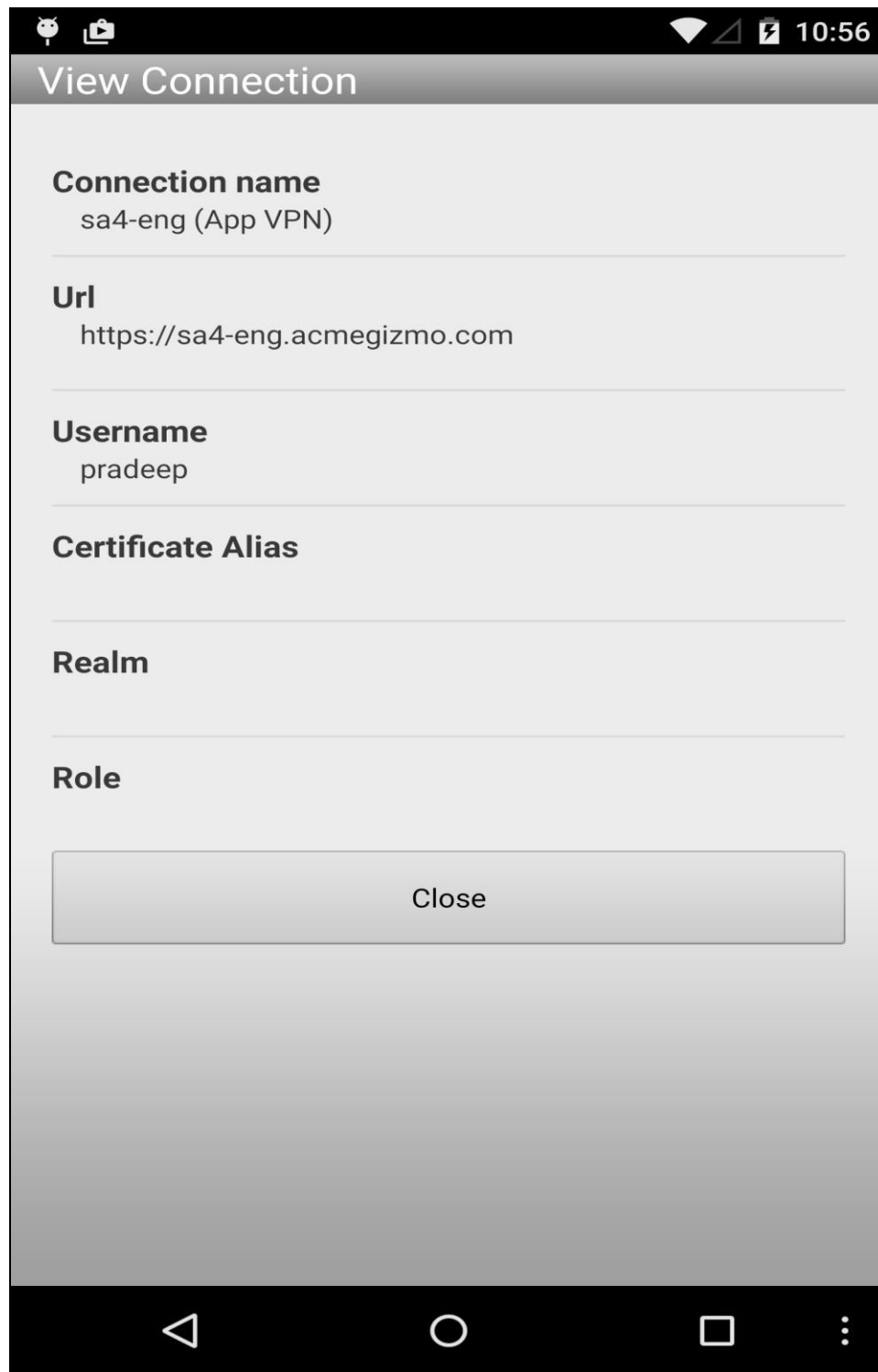
5. On VPN tab of home screen, Pulse Secure Android application calls `getApplicationRestrictions` API and this screen is created. If the DPC application has set restrictions for Pulse Secure Android application and the restriction is for creating a valid VPN profile. User Interface shows a VPN connection configured in the Connections button and screen.

Figure 3 VPN Connections



6. VPN connection profile configured from DPC application is not editable. When application VPN is configured, the connection name on Connection page shows 'App VPN' concatenated to the connection name.

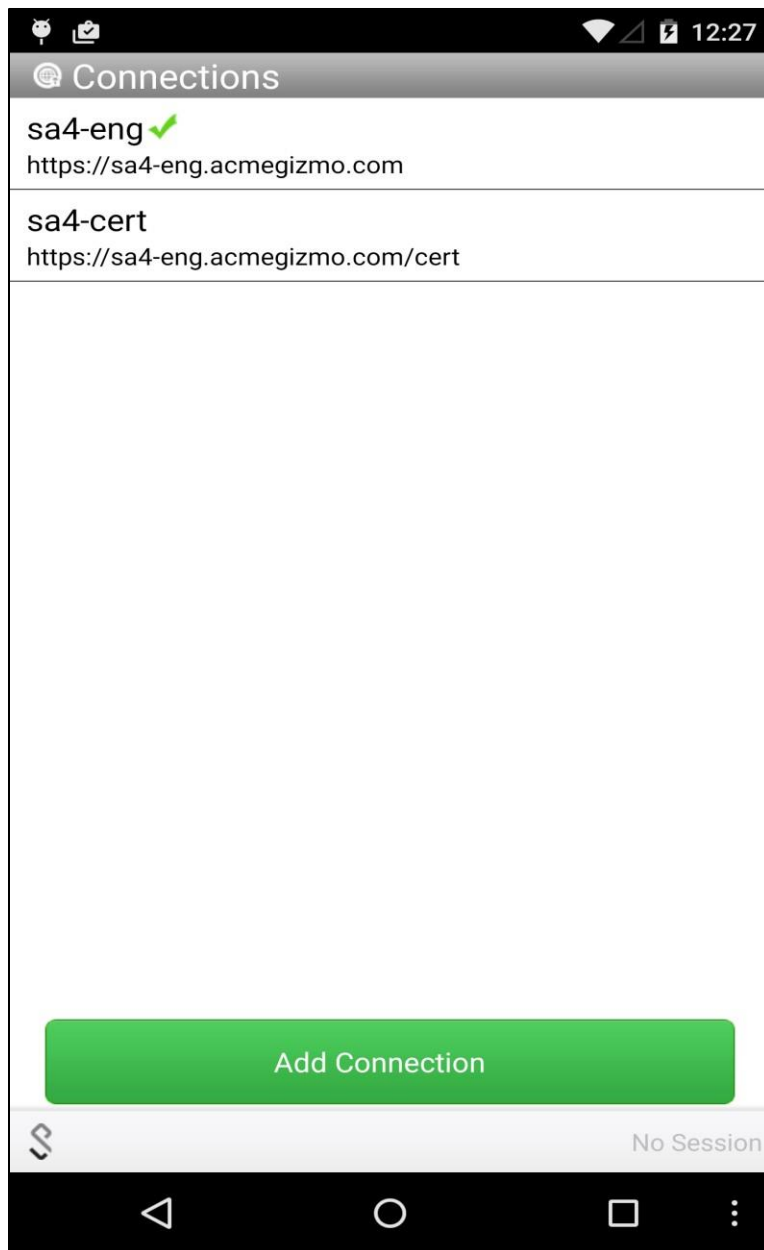
Figure 4 View Connection – App VPN



7. If DPC application applies new restrictions for Pulse Secure Android application, then it retrieves and applies those in background. Pulse Secure Android application need not be

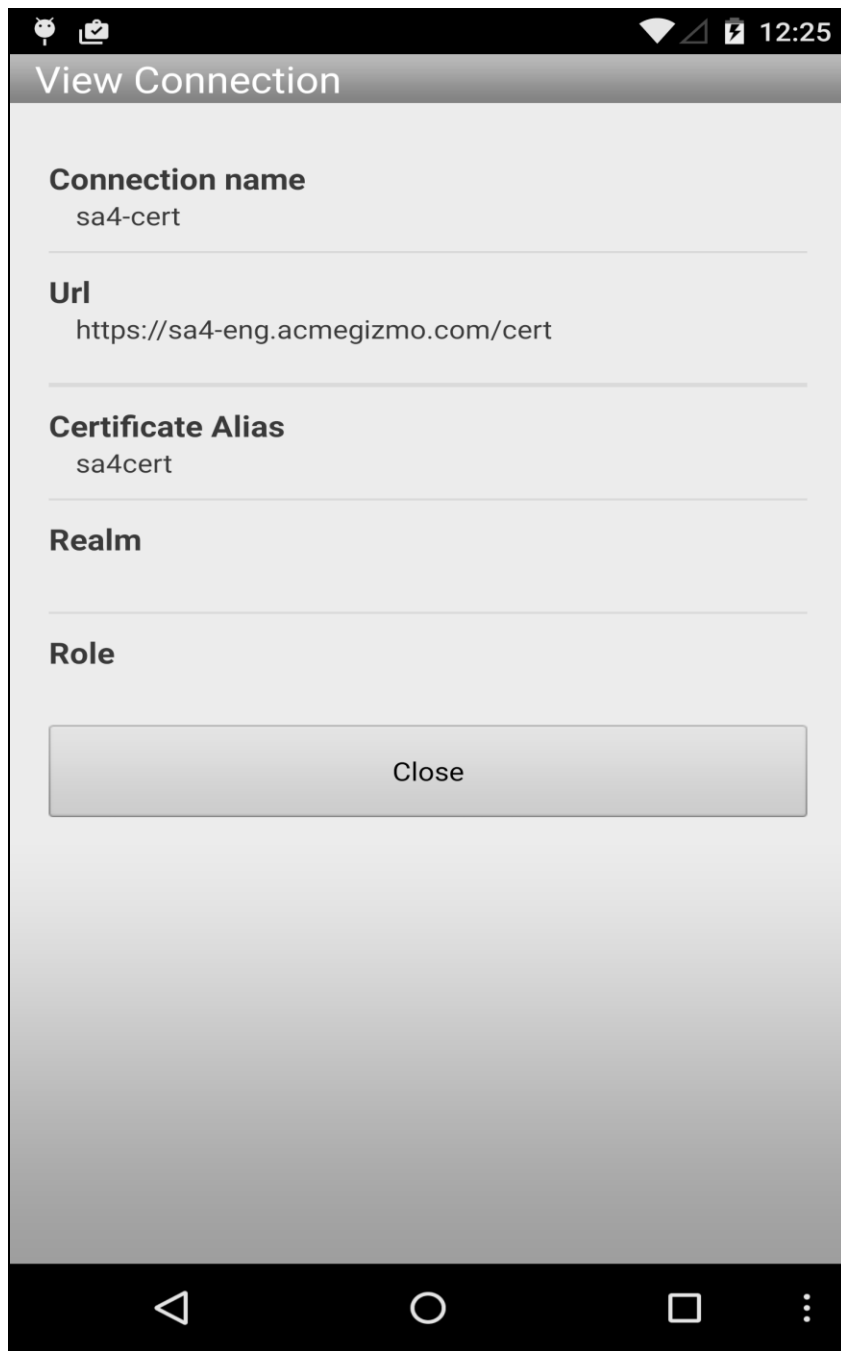
on the foreground to receive new restrictions. It needs to be running. The default VPN profile is not changed when a new profile gets added. You have to manually choose the correct VPN profile before making a connection.

*Figure 5 Connections– VPN Profile*



8. Click Connect to manually start the VPN connection. In case of certificate authentication, initial connection shows a dialog for approving Pulse Secure Android application to access the keystore and then a system dialog that has a pre-selected certificate alias. Click OK and proceed. In case of username/password authentication, password must be entered in the client Webview.

Figure 6 View Connection - Connection Name



The screenshot shows a mobile application interface with a black status bar at the top containing icons for Android, a clipboard, Wi-Fi, signal strength, battery, and the time 12:25. Below the status bar is a grey header with the text "View Connection". The main content area is light grey and contains several sections separated by horizontal lines. Each section has a bold label followed by a text value. At the bottom of the content area is a grey button with the text "Close". The bottom of the screen features a black navigation bar with four white icons: a back arrow, a circle, a square, and a vertical ellipsis.

Field	Value
Connection name	sa4-cert
Url	https://sa4-eng.acmegizmo.com/cert
Certificate Alias	sa4cert
Realm	
Role	

Close

Figure 7 Select Connection

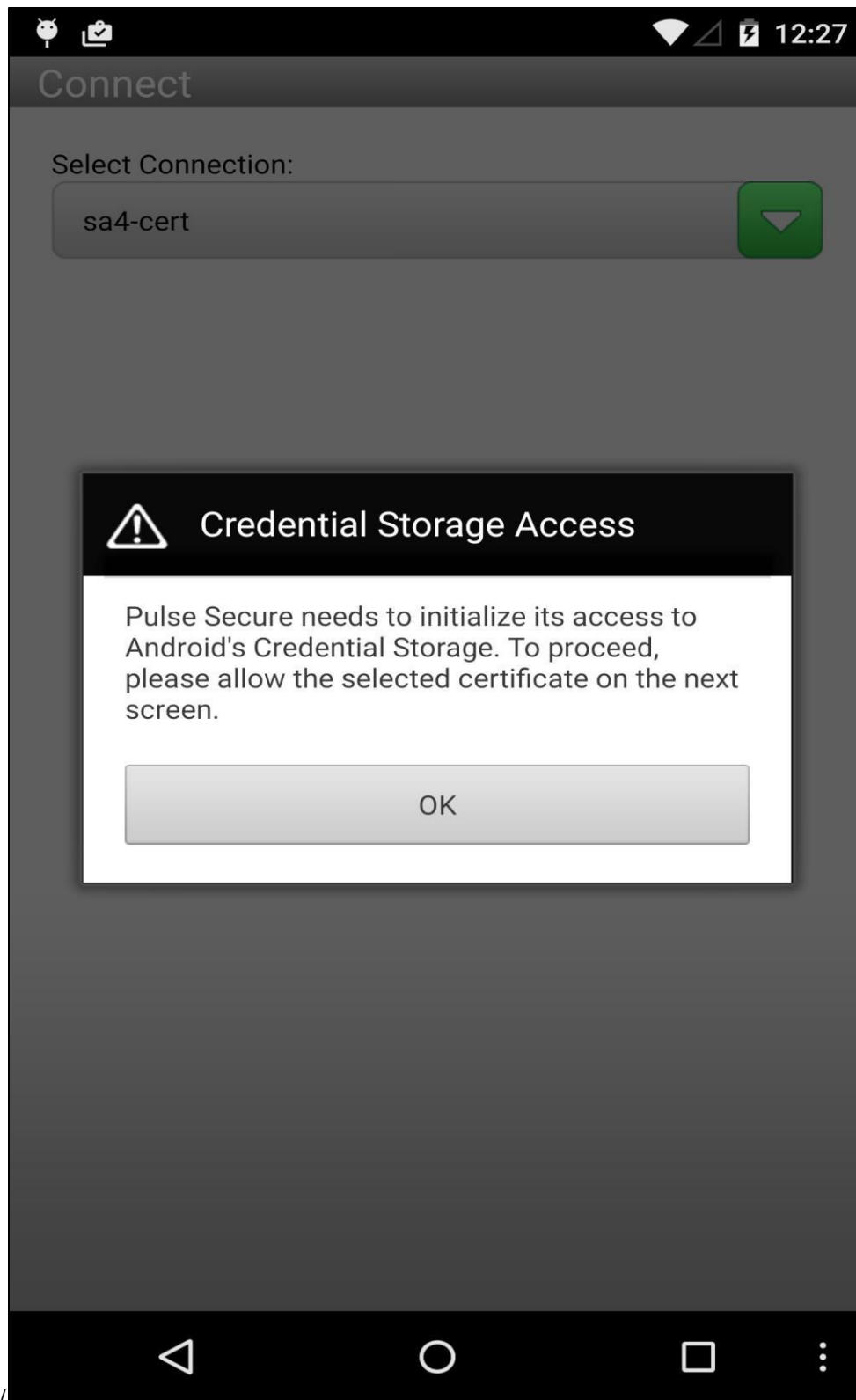
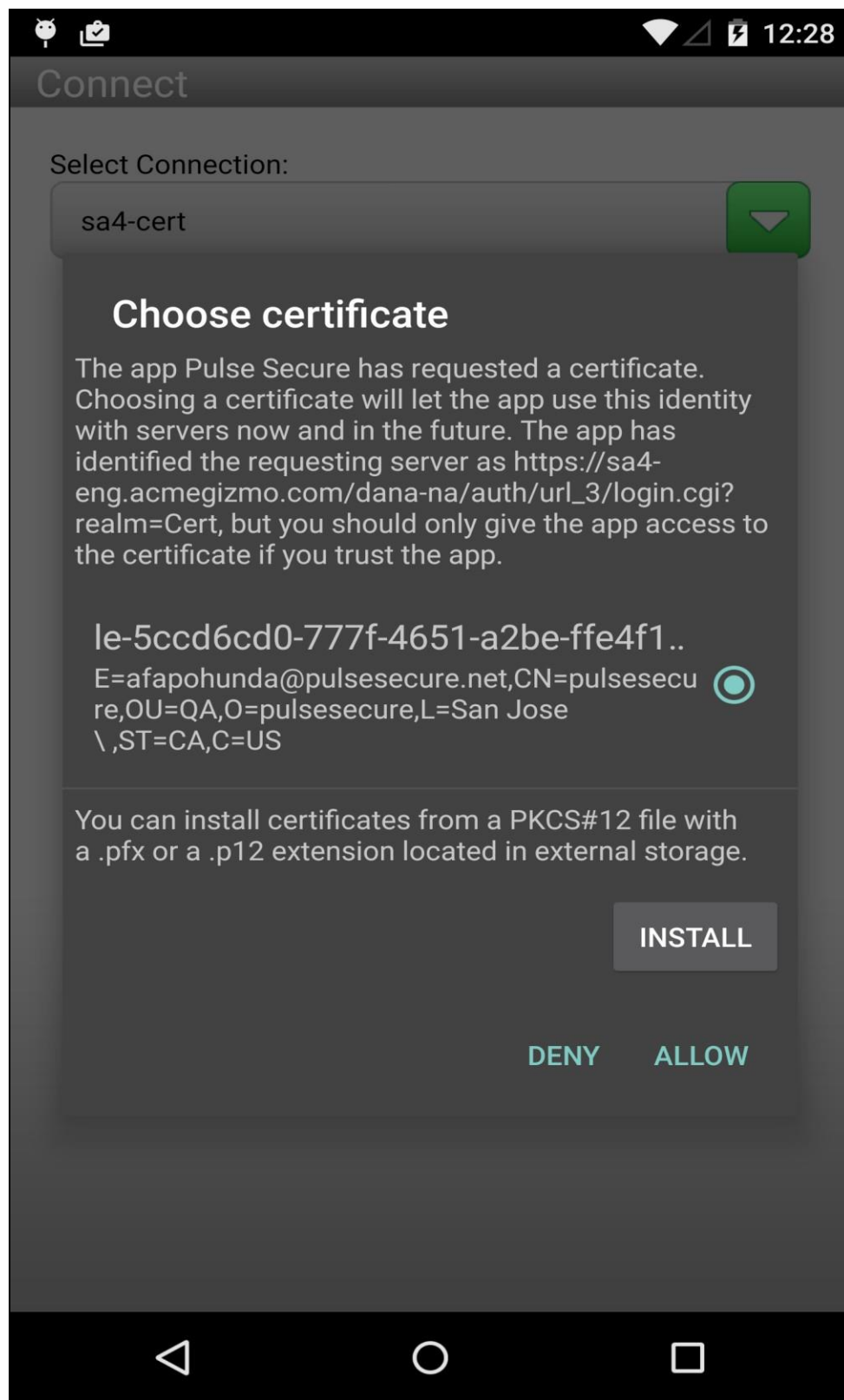
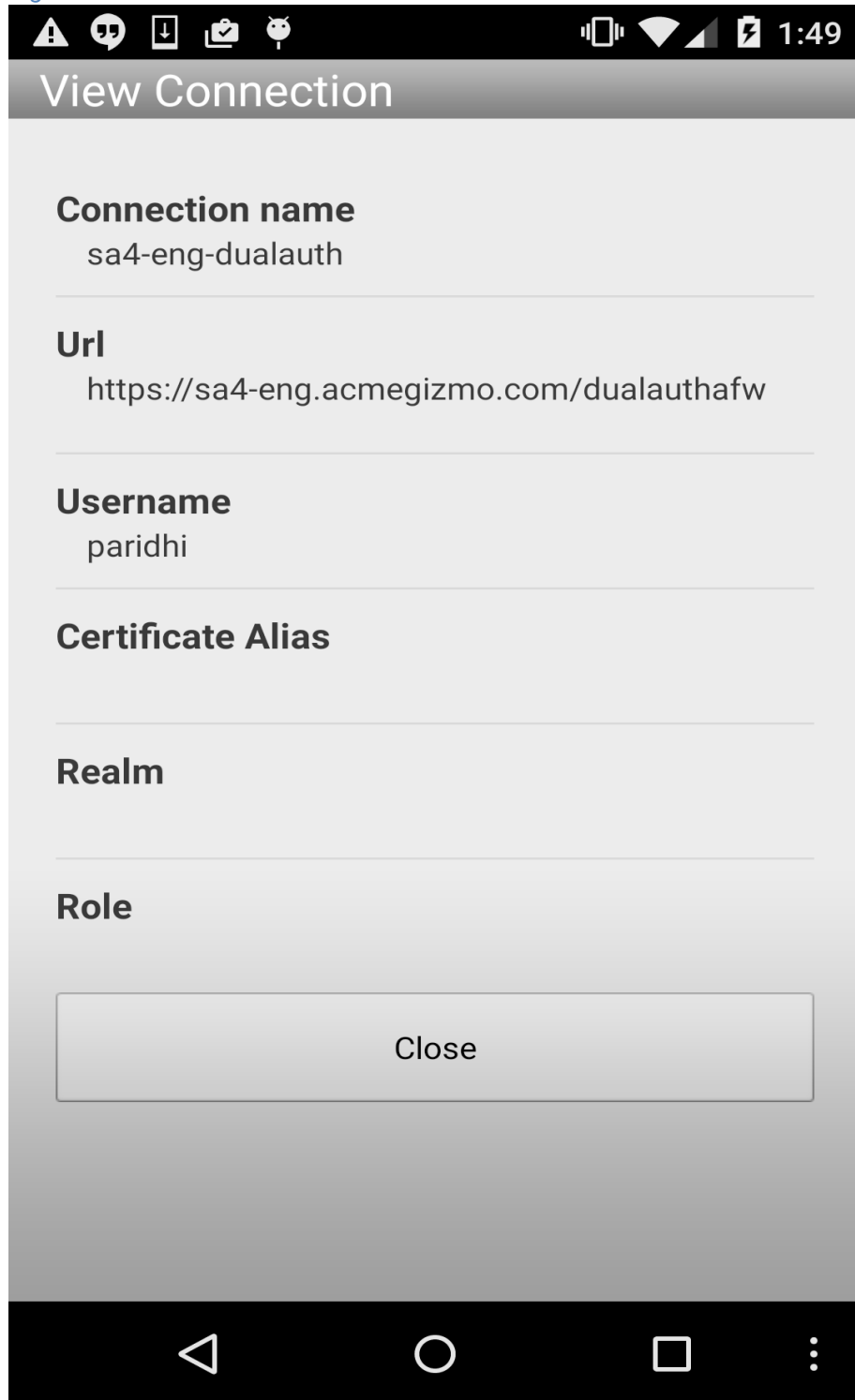


Figure 8 Choose Certificate



9. EMM providers can create two kinds of dual auth profiles.
  1. Two username/passwords
  2. 1 username/password and 1 certificate

*Figure 9 View Connection –dual auth*



The screenshot shows a mobile application interface with a black status bar at the top containing various icons and the time 1:49. Below the status bar is a grey header bar with the title "View Connection". The main content area is light grey and contains several fields, each with a bold label and a text input field. The fields are: "Connection name" with the value "sa4-eng-dualauth", "Url" with the value "https://sa4-eng.acmegizmo.com/dualauthafw", "Username" with the value "paridhi", "Certificate Alias" (empty), "Realm" (empty), and "Role" (empty). At the bottom of the form is a large, light grey button labeled "Close". The bottom of the screen features a black navigation bar with white icons for back, home, and recent apps.

**View Connection**

**Connection name**  
sa4-eng-dualauth

**Url**  
https://sa4-eng.acmegizmo.com/dualauthafw

**Username**  
paridhi

**Certificate Alias**

**Realm**

**Role**

Close




Figure -10 Login page for dual auth profile

Connect

Select Connection:

sa4

Login

 Pulse Secure

Welcome to

**Pulse Connect Secure**

<b>Username</b>	paridhi
<b>Password</b>	Password
<b>Secondary username</b>	testuser
<b>Secondary password</b>	Secondary password

**Sign In**

Please sign in to begin your secure session.

10. Add a VPN configuration with realm and role.

*Figure-11 View connection*

The screenshot shows an Android application interface with a 'View Connection' dialog box. The dialog has a title bar with the text 'View Connection'. Below the title bar, there are several fields with labels and values:

- Connection name**: sa4
- Url**: https://sa4-eng.acmegizmo.com
- Username**: pradeep
- Certificate Alias**: (empty field)
- Realm**: Users
- Role**: Users

At the bottom of the dialog, there is a button labeled 'Close'.

11. If the device is rebooted, Pulse Secure Android application must be launched again before it can receive VPN configuration from the restrictions framework.
12. Set a default profile

*Figure -12 View connections before changing default VPN configuration*

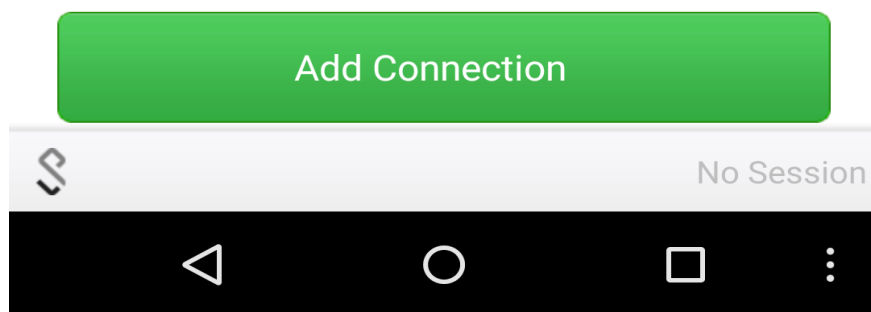
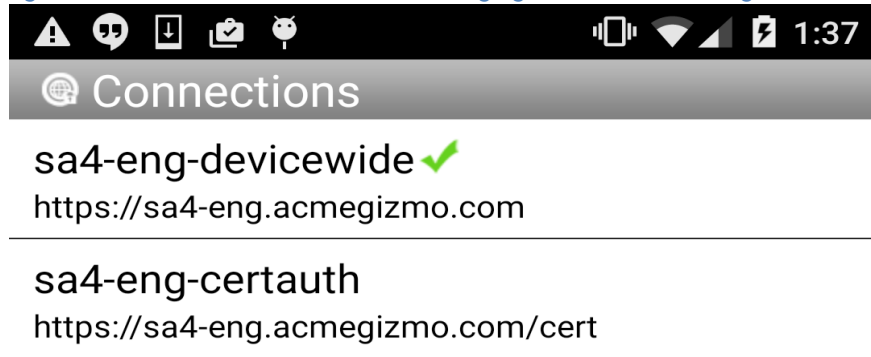
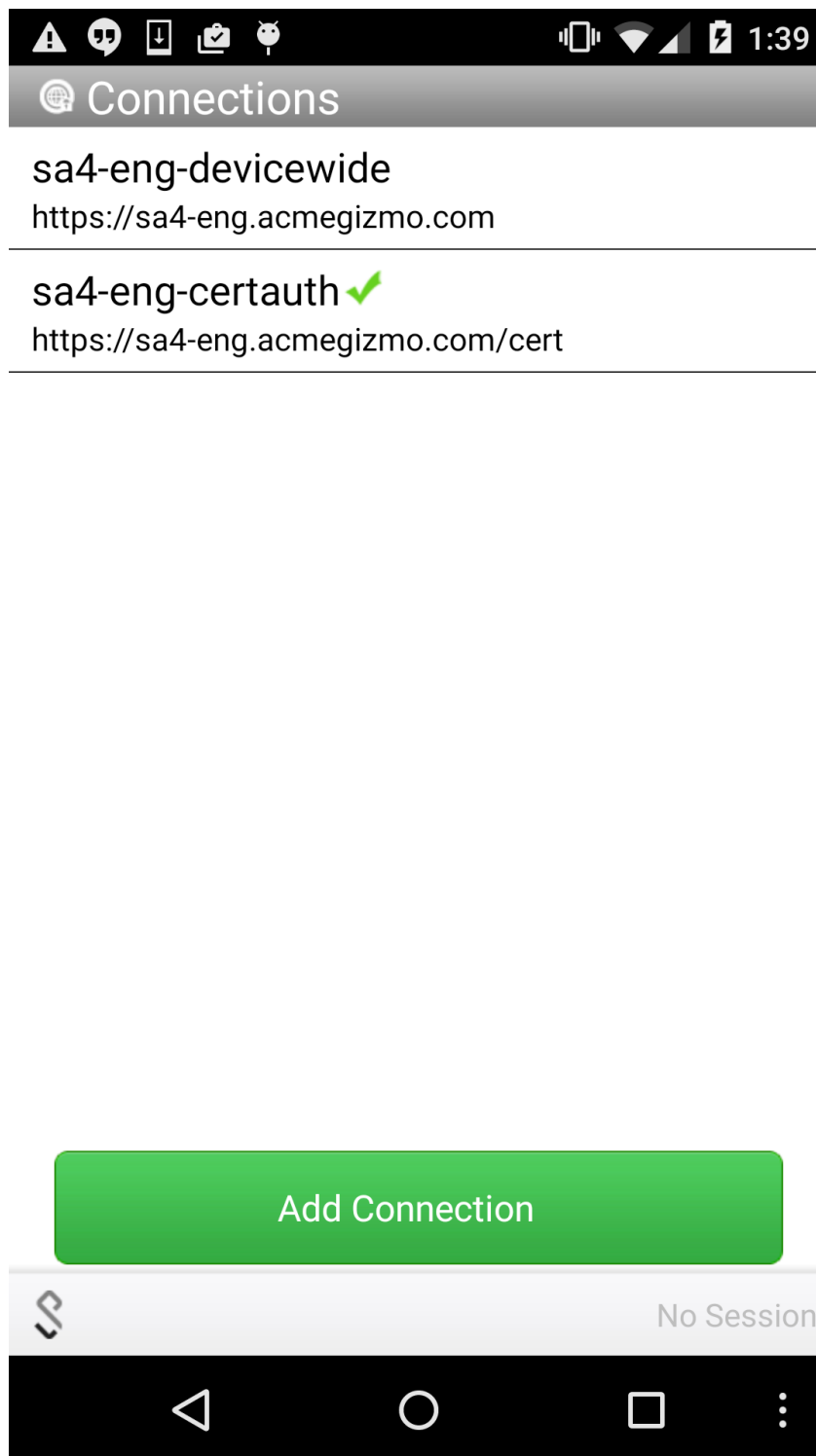


Figure -13 View connections after changing default VPN configuration



### 13. Deleting a VPN profile

*Figure -14 View connections before deleting a VPN configuration*

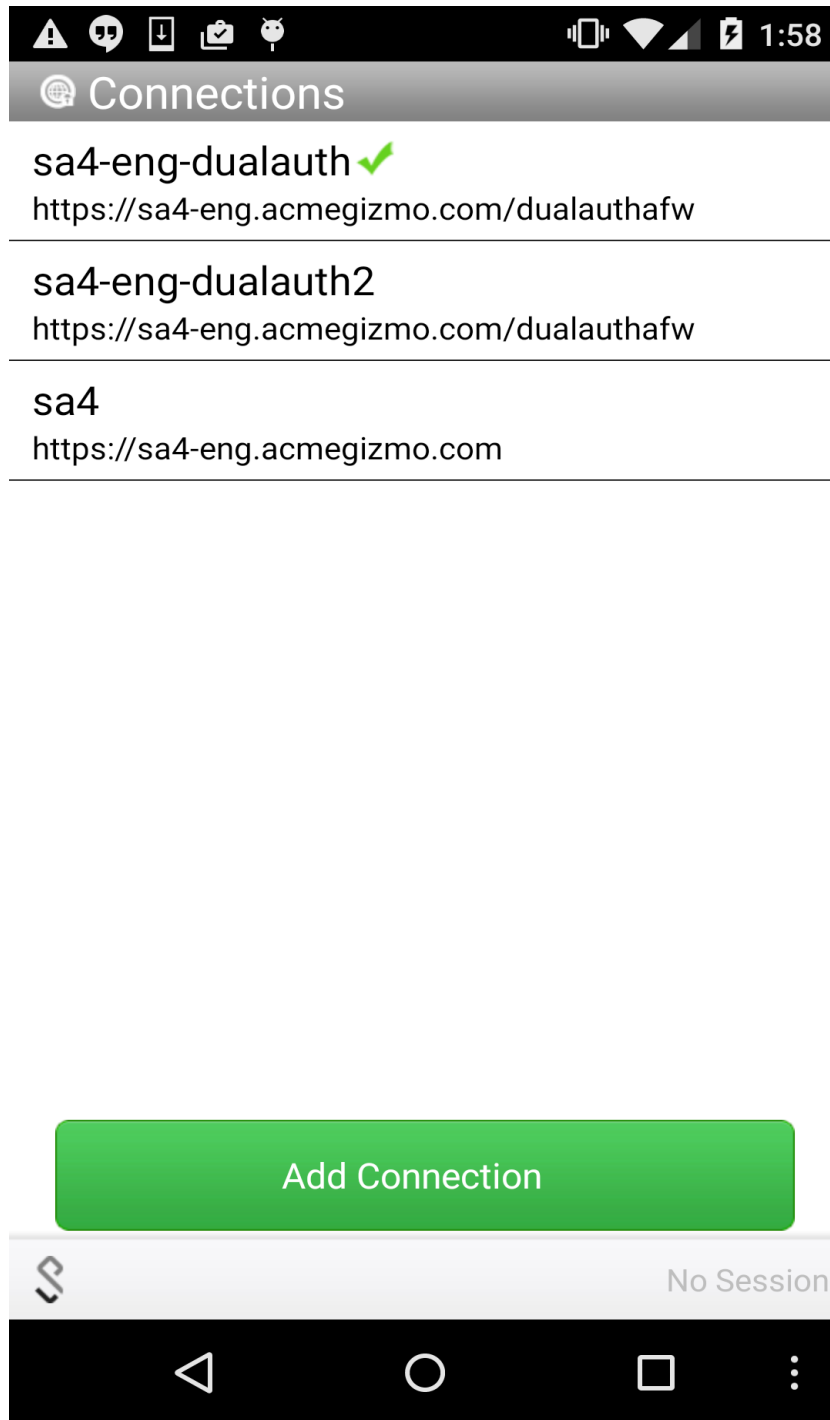
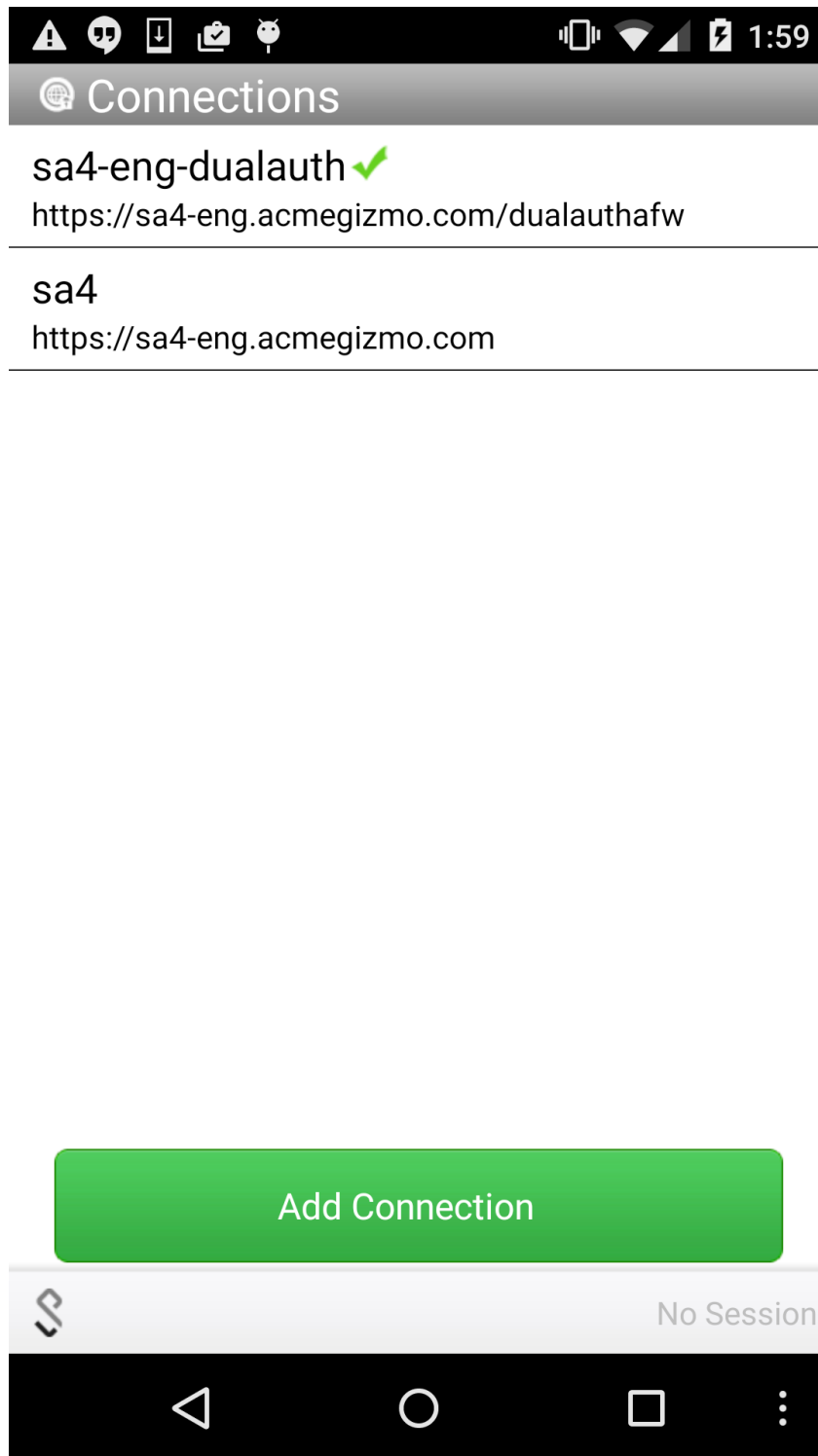


Figure -15 View connections after deleting a VPN configuration



## Limitations

- RSA authentication is not supported.
- Upon reboot, Pulse Secure Android application needs to be launched before it can get VPN profile from restrictions framework.

## Supported Devices

Android 5.0 and above devices that support Android for Work.

<https://www.google.com/work/android/features/devices.html>

## Known Issues

- If the system or user terminates the application process then restrictions will not be read by Pulse Secure Android application.
  - Workaround: Application needs to be restarted if terminated.
- Android 5.0 & 5.0.x issue: If Pulse Secure Android application is uninstalled and installed; device must to be rebooted before VPN can be established.
  - Issue is fixed in Android 5.1.