



MotionPro

Administration Guide

Copyright Statement

Copyright©2015 Array Networks, Inc., 1371 McCarthy Blvd, Milpitas, California 95035, USA.
All rights reserved.

This document is protected by copyright and distributed under licenses restricting its use, copying, distribution, and compilation. No part of this document may be reproduced in any form by any means without prior written authorization of Array Networks, Inc. Documentation is provided “as is” without warranty of any kind, either express or implied, including any kind of implied or express warranty of non-infringement or the implied warranties of merchantability or fitness for a particular purpose.

Array Networks, Inc., reserves the right to change any products described herein at any time, and without notice. Array Networks, Inc. assumes no responsibility or liability arising from the use of products described herein, except as expressly agreed to in writing by Array Networks, Inc. The use and purchase of this product does not convey a license to any patent copyright, or trademark rights, or any other intellectual property rights of Array Networks, Inc.



Warning: Modifications made to the Array Networks unit, unless expressly approved by Array Networks, Inc., could void the user’s authority to operate the equipment.

Declaration of Conformity

We, Array Networks, Inc., 1371 McCarthy Blvd, Milpitas, CA 95035, 1-866-992-7729; declare under our sole responsibility that the product(s) Array Networks, Inc., Array Appliance complies with Part 15 of FCC Rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.



Warning: Array Appliance is a Class A digital device, pursuant to Part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy, and if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. In a residential area, operation of this equipment is likely to cause harmful interference in which case the user may be required to take adequate measures or product. In a domestic environment this product may cause radio interference in which case the user may be required to take adequate measures.

About Array Networks

Array Networks is a global leader in networking solutions for connecting users and applications while ensuring performance, availability and security. Using Array, companies can provide access for any user, anywhere, on any device to applications, desktops and services running in either the cloud or the enterprise data center. From Web sites to e-commerce to enterprise applications to cloud services, Array solutions deliver a premium end-user experience and demonstrable security while ensuring that revenue and productivity gains always outweigh CAPEX and OPEX.

Engineered for the modern data center, Array Networks application, desktop and cloud service delivery solutions support the scalability, price-performance, software agility and leading-edge feature innovation essential for successfully transforming today's challenges in mobile and cloud computing into opportunities for mobilizing and accelerating business.

Contacting Array Networks

Please use the following information to contact us at Array Networks:

➤ **Website:**

<http://www.arraynetworks.com/>

➤ **Telephone:**

Phone: (408)240-8700

Toll Free: 1-866-692-7729 (1-866-MY-ARRAY)

Support: 1-877-992-7729 (1-877-99-ARRAY)

Fax: (408)240-8754

Telephone access to Array Networks is available Monday through Friday, 9 A.M. to 5 P.M. PST.

➤ **E-mail:**

info@arraynetworks.com

➤ **Address:**

1371 McCarthy Boulevard

Milpitas, California 95035, USA

Table of Contents

Copyright Statement	I
Declaration of Conformity	I
About Array Networks.....	II
Contacting Array Networks	II
Table of Contents	III
Chapter 1 MotionPro Overview	1
Chapter 2 Basic Settings and Configuration	3
2.1 Initial System Configuration	3
2.2 Virtual Site Configuration.....	3
Chapter 3 MotionPro Pilot.....	9
3.1 Overview	9
3.2 Apply and Save Configuration.....	11
3.3 Main Configuration Page	11
Chapter 4 Enterprise Application Portal	13
4.1 AAA.....	13
4.1.1 Authentication	13
4.1.2 Authorization	26
4.1.3 Auditing	28
4.2 Authorized Resources	29
4.2.1 Secure Browser	29
4.2.2 Web Resources.....	29
4.2.3 Native Applications.....	31
4.2.4 DesktopDirect Resources	34
4.3 VPN on Demand	34
Chapter 5 Enterprise Application Store	39
5.1 Add Enterprise Applications to the Enterprise Application Store.....	39
5.2 Release Enterprise Applications to Mobile Users.....	42
Chapter 6 Enterprise Application Security	44

6.1 Security Policy	44
6.1.1 Client Policy	44
6.1.2 Server Policy	49
6.2 Remote Device Management	51
6.2.1 Enable MDM and Set MDM Properties	51
6.2.2 Device Status/Application Poll	53
6.2.3 Remote Device Action	54
Chapter 7 System Monitor	57
7.1 System Monitor	57
7.1.1 Device Registration and Management	57
7.1.2 DeviceID Import and Export	59
7.1.3 Session Management	59
7.2 System Management	60
7.2.1 Import and Export	60
7.2.2 Backup and Restore	61
7.2.3 Portal Configuration	62
Appendix I Set SSO Parameters	63
Appendix II FAQs	65

Chapter 1 MotionPro Overview

MotionPro provides mobile users with flexible use of enterprise applications and secure access to enterprise resources, including Browser/Server (B/S) and Client/Server (C/S) resources.

MotionPro also provides the administrator with mobile application management for remote devices, such as Enterprise Application Store and remote application and data wipe. After downloading and installing the MotionPro client from the Apple App store or Google Play store, users can access all these functions.

The MotionPro feature mainly has the following functions:

- **Enterprise Application Portal:** Enterprise applications will be provided to mobile users through the MotionPro virtual site after authentication and authorization. MotionPro supports authentication by various methods, authorization by user/local group/Active Directory (AD), LDAP and RADIUS groups, and auditing by user/traffic logs.
- **Secure Browser:** This is a build-in application of the MotionPro client for accessing B/S (Web) resources. All the data transmitted through Secure Browser will be encrypted by the SSL L3VPN tunnel. Secure Browser also integrates the Post SSO function.
- **Application Tunnel API:** This is a software development kit (SDK). If Application Tunnel API is integrated with a C/S (SDK built-in native) application, SSL L3VPN tunnels can be established by directly using the built-in application.
- **VPN on Demand:** SSL L3VPN/IPsec VPN tunnels can be established between AG and mobile devices when native applications that are not integrated with Application Tunnel API need to access enterprise resources.
- **Enterprise Application Store:** This function greatly facilitates the operation of releasing and upgrading enterprise applications to mobile users.
- **Security Policies:** This function allows the administrator to define different levels of security policies for the client and the server sides. These policies will be executed without the administrator's intervention if the conditions of the policies are met.
- **Remote Device Management:** This function allows the administrator to remotely operate mobile devices such as install or uninstall applications, restore factory settings, lock screen and clear passcode.

The following chapters illustrate all the features of MotionPro and demonstrate the process to configure each function. Configuration results on the MotionPro client are also provided as a reference to help administrators better understand and use our product.



Note: The MotionPro client can be downloaded from the Google Play store (Android 4.0 or later) or the Apple App store (iOS 6.0 or later). Under most circumstances, these two clients perform very much alike, so we only display the Android demonstration effect.

When there are significant differences, we will display both Android and iOS effects.

Chapter 2 Basic Settings and Configuration

2.1 Initial System Configuration

The MotionPro virtual site can be configured on the AG appliance. The administrator can access the MotionPro Pilot of the configured virtual site to configure MotionPro settings.

Before the configuration of the MotionPro virtual site, some initial settings of the AG appliance are required such as configuration of default route, IP addresses, DNS and WebUI.

For detailed introduction of initial connection, basic setup and configuration of the AG appliance, please refer to Chapter 2 Initial System Setup & Configuration in the ArrayOS AG 9.3 User Guide.

2.2 Virtual Site Configuration

The first step of MotionPro configuration is to create a virtual site of the MotionPro type. Detailed steps are as follows:

➤ **Add a Virtual Site of the MotionPro Type**

Under the global scope, select **Virtual Sites > Virtual Sites > Virtual Sites**, and click the **Add** action link in the **Virtual Sites** area, as shown in Figure 2–1.



Figure 2–1 Add a Virtual Site

In the **Add a New Virtual Site** configuration window, select “motionpro” from the **Virtual Site Type** drop-down list, and specify the parameters **Site Name**, **Description**, **Site FQDN** and **IP Address** as required, as shown in Figure 2–2.

Virtual Sites
QuickLink
IPsec
Certificate Info

ADD A NEW VIRTUAL SITE
Cancel | Save & Add Another | Save

BASIC SETUP [Virtual Site Type: MotionPro ▼]

Site Name:

Description: (Optional)

Site FQDN:

www.example.com

* Note: Each line is a complete FQDN. A Fully Qualified Domain Name (FQDN), also referred to as an absolute domain name, is a domain name that specifies a computer's exact location in the tree hierarchy of the Domain Name System (DNS). FQDN consists of the host name and domain name. For example, if the local hostname of a device is myhost and the parent domain name is example.com, the FQDN of the device is myhost.example.com.

IP Address:

10.8.6.88 443

* Note: Please separate IP and port with a space. For multiple IP/port pairs, please enter them in different lines.
e.g., single IP/Port: 192.168.2.1 443
multi IP/Port: 192.168.2.1 443
192.168.2.2 443

SSL CERTIFICATE [Generate Import Import via TFTP

* Note: The following fields will be used to create a Certificate Signing Request and a test SSL certificate. If you choose not to complete these fields and an existing CSR cannot be found, SSL will be disabled for this virtual site and portal access will not be available.

CSR Key Length: 1,024 Bit 2,048 Bit 4,096 Bit

CSR Signature Algorithm: SHA1 SHA256 SHA384 SHA512

Country Code:

State/Province:

City/Locality:

Organization:

Organizational Unit:

Administrator's Email:

Private Key Exportable: No Yes

Site FQDN as Common Name: No Yes

* Note: If the virtual site deploys QuickLink, it is recommended to use wildcard host as common name (eg. *.abc.com), or import a third party wildcard certificate.

Figure 2–2 Add a MotionPro Type Virtual Site

After the MotionPro type virtual site is created, the administrator needs to generate or import an SSL certificate, configure AAA, L3VPN/IPSec and other advanced configurations which will be introduced in the following chapters.

Alternatively, the administrator can use the **MotionPro Deployment** action link as shown in Figure 2–1 to quickly create a MotionPro type virtual site. The administrator can just specify the **IP Address** parameter in the **Setup A MotionPro Site** area and the parameters **First IP Address** and **Last IP Address** in the **Virtual Private Network (L3VPN)** area, then create the MotionPro type virtual site with other configurations left as defaulted, as shown in Figure 2–3.

©2015 Array Networks, Inc.
All Rights Reserved.

4

Virtual Sites
QuickLink
IPsec
Certificate Info

[Cancel](#) | [Save & Add Another](#) | [Save](#)

SETUP A MOTIONPRO SITE

Site Name: *

IP Address: *

Port: (Integer from 1 to 65535) *

Site FQDN:

SSL CERTIFICATE [Generate Import Import via TFTP 2,048 Bit 4,096 Bit SHA256 SHA384 SHA512 *

State/Province: *

City/Locality: *

Organization: *

Organizational Unit: *

Administrator's Email: *

Private Key Exportable: No Yes Yes LDAP RADIUS *

Password: (Default value: test) *

VIRTUAL PRIVATE NETWORK (L3VPN)

Configure a Dynamic IP Range

First IP Address: *

Last IP Address: *

Enable NAT:

Configure a VPN Resource

Network Resource: *

Example for Network Resource:

0.0.0.0/0

10.10.10.0/24

IPSEC

Profile Name: *

VOD Domain: *

Figure 2–3 MotionPro Deployment



Note: The administrator should configure the dynamic IP range according to the number of users accessing the virtual site. If more users need to access this virtual site, the administrator can extend the number of IP addresses in the dynamic IP range via WebUI or the CLI command “**vpn netpool iprange dynamic <netpool> <start_ip> <end_ip> [unit_name]**”.

➤ **Add an SSL Certificate for the Virtual Site**

For the functioning of the MotionPro type virtual site, the administrator needs to generate or import an SSL certificate first. A test certificate/key pair can be generated by the AG appliance for

test purpose only. For commercial use, the administrator must import a certificate/key pair issued by a trusted certificate authority in either of the following ways:

- Import an SSL certificate/key pair from the local host

Select the **Import** radio button in the **SSL Certificate** area in the middle part of the **Add A New Virtual Site** or **MotionPro Deployment** configuration page. Paste the certificate and key respectively into the **Paste SSL Certificate Here** and **Paste SSL Key Here** text boxes, as shown in Figure 2–4.



Figure 2–4 Import an SSL Certificate/Key Pair from the Local Host

- Import an SSL certificate/key pair from a remote TFTP server

Select the **Import via TFTP** radio button in the **SSL Certificate** area in the middle part of the **Add A New Virtual Site** or **MotionPro Deployment** configuration page. Specify the parameters **TFTP Server IP for SSL Cert**, **File Name**, **TFTP Server IP for SSL Key**, **File Name** and **Key Password**, as shown in Figure 2–5.

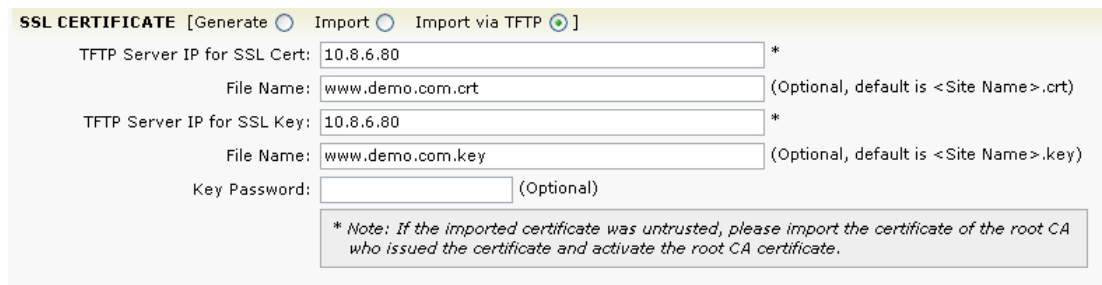


Figure 2–5 Import an SSL Certificate/Key Pair from a Remote TFTP Server



Note: In order to use the VPN on Demand function for iOS (for details, please refer to section 4.3 VPN on Demand), the CN value of the SSL certificate issued by the trusted

certificate authority must be the same as the **Site FQDN** value of the virtual site.

➤ **Activate an Imported SSL Certificate/Key Pair**

Under the virtual site scope, select **Site Configuration > SSL/DTLS Certificates > Certificates/Key**, check the radio button of the desired certificate/key pair and click the **Set Active** action link to activate it, as shown in Figure 2–6.



Figure 2–6 Activate an Imported SSL Certificate/Key Pair

➤ **Enable SSL for the Virtual Site**

Under the virtual site scope, select **Site Configuration > SSL/DTLS Certificates > SSL Settings > General**, select the **Enable SSL** check box, and click the **Save Changes** button in the upper right corner to save the configuration, as shown in Figure 2–7.

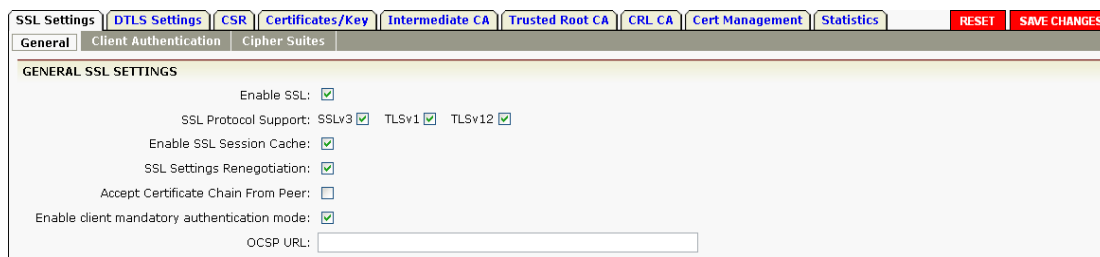
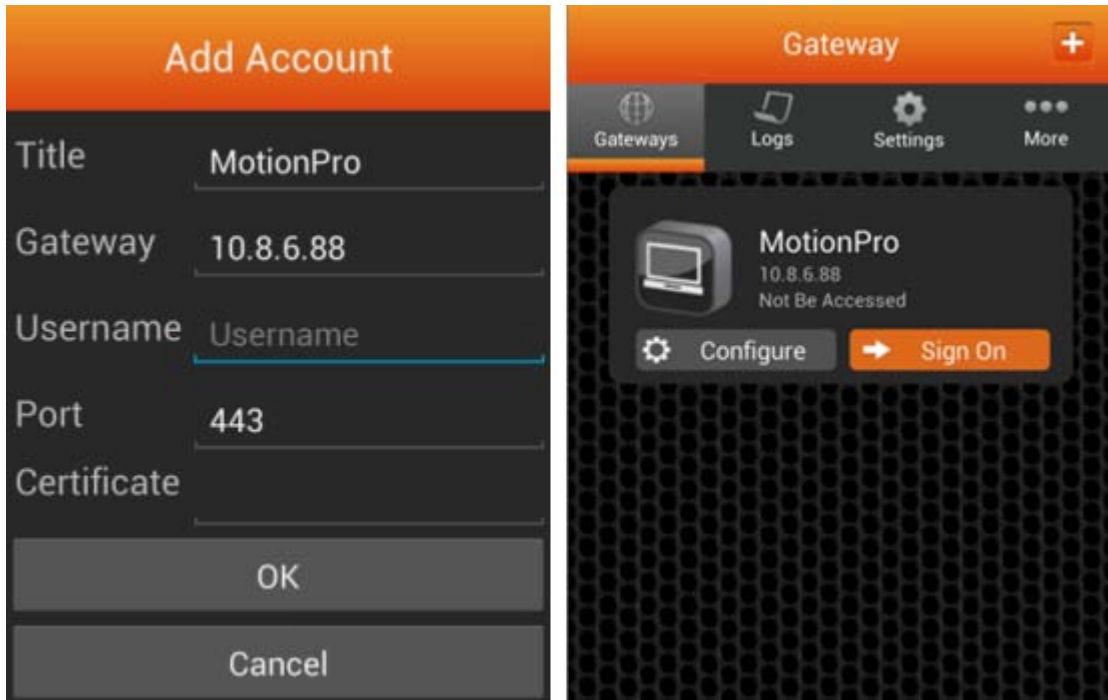


Figure 2–7 Enable SSL

[Client Effect](#)

After successful installation of the MotionPro client, users can create a gateway to get access to the newly added virtual site later. The gateway can be easily deleted with a long press on Android and a swipe on iOS.



Client Effect End

Chapter 3 MotionPro Pilot

This chapter gives a basic introduction to the MotionPro Pilot. Please read this chapter to get familiar with the MotionPro Pilot before configuring MotionPro settings.

3.1 Overview

The MotionPro Pilot configuration interface is designed for easy navigation through the MotionPro configuration tasks and consists of various configuration pages.

Under the MotionPro type virtual site scope, select the **Virtual Site Home** feature link, and click **Go to MotionPro Pilot** in the **Virtual Site Information** area to access the MotionPro Pilot, as shown in Figure 3–1.

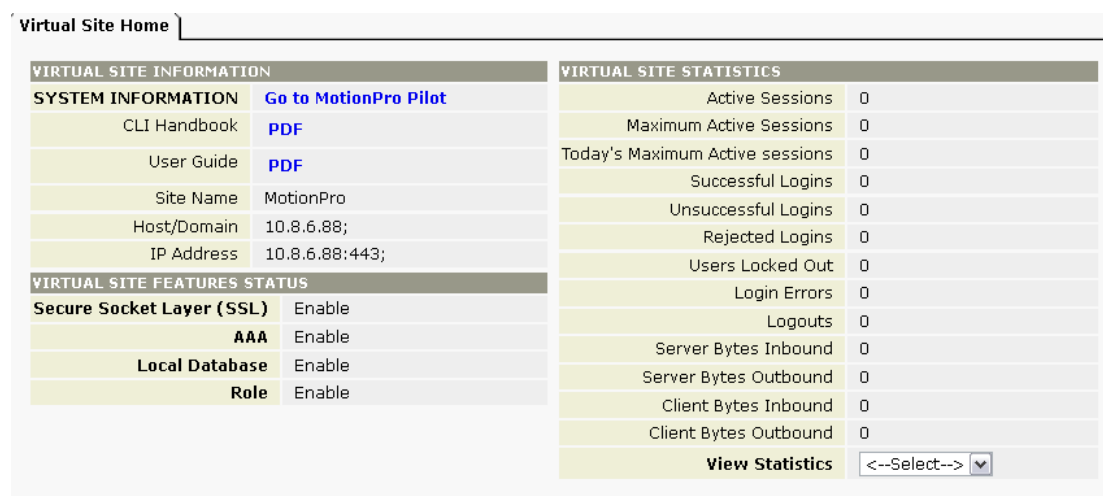


Figure 3–1 Go to MotionPro Pilot



Note:

- MotionPro Pilot supports IE 8.0~11.0 and Firefox 3.6~25 browsers. It is recommended to use IE 10.0 or Firefox 25 to access the MotionPro Pilot.
- MotionPro Pilot supports the English, Simplified Chinese, and Japanese languages. However, the password parameters do not support Chinese and Japanese characters.
- MotionPro Pilot does not support the single quote mark ('), double quote mark (") and escape character (\), which are reserved for system use.

Each MotionPro Pilot configuration page consists of four main areas, as shown in Figure 3–2.

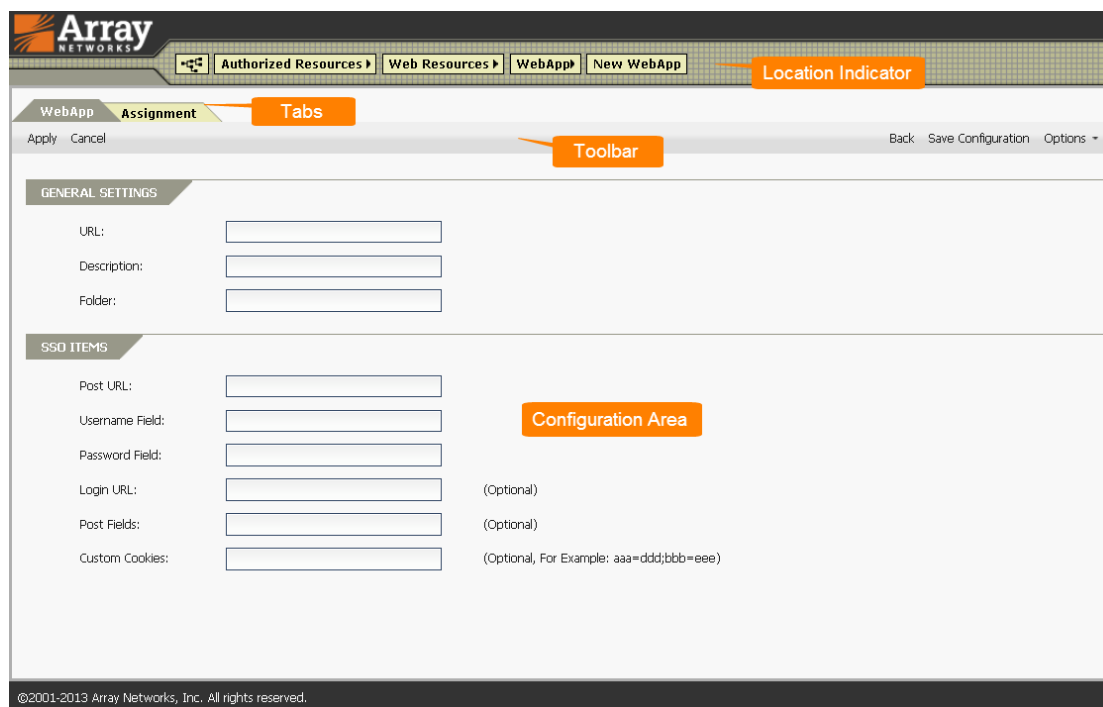


Figure 3–2 Configuration Page

- **Location Indicator**

The location indicator shows the function that the administrator is currently working on.

- **Tabs**

Every configuration page consists of one or more tabs.

- **Toolbar**

The toolbar consists of two parts, as shown in Figure 3–3.



Figure 3–3 Toolbar

On the right side are general options:

- **Back** – Navigating back to the previous configuration screen.
- **Save Configuration** – Writing the existing configuration to memory (including all virtual site configurations).
- **Options** – **Go to WebUI** for switching back to the AG WebUI; **Go to DD Pilot** for switching to the DD Pilot; **User Manual** for downloading the MotionPro

Administration Guide; **Logout** for logging out the appliance; **Language** for setting the language of MotionPro Pilot.

The left side of the toolbar hosts various action links that appears as needed. These actions usually appear in the following combinations:

- **Apply** – Allowing the administrator to apply the current configuration.
- **Cancel** – Allowing the administrator to revert to the pervious configuration.

3.2 Apply and Save Configuration

To apply the changes done through the MotionPro Pilot, the administrator needs to click the **Apply** action link on the toolbar. To write current running configurations into memory, the administrator needs to click the **Save Configuration** action link on the toolbar. If these configurations are not written into memory, they will be cleared after system reboot or system upgrade.

3.3 Main Configuration Page

The main configuration page is the hub from which all of MotionPro configurations are performed.

The main page consists of two tabs:

➤ System Monitor

This tab page provides access to system monitor functions including **Device Registration and Management**, **DeviceID Import and Export** and **Session Management**, and system management functions including **MotionPro Import and Export**, **MotionPro Backup and Restore** and **MotionPro Portal Configurations**, as shown in Figure 3–4.

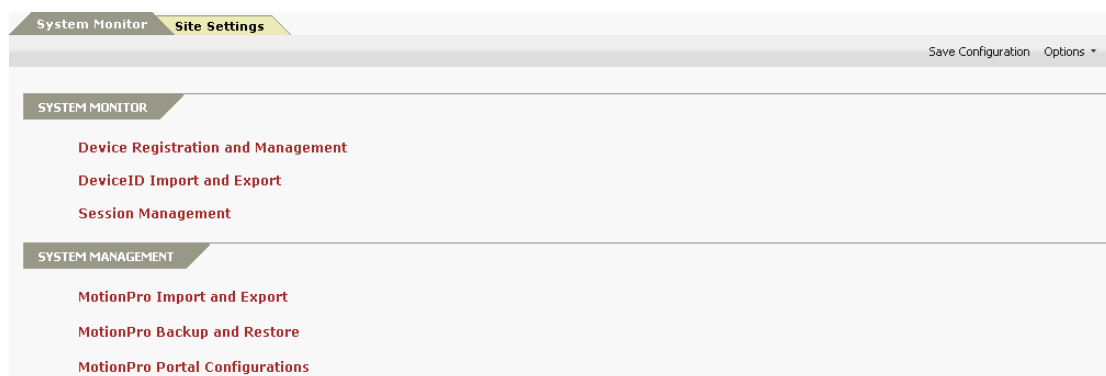


Figure 3–4 System Monitor

➤ Site Settings

This tab page provides access to site setting functions including **AAA**, **Authorized Resources**, **VPN on Demand**, **Enterprise Application Store** and **Enterprise Application Security**, as shown in Figure 3–5.

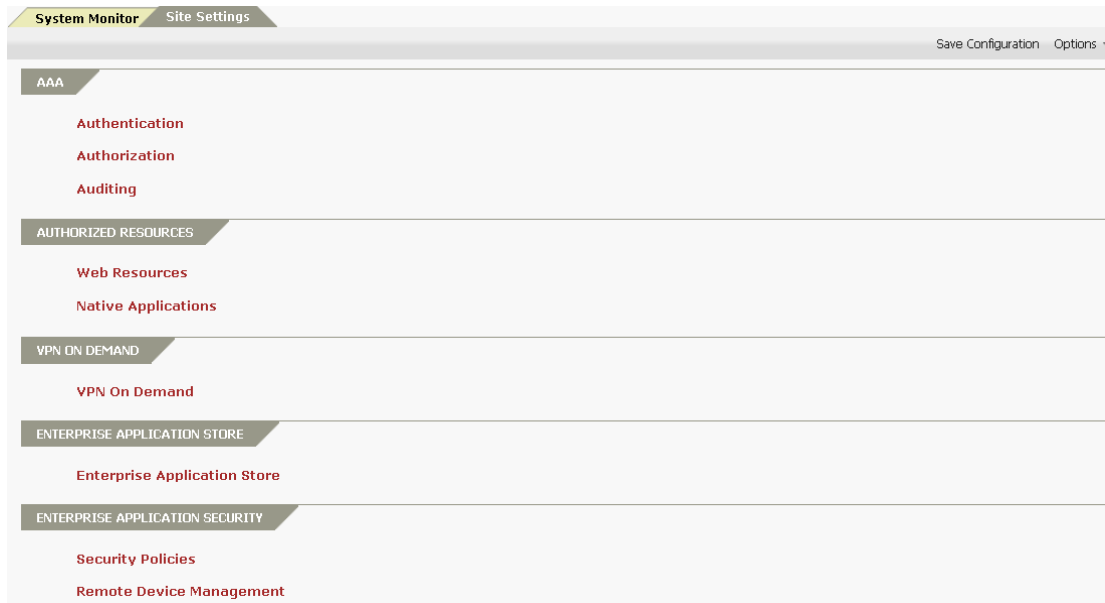


Figure 3–5 Site Settings

Chapter 4 Enterprise Application Portal

The AG appliance supports multiple enterprise application portals (MotionPro virtual sites). Applications, resources, Authentication, Authorization and Auditing (AAA) and VPN settings can be configured for each portal independently.

4.1 AAA

AAA is a series of combined features and operations providing Authentication, Authorization and Auditing for all connections and transactions carried out across the portal. AAA allows the administrator to control user access to enterprise applications and resources, grant users with specific authorities to internal resources and keep track of all user behaviors.

4.1.1 Authentication

Authentication is the first process in the AAA feature. In this process, the system will check the validity of the user identities, certificates or device IDs before permitting user logins. Users can log into the portal only with the valid user identities, certificates or device IDs.

4.1.1.1 DeviceID Authentication

With DeviceID authentication, the system will validate the ID of the mobile device that the user uses to log into the portal. Users can access internal resources only from the mobile devices with the valid device IDs.

On MotionPro Pilot, select **Site Settings > AAA > Authentication > Authentication Method**, select “DeviceID” from the **Authentication Method** drop-down list in the **Authentication Method** area, as shown in Figure 4–1.

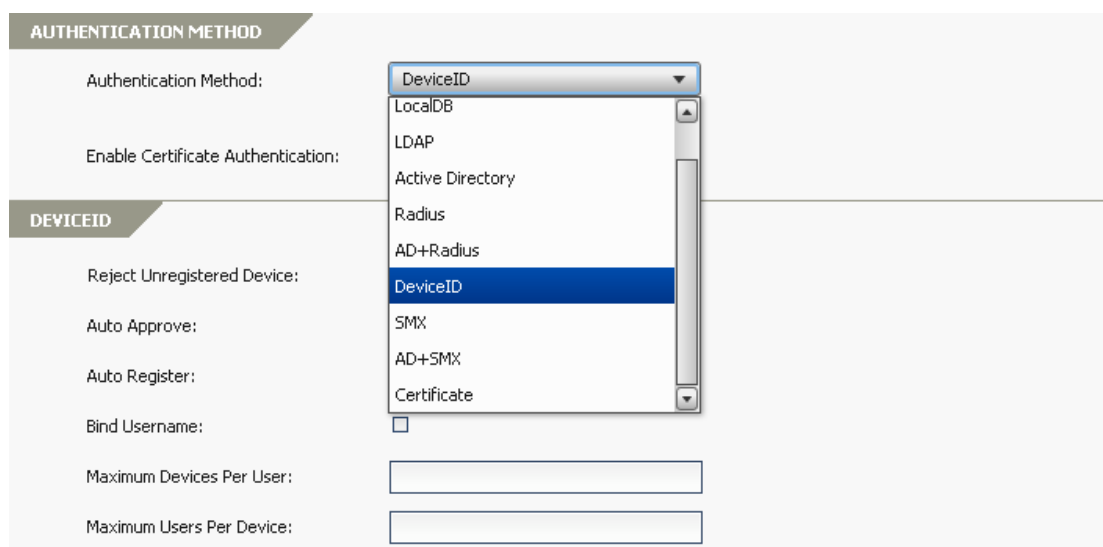


Figure 4–1 Select the Authentication Method




Note: DeviceID authentication requires the user to register the device used to the system. MotionPro supports two ways of device registration:

- **Register in advance:** Devices can be manually registered by the administrator in advance on MotionPro Pilot. For details about how to register the devices to the system, please refer to section 7.1.1.1 Device Registration.
- **Register through login:** Devices can be manually registered by end users on the client or be registered without intervention on end users' first enrollment.

After device registration, the administrator can monitor and manage device status. For details, please refer to section 7.1.1.2 Device Management.

In the **DeviceID** area, select the check boxes **Reject Unregistered Device**, **Auto Approve**, **Auto Register** and **Bind Username** if required, and specify the parameters **Maximum Devices Per User** and **Maximum Users Per Device**, as shown in Figure 4–2.



The screenshot shows a configuration panel titled "DEVICEID" with the following settings:

- Reject Unregistered Device:
- Auto Approve:
- Auto Register:
- Bind Username:
- Maximum Devices Per User:
- Maximum Users Per Device:

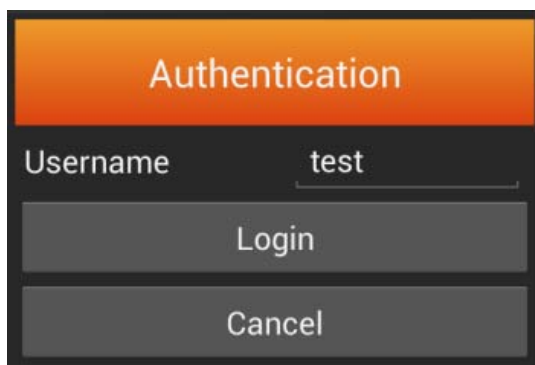
Figure 4–2 DeviceID Authentication

The **DeviceID** area has the following options:

- **Reject Unregistered Device:** The devices not registered to the system will be rejected.
- **Auto Approve:** The registered devices will be automatically approved; otherwise, the device status will be “pending” and the administrator needs to approve the devices manually.
- **Auto Register:** Unregistered devices will be registered without users' intervention and users can log in successfully if passing other authentication(s). If the check boxes **Reject Unregistered Device** and **Auto Register** are both selected, **Auto Register** will not take effect.
- **Bind Username:** This option is to track the username and DeviceID relations for the following options. The following options are available only when this option is checked.
- **Maximum Devices Per User:** This option specifies the maximum devices a user can have.
- **Maximum Users Per Device:** This option specifies the maximum users a device can be associated with.

Client Effect

When **Bind Username** option is enabled, only the username is needed for authorization, and no password will be required to log into the portal with a registered device.



Client Effect End

4.1.1.2 User Authentication

MotionPro supports the following types of user authentication methods:

- LocalDB
- Active Directory (AD)
- LDAP
- RADIUS
- SMX

MotionPro also supports combinations of the above user authentication methods:

- AD+LocalDB
- LDAP+LocalDB
- RADIUS+LocalDB
- SMX+LocalDB
- AD+RADIUS
- AD+SMX

For all user authentication methods, DeviceID authentication is always enabled to enhance the security level.

4.1.1.2.1 LocalDB

LocalDB users need to be defined in advance for LocalDB authentication. For details about how to add a LocalDB user, please refer to section 4.1.2.1 User/Group.

On MotionPro Pilot, select **Site Settings > AAA > Authentication > Authentication Method**, and select “LocalDB” from the **Authentication Method** drop-down list in the **Authentication Method** area, as shown in Figure 4–3.

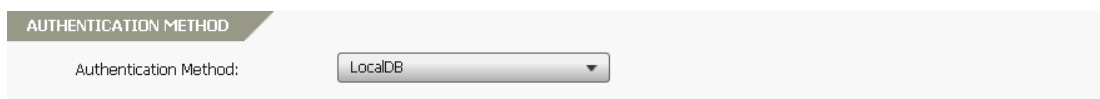


Figure 4–3 LocalDB Authentication

4.1.1.2.2 Active Directory (AD)

On MotionPro Pilot, select **Site Settings > AAA > Authentication > Authentication Method**, and select “Active Directory” from the **Authentication Method** drop-down list in the **Authentication Method** area, as shown in Figure 4–4.

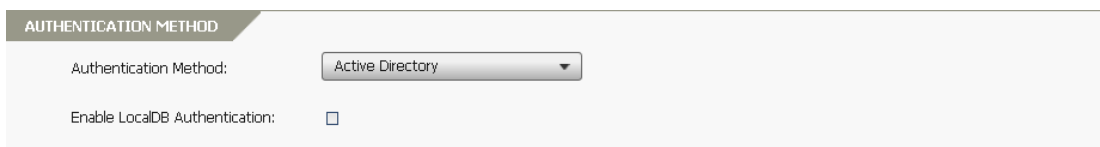


Figure 4–4 AD Authentication

Specify the parameters **Domain**, **Administrator** and **Password** in the **Active Directory Servers** area, as shown in Figure 4–5.

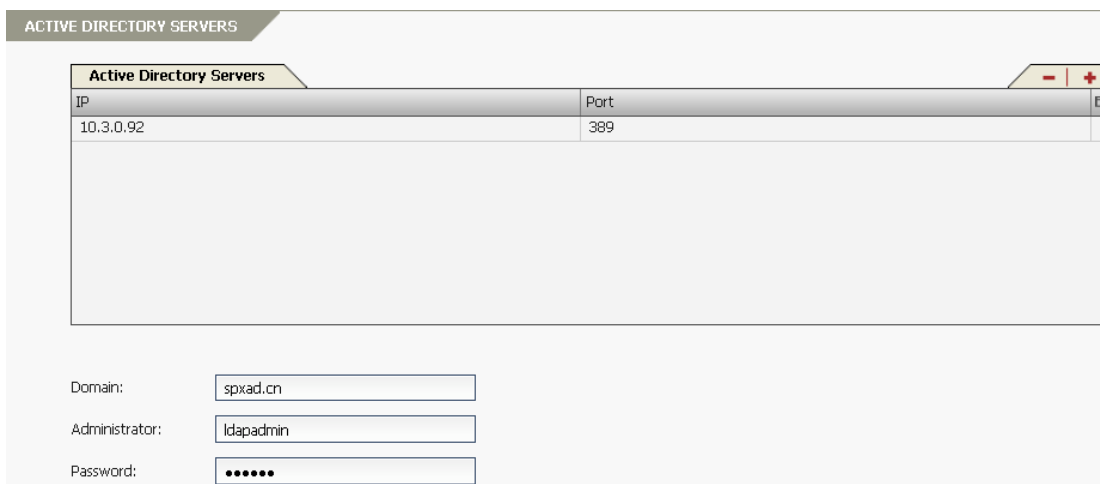


Figure 4–5 AD Servers

Click + in the **Active Directory Servers** area, specify the parameters **IP Address** and **Port** in the **Active Directory Server** area, and click **Apply** to add an Active Directory server, as shown in Figure 4–6.

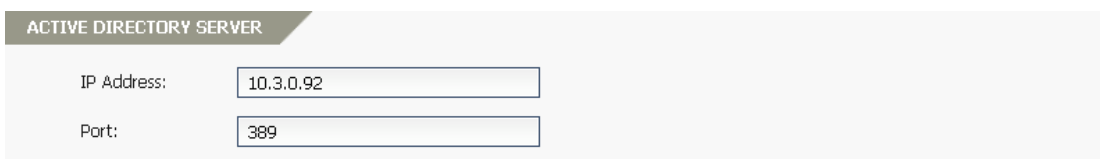


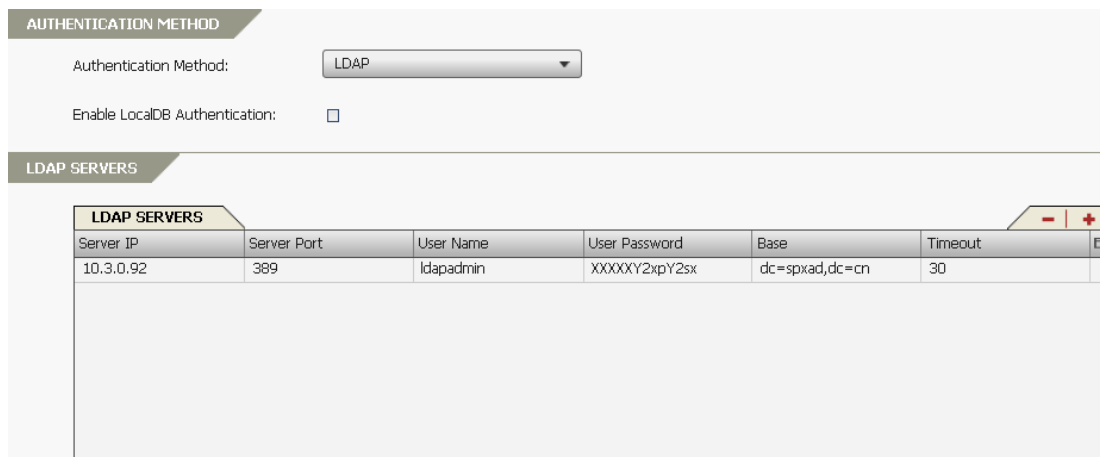
Figure 4–6 Add an AD Server



Note: A maximum of three AD servers can be added.

4.1.1.2.3 LDAP

On MotionPro Pilot, select **Site Settings > AAA > Authentication > Authentication Method**, and select “LDAP” from the **Authentication Method** drop-down list in the **Authentication Method** area, as shown in Figure 4–7.



AUTHENTICATION METHOD

Authentication Method: LDAP

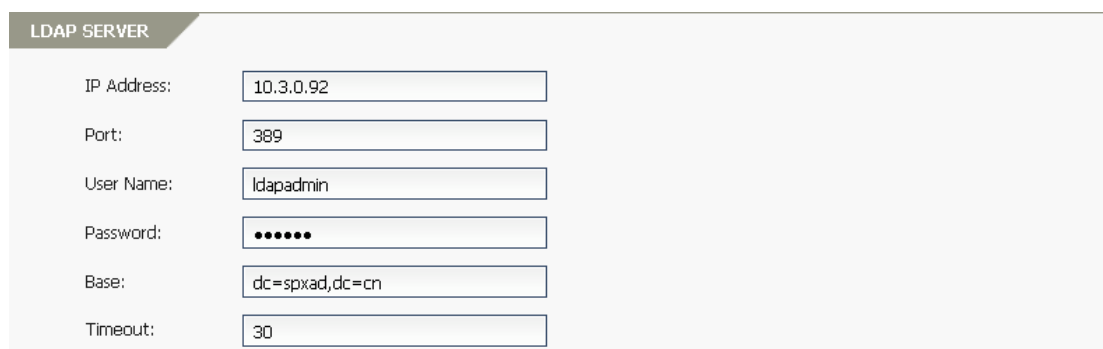
Enable LocalDB Authentication:

LDAP SERVERS

Server IP	Server Port	User Name	User Password	Base	Timeout	
10.3.0.92	389	ldadmin	XXXXXY2xpY2sx	dc=spxad,dc=cn	30	

Figure 4–7 LDAP Authentication

Click + in the **LDAP Servers** area, specify the parameters **IP Address**, **Port**, **User Name**, **Password**, **Base** and **Timeout** in the **LDAP Server** area, and click **Apply** to add an LDAP server, as shown in Figure 4–8.



LDAP SERVER

IP Address:

Port:

User Name:

Password:

Base:

Timeout:

Figure 4–8 Add an LDAP Server

Specify the parameters **LDAP Attribute Group**, **LDAP Attribute Default Group**, **Search Filter** and **Authenticate with Bind** in the **Advanced LDAP Configurations** area, as shown in Figure 4–9.

ADVANCED LDAP CONFIGURATIONS

LDAP Attribute Group:

LDAP Attribute Default Group:

Search Filter:

Authenticate with Bind: Dynamic Static

Figure 4–9 Advanced LDAP Configurations



Note: A maximum of three LDAP servers can be added.

4.1.1.2.4 RADIUS

On MotionPro Pilot, select **Site Settings > AAA > Authentication > Authentication Method**, and select “Radius” from the **Authentication Method** drop-down list in the **Authentication Method** area, as shown in Figure 4–10.

AUTHENTICATION METHOD

Authentication Method:

Enable LocalDB Authentication:

Figure 4–10 RADIUS Authentication

Specify the parameters **RADIUS NASIP**, **RADIUS Attribute Group** and **RADIUS Attribute Default Group** in the **RADIUS Servers** area, as shown in Figure 4–11.

RADIUS SERVERS

Server IP	Server Port	Timeout	Retries	
10.4.7.200	1812	60	2	

RADIUS NASIP:

RADIUS Attribute Group:

RADIUS Attribute Default Group:

Figure 4–11 RADIUS Servers

Click + in the **RADIUS Servers** area, specify the parameters **IP Address**, **Port**, **Secret Password**, **Timeout** and **Retries** in the **RADIUS Servers** area, and click **Apply** to add a RADIUS server, as shown in Figure 4–12.

RADIUS SERVERS

IP Address:

Port:

Secret Password:

Timeout:

Retries:

Figure 4–12 Add a RADIUS Server



Note: A maximum of three RADIUS servers can be added.

4.1.1.2.5 SMX

On MotionPro Pilot, select **Site Settings > AAA > Authentication > Authentication Method**, and select “SMX” from the **Authentication Method** drop-down list in the **Authentication Method** area, as shown in Figure 4–13.

AUTHENTICATION METHOD

Authentication Method:

Enable LocalDB Authentication:

Figure 4–13 SMX Authentication

Add the primary SMX server by clicking the **Change** button in the **SMX Servers** area, as shown in Figure 4–14.

SMX SERVERS

Primary Server: Not Configured

Secondary Server: Not Configured

Figure 4–14 Add an SMX Server

In the **Server** area, specify the parameters **Hostname**, **Port** and **Import Certificate from**, as shown in Figure 4–15.

SERVER

Hostname:

Port:

Import Certificate from: Local Host SMX Server Remote Host

Source File Path:

Figure 4–15 Set SMX Server Parameters

MotionPro Pilot supports three ways of importing the SMX certificate:

- From the local host

Select the **Local Host** radio button and click the **Browser** button to select the certificate stored on the local host to import, as shown in Figure 4–16.

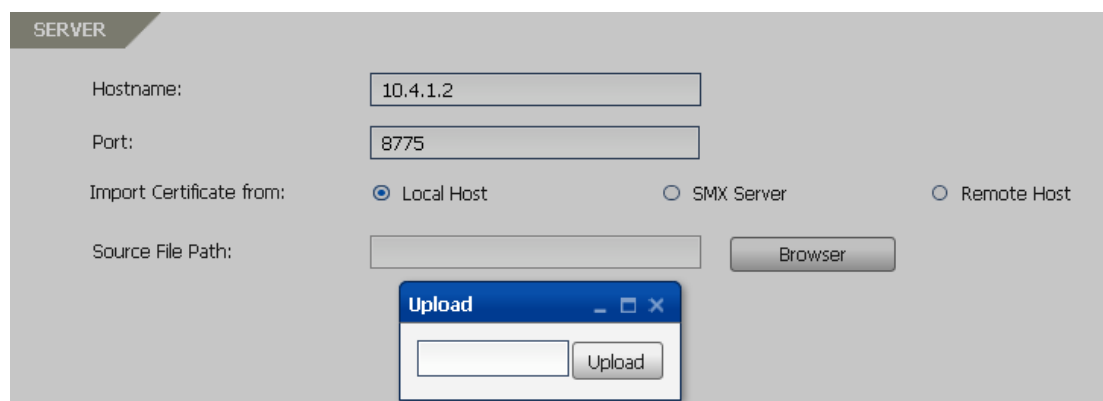


Figure 4–16 Import the SMX Certificate from the Local Host

- From the SMX server

Select the **SMX Server** radio button and specify the parameters **Username** and **Password** for downloading the SMX certificate from the SMX server, as shown in Figure 4–17.

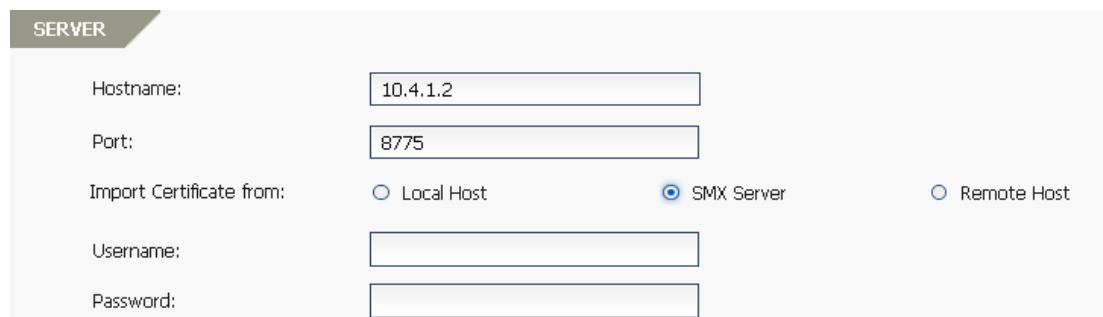


Figure 4–17 Import the SMX Certificate from the SMX Server

- From an remote host

Select **Remote Host** radio button and specify the parameters **Hostname**, **Username**, **Password** and **Source File Path**, as shown in Figure 4–18. The parameters **Username** and **Password** are the credentials that can be used to log into the remote host. The **Source File Path** parameter indicates the path storing the SMX certificate on the remote host.

SERVER

Hostname:	<input style="width: 80%;" type="text" value="10.4.1.2"/>
Port:	<input style="width: 80%;" type="text" value="8775"/>
Import Certificate from:	<input type="radio"/> Local Host <input type="radio"/> SMX Server <input checked="" type="radio"/> Remote Host
Hostname:	<input style="width: 80%;" type="text"/>
Username:	<input style="width: 80%;" type="text"/>
Password:	<input style="width: 80%;" type="text"/>
Source File Path:	<input style="width: 80%;" type="text"/>

Figure 4–18 Import the SMX Certificate from a Remote Host

Add the secondary SMX server in the same way as the primary SMX server. The secondary SMX server is used only when the primary SMX server is unavailable.



Note:

- When SMX authentication is enabled, the DeviceID authentication is enabled by default, and the LocalDB username and password are used for device registration.
- When logging into the portal with SMX authentication, users need to provide a LocalDB username for authorization.

4.1.1.2.6 User Authentication Methods Combination

Some user authentication methods can be simply combined. Here we use AD+RADIUS authentication method as an example.

To configure this authentication method, both the AD server and the RADIUS server need to be configured. If these two servers are already configured before, we can use the existing configurations directly for the AD+RADIUS authentication method.

On MotionPro Pilot, select **Site Settings > AAA > Authentication > Authentication Method**, and select “AD+Radius” from the **Authentication Method** drop-down list in the **Authentication Method** area, as shown in Figure 4–19.

AUTHENTICATION METHOD

Authentication Method: AD+Radius

ACTIVE DIRECTORY SERVERS

Active Directory Servers	
IP	Port
10.3.0.92	389

Domain:

Administrator:

Password:

RADIUS SERVERS

RADIUS SERVERS			
Server IP	Server Port	Timeout	Retries
10.4.7.200	1812	60	2

RADIUS NASIP:

RADIUS Attribute Group:

RADIUS Attribute Default Group:

Figure 4–19 AD+RADIUS Authentication

4.1.1.2.7 User/DeviceID Authentication Combination

For every user authentication method or every combination of user authentication methods, the DeviceID area is available, as shown in Figure 4–20.

AUTHENTICATION METHOD

Authentication Method: LocalDB

DEVICEID

Reject Unregistered Device:

Auto Approve:

Auto Register:

Bind Username:

Maximum Devices Per User:

Maximum Users Per Device:

Figure 4–20 User/DeviceID Authentication Combination



Note: When using SMX+DeviceID authentication, the registered username of DeviceID authentication must be the same with the LocalDB username of SMX authentication.

For detailed steps of configuring DeviceID authentication, please refer to section 4.1.1.1 DeviceID Authentication.

4.1.1.3 Certificate Authentication

With certificate authentication, the system will validate the certificate of the mobile device that the user uses to log into the portal. Users can access internal resources only after the AG server verifies the certificate received from the client and sends the corresponding certificate to the client for authentication.

On MotionPro Pilot, select **Site Settings > AAA > Authentication > Authentication Method**, and select “Certificate” from the **Authentication Method** drop-down list in the **Authentication Method** area, as shown in Figure 4–21.



Figure 4–21 Certificate Authentication

Under the virtual site scope, select **Site Configuration > SSL/DTLS Certificates > SSL Settings > General**, clear the **Enable SSL** check box in the **General SSL Settings** area, as shown in Figure 4–22.

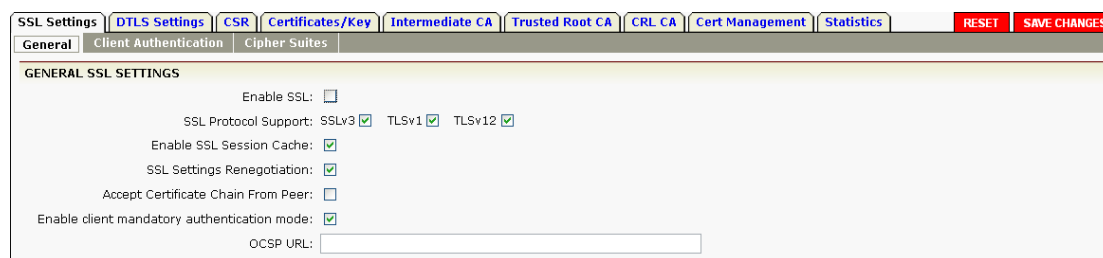


Figure 4–22 Disable SSL

The trusted root CA can be imported in either of the following ways:

- Import the trusted root CA from the local host

On the **Trusted Root CA** tab, click the **Import** action link in the **Trusted Root CA** area and import the trusted root CA in the **Paste Trusted Root CA Below** text box in the **Import Certificate** area, then click the **Submit** action link, as shown in Figure 4–23.



Figure 4–23 Import the Trusted Root CA from the Local Host

- Import the trusted root CA from a remote TFTP server

On the **Trusted Root CA** tab, click the **Import via TFTP** action link in the **Trusted Root CA** area and specify the parameters **TFTP Server IP for SSL Cert** and **File Name** in the **Import Certificate via TFTP** area, then click the **Submit** action link, as shown in Figure 4–24.

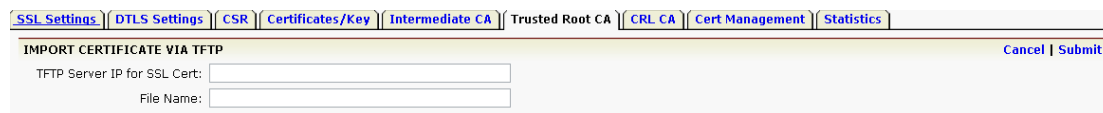


Figure 4–24 Import the Trusted Root CA from a Remote TFTP Server

Select the **Client Authentication** sub-tab under the **SSL Settings** tab, and check the **Enable Client Authentication** check box in the **Client Authentication** area, as shown in Figure 4–25.

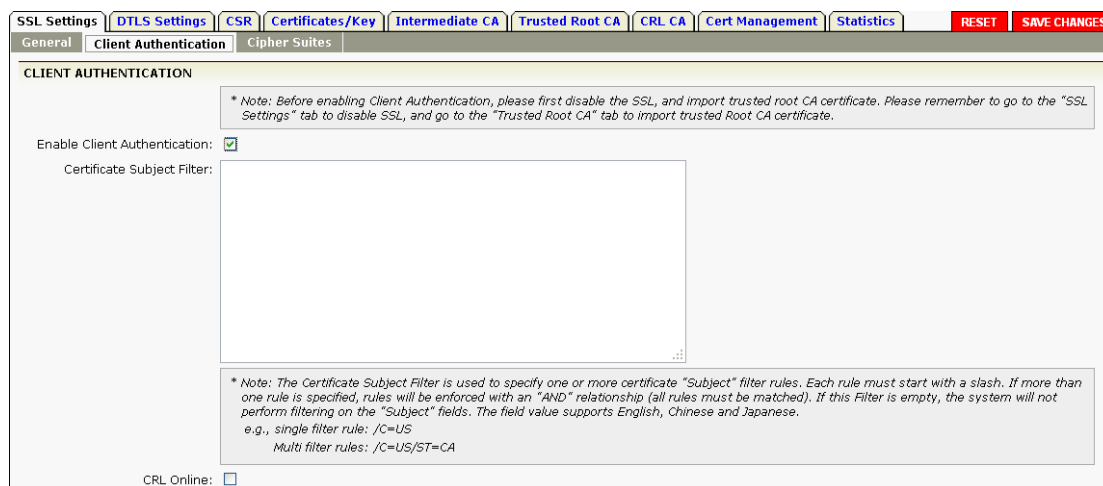


Figure 4–25 Enable Client Authentication

Go back to **SSL Settings > General**, and enable SSL again by selecting the **Enable SSL** check box in the **General SSL Settings** area.

Under the virtual site scope, select **Site Configuration > AAA > Server > Client Certificates**, and click the **Add Certificate Server** action link in the **Certificate Server Configuration** area. Specify the parameters as needed in the **Add Certificate Server** area and click the **Save** action link to add a certificate server, as shown in Figure 4–26.

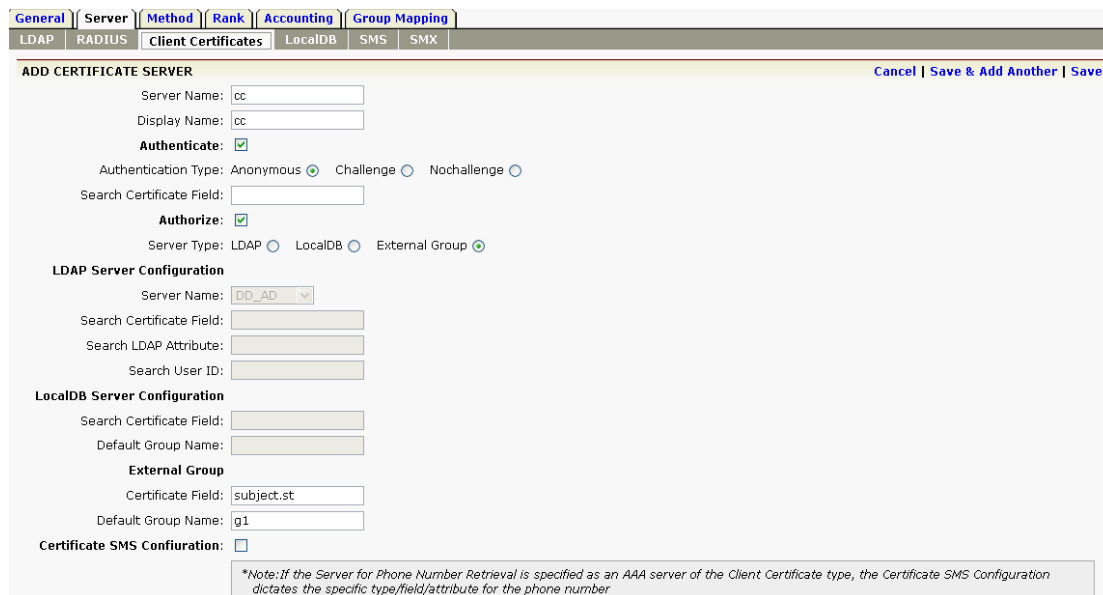


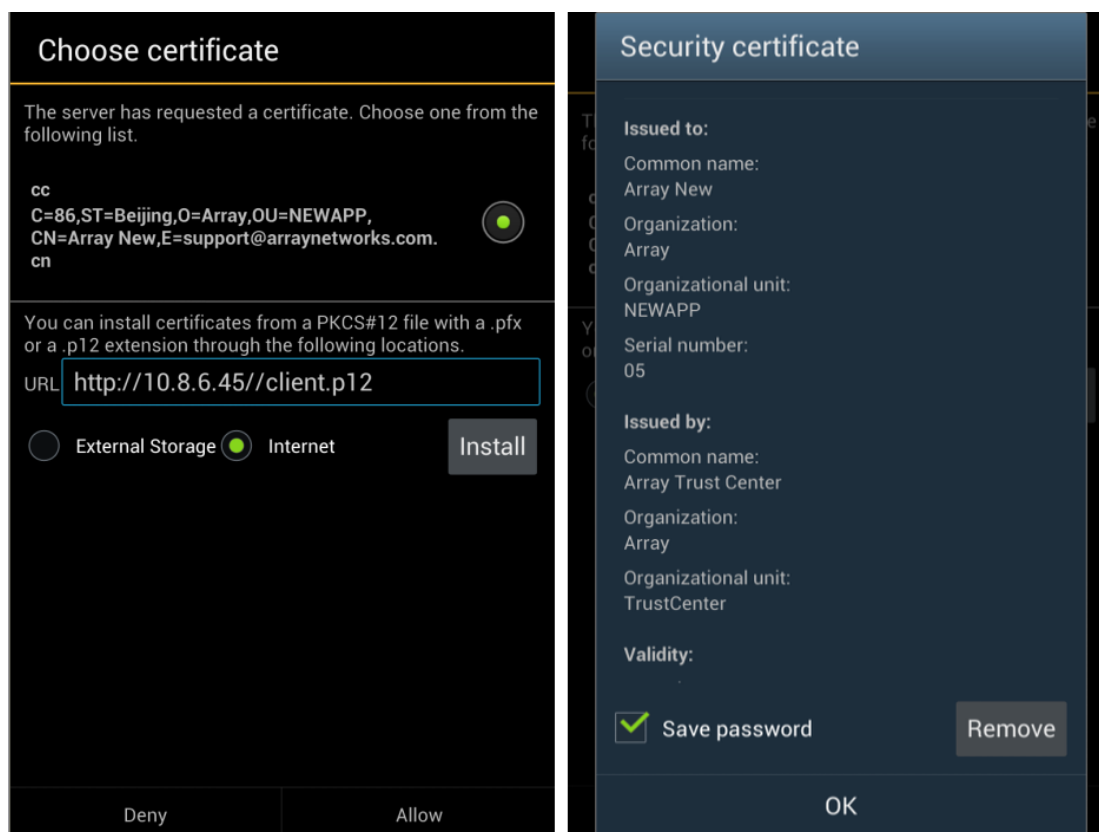
Figure 4–26 Add a Certificate Server



Note: Certificate authentication can be combined with DeviceID authentication. To combine them, just select “DeviceID” from the **Authentication Method** drop-down list and select the **Enable Certificate Authentication** check box.

Client Effect

Users can install the client side certificates from their local devices or external internet URL, and assign the certificates to specified virtual sites.



Client Effect End

4.1.2 Authorization

After users pass the authentication, Authorization will assign enterprise resources to the users based on usernames and groups.

To use the Authorization function, the administrator needs to define users and groups, define resources, and assign resources to users or groups. This section will describe how to define users and groups. For details on how to define resources and assign resources to users or groups, please refer to section 4.2 Authorized Resources.



Note: When only DeviceID authentication is used, the username used to register the mobile device will be used for authorization.

4.1.2.1 User/Group

The **User** and **Group** feature links are for LocalDB user and group account management.

To add a LocalDB user, select **Site Settings > AAA > Authorization > Authorization**, select the **Users** feature link in the **Basic Tasks** area, and click + in the **Users** area, as shown in Figure 4–27.

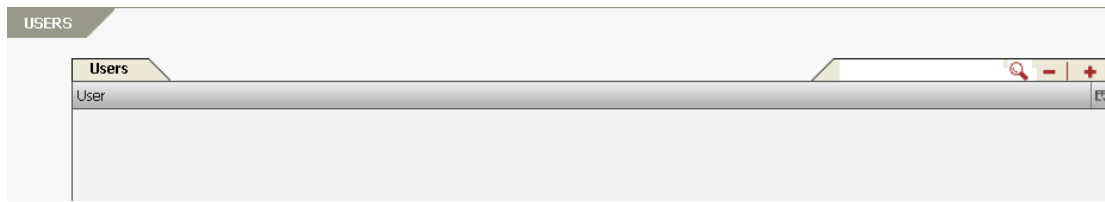


Figure 4–27 Users

Specify the parameters **Username**, **Password**, and **Confirm Password** in the **Users** area, and click **Apply** to add a user, as shown in Figure 4–28.

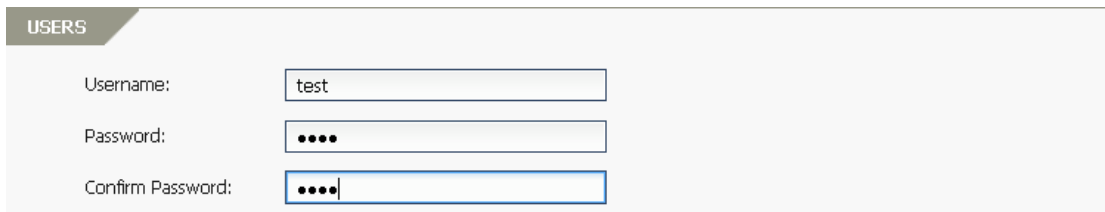


Figure 4–28 Add a User

To add a LocalDB group, select **Site Settings > AAA > Authorization > Authorization**, select the **Groups** feature link in the **Basic Tasks** area, and click + in the **Groups** area, as shown in Figure 4–29.

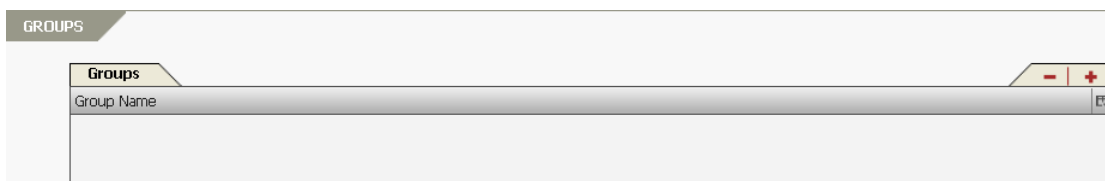


Figure 4–29 Groups

Specify the **Group Name** in the **Add Group** area, select specific users from the **Available Users** table, and click >> to add them to the group, as shown in Figure 4–30.

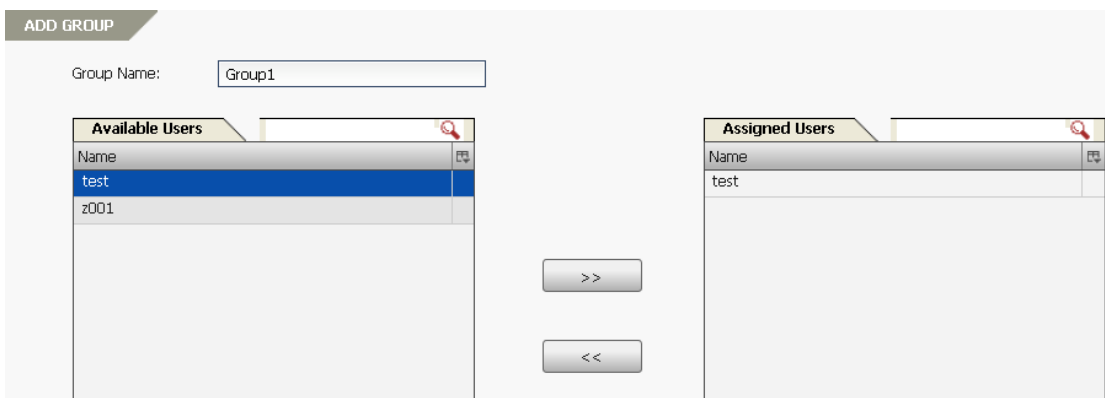


Figure 4–30 Add a Group

4.1.2.2 Group Mapping

With the Group Mapping function, AG can assign resources to users based on the external groups to which they belong.

To use this function, the administrator can add a group mapping entry to map an AD, LDAP or RADIUS external group to a local group. The users of the external group will be authorized with resources that are authorized to the mapped local group.

To add a group mapping entry, select **Site Settings > AAA > Authorization > Group Mapping > Group Mapping**, and click + in the **Group Mapping** area, as shown in Figure 4–31.

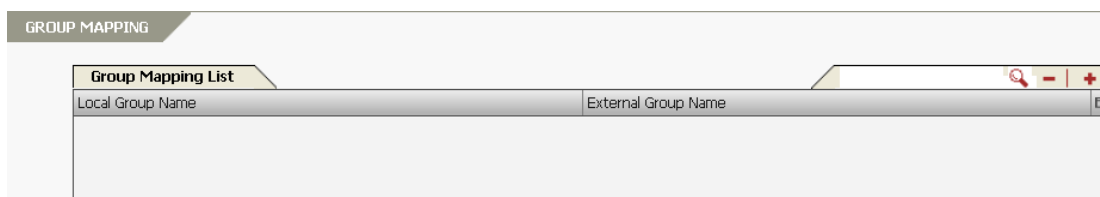


Figure 4–31 Group Mapping

Select a LocalDB group from the **Local Group Name** drop-down list in the **Group Mapping** area, and specify the **External Group Name** text box, as shown in Figure 4–32.

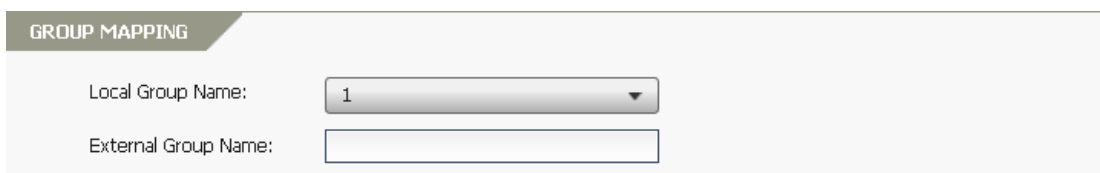


Figure 4–32 Adding a Group Mapping Entry



Note: If the authentication method is not LocalDB, a corresponding LocalDB user/group or group mapping for this user authentication method must be created for authorization.

4.1.3 Auditing

The Auditing function allows the administrator to view the session logs and traffic logs of MotionPro clients.

On MotionPro Pilot, select **Site Settings > AAA > Auditing**, specify the **Options** parameter and the **Content** text box in the **Device Auditing** area and then click **Filter** action link to search for specific session logs. These session logs will be listed in the **Device Auditing** table, and can be cleared or exported by clicking the **Clear** or **Export** action link, as shown in Figure 4–33.

DEVICE AUDITING Filter | Clear | Export

Options: ▼

Content:

Device Auditing							
Time	Level	Type	Eid	DeviceID	User Name	Message	ES
2013-10-24 17:50:49	INFO					Session deletion succeeded.	
2013-10-24 17:50:49	INFO	vpn			z001	VPN: Virtual IP (1.0.0.1) has been released.	
2013-10-24 17:50:49	NOTICE	vpn			z001	VPN: An existing VPN tunnel has been terminated.	
2013-10-24 17:50:49	INFO	\"MotionPro\"	1000000d	J7MEOMA...	z001	session idletime timeout	
2013-10-24 17:50:49	INFO				z001	Session idletime has reached the configured limit (last active t...	

Figure 4–33 Device Auditing

4.2 Authorized Resources

The MotionPro virtual site can assign Web resources, Native Applications and DesktopDirect resources to mobile users.

4.2.1 Secure Browser

Secure Browser is a build-in application of the MotionPro client for accessing Web resources. All the data transmitted through Secure Browser will be encrypted by the SSL L3VPN tunnel. Therefore, users are assured a higher level security when they access Web resource using Secure Browser than other regular browsers.

Secure Browser supports the Post SSO function for Web resources. This function records the user credential for logging into the virtual site and sends the user credentials to the Web server once the Web resource is accessed. With this function, the user can log into the specified Web resource without re-entering the user credential.

4.2.2 Web Resources

MotionPro can display the links to Web resources authorized for users on the MotionPro client. Users can have direct access to authorized Web resources via Secure Browser by clicking these links on the MotionPro client.

To complete the configuration of Web resources, the administrators need to configure the Web applications.

4.2.2.1 Web App

On MotionPro Pilot, select **Site Settings > Authorized Resources > Web Resources > Web Resources**, select the **Web App** feature link in the **Basic Tasks** area, and click + in the **WebApp** area, as shown in Figure 4–34.



Figure 4–34 Web App

On the **WebApp** tab, specify the parameters **URL**, **Description**, and **Folder** in the **General Settings** area, and click **Apply** to add a Web app, as shown in Figure 4–35.



Figure 4–35 Add a Web App

On the **Assignment** tab, select the users or groups from the **Type** drop-down list in the **Assignment** area, choose specific users or groups from the **Available** table and click >> to assign the Web app to them, as shown in Figure 4–36.

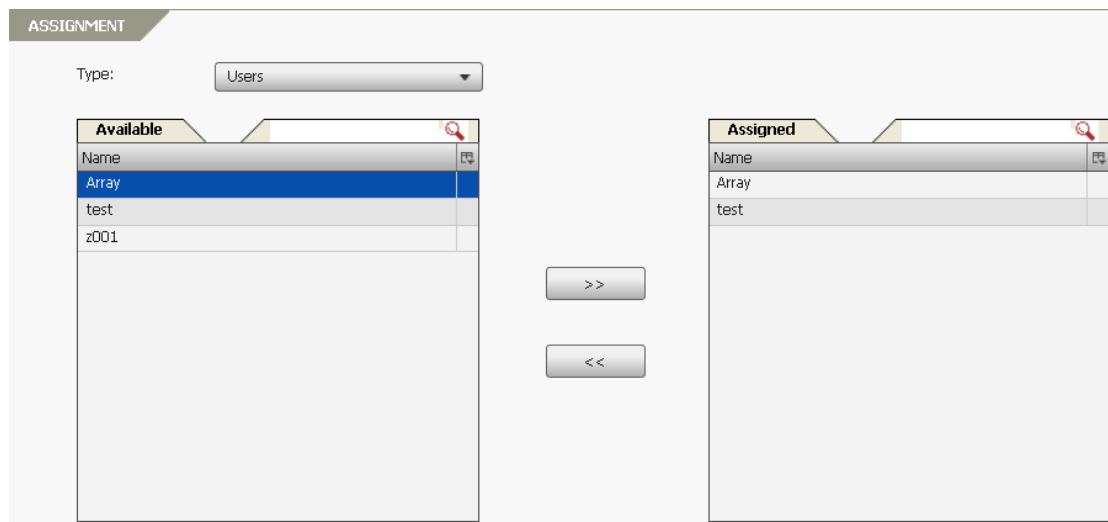


Figure 4–36 Assign a Web App

On the **WebApp** tab, specify the parameters **Post URL**, **Username Field**, **Password Field**, **Login URL**, **Post Fields**, and **Custom Cookies** in the **SSO Items** area, as shown in Figure 4–37.

GENERAL SETTINGS

URL:

Description:

Folder:

SSO ITEMS

Post URL:

Username Field:

Password Field:

Login URL: (Optional)

Post Fields: (Optional)

Custom Cookies: (Optional, For Example: aaa=ddd;bbb=eee)

Figure 4–37 Post SSO



Note: For details, please refer to Appendix I Set SSO Parameters.

4.2.3 Native Applications

Native Applications are local applications installed on mobile devices. MotionPro allows the administrator to create shortcuts to these applications; therefore users can directly and securely access such applications through the portal. If an application is not already installed, users will be prompted to download and install the application when they click the icon of the application on the MotionPro Client.

Native Applications can be divided into two types:

- **SDK Built-in Native Applications** integrate Application Tunnel API. All the data transmitted through this type of applications will be encrypted by the SSL L3VPN tunnel established by directly using the built-in application.
- **Other Native Applications** do not integrate Application Tunnel API. In order to encrypt the data transmitted through this type of applications, SSL L3VPN/IPsec VPN tunnels need to be established using the VPN on Demand (VoD) function for accessing enterprise resources.

On MotionPro Pilot, select **Site Settings > Authorized Resources > Native Applications > NativeApp**, and click + in the **NativeApp** area, as shown in Figure 4–38.

NATIVEAPP

NativeApp				
Name	Description	OS Type	App Type	Parameter

Figure 4–38 Native Applications

Specify the parameters **Application Name**, **Description**, **OS Type**, **Application Type** and **Parameters** in the **NativeApp** area on the **NativeApp** tab, and click **Apply** to add a native application, as shown in Figure 4–39.



Figure 4–39 Add a Native Application



Note:

- For Android, fill in the **Application Name** text box with the real application name to match the local applications on the mobile devices, and the real application names are listed on the Application manager settings of Android system.
- For iOS, the **Parameters** must be specified to match the local applications. For example, the **Parameters** for Safari can be “http://www.arraynetworks.com”. If the **Parameters** is not configured, the application will not be displayed on the MotionPro client.
- The uploaded custom icon has a higher priority than that of the Native application itself. After the administrator uploads a custom icon using the **Upload Icon** button, the custom icon will be displayed in the MotionPro client for the Native application.

On the **Assignment** tab, select the users or groups from the **Type** drop-down list in the **Assignment** area, choose specific users or groups from the **Available** table and click >> to assign the native application to them, as shown in Figure 4–40.

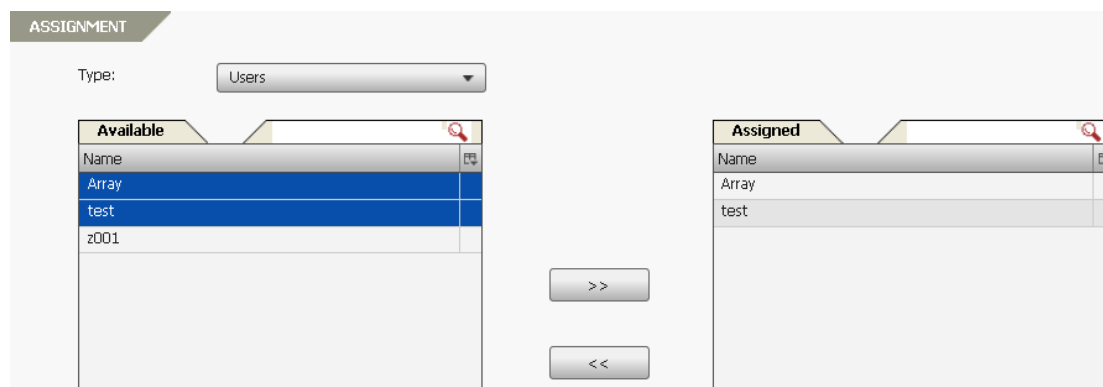
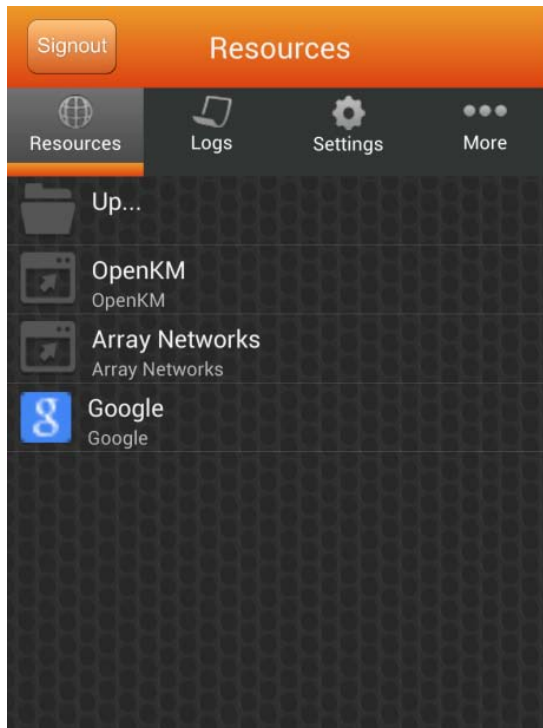


Figure 4–40 Assign a Native Application

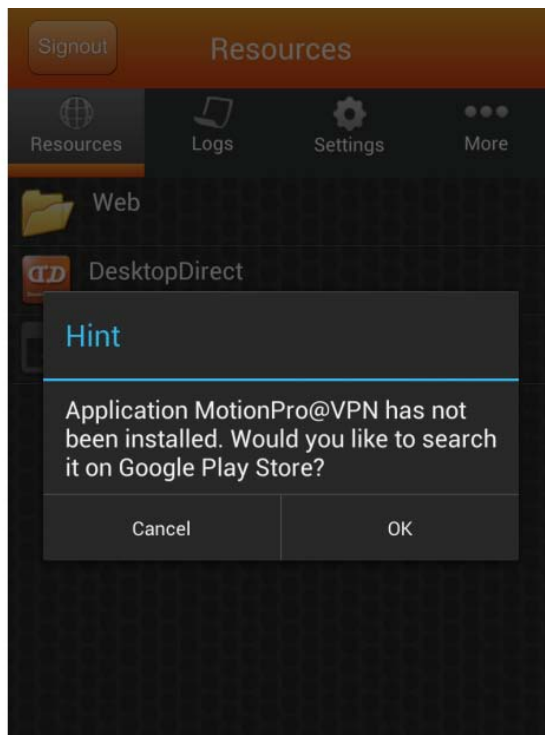
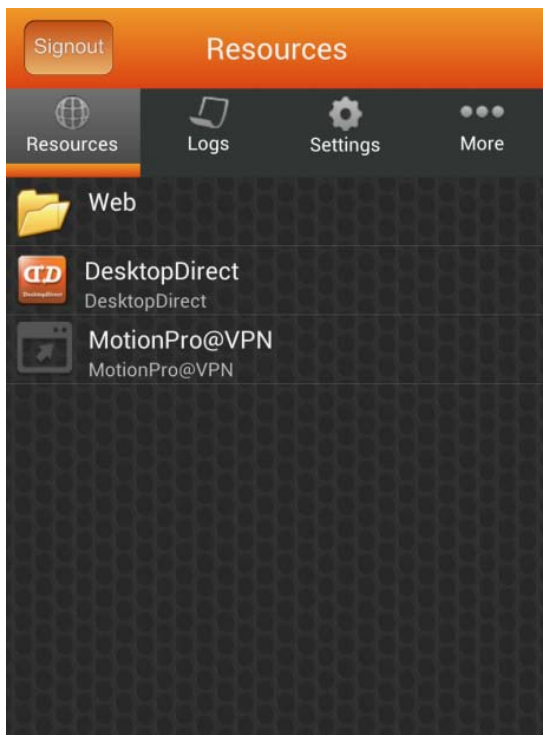
[Client Effect](#)

Users can click the web links to access Web resources.



Access denied by security policy, please contact your administrator.

Users can click the shortcuts to access native applications. If an application is not already installed, users will be prompted to download and install the application from the Google Play store or the Apple App store.



Client Effect End

4.2.4 DesktopDirect Resources

MotionPro now integrates MotionPro Desktop as a Native Application, through which the administrator can provide users with simple and secure access to DesktopDirect resources such as desktops and applications.

To distribute the DesktopDirect resources to end users, the administrator needs to configure DesktopDirect for a MotionPro type virtual site on DesktopDirect Pilot. For detailed configuration information, please refer to the DesktopDirect 4.0 Administration Guide.



Note:

- For iOS and Android to use the MotionPro Desktop feature, MotionPro client 2.1 or higher is required.
- To use the MotionPro client to access DesktopDirect resources, end users must install the Microsoft RD client first on their devices.

4.3 VPN on Demand

MotionPro will automatically establish the VPN tunnel between the AG appliance and mobile devices upon startup of a native application without VPN SDK built-in or access to intranet resources. By default, all VPN resources can be accessed. The Authorized Network is per-virtual-site, instead of per-user or per-group.

On MotionPro Pilot, select **Site Settings > VPN on Demand > VPN on Demand > VPN on Demand**, and click + in the **Authorized Network** area, as shown in Figure 4–41.

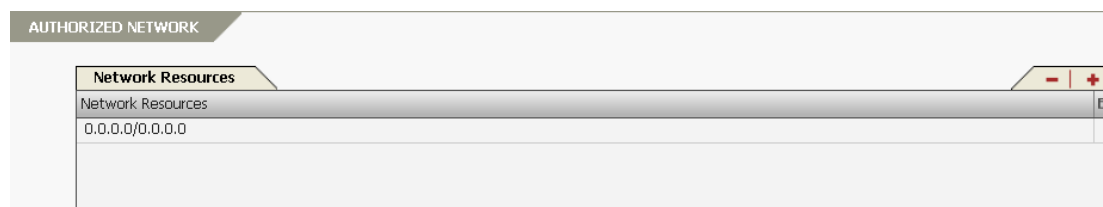


Figure 4–41 Network Resources

Specify **Network Resource** in the **Authorized Network** area, and click **Apply** to add an authorized network resource, as shown in Figure 4–42.

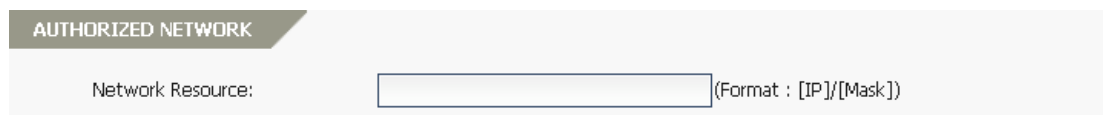


Figure 4–42 Add a Network Resource



Note: In split tunnel mode, data packets of applications on the mobile device will be transmitted through the VPN tunnel only when the destination IPs matching the authorized network. However, the data packets of the secure browser will always be transmitted

through the VPN tunnel established for the secure browser only.

Click + in the **Split DNS** area, as shown in Figure 4–43.

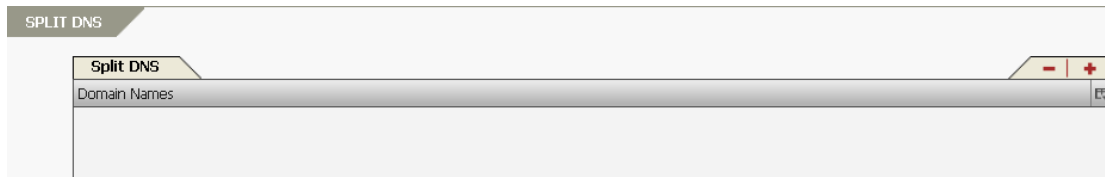


Figure 4–43 Split DNS

Specify **Split DNS Domain Name** in the **Split DNS** area, and click **Apply** to add a split DNS, as shown in Figure 4–44.

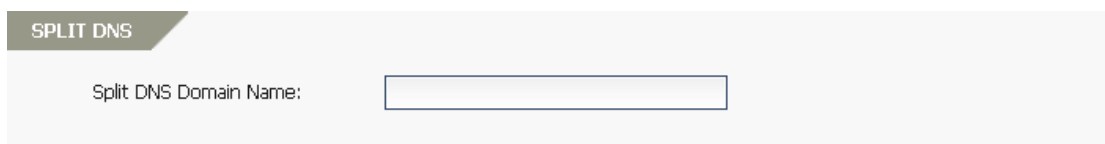


Figure 4–44 Add a Split DNS

➤ **VPN on Demand for Android**

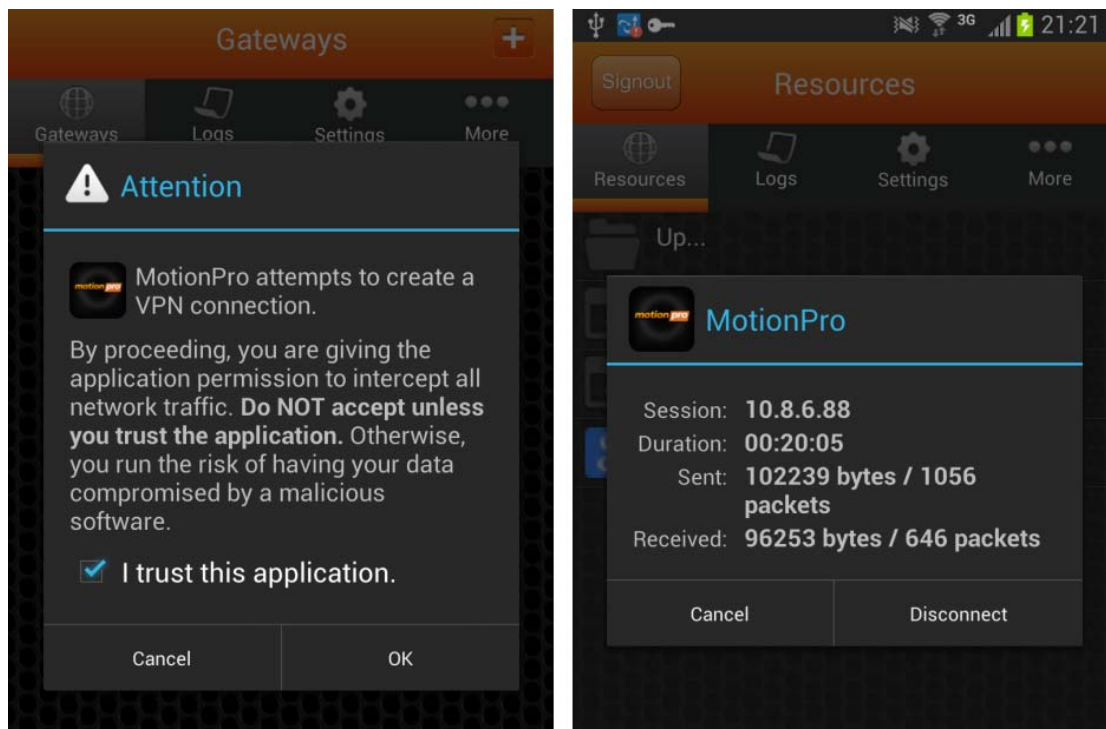
The standard SSL L3VPN tunnel will be established for Android clients, and it will not be terminated until the user logs out.



Note: Split DNS does not work for Android.

- In split tunnel mode, the DNS servers defined on AG will always take effect for VPN tunnel. If there’s no DNS server defined on AG, then the local DNS will take effect.
- In full tunnel mode, only the DNS servers defined on AG can take effect.

[Client Effect](#)



Client Effect End

➤ **VPN on Demand for iOS**

The IPSec VPN tunnel will be established for iOS clients. When the VPN tunnel disconnects after idle timeout, it can be restarted by launching the native application without VPN SDK built-in on the MotionPro client or accessing a VPN on Demand (VoD) domain through Safari.

Click + in the **VOD Domain** area, as shown in Figure 4-45.

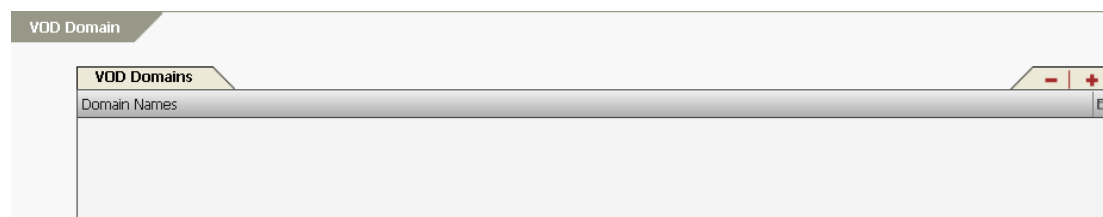


Figure 4-45 VOD Domain

Specify **VOD Domain Names** in the **VOD Domain** area, and click **Apply** to add a VOD domain name, as shown in Figure 4-46.



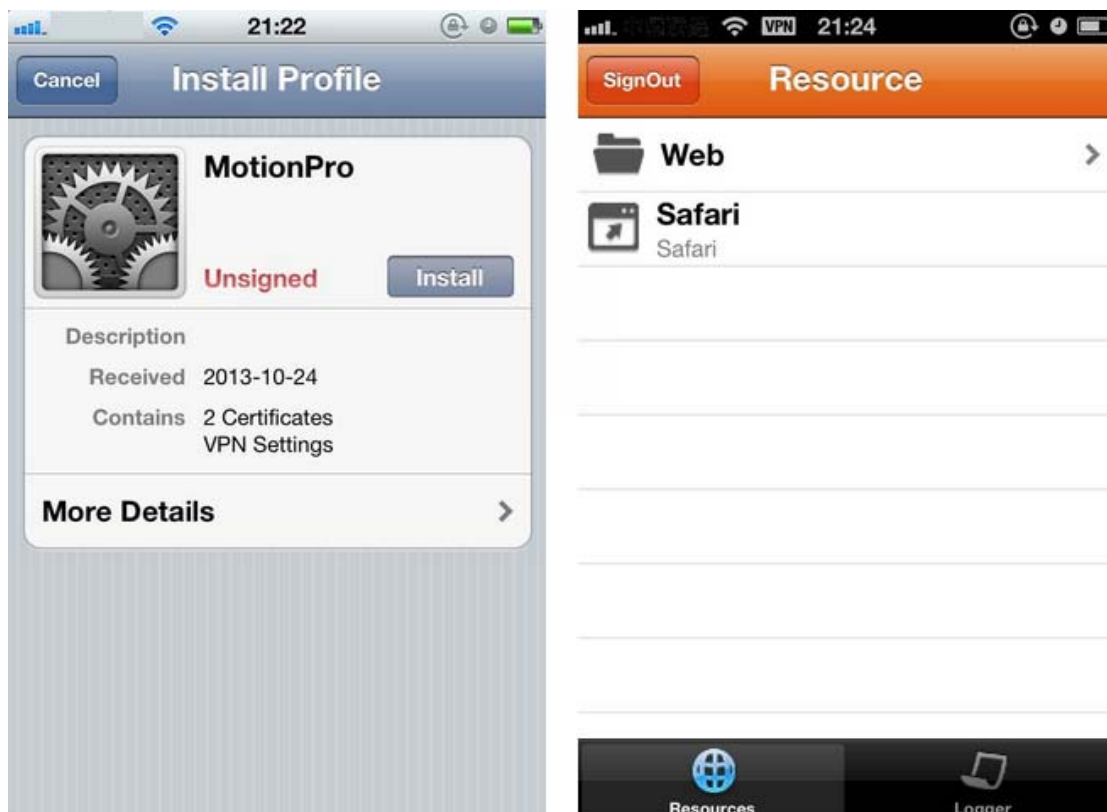
Figure 4-46 Add a VOD Domain Name



Note:

- The VoD domain cannot be configured as the virtual site FQDN or the domain name of other application servers. Otherwise, the iOS client will try to establish the VPN tunnel first when end users log into the virtual site or access the application server. As a result, end users cannot log into the virtual site with the MotionPro client or may fail to access the application server.
- Please make sure that ports 500 and 4500 can work normally.

Client Effect



Note: For iOS devices, the VPN profile must be installed to establish the IPSec VPN tunnel with AG. The administrator needs to instruct end users to reinstall the VPN profiles on iOS 7 or earlier in any of the following situations:

- The IP address of the virtual site has changed.
- The server certificate, root CA or intermediate CA is activated or deactivated for the virtual site.
- The VoD domain is added, deleted or edited for the virtual site (end users should reinstall the VPN profiles if they use the VPN on Demand function).

Client Effect End

Chapter 5 Enterprise Application Store

The Enterprise Application Store function provides the administrator with a convenient and effective way to release and upgrade enterprise applications to mobile users.

The administrator can upload the enterprise application packages or add the enterprise application links to the Enterprise Application Store of the MotionPro virtual site. After the administrator associates these enterprise applications with Native Applications which have been authorized to specific users, these users will have privileges to install or upgrade the enterprise applications with the MotionPro client.

5.1 Add Enterprise Applications to the Enterprise Application Store

On MotionPro Pilot, select **Site Settings > Enterprise Application Store > Enterprise Application Store > App Store**, click + in the **App Store** area, as shown in Figure 5–1.

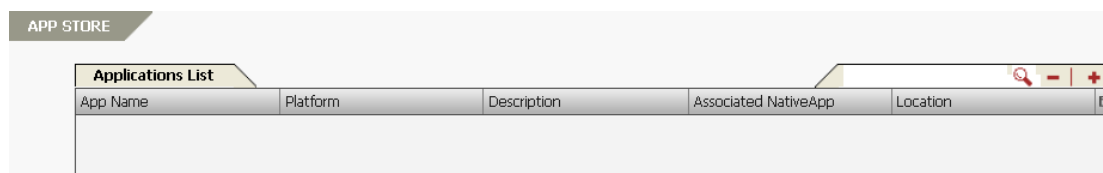


Figure 5–1 Enterprise Application Store

➤ **Upload a Local Enterprise Application Package**

- Upload the enterprise application package for iOS

On the **App Management** tab, select the **Platform** as “iOS” in the **Properties** area. Specify the parameters **App Name**, **Description** and **Location** (as “Local”). Click **Apply** to save the configuration first, then specify the parameter **Application Type** and click the **Upload** action link in the **App Package** area to upload local application packages. All the packages uploaded will be listed in the **Packages List** table and can be activated or removed by clicking the **Activate** or **Remove** action link, as shown in Figure 5–2.

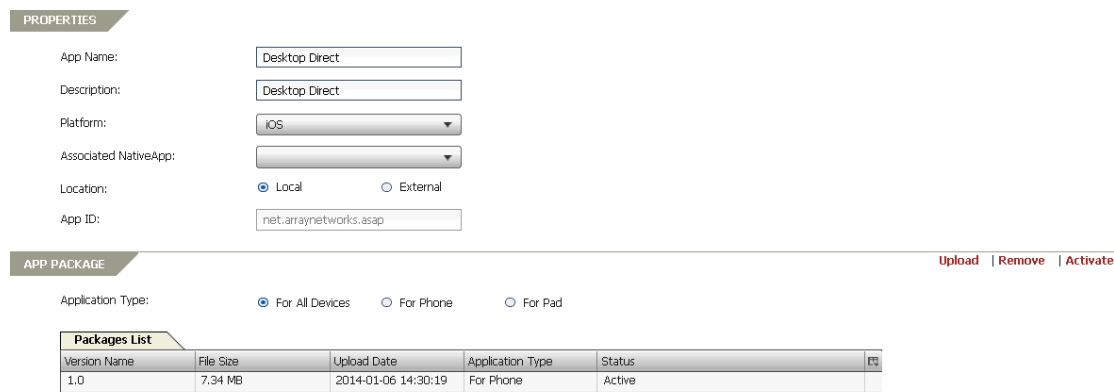


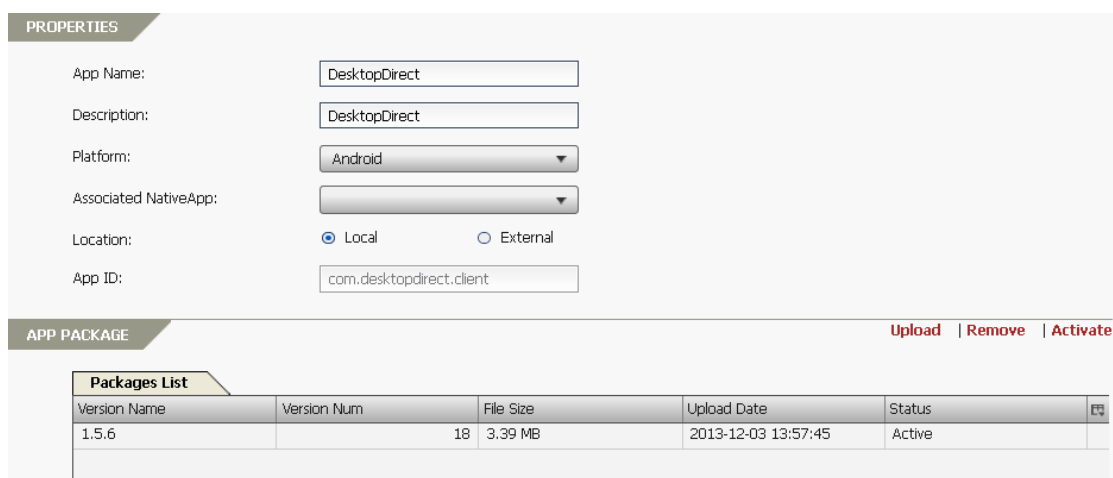
Figure 5–2 Upload a Local Application Package for iOS



Note: The iOS enterprise application packages need to be re-uploaded to the Enterprise Application Store if the IP address, port or FQDN of the virtual site is changed after they have been uploaded.

- Upload the enterprise application package for Android

On the **App Management** tab, select the **Platform** as “Android” in the **Properties** area. Specify the parameters **App Name**, **Description** and **Location** (as “Local”). Click **Apply** to save the configuration first, and then click the **Upload** action link in the **App Package** area to upload local application packages. All the packages uploaded will be listed in the **Packages List** table and can be activated or removed by clicking the **Activate** or **Remove** action link, as shown in Figure 5–3.



The screenshot shows the 'PROPERTIES' section with the following fields:

- App Name: DesktopDirect
- Description: DesktopDirect
- Platform: Android
- Associated NativeApp: (empty dropdown)
- Location: Local External
- App ID: com.desktopdirect.client

The 'APP PACKAGE' section shows a table with the following data:

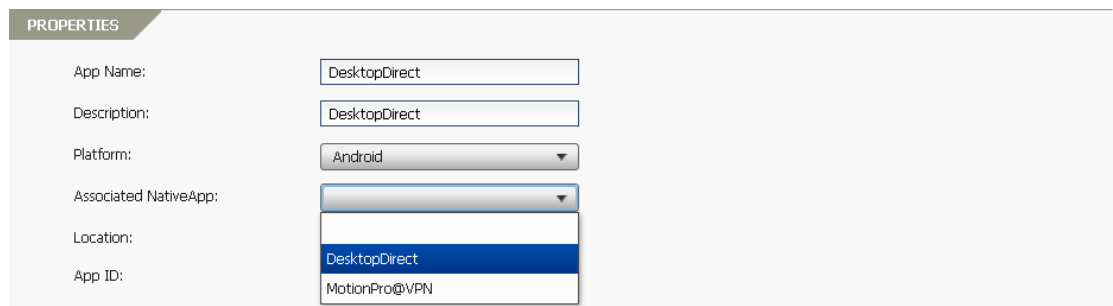
Version Name	Version Num	File Size	Upload Date	Status	
1.5.6	18	3.39 MB	2013-12-03 13:57:45	Active	

Figure 5–3 Upload a Local Application Package for Android



Note: The App ID of the first application package uploaded will be saved and cannot be changed. After that, only packages sharing the same App ID can be uploaded for this application.

After uploading the local package, choose the specific Native Application to be associated from the **Associated NativeApp** drop-down list in the **Properties** area, as shown in Figure 5–4.



The screenshot shows the 'Associated NativeApp' dropdown menu open, with the following options:

- DesktopDirect
- MotionPro@VPN

Figure 5–4 Associate the Local Application Package with a Native Application



Note: To remove an application from the Enterprise Application Store, the administrator must remove it before removing the associated Native Application.

➤ **Add an Enterprise Application from an External Link**

- Add the application link for iOS

On the **App Management** tab, select the **Platform** as “iOS” in the **Properties** area. Specify the parameters **App Name**, **Description** and **Location** (as “External”). Enter the official Apple App store installation link of the application package in the **Location URL** text box, as shown in Figure 5–5.

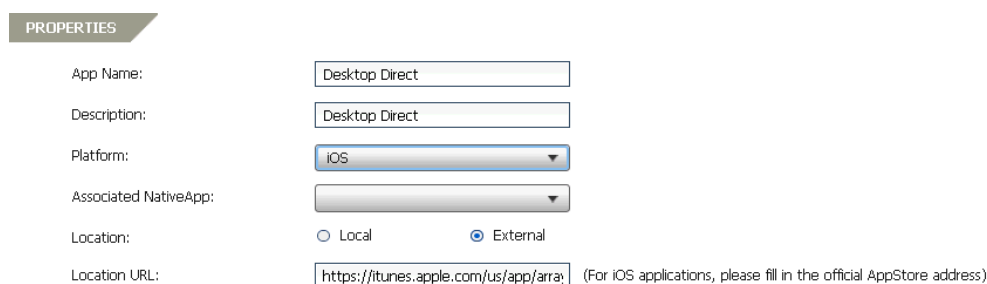


Figure 5–5 Upload an Application Package Link for iOS

- Add the application link for Android

On the **App Management** tab, select the **Platform** as “Android” in the **Properties** area. Specify the parameters **App Name**, **Description** and **Location** (as “External”). Enter the installation link of the application package in the **Location URL** text box, as shown in Figure 5–6.



Figure 5–6 Upload an Application Package Link for Android

After adding the package links, choose the specified Native Applications to be associated from the **Associated NativeApp** drop-down list in the **Properties** area, as shown in Figure 5–7.

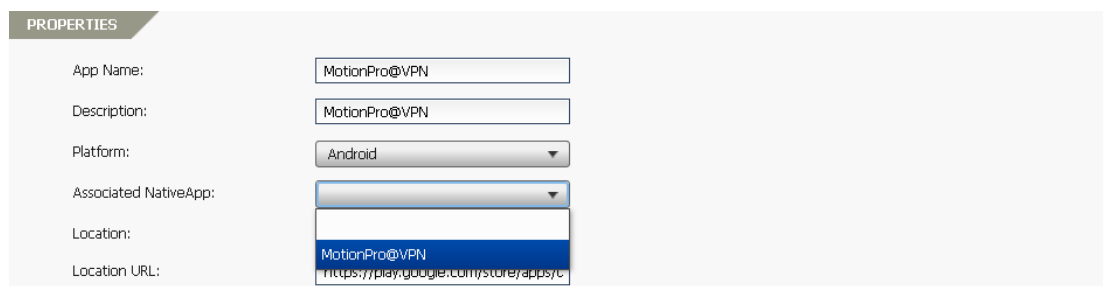


Figure 5–7 Associate the Application Package Link with a Native Application



Note: The application package links can only be associated with Native Applications that are not installed. Only under this circumstance, when users click the Native Application icon and the corresponding local application cannot be launched, the client will try to access the associated application package link; otherwise, the client will just launch the local application.

5.2 Release Enterprise Applications to Mobile Users

The Enterprise Application Store function can help the administrator to release enterprise applications to mobile users.

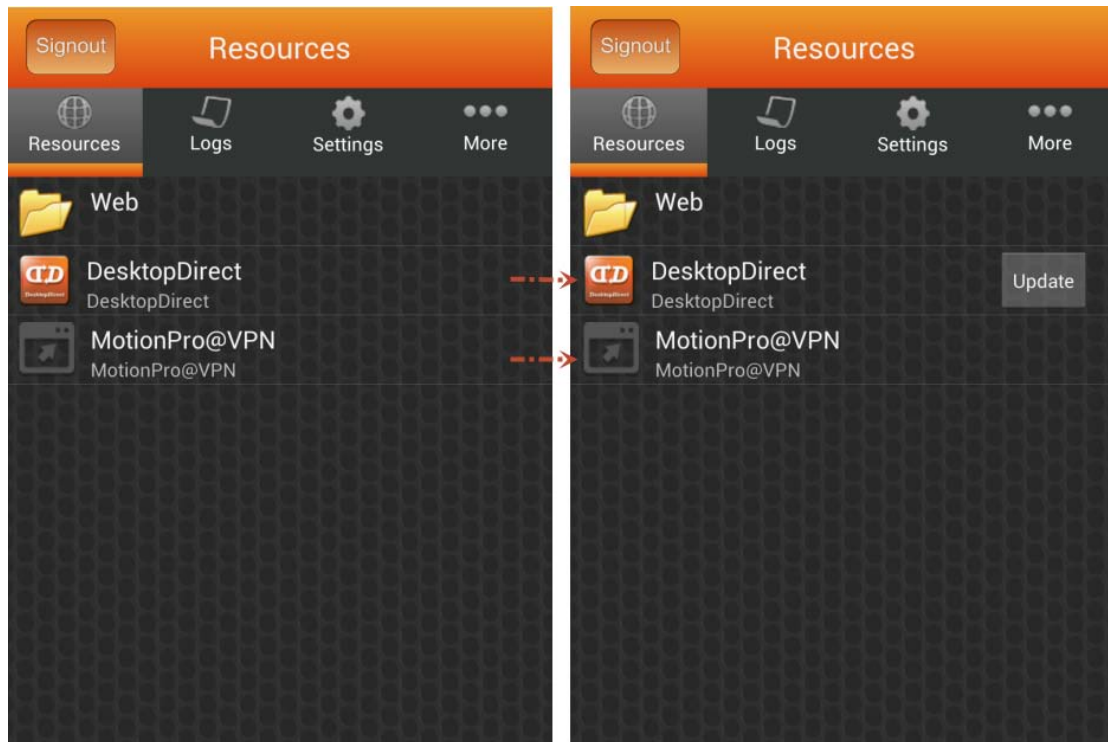
When the Enterprise Application Store releases a new enterprise application, the icon of the application and the **Install** button will be displayed on the MotionPro clients after mobile users successfully log into the MotionPro virtual site and have privileges to this application. Mobile users can install this application on their mobile devices by simply clicking the **Install** button.

When the Enterprise Application Store releases an updated enterprise application, the **Update** button will be displayed for the application on the MotionPro clients. Mobile users can update this application on their mobile devices by simply clicking the **Update** button.

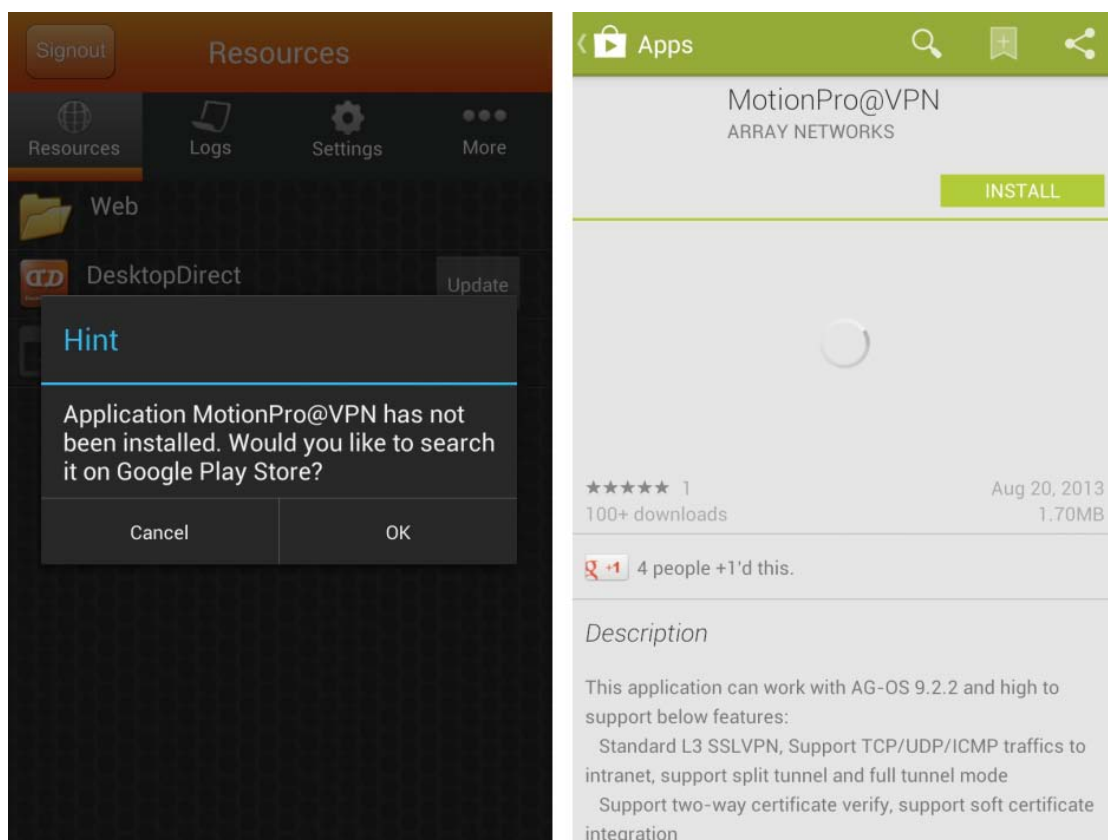
If the enterprise application to be released comes from an external URL, the Enterprise Application Store can release this application as a new application and the **Install** button will not be displayed. After clicking the icon of this application on the MotionPro clients, mobile users can download and install this application from the external URL.

Client Effect

After associating the enterprise application packages with Native Applications, mobile users will be notified when updated versions of the Native Applications are available.



After associating the application package links with Native Applications that are not installed yet, the client will try to access the associated application package link.



Client Effect End

Chapter 6 Enterprise Application Security

6.1 Security Policy

The Security Policy function allows the administrator to define different levels of security policies for the client and the server sides. These policies will execute automatically without the administrator’s intervention if the conditions of the policies are met.

6.1.1 Client Policy

The Client Policy function allows the administrator to define the client verification rule and apply the rule to specific users or groups. Actions defined in the rule will be performed when the associated trigger and conditions are met.

➤ **Basic configuration steps**

On MotionPro Pilot, select **Site Settings > Enterprise Application Security > Security Policies > Security Policies**, select the **Client Policy** feature link in the **Basic Tasks** area, and click + in the **Client Verification** area, as shown in Figure 6–1.

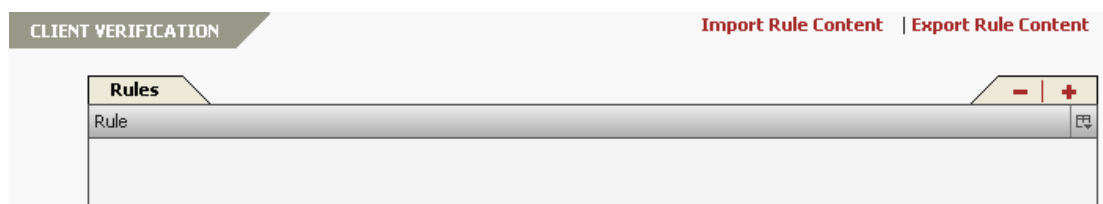


Figure 6–1 Client Verification

On the **Rule** tab, specify the parameters **Name** and **Trigger** in the **Rule** area, then right-click **Begin Rule** and select **Add Condition** to add a condition for the rule, as shown in Figure 6–2.

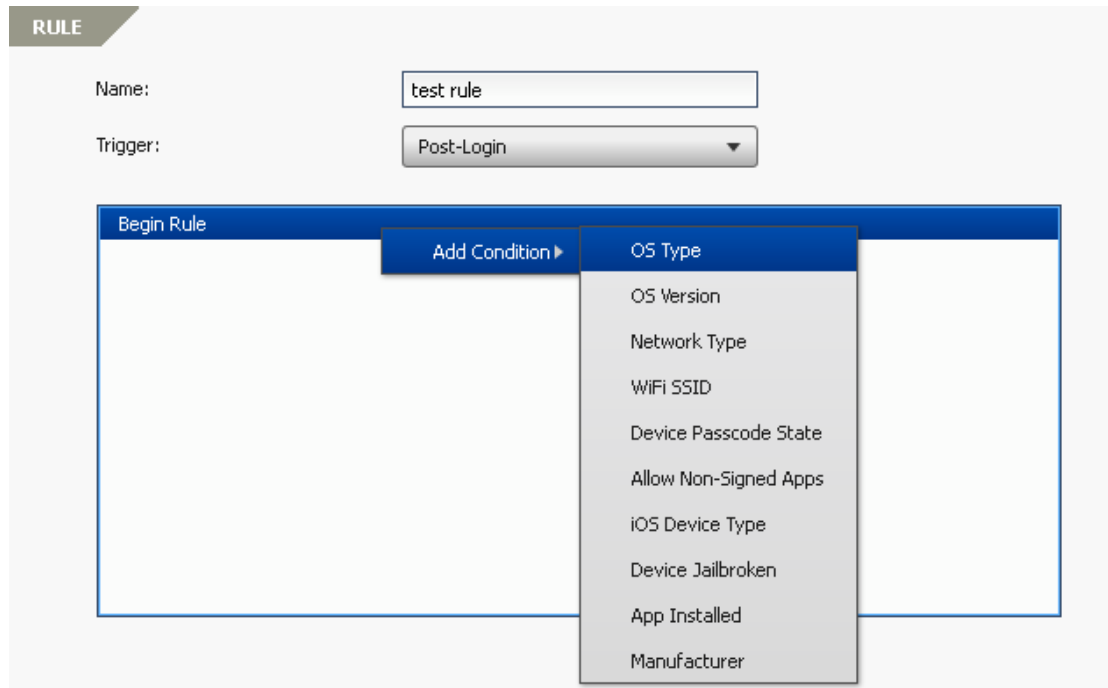


Figure 6–2 Add a Condition for a Rule

Right click the added condition and select **Add Action** to add an action for the rule. For example, certain message can be displayed to users using Android OS type, as shown in Figure 6–3.

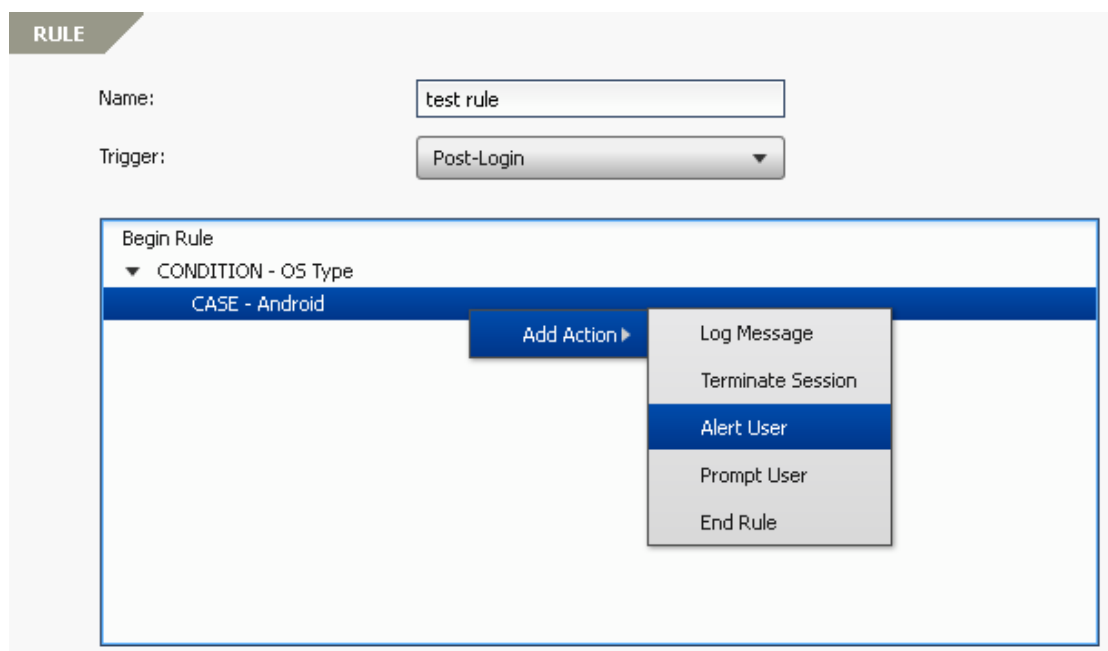


Figure 6–3 Add an Action for a Rule

On the **Associations** tab, select the users or groups from the **Associate With** drop-down list in the **Associations** area, choose specific users or groups from the **Available** table and click >> to assign client verification rules to them, as shown in Figure 6–4.

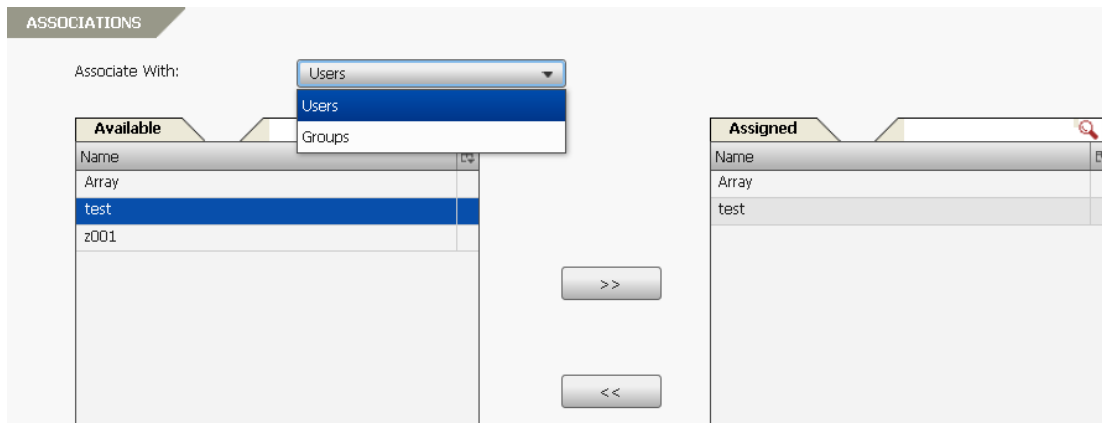


Figure 6–4 Associate the Client Verification Rule

To export a client verification rule, select a rule entry in the **Rules** table in the **Client Verification** area, click the **Export Rule Content** action link and click the **Yes** button in the prompted **Confirm** message box, as shown in Figure 6–5. Then choose a local path to save the file containing the configuration of the rule.



Figure 6–5 Export the Client Verification Rule

To import a client verification rule, click the **Import Rule Content** action link in the **Client Verification** area and click the **Upload** button in the prompted **Import Rule Content** dialog box to upload a file containing the configuration of the rule, as shown in Figure 6–6.

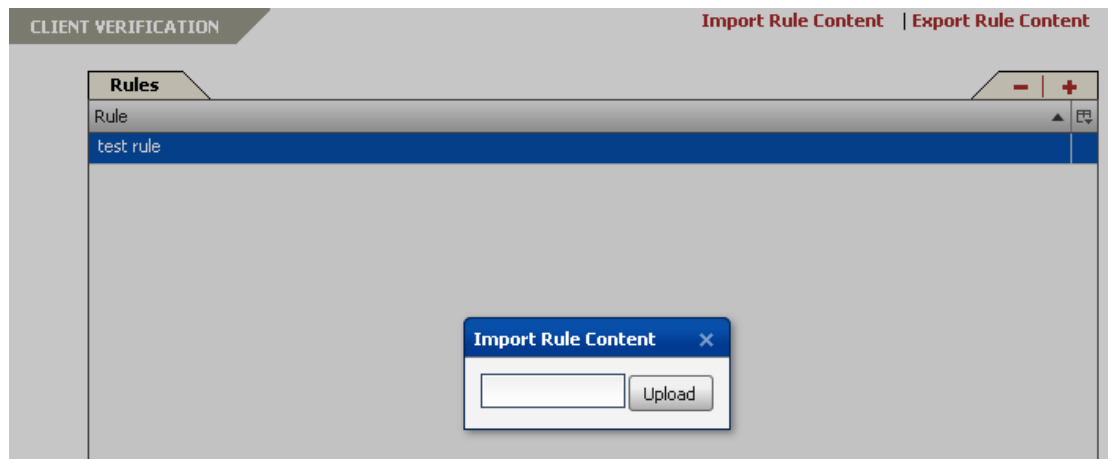
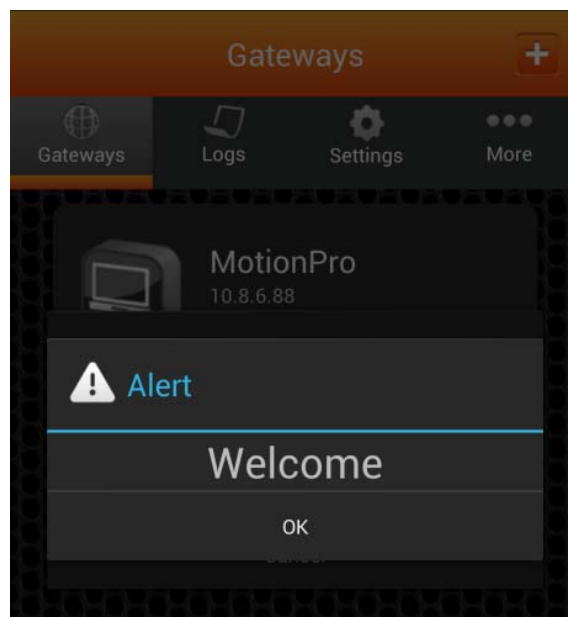


Figure 6–6 Import the Client Verification Rule

Client Effect

According to the example mentioned above, after login, an alert message will be displayed to users using Android OS type.



Client Effect End

➤ **Detailed description of the rule-related options**

Trigger:

- **Pre-Login:** CANNOT be assigned to any user or group because it affects all users by default. The check takes effect right before user login.
- **Post-Login:** MUST be assigned to a user or group. The check takes effect right after user login.
- **Timer:** MUST be assigned to a user or group. The check takes effect at a specified time after user login.

Condition:

- **OS Type:** iOS or Android
- **OS Version:** a string to fully match the OS version, such as “6.0.2” or “Android4.2”. Note that:
 - For iOS devices, the string is the version number which is exactly the same with that on the device. For example, “6.0” cannot stand for iOS 6.0.x devices.
 - For Android devices, the string is consisted of two parts: Case-sensitive OS type “Android” and the version number which can only be two digits. For example, “Android4.2” stands for Android 4.2.x devices. There is no space character between the OS type and the version number.
- **Network Type:** Cellular or WiFi
- **WiFi SSID:** a string list to fully match the WiFi SSID. Generally speaking, WiFi SSID is the name of the WIFI used on the device, and can be found in the WiFi settings of the device, such as “MyWIFI”.
- **Device Passcode State:** On or Off, to check whether the passcode of the device is enabled.
- **Allow Non-Signed Apps:** True or False, to check whether the Android device allows non-signed applications.
- **iOS Device Type:** iPhone or iPad, to choose what type of iOS device the action should perform on.
- **Device Jailbroken:** True or False, to check whether the iOS device is jailbroken, or the Android device has root access.
- **App Installed:** to check whether the specific application is installed on the device.
- **Manufacturer:** to check whether the device is of the specific manufacturer, such as Samsung or Apple.



Note: The administrator cannot define conditions under another condition.

Action:

- **Log Message:** send the message to the AG appliance in silence.
- **Terminate Session:** terminate the session and enforce user to log out.
- **Alert User:** prompt an alert message to the user.
- **Prompt User:** prompt the message to the user with a log message and two options, the log message and the option selected by the user will be sent to the AG appliance.
- **End Rule:** this is a sign indicating the end of a rule. For example, if there are three actions in this rule, and this “End Rule” is the second action, then the third one will be skipped.

6.1.2 Server Policy

The Server Policy function allows the administrator to define the remote device management policy. The actions defined in this policy will be performed when associated conditions are met.

For example, through the blacklist/whitelist policy, the MotionPro server will install whitelist applications on the mobile devices automatically, or the MotionPro server will terminate the VPN session when blacklist applications are installed on mobile devices.

➤ Basic configuration steps

On MotionPro Pilot, select **Site Settings > Enterprise Application Security > Security Policies > Security Policies**, select the **Server Policy** feature link in the **Basic Tasks** area, and click + in the **Policy** area on the **Policy** tab, as shown in Figure 6–7.

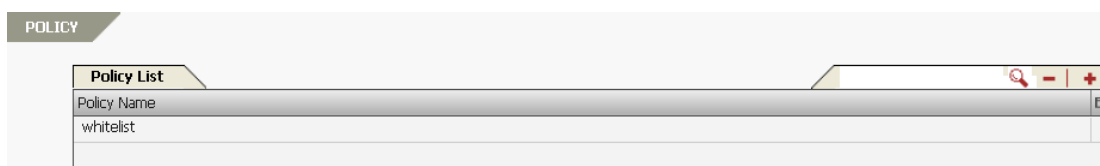


Figure 6–7 Add Server Policy

On the **Policy Management** tab, specify the parameters **Policy Name**, **Execute Condition When** and **Break** in the **Properties** area, as shown in Figure 6–8.

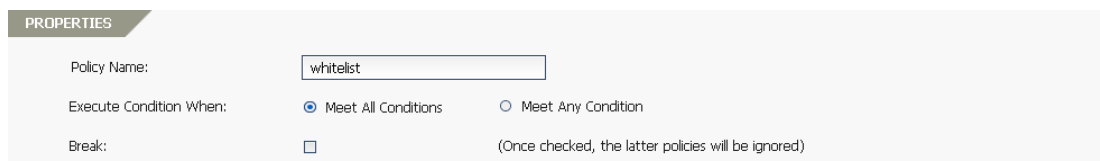


Figure 6–8 Set Sever Policy Properties

Specify the parameters **Condition Name**, **Subject**, **Predicate** and **Content** of the policy condition in the **Policy Condition** area, and click **Add** action link to add the condition to the **Condition List** table, as shown in Figure 6–9.

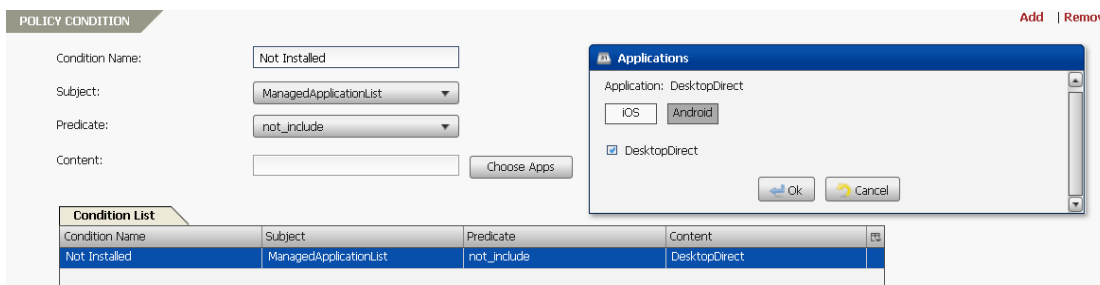


Figure 6–9 Set Server Policy Condition

Specify the **Action** parameter in the **Policy Action** area, and click **Add** action link to add the action to the **Action List** table, as shown in Figure 6–10.

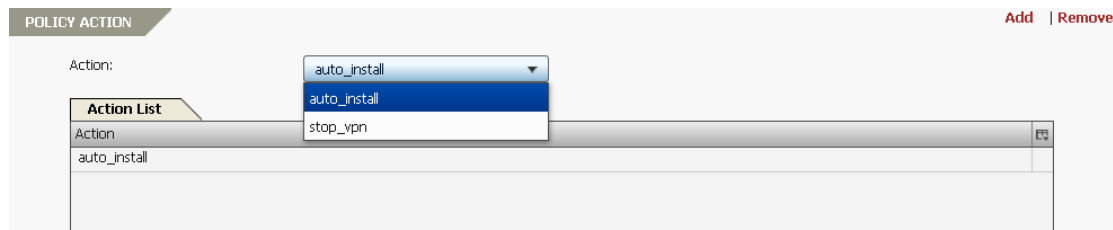


Figure 6–10 Set Server Policy Action

The newly added policy is listed in the **Policy List** table in the **Policy** area, as shown in Figure 6–7. On the **Assignment** tab, specify the **Type** parameter and assign the available policy, as shown in Figure 6–11.

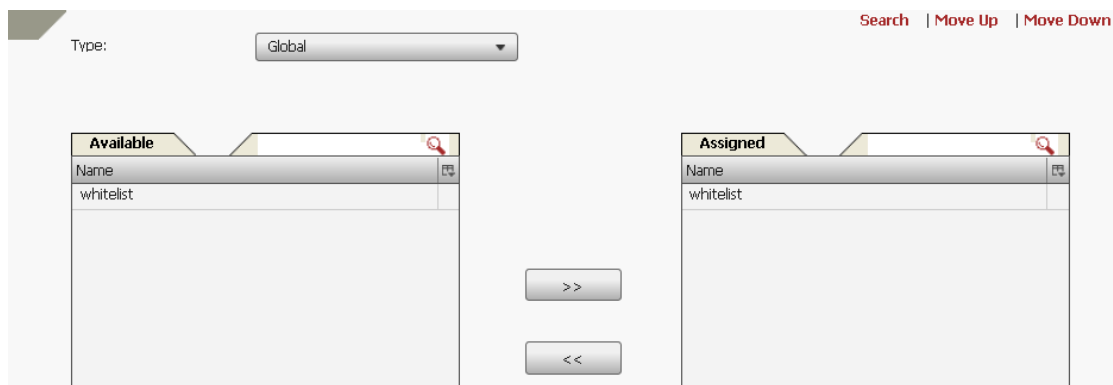


Figure 6–11 Assign the Policy

➤ **Detailed description of the rule-related options**

Properties:

- **Policy name:** specify the name of the policy.
- **Execute Condition When:** the administrator can define multiple conditions in the **Policy Condition** area. **Meet All Conditions** means the action will be executed only when all of the conditions are met. **Meet Any Condition** means the action will be executed when any of the conditions is met.
- **Break:** If this option is selected, when the action of this policy is executed, other policies associated to the same user will not be executed. If this option is cleared, every policy will be executed if the conditions are met.

Policy Condition:

- **Condition name:** specify the name of the condition.
- **Subject, Predicate and Content:** these three parameters specify the detailed configuration of a condition.
 - If the **Subject** is “username” or “group”, **Predicate** is “==”, and the **Content** is “admin”, that means when the login user or group is “admin”, the action defined in the **Policy**

Action area will be executed immediately. If the **Predicate** is “!=”, that means when the login user or group is not “admin”, the action will be executed.

- If the **Subject** is “InstalledApplicationList”, **Predicate** is “intersect”, and the **Content** is “Microsoft Remote Desktop”, that means when the Microsoft Remote Desktop is in the Installed Application List, the action defined in the **Policy Action** area will be executed immediately. Note: The administrator can get the name of an Android application through **System Settings > Applications list** on the Android device.
- If the **Subject** is “ManagedApplicationList”, **Predicate** is “not_include”, and the **Content** is “Microsoft Remote Desktop”, that means when the Microsoft Remote Desktop is not in the Managed Application List, the action defined in the **Policy Action** area will be executed immediately. Note: The **Content** of “ManagedApplicationList” can only be selected from the applications in the Enterprise Application Store by clicking the **Choose Apps** button besides the **Content** text box.



Note: To view the “InstalledApplicationList” or “ManagedApplicationList”, specify the **Type** drop-down list in the **Resource Information** area, which can be accessed by double clicking one specific entry in the **Devices** table of **Enterprise Application Security > Remote Device Management**, as shown in Figure 6–16 and Figure 6–17.

Policy Action:

- **stop_vpn** and **auto_install**: the action “stop_vpn” can be executed for any condition while the action “auto_install” can only be executed when the condition **Subject** is “ManagedApplicationList”.

6.2 Remote Device Management

The Remote Device Management function allows the administrator to remotely operate mobile devices. To realize this function, the Mobile Device Management (MDM) server is used to manage various remote operations such as installing or uninstalling applications, restoring factory settings, locking screen and clearing passcode.

6.2.1 Enable MDM and Set MDM Properties

On MotionPro Pilot, select **Site Settings > Enterprise Application Security > Remote Device Management > Remote Device Management**. In the **Property** area, select the **Enable MDM** check box and import the remote device management certificate by clicking the **Browser** button of **Import MDM Certificate**. Specify the parameters **Device Check Interval**, **Device Inactive Check Times**, **Database Check Interval** and **APN SSL Reconnect Interval (iOS only)** if required, as shown in Figure 6–12.

PROPERTY

Enable MDM:

Import MDM Certificate:

Device Check Interval: (Interval for MDM server to check mobile device status)

Device Inactive Check Times: (Max times of consecutive device checks for setting mobile device status as inactive)

Database Check Interval: (Interval for MDM server to check database for notification to be sent to mobile devices (Android) or APN (iOS))

APN SSL Reconnect Interval(iOS only): (Interval of SSL reconnection between MDM server and Apple push notification (APN) server)

Figure 6–12 Enable Remote Device Management



Note: To use this function, please make sure that ports 65200 and 65202 can work normally.

Before a mobile device can enroll in the remote device management, it must be registered with exactly the same username and DeviceID in **Device Registration and Management** first.

To register another user who shares the same device with an already registered user, select the **Bind Username** check box as mentioned in section 4.1.1.1 DeviceID Authentication, as shown in Figure 6–13.

DEVICEID

Reject Unregistered Device:

Auto Approve:

Bind Username:

Maximum Devices Per User:

Maximum Users Per Device:

Figure 6–13 Bind Username

The user will be asked to register his/her username when login. After registration, different users with the same device will be listed in the **DeviceID Accounts** table separately in the **Device Registration and Management** area, as shown in Figure 6–14.

DEVICE REGISTRATION AND MANAGEMENT

Search By:

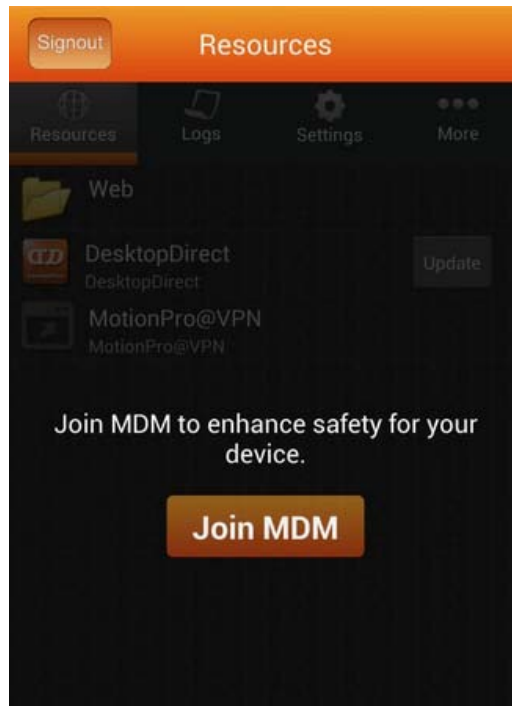
Search For:

DeviceID Accounts			
User Name	Device ID	Device Name	Status
	4E460B1D-55C5-4E77-825A-923050F45076	iphone Apple;iPhone6,2;iOS 7.0.4	approve
test	J7MEOMAQFCPDRHB7JH30S04CLFOCH3YK9DPGAVA9CVK=	test samsung;GT-19228;Android 4.1.2	approve
mdm	J7MEOMAQFCPDRHB7JH30S04CLFOCH3YK9DPGAVA9CVK=	mdm samsung;GT-19228;Android 4.1.2	approve

Figure 6–14 DeviceID Accounts

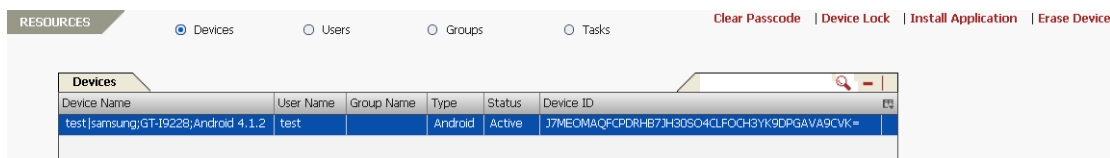
Client Effect

After login, users will be promoted to join remote device management (MDM).



Client Effect End

After joining MDM, all the information of registered devices will be listed in the **Resources** area and can be viewed according to **Devices**, **Users** or **Groups**, as shown in Figure 6–15.



Device Name	User Name	Group Name	Type	Status	Device ID
test[samsung;GT-I9228;Android 4.1.2]	test		Android	Active	J7MECMAQFCPDRHB7JH3DSO4CLFOCH3YK9DPGAVA9CVK=

Figure 6–15 Resource Information

6.2.2 Device Status/Application Poll

➤ **Device Status**

After enrollment, the MDM server will timely update device status including:

- **Un-joined**
- **Unmanaged:** Join but check out
- **Active:** Join and can manage
- **Un-active:** Join but offline

➤ **Application Poll**

The MDM server can also timely update the application status of the device:

- **Installed Application List:** List the information of all the applications installed on the device.

- **Managed Application List:** List the information of the applications managed by the MDM server.

Double click one specific entry in the **Devices** table, and select “Installed Application List” from the **Type** drop-down list in the **Resource Information** area, and all the installed applications of this device will be listed in the **Installed Application List** table, as shown in Figure 6–16.

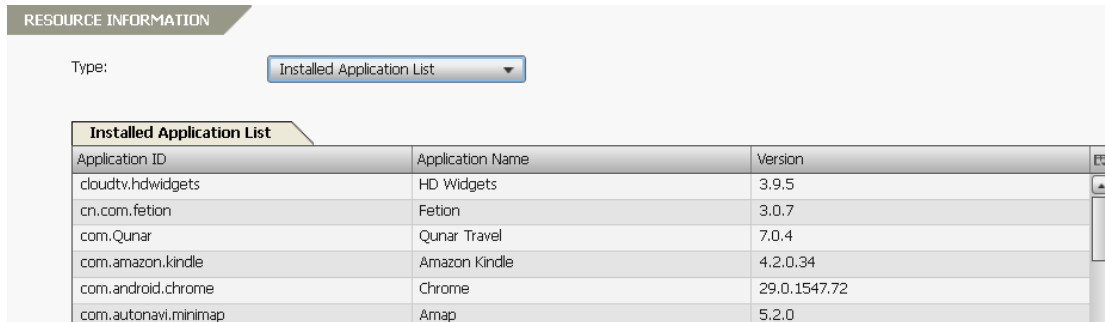


Figure 6–16 Installed Application List

Select the “Managed Application List” from the **Type** drop-down list in the **Resource Information** area, and all the managed applications of this device will be listed in the **Managed Application List** table, as shown in Figure 6–17.

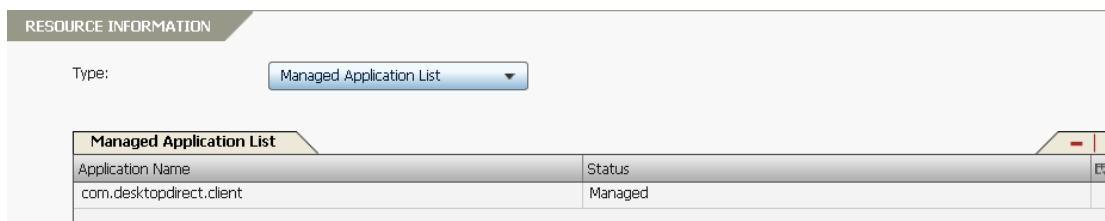


Figure 6–17 Managed Application List

6.2.3 Remote Device Action

➤ Install/Uninstall Application

To install an application, select the specific devices, users or groups to be installed on, and click the **Install Application** action link. Specify the **Task Name** text box, select the application to be installed from the **Apps** drop-down list in the **Task** message box and click the **Ok** button, as shown in Figure 6–18.

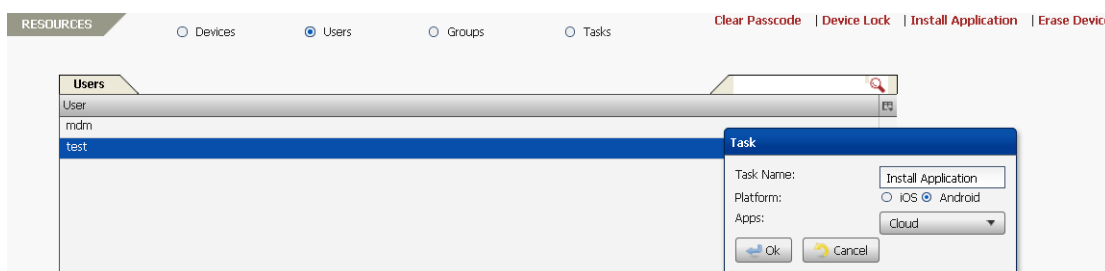
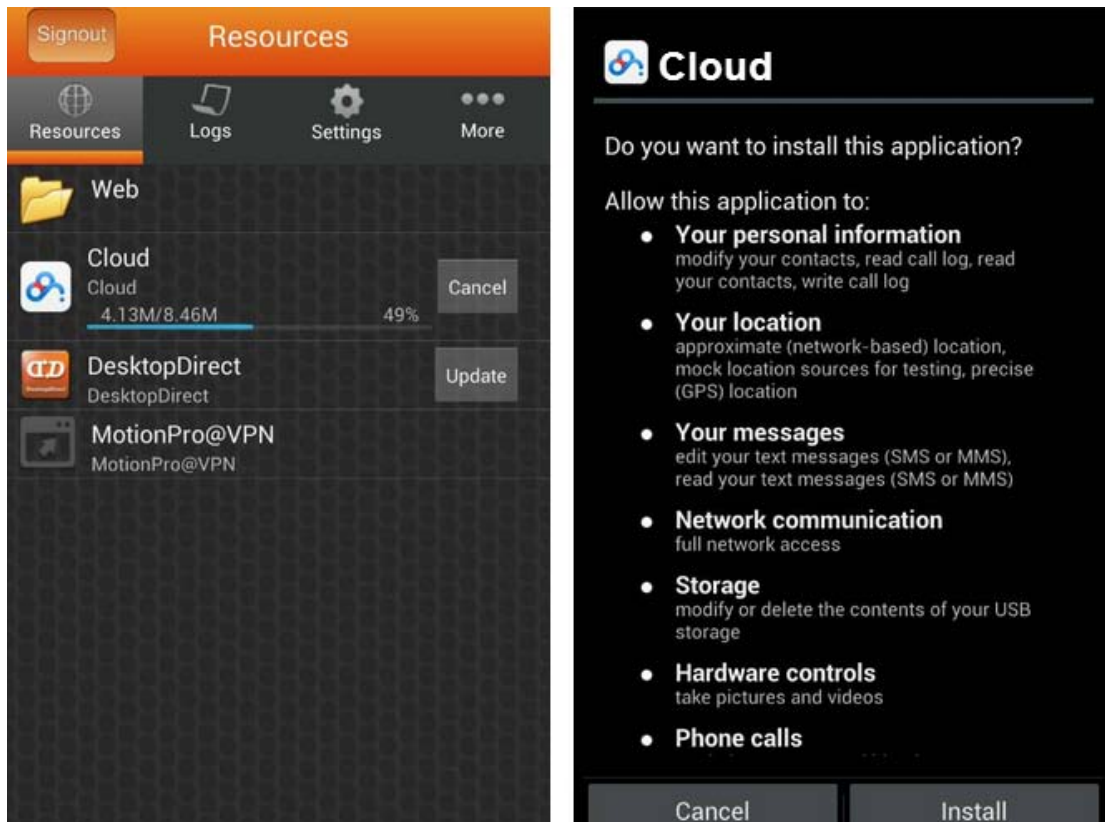


Figure 6–18 Install an Application

Client Effect



Client Effect End

To remove an application, select the application to be removed from the **Managed Application List** (see Figure 6–17) and click - to remove it.

➤ **Restore Factory Settings**

To wipe all the data of a device, select the action target and click the **Erase Device** action link in the **Resources** area, and click the **Ok** button to add the task, as shown in Figure 6–19.

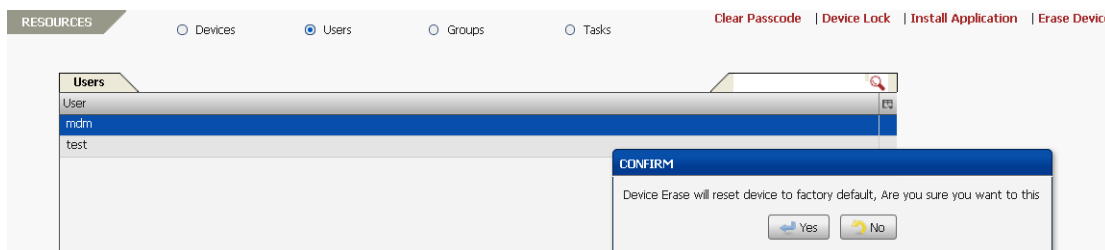


Figure 6–19 Restore Factory Settings

➤ **Lock Screen**

To lock the screen of a device, select the action target and click the **Device Lock** action link in the **Resources** area, specify the **Task Name** in the **Task** message box and click the **Ok** button to add the task, as shown in Figure 6–20.

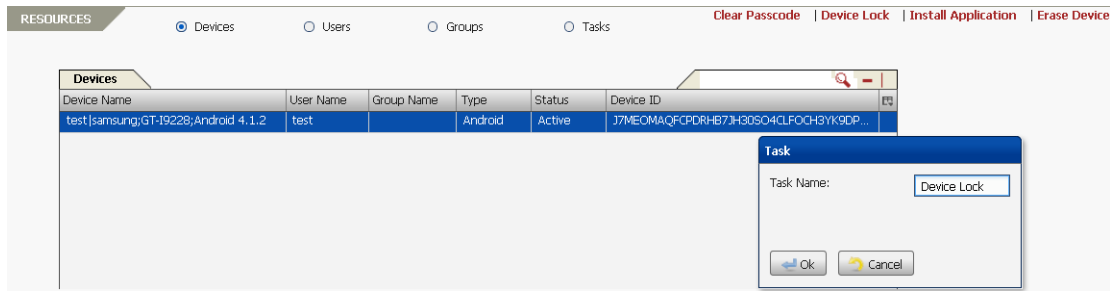


Figure 6–20 Lock Screen

➤ **Clear Passcode**

To clear the passcode of a device, select the action target and click the **Clear Passcode** action link in the **Resources** area, specify the **Task Name** in the **Task** message box and click the **Ok** button to add the task, as shown in Figure 6–21.

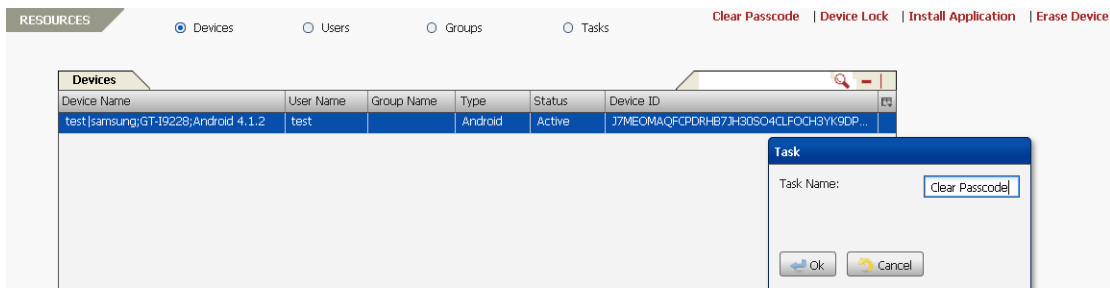


Figure 6–21 Clear Passcode

After adding tasks, select the **Tasks** radio button to view the status of each task in the **Tasks** table, as shown in Figure 6–22.

Task Name	Task Type	CMD Numbers	Success Numbers	Failure Numbers	Create Time
Clear Passcode	ClearPasscode		1	0	Tue Dec 10 2013 10...
Device Lock	DeviceLock		1	0	Tue Dec 10 2013 10...
Install Application	InstallApplication		1	0	Tue Dec 10 2013 10...

Figure 6–22 Tasks

Click the task to view the task information listed in the **Task Information** table in the **Task Information** area, as shown in Figure 6–23.

Device ID	Status	Error
J7MEOMAQFCPDRHB7JH30S04CLFOCH3YK9DPGAVA9CVK=	Success	

Figure 6–23 Task Information

Chapter 7 System Monitor

7.1 System Monitor

7.1.1 Device Registration and Management

7.1.1.1 Device Registration

The administrator can register devices to the system in advance.

On MotionPro Pilot, select **System Monitor > System Monitor > Device Registration and Management > Device Registration and Management**, click + to add a DeviceID account for a mobile device, as shown in Figure 7–1.

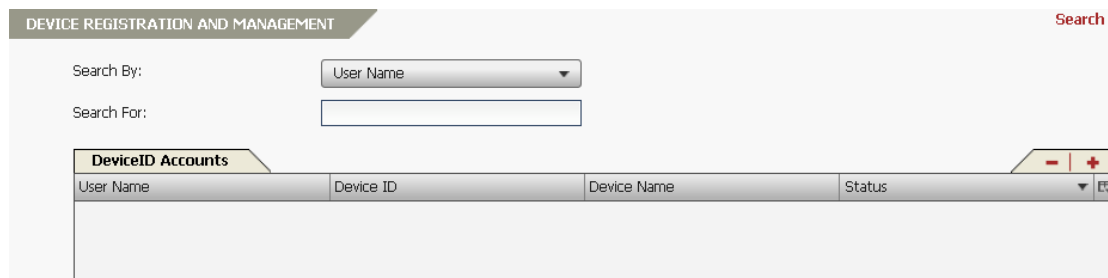


Figure 7–1 Device Registration

In the **Device Account** area, specify the parameters **Username**, **Device_ID**, **Device_name** and **Status**, as shown in Figure 7–2.

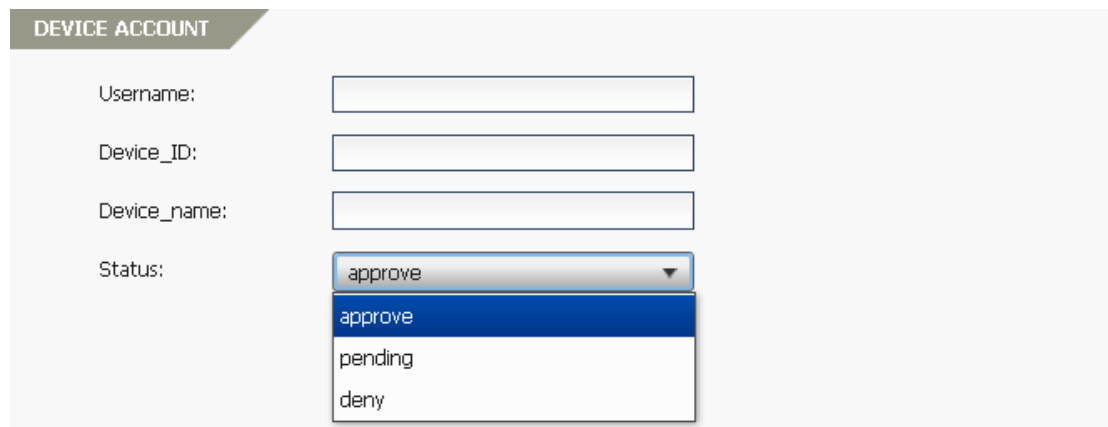


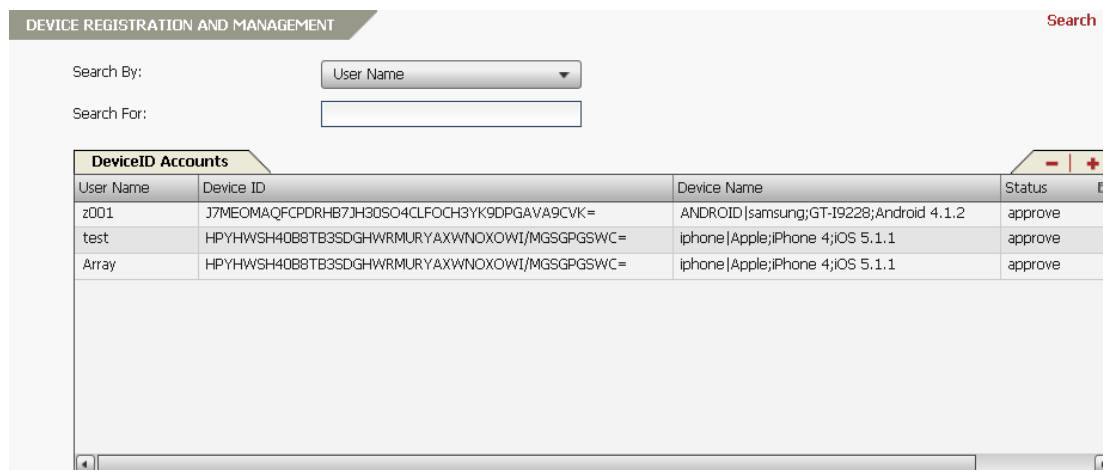
Figure 7–2 Add a Device Account

Mobile users can register their devices during the DeviceID authentication (please refer to section 4.1.1.1 DeviceID Authentication) when the devices have not been registered. Note that the administrator needs to provide the mobile user with a LocalDB username and password to be used for registration. For details about how to add a LocalDB user, please refer to section 4.1.2.1 User/Group.

7.1.1.2 Device Management

After device registration, the administrator can monitor and manage device status.

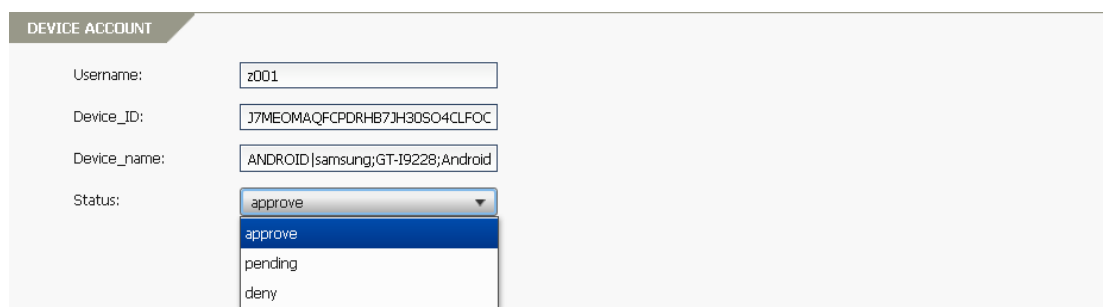
On MotionPro Pilot, select **System Monitor > System Monitor > Device Registration and Management > Device Registration and Management**, and all the registered devices will be listed in the **DeviceID Accounts** table in the **Device Registration and Management** area. Specify the **Search By** drop-down list and the **Search For** text box, and click **Search** action link to search for specific device information, as shown in Figure 7–3.



DEVICE REGISTRATION AND MANAGEMENT				Search
Search By:		User Name		
Search For:				
DeviceID Accounts				- +
User Name	Device ID	Device Name	Status	
z001	J7MEOMAQFCPDRHB7JH30SO4CLFOCH3YK9DPGAVA9CVK=	ANDROID samsung;GT-19228;Android 4.1.2	approve	
test	HPYHWSH40B8TB3SDGHWRMURYAXWNOXOWI/MGSGPGSWC=	iphone Apple;iPhone 4;iOS 5.1.1	approve	
Array	HPYHWSH40B8TB3SDGHWRMURYAXWNOXOWI/MGSGPGSWC=	iphone Apple;iPhone 4;iOS 5.1.1	approve	

Figure 7–3 DeviceID Accounts List

Click the specific DeviceID account entry, and specify the **Status** drop-down list, as shown in Figure 7–4.



DEVICE ACCOUNT

Username:

Device_ID:

Device_name:

Status:

- approve
- pending
- deny

Figure 7–4 Manage a Device Account

The administrator can set status of devices to:

- **Approve:** Device access is permitted.
- **Pending:** Device access is not permitted until status is approved by the administrator.
- **Deny:** Device access is not permitted.

7.1.2 DeviceID Import and Export

The Import and Export function allows the administrator to:

- Import the device IDs from a configuration file on the appliance’s disk or the specified remote TFTP server to the virtual site’s database.
- Export the device IDs from the virtual site’s database to a configuration file on the appliance’s disk or the specified remote TFTP server.

Select **System Monitor > System Monitor > DeviceID Import and Export**, specify the **Options** parameter and other parameters as required, and then click the **Import** or **Export** action link in the upper-right corner of the **DeviceID Import and Export** area, as shown in Figure 7–5.

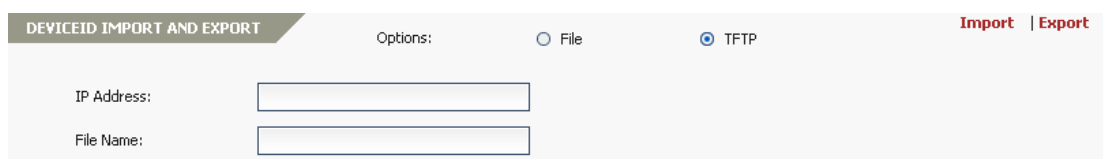


Figure 7–5 Import or Export the Device IDs



Note:

- The files imported from the appliance’s disk or the remote TFTP server must be in the UTF-8 encoding format. Otherwise, the importing might fail.
- The files exported to the appliance’s disk or the remote TFTP server are in the UTF-8 encoding format. To read or edit the exported file, make sure that your file viewer or editor supports UTF-8 encoding.

7.1.3 Session Management

The administrator can also manage mobile client sessions.

On MotionPro Pilot, select **System Monitor > System Monitor > Session Management > Session Management**, and all the active sessions will be displayed in the **Active Sessions** table in the **Session Management** area. Specify the parameters **Session Type**, **Session User Name** and **Session DeviceID** as filters to search for specific sessions, as shown in Figure 7–6.

SESSION MANAGEMENT Search

Session Type:

Session User Name:

Session DeviceID:

Active Sessions							
Session User Name	Session Type	Session ID	Session Age(hh:mm:ss)	Last Active(hh:mm:ss)	Authenticate	Device ID	Parent Session ID
z001	ssl	C5CF5C28	00:12:47	00:12:42	Authenticated	J7MEOMAQ...	0

Figure 7–6 Session Management

To terminate specific sessions, select the active session entry and click -.



Note: MotionPro session behavior changes in different situations:

- For Android devices:
 - AG will update the “Last Active” timer for the SSL session once there is real traffic in the SSL VPN tunnel, and will terminate the SSL session after lifetime/idle timeout.
- For iOS devices:
 - If the IPsec session is established via the Microsoft RD client, AG will update the “Last Active” timer for the parent login session and the child IPsec session simultaneously every 5 seconds until both sessions are terminated after lifetime timeout.
 - If no IPsec session is established, AG will update the “Last Active” timer according to MotionPro login/logout action and terminate the login session after lifetime/idle timeout.

7.2 System Management

7.2.1 Import and Export

The Import and Export function allows the administrator to:

- Import the MotionPro CLI configurations from a configuration file on the appliance’s disk or the specified remote TFTP server to the virtual site’s database.
- Export the MotionPro CLI configurations from the virtual site’s database to a configuration file on the appliance’s disk or the specified remote TFTP server.

Select **System Monitor > System Management > MotionPro Import and Export**, specify the **Options** parameter and other parameters as required, and then click the **Import** or **Export** action link in the upper-right corner of the **MotionPro Import and Export** area, as shown in Figure 7–7.

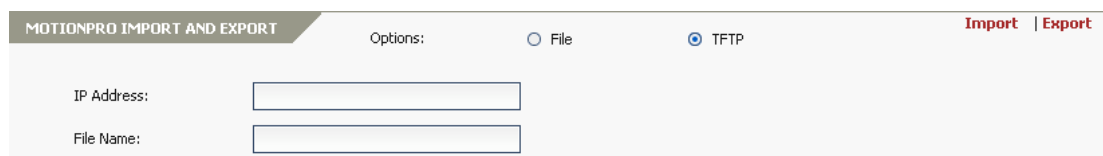


Figure 7–7 Import or Export the MotionPro Configurations



Note:

- The files imported from the appliance’s disk or the remote TFTP server must be in the UTF-8 encoding format. Otherwise, the importing might fail.
- The files exported to the appliance’s disk or the remote TFTP server are in the UTF-8 encoding format. To read or edit the exported file, make sure that your file viewer or editor supports UTF-8 encoding.

7.2.2 Backup and Restore

The administrator can back up the MotionPro configurations to the remote TFTP server or restore the MotionPro configurations from the remote TFTP server.

Select **System Monitor > System Management > MotionPro Backup and Restore**, specify the parameters **TFTP Server IP** and **File Name**, and then click the **Backup** or **Restore** action link in the upper-right corner of the **MotionPro Backup and Restore** area, as shown in Figure 7–8.

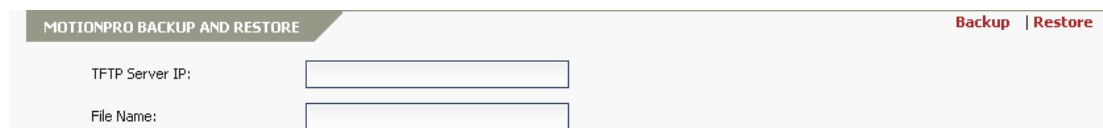


Figure 7–8 Back Up or Restore the MotionPro Configurations



Note:

- The files backed up to the remote TFTP server are in the UTF-8 encoding format. To read or edit the backed up file, make sure that your file viewer or editor supports UTF-8 encoding.
- The files restored from the remote TFTP server must be in the UTF-8 encoding format. To read or edit the restored file, make sure that your file viewer or editor supports UTF-8 encoding.

7.2.3 Portal Configuration

The administrators can configure whether a specific tab page will be displayed on the MotionPro portal. With this function, administrators can hide corresponding tab pages from end users when the system does not have the specific feature licensed.

Select **System Monitor > System Management > MotionPro Portal Configurations**, and specify the parameters **Web**, **Application** and **Desktop** in the **Tabpage Configurations** area, as shown in Figure 7–9.

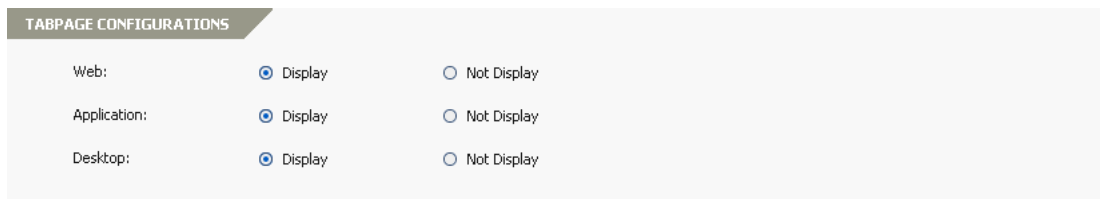


Figure 7–9 Configure Tab Page Display Mode

Appendix I Set SSO Parameters

Use **HttpWatch Professional** to help specify the parameters in **SSO Items** area.

HttpWatch Professional is a browser plug-in that collects and displays information about websites. After installation, launch it and then access the Web application to be added, as shown in Figure I-1.

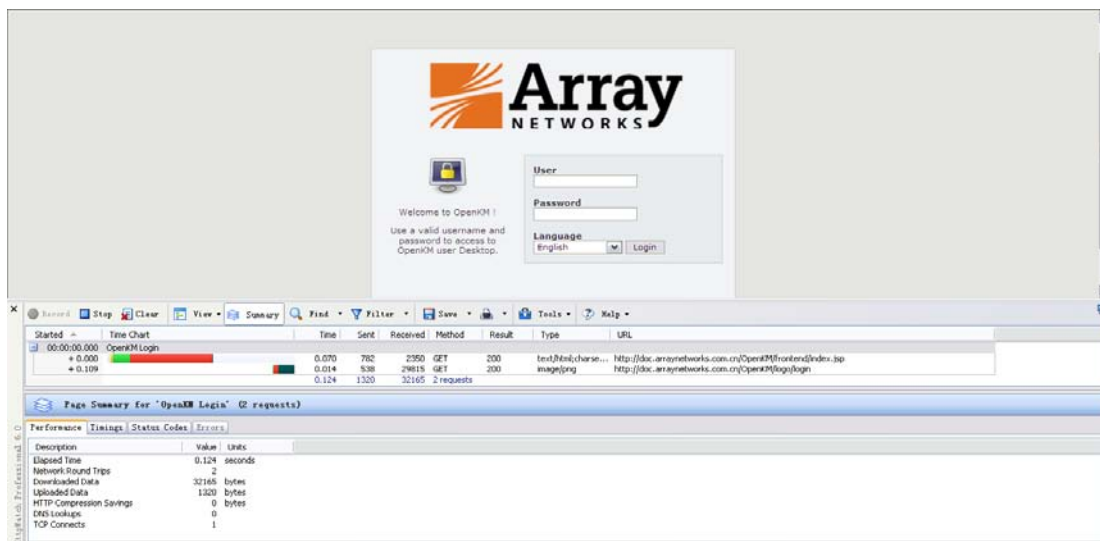


Figure I-1 Enable HttpWatch Professional

After login, user credentials are recorded on the **Headers** and **Post Data** tabs, as shown in Figure I-2 and Figure I-3.

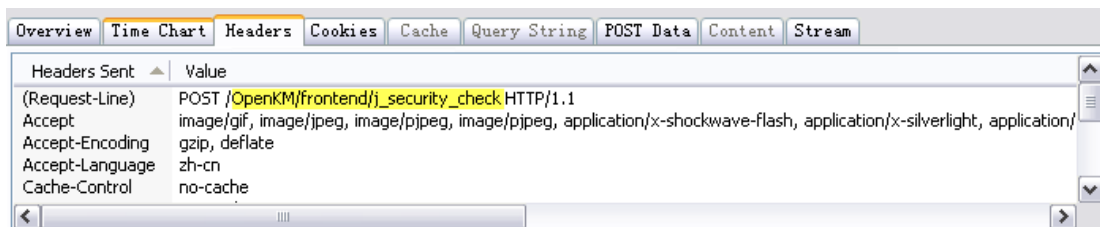


Figure I-2 Get Post URL Parameter

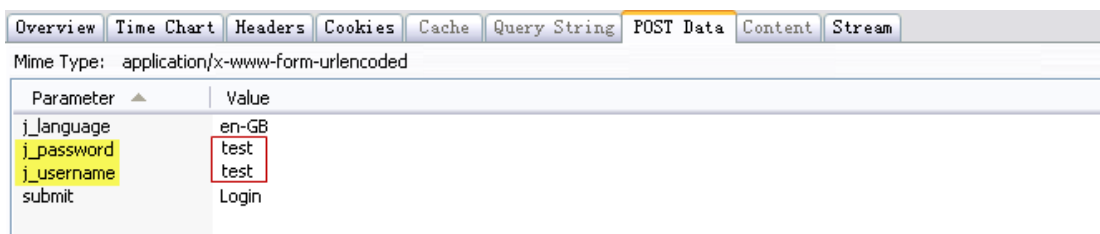


Figure I-3 Get Username and Password Parameters

Specify the SSO parameters in the **SSO Items** area, as shown in Figure I-4.

The parameter **Post URL** is the regular website URL followed by the highlighted part in Figure I-2. The parameters **Username Field** and **Password Field** are the corresponding parameters indicating the user credentials in Figure I-3.

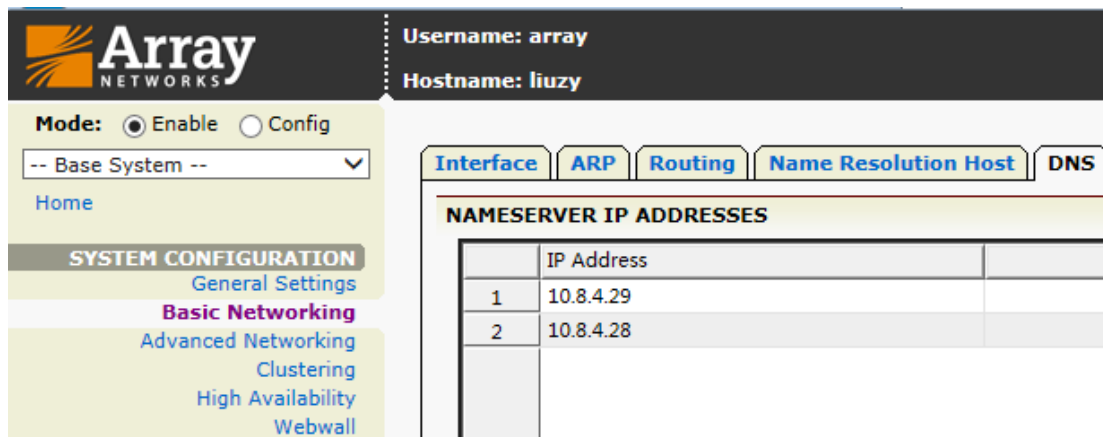
GENERAL SETTINGS	
URL:	<input type="text" value="http://doc.arraynetworks.com.cn/Op"/>
Description:	<input type="text" value="OpenKM"/>
Folder:	<input type="text" value="Web"/>
SSO ITEMS	
Post URL:	<input type="text" value="/OpenKM/frontend/j_security_check"/>
Username Field:	<input type="text" value="j_username"/>
Password Field:	<input type="text" value="j_password"/>
Login URL:	<input type="text"/> (Optional)
Post Fields:	<input type="text"/> (Optional)
Custom Cookies:	<input type="text"/> (Optional, For Example: aaa=ddd;bbb=eee)

Figure I-4 Set SSO Parameters

Appendix II FAQs

➤ **Why the Secure Browser cannot access websites?**

The DNS server is not correctly configured on AG. The Secure Browser and all other built-in applications always depend on the DNS servers defined on AG.



➤ **What is the difference between Installed Application List and Managed Application List?**

The applications in the Installed Application List are installed in the device system, and cannot be removed by using MDM commands.

The applications in the Managed Application List are installed through MDM command “Install Application” from the AG WebUI, and can be removed by using MDM commands.

➤ **Why the profile for MDM fails to be installed on iOS?**

The URL for downloading the profile is wrong.

Resolution: It is recommended to set a Domain Name to the FQDN field instead of an IP address. If you do not have a Domain Name and the FQDN is set as an IP address, please make sure that the client uses the same IP address to log in; otherwise, the profile cannot be successfully downloaded.

➤ **How to generate the MDM certificate?**

Case A: The customer does not want to be the MDM vendor.

1. Create a CSR using any toolkit, i.e. openssl:


```
openssl genrsa -des3 -out key.pem 2048
```

```
openssl req -new -key key.pem -out customer.csr
```
2. Convert “customer.csr” to “der” format:


```
openssl req -inform pem -outform der -in customer.csr -out customer.der
```
3. Remove the passphrase from key.pem using this command:

```
openssl rsa -in key.pem -out PlainKey.pem
```

4. Send the “customer.der” to the MDM vendor (i.e. ArrayNetworks).
5. Once the vendor delivers the signed CSR back, log into:

[<https://identity.apple.com/pushcert/>] (<https://identity.apple.com/pushcert/>) using a verified Apple ID, and upload the CSR to the Apple Push Certificates Portal. After that, download the certificate (for example: CustomerCompanyName.pem).

6. Merge the certificate and key:

```
cat CustomerCompanyName.pem PlainKey.pem > MDM.pem
```

7. Upload the MDM.pem to AG.

Case B: The customer wants to be the MDM vendor.

1. The customer should have a valid Enterprise developer account.
2. Download an “MDM Signing Certificate” and associated trust certificates via the [iOS Provisioning Portal] (<https://developer.apple.com/account/ios/certificate/certificateList.action>).
3. Create a CSR (follow steps 1-3 of Case A).
4. Download a tool “mdm_vendor_sign.py” from: [github](<https://github.com/grinich/mdmvendorsign>), and use it to sign the csr.
5. Follow steps 5-7 of Case A.

Case C: The customer does not want to create the certificate by themselves.

Send their company information (common name, country and so on) to Array Customer Support. We will deliver a certificate signed by our MDM Signing Certificate.



Note: The created certificate has an expiration date. If it is expired, MDM will not work until a new certificate is uploaded.