Administrators Guide

Dell® Management Console for Dell Enterprise Mobility Management and Dell Wyse Cloud Client Management

Issue: 072914
PN: 883934-01 Rev. K

Copyright Notices

End User License Agreement ("License")

Trademarks

Restricted Rights Legend

You acknowledge that the Software is of U.S. origin. You agree to comply with all applicable international and national laws that apply to the Software, including the U.S. Export Administration Regulations, as well as end-user, end-use and country destination restrictions issued by U.S. and other governments. For additional information on exporting the Software, see http://www.microsoft.com/exporting.

Ordering Information

For availability, pricing, and ordering information in the United States and Canada, call 1-800-438-9973 or visit us at **Dell.com**. In all other countries, contact your sales representative.

Contents

1 Introduction

The Dell Management Console provides IT administrators with a tool to help securely manage and enable corporate access to a wide range of solutions and devices including thin clients, zero clients, cloud devices, workspace applications, smartphones, and tablets. It provides visibility not only into managed devices, but also insight into which employees have used them, and what IT assets have been accessed. The management console is available from any location through standard Web browsers over the Internet.

This guide provides instructions for the management console included with the Dell Enterprise Mobility Management and Dell Wyse Cloud Client Management solutions. For product and solution details (including technical specifications and support), visit the following links:

- Dell Enterprise Mobility Management Solution: http://www.dellmobilitymanager.com
- Dell Wyse Cloud Client Management Solution: http://www.cloudclientmanager.com

See the following sections below for device requirement details:

- "Thin Client Requirements"
- "Dell Wyse Cloud Connect Requirements"
- "Mobile Workspace Requirements"
- "iOS Requirements"
- "Android Requirements"

Thin Client Requirements

IMPORTANT: Use of the latest INI parameters, found in the latest client documentation, requires the “recommended” firmware builds below.

Thin Client Device Requirements:

- 5212 (Dell Wyse Thin Client All-in-One, Series 5000 Hardware Platform) running firmware ThinOS 8.0_307 or later (new platform added) - **NOTE**: To update 5212 devices, configure to use firmware for D10D/Z10D (ZD10_wnos) on the Firmware Upgrade page in the group policy settings (see "Details: Thin Client Policy Settings")
- C00X (Xenith) running firmware 2.0_021 or later (recommended 2.0_305 or later)
- R00LX (Xenith Pro) running firmware 2.0_021 or later (recommended 2.0_305 or later)
- 3000-T00X (Xenith 2) running firmware 2.0_021 or later (recommended 2.0_305 or later)
- 3002-T00DX (Xenith 3) running firmware 2.0_305 or later (new platform added)
- 5000-D00DX (Xenith Pro 2) running firmware 2.0_104 or later (recommended 2.0_305 or later)
- C10LE running firmware ThinOS 8.0_037 or later (recommended 8.0_210 or later)
- R10L running firmware ThinOS 8.0_037 or later (recommended 8.0_210 or later)
- T10 running firmware ThinOS 8.0_037 or later (recommended 8.0_210 or later)
- T10D running firmware ThinOS 8.0_210 or later (recommended 8.0_306 or later)
- D10D running firmware ThinOS 8.0_037 or later (recommended 8.0_307 or later)
- D10DP running firmware ThinOS 8.0_117 or later (recommended 8.0_307 or later)
- Z10D running firmware ThinOS 8.0_037 or later (recommended 8.0_307 or later)

For supported thin clients running earlier versions, a firmware update is required to enable management console connectivity. Updates can be downloaded from the Self-Service Center (see http://www.dell.com/wyse/support).

IMPORTANT: You must use your ThinOS Maintenance (you should have received an email from Dell or your reseller with full instructions) to obtain any available firmware update (if you did not receive this email, contact your reseller). If you are unfamiliar with updating firmware on your ThinOS cloud client, refer to Knowledge Base Solution #**10566** (go to http://www.dell.com/wyse/knowledgebase and search for **10566**).

Connectivity Requirements:

- TCP port 443 (outbound) to https://us1.cloudclientmanager.com
- TCP port 1883 (outbound) to us1-pns.cloudclientmanager.com

Dell Wyse Cloud Connect Requirements

IMPORTANT: Dell Wyse Cloud Connect devices require a valid management console user account configured as part of the device activation process.

Cloud Device Requirements:

- Devices running Android Version 4.1 and later

Connectivity Requirements:

- TCP port 443 (outbound) to https://us1.cloudclientmanager.com
- TCP port 1883 (outbound) to us1-pns.cloudclientmanager.com

Mobile Workspace Requirements

Mobile Device Requirements:

- Most popular Android devices running Android Version 4.0 and later
- iPhone, iPad, and iPod Touch running iOS Version 7.0 and later

Other Support:

- Exchange Server 2010 and later

iOS Requirements

Mobile Device Requirements:

- iPhone, iPad, and iPod Touch running iOS Version 5.x and later

Connectivity Requirements:

- TCP port 443 (outbound) to https://us1.cloudclientmanager.com
- TCP port 80 (outbound) to https://us1.cloudclientmanager.com
- TCP port 8443 (outbound) to us1-mdm.cloudclientmanager.com
- TCP port 5223 (outbound) - for Apple APNS

MDM Requirements:

- A Mobile Device Management (MDM) Apple Push Notification Service (APNs) certificate is required for iOS device management - this process requires an Apple ID. As the Apple ID account will be linked to the APNs certificate, which must be renewed annually, a corporate Apple ID account should be used and not a personal one

Android Requirements

Mobile Device Requirements:

- Devices running Android Version 2.3 and later

Connectivity Requirements:

- TCP port 443 (outbound) to https://us1.cloudclientmanager.com
- TCP port 1883 (outbound) to us1-pns.cloudclientmanager.com

About this Guide

This guide is intended for administrators. It provides instructions for the management console included with the Dell Enterprise Mobility Management and Dell Wyse Cloud Client Management solutions.

Finding the Information You Need in this Guide

You can use either the Search window or Find toolbar to locate a word, series of words, or partial word in an active PDF document. For detailed information on using these features, refer to the Help in your PDF reader.

Technical Support

To access Dell Wyse Cloud Client Management technical resources (self-service portal, knowledge base, software downloads, registration, warranty extensions/RMAs, reference manuals, and so on), visit http://www.dell.com/wyse/support.
If you still need help, you can call Customer Support at 1.800.800.9973 (toll free in U.S. and Canada). Hours of operation are from 6:00 A.M. to 5:00 P.M. Pacific Time, Monday through Friday.

To access Dell Enterprise Mobility Management technical resources (create a Service Request), visit https://support.software.dell.com/create-service-request.
NOTE: You will need to register with Dell Support to place a service request. New to Dell Software Support? Check out the "Getting Started" section of Dell Software Support at https://support.software.dell.com/essentials/getting-started.
If you still need help, you can call Technical Support at 1.800.306.9329 (toll free in U.S. and Canada) or 949.754.8000 or 949.754.8080. Hours of operation are from 5:00 A.M. to 5:00 P.M. Pacific Standard Time, Monday through Friday.

2 Brief Overview of the Management Console

This section provides a brief overview of the functional areas within the management console. It provides important information on the general features to help you quickly get started as an administrator.

Topics include:

- "Functional Areas of the Management Console"
- "Logging In"
- "Understanding the Dashboard Page"
- "Changing Your Password"
- "Logging Out"

Functional Areas of the Management Console

In addition to the Dashboard page, the management console is divided into several functional areas:

- **Dashboard** - Allows you to quickly view important summary information for each functional area of the system.
- **Groups** - Allows you to view and manage Policy Groups.
- **Users** - Allows you to view and manage Users and group membership of Users.
- **Devices** - Allows you to view and manage Devices, Device Types, and Configuration Groups.
- **Apps & Data** - Allows you to view and manage device Application Inventory and Policies, and File Repository Inventory (thin client firmware and certificate files).
- **Events** - Allows you to view and audit system events and alerts.
- **Portal Admin** - Allows administrators to perform system administration tasks (manage Administrators, APNs, Active Directory Connector operations, Subscriptions, and other Self-Service settings/agreements) out of the system (see the Roles tab in "Quick Setup: Get Your Devices Under Management" and "Managing Administrators and Viewers of the Management Console").

Each functional area has a set of automated tools that helps you to perform your administrator duties and daily activities in that functional area. The management console tracks the status of each of the functional areas necessary to successfully maintain your environment.

TIP: The management console supports Microsoft Internet Explorer (IE) 8 or later, Google Chrome 20 or later, and Firefox 10 or later.

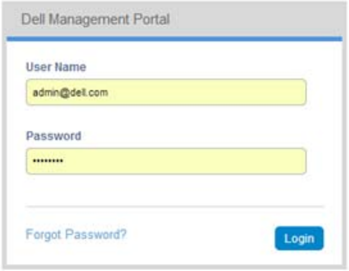
Logging In

IMPORTANT: To log in to the management console, be sure to use your correct User Name and Password (defaults are provided to you by your Account Representative). **CAUTION**: It is highly recommended that you change your password after logging in the first time (see "Changing Your Password").

TIP: Use the Forgot Password link to reset a forgotten password.

To log in to the management console:

1. Open the management console Login page by using a supported Web browser from any machine with access to the Internet and go to: https://us1.cloudclientmanager.com.



Dell Management Portal

User Name

admin@dell.com

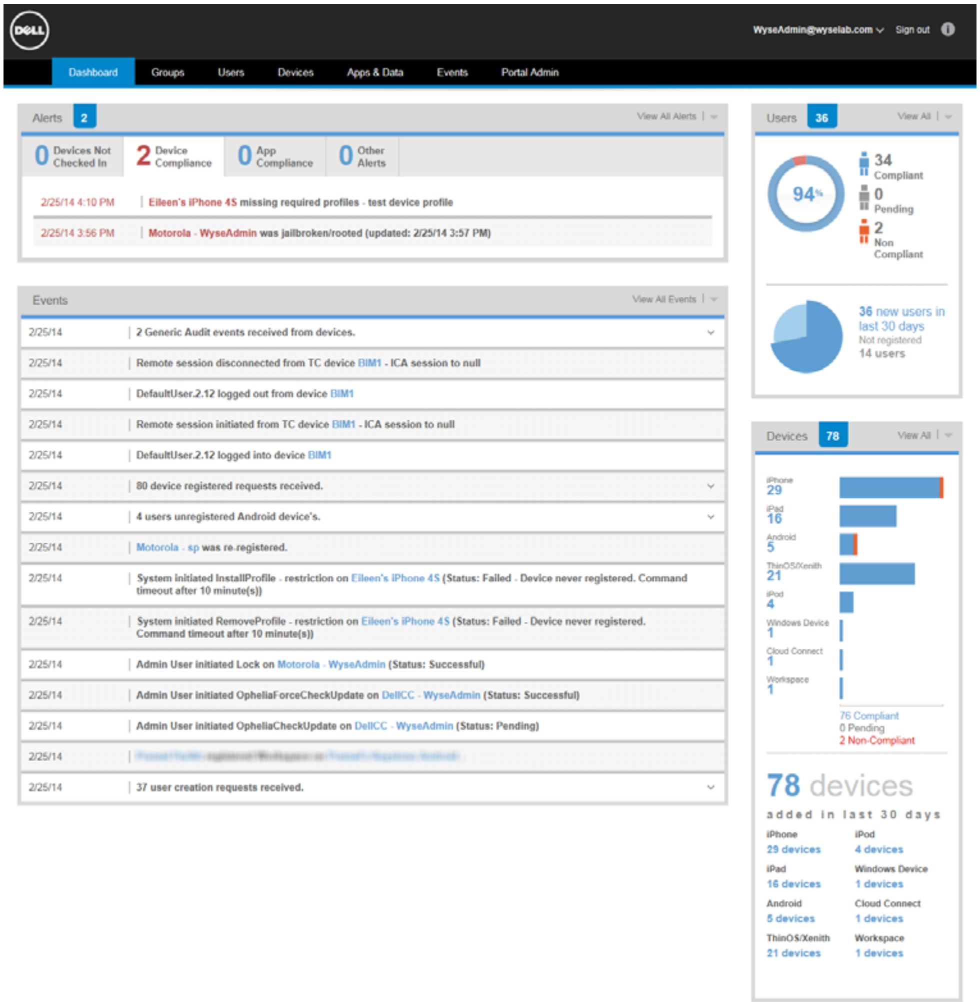
Password

••••••••

2. Enter your User Name and Password.
3. Click **Login** to open the Dashboard page.

Understanding the Dashboard Page

The Dashboard page allows you to quickly view important status information about the system and recent events that have been performed within the system. By clicking a link in the Alerts area, you can view details about that item.



Alerts 2

0 Devices Not Checked In | 2 Device Compliance | 0 App Compliance | 0 Other Alerts

2/25/14 4:10 PM	Eileen's iPhone 4S missing required profiles - test device profile
2/25/14 3:56 PM	Motorola - WyseAdmin was jailbroken/rooted (updated: 2/25/14 3:57 PM)

Events

2/25/14	2 Generic Audit events received from devices.
2/25/14	Remote session disconnected from TC device BIM1 - ICA session to null
2/25/14	DefaultUser.2.12 logged out from device BIM1
2/25/14	Remote session initiated from TC device BIM1 - ICA session to null
2/25/14	DefaultUser.2.12 logged into device BIM1
2/25/14	80 device registered requests received.
2/25/14	4 users unregistered Android device's.
2/25/14	Motorola - sp was re-registered.
2/25/14	System initiated InstallProfile - restriction on Eileen's iPhone 4S (Status: Failed - Device never registered. Command timeout after 10 minute(s))
2/25/14	System initiated RemoveProfile - restriction on Eileen's iPhone 4S (Status: Failed - Device never registered. Command timeout after 10 minute(s))
2/25/14	Admin User initiated Lock on Motorola - WyseAdmin (Status: Successful)
2/25/14	Admin User initiated OpheliaForceCheckUpdate on DellCC - WyseAdmin (Status: Successful)
2/25/14	Admin User initiated OpheliaCheckUpdate on DellCC - WyseAdmin (Status: Pending)
2/25/14	[redacted]
2/25/14	37 user creation requests received.

Users 36

94%

34 Compliant
0 Pending
2 Non Compliant

36 new users in last 30 days
Not registered
14 users

Devices 78

iPhone	29
iPad	16
Android	5
ThinOS/Xenith	21
iPod	4
Windows Device	1
Cloud Connect	1
Workspace	1

76 Compliant
0 Pending
2 Non-Compliant

78 devices

added in last 30 days

iPhone 29 devices	iPod 4 devices
iPad 16 devices	Windows Device 1 devices
Android 5 devices	Cloud Connect 1 devices
ThinOS/Xenith 21 devices	Workspace 1 devices

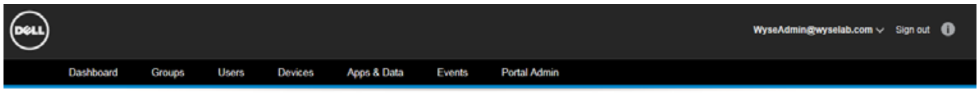
Links on the Dashboard page include:

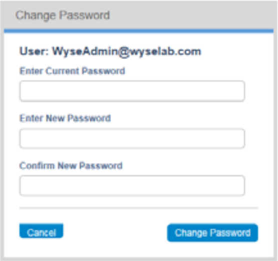
- **Account Link** - (Name of your account) Allows you to change your password (see "Changing Your Password"). This link is always available in the upper-right corner of the management console.
- **Sign out** - Allows you to log out of the system. This link is also located on the main page of each functional area.
- **Alerts** - Allows you to quickly go to functional areas of the system that require your attention.
- **Functional Areas** - Located across the top, these links provide you with quick access to the main functional areas. Functional area links are also located across the top of the main page of each functional area.
- **Quick-Links** - (Highlighted in blue throughout the system pages) Allows you to quickly go to the content of that link to view and manage those details (for example, a user name link will bring you to the User Details page; a device name link will bring you to the Device Details page; and so on).

Changing Your Password

To change your log-in password to the management console:

1. Click your **Account Link** at the top right of the management console (for example, DellAdmin@Delllab.com), and then click **Change Password** in the menu to open the Change Password page.




Change Password

User: WyseAdmin@wyselab.com

2. Enter your Current Password.
3. Enter a New Password.
4. Enter your new password in the Confirm New Password box.
5. Click **Change Password**.

Logging Out

To log out of the management console, click the **Sign out** link. This link is always available in the upper-right corner of the management console.

3 Quick Setup: Get Your Devices Under Management

This section provides an overview of the essential steps required to get your devices under management quickly.

Steps include:

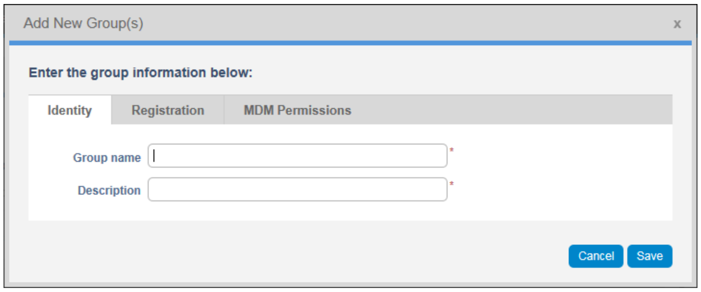
- "Step 1: Create a Group"
- "Step 2: Set Up Thin Client Device Management"
- "Step 3: Set Up iOS and Android Device Management"

TIP: After you complete these steps, you will have your devices under basic management. While this guide helps you with all functional areas of the system, you can continue to configure your system for a more granular level of management by referring to the following sections:

- "Managing Administrators and Viewers of the Management Console"
- "Managing Groups and Group Policies"
- "Managing Users"
- "Managing Devices"
- "Managing Application Inventory and Application Policies"

Step 1: Create a Group

1. **Use the Add New Group page to Create a Group**:
   Log in to the management console, click the **Groups** tab to open the Groups page to see a list of all groups in the system (by default there is always a Default Policy Group), and then click the **Create Group** button to open and use the Add New Group page.
   On the Identity tab, enter the group information—Group Name and Description.
   IMPORTANT: You cannot locally change the name and description of a group that has been imported from Active Directory as part of a Manual AD Sync import option (see "Active Directory Connector: Importing Existing Active Directory Users into the System").
   On the Registration tab, configure the preferences for how devices and users can register to this group.



Add New Group(s) x

Enter the group information below:

Identity | Registration | MDM Permissions

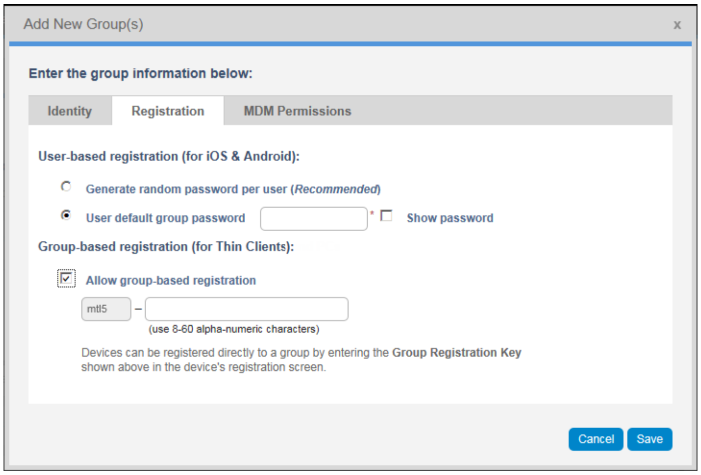
Group name *

Description *

Cancel Save

Step 2: Set Up Thin Client Device Management

1. **Enable Group-Based Registration**:
   On the Registration tab, select the **Allow group-based registration** option (to configure a common registration key for all thin clients in this Group—it registers thin clients directly to this Group), enter an 8 to 64 alpha-numeric character key into the Group Registration Key box (this is the key for User registration of their thin client—the first four digits are hard-coded by the system and uniquely identifies your tenant), and then click **Save**.
   TIP: Thin clients can only register to Groups directly and must have a Group Registration Key enabled to do so (the key is the unique identifier for this cloud-based policy group).



Add New Group(s) x

Enter the group information below:

Identity | Registration | MDM Permissions

User-based registration (for iOS & Android):

○ Generate random password per user (*Recommended*)

● User default group password * □ Show password

Group-based registration (for Thin Clients):

☑ Allow group-based registration

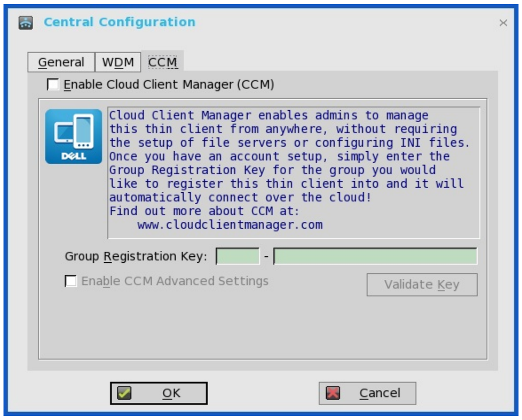
mtl5 –

(use 8-60 alpha-numeric characters)

Devices can be registered directly to a group by entering the **Group Registration Key** shown above in the device's registration screen.

Cancel Save

2. **Register Thin Client Devices with the Management Service**:
   On your supported thin client (see "Thin Client Requirements"), open the **Central Configuration** dialog box (for example, **System Settings icon on the Zero Toolbar > Central Configuration**-see your client documentation for details on your client/ software build). Ensure the **Enable Cloud Client Manager (CCM)** check box is selected, enter the **Group Registration Key** as configured (see previous step) for the desired group, click **OK**, and then follow the on-screen instructions. When prompted, log in with corporate credentials in order to complete the registration process.
   TIP: You can use the Validate Key button to verify your entry is correct. If you see a success message, click **OK** to reboot the device and finish the registration process. If you see a failure message, double check the Group Registration Key you entered and verify you have network connectivity defined in the prerequisites section (see "Thin Client Requirements").



Central Configuration

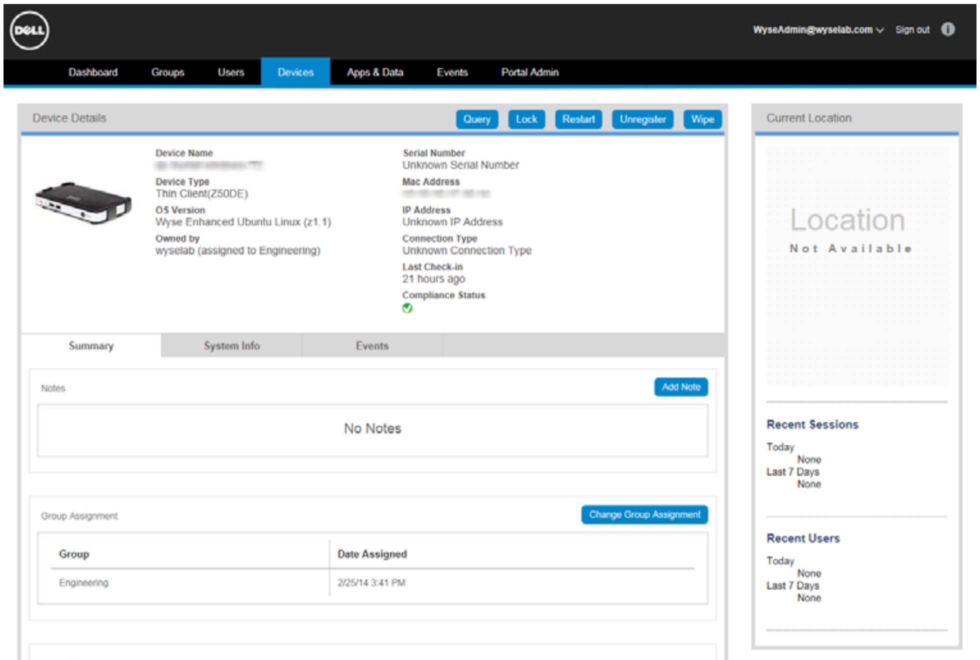
□ Enable Cloud Client Manager (CCM)

```
Cloud Client Manager enables admins to manage
this thin client from anywhere, without requiring
the setup of file servers or configuring INI files.
Once you have an account setup, simply enter the
Group Registration Key for the group you would
like to register this thin client into and it will
automatically connect over the cloud!
Find out more about CCM at:
    www.cloudclientmanager.com
```

Group Registration Key: [   ] - [   ]

□ Enable CCM Advanced Settings

3. **Verify Connectivity is OK for Real-Time Commands**:
   On the Devices page of the management console, click the **Name** link to open the Device Details page for your thin client (see previous step), click the **Restart** button to reboot the thin client.
   NOTE: Thin client basic connectivity is complete. At this point you have successfully registered and configured your thin client. You can now send real-time commands to the thin clients. You can continue by configuring policies and configurations either at the Group level (see "Managing Groups and Group Policies") or by creating a device specific exception (see "Managing Devices").



Device Details

Device Name
[redacted]

Device Type
Thin Client(Z50DE)

OS Version
Wyse Enhanced Ubuntu Linux (z1.1)

Owned by
wyselab (assigned to Engineering)

Serial Number
Unknown Serial Number

Mac Address
[redacted]

IP Address
Unknown IP Address

Connection Type
Unknown Connection Type

Last Check-in
21 hours ago

Compliance Status
✓

Notes

No Notes

Group Assignment

Group	Date Assigned
Engineering	2/25/14 3:41 PM

Current Location

Location
Not Available

Recent Sessions
Today
None
Last 7 Days
None

Recent Users
Today
None
Last 7 Days
None

Step 3: Set Up iOS and Android Device Management

1. **Add Users**:
   On the Users page of the management console, click the **Add Mobile User** button to open the New Mobile User page, and then use the tabs to configure the settings (be sure to click **Save** when you are finished configuring a User):

   Personal Information tab:

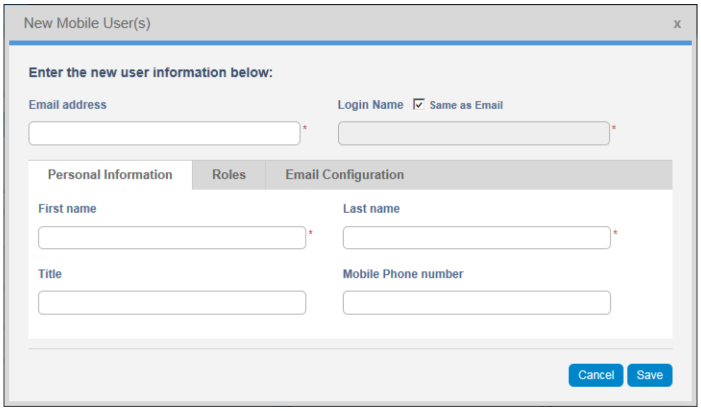
   - **Email Address**: Must be a valid email address (used for password recovery).
   - **Login Name**: The Login Name is the username used for device registration and for logging into the Self-Service portal (see "Other Settings: APNS Warnings, License Expiration Warnings, and Self Service Legal Agreements (Enforcing the Agreement for All Self Service Users)") and can be the same as the email address or customized. **CAUTION**: Once created, this Login Name cannot be modified (you must deactivate and delete the User, and then create a new User with same email address but different Login Name if desired).
   - **First Name / Last Name / Title / Mobile Phone Number**

   Roles tab:

   - **Enable Mobile User Role**: Select if you want to enable device registration and Self-Service portal access for this mobile-device User; and then select the policy group to which you want to assign the User (the mobile user role requires a policy group).
   - **Portal Administrator**: Select this option if you want to enable administration access to the system for this User (administrator access rights), and then select the role (Global Administrator or Global Viewer) to which you want to assign the User. In general, **Global Viewers** have read-only access to the management console, but can also be given rights to issue any of the following Real-Time commands that you specify: Query, Lock, Clear Passcode, Unregister, Wipe, Restart (see "Managing Administrators and Viewers of the Management Console"). Note that newly created administrators will be forced to enter a new password at their first login.
   - **Password**: The password is used for device registration and is the password for logging into the Self-Service portal. Select a User-based option to either generate a random password or to enter a custom password:
     Random password: System assigns a random password for the User.
     Custom password: Manually enter the password you want (passwords must contain a minimum of 8 characters (up to a maximum of 64) including 1 upper case letter, 1 lower case letter, and 1 numerical digit). If a group password has been configured, this is the default custom password.
     TIP: Users will register their client device using the credentials you provide to them (they must enter the credentials into the management software installed on their device and register into the management system).
     CAUTION: It is highly recommended that this password be changed at first login. (see "Changing Your Password"). Newly created administrators, and any Mobile User trying to activate the Self-Service portal for first time, will be forced to enter a new password at their first login.

Email Configuration tab:

- **Exchange/IMAP/POP**: Configure the email information you require. The Email Configuration tab is used to link user-specific account information for Exchange ActiveSync and Email policies for iOS devices. Whenever the Dynamic User Info option is selected on either an Exchange ActiveSync or Email policy, the user-specific information configured in this tab will be sent to the device to simplify configuration on the iOS device - the user will simply be prompted to enter their password to complete the configuration of their email account. **ADMINISTRATOR NOTE**: Email information is required for those administrators who also have a Mobile User role assigned (otherwise it is not really applicable to users who exclusively have a Global Administrator or Global Viewer role).



New Mobile User(s)

Enter the new user information below:

Email address: *

Login Name ☑ Same as Email: *

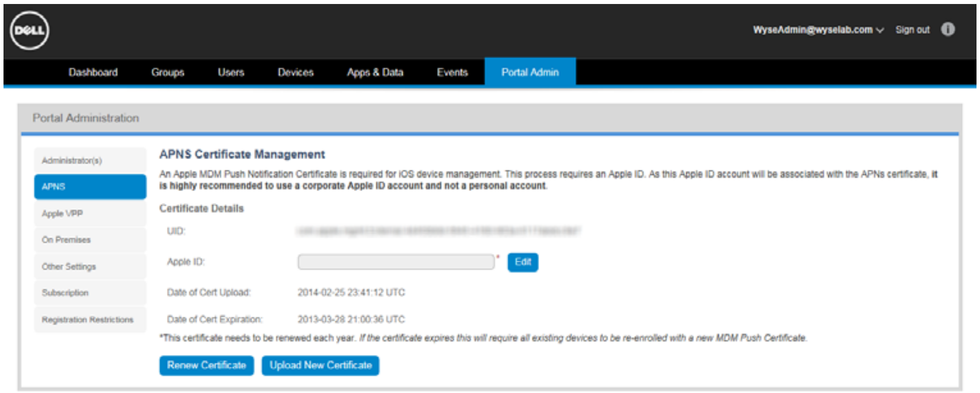
First name: *

Last name: *

Title:

Mobile Phone number:

2. **(iOS ONLY) Generate APNs Certificate**:
   The APNs Certificate Management page of the management console (**Portal Admin > APNs**) allows you to generate an Apple MDM Push Notification Certificate that is required for iOS device management. Simply follow the instruction on the APNs Certificate Management page. For details, see "Generating an APNs Certificate (iOS Only)."



APNS Certificate Management

An Apple MDM Push Notification Certificate is required for iOS device management. This process requires an Apple ID. As this Apple ID account will be associated with the APNs certificate, **it is highly recommended to use a corporate Apple ID account and not a personal account.**

Certificate Details

UID: [redacted]

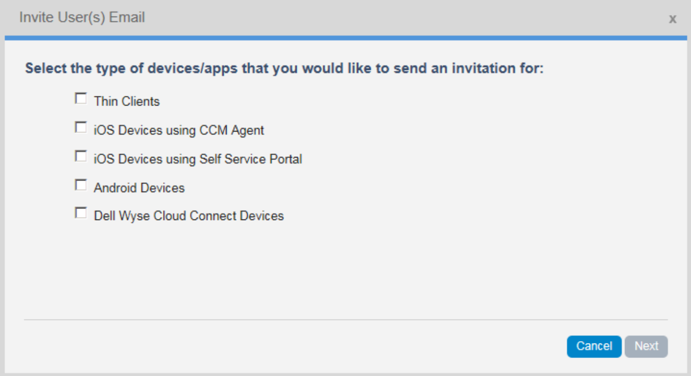
Apple ID: *

Date of Cert Upload: 2014-02-25 23:41:12 UTC

Date of Cert Expiration: 2013-03-28 21:00:36 UTC

*This certificate needs to be renewed each year. *If the certificate expires this will require all existing devices to be re-enrolled with a new MDM Push Certificate.*

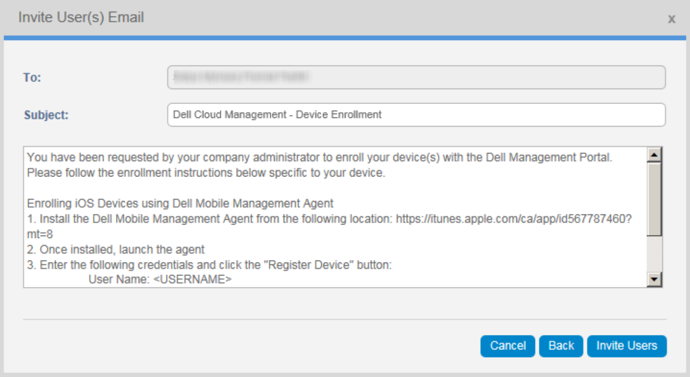
3. **(iOS Example) Register iOS Devices with Single Sign-On Credentials**:
Once Users have been added to the system, they can register their iOS device. Email invitations can be sent to users providing the instructions to register their device. On the Users page of the management console, select the check box next to the name of the User you want, and then click **Invite Users** to open and use the Invite Users Email wizard to send Users information about how to register their devices



Select the type of devices/apps that you would like to send an invitation for:

□ Thin Clients
□ iOS Devices using CCM Agent
□ iOS Devices using Self Service Portal
□ Android Devices
□ Dell Wyse Cloud Connect Devices

A set of different template email messages are pre-configured according to your needs. For details, see "Inviting Users to Register Devices."



To: [redacted]

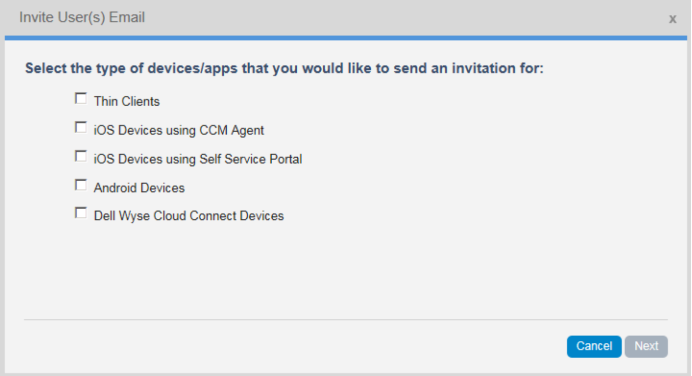
Subject: Dell Cloud Management - Device Enrollment

You have been requested by your company administrator to enroll your device(s) with the Dell Management Portal.
Please follow the enrollment instructions below specific to your device.

Enrolling iOS Devices using Dell Mobile Management Agent
1. Install the Dell Mobile Management Agent from the following location: https://itunes.apple.com/ca/app/id567787460?mt=8
2. Once installed, launch the agent
3. Enter the following credentials and click the "Register Device" button:
User Name: <USERNAME>

IMPORTANT: If corporate email is not configured on the user’s device, they can follow the steps described in the email to enroll the device. The email includes the URL address the user will need to navigate to using Safari on the iOS device, their login credentials, and the instructions to click the **Register iOS Device** button to initiate the registration process from the device. **TIP**: Users can also use the Dell Mobile Management Agent for iOS downloadable from the Apple App Store to register the device.

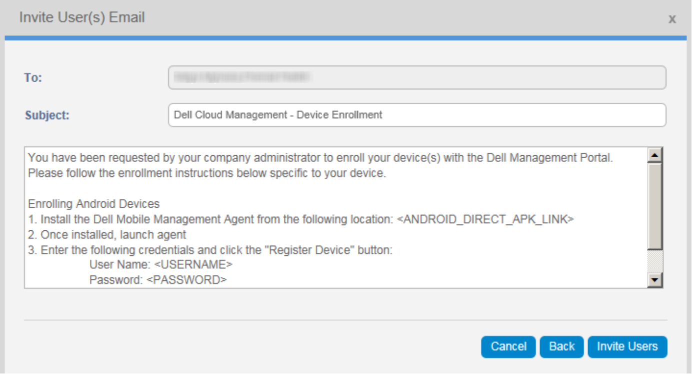
4. **(Android Example) Register Android Devices with the Management Service**: Once Users have been added to the system, they can register their Android device. Email invitations can be sent to users providing the instructions to register their device. On the Users page of the management console, select the check box next to the name of the User you want, and then click **Invite Users** to open and use the Invite Users Email wizard to send Users information about how to register their devices.



Select the type of devices/apps that you would like to send an invitation for:

☐ Thin Clients
☐ iOS Devices using CCM Agent
☐ iOS Devices using Self Service Portal
☐ Android Devices
☐ Dell Wyse Cloud Connect Devices

A set of different template email messages are pre-configured according to your needs. For details, see "Inviting Users to Register Devices."



To: [redacted]

Subject: Dell Cloud Management - Device Enrollment

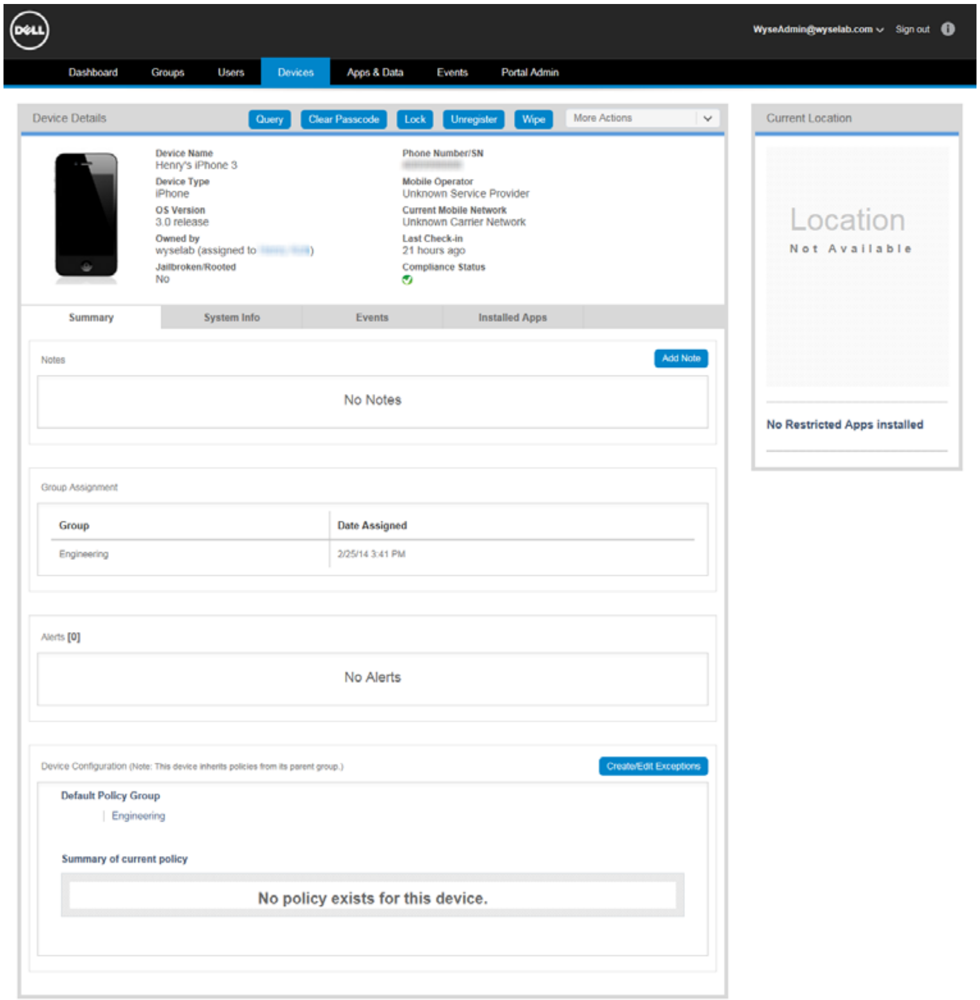
You have been requested by your company administrator to enroll your device(s) with the Dell Management Portal.
Please follow the enrollment instructions below specific to your device.

Enrolling Android Devices
1. Install the Dell Mobile Management Agent from the following location: <ANDROID_DIRECT_APK_LINK>
2. Once installed, launch agent
3. Enter the following credentials and click the "Register Device" button:
User Name: <USERNAME>
Password: <PASSWORD>

IMPORTANT: If corporate email is not configured on the user's device, they can follow the steps described in the email to enroll the device. The email includes the link to download the Dell Mobile Management Agent for Android (from Google Play) and the required login credentials to initiate the registration process from the device.

5. **Verify Connectivity is OK for Real-Time Commands**:
   On the Devices page of the management console, click the **Name** link to open the Device Details page for your mobile device (see previous example step for either iOS or Android), click the **Lock** button to lock the device screen (requires a device passcode to unlock it when a passcode is configured).
   NOTE: Mobile device basic connectivity is complete. At this point you have successfully registered and configured your mobile device. You can now send real-time commands to the mobile devices. You can continue by configuring policies and configurations either at the Group level (see "Managing Groups and Group Policies") or by creating a device specific exception (see "Managing Devices").

iOS - Phone example



Device Name
Henry's iPhone 3

Device Type
iPhone

OS Version
3.0 release

Owned by
wyselab (assigned to [redacted])

Jailbroken/Rooted
No

Phone Number/SN
[redacted]

Mobile Operator
Unknown Service Provider

Current Mobile Network
Unknown Carrier Network

Last Check-in
21 hours ago

Compliance Status
✓

Location
Not Available

No Restricted Apps installed

Notes

No Notes

Group Assignment

Group	Date Assigned
Engineering	2/25/14 3:41 PM

Alerts [0]

No Alerts

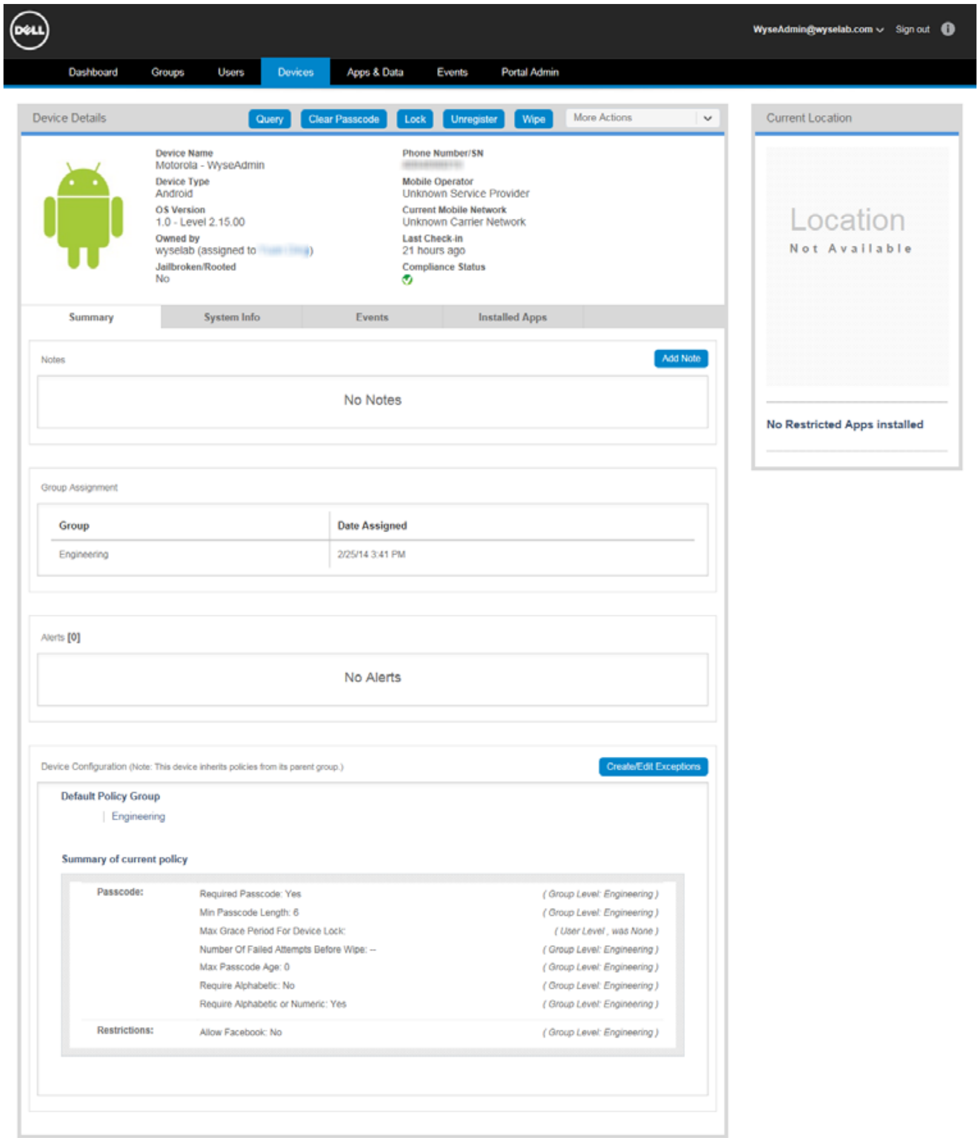
Device Configuration (Note: This device inherits policies from its parent group.)

Default Policy Group
| Engineering

Summary of current policy

No policy exists for this device.

Android - Phone example



Device Details

Device Name Motorola - WyseAdmin	**Phone Number/SN** [redacted]
Device Type Android	**Mobile Operator** Unknown Service Provider
OS Version 1.0 - Level 2.15.00	**Current Mobile Network** Unknown Carrier Network
Owned by wyselab (assigned to [redacted])	**Last Check-in** 21 hours ago
Jailbroken/Rooted No	**Compliance Status** ✓

Current Location

Location

Not Available

No Restricted Apps installed

Notes

No Notes

Group Assignment

Group	Date Assigned
Engineering	2/25/14 3:41 PM

Alerts **[0]**

No Alerts

Device Configuration (Note: This device inherits policies from its parent group.)

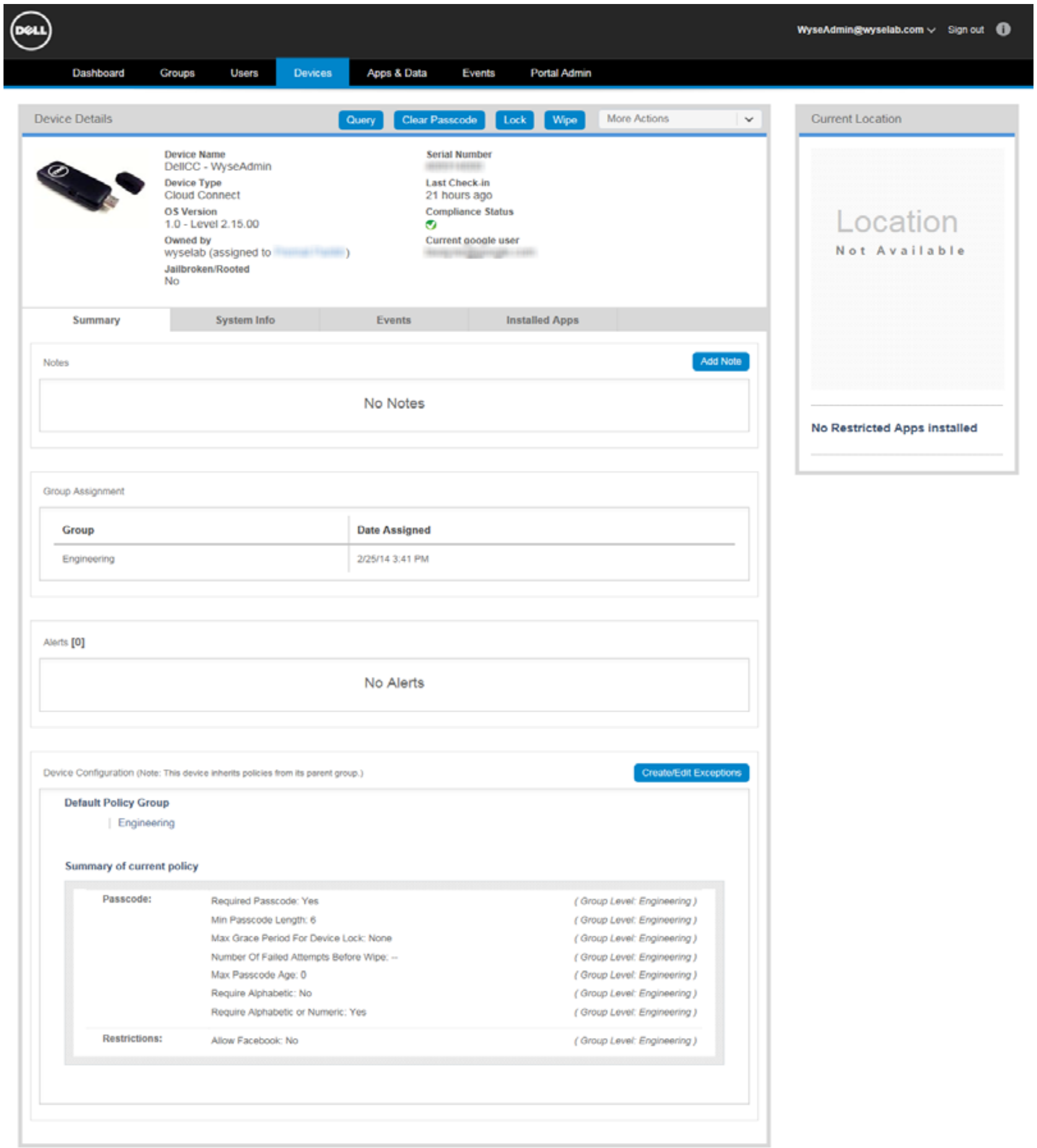
Default Policy Group

| Engineering

Summary of current policy

Passcode:	Required Passcode: Yes	*(Group Level: Engineering)*
	Min Passcode Length: 6	*(Group Level: Engineering)*
	Max Grace Period For Device Lock:	*(User Level , was None)*
	Number Of Failed Attempts Before Wipe: --	*(Group Level: Engineering)*
	Max Passcode Age: 0	*(Group Level: Engineering)*
	Require Alphabetic: No	*(Group Level: Engineering)*
	Require Alphabetic or Numeric: Yes	*(Group Level: Engineering)*
Restrictions:	Allow Facebook: No	*(Group Level: Engineering)*

Dell Wyse Cloud Connect example



Device Details

Device Name
DellCC - WyseAdmin

Device Type
Cloud Connect

OS Version
1.0 - Level 2.15.00

Owned by
wyselab (assigned to [redacted])

Jailbroken/Rooted
No

Serial Number
[redacted]

Last Check-in
21 hours ago

Compliance Status
✓

Current google user
[redacted]

Current Location

Location
Not Available

No Restricted Apps installed

Notes

No Notes

Group Assignment

Group	Date Assigned
Engineering	2/25/14 3:41 PM

Alerts **[0]**

No Alerts

Device Configuration (Note: This device inherits policies from its parent group.)

Default Policy Group
| Engineering

Summary of current policy

Passcode:	Required Passcode: Yes	*(Group Level: Engineering)*
	Min Passcode Length: 6	*(Group Level: Engineering)*
	Max Grace Period For Device Lock: None	*(Group Level: Engineering)*
	Number Of Failed Attempts Before Wipe: --	*(Group Level: Engineering)*
	Max Passcode Age: 0	*(Group Level: Engineering)*
	Require Alphabetic: No	*(Group Level: Engineering)*
	Require Alphabetic or Numeric: Yes	*(Group Level: Engineering)*
Restrictions:	Allow Facebook: No	*(Group Level: Engineering)*

4 Groups

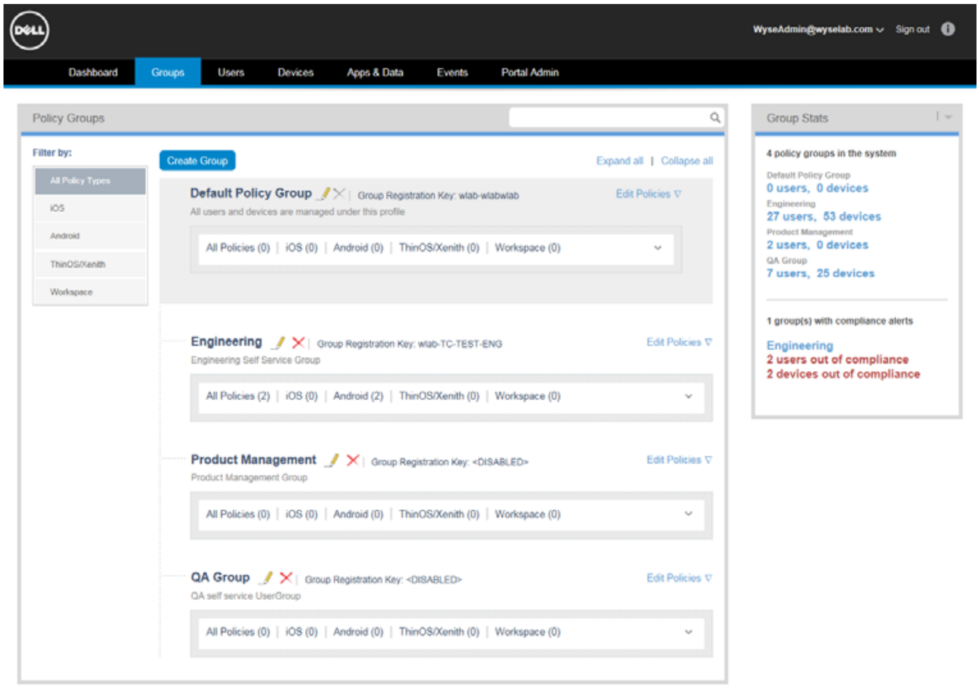
This section describes how to perform routine Policy Group management tasks using the management console. The management console allows administrators the flexibility to employ hierarchical Group Policy management (with the highest Group Policy level being the Global Group Policy). Optionally, sub-groups of the Global Group Policy can be created to segment Users according to corporate standards (for example, job functions, device type, bring-your-own-device, and so on).

Topics include:

- "Managing Groups and Group Policies"
  - "Adding/Editing Groups"
  - "Configuring and Managing Policies (Global, Group-level, and Exception-based Policy Management)"

Managing Groups and Group Policies

The Groups page allows you to quickly view and manage the Policy Groups that are available (see Table 1). It also allows you to easily display the Groups you want by using the filtering feature.



Default Policy Group | Group Registration Key: wlab-wlabwlab
All users and devices are managed under this profile
All Policies (0) | iOS (0) | Android (0) | ThinOS/Xenith (0) | Workspace (0)

Engineering | Group Registration Key: wlab-TC-TEST-ENG
Engineering Self Service Group
All Policies (2) | iOS (0) | Android (2) | ThinOS/Xenith (0) | Workspace (0)

Product Management | Group Registration Key: <DISABLED>
Product Management Group
All Policies (0) | iOS (0) | Android (0) | ThinOS/Xenith (0) | Workspace (0)

QA Group | Group Registration Key: <DISABLED>
QA self service UserGroup
All Policies (0) | iOS (0) | Android (0) | ThinOS/Xenith (0) | Workspace (0)

4 policy groups in the system
Default Policy Group
0 users, 0 devices
Engineering
27 users, 53 devices
Product Management
2 users, 0 devices
QA Group
7 users, 25 devices

1 group(s) with compliance alerts
Engineering
2 users out of compliance
2 devices out of compliance

Note that the Active Directory icon helps you to distinguish between locally created/ managed Groups and those created as part of an Active Directory import (Manual AD Sync option only).

AD

This icon is shown in the Groups page, and anywhere else the Group name is shown (for example, Users page—Group column, Group filters/stats, Event messages, and so on). For Active Directory information, see "Active Directory Connector: Importing Existing Active Directory Users into the System."

Use the following guidelines:

- **Filter By area** - Click the filter button you want to view the Group Policies you want. **IMPORTANT**: Using the filter buttons provides a quick way to view policies for a specific device type across all groups (it filters out any groups without the type of device policy you selected and switches the view to the selected button)
- **Edit Policies links** - Use the Edit Policies link of a Group to edit the Group Policy for that Group (see "Configuring and Managing Policies (Global, Group-level, and Exception-based Policy Management)"). **IMPORTANT**: All policies created in the Default Policy Group are automatically inherited by all Groups, Devices, and Users in the system unless a specific exception is configured for those assets.
- **Details and Show Less links** - Use the Details and Show Less links of a Group to expand or collapse the amount of information you want displayed. **IMPORTANT**: In the expanded Group view, any user added groups (that is, any Group you added other than the Default Policy Group) will only display a summary of the configuration that you have set at that level (that is, anything the Group you added inherits from the Default Policy Group will not be displayed so as not to be redundant).
- **Group Stats area** - Use this area to view a summary of the groups statistics/analytics available and to use the links available to view details of items (click a link in the Group Stats area).

Table 1 provides a quick overview of what you can do using the Groups page.

IMPORTANT: Depending on your Active Directory integration with the management console and your management console Active Directory Connector settings, you will manage your user and group details from the management console or your Active Directory (see "Active Directory Connector: Importing Existing Active Directory Users into the System").

Table 1 Routine Group Tasks - Groups page

Tasks You Can Do	How	Details
Add a Group to the system.	Click the **Create Group** button to open the Add New Group page, and then use the tabs to configure the settings.	"Adding/Editing Groups."
Edit a Group in the system.	Click the **Edit** icon (pencil) next to the name of the Group you want in the Groups page and make your changes.	Use same guidelines in "Adding/ Editing Groups." **IMPORTANT**: You cannot locally change the name and description of a group that has been imported from Active Directory as part of a Manual AD Sync import option (see "Active Directory Connector: Importing Existing Active Directory Users into the System"). You must use Active Directory to change the name and description of a group, and then synch.
Configure/Edit a Group Policy or the Default Policy Group in the system.	Click the **Edit Policies** link of a Group Policy or the Default Policy Group, select the device you want (**iOS**, **Android**, **ThinOS/Xenith**) from the menu, click the Settings button you want, and then click the **Configure this item** button to open and use the settings page to configure your settings (be sure to click **Save and Publish** after configuring your settings).	"Configuring and Managing Policies (Global, Group-level, and Exception-based Policy Management)."
Delete a Group from the system.	Click the delete icon (red **X**) next to the name of the Group you want in the Groups page, and confirm the deletion. The Group is deleted and is no longer shown in the list of available Groups on the Groups page.	**IMPORTANT**: You can only delete Groups that have no Users or Devices registered to it. If assets are registered to the Group, you will be prompted to re-assign those assets to a new Group before you can delete the Group. In addition, if the new Group has different iOS MDM Permissions, these re-assigned Users must re-register any managed iOS devices.

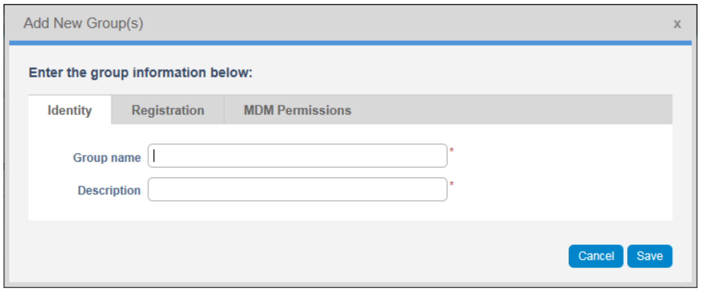
Adding/Editing Groups

As an administrator you can add a Group. Once a Group is added, you can then add members (Users).

To add a Group:
On the Groups page, click the **Create Group** button to open the Add New Group page, and then use the tabs to configure the settings.

Detailed guidelines:

1. On the Groups page, click the **Create Group** button to open the Add New Group page.

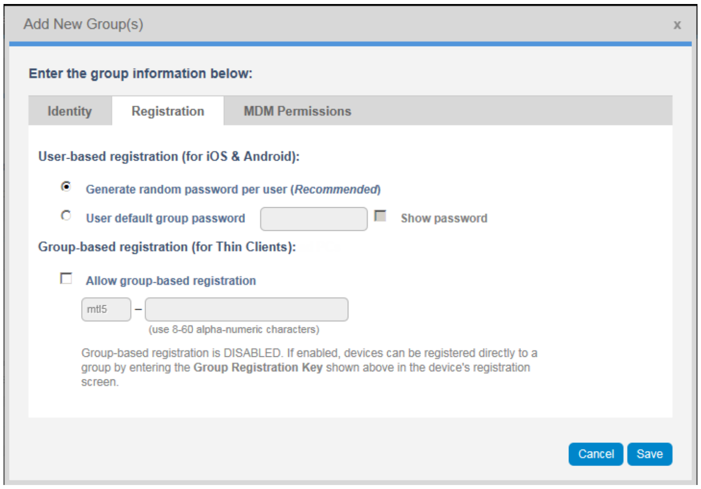


Enter the group information below:

Group name *

Description *

2. On the Identity tab, enter the group information—Group Name and Description. **IMPORTANT**: You cannot locally change the name and description of a group that has been imported from Active Directory as part of a Manual AD Sync import option (see "Active Directory Connector: Importing Existing Active Directory Users into the System"). You must use Active Directory to change the name and description of a group, and then synch.
3. Click the **Registration** tab.



Enter the group information below:

User-based registration (for iOS & Android):

● Generate random password per user (*Recommended*)

○ User default group password □ Show password

Group-based registration (for Thin Clients):

□ Allow group-based registration

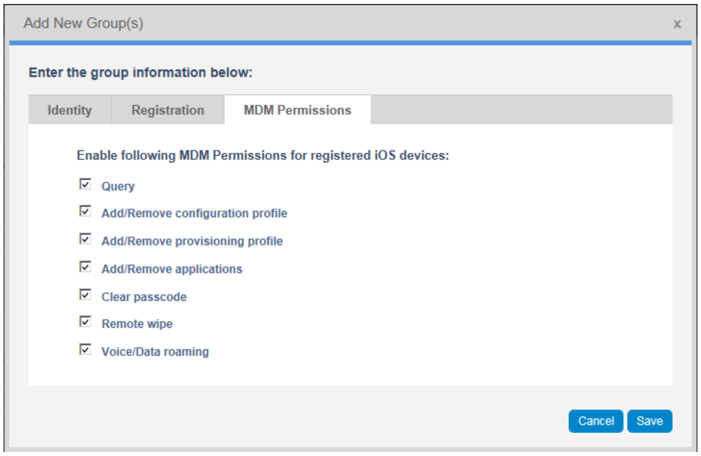
mtl5 –
(use 8-60 alpha-numeric characters)

Group-based registration is DISABLED. If enabled, devices can be registered directly to a group by entering the **Group Registration Key** shown above in the device's registration screen.

4. On the Registration tab, configure the registration information you want to use (device, passwords, and so on) for User registration (from their client devices). **NOTE**: The User-based options allow you to configure passwords (either generate a random password or to enter a default group password) for iOS and Android devices. The Allow group-based registration option configures a common registration key for all Thin Clients in this Group—and registers them directly to this Group.
TIP: Users will register their client device using the credentials you provide to them (they must enter the credentials into the management software installed on their device and register into the management system).

IMPORTANT: Thin clients can only register to Groups directly and must have a Group Registration Key enabled to do so (the key is the unique identifier for this cloud-based policy group). Select the **Allow group-based registration** option (to configure a common registration key for all Thin Clients in this Group—it registers them directly to this Group), enter an 8 to 64 alpha-numeric character key into the Group Registration Key box (this is the key for User registration of their thin client—the first four digits are hard-coded by the system and uniquely identifies your tenant).
NOTE: Group Registration Key for thin client device registration can be applied from multiple sources (in order of precedence: 1 - DHCP option tag 199, 2 - INI configuration file parameters cccmenable and groupkey, 3 - client local configuration Central Configuration > CCM tab, and 4 - a Group Registration Key update from the management console using a Change Group request). For details on these options, see the management console usage documentation within your supported thin client Administrator and INI documentation.

5. Click the **MDM Permissions** tab.



Add New Group(s) x

Enter the group information below:

Identity | Registration | MDM Permissions

Enable following MDM Permissions for registered iOS devices:

☑ Query
☑ Add/Remove configuration profile
☑ Add/Remove provisioning profile
☑ Add/Remove applications
☑ Clear passcode
☑ Remote wipe
☑ Voice/Data roaming

Cancel Save

6. On the MDM Permissions tab, enable the permissions you want to allow Administrators to use (for client device management from the management console) after a client device is registered by a user. The Administrator permissions allow you to remotely:
   - **Query** - Query installed configuration profiles, provisioning profiles, installed applications, device restrictions, and security settings.
   - **Add/Remove Configuration Profile** - Install and remove policy configuration profiles.
   - **Add/Remove Provisioning Profile** - Install and remove provisioning profiles.
   - **Add/Remove Applications** - Install and remove device applications.
   - **Clear Passcode** - Clear the configured device passcode (useful for forgotten passcodes).
   - **Remote Wipe** - Wipe the device, erasing all data and applications (sets the device to factory defaults —not recommended for employee-owned devices).
   - **Voice/Data Roaming** - Enable and disable voice and data roaming settings.
7. Click **Save**. The Group is added to the list of available Groups on the Groups page.

Configuring and Managing Policies (Global, Group-level, and Exception-based Policy Management)

Policies can be managed at many different levels. Policies can be assigned organization-wide, on a per-Group basis, on a per-User basis, or on a per-Device basis.

If a policy configuration has conflicts between the different levels (for example, a passcode policy is applied at the User and Group levels with different passcode complexities) the lowest-level (most-detailed level) policy takes precedence (in our example case, the User level—the more detailed level—will take precedence over the Group level).

IMPORTANT: Policies are enforced in the following order:

1. **Device** (see "Device Level Exceptions")
2. **User** (see "User Level Exceptions")
3. **Group** (see "Group Level Policies")
4. **Global** (see "Global Level Policies")

TIP: Use the following general guidelines when working with policies:

- Policies can be modified on multiple levels and the information will automatically be consolidated into one policy for each User/Device.
- iOS and Android policies can be configured at Global, Per Group, Per User, and Per Device levels.
- Thin client policies can be configured at Global, Per Group, and Per Device levels.
- Policies are inherited in the order they are created. Any settings you configure in a Default Policy Group will be the default in all the policies below that Default Policy Group (likewise for a Group—all Users and Devices in that Group have the Default Policy Group as their default).
- You can always create an exception for a User/Device in a Group to have a subset of policies to be different than the Group default. You can do this using the User Details page or the Device Details page. These detail pages display the configuration for that asset with details of where configurations are set (Global, Group, User, Device levels) and allows you the option to create exceptions.
- When modifying lower-level policies, any policy that is an override to a higher-level policy will be indicated by a bullet symbol to the left of the policy type (for example, Passcode, Restrictions, Wi-Fi, and so on).
- While modifying policies, an asterisk (*) will be placed to the right of the policy types to indicate that there are unsaved (and unpublished) changes. To review these changes prior to publishing them, click on the **View pending changes** link at the right of the panel.
- As soon as you click the **Save & Publish** button, the devices are notified about the changes and the changes will take effect based on the behavior of the devices (that is, mobile devices always apply changes immediately while thin client changes usually occur after a reboot—many thin client settings force a reboot immediately to apply your changes).

Global Level Policies

To configure the settings of a policy at the Global level, click the **Edit Policies** link of the Default Policy Group, select the device you want (**iOS**, **Android**, **ThinOS/Xenith**) from the menu, click the Settings button you want, and then click the **Configure this item** button to open and use the settings page to configure your settings (be sure to click **Save and Publish** after configuring your settings).

For details on the device you want, see "Details: Thin Client Policy Settings," "Details: IOS Policy Settings," or "Details: Android Policy Settings."

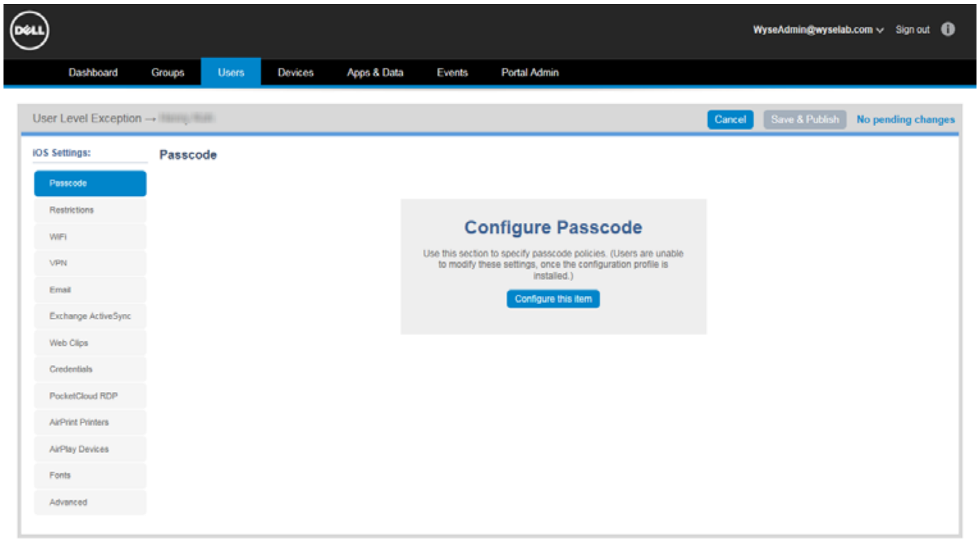
Group Level Policies

To configure the settings of a policy at the Group level, click the **Edit Policies** link of a Group Policy, select the device you want (**iOS**, **Android**, **ThinOS/Xenith**) from the menu, click the Settings button you want, and then click the **Configure this item** button to open and use the settings page to configure your settings (be sure to click **Save and Publish** after configuring your settings).

For details on the device you want, see "Details: Thin Client Policy Settings," "Details: IOS Policy Settings," or "Details: Android Policy Settings."

User Level Exceptions

To configure a policy at the User level, click the **Users** tab to open the Users page, click a Name link to open the User Details page, click the **Summary** tab, scroll to the User Configuration section, click **Create/Edit Exceptions** and select the device type for which you want to manage the exceptions from the menu to open and use the User Level Exceptions page.

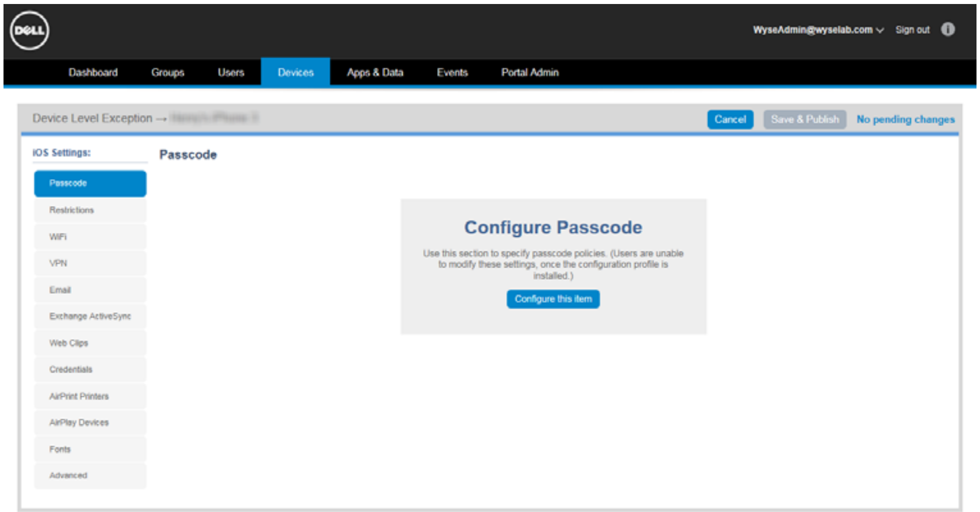


Use this section to specify passcode policies. (Users are unable to modify these settings, once the configuration profile is installed.)

For details on the device you want, see "Details: Thin Client Policy Settings," "Details: IOS Policy Settings," or "Details: Android Policy Settings."

Device Level Exceptions

To configure a policy at the Device level, click the **Devices** tab to open the Devices page, click a Name link to open the Device Details page, click the **Summary** tab, scroll to the Device Configuration section, click **Create/Edit Exceptions** and select the device type for which you want to manage the exceptions from the menu to open and use the Device Level Exceptions page.

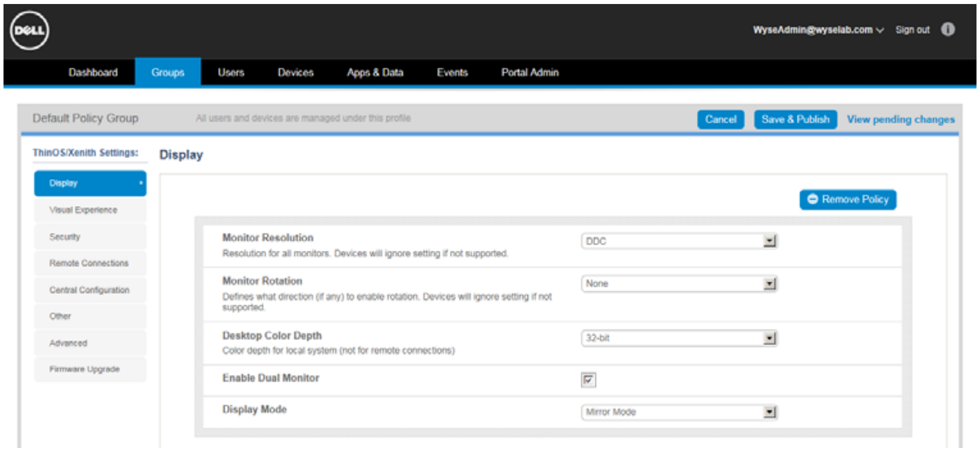


Use this section to specify passcode policies. (Users are unable to modify these settings, once the configuration profile is installed.)

For details on the device you want, see "Details: Thin Client Policy Settings," "Details: IOS Policy Settings," or "Details: Android Policy Settings."

Details: Thin Client Policy Settings

To edit the thin client policy settings of a Group or the Default Policy Group, click the **Edit Policies** link of a Group or the Default Policy Group, select **ThinOS/Xenith** from the menu, click the ThinOS/Xenith Settings button you want, and then click the **Configure this item** button to open and use the settings page (be sure to click **Save and Publish** after configuring).



Default Policy Group — All users and devices are managed under this profile

Display

Monitor Resolution — Resolution for all monitors. Devices will ignore setting if not supported. — DDC

Monitor Rotation — Defines what direction (if any) to enable rotation. Devices will ignore setting if not supported. — None

Desktop Color Depth — Color depth for local system (not for remote connections) — 32-bit

Enable Dual Monitor — ☑

Display Mode — Mirror Mode

Thin client policy settings include the following:

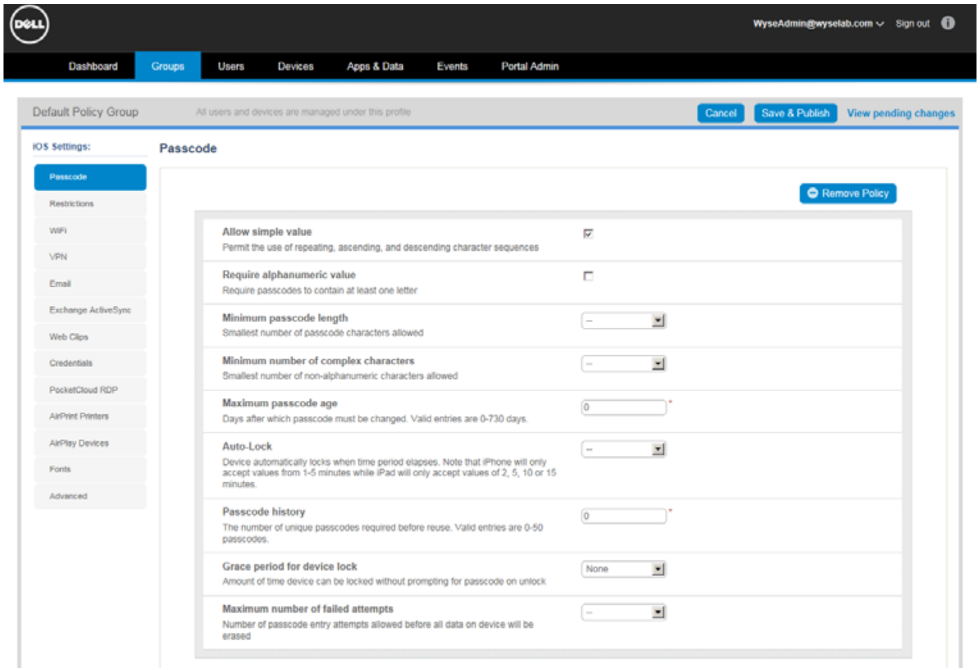
- **Display** - Use this page to configure thin client display settings such as resolution, rotation, color depth, and dual monitor.
- **Visual Experience** - Use this page to configure thin client visual experience settings such as desktop display (Classic or Zero Launchpad) and session functionality.
- **Security** - Use this page to configure thin client security settings such as user privilege, G-key reset, Trace, VNC, user prompts, Force 8bit, and certificate installation.
  NOTES:
  Remote firmware imaging from the cloud is supported with ThinOS firmware version 8.0_037 or later.
  Certificate assignment can be managed at Global level, group level or device level.
  Selecting Auto-Install Certificates will load the list of Certificates uploaded to the File Repository Inventory page (see "Apps & Data").
  Selecting the certificates to be auto-installed on thin clients is only for automating the deployment of certificates. Un-selecting from the policy will not remove any certificate already installed on the device.
- **Remote Connections** - Use this page to configure thin client remote connection settings such as addresses and credentials for brokered (Citrix, Microsoft, VMware) and direct (RDP) connections.
- **Central Configuration** - Use this page to configure thin client central configuration settings such as server protocol, location, and credentials (for INI files).
- **Other** - Use this page to configure thin client settings such as default sign-on credentials, time servers, and time zone.
- **Advanced** - Use this page to configure thin client advanced settings such as custom INI commands and Global INI functionality (10 item limit).
- **Firmware Upgrade** - Use this page to configure thin client firmware upgrade settings such as live upgrade (for next boot or immediate firmware download preferences), Firmware Update Logic, local firmware check preferences, and platform firmware mappings.
  NOTES: Remote firmware imaging from the cloud is supported with ThinOS firmware version 8.0_037 or later.
  Certificate assignment can be managed at Global level, group level or device level.

Additional Details for Policy-based Firmware Deployment:

- **Disable Live Upgrade**: Live Upgrade means the thin client will immediately begin downloading and apply new firmware based on defined policies. If you prefer that the thin client only check for new firmware on each boot-up, then you can disable Live Upgrade.
- **Firmware Update Logic**: Determines how the thin client behaves when a new firmware is published from the management console:
  - **Any different firmware**: Thin client updates firmware to the version assigned by the management policy (even if version is lower than current image on device)
  - **New firmware only**: Thin client updates firmware only when a newer version is assigned to the management policy.
  - **Do not update**: Thin client ignores firmware versions assigned to the management policies.
- **Skip Local Firmware Check**: When enabled, thin client will bypass local fileserver checks for firmware updates.
  NOTE: It is highly recommended to always have this option enabled if you define firmware on the management console. Otherwise, if you have firmware policies in the management console and firmware located on a local file server, it will lead to an endless reboot as the thin client applies differing images. This option is available to assist in certain migration scenarios where this flexibility is needed.
- **Platform Type and Firmware to auto-deploy (version assignment)**: This area maps specific firmware versions to different platform types (for example, T10, R10, Xenith Pro, and so on) allowing for different firmware versions to be assigned to different platforms.
  To map a platform type to a specific firmware version select the desired platform from the Platform Type list and then select the desired firmware version from the Firmware to auto-deploy list. The list of platform types displays in parentheses the number of firmware versions currently uploaded to the File Repository Inventory page that are supported.

Details: IOS Policy Settings

To edit the iOS Policy settings of a Group or the Default Policy Group, click the **Edit Policies** link of a Group or the Default Policy Group, select **iOS** from the menu, click the iOS Settings button you want, and then click the **Configure this item** button to open and use the settings page (be sure to click **Save and Publish** after configuring).



Passcode

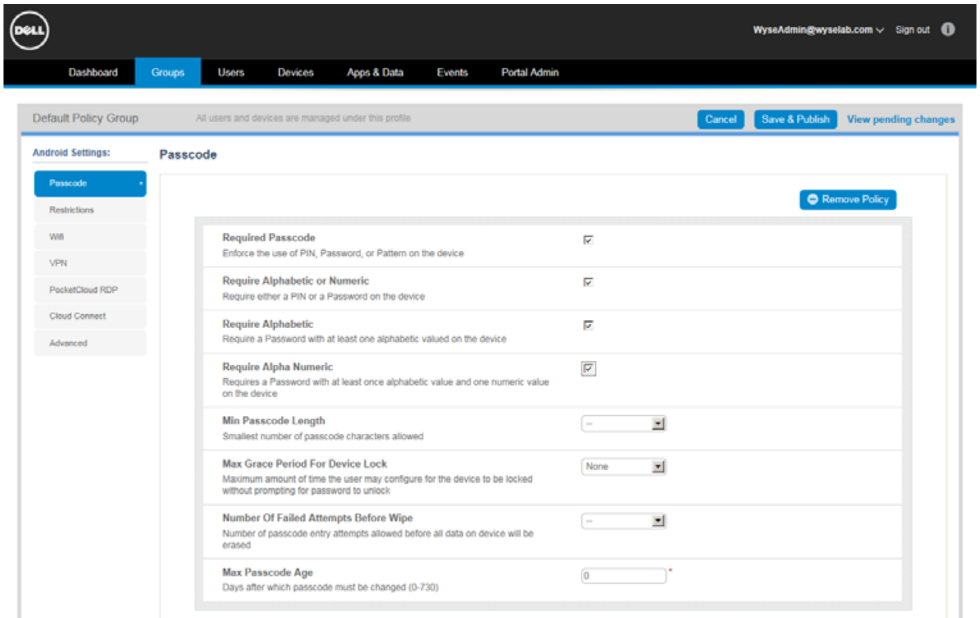
Allow simple value Permit the use of repeating, ascending, and descending character sequences	☑
Require alphanumeric value Require passcodes to contain at least one letter	☐
Minimum passcode length Smallest number of passcode characters allowed	--
Minimum number of complex characters Smallest number of non-alphanumeric characters allowed	--
Maximum passcode age Days after which passcode must be changed. Valid entries are 0-730 days.	0 *
Auto-Lock Device automatically locks when time period elapses. Note that iPhone will only accept values from 1-5 minutes while iPad will only accept values of 2, 5, 10 or 15 minutes.	--
Passcode history The number of unique passcodes required before reuse. Valid entries are 0-50 passcodes.	0 *
Grace period for device lock Amount of time device can be locked without prompting for passcode on unlock	None
Maximum number of failed attempts Number of passcode entry attempts allowed before all data on device will be erased	--

iOS Policy settings include the following:

- **Passcode** - Use this page to configure iOS device passcodes and locking settings.
- **Restrictions** - Use this page to configure iOS device restrictions such as iCloud, applications, Safari options, device functionality, camera use, security and privacy, content ratings, and allowed content ratings.
- **WiFi** - Use this page to configure iOS device WiFi settings such as functionality, proxy, and security.
- **VPN** - Use this page to configure iOS VPN settings such as name, server, account, type, and proxy.
- **Email** - Use this page to configure iOS device Email settings for IMAP or POP email access such as account, incoming mail, and outgoing mail.
- **Exchange ActiveSync** - Use this page to configure iOS device Exchange server settings such as account, synchronization, and device functionality.
- **Web Clips** - Use this page to configure iOS device Web Clips settings such as displayed URL information, icons, and Web display functionality.
- **Credentials** - Use this page to upload certificates for iOS device credential use such as validation and authentication.
- **PocketCloud RDP** - (Dell Management Console Pro Version Only) Use this page to configure iOS device PocketCloud RDP settings such as host address, credentials, display, and device functionality.
- **AirPlay Devices** - Use this page to configure iOS device AirPlay settings such as destination device name and password.
- **AirPrint Printers** - Use this page to configure iOS device AirPrint settings such as printer IP Address and path.
- **Fonts** - Use this page to configure iOS device font settings.
- **Advanced** - Use this page to configure iOS device settings to Allow Non-Encrypted Devices.

Details: Android Policy Settings

To edit the Android Policy settings of a Group or the Default Policy Group, click the **Edit Policies** link of a Group or the Default Policy Group, select **Android** from the menu, click the Android Settings button you want, and then click the **Configure this item** button to open and use the settings page (be sure to click **Save and Publish** after configuring).



Default Policy Group — All users and devices are managed under this profile

Passcode

Required Passcode ☑
Enforce the use of PIN, Password, or Pattern on the device

Require Alphabetic or Numeric ☑
Require either a PIN or a Password on the device

Require Alphabetic ☑
Require a Password with at least one alphabetic valued on the device

Require Alpha Numeric ☑
Requires a Password with at least once alphabetic value and one numeric value on the device

Min Passcode Length --
Smallest number of passcode characters allowed

Max Grace Period For Device Lock None
Maximum amount of time the user may configure for the device to be locked without prompting for password to unlock

Number Of Failed Attempts Before Wipe --
Number of passcode entry attempts allowed before all data on device will be erased

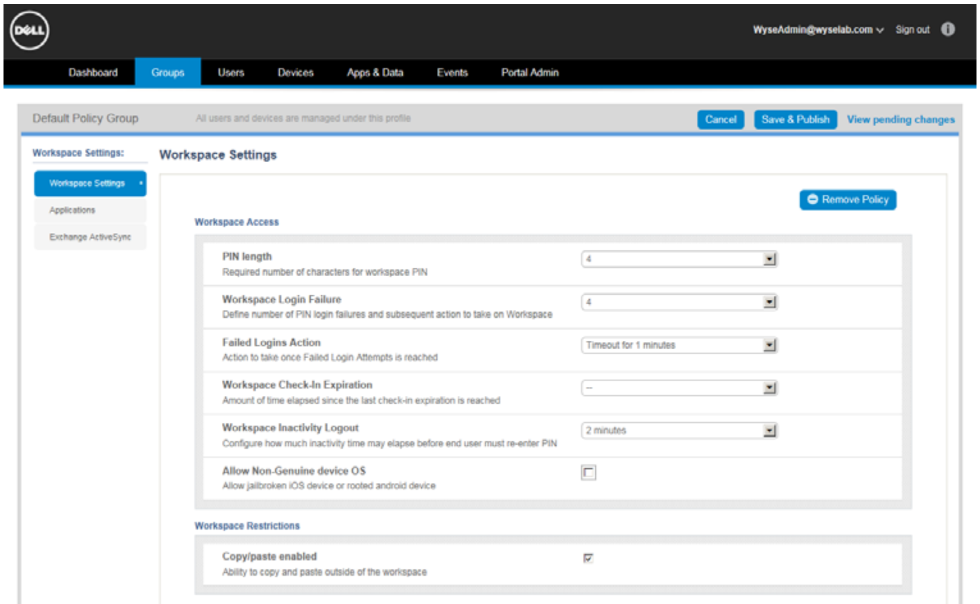
Max Passcode Age 0 *
Days after which passcode must be changed (0-730)

Android Policy settings include the following:

- **Passcode** - Use this page to configure Android device passcodes and locking settings.
- **Restrictions** - Use this page to configure Android device restrictions such as use of camera, YouTube, browser, Google Play, and Facebook.
- **WiFi** - Use this page to configure Android device WiFi settings such as functionality, network, and security.
- **VPN** - Use this page to configure iOS VPN settings such as name, server, account, type, and proxy.
- **PocketCloud RDP** - (Dell Management Console Pro Version Only) Use this page to configure Android device PocketCloud RDP settings such as host address, credentials, display, and device functionality.
- **Dell Wyse Cloud Connect** - (Dell Wyse Cloud Connect Only) Use this page to configure Dell Wyse Cloud Connect settings such as external storage, Bluetooth privileges, notifications, App installation, certificate installation, Administrator Mode password management, and visual experience.
  NOTE: The Kiosk option allows you to add a single App to the Select App list. The LaunchPad option allows you to add up to eight Apps to the Select Apps list.
- **Dell Wyse Cloud Connect Advanced** - (Dell Wyse Cloud Connect Only) If enabled (see "Other Settings: APNS Warnings, License Expiration Warnings, and Self Service Legal Agreements (Enforcing the Agreement for All Self Service Users)"), use this page to configure advanced commands. These Advanced Dell Wyse Cloud Connect options allow you to specify native commands using Dell Wyse Cloud Connect specific parameters (up to 10).
  NOTE: These options should only be used for specific commands when provided by the Dell Wyse Cloud Connect team.
- **Advanced** - Use this page to configure Android device settings to Allow Non-Encrypted Devices.

Details: Workspace Policy Settings

To edit the Workspace Policy settings of a Group or the Default Policy Group, click the **Edit Policies** link of a Group or the Default Policy Group, select **Workspace** from the menu, click the Workspace Settings button you want, and then click the **Configure this item** button to open and use the settings page (be sure to click **Save and Publish** after configuring).



Default Policy Group — All users and devices are managed under this profile

Workspace Settings

Workspace Access

PIN length Required number of characters for workspace PIN	4
Workspace Login Failure Define number of PIN login failures and subsequent action to take on Workspace	4
Failed Logins Action Action to take once Failed Login Attempts is reached	Timeout for 1 minutes
Workspace Check-In Expiration Amount of time elapsed since the last check-in expiration is reached	--
Workspace Inactivity Logout Configure how much inactivity time may elapse before end user must re-enter PIN	2 minutes
Allow Non-Genuine device OS Allow jailbroken iOS device or rooted android device	☐

Workspace Restrictions

Copy/paste enabled Ability to copy and paste outside of the workspace	☑

Workspace Policy settings include the following:

- **Workspace Settings** - Use this page to configure general device settings such as access and restrictions.
- **Applications** - Use this page to configure general application settings such as email, synch frequency, calendar, browser, and so on.
- **Exchange Activesync**- Use this page to configure general Microsoft Exchange Server settings such as SSL use, domain, user, email, and so on.

This page intentionally blank.

5 Users

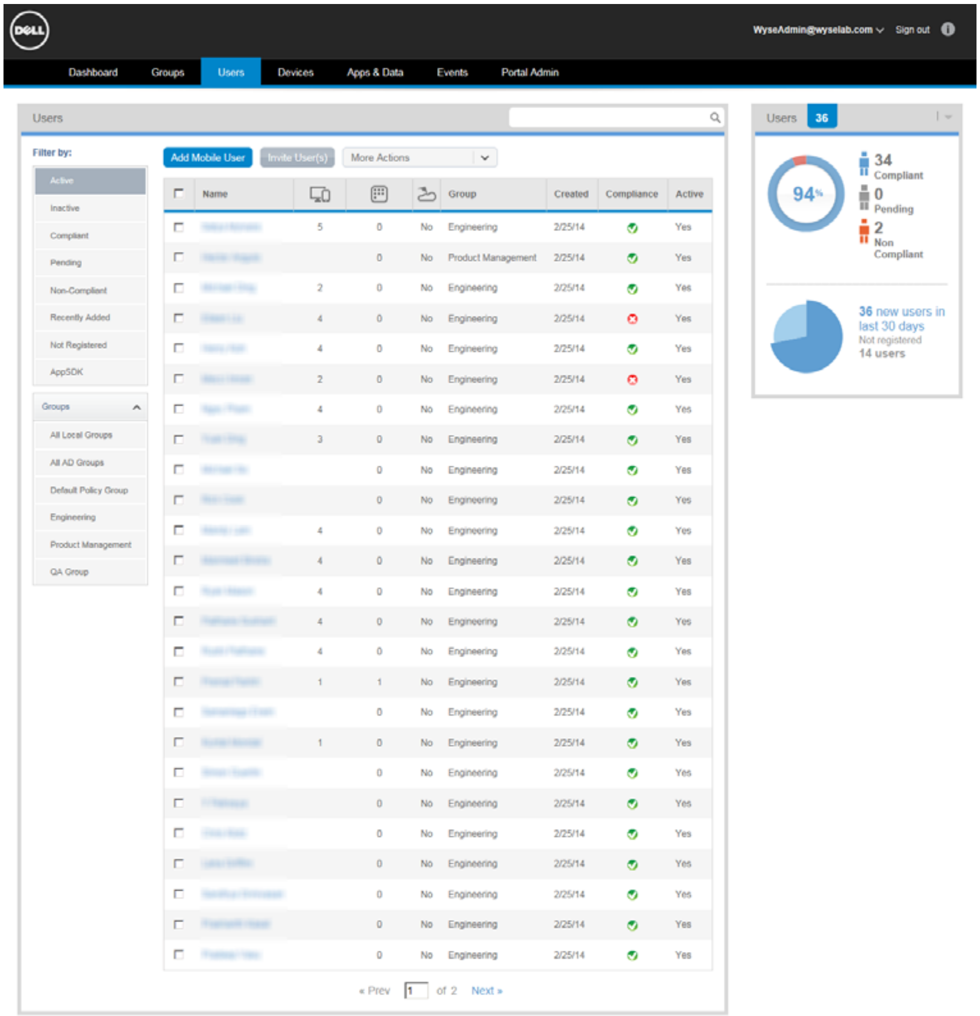
This section describes how to perform routine User management tasks using the management console. Users can be added to the Global Group Policy (the top-level policy) or to any existing Group Policies you created in the system.

Topics include:

- "Managing Users"
    - "Adding/Editing Users"
    - "Inviting Users to Register Devices"
    - "Viewing and Managing User Details"
    - "Changing Group Membership of Users"

Managing Users

The Users page allows you to quickly view and manage the Users that are available (see Table 2). It also allows you to easily display the Users you want by using the filtering feature.



□	Name				Group	Created	Compliance	Active
□	[illegible]	5	0	No	Engineering	2/25/14	✓	Yes
□	[illegible]		0	No	Product Management	2/25/14	✓	Yes
□	[illegible]	2	0	No	Engineering	2/25/14	✓	Yes
□	[illegible]	4	0	No	Engineering	2/25/14	✗	Yes
□	[illegible]	4	0	No	Engineering	2/25/14	✓	Yes
□	[illegible]	2	0	No	Engineering	2/25/14	✗	Yes
□	[illegible]	4	0	No	Engineering	2/25/14	✓	Yes
□	[illegible]	3	0	No	Engineering	2/25/14	✓	Yes
□	[illegible]		0	No	Engineering	2/25/14	✓	Yes
□	[illegible]		0	No	Engineering	2/25/14	✓	Yes
□	[illegible]	4	0	No	Engineering	2/25/14	✓	Yes
□	[illegible]	4	0	No	Engineering	2/25/14	✓	Yes
□	[illegible]	4	0	No	Engineering	2/25/14	✓	Yes
□	[illegible]	4	0	No	Engineering	2/25/14	✓	Yes
□	[illegible]	4	0	No	Engineering	2/25/14	✓	Yes
□	[illegible]	1	1	No	Engineering	2/25/14	✓	Yes
□	[illegible]		0	No	Engineering	2/25/14	✓	Yes
□	[illegible]	1	0	No	Engineering	2/25/14	✓	Yes
□	[illegible]		0	No	Engineering	2/25/14	✓	Yes
□	[illegible]		0	No	Engineering	2/25/14	✓	Yes
□	[illegible]		0	No	Engineering	2/25/14	✓	Yes
□	[illegible]		0	No	Engineering	2/25/14	✓	Yes
□	[illegible]		0	No	Engineering	2/25/14	✓	Yes
□	[illegible]		0	No	Engineering	2/25/14	✓	Yes
□	[illegible]		0	No	Engineering	2/25/14	✓	Yes

Note that the Active Directory icon helps you to distinguish between locally created/ managed Groups and those created as part of an Active Directory import (Manual AD Sync option only).

AD

This icon is shown in the Users page (Group column), and anywhere else the Group name is shown (for example, Groups page, Group filters/statistics, Event messages, and so on). For Active Directory information, see "Active Directory Connector: Importing Existing Active Directory Users into the System."

Use the following guidelines:

- **Filter By area** - Click the button you want to view the Users you want.
- **Name links** - Click the Name link of a User to view and manage User details (see "Viewing and Managing User Details").
- **Users Statistics area** - Use this area to view a summary of the users statistics/ analytics available from your filter results.

TIP: AppSDK displays whether or not a user has logged into the management console though the PocketCloud Remote Desktop Pro app for iOS or Android.

Table 2 provides a quick overview of what you can do using the Users page.

IMPORTANT: Depending on your Active Directory integration with the management console and your management console Active Directory Connector settings, you will manage your user and group details from the management console or your Active Directory (see "Active Directory Connector: Importing Existing Active Directory Users into the System").

Table 2 Routine User Tasks - Users page

Tasks You Can Do	How	Details
Add a User to the system.	Click the **Add Mobile User** button to open the New Mobile User page, and then use the tabs to configure the settings.	"Adding/Editing Users." **NOTE**: After policy groups are configured, users can be added to these Groups (users can also be associated to the top-level Global Group Policy). Users register directly from their mobile devices to the management system.
Invite a User	Select the check box next to the name of the User you want in the Users page, and then click **Invite Users** to open and use the Invite Users Email page to send users information about how to register their devices (a set of different template email messages are pre-configured).	"Inviting Users to Register Devices." **NOTE**: Users in system are not automatically notified about registration. You must use the **Invite Users** button to send users information about how to register their devices.
View and manage User details.	Click a Name link in the Users page to open and use the User Details page.	"Viewing and Managing User Details."
Change the Group to which a User belongs.	Select the check box next to the name of the User you want in the Users page, and then click **More Actions > Change Group** to open and use the **Alert/Change Group** page.	"Changing Group Membership of Users."

Table 2 Routine User Tasks - Users page , Continued

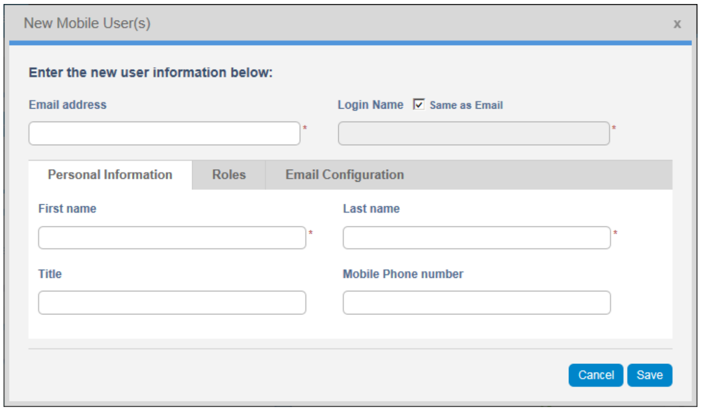
Tasks You Can Do	How	Details
Edit a User account in the system.	Click a Name link in the Users page to open the User Details page, click **Edit User**, and then make your changes.	Use same guidelines in "Adding/Editing Users."
Deactivate a User.	Select the check box next to the name of the User you want in the Users page, and then click **More Actions > Deactivate User** to deactivate/disable the user in the system.	You can also use the **Deactivate User** button on the User Details page (see "Viewing and Managing User Details"). **NOTE**: After deactivating a User, a User attempting to register a device or log in to the Self-Service portal will not be able to do so.
Activate a User.	Select the check box next to the name of the User you want in the Users page, and then click **More Actions > Activate User** to activate/enable the user in the system.	You can also use the **Activate User** button on the User Details page (see "Viewing and Managing User Details"). **NOTE**: After activating a User, they will be able to register a device and log in to the Self-Service portal.
Delete a user.	Select the check box next to the Name link of a user not currently active (does not have an Active status) that you want in the Users page, and then click **Delete User(s)** to delete/remove the user from the system.	**NOTE**: Only a user that is not currently active (does not have an Active status) can be deleted from the system. A user must be deactivated prior to deleting.

Adding/Editing Users

To add a User:
On the Users page, click the **Add Mobile User** button to open the New Mobile User page, and then use the Personal Information tab, Roles tab, and Email Configuration tab, to enter the user information (passwords and so on), select the Policy Group (Group Policy) and Role (Global Administrator or Global Viewer — see "Managing Administrators and Viewers of the Management Console") to which you want to assign the user, and configure email information.

Detailed guidelines:

1. On the Users page, click the **Add Mobile User** button to open the New Mobile User page.



New Mobile User(s)

Enter the new user information below:

Email address *

Login Name ☑ Same as Email *

Personal Information | Roles | Email Configuration

First name *

Last name *

Title

Mobile Phone number

2. Use the following tabs to configure the settings:

   Personal Information tab:

   - **Email Address**: Must be a valid email address (used for password recovery).
   - **Login Name**: The Login Name is the username used for device registration and for logging into the Self-Service portal (see "Other Settings: APNS Warnings, License Expiration Warnings, and Self Service Legal Agreements (Enforcing the Agreement for All Self Service Users)") and can be the same as the email address or customized. **CAUTION**: Once created, this Login Name cannot be modified (you must deactivate and delete the User, and then create a new User with same email address but different Login Name if desired).
   - **First Name / Last Name / Title / Mobile Phone Number**

   Roles tab:

   - **Enable Mobile User Role**: Select if you want to enable device registration and Self-Service portal access for this mobile-device User; and then select the policy group to which you want to assign the User (the mobile user role requires a policy group).
   - **Portal Administrator**: Select this option if you want to enable administration access to the system for this User (administrator access rights), and then select the role (Global Administrator or Global Viewer) to which you want to assign the User. In general, **Global Viewers** have read-only access to the management console, but can also be given rights to issue any of the following Real-Time commands that you specify: Query, Lock, Clear Passcode, Unregister, Wipe, Restart (see "Managing Administrators and Viewers of the Management Console"). Note that newly created administrators will be forced to enter a new password at their first login.

- **Password**: The password is used for device registration and is the password for logging into the Self-Service portal. Select a User-based option to either generate a random password or to enter a custom password:
  Random password: System assigns a random password for the User.
  Custom password: Manually enter the password you want (passwords must contain a minimum of 8 characters (up to a maximum of 64) including 1 upper case letter, 1 lower case letter, and 1 numerical digit). If a group password has been configured, this is the default custom password.
  TIP: Users will register their client device using the credentials you provide to them (they must enter the credentials into the management software installed on their device and register into the management system).
  CAUTION: It is highly recommended that this password be changed at first login. (see "Changing Your Password"). Newly created administrators, and any Mobile User trying to activate the Self-Service portal for first time, will be forced to enter a new password at their first login.

Email Configuration tab:

- **Exchange/IMAP/POP**: Configure the email information you require. The Email Configuration tab is used to link user-specific account information for Exchange ActiveSync and Email policies for iOS devices. Whenever the Dynamic User Info option is selected on either an Exchange ActiveSync or Email policy, the user-specific information configured in this tab will be sent to the device to simplify configuration on the iOS device - the user will simply be prompted to enter their password to complete the configuration of their email account.
  ADMINISTRATOR NOTE: Email information is required for those administrators who also have a Mobile User role assigned (otherwise it is not really applicable to users who exclusively have a Global Administrator or Global Viewer role).

3. After configuring, click **Save**. The User is added to the list of available Users on the Users page and to the assigned Group on the Group Details page.

Inviting Users to Register Devices

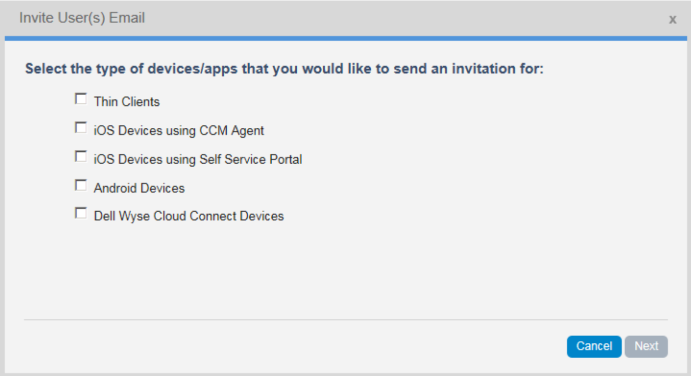
To invite a User to register a device:
Select the check box next to the name of the User you want in the Users page, and then click **Invite Users** to open and use the Invite Users Email wizard to send Users information about how to register their devices (a set of different template email messages are pre-configured).

iOS IMPORTANT: If corporate email is not configured on the user’s device, they can follow the steps described in the email to enroll the device. The email includes the URL address the user will need to navigate to using Safari on the iOS device, their login credentials, and the instructions to click the **Register iOS Device** button to initiate the registration process from the device. **TIP**: Users can also use the Dell Mobile Management Agent for iOS downloadable from the Apple App Store to register the device.

Android IMPORTANT: If corporate email is not configured on the user’s device, they can follow the steps described in the email to enroll the device. The email includes the link to download the Dell Mobile Management Agent for Android (from Google Play) and the required login credentials to initiate the registration process from the device.

Detailed guidelines:

1. On the Users page, select the check box next to the name of the User you want, and then click **Invite Users** to open and use the Invite Users Email wizard.



Invite User(s) Email

Select the type of devices/apps that you would like to send an invitation for:

☐ Thin Clients
☐ iOS Devices using CCM Agent
☐ iOS Devices using Self Service Portal
☐ Android Devices
☐ Dell Wyse Cloud Connect Devices

2. Select the criteria you want and follow the wizard until you reach the Template you want to email to the user (a set of different template email messages are pre-configured).
   NOTE: All messages can be edited prior to sending (edits will not be saved to template). Also, note that any text that appears between brackets < > will be replaced with appropriate information specific for the User (therefore, do not change anything within the brackets).

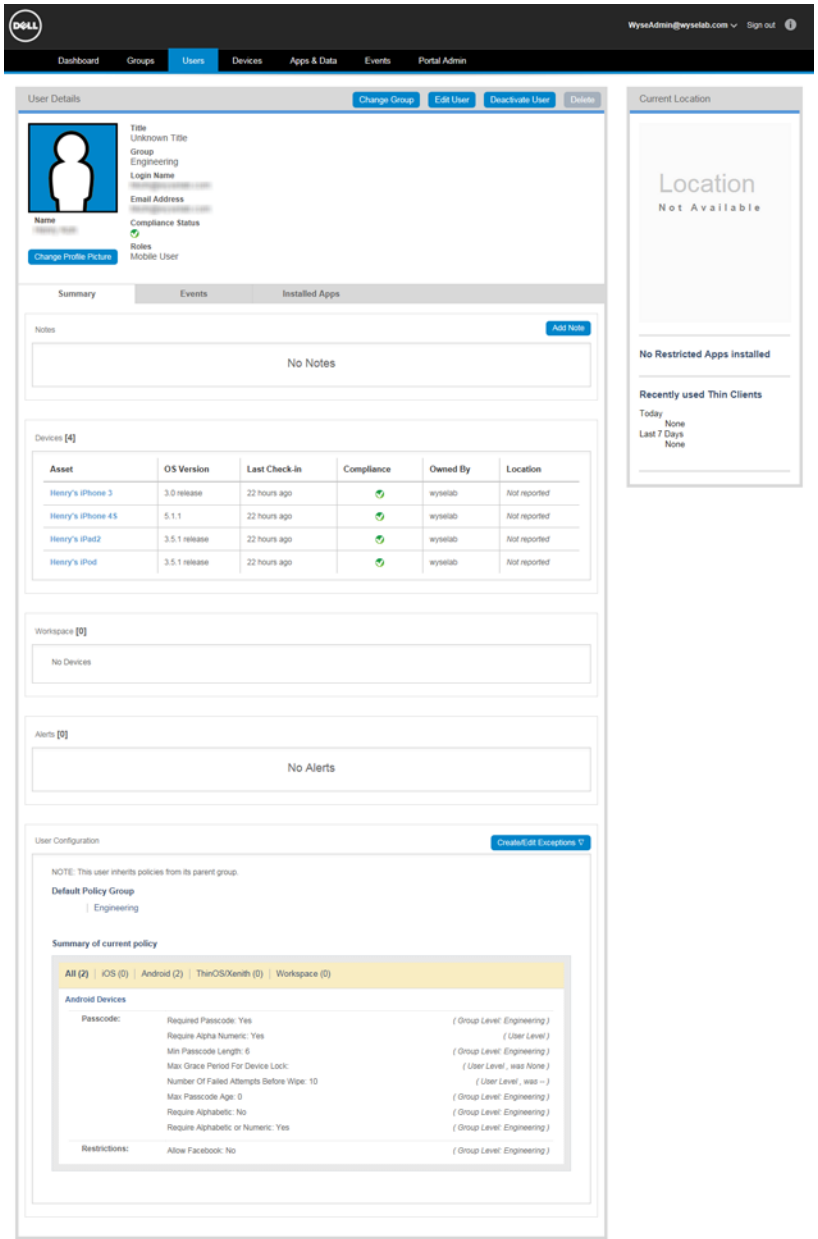
3. Click **Invite Users**. Users will use the instructions to register their device.

Viewing and Managing User Details

To view and manage User details:
On the Users page, click a **Name** link to open the User Details page and then perform your tasks.

Detailed guidelines:

1. On the Users page, click a **Name** link to open the User Details page.



Title
Unknown Title
Group
Engineering
Login Name
[redacted]
Email Address
[redacted]
Compliance Status
✓
Roles
Mobile User
Name
[redacted]

Notes

No Notes

Devices [4]

Asset	OS Version	Last Check-in	Compliance	Owned By	Location
Henry's iPhone 3	3.0 release	22 hours ago	✓	wyselab	*Not reported*
Henry's iPhone 4S	5.1.1	22 hours ago	✓	wyselab	*Not reported*
Henry's iPad2	3.5.1 release	22 hours ago	✓	wyselab	*Not reported*
Henry's iPod	3.5.1 release	22 hours ago	✓	wyselab	*Not reported*

Workspace [0]

No Devices

Alerts [0]

No Alerts

User Configuration

NOTE: This user inherits policies from its parent group.

Default Policy Group
| Engineering

Summary of current policy

All (2) | iOS (0) | Android (2) | ThinOS/Xenith (0) | Workspace (0)

Android Devices

Passcode:	Required Passcode: Yes	*(Group Level: Engineering)*
	Require Alpha Numeric: Yes	*(User Level)*
	Min Passcode Length: 6	*(Group Level: Engineering)*
	Max Grace Period For Device Lock:	*(User Level , was None)*
	Number Of Failed Attempts Before Wipe: 10	*(User Level , was --)*
	Max Passcode Age: 0	*(Group Level: Engineering)*
	Require Alphabetic: No	*(Group Level: Engineering)*
	Require Alphabetic or Numeric: Yes	*(Group Level: Engineering)*
Restrictions:	Allow Facebook: No	*(Group Level: Engineering)*

Current Location

Location
Not Available

No Restricted Apps installed

Recently used Thin Clients
Today
None
Last 7 Days
None

2. Although the User Details page shows you all detailed information and current location for a User in the system, you can use the following guidelines to perform tasks and view the information you want:
   - **Change Group** - Use the Change Group button to change the Group to which the User is assigned (see "Changing Group Membership of Users").
   - **Edit User** - Use the Edit User button to edit the account settings of the User. (see "Adding/Editing Users").
   - **Deactivate User** - Use the Deactivate User button to deactivate/disable the User in the system.

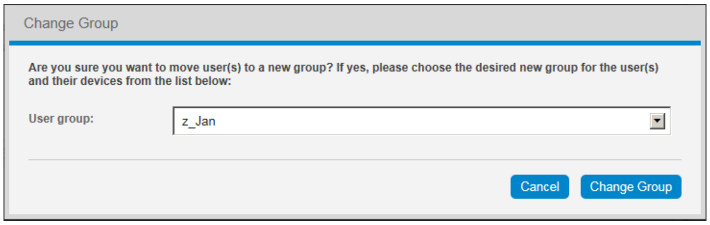
- **Delete** - Use the Delete button to delete the User in the system. **IMPORTANT**: Only a user that is not currently active (does not have an Active status in the Users page) can be deleted from the system. A user must be deactivated prior to deleting.
- **Summary tab** - Use the Summary tab to view and manage information on the Notes, Devices, Alerts, and User Configuration of a User.
  For information on **Create/Edit Exceptions**, see "User Level Exceptions."
  For information on device/asset details (clicking the Device Asset link), see "Viewing and Managing Device Details."
- **Events tab** - Use the Events tab to view and manage information on the system events pertaining to a User (creation, device registration, and various tasks performed by the system and the User).
- **Installed Apps tab** - Use the Installed Apps tab to view information on the Apps installed on the devices of the User (versions, App Policies, and so on). For information on managing Apps, see"Apps & Data."

Changing Group Membership of Users

To change the Group to which a User belongs:
Select the check box next to the name of the User you want in the Users page, and then click **Change Group** to open and use the **Alert/Change Group** page.

Detailed guidelines:

1. On the Users page, click **Change Group** to open the **Change Group** page.



Change Group

Are you sure you want to move user(s) to a new group? If yes, please choose the desired new group for the user(s) and their devices from the list below:

User group: z_Jan

2. Select the User Group to which you want to assign the user. **IMPORTANT**: If the new Group has different iOS MDM Permissions, these re-assigned Users must re-register any managed iOS devices.
3. (Optional) You can also send an email (click **Send Invitation Email**) to the user with any instructions they may need for group changes (for example, for cases where devices may need to be re-registered; otherwise, policy changes will be seamless to Users).
4. Click **Change Group**. The User is added to the group to which you assigned the user.

6 Devices

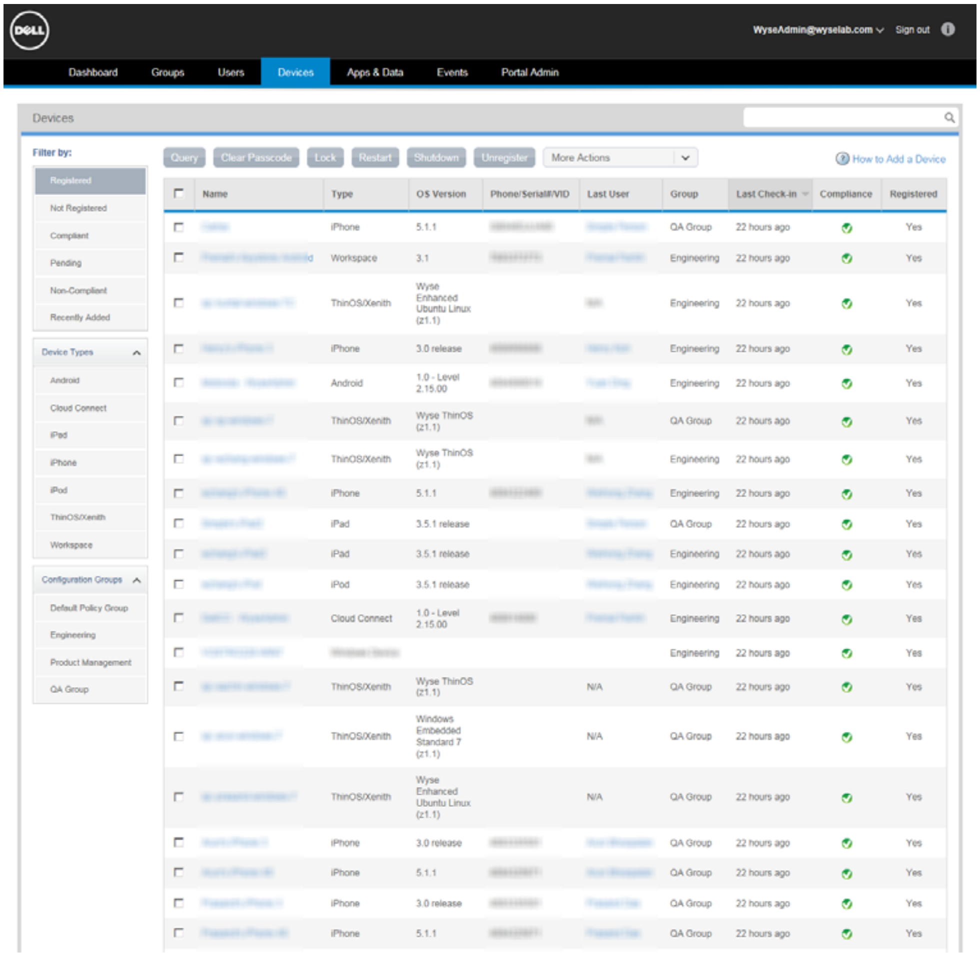
This section describes how to perform routine Device management tasks using the management console.

Topics include:

- "Managing Devices"
  - "Adding Devices"
  - "Viewing and Managing Device Details"

Managing Devices

The Devices page allows you to quickly view and manage the Devices that are available (see Table 3). It also allows you to easily display the Devices you want by using the filtering feature.



☐	Name	Type	OS Version	Phone/Serial#/VID	Last User	Group	Last Check-in	Compliance	Registered
☐	[redacted]	iPhone	5.1.1	[redacted]	[redacted]	QA Group	22 hours ago	✓	Yes
☐	[redacted]	Workspace	3.1	[redacted]	[redacted]	Engineering	22 hours ago	✓	Yes
☐	[redacted]	ThinOS/Xenith	Wyse Enhanced Ubuntu Linux (z1.1)		[redacted]	Engineering	22 hours ago	✓	Yes
☐	[redacted]	iPhone	3.0 release	[redacted]	[redacted]	Engineering	22 hours ago	✓	Yes
☐	[redacted]	Android	1.0 - Level 2.15.00	[redacted]	[redacted]	Engineering	22 hours ago	✓	Yes
☐	[redacted]	ThinOS/Xenith	Wyse ThinOS (z1.1)		[redacted]	QA Group	22 hours ago	✓	Yes
☐	[redacted]	ThinOS/Xenith	Wyse ThinOS (z1.1)		[redacted]	Engineering	22 hours ago	✓	Yes
☐	[redacted]	iPhone	5.1.1	[redacted]	[redacted]	Engineering	22 hours ago	✓	Yes
☐	[redacted]	iPad	3.5.1 release		[redacted]	QA Group	22 hours ago	✓	Yes
☐	[redacted]	iPad	3.5.1 release		[redacted]	Engineering	22 hours ago	✓	Yes
☐	[redacted]	iPod	3.5.1 release		[redacted]	Engineering	22 hours ago	✓	Yes
☐	[redacted]	Cloud Connect	1.0 - Level 2.15.00	[redacted]	[redacted]	Engineering	22 hours ago	✓	Yes
☐	[redacted]	[redacted]				Engineering	22 hours ago	✓	Yes
☐	[redacted]	ThinOS/Xenith	Wyse ThinOS (z1.1)		N/A	QA Group	22 hours ago	✓	Yes
☐	[redacted]	ThinOS/Xenith	Windows Embedded Standard 7 (z1.1)		N/A	QA Group	22 hours ago	✓	Yes
☐	[redacted]	ThinOS/Xenith	Wyse Enhanced Ubuntu Linux (z1.1)		N/A	QA Group	22 hours ago	✓	Yes
☐	[redacted]	iPhone	3.0 release	[redacted]	[redacted]	QA Group	22 hours ago	✓	Yes
☐	[redacted]	iPhone	5.1.1	[redacted]	[redacted]	QA Group	22 hours ago	✓	Yes
☐	[redacted]	iPhone	3.0 release	[redacted]	[redacted]	QA Group	22 hours ago	✓	Yes
☐	[redacted]	iPhone	5.1.1	[redacted]	[redacted]	QA Group	22 hours ago	✓	Yes

Use the following guidelines:

- **Filter By area** - Click the button you want to view the Devices you want.
- **Quick-Links** - Allows you to quickly go to the content of that link to view and manage those details (for example, a user link will bring you to the User Details page; a device link will bring you to the Device Details page; and so on).

Table 3 provides a quick overview of what you can do using the Devices page.

Table 3 Routine Group Tasks - Groups page

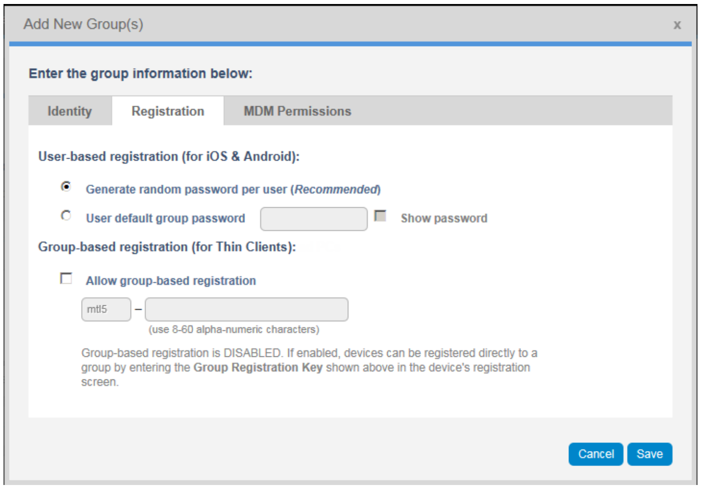
Tasks You Can Do	How	Details
Add a Device to the system.	Devices are added/registered into the management system by the user using the credentials you provided to them on the Registration tab when you added the user into the system.	See "Adding Devices" and "Adding/ Editing Users." **NOTE**: You can also click the How to Add a Device link to display the help window containing an overview of how to add devices.
View and manage Device details.	Click a Name link in the Devices page to open and use the Device Details page. **IMPORTANT**: You can also use the Devices page to select the check box next to the names of the Devices you want to manage, click a command button (for example **Query**), and then confirm. Note however, that only supported commands are performed on a device. Thus, if you select different "types" of devices (for example, iOS devices and thin clients), the unsupported command button will not be available for use on your selections (for example, **Restart** is supported with thin clients and not supported with iOS devices, and therefore, will not be available for use on your "mixed" selections). **NOTE**: You can also use the **More Actions** drop down list to perform management tasks supported on the selected devices.	See "Viewing and Managing Device Details." **NOTE**: The Device Details page allows you to: • **Query** - Send a command to the device to update its information in the system. • **Clear Passcode** - (iOS and Android Only) Removes the local passcode on the device (useful for forgotten passcodes). • **Lock** - Locks the device screen (and requires a device passcode to unlock it when a passcode is configured). • **Restart** - (Thin Client Only) Reboot the thin client.. • **Shutdown** - (Thin Client Only) Shuts down the thin client. • **Unregister** - Remove the Device from system policies and management. **TIP**: Recommended to remove users from the system as it does a clearing of only corporate assigned data from employee-owned devices. • **Delete Device** - Deletes the Device from system. Only a device that is not currently registered (does not have a Registered status) can be deleted from the system. A device must be unregistered/deactivated prior to deleting. • **Wipe** - Removes all data and applications from the Device (sets the device to factory defaults —not recommended for employee-owned devices). • **Send Message** - Sends a message (128 characters or less) to the device. • **Change Group (TC)** - (Thin Client Only) Change the Group to which the thin client belongs.

Table 3 Routine Group Tasks - Groups page , Continued

Tasks You Can Do	How	Details
View and manage Device details (continued).		• **Republish All (Android)** - (Android Only) Republishes all policies applied to selected Android devices. • **Republish (iOS)** - (iOS Only) Republishes the following policies applied to selected iOS devices: • Passcode & Restrictions • Exchange ActiveSync & Email • Wi-Fi • Web Clips • All Policies • **Check Update (Cloud Connect)** - (Cloud Connect Only) Use this action to remotely request the device to verify if a system update is available. • **Export Devices to CSV** - Use this action to generate a CSV with a list of the asset information for all the devices currently filtered on screen. • **Summary tab** - View and manage information on the Notes, Group Assignment, Alerts, and Device Configuration. • **System Info tab** - View available system information on the device (for example, Terminal Name, Serial Number, IP Address, Hardware and Software information, Installed Certificates, and so on. • **Events tab** - View and manage information on the system events pertaining to a Device (creation, device registration, and various tasks performed by the system and the Device). • **Installed Apps tab** - (Cloud Connect, iOS, and Android Only) View information on the programs and Apps installed on the device (versions, App Policies, and so on}.

Adding Devices

Devices are added/registered into the management system by the user using the credentials you provided to them on the Registration tab when you added the user into the system (see "Adding/Editing Users").



Add New Group(s)

Enter the group information below:

User-based registration (for iOS & Android):

● Generate random password per user (*Recommended*)

○ User default group password ☐ Show password

Group-based registration (for Thin Clients):

☐ Allow group-based registration

mtl5 –

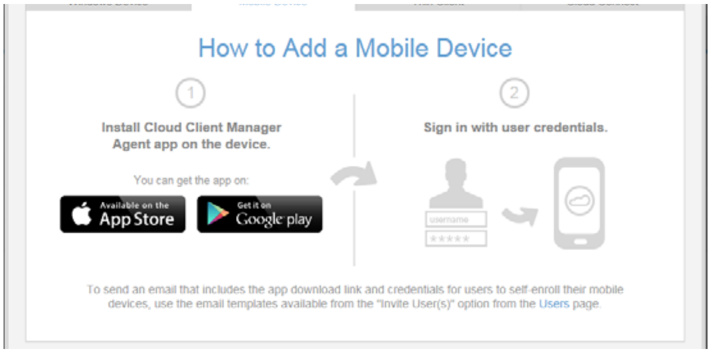
(use 8-60 alpha-numeric characters)

Group-based registration is DISABLED. If enabled, devices can be registered directly to a group by entering the **Group Registration Key** shown above in the device's registration screen.

Users must enter the credentials into the management software installed on their device and register into the management system from their device. Once their device is registered into the management console, their device and other information appears on the Devices page (and other relevant console pages).

NOTE: You can also click the How to Add a Device link to display the help window containing an overview of how to add devices:

- Adding a Mobile Device



How to Add a Mobile Device

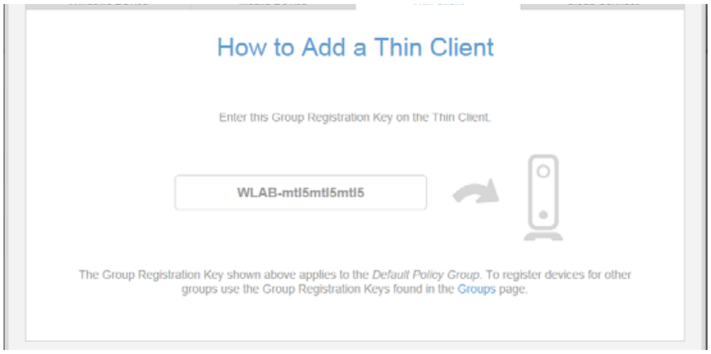
1 Install Cloud Client Manager Agent app on the device.

You can get the app on:

2 Sign in with user credentials.

To send an email that includes the app download link and credentials for users to self-enroll their mobile devices, use the email templates available from the "Invite User(s)" option from the Users page.

- Adding a Thin Client



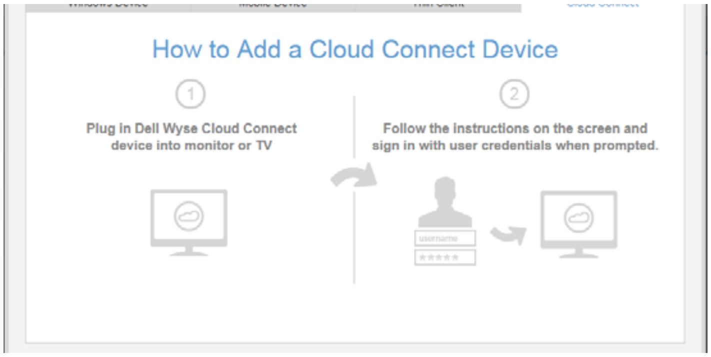
How to Add a Thin Client

Enter this Group Registration Key on the Thin Client.

WLAB-mtl5mtl5mtl5

The Group Registration Key shown above applies to the *Default Policy Group*. To register devices for other groups use the Group Registration Keys found in the Groups page.

- Adding a Cloud Connect Device



How to Add a Cloud Connect Device

1 Plug in Dell Wyse Cloud Connect device into monitor or TV

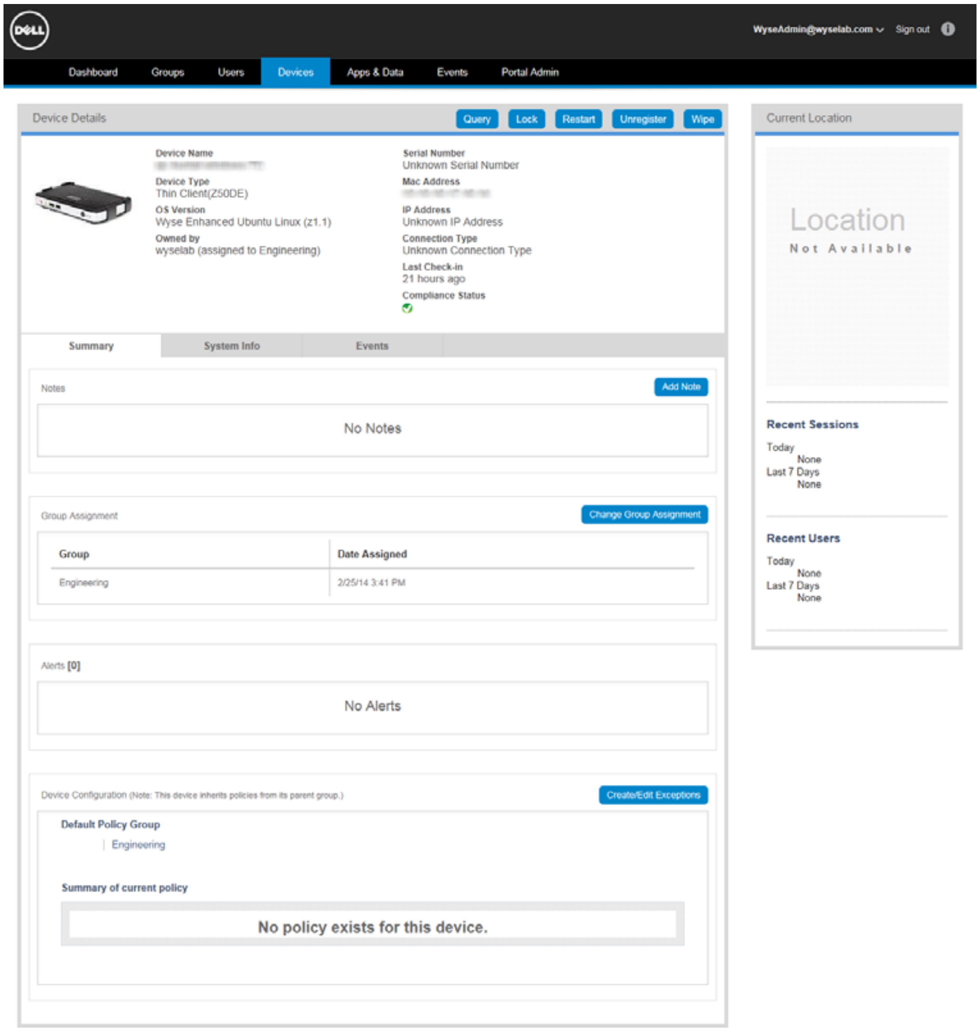
2 Follow the instructions on the screen and sign in with user credentials when prompted.

Viewing and Managing Device Details

To view and manage Device details:
On the Devices page, click a **Name** link to open the Device Details page and then perform your tasks.

Detailed guidelines:

1. On the Devices page, click a **Name** link to open the Device Details page for your device.
   Example: Thin Client



Device Details

Device Name
[redacted]
Device Type
Thin Client(Z50DE)
OS Version
Wyse Enhanced Ubuntu Linux (z1.1)
Owned by
wyselab (assigned to Engineering)

Serial Number
Unknown Serial Number
Mac Address
[redacted]
IP Address
Unknown IP Address
Connection Type
Unknown Connection Type
Last Check-in
21 hours ago
Compliance Status
✓

Notes

No Notes

Group Assignment

Group	Date Assigned
Engineering	2/25/14 3:41 PM

Alerts [0]

No Alerts

Device Configuration (Note: This device inherits policies from its parent group.)

Default Policy Group
Engineering

Summary of current policy

No policy exists for this device.

Current Location

Location
Not Available

Recent Sessions
Today
None
Last 7 Days
None

Recent Users
Today
None
Last 7 Days
None

2. Use the following guidelines:
   - **Query** - Use the Query button to send a command to the device asking it to update its information in the system.
   - **Clear Passcode** - (iOS and Android Only) Use the Clear Passcode button to remove the local passcode on the device (useful for forgotten passcodes).
     NOTE: If a Passcode policy is applied to the device, the user will be immediately requested to configure a new device passcode.
   - **Lock** - Use the Lock button to lock the device screen (requires a device passcode to unlock it when a passcode is configured).
   - **Restart** - (Thin Client Only) Use the Restart button to reboot the thin client.
   - **Shutdown** - (Thin Client Only) Use the Shutdown button to shut down the thin client.

- **Unregister** - Use the Unregister button to remove the Device from system policies and management. **TIP**: Recommended to remove users from the system as it does a clearing of only corporate assigned data from employee-owned devices.
- **Delete Device** - Use the Unregister button to delete the Device from system. Only a device that is not currently registered (does not have a Registered status) can be deleted from the system. A device must be unregistered/deactivated prior to deleting.
- **Wipe** - Use the Wipe button to remove all data and applications from the Device (sets the device to factory defaults —not recommended for employee-owned devices).
- **Send Message** - Use the Send Message button to send a message (128 characters or less) to the device.
- **Republish All (Android)** - (Android Only) Use this action to republish all policies applied to selected Android devices.
- **Republish (iOS)** - (iOS Only) Use this action to republish the following policies applied to selected iOS devices:
  Passcode & Restrictions
  Exchange ActiveSync & Email
  Wi-Fi
  Web Clips
  All Policies
- **Check Update** - (Cloud Connect Only) Use this action to remotely request the device to verify if a system update is available.
- **Export Devices to CSV** - Use this action to generate a CSV with a list of the asset information for all the devices currently filtered on screen.
- **Summary tab** - Use the Summary tab to view and manage information on the Notes, Group Assignment, Alerts, and Device Configuration.
  For information on **Create/Edit Exceptions**, see "Device Level Exceptions."
  For information on device/asset details (clicking the Device Asset link), see "Viewing and Managing Device Details."
  Change Group Assignment - (Thin Client Only) Use the Change Group Assignment button (in Group Assignment area) to change the Group to which the Thin Client belongs.
- **System Info** - Use the System Info tab to view available system information on the device (for example, Terminal Name, Serial Number, IP Address, Hardware and Software information, Installed Certificates, and so on.
- **Events tab** - Use the Events tab to view and manage information on the system events pertaining to a Device (creation, device registration, and various tasks performed by the system and the Device).
- **Installed Apps tab** - (Cloud Connect, iOS, and Android Only) Use the Installed Apps tab to view information on the programs and Apps installed on the device (versions, App Policies, and so on).

This page intentionally blank.

7 Apps & Data

(Dell Management Console Pro Version Only) This section describes how to perform routine device Application (Inventory and Policies) and File Repository Inventory management tasks using the management console.

Topics include:

- "Managing Application Inventory and Application Policies"
  - "Adding Applications to the System Inventory (Google Play or Apple App Store)"
  - "Adding Applications to the System Inventory (Enterprise Store)"
  - "Configuring Application Policies"
- "Managing File Repository Inventory"
  - "Adding/Editing Files to the File Repository Inventory"

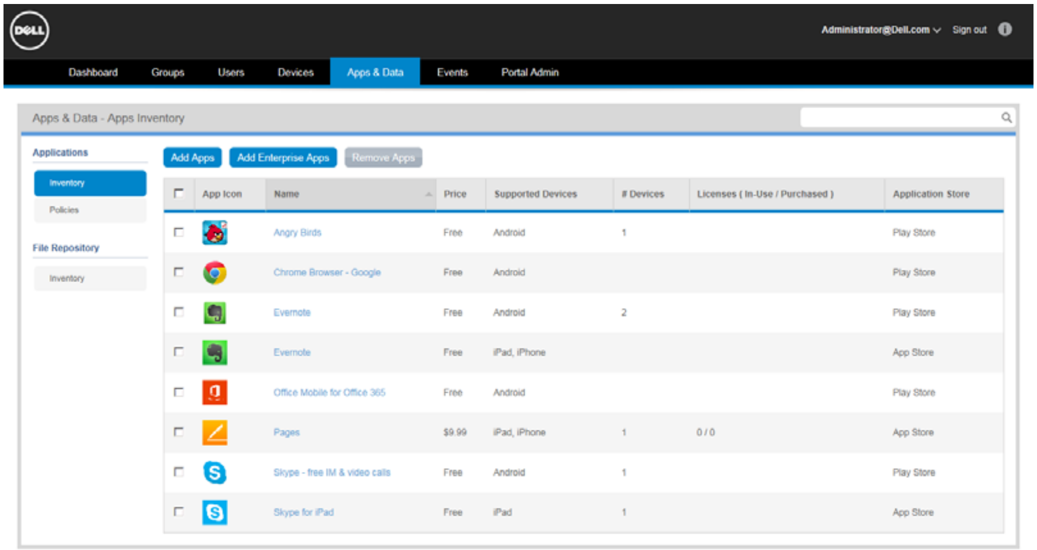
IMPORTANT NOTES:

- **Application Policies are Global and per Group**: Application policies are currently assigned at the Global and Group levels (however, in subsequent management console releases they will be manageable at the other User and Device levels as well). However, note that Default Policy Group is considered a stand-alone policy group for Application Policies. Therefore, assigning an application policy at the Default Policy Group will only apply to Mobile Users assigned directly to this group. To assign to all groups, all groups must be selected when configuring the policy.
- **iOS Requirements**:
  - Devices must have access to the Apple App Store (that is, no MDM restriction to prevent installation of applications) for non-customized applications.
  - To push applications from the App Store, the user must enter their Apple iTunes account information before the application will be installed.
  - To push paid iOS applications, the apps must have been purchased by the enterprise via the Apple Volume Purchasing Program (VPP).
- **Android Requirements**:
  - Devices must have access to Google Play for non-customized applications.
  - To install applications from Google Play, the user must have a Google account configured on the device.
  - To install paid applications, the user must enter their own payment information from the device.

Managing Application Inventory and Application Policies

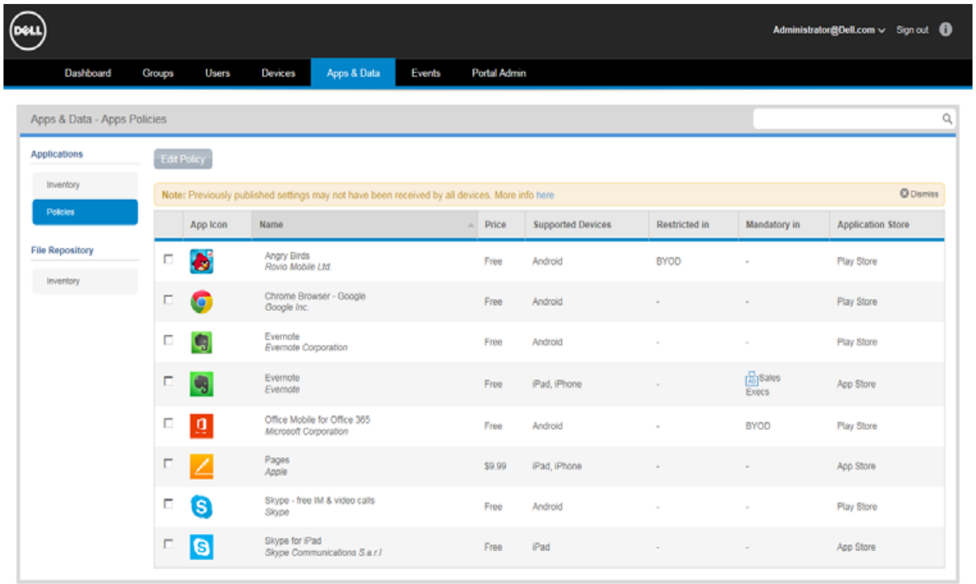
The Application Inventory page (**Apps & Data > Applications Inventory**) and the Application Policies page (**Apps & Data > Applications Policies**) allows you to quickly view and manage the device Application Inventory and Policies that are available (see Table 4).

NOTE: Managing application policies is a two-step process: First, the application must be added to the application inventory. Second, policies must be applied to applications within the inventory.



Apps & Data - Apps Inventory

□	App Icon	Name	Price	Supported Devices	# Devices	Licenses (In-Use / Purchased)	Application Store
□		Angry Birds	Free	Android	1		Play Store
□		Chrome Browser - Google	Free	Android			Play Store
□		Evernote	Free	Android	2		Play Store
□		Evernote	Free	iPad, iPhone			App Store
□		Office Mobile for Office 365	Free	Android			Play Store
□		Pages	$9.99	iPad, iPhone	1	0 / 0	App Store
□		Skype - free IM & video calls	Free	Android	1		Play Store
□		Skype for iPad	Free	iPad	1		App Store



Apps & Data - Apps Policies

Note: Previously published settings may not have been received by all devices. More info here

	App Icon	Name	Price	Supported Devices	Restricted in	Mandatory in	Application Store
□		Angry Birds *Rovio Mobile Ltd.*	Free	Android	BYOD	-	Play Store
□		Chrome Browser - Google *Google Inc.*	Free	Android	-	-	Play Store
□		Evernote *Evernote Corporation*	Free	Android	-	-	Play Store
□		Evernote *Evernote*	Free	iPad, iPhone	-	Sales Execs	App Store
□		Office Mobile for Office 365 *Microsoft Corporation*	Free	Android	-	BYOD	Play Store
□		Pages *Apple*	$9.99	iPad, iPhone	-	-	App Store
□		Skype - free IM & video calls *Skype*	Free	Android	-	-	Play Store
□		Skype for iPad *Skype Communications S.a.r.l*	Free	iPad	-	-	App Store

Table 4 provides a quick overview of what you can do using the Application Inventory page and the Application Policies page.

Table 4 Routine Application and Application Policy Tasks

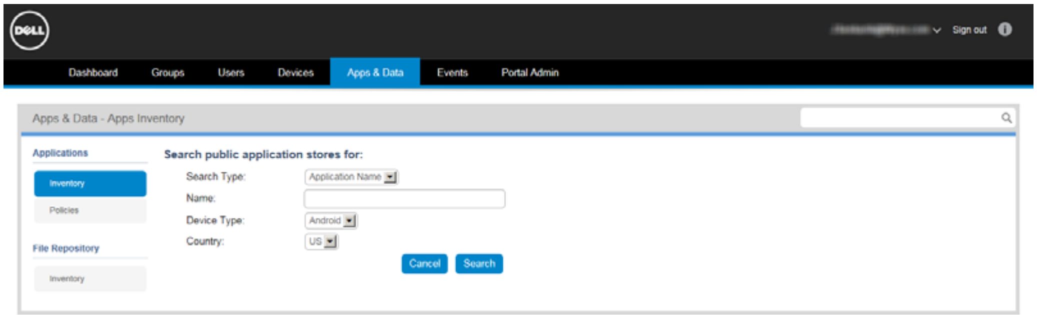
Tasks You Can Do	How	Details
Add an Application to the system inventory.	On the Application Inventory page (**Apps & Data > Applications Inventory**), click the **Add Apps** button to open and use the Application Inventory page, or click the **Add Enterprise Apps** to open and use the Add Enterprise App wizard.	For Applications from the Google Play Store or the Apple App Store, see "Adding Applications to the System Inventory (Google Play or Apple App Store)." For Applications from your Enterprise Store, see "Adding Applications to the System Inventory (Enterprise Store)."
View Application details	On the Application Inventory page (**Apps & Data > Applications Inventory**), click the Name link of the App you want to open and view the Application Detail page.	**NOTE**: You can view Application Name, Version, Application ID, Price, Supported Devices, and Bundle ID. For Enterprise Apps, you can also view the File Name (for example TanalyticsBeta1v21.ipa) or URL (for example, https://myserver/myapp.plist).
Configure an Application Policy in the system.	On the Application Policies page (**Apps & Data > Applications Policies**), scroll or page to the application you want to manage, select the option you want (Not Managed, Restricted, or Mandatory), and then click **Save & Publish**.	See "Configuring Application Policies." **NOTE**: The Application Policies page allows you to manage the following: • **Not Managed** - Simply keep the application in your application inventory (you can configure the policies you want to apply for application use at a later time). • **Restricted** - Application is restricted from installation and use. If this application is detected on a device, an Alert will be raised and the device will be flagged as Non Compliant. • **Mandatory** - Application is forced onto all supported devices that are registered and compliant. **Extra Options** - (iOS Only) Mandatory applications also allow you to select extra options (Remove When Unmanaged and Allow Data Backup) for further configuration.
Delete an Application from the system.	On the Application Inventory page (**Apps & Data > Applications Inventory**), select the check box next to the application you want to delete, click the **Remove Apps** button, and confirm the deletion. The Application is deleted and is no longer shown in the list of available applications on the Application Inventory page.	**IMPORTANT**: Only applications that are Not Managed can be deleted.

Adding Applications to the System Inventory (Google Play or Apple App Store)

To add an Application:
On the Application Inventory page (**Apps & Data > Applications Inventory**), click the **Add Apps** button to open and use the Application Inventory page.

Detailed guidelines:

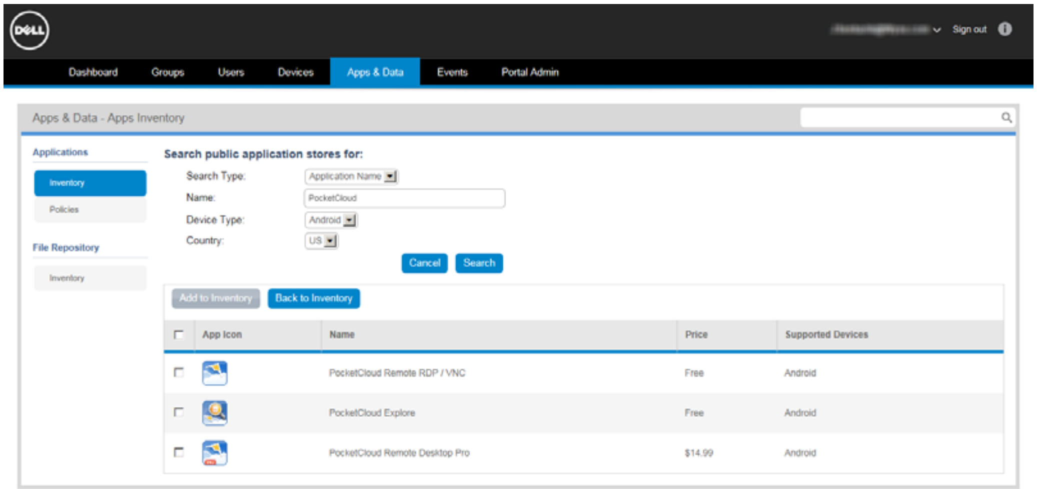
1. On the Application Inventory page (**Apps & Data > Applications Inventory**), click the **Add Apps** button to open the Application Inventory page.



Search public application stores for:

Search Type: Application Name
Name:
Device Type: Android
Country: US

2. Use the following guidelines:
   - **Search Type** - Enter the type of name search you want to perform (Application Name or Developer Name) to find the application you want to obtain.
   - **Name** - Enter the name of the application you want to obtain.
   - **Device Type** - Select the type of device you have (Android, iPad, or iPhone) to go to the application store that supports the device (Google Play or Apple App Store).
   - **Country** - Select the name of the country to which the application belongs for use.
3. Click **Search** to search the application store that supports the Device Type you selected.
   NOTE: If you selected either iPad or iPhone in Device Type, the Supported Devices column of the search results table will display if the application is supported for both iPad and iPhone devices.



Search public application stores for:

Search Type: Application Name
Name: PocketCloud
Device Type: Android
Country: US

□	App Icon	Name	Price	Supported Devices
□		PocketCloud Remote RDP / VNC	Free	Android
□		PocketCloud Explore	Free	Android
□		PocketCloud Remote Desktop Pro	$14.99	Android

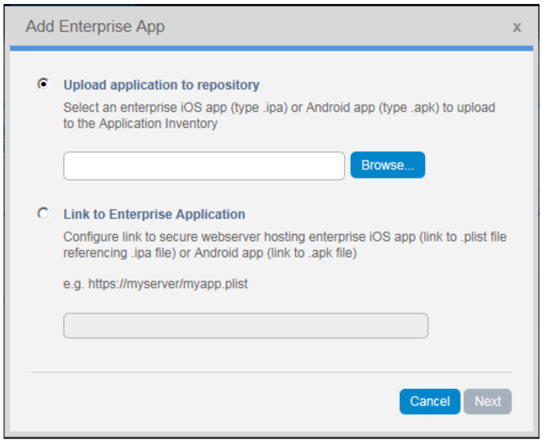
4. On the Results page, select the application you want, and then click the **Add to Inventory** button. The Application will appear on the Application Inventory page (**Apps & Data > Applications Inventory** or simply click the **Back to Inventory** button) and is now ready for you to configure the policies you want to apply for application use (see "Configuring Application Policies").

Adding Applications to the System Inventory (Enterprise Store)

To add an Application:
On the Application Inventory page (**Apps & Data > Applications Inventory**), click the **Add Enterprise Apps** button to open and use the Add Enterprise App wizard.

Detailed guidelines:

1. On the Application Inventory page (**Apps & Data > Applications Inventory**), click the **Add Enterprise Apps** button to open the Add Enterprise App wizard.



Add Enterprise App

● Upload application to repository

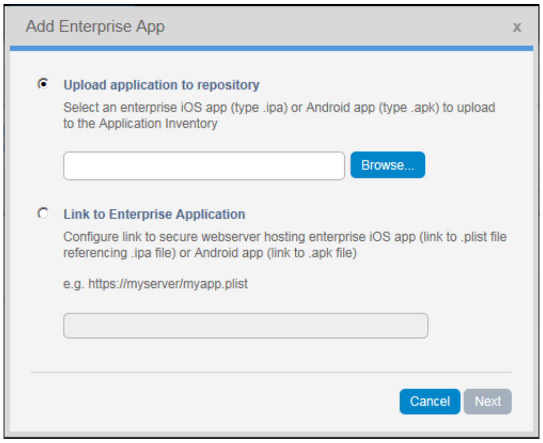
Select an enterprise iOS app (type .ipa) or Android app (type .apk) to upload to the Application Inventory

○ Link to Enterprise Application

Configure link to secure webserver hosting enterprise iOS app (link to .plist file referencing .ipa file) or Android app (link to .apk file)

e.g. https://myserver/myapp.plist

2. Use the following guidelines:
   - **Upload Application to Repository** - Use the Browse button to select an enterprise iOS app (type .ipa) or Android app (type .apk) to upload to the Application Inventory, click **Next**, and then follow the wizard to enter the App Icon.



Add Enterprise App

● Upload application to repository

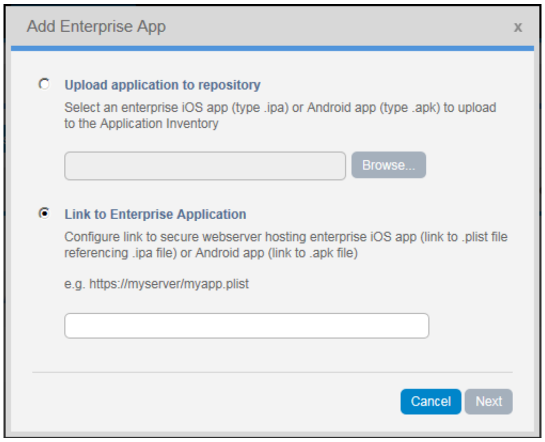
Select an enterprise iOS app (type .ipa) or Android app (type .apk) to upload to the Application Inventory

○ Link to Enterprise Application

Configure link to secure webserver hosting enterprise iOS app (link to .plist file referencing .ipa file) or Android app (link to .apk file)

e.g. https://myserver/myapp.plist

   - **Link to Enterprise Application** - Enter the link to the secure Web server hosting your enterprise iOS app (link to .plist file referencing .ipa file) or Android app (link to .apk file), click **Next**, and then follow the wizard to enter the App Name, App ID, Version, Supported Devices, and App Icon.



Add Enterprise App

○ **Upload application to repository**

Select an enterprise iOS app (type .ipa) or Android app (type .apk) to upload to the Application Inventory

● **Link to Enterprise Application**

Configure link to secure webserver hosting enterprise iOS app (link to .plist file referencing .ipa file) or Android app (link to .apk file)

e.g. https://myserver/myapp.plist

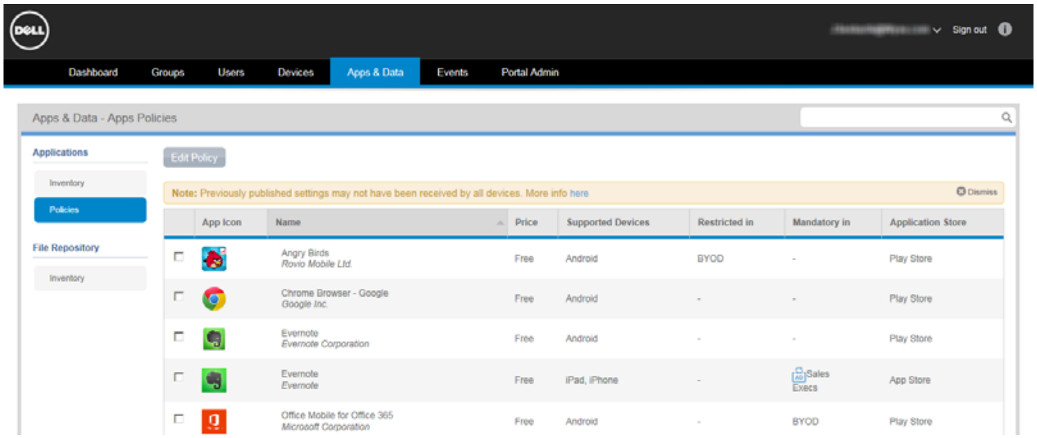
3. After clicking **Save**, the Application will appear on the Application Inventory page (**Apps & Data > Applications Inventory** or simply click the **Back to Inventory** button) and is now ready for you to configure the policies you want to apply for application use (see "Configuring Application Policies").

Configuring Application Policies

To configure the usage of an Application:
On the Application Policies page (**Apps & Data > Applications Policies**), scroll or page to the application you want to manage, select the option you want (Not Managed, Restricted, or Mandatory), and then click **Save & Publish**.

Detailed guidelines:

1. On the Application Policies page (**Apps & Data > Applications Policies**), scroll or page to the application you want to manage.

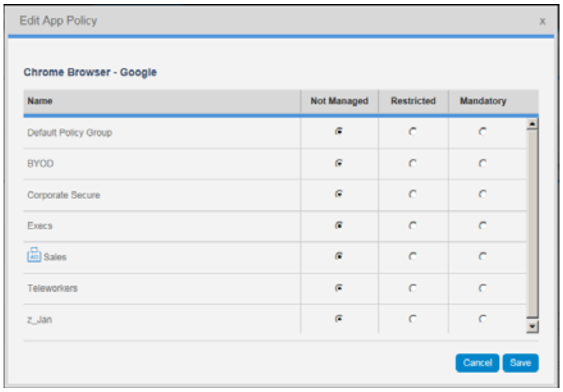


Apps & Data - Apps Policies

Note: Previously published settings may not have been received by all devices. More info here

	App Icon	Name	Price	Supported Devices	Restricted in	Mandatory in	Application Store
□		Angry Birds *Rovio Mobile Ltd.*	Free	Android	BYOD	-	Play Store
□		Chrome Browser - Google *Google Inc.*	Free	Android	-	-	Play Store
□		Evernote *Evernote Corporation*	Free	Android	-	-	Play Store
□		Evernote *Evernote*	Free	iPad, iPhone	-	Sales Execs	App Store
□		Office Mobile for Office 365 *Microsoft Corporation*	Free	Android	-	BYOD	Play Store

2. Select the check box next to the App you want to edit, and click **Edit Policy** to open the Edit App Policy page.



Edit App Policy

Chrome Browser - Google

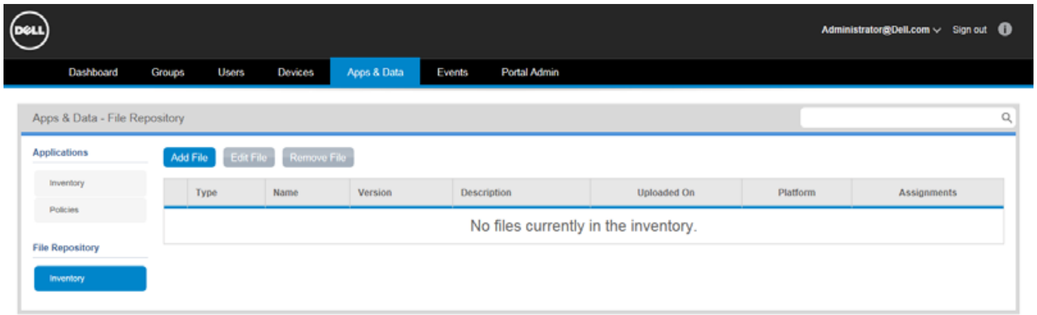
Name	Not Managed	Restricted	Mandatory
Default Policy Group	●	○	○
BYOD	●	○	○
Corporate Secure	●	○	○
Execs	●	○	○
Sales	●	○	○
Teleworkers	●	○	○
z_Jan	●	○	○

3. Use the following guidelines:
   - **Not Managed** - Select if you want the application to simply remain in your application inventory (you can configure the policies you want to apply for application use at a later time).
   - **Restricted** - Select if you want the application to be restricted from installation and use. If this application is detected on a device, an Alert will be raised and the device will be flagged as Non Compliant.
   - **Mandatory** - Select if you want the application to be forced onto all supported devices that are registered and compliant.
     Extra Options - (iOS Only) Mandatory applications also allow you to select extra options (Remove When Unmanaged and Allow Data Backup) for further configuration.
     IMPORTANT: The Mandatory option will install the App, regardless of the install App options on the Dell Wyse Cloud Connect device.

4. Click **Save** to enforce your inventory policies.

Managing File Repository Inventory

The File Repository Inventory page (**Apps & Data > File Repository Inventory**) allows you to quickly view and manage the File Repository Inventory (thin client firmware and certificate files) that are available (see Table 4).



Type	Name	Version	Description	Uploaded On	Platform	Assignments

No files currently in the inventory.

Table 5 provides a quick overview of what you can do using the File Repository Inventory page.

Table 5 Routine File Repository Inventory Tasks

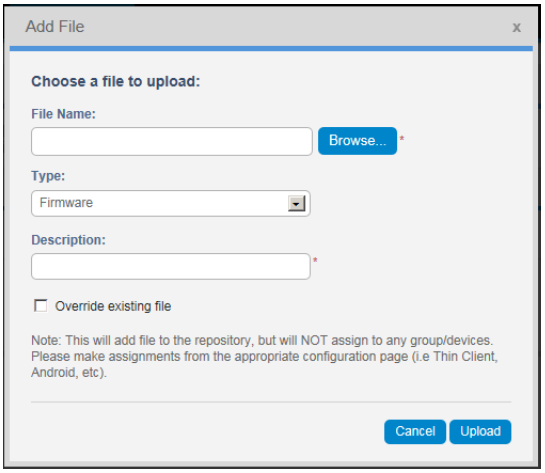
Tasks You Can Do	How	Details
Add a file to the File Repository inventory.	On the File Repository Inventory page (**Apps & Data > File Repository Inventory**), click the **Add File** button to open and use the Add File page.	See "Adding/Editing Files to the File Repository Inventory."
Edit a file in the File Repository.	On the File Repository Inventory page (**Apps & Data > File Repository Inventory**), select the check box next to the file you want to edit, click **Edit File**, and then make your changes.	Use same guidelines in "Adding/ Editing Files to the File Repository Inventory."
Delete a file from the File Repository.	On the File Repository Inventory page (**Apps & Data > File Repository Inventory**), select the check box next to the application you want to delete, click the **Remove File** button, and confirm the deletion. The file is deleted and is no longer shown in the list of available files on the File Repository Inventory page.	**IMPORTANT**: Only files that are Not Assigned to a policy group or a device can be deleted.

Adding/Editing Files to the File Repository Inventory

To add a file:
On the File Repository Inventory page (**Apps & Data > File Repository Inventory**), click the **Add File** button to open and use the File Repository Inventory page.

Detailed guidelines:

1. On the File Repository Inventory page (**Apps & Data > File Repository Inventory**), click the **Add File** button to open the File Repository Inventory page.



Note: This will add file to the repository, but will NOT assign to any group/devices. Please make assignments from the appropriate configuration page (i.e Thin Client, Android, etc).

2. Use the following guidelines:
   - **Browse** - Use the Browse button to find and select the file you want to upload to the File Repository Inventory.
   - **Type** - Select the type of file you have (Firmware, Certificate, Wallpaper, Logo, EULA Text File).
     NOTES:
     Logo (for use on Login dialog box) supports ico, bmp, jpg, gif formats; recommended size is 100H x 360W pixels.
     EULA/licensing file (for use at log-in) supports plain text only; limited to 100 KB size.
   - **Description** - Enter the description of the file you want to use.
   - **Override Existing File** - Select the Override Existing File check box if you want the file to override the existing file of the same name.

3. Click **Upload** to upload the file to the File Repository Inventory page.
   NOTE: This will add a file to the repository, but will not assign it to any group or devices. For ThinOS firmware images, the file version and platform will be automatically detected.

4. You can assign files to policy groups or to devices from either the Groups page (Android for Dell Wyse Cloud Connect or ThinOS/Xenith for thin client) or from the Device Details page by assigning an exception at the device level. For details, see Dell Wyse Cloud Connect policy-based certificate installation in "Details: Android Policy Settings" and policy-based firmware deployment in "Details: Thin Client Policy Settings." Note that the policy assignments can be reviewed from the File Repository Inventory page. The number of policy groups and devices (device-level exceptions) that each file has been assigned to is displayed in the assignments column. By hovering over the number next to Groups or Devices you can display the names of the policy groups and devices.

This page intentionally blank.

8 Events

This section describes how to display all events and alerts in the management system using the management console. It also provides instructions on displaying an Audit of the events and alerts for system auditing purposes.

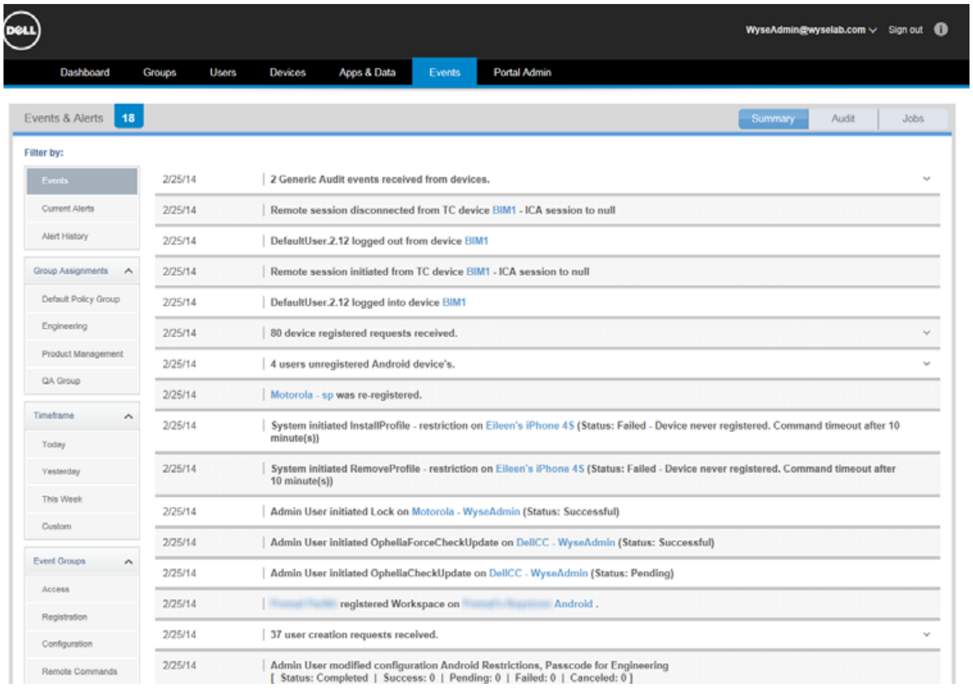
TIP: Use the Summary of Events and Alerts page to obtain an easy-to-read daily summary of what has happened in system.
Use the Audit page to format the information into a typical audit log-view, where one line is displayed for each event in the order of time.

Topics include:

- "Displaying a Summary of Events"
- "Displaying an Audit of Events"
- "Displaying the Jobs of Events"

Displaying a Summary of Events

The Summary of Events and Alerts page (**Events > Summary**) allows you to quickly display all of the events and alerts that have taken place in the system.



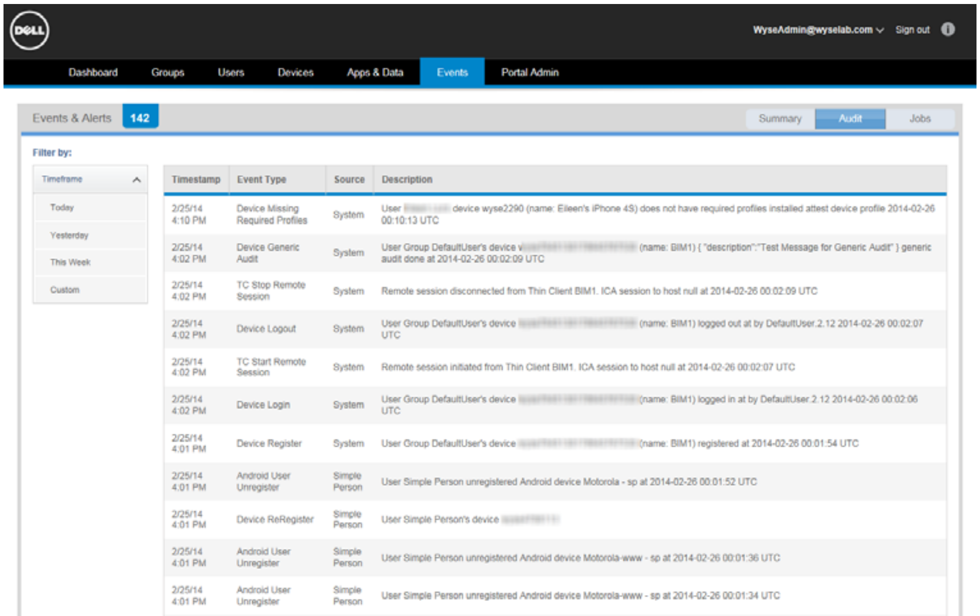
2/25/14	2 Generic Audit events received from devices.
2/25/14	Remote session disconnected from TC device BIM1 - ICA session to null
2/25/14	DefaultUser.2.12 logged out from device BIM1
2/25/14	Remote session initiated from TC device BIM1 - ICA session to null
2/25/14	DefaultUser.2.12 logged into device BIM1
2/25/14	80 device registered requests received.
2/25/14	4 users unregistered Android device's.
2/25/14	Motorola - sp was re-registered.
2/25/14	System initiated InstallProfile - restriction on Eileen's iPhone 4S (Status: Failed - Device never registered. Command timeout after 10 minute(s))
2/25/14	System initiated RemoveProfile - restriction on Eileen's iPhone 4S (Status: Failed - Device never registered. Command timeout after 10 minute(s))
2/25/14	Admin User initiated Lock on Motorola - WyseAdmin (Status: Successful)
2/25/14	Admin User initiated OpheliaForceCheckUpdate on DellCC - WyseAdmin (Status: Successful)
2/25/14	Admin User initiated OpheliaCheckUpdate on DellCC - WyseAdmin (Status: Pending)
2/25/14	[redacted] registered Workspace on [redacted] Android .
2/25/14	37 user creation requests received.
2/25/14	Admin User modified configuration Android Restrictions, Passcode for Engineering [Status: Completed | Success: 0 | Pending: 0 | Failed: 0 | Canceled: 0]

Although the Summary of Events and Alerts page shows you all of the events and alerts that have taken place in the system, you can use the following guidelines to view the information you want:

- **Filter By area** - Click the button you want to view the Events you want.
- **Quick-Links** - Allows you to quickly go to the content of that link to view and manage those details (for example, a user link will bring you to the User Details page; a device link will bring you to the Device Details page; and so on).

Displaying an Audit of Events

The Audit page (**Events > Audit**) allows you to quickly format the information into a typical audit log-view, where one line is displayed for each event in the order of time.



Timestamp	Event Type	Source	Description
2/25/14 4:10 PM	Device Missing Required Profiles	System	User [redacted] device wyse2290 (name: Eileen's iPhone 4S) does not have required profiles installed attest device profile 2014-02-26 00:10:13 UTC
2/25/14 4:02 PM	Device Generic Audit	System	User Group DefaultUser's device v[redacted] (name: BIM1) { "description":"Test Message for Generic Audit" } generic audit done at 2014-02-26 00:02:09 UTC
2/25/14 4:02 PM	TC Stop Remote Session	System	Remote session disconnected from Thin Client BIM1. ICA session to host null at 2014-02-26 00:02:09 UTC
2/25/14 4:02 PM	Device Logout	System	User Group DefaultUser's device [redacted] (name: BIM1) logged out at by DefaultUser.2.12 2014-02-26 00:02:07 UTC
2/25/14 4:02 PM	TC Start Remote Session	System	Remote session initiated from Thin Client BIM1. ICA session to host null at 2014-02-26 00:02:07 UTC
2/25/14 4:02 PM	Device Login	System	User Group DefaultUser's device [redacted](name: BIM1) logged in at by DefaultUser.2.12 2014-02-26 00:02:06 UTC
2/25/14 4:01 PM	Device Register	System	User Group DefaultUser's device [redacted](name: BIM1) registered at 2014-02-26 00:01:54 UTC
2/25/14 4:01 PM	Android User Unregister	Simple Person	User Simple Person unregistered Android device Motorola - sp at 2014-02-26 00:01:52 UTC
2/25/14 4:01 PM	Device ReRegister	Simple Person	User Simple Person's device [redacted]
2/25/14 4:01 PM	Android User Unregister	Simple Person	User Simple Person unregistered Android device Motorola-www - sp at 2014-02-26 00:01:36 UTC
2/25/14 4:01 PM	Android User Unregister	Simple Person	User Simple Person unregistered Android device Motorola-www - sp at 2014-02-26 00:01:34 UTC

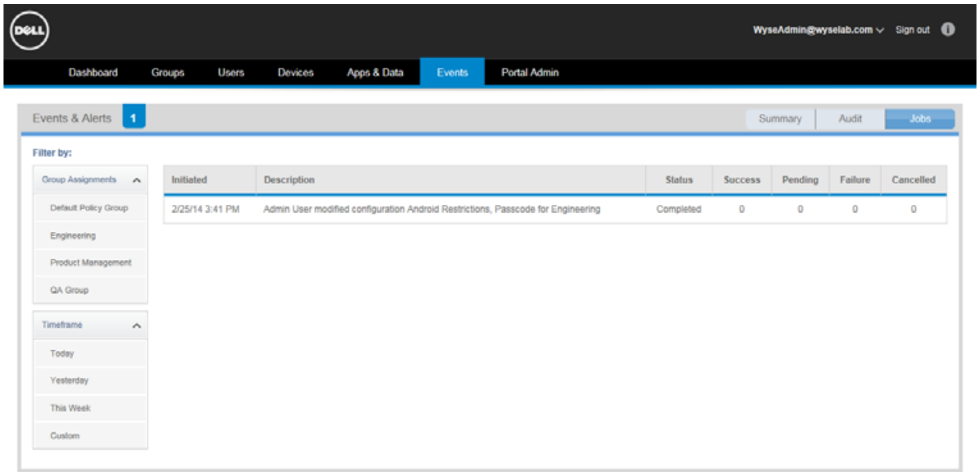
Although the Audit page shows you all of the events and alerts that have taken place in the system, you can use the following guidelines to view the information you want:

- **Filter By area** - Click the button you want to view the Events you want.

Displaying the Jobs of Events

The Jobs page (**Events > Jobs**) allows you to quickly display details (status, success, pending, failure, cancelled) of initiated jobs that have taken place in the system. Jobs are only created for group policy changes at the Group level and for application policies (since these are always at Group level). Jobs do not apply for user or device exceptions.
TIP: See "Managing Groups and Group Policies" and "Managing Application Inventory and Application Policies."

NOTE: Jobs will also appear in the Dashboard page (within Events) and in the Groups page for any job that is still ongoing (or if any action failed).



Initiated	Description	Status	Success	Pending	Failure	Cancelled
2/25/14 3:41 PM	Admin User modified configuration Android Restrictions, Passcode for Engineering	Completed	0	0	0	0

Although the Jobs page shows you details of initiated jobs of all events that have taken place in the system, you can use the following guidelines to view the information you want:

- **Filter By area** - Click the button you want to view the Events you want.

NOTE: For policy or application policy changes at the Group level, the change will create a corresponding Job that will track the status for all devices affected by change: Success, Pending, Failure, Cancelled. For a non-success status (Pending, Failure, Cancelled), you can also click the link to view more details regarding the Job.

This page intentionally blank.

9 Portal Administration

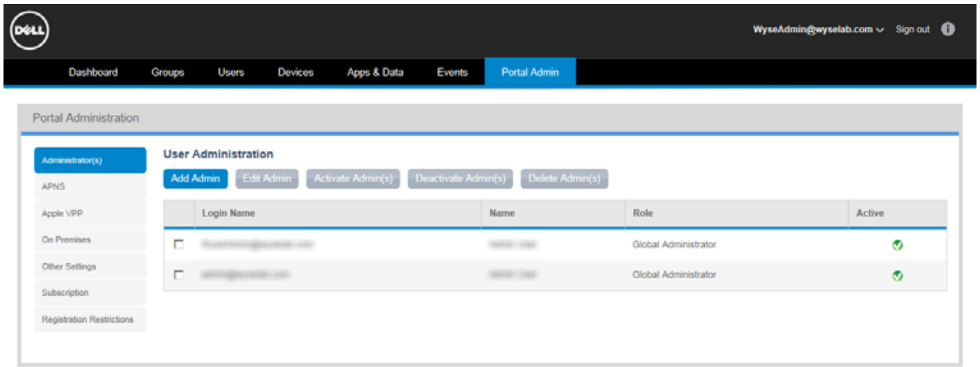
This section contains a brief overview of your system administration tasks that are required to set up and maintain your system.

Topics include:

- "Managing Administrators and Viewers of the Management Console"
  - "Adding Administrators and Viewers"
- "Generating an APNs Certificate (iOS Only)"
- "Viewing and Managing Your Apple VPP Subscriptions"
- "On Premises Service (Single Sign-On, KACE, and Active Directory Connector)"
  - "Installing and Registering Your On Premises Service"
  - "Single Sign-On (Installing and Using)"
  - "KACE"
  - "Active Directory Connector: Importing Existing Active Directory Users into the System"
- "Other Settings: APNS Warnings, License Expiration Warnings, and Self Service Legal Agreements (Enforcing the Agreement for All Self Service Users)"
- "Viewing and Managing Your Management Console License Subscriptions"
- "Registration Restrictions (Installing and Using)"

Managing Administrators and Viewers of the Management Console

The User Administration page (**Portal Admin > Administrators**) allows you to quickly view and manage the system administrators and viewers that are available (see Table 6). **NOTE**: In general, Global Viewers have read-only access to the management console, but can also be given rights to issue any of the following Real-Time commands that you specify: Query, Lock, Clear Passcode, Unregister, Wipe, Restart.



User Administration

	Login Name	Name	Role	Active
□	[redacted]	[redacted]	Global Administrator	✓
□	[redacted]	[redacted]	Global Administrator	✓

Table 6 provides a quick overview of what you can do using the User Administration page.

Table 6 Routine System Administration Tasks - User Administration page

Tasks You Can Do	How	Details
Add an Administrator/ Viewer to the system.	Click the **Add Admin** button to open the New Admin User page, and then use the tabs to configure the settings.	"Adding Administrators and Viewers."
Edit an Administrator/ Viewer in the system.	Select the check box next to the Login Name you want in the User Administration page, click **Edit Admin** to open the Edit Admin User page, and then make your changes.	Use same guidelines in "Adding Administrators and Viewers." **TIP**: You can use the Change Login Name link to update the Login Name for administrators (**NOTE**: This option is only available for users with Administrator roles and only accessible from Portal Admin > Administrators view, not from the Users page).
Activate an Administrator/Viewer.	Select the check box next to the Login Name of an administrator not currently active (does not have an Active status) that you want in the User Administration page, and then click **Activate Admin(s)** to activate the Administrator/Viewer in the system.	**NOTE**: After activating an Administrator/Viewer, they will be able to access the system.
Deactivate an Administrator/Viewer.	Select the check box next to the Login Name of an administrator currently active (has an Active status) that you want in the User Administration page, and then click **Deactivate Admin(s)** to deactivate the Administrator/Viewer in the system.	**NOTE**: After deactivating an Administrator/Viewer, an Administrator/Viewer attempting to access the system will not be able to do so. Also note that if the Administrator/ Viewer also has a Mobile User role, any devices currently registered to them will be automatically unregistered when they are deactivated.
Delete an Administrator/Viewer.	Select the check box next to the Login Name link of an administrator not currently active (does not have an Active status) that you want in the User Administration page, and then click **Delete Admin(s)** to delete/ remove the Administrator/Viewer from the system.	**NOTE**: Only an Administrator/Viewer that is not currently active (does not have an Active status) can be deleted from the system. An Administrator/ Viewer must be deactivated prior to deleting.

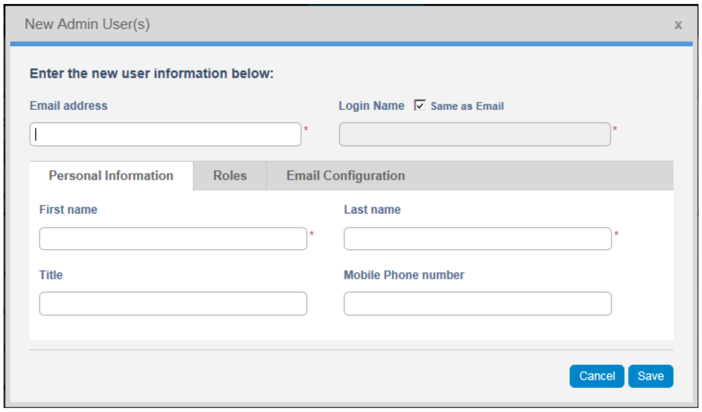
Adding Administrators and Viewers

TIP: You can also use the guidelines in this section when editing an administrator/ viewer. You can use the Change Login Name? link to update the Login Name for administrators (**NOTE**: This option is only available for users with Administrator roles and only accessible from Portal Admin > Administrators view, not from the Users page).

To add an Administrator/Viewer:
On the User Administration page, click the **Add Admin** button to open the New Admin User page, and then use the Personal Information tab, Roles tab, and Email Configuration tab, to enter the user information (passwords and so on), select the Policy Group (Group Policy) and Role (Global Administrator or Global Viewer) to which you want to assign the user, and configure email information.

Detailed guidelines:

1. On the User Administration page, click the **Add Admin** button to open the New Admin User page.



New Admin User(s)

Enter the new user information below:

Login Name ☑ Same as Email

2. Use the following tabs to configure the settings:

   Personal Information tab:

   - **Email Address**: Must be a valid email address (used for password recovery).
   - **Login Name**: The Login Name is the username used for device registration and for logging into the Self-Service portal (see "Other Settings: APNS Warnings, License Expiration Warnings, and Self Service Legal Agreements (Enforcing the Agreement for All Self Service Users)") and can be the same as the email address or customized. **CAUTION**: Once created, this Login Name cannot be modified (you must deactivate and delete the User, and then create a new User with same email address but different Login Name if desired).
   - **First Name / Last Name / Title / Mobile Phone Number**

   Roles tab:

   - **Enable Mobile User Role**: Select if you want to enable device registration and Self-Service portal access for this mobile-device User; and then select the policy group to which you want to assign the User (the mobile user role requires a policy group).
   - **Portal Administrator**: Select this option if you want to enable administration access to the system for this User (administrator access rights), and then select the role (Global Administrator or Global Viewer) to which you want to assign the User. In general, **Global Viewers** have read-only access to the management console, but can also be given rights to issue any of the following Real-Time commands that you specify: Query, Lock, Clear Passcode, Unregister, Wipe, Restart (see "Managing Administrators and Viewers of the Management Console"). Note that newly created administrators will be forced to enter a new password at their first login.

- **Password**: The password is used for device registration and is the password for logging into the Self-Service portal. Select a User-based option to either generate a random password or to enter a custom password:
  Random password: System assigns a random password for the User.
  Custom password: Manually enter the password you want (passwords must contain a minimum of 8 characters (up to a maximum of 64) including 1 upper case letter, 1 lower case letter, and 1 numerical digit). If a group password has been configured, this is the default custom password.
  TIP: Users will register their client device using the credentials you provide to them (they must enter the credentials into the management software installed on their device and register into the management system).
  CAUTION: It is highly recommended that this password be changed at first login. (see "Changing Your Password"). Newly created administrators, and any Mobile User trying to activate the Self-Service portal for first time, will be forced to enter a new password at their first login. When an administrator wants to change their password after the initial password change, the administrator must use the Forgot Password link on the Login page to change their password (you cannot change the password using the Roles tab).

Email Configuration tab:

- **Exchange/IMAP/POP**: Configure the email information you require. The Email Configuration tab is used to link user-specific account information for Exchange ActiveSync and Email policies for iOS devices. Whenever the Dynamic User Info option is selected on either an Exchange ActiveSync or Email policy, the user-specific information configured in this tab will be sent to the device to simplify configuration on the iOS device - the user will simply be prompted to enter their password to complete the configuration of their email account.
  ADMINISTRATOR NOTE: Email information is required for those administrators who also have a Mobile User role assigned (otherwise it is not really applicable to users who exclusively have a Global Administrator or Global Viewer role).

3. After configuring, click **Save**. The Administrator/Viewer is added to the list of available users on the User Administration page.

Generating an APNs Certificate (iOS Only)

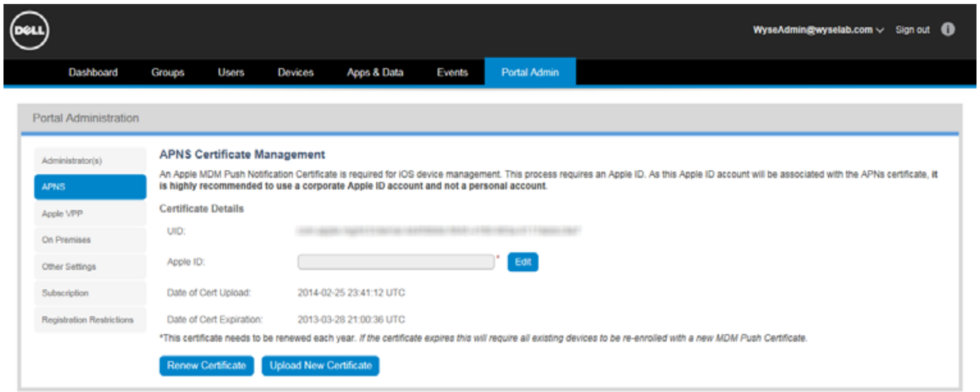
The management console integrates the Apple iOS Mobile Device Management (MDM) framework, allowing for IT Administrators to remotely manage iOS devices by leveraging the Apple Push Notification service (APNs) to securely interact with enterprise iOS devices. This process requires the enterprise to generate a certificate that is used to secure the communication link via the APNs. An Apple ID account is used to login to the Apple Push Certificates portal (https://identity.apple.com/pushcert) for management of the MDM APNs certificates. As the Apple ID account will be associated with the APNs certificate (which must be renewed annually), it is highly recommended to use a corporate Apple ID account and not a personal account.

The APNs Certificate Management page of the management console (**Portal Admin > APNs**) allows you to generate an Apple MDM Push Notification Certificate that is required for iOS device management. Simply follow the instruction on the APNs Certificate Management page and use the following guidelines:

CAUTION: If you have an existing MDM APNs certificate generated via the Apple EDP program, use the click here to upload now link at the bottom of the APNs Certificate Management page and follow the instructions.

TIP: You can also renew the certificate (click the **Renew Certificate** button and follow instructions).

1. After you click the **Generate Signed CSR File** button, you will download the .plist file to a folder on your machine (save it locally on the machine to which you are currently logged in to the management console).
2. When you login to the Apple Push Certificates portal (https://identity.apple.com/pushcert), click the **Create a Certificate** button and follow the instructions on screen, you must select the .plist file that you just downloaded (using the **Generate Signed CSR File** button in the previous step) when requested to upload the CSR file. Once this process is completed, download the certificate file (the filename will be: MDM_ Wyse Technology LLC_Certificate.pem) to a folder on your machine.
3. Click the **Upload Certificate** button to upload the MDM_ Wyse Technology LLC_Certificate.pem file you downloaded from the Apple Push Certificates portal.



APNS Certificate Management

An Apple MDM Push Notification Certificate is required for iOS device management. This process requires an Apple ID. As this Apple ID account will be associated with the APNs certificate, it **is highly recommended to use a corporate Apple ID account and not a personal account.**

Certificate Details

UID: [redacted]

Apple ID: *

Date of Cert Upload: 2014-02-25 23:41:12 UTC

Date of Cert Expiration: 2013-03-28 21:00:36 UTC

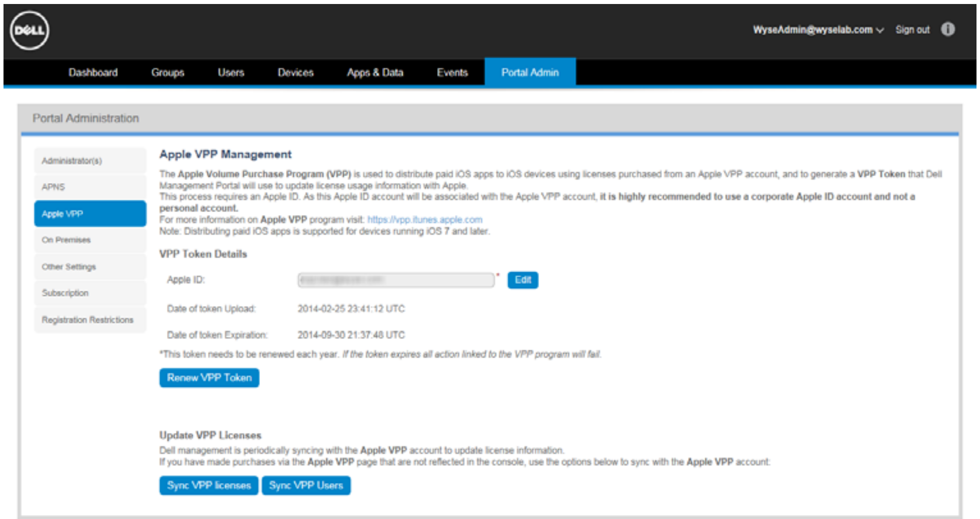
*This certificate needs to be renewed each year. *If the certificate expires this will require all existing devices to be re-enrolled with a new MDM Push Certificate.*

Viewing and Managing Your Apple VPP Subscriptions

The Apple Volume Purchase Program (VPP) is used to distribute paid iOS apps to iOS devices using licenses purchased from an Apple VPP account, and to generate a VPP Token that the management console will use to update license usage information with Apple (only supported on iOS7 and later devices).

This process requires an Apple ID. As this Apple ID account will be associated with the Apple VPP account, it is highly recommended to use a corporate Apple ID account and not a personal account. Simply click the **Upload New VPP Token** button and follow the instructions. For more information on Apple VPP program visit: https://vpp.itunes.apple.com.

NOTE: Distributing paid iOS apps is supported for devices running iOS 7 and later.



Apple VPP Management

The **Apple Volume Purchase Program (VPP)** is used to distribute paid iOS apps to iOS devices using licenses purchased from an Apple VPP account, and to generate a **VPP Token** that Dell Management Portal will use to update license usage information with Apple.
This process requires an Apple ID. As this Apple ID account will be associated with the Apple VPP account, **it is highly recommended to use a corporate Apple ID account and not a personal account.**
For more information on **Apple VPP** program visit: https://vpp.itunes.apple.com
Note: Distributing paid iOS apps is supported for devices running iOS 7 and later.

VPP Token Details

Apple ID: [redacted] *

Date of token Upload: 2014-02-25 23:41:12 UTC

Date of token Expiration: 2014-09-30 21:37:48 UTC

*This token needs to be renewed each year. *If the token expires all action linked to the VPP program will fail.*

Update VPP Licenses

Dell management is periodically syncing with the **Apple VPP** account to update license information.
If you have made purchases via the **Apple VPP** page that are not reflected in the console, use the options below to sync with the **Apple VPP** account:

On Premises Service (Single Sign-On, KACE, and Active Directory Connector)

The Dell On-Premises Gateway is an application that can be installed on-premises as an extension to the management console functionality provided in the cloud. By installing and configuring the gateway, the following features can be enabled:

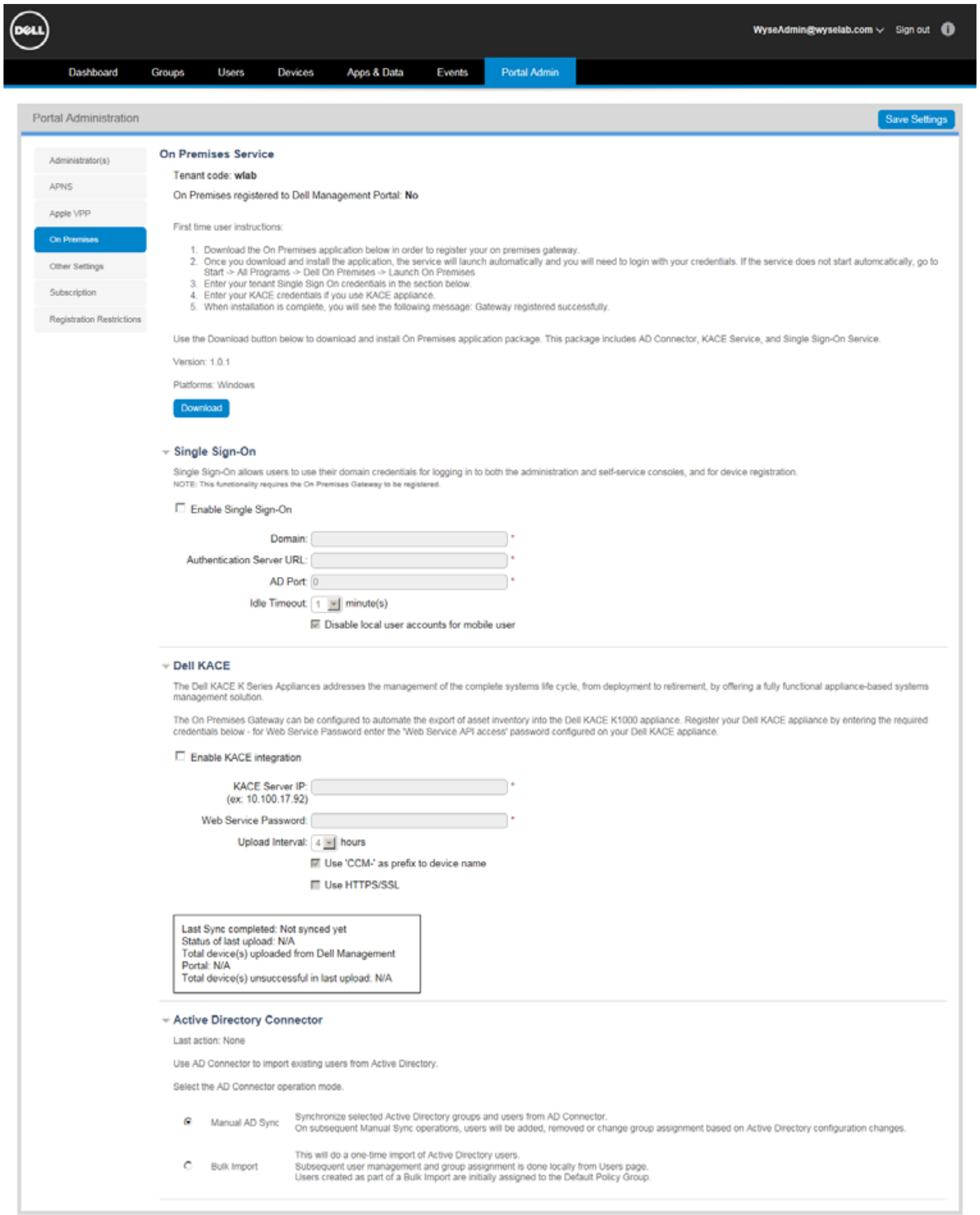
- Single Sign-On: Support for Single Sign-On for management console authentication (Admin and Self-Service views) and for mobile device registration. Management console administrators and mobile administrator users can now use domain credentials instead of local management console credentials for these functions (see "Single Sign-On (Installing and Using)").
- Dell Kace K1000 Integration: Ability to automate export of asset inventory into the Dell Kace K1000 appliance (see "KACE").
- Active Directory Connector: The AD Connector is now bundled with the On-Premises Gateway installer. This allows for bulk import and manual sync for AD Groups and Users with the Dell Management Console (see "Active Directory Connector: Importing Existing Active Directory Users into the System").

Installing and Registering Your On Premises Service

First time user instructions:

1. Download and install the Dell On-Premises Gateway application.
2. Once you download and install the application, the service will launch automatically, and you will need to login with your credentials. If the service does not start automatically, go to **Start > All Programs > On Premises > Launch On Premises**.
3. Enter your tenant Single Sign On credentials in the appropriate section.
4. Enter your KACE credentials if you use KACE appliance.
5. When installation is complete, you will see the following message: Gateway registered successfully.

Use the **Download** button to download and install On Premises application package. This package includes the AD Connector, KACE Service, and Single Sign On Service.



On Premises Service

Tenant code: **wlab**

On Premises registered to Dell Management Portal: **No**

First time user instructions:

1. Download the On Premises application below in order to register your on premises gateway.
2. Once you download and install the application, the service will launch automatically and you will need to login with your credentials. If the service does not start automcatically, go to Start -> All Programs -> Dell On Premises -> Launch On Premises
3. Enter your tenant Single Sign On credentials in the section below.
4. Enter your KACE credentials if you use KACE appliance.
5. When installation is complete, you will see the following message: Gateway registered successfully.

Use the Download button below to download and install On Premises application package. This package includes AD Connector, KACE Service, and Single Sign-On Service.

Version: 1.0.1

Platforms: Windows

Single Sign-On

Single Sign-On allows users to use their domain credentials for logging in to both the administration and self-service consoles, and for device registration.

NOTE: This functionality requires the On Premises Gateway to be registered.

□ Enable Single Sign-On

Domain: *

Authentication Server URL: *

AD Port: 0 *

Idle Timeout: 1 minute(s)

☑ Disable local user accounts for mobile user

Dell KACE

The Dell KACE K Series Appliances addresses the management of the complete systems life cycle, from deployment to retirement, by offering a fully functional appliance-based systems management solution.

The On Premises Gateway can be configured to automate the export of asset inventory into the Dell KACE K1000 appliance. Register your Dell KACE appliance by entering the required credentials below - for Web Service Password enter the 'Web Service API access' password configured on your Dell KACE appliance.

□ Enable KACE integration

KACE Server IP: *
(ex: 10.100.17.92)

Web Service Password: *

Upload Interval: 4 hours

☑ Use 'CCM-' as prefix to device name

□ Use HTTPS/SSL

Last Sync completed: Not synced yet
Status of last upload: N/A
Total device(s) uploaded from Dell Management Portal: N/A
Total device(s) unsuccessful in last upload: N/A

Active Directory Connector

Last action: None

Use AD Connector to import existing users from Active Directory.

Select the AD Connector operation mode.

● Manual AD Sync — Synchronize selected Active Directory groups and users from AD Connector.
On subsequent Manual Sync operations, users will be added, removed or change group assignment based on Active Directory configuration changes.

○ Bulk Import — This will do a one-time import of Active Directory users.
Subsequent user management and group assignment is done locally from Users page.
Users created as part of a Bulk Import are initially assigned to the Default Policy Group.

Single Sign-On (Installing and Using)

Configuring for Single Sign-On authentication allows administrator users to reuse existing domain credentials (username/password) for logging into the management console and self-service console, and for registering devices.

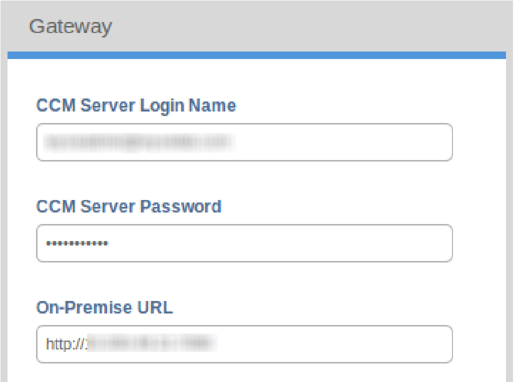
IMPORTANT Requirements: Single Sign-On requires:

- Dell On-Premises Gateway is installed (see "Installing and Registering Your On Premises Service").
- Administrator User with the "Global Administrator" role enabled (see Roles tab in "Adding/Editing Users").
- Company domain/credentials for the administrator user are entered in the appropriate fields of the Single Sign-On section in the On Premises Service page.
  NOTE: Selecting the Disable local user accounts for mobile user check box will disable the administrator’s local user credentials from signing into the management console and force the administrator to use their Single Sign On credentials to sign in to the management console.

Single Sign-On Registration

Use the following guidelines:

1. After installing the Dell On-Premises Gateway application on your server, the installer will start the gateway, launch the web browser, and go to http://localhost:8080/ccmproxy to open the Gateway Registration window you will use to register the gateway with the management system:
   NOTE: You can also launch a web browser to register the gateway by using the On Premises application (**Start > All Programs > On Premises > Launch On Premises**: or double-click on the **On Premises** shortcut on your desktop).



Gateway

CCM Server Login Name

[redacted]

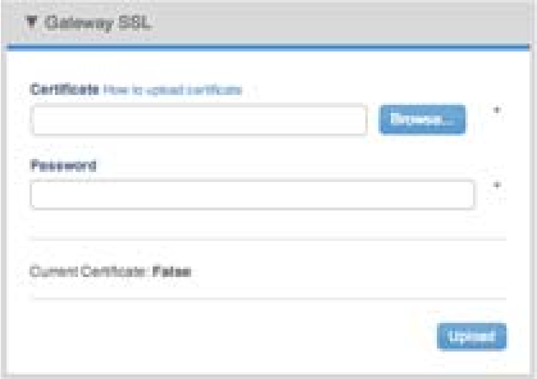
CCM Server Password

•••••••••••

On-Premise URL

http://[redacted]

2. Enter the management console Login Name, Password, and On-Premise URL (the On-Premise URL is the location of your running Dell On-Premises Gateway server), and then click **Register** to open the Gateway SSL Certificate window.



▼ Gateway SSL

Certificate How to upload certificate

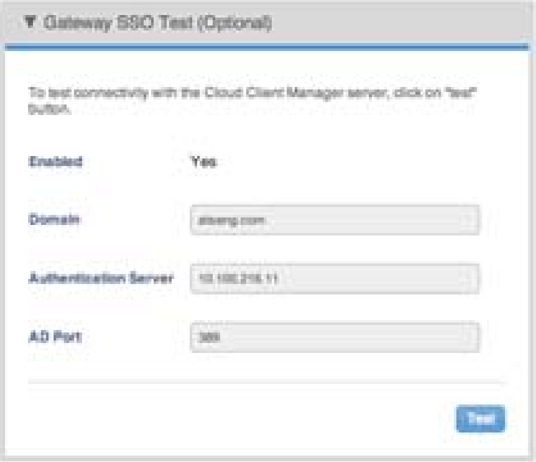
Password

Current Certificate: False

3. Enter your Certificate and Password and click **Upload**.
NOTE: You can use the upload certificate link or go to
https://support.cloudclientmanager.com/entries/30214046
and follow the how to upload certificate instructions. After the certificate is successfully uploaded, you will see the Current Certificate: True message.

4. On the Gateway Registration window, click the **Register** button to register. After successful registration you will see the message: Registered Successfully.
NOTE: You will also see an Unregister page where you can unregister the device if needed, however, you can ignore this page if you want to stay registered.

5. (Optional) You can test connectivity with the Dell Management Console using the **Test** button on the Gateway SSO Test window. You must enter your domain, authentication server, and your AD Port information to perform this test.



▼ Gateway SSO Test (Optional)

To test connectivity with the Cloud Client Manager server, click on "test" button.

Enabled Yes

Domain alseng.com

Authentication Server 10.100.216.11

AD Port 389

KACE

The Dell KACE K Series Appliances address the management of the complete systems life cycle, from deployment to retirement, by offering a fully functional appliance-based systems management solution. The management console On Premise module can be configured to extend the asset management reporting offered by Dell KACE K1000 appliance by automating importing of the mobile device asset inventory from the management console into the K1000 appliance.

TIP: If you already have a KACE appliance you may register it by entering the required credentials. For WS Password enter the Web Service API access password.

Configuring KACE

NOTE: Communication between KACE and the management console happens via Web Service calls. Therefore, you must configure the KACE server first and enable its Inventory API access as specified in the KACE administrator guide. Once the KACE server is configured, you must update the management console appropriately with KACE configuration values:

1. Go to the KACE section in the On Premises Service page in the management console (**Login to the management console > Portal Admin > On Premises > Scroll down to the KACE section**).
2. Select the Enable KACE integration check box.
3. Enter the KACE Server IP (IP or Hostname of the KACE Server - for example, 10.200.29.71).
4. Enter the Web Service Password (Web Service API Access password which was set by the KACE administrator in the KACE **Settings > Security Settings**).
5. Enter the Upload Interval you want (Interval to upload new/updated devices from the management console server to the KACE inventory - 4 to 8 hours).
6. (Optional) Select the Use “CCM-” as prefix to device name option to indicate if the “CCM-” prefix needs to be added to the “device name” being uploaded to the KACE device inventory. This can be used to help distinguish which assets were imported from the management console.
7. (Optional) Select the Use HTTPS/SSL option for secured communication between the K1000 appliance and the On Premises Gateway. Note that the K1000 appliance must be SSL-enabled first.

KACE Workflow

As soon as the KACE component becomes active within the management console On-Premises Gateway, it will start pulling KACE-configuration from the management console at an interval of 30 seconds until it receives a valid configuration. As part of upload activity following steps will be performed:

1. All the mobile devices from the management console will be added/updated after the last successful upload. So for the very first upload all existing mobile devices are processed.
2. Based on the total number of devices, the upload activity can take several minutes or hours.
3. The KACE inventory page will show all the uploaded mobile devices.
4. The KACE section in the On Premises Service page of the Administrators console will also update and display the number of updated devices, successful/failed, last upload date/timestamp.

NOTE: After synchronizing, the Status of the Last Sync area will contain one of the following values:

- **Pending** (upload is currently in progress)
- **Success** (upload successfully completed}
- **Failure** {upload failed for some reason)
- **No upload required** (No new devices added or updated - no upload was required)
- **Error (TIMED OUT)** (in cases where the KACE server is not reachable or non-responding)
- **Error (BAD PASSWORD)** (in cases where the Web Service password is incorrect)

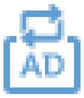
Active Directory Connector: Importing Existing Active Directory Users into the System

(Dell Management Console Pro Version Only) After installing On Premises Service (see "Installing and Registering Your On Premises Service") you can use the Active Directory Connector wizard to complete the publishing of your Active Directory users (import existing users from Active Directory into the management console for use in the system). Simply go to **Start > All Programs > On Premises** and click on **Active Directory Connector** to launch the wizard.

The Active Directory Connector section in the On Premises Service page of the Administrators console (**Portal Admin > On Premises > Active Directory Connector area**) allows you to select the mode of importing that you want to use. You can manually add and synchronize your selected groups and users from the Active Directory Connector or you can perform a one-time import of all Active Directory users (after selecting your option, be sure to click **Save Settings**):

- **Manual AD Synch** - This option synchronizes selected Active Directory groups and users from the Active Directory Connector. On subsequent Manual Sync operations, users will be added, removed, or change group assignment based on Active Directory configuration changes.
- **Bulk Import** - This option performs a one-time import of Active Directory users. Subsequent user management and group assignment is done locally from the management console.
  IMPORTANT: Users created as part of a Bulk Import are initially assigned to the Default Policy Group.

NOTE: After import, users will be added to the Users page (see "Managing Users") and Groups page (see "Managing Groups and Group Policies") according to your Active Directory Connector settings. Also note that the Active Directory icon helps you to distinguish between locally created/managed Groups and those created as part of an Active Directory import (Manual AD Sync option only).

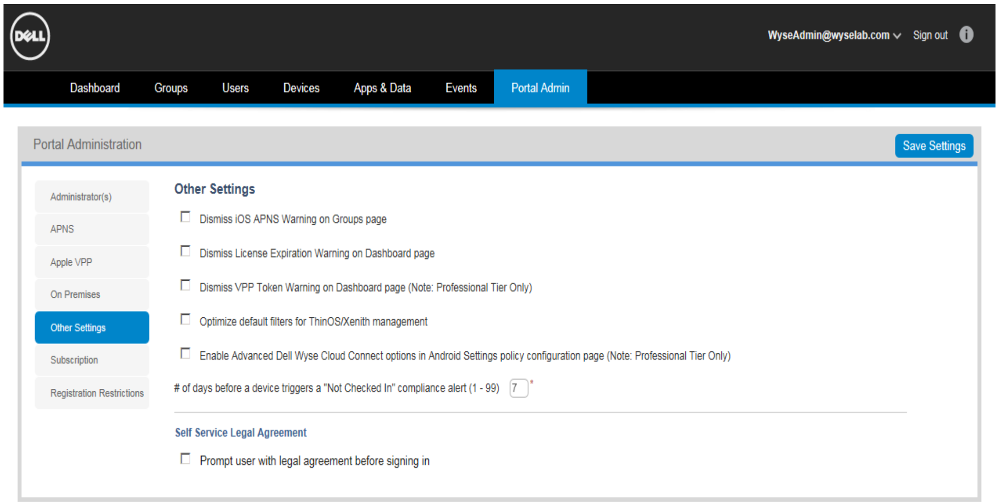


This icon is shown in the Groups page, and anywhere else the Group name is shown (for example, Users page—Group column, Group filters/statistics, Event messages, and so on).

Other Settings: APNS Warnings, License Expiration Warnings, and Self Service Legal Agreements (Enforcing the Agreement for All Self Service Users)

The Other Settings page of the management console (**Portal Admin > Self-Service**) allows you to:

- Dismiss iOS APNS Warning on the Groups page (select this check box, and then click **Submit**). This will remove the warning that appears in the Group page when an iOS APNS certificate has been uploaded from Portal Admin page (see "Generating an APNs Certificate (iOS Only)").
- Dismiss License Expiration Warning on Dashboard page (select this check box, and then click **Submit**). This disables the warning for a license expiration from appearing on the Dashboard page.
- Dismiss VPP Token Warning on Dashboard page (**NOTE**: Professional Tier Only) - This disables the warnings on the Dashboard page when there is less than 30 days before the Apple VPP Token will expire.
- Optimize default filters for Thin Client management (select this check box, and then click **Submit**). This enables the Thin Client filter to be the default view for the Devices page (see "Managing Devices") and the File Repository Inventory page to be the default view for the Apps & Data functional area (see "Managing File Repository Inventory").
- (Dell Management Console Pro Version Only) Enable the Dell Wyse Cloud Connect Advanced options in Android Settings policy configuration page (see "Details: Android Policy Settings"). These options allow you to specify native commands using Dell Wyse Cloud Connect specific parameters (up to 10).
  NOTE: These options should only be used for specific commands when provided by the Dell Wyse Cloud Connect team.
- # of days before a device triggers a Not Checked In compliance alert (enter the number of days from 1 to 99 before a device triggers a Not Checked In compliance alert, and then click **Submit**). This enables the Not Checked In compliance alert to be displayed for devices that do not check in with the management console within the number of days you entered.
- Have a Legal Agreement pop-up before a non-administrator self-service user logs in to the Self-Service page. Simply enter the text that you want to display before the non-administrator self-service user is allowed to log in, select the **Enforce the agreement for all self service users** check box, and then click **Submit**.



Other Settings

□ Dismiss iOS APNS Warning on Groups page

□ Dismiss License Expiration Warning on Dashboard page

□ Dismiss VPP Token Warning on Dashboard page (Note: Professional Tier Only)

□ Optimize default filters for ThinOS/Xenith management

□ Enable Advanced Dell Wyse Cloud Connect options in Android Settings policy configuration page (Note: Professional Tier Only)

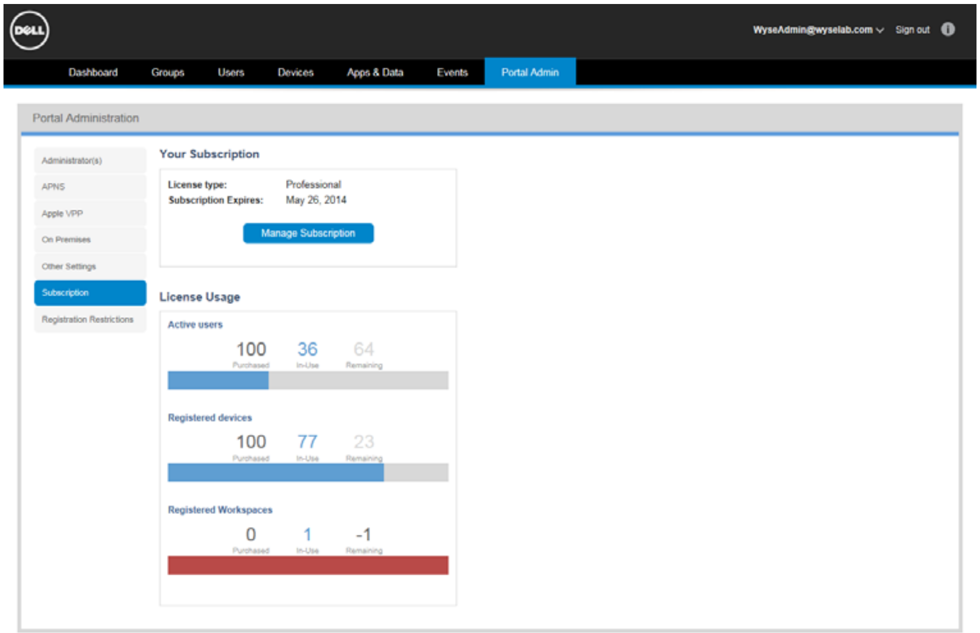
# of days before a device triggers a "Not Checked In" compliance alert (1 - 99) 7 *

Self Service Legal Agreement

□ Prompt user with legal agreement before signing in

Viewing and Managing Your Management Console License Subscriptions

The Subscriptions page of the management console (**Portal Admin > Subscriptions**) allows you to view your management console license subscription information and usage, and to manage your license subscriptions.



Your Subscription

License type: Professional
Subscription Expires: May 26, 2014

License Usage

Active users

100	36	64
Purchased	In-Use	Remaining

Registered devices

100	77	23
Purchased	In-Use	Remaining

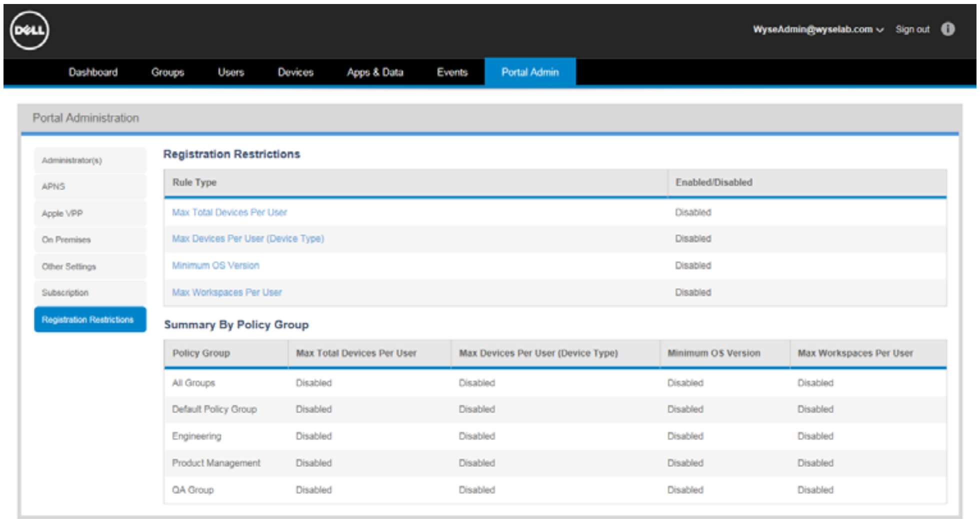
Registered Workspaces

0	1	-1
Purchased	In-Use	Remaining

TIP: Click the **Manage Subscription** button to access and use your management console product and billing account.

Registration Restrictions (Installing and Using)

The Registration Restrictions page of the management console (**Portal Admin > Registration Restrictions**) allows you to configure rules that prevent users from registering mobile devices unless they meet the defined criteria.



Registration Restrictions

Rule Type	Enabled/Disabled
Max Total Devices Per User	Disabled
Max Devices Per User (Device Type)	Disabled
Minimum OS Version	Disabled
Max Workspaces Per User	Disabled

Summary By Policy Group

Policy Group	Max Total Devices Per User	Max Devices Per User (Device Type)	Minimum OS Version	Max Workspaces Per User
All Groups	Disabled	Disabled	Disabled	Disabled
Default Policy Group	Disabled	Disabled	Disabled	Disabled
Engineering	Disabled	Disabled	Disabled	Disabled
Product Management	Disabled	Disabled	Disabled	Disabled
QA Group	Disabled	Disabled	Disabled	Disabled

To configure a rule, click on the rule name link and select the **Enable Rule** check box. Each registration rule can be configured in one of two ways:

- Same Value for all Policy Groups - Select the Same value for all groups option.
- Individual Value for Each Policy Group - Select the On a per-Policy Group basis option.

NOTE: If a device has already been registered prior to the rule being modified, the device will not be automatically blocked from checking in to the management console. To remove these devices from management, use the Unregister option from the Devices page.

There are four types of Registration Rules that you can configure:

- **Max Total Devices Per User**: The total number of registered mobile devices (iOS, Android, and Cloud Connect) allowed per user. Once users reach the maximum they will be blocked from registering further mobile devices.
- **Max Devices Per User (Device Type)**: The number of iOS, Android, and Cloud Connect devices registered allowed per user (according to device type). For iOS-type devices, a rule can be configured either for the total number of iOS devices or by specific iOS device model (iPhone, iPad, iPod). Both total number of iOS devices and specific iOS device models can be configured at the same time, however, the total for specific iOS device models cannot exceed the value set for the total number of iOS devices.
  For example, if the total number of iOS devices (iPhone, iPad, iPod) are all set to 2, any combination of iPhone, iPad, and iPad can be registered as long as the total number of iOS devices does not exceed two registered iOS devices.
  IMPORTANT: In all cases, users cannot register more devices than allowed by the Max Total Devices Per User rule.
- **Minimum OS Version**: The minimum OS version accepted for device registration.
  IMPORTANT: This rule is supported for iOS (iPhone, iPad, iPod) and Android devices only.
  NOTE: Version number can be configured up to 3 decimal places.
- **Max Workspace Apps Per User**: The total number of Workspace apps registered allowed per user. Once users reach the maximum they will be blocked from registering further Workspace apps.

Tables

Administrators Guide

Dell® Management Console for Dell Enterprise Mobility Management and Dell Wyse Cloud Client Management
Issue: 072914

Written and published by:
Dell Inc., July 2014

Created using FrameMaker® and Acrobat®