Oracle® Fusion Middleware

Administrative Console Guide for Oracle Mobile Security Suite

Release 3.0 **E51933-01**

February 2014

The Oracle Mobile Security Container is an important feature of Oracle Mobile Security Suite. The container isolates your enterprise access on personal devices, enabling corporate "Bring Your Own Device" (BYOD).

The Mobile Security Administrative Console is the administrative interface to the Oracle Mobile Security Container. Your information technology department manages enterprise access through the console. Administrative users establish what containers can do through by using the Mobile Security Administrative Console. Console features include modifying permissions, applications, and settings, and setting policy on containers.

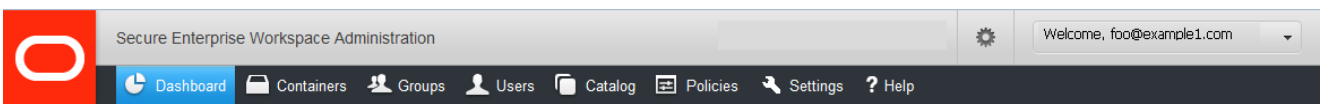
You log in to the Mobile Security Administrative Console by typing a URL into your web browser and entering your user credentials into the login dialog. The URL is of the form:

`https://`*`yourserver`*`/acp`

This guide contains the following sections:

1 Introduction to the Mobile Security Administrative Console

The Mobile Security Administrative Console has a standard menu bar, which is functionally organized as follows:



- The grey bar at the top enables simple preferences to be set or modified.
- The Preferences bar above the menu provides display and user-selection options:
- The welcome message displays the active user account. By clicking on it, you can switch between administrative user accounts or log out of the active user account.
- The Preferences wheel enables you to modify the Mobile Security Administrative Console interface. You can display icons with or without labels.

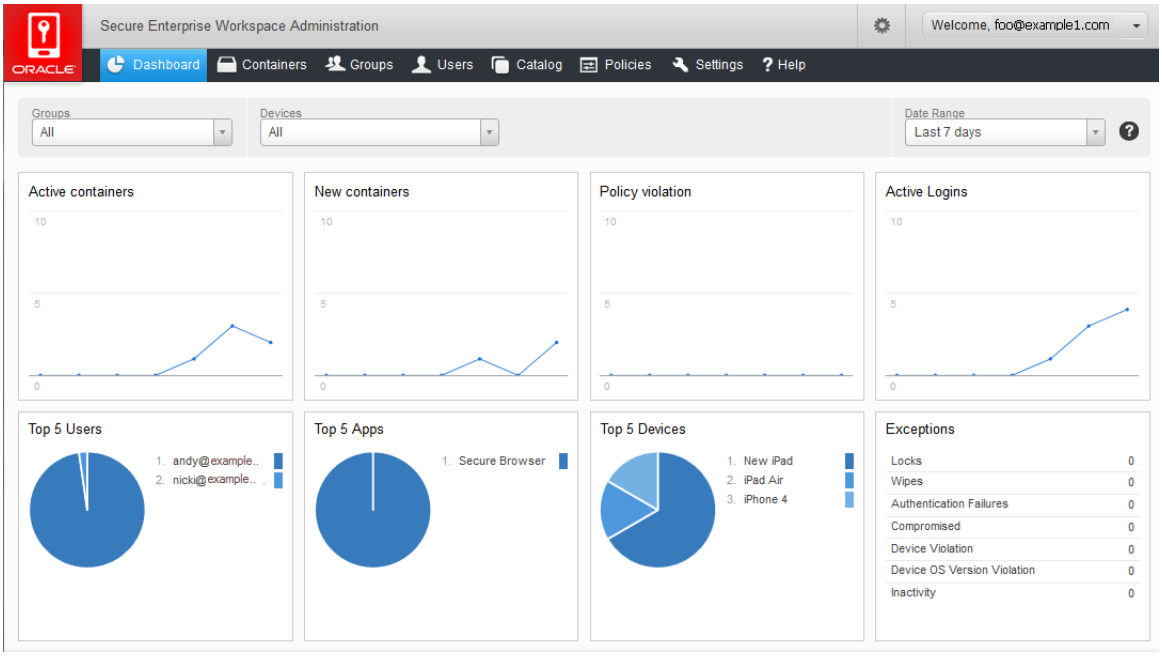
  You can also modify the time zone by selecting a time zone from the list at the bottom of the preferences dialog.
- In the menu bar, the tab for the active page is highlighted.

  The name and functions of each page are summarized in the following table:

Page Name	Functions Performed on Page
Dashboard	Display analytics on corporate usage and monitor exceptions
Containers	Display container activity, location, and status. Lock and wipe containers remotely
Groups	Manage groups of users, which can be uniformly provisioned in real-time
Users	Manage users who have containers on their devices and administrative users of Mobile Security Administrative Console
Catalog	List apps that are available to the entire company
Policies	Manage container access and limitations, to be applied to groups
Settings	Company specific settings, (available to company administrators and system administrators)
Help	On-line help guide, which can be viewed from any page and saved as entire PDF

2 Dashboard

By default, the Dashboard page displays all groups for all devices over the last seven days.



You customize your view by making specific selections from the lists, **Groups** and **Devices**.

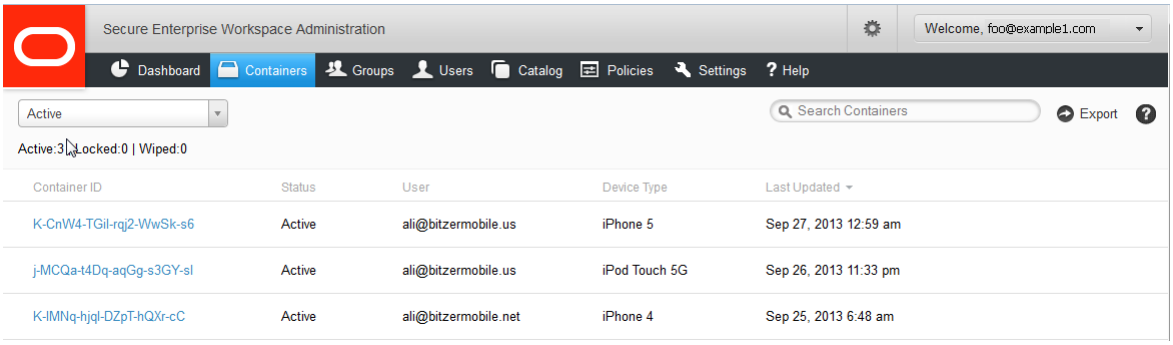
These boxes are updated each time the page is refreshed or any of the selection criteria modified. Groups and Devices can be selected individually. Date Range can be customized between pre-set or custom-specified ranges.

The information boxes on the Dashboard page are:

- **Active Containers**: Date-stamped count of unique active containers on each day.
- **New Containers**: Count of individual containers created each day.
- **Policy Violations**: Day-by-day summary graph of total policy violations.
- **Active Logins**: Daily graph of the total number of logins.
- **Top 5 Users**: Users with the most container activity over the specified time period.
- **Top 5 Apps**: Most heavily-used container apps over the specified time period.
- **Top 5 Devices**: Top active container device types.
- **Exceptions**: Total count of Locks and Wipes due to Policy Violations, Authentication Failures, Compromised devices, Device Type violation, Device OS violation and Inactivity detected.

3 Containers

The Containers page enables you to view or export a list of containers sorted by any criteria.



There are several ways to reorganize your containers. The grey headings below the Search box serve as sort buttons. The list in the image above is sorted in descending order for Last Updated (device container).

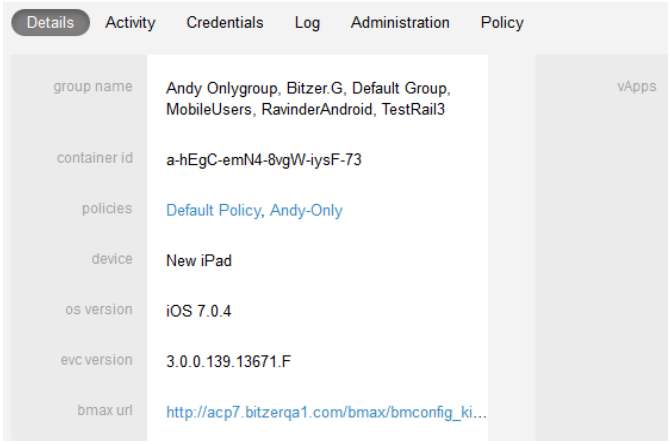
By default, the Containers page displays only the Active containers. Selecting **All** from the list on the top left displays Active, Locked, and Wiped containers. The other way to view inactive containers is to search for them.

Search by ID, Status, Username, or Device Type to locate specific containers.

Clicking **Export** gives you a *.csv* file of your containers, which you can view in any spreadsheet or text editor.

You can click anywhere on a container record, (with the exception of the **Lock** and **Wipe** buttons on the far right,) to display several tabs with additional information about it:

- **Details**: Lists detailed information about this container. This includes the groups it is in, the container ID, policies, device type, OS version, and Virtual Apps (vApps) installed.



- **Activity**: Lists event-based information with map-enabled location and time specifics.
- **Credentials**: View of certificate details that are provisioned inside that container including when it was created and when it expires.
- **Log**: Enables different levels of logging to be implemented on the container. Any changes have to be secured by pressing the **Save** button.
- **Administration**: Enables specific administrative functions like passcode generation.
- **Policy**: Consolidated view of policy settings for that particular user. This is what is getting sent to the client based on all policies to which the user is assigned.

Hovering over a container or selecting it causes the **Lock** and **Wipe** buttons to be displayed.

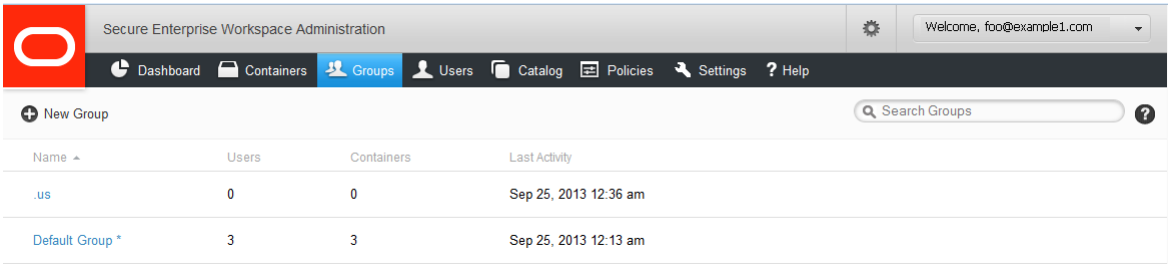
- The **Lock** button disables a container from operating and stops user access to vApps or information. Lock presents a default message window, where administrators can add a message to the lock alert for users to see.

- **Wipe** is a severe action applied to containers, located on the far right side. When the Wipe command is received, all data in the container disappears, essentially 'wiping' it and returning it to factory default. Wipe cannot be undone.

You can click anywhere on the container record, (except for the **Lock** or **Wipe** buttons) to close the Container view.

4 Groups

Groups are used to apply uniform actions across multiple categories of users. If Active Directory (AD) or Oracle Unified Directory (OUD) sync is configured, then group names and user associations come from the directory and adding and deleting groups from Mobile Security Administrative Console is disabled.



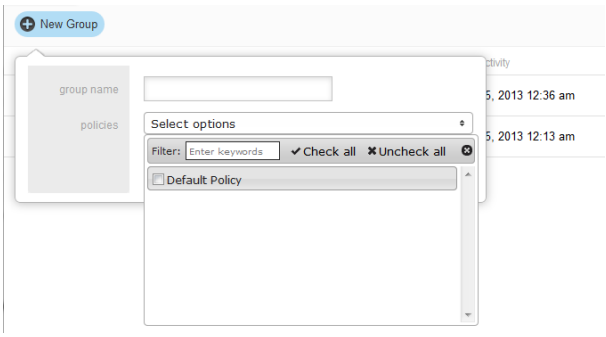
The **Default** group includes all users and cannot be deleted.

Clicking on any group enables you to modify the Group Name and Policies that apply to it. Valid for non-AD or non-OUD groups only.

The **New Group** button enables group creation with a view similar to the Group Edit screen. Policies are selected by typing policy name.

Note: You cannot modify or create groups in Active Directory (AD) or Oracle Unified Directory (OUD) sync configurations. All group actions are taken from the directory.

Add policies that apply to group by selecting applicable policies from the **Select Options** list. Close the list by selecting outside window.



Selecting or hovering over a group causes the following buttons to be displayed:

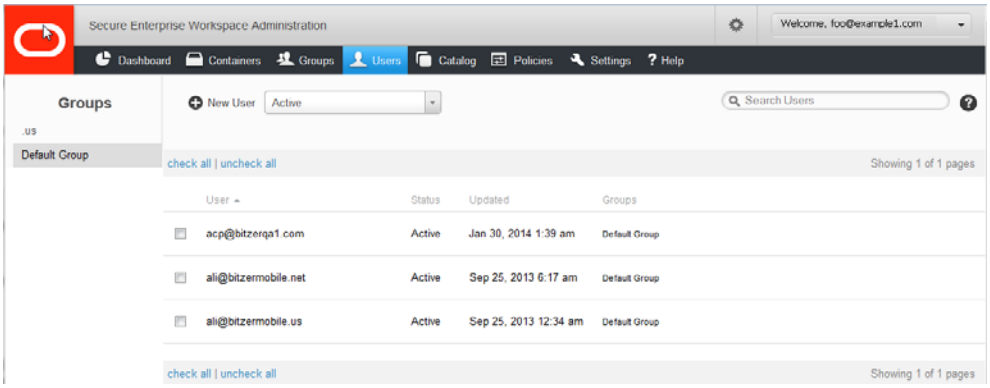
- **Lock** locks all containers owned by current group users. Lock also gives you the ability to enter a message that resides in the lock alert.
- **Unlock** releases all containers that belong to the group to an Active status, essentially recovering any that were Locked.

- **Wipe** causes all containers currently in that Group to have their data wiped. This cannot be undone.
- **Delete** disbands a group, releasing all users from all Policies that acted on that group. This affects the containers on the devices of those users, as they are no longer linked under an umbrella grouping receiving policies. Deleted group entries disappear from Mobile Security Administrative Console.

> **Note:** The **Delete** button is not available in Active Directory or Oracle Unified Directory sync configuration. All group actions are taken from the directory.

- **Invite** sends an invite email to all users in a group based on assigned invite template. Invite email provides instructions to a user for how to install and configure the Mobile Security Container for usage. An option is provided to not send invites to already registered users.

5 Users

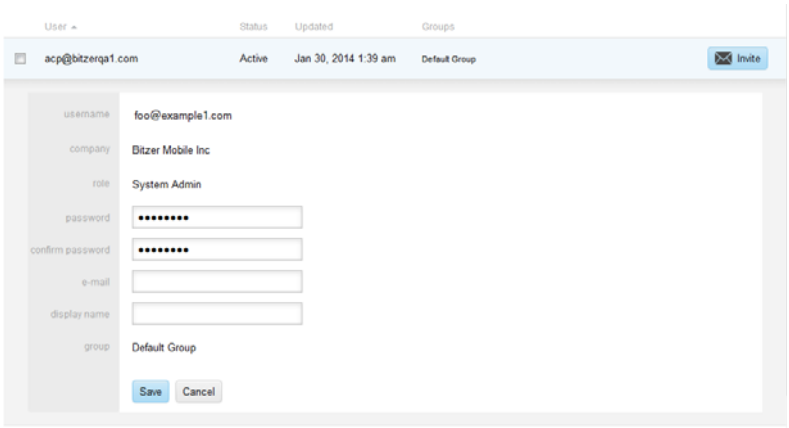


Users can be entered manually or imported from Active Directory or Oracle Unified Directory integration, provided Active Directory or Oracle Unified Directory sync is NOT enabled.

If Active Directory or Oracle Unified Directory sync is enabled, then all user and group management must be performed in that directory. Add, delete, and edit of users and groups cannot be performed from Mobile Security Administrative Console.

Users are assigned to Groups in this Users tab.

The edit screen is identical to the New User dialog. To edit a user, click on the User record



The fields on the Edit screen are as follows:

- **Username**, an email address, is a required value which serves as a unique identifier.
- **Company** is a default value.
- **Role** has the following selection options available:
  - **End User**: Views Dashboard, Containers, Groups, Users, Catalog, and Policies. Can only edit containers that the user has access to. Can invite self.
  - **Help Desk**: Views Dashboard, Containers, Groups, Users, Catalog, and Policies. Can edit only Containers. Can invite users, but not groups.
  - **Company Admin**: Views everything, cannot make a company or system administrative user. Can invite users and groups. Can update Catalog, Settings and Policies. Restricted to one company ID.
  - **System Admin**: Views and edits everything. Can access all company IDs
- **Email** address field must be filled in order to enable invite provisioning messages to be sent.
- **Display name** is the user's Active Directory or Oracle Unified Directory display name
- **Password** and **Confirm Password** fields require identical inputs for new or changed passwords.

> **Note:** This password is for Mobile Security Administrative Console access only and doesn't apply if Mobile Security Administrative Console is on IIS that is integrated with Windows Authentication.

- **Groups** displays a list for you to select from. There is no limit to the number of groups a User can belong to.

> **Note:** You MUST click Save before you go to another page, refresh the screen, or click Cancel. Otherwise, all inputs or changes are lost.

Selecting or hovering over a user causes the following buttons to be displayed:

- **Invite** sends an invite email to user based on assigned invite template. Invite email provides instructions to user for how to install and configure the Mobile Security Container for usage.
- **Disable** disables user account and sends a wipe command to any active or locked containers for that user. The User can not register a new container when the account is disabled
- **Activate** re-activates a disabled user account. User are now be able to register new containers
- **Delete** removes the user from the database and wipes any active containers. All audit records are kept for old containers.

> **Note:** **Disable**, **Activate**, and **Delete** buttons are not available in Active Directory or Oracle Unified Directory sync configurations. All user actions are taken from the directory.

Selecting users enables assigning of users to group(s) by selecting group(s) and save.

Selecting group name on left side of screen displays all users in that group

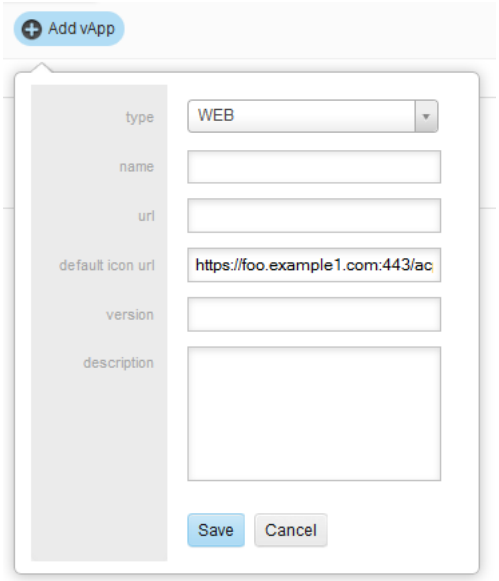
6 Catalog

The Catalog page displays a list of currently available virtual apps (vApps). Mobile Security Administrative Console administrators use this page to control company access to apps, sites, and folders.

The list of available Virtual Apps (vApps) can be sorted in ascending or descending order by clicking on **Info**. Clicking on **Installed on** enables you sort vApps by number of containers. This enables you to examine the most or least common vApps.

To edit an existing vApp, click on the entry for it. To add a vApp, click **Add**. The Edit and Add vApps screens are identical.

Required fields are name, url, and version. Description is an optional field.



Types of vApps include:

- **WEB**: any URL accessible via browser or HTML5 app
- **SHARED FOLDER**: any Windows file system folder or SharePoint folder. Windows share URL format should be `smb://server_name/shared_folder/`*`samaccountname`*

  Examples of Active Directory user attributes used in URLs:

  `samaccountname`
  `upn`
- **Containerized App**: any native app that has been containerized with the Mobile Security App Containerization Tool can be configured or uploaded to the Catalog. Containerized apps that are uploaded to Oracle Mobile Security Administrative Console can be installed and updated by user from the Catalog in their container. Containerized app details like name, version, url path, and icon are pulled directly from the app file. Multiple containerized app can be uploaded simultaneously by selecting multiple files from the browse location.
- **Oracle Container App**: the main Mobile Security Container. It is loaded in a publicly available location. Invite template can be configured so that they are automatically populated with correct download URL. (See the Settings: Invite Template tab for more details) Updates to Mobile Security Container App are also available through the Catalog

Note: For clustered Mobile Security Administrative Console deployments, Oracle Container and any Containerized apps must be uploaded to each Mobile Security Administrative Console in the cluster.

For more information on clustered server installations, see "Configuring Mobile Security Access Server Load Balancing" section of *Oracle Mobile Security Suite Installation Guide.*

Once the vApp is created, it is listed on this page. Clicking on any vApp enables you to update certain vApp information. New versions of Containerized or Oracle Container Apps can also be uploaded. Based on the policy, users who have installed the apps can get an upgrade alert and will see a badge on the container's catalog. For a Containerized App, an upgrade will be triggered if either the actual application version or containerization version is changed. Different versions can be uploaded separately to extend version compatibility and upgrade independence.

7 Policies

Policies enable Mobile Security Administrative Console users and administrators to implement group-based access and manage vApp availability.

Notes:

- The Default policy is always overridden by a secondary policy except for Catalog, Timefence and Geofence, where users get the combination of authorizations. As an example, if a user has Policy A in addition to Default and compromised platform for Default policy = wipe and geofence = San Francisco and Policy A compromised platform = lock and geofence = New York. What is applied is compromised platform = lock and geofence = San Francisco + New York.
- If a user is assigned multiple secondary policies (in addition to Default) then the most restrictive policy is applied. As an example, if a user has two policies in addition to Default and authentication frequency in Policy A = always and in Policy B = session then the more restrictive is applied, that is, authentication frequency = always.

- Click a policy to edit.
- Click **Add** to add a new policy.
- Click **Save** after entering information. When you modify or create a new policy, nothing is saved until you click **Save**. If you do not do so, all modifications are lost when you go to another page, refresh the screen, or press **Cancel**.
- **Cancel**: Discards all changes made within any and all the tabs of the current page since the last Save.

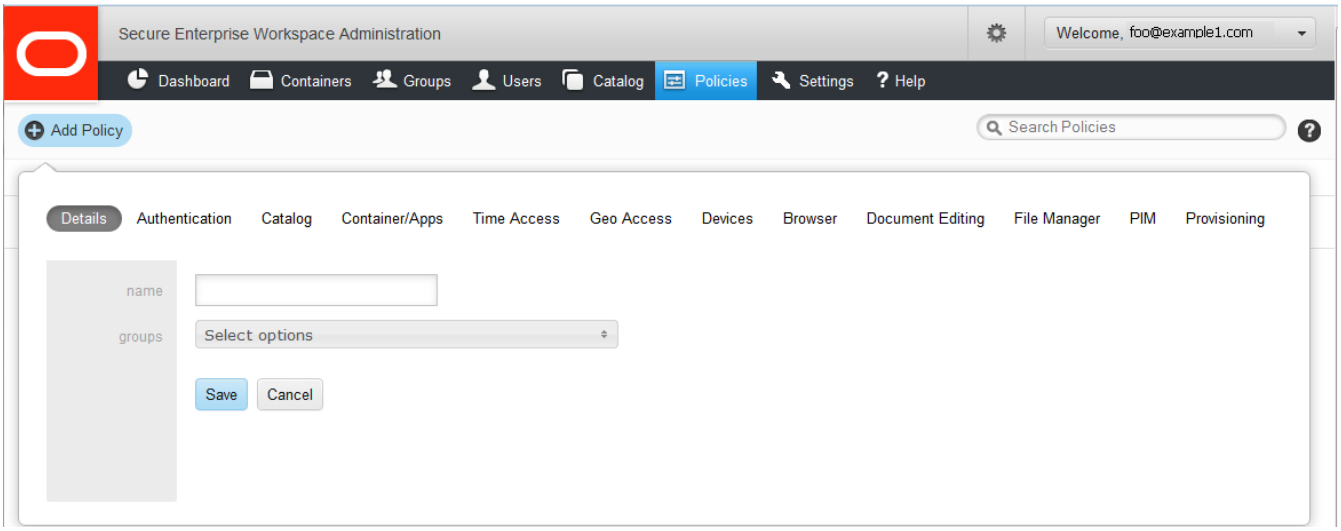
The **Edit** and **Add Policy** dialogues are identical and contain the following tabs:

- Details
- Authentication
- Catalog
- Container/Apps
- Time Access
- Geo Access
- Devices

- Browser
- Document Editing
- File Manager
- PIM
- Provisioning

7.1 Details

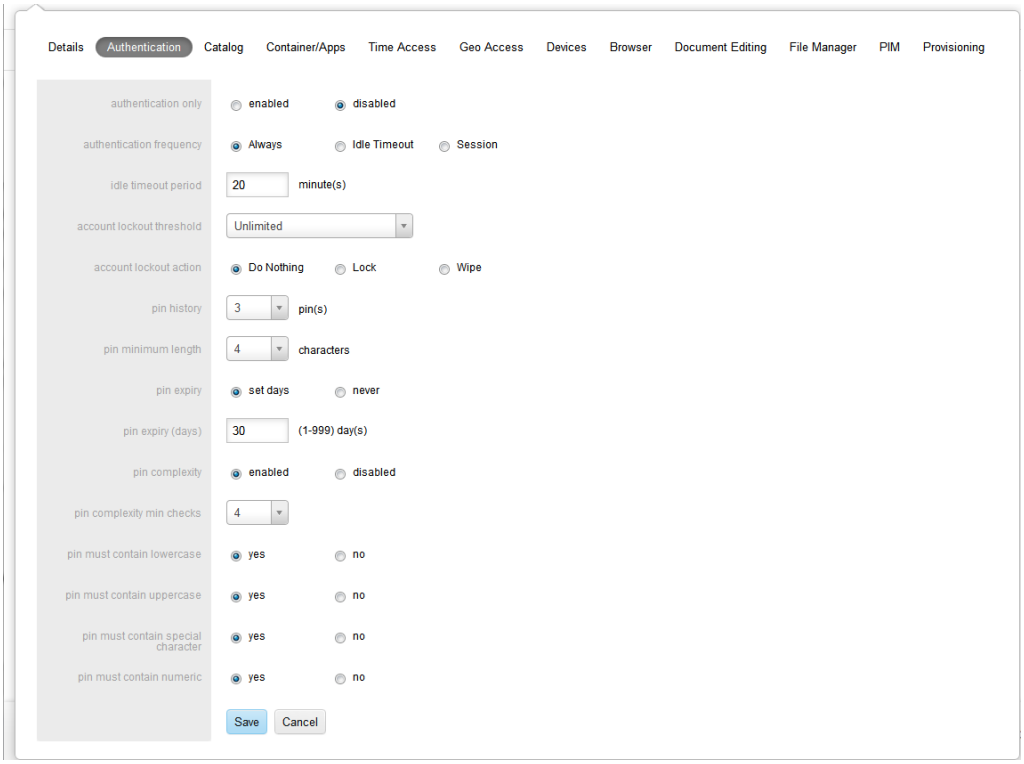
Use this tab to control the policy name and the groups that the policy acts upon.



- **Name** is a required field. The validity of every new or modified name is verified when you click **Save**.
- **Groups** are selected by checking the corresponding boxes. There is no limit to the number of groups a policy can act upon.

7.2 Authentication

You use this tab to control authentication permissions for the Oracle Mobile Security Container.



- **Authentication Only** enables the ability to hide the contents of the container from the user IF container is purely being used as authentication client and not for any app UI.
- **Authentication Frequency** specifies how often users see the login screen.
  - A setting of **Always** makes them authenticate every time they try to access the Mobile Security Container on their device.
  - **Idle Timeout** enforces authentication each time the Idle Timeout Period has been reached. The Timeout Period is the number of minutes a container is allowed to remain inactive before prompting with the login screen with a maximum of two hours. This period continues to apply while the user is outside the container.
  - **Session** allows users to exit the Mobile Security Container to use other apps and does not require them to log in upon return until the session ends. A session expires when the Oracle stoken expires (configurable with default of 10 hours) or the device closes the app due to low memory.
- **Account Lockout Threshold** specifies the number of incorrect login attempts that are allowed before the Account Lock Action is taken on their container.
- **Account Lockout Action** is what the container does when a user reaches their lockout threshold. **Do Nothing** causes no change. **Lock** causes the container to be locked. **Wipe** assures nothing remains on the device for anyone to access. **Lock** requires users to contact their IT help desk to get unlocked.
- **Pin History** enforces how soon we can reuse old pins. It specifies how many unique pins are created for login before a previous pin can be reused. In case of a pin-history of 3, if a user changes an initial pin of `demo1` to `demo2`, and wants to change it back, they can not do so until they have changed the pin to different values a total of 3 times.

Note: PIN options only apply to customers using certificate-based authentication

---

- **Pin Maximum Age** is the number of days a user can use their pin before the system enforces a change. This can be anywhere from 1 to 999 days.
- **Pin Minimum Length** can be set up to be anywhere between 4 to 14 characters.
- Enabling **Pin Complexity** exposes the PIN complexity options. These options control the requirements for pin complexity.
  - **Pin Complexity Min Checks** is a number between 1 and 4, which indicates how many of the following four options must be set to **YES**.
  - **Pin Must Contain Lowercase** requires users to set at least one lowercase character.
  - **Pin Must Contain Uppercase** requires users to set at least one uppercase character.
  - **Pin Must Contain Special Character** requires users to set at least one special character.
  - **Pin Must Contain Numeric** requires users to set at least one numeric character.

Note: If the number of options marked **YES** is greater than **Min Checks**, users may set their pin with any combination of options that meets the requirements. For example, if **Min Checks** is 2 and all four complexity types are set to **YES**, a password with any combination of two or more of the requirements is acceptable.

7.3 Catalog

This is the list of virtual apps to which users have access on their containers.

You can **Add vApp to User Catalog** by beginning to type its name. All the vApps that match the characters you entered appear in a list for you to select from. When you select it, the vApp gets added to that policy's User Catalog, showing up in the list of apps below and its full name.

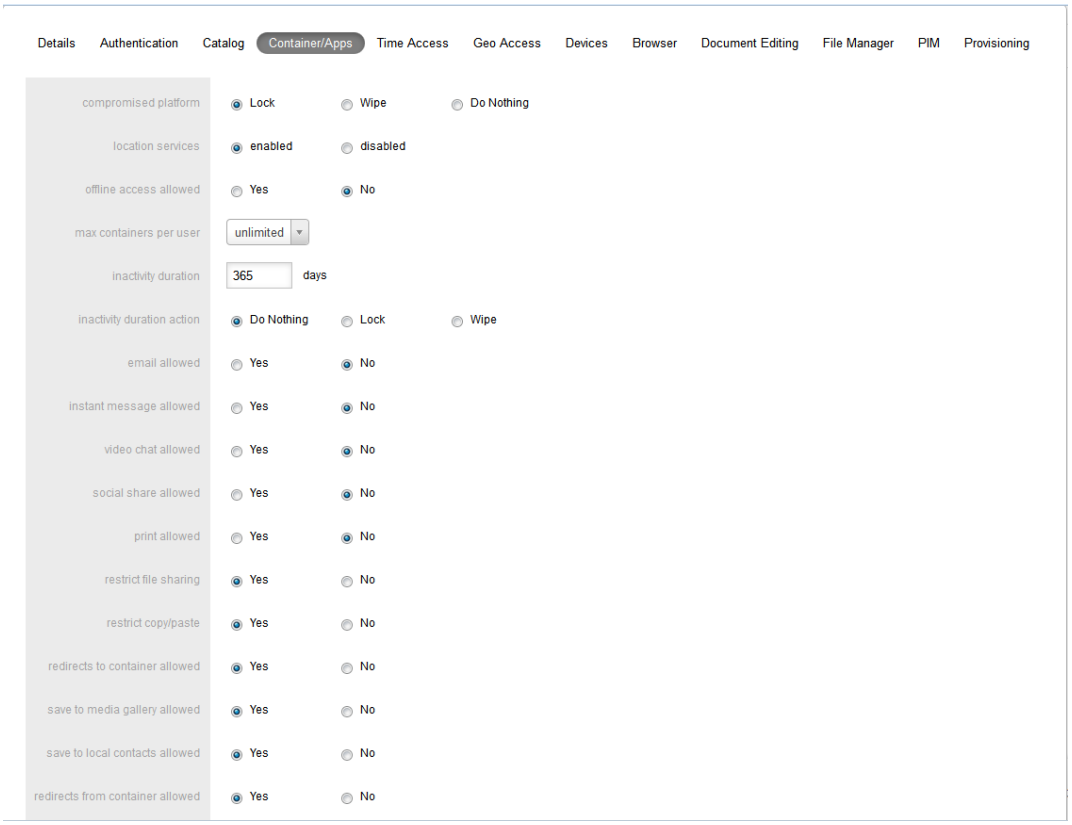
You can click the **x** on the top-left of any vApp icon to remove it from that policy's User Catalog. Any vApp removed from the User Catalog is removed from groups where this policy applies.

Every vApp that is added to the User Catalog gets a check-box to the right, which determines how the vApp appears in the container.

- Install on Homepage (checked) makes vApps appear on the user's main screen or homepage, where they see the browser icon.
- Install on Homepage (unchecked) makes the vApp available in the user's catalog, which can be accessed if they go to the Catalog page on their container. This selection does not automatically put the vApp on the container home page.
- Additional check-boxes appear for vApp types Bitzer Container and Containerized App:
  - Upgrade Alert (checked) alerts the user each time app is launched that an upgrade app is available, until such time as it is installed.
  - Upgrade Alert (unchecked) displays a badge on the catalog app indicating that an update is available, but does not alert the user at login.

7.4 Container/Apps

This tab covers security and sharing requirements for the Mobile Security Container as well as any apps containerized with Oracle Mobile Security App Containerization Tool.



- **Compromised Platform** defines the action to be taken in the case of an iOS device that has been jailbroken, or an Android device that has been rooted. In the case of the Do nothing action, no action is taken (this should ONLY be used for testing purposes, NOT in production). In case of the Lock action, the container continues to be locked until the device is no longer compromised. A Wipe clears the container data in the Mobile Security Container.
- **Location Services** allows administrator to turn on/off location services for users. If Disabled then the user is not asked to accept location services during installation and user location is not tracked.
- **Offline Access Allowed** is a simple Yes or No selection. A Yes setting permits access to the information already in the container while the user is offline. Syncing is not possible while offline. A No setting ensures that the user cannot use their Mobile Security Container unless they are online and logged in.
- **Max Containers Per User** controls the max number of containers that a user is allowed to register with a single Admin Control Panel.
- **Inactivity Duration Period** is the period of time in days before the Inactivity Duration Action is taken IF the client has not accessed the Mobile Security Administrative Console. User account is automatically disabled in ACP upon passing of Inactivity Duration Period.
- **Inactivity Duration Action** is the action that is taken if client has not accessed the Mobile Security Administrative Console before Inactivity Duration Period. Action is taken on the client as soon as container is accessed and Inactivity Duration Period is passed. **Do nothing** causes no action to be taken, **Lock** automatically locks the container, Wipe automatically wipes container.

The following data leakage protection policies restrict how and if users can share data within an app:

- **Email allowed** can restrict the ability to send email from an app.
- **Instant Message allowed** can restrict the ability to send Instant Message from an app.
- **Video chat** allowed restricts the ability to share information via services such as FaceTime.

- **Social Share** allowed restricts the ability to share through integrated services such as Facebook or Twitter.
- **Print allowed** restricts the ability of the user to print.
- **Restrict file sharing** restricts the ability of the user to share files outside the secure enterprise workspace.
- **Restrict copy/paste** only allows copy/paste inside the secure container, containerized apps or between containerized apps, but not to apps outside the secure enterprise workspace.
- **Redirects to container allowed** prevents any app outside the Mobile Security Container workspace from redirecting a URL into the container
- **Save to media gallery allowed** prevents images, videos and audio files from being saved to media gallery and photo stores.
- **Save to local contacts allowed** prevents contacts inside secure enterprise workspace apps from being saved down to native device contacts app.
- **Redirects from container allowed** prevents any vApp from the Mobile Security Container workspace or containerized app from redirecting a URL outside the Mobile Security Container workspace or containerized app.

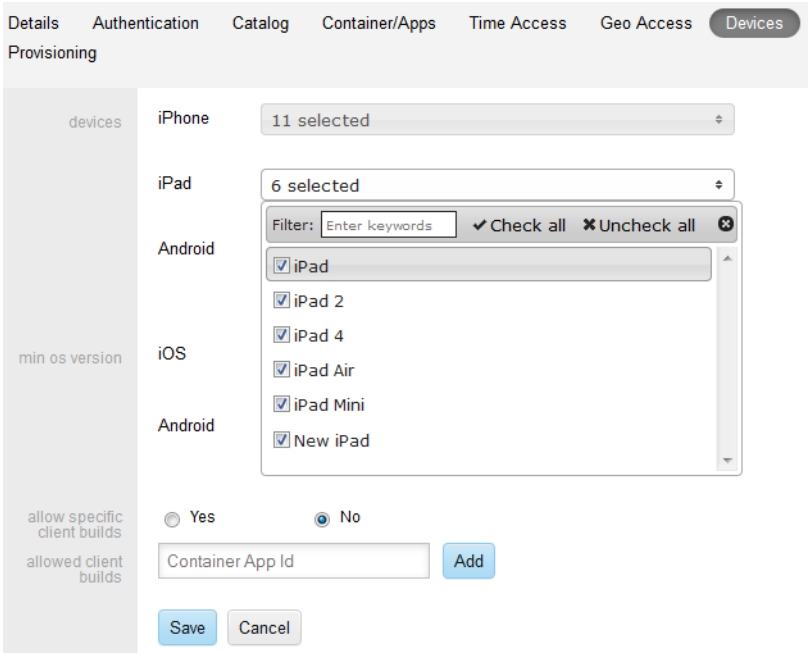
7.5 Time Access

You can set up to five access windows between 12:00 midnight and 11:59 pm. Click **Add** to create access windows. The **Save** button must be pressed to apply changes.

7.6 Geo Access

You can specify a number of cities, states or countries and allow access to only those locations. There is no limit to how many cities, states, and countries you can specify and leaving it blank defaults to no restrictions.

7.7 Devices



On this tab you select which of hundreds of available iOS and Android devices can utilize the Mobile Security Container. Any unselected device is disallowed. There is also a selection for **Other Devices**, which enables devices not listed here.

Minimum OS version is the minimum OS level that is allowed for any device type.

> **Note:** If a previously permitted device or OS is deselected after it has been in use, the device is wiped the next time a user logs into the Mobile Security Container with that device.

Allow specific client builds can be used to specify only specific app IDs to register. For example, it can allow ONLY customer-specific apps to register and prevent the registration of the Oracle Mobile Security Container app from the Apple AppStore.

7.8 Browser

Use this tab to control security settings for browser access.

- **Address Bar Enabled** displays the address bar and browser app icon if set to Yes, or hides it if set to No. However, web vApps can still be pushed to the user and utilized.
- **Download Enabled** permits files to be downloaded if set to Yes, and disabled if set to No. This is an option under the Browser's Menu.

7.9 Document Editing

Use this tab to control data leakage settings for document editor.

Toggling **Allowed** causes the Document Editor app on the secure container home page to appear or not appear.

7.10 File Manager

This tab controls access and security settings for mobile file manager.

- Toggling **Allowed** causes the File Manager app to appear or not appear on the secure container home page.
- **Download allowed** enables a user to save files to the local file store.
- **file manager server base url** provides the URL where the File Manager Server is deployed.

7.11 PIM

- **Email server url** provides Email Server url for the ActiveSync server applicable to users assigned to this policy. Mobile Security Administrative Console supports different mail servers for different user groups.

7.12 Provisioning

Select appropriate invite templates and certificates. Select which invite email template should be used for users with the policy. An example could be separate provisioning instructions for two different geographical locations. Additionally, select users primary authentication certificate and any additional certificate templates that should be managed by Oracle.

8 Settings

The Settings page is only available to System, Company, and enables administrators to manage and maximize the performance of the Mobile Security Administrative Console.

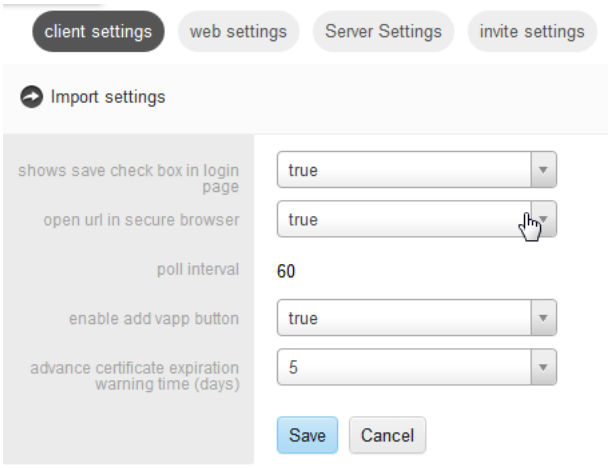
Client Settings are company level settings that apply to ALL containers deployed for that customer. Web Settings apply to Mobile Security Access Server for proxy settings of sites allowed to be proxied and sites that should be blacklisted. Invite Settings are smtp mail server settings and Invite Templates define email templates used for container provisioning to end users.

The Settings page has the following tabs:

- Client Settings
- Web Settings
- Server Settings
- Invite Settings
- Invite Templates
- LDAP Settings
- Notification Settings
- CA Settings

8.1 Client Settings

Selecting **Import Settings** causes the current settings to be imported from the configuration file after Mobile Security Administrative Console installation or configuration change.



This tab has the following fields:

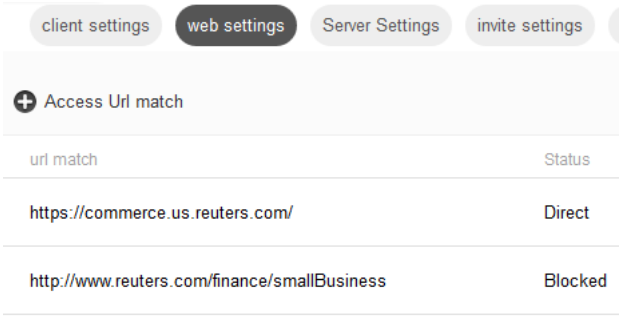
- **Shows Save Check Box in Login Page** controls whether users must enter their username and password each time they log in. An option to remember the username appears on the login screen if the client is configured as the KINIT or OTP Authentication type and this field is set to **True**.
- **Open URL in Secure Browser** controls whether a URL is opened in the Secure Browser. When users click on a protected URL, your company's SharePoint for example, if this value is set to **True**, the URL then opens in the Secure Browser inside the container. If it set to **False**, then the website opens in the default browser of the device.
- **Poll Interval** displays the frequency, in seconds, at which the client polls the server for new policies and commands. Values can only be reset by Oracle Professional Services.

- **Enable Add vApp button** controls whether the Catalog app (Add vApp) is present on the users' home screen.
- **Advance Certificate Expiration Warning Time (days)** provides a menu that can be set to 1 to 30 days. This causes the container to warn users about upcoming certificate expirations, that many days in advance.

> **Note:** Remember to press the Save button if you make any changes in Settings.

8.2 Web Settings

This tab controls which web sites are proxied through Mobile Security Notification Servers and which sites are blacklisted.



To add a new URL to web settings, proceed as follows:

1. Click **Access URL Match**.
2. Enter the **access URL**.
3. Select an **Access Type**:
   - **Proxy** causes matching URLs to proxy requests through Mobile Security Access Server.
   - **Direct** causes matching URLs to go direct to the Internet.
   - **Block** causes matching URLs to not be accessed, that is, it puts those URLs on a blacklist.
   - **Delete** removes the URL from web settings.

> **Note:** Remember to press the **Save** button if you make any changes.

The web settings configuration is retrieved by each Oracle Mobile Security Access Server every 15 minutes, and is used to update the `bmaxaccess.conf`, `bmax.pac`, and `stunnel.pac` files. The `.pac` files control which URLs are proxied by the client devices through the Oracle Mobile Security Access Server.

The URLs listed in all lines are matched against the requested URLs, as follows

- Simple string matching is performed.
- Each entry can include any portion of the requested URL, including the scheme, host, path, or query string, or any parts of those.
- All requested URLs and entries in the access list are converted to lowercase before matching.

Each entry in the access list is comprised of the URL part to match against and a directive on whether the requested URL should be allowed or denied.

- Requested URLs can match multiple entries in the access list.

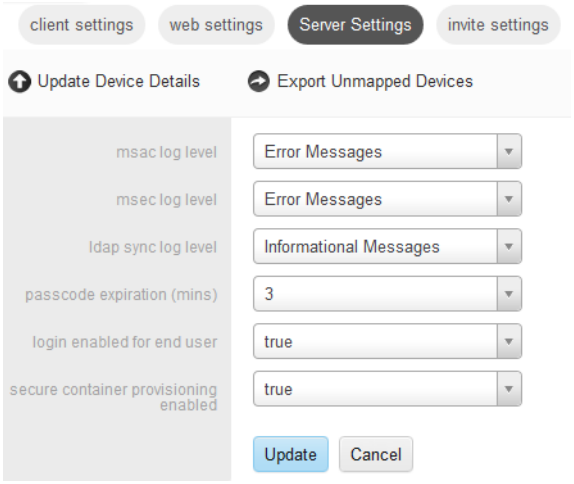
- Block overrides Direct which overrides Proxy, such that requested URLs matching all three are blocked.

By default, if a requested URL does not match any entries in the access list, then the requested URL is denied.

On a fresh installation, the default configuration is that all URLs are allowed, and all URLs are proxied by the client devices through their associated Oracle Mobile Security Access Server. The web settings configured in Mobile Security Administrative Console become active as soon as a single edit is made to the web settings.

On an upgrade installation, the previous `bmax.pac` and `stunnel.pac` files are retained, but are overwritten by the configuration in Mobile Security Administrative Console as soon as a single edit is made to the web settings.

8.3 Server Settings



Server settings allows administrators to change settings for Mobile Security Administrative Console including log levels and device details.

- **Passcode Expiration (mins)** is the number of minutes that the Time Limited Passcode (TLP) that is used to reset forgotten PINs or provision containers is valid.
- **Login Enabled for End User** allows end users to log in to Mobile Security Administrative Console.
- **Secure Container Provisioning Enabled** controls the ability to set and send Invite emails to users, including certificate provisioning.
- Select **Update Device Details** to upload the device and OS detail mappings for new devices.

> **Note:** Previously generated dashboard reports are not recreated with the newly mapped device details. Newly mapped device details will be used for subsequent dashboard report generation. As a result, you might see older activities counted as coming from unmapped or previously mapped device.

- Select **Export Unmapped Devices** to download list of devices and os versions which are not mapped on Mobile Security Administrative Console.

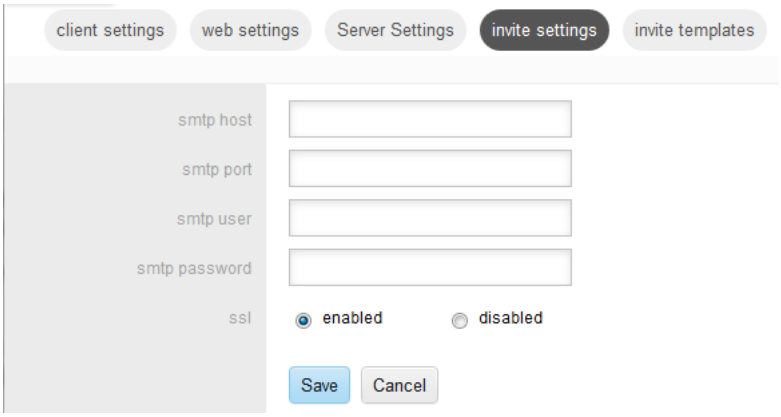
The logs are as follows:

- Mobile Security Administrative Console logs (also known as `msac` logs) are for administrative console panel actions and are generated at *`install_dir`*`/BMAX/ACP/logs/acp-console`;

- Mobile Security Enterprise Control logs (also known as `msec` logs) are for the Web service that clients use to communicate with Mobile Security Administrative Console. They are generated at *`install_dir`*`/BMAX/ACP/logs/ecpservice`.

> **Note:** `msac` and `msec` log levels are not replicated, and the changes are effective *only* on the local host.

8.4 Invite Settings



You use this tab to define all SMTP settings for sending Invite emails to end users. The fields are as follows:

- **SMTP Host** is the hostname of the SMTP server which will be used to send Invite email.
- **SMTP Port** is the port number on which SMTP server is listening for connections.
- **SMTP User**, SMTP Password are the username and password used to authenticate with the SMTP Server to send Invite emails.
- **SSL**: **Enabled** or **Disabled** determines if a secure connection is used to send Invite email through the SMTP Server.

8.5 Invite Templates

Use this tab to define email templates for sending provisioning e-mails to end users. From this tab you can **Edit** the existing template and **Create** new templates. Examples of reasons for multiple templates could be different instructions for different classes of users or users in different locations.

When creating or editing a template you can change the text in each section.

<username> automatically fills in the user name of the end user.

Include TLP includes Time Limited Passcode that can be used for securing certificate provisioning of user authentication certificates.

Include UPN selection fills in the Active Directory or Oracle Unified Directory user principle name (UPN)

Oracle Mobile Security Container App Download Links for iOS and Android can be added programmatically.

- iOS Download Link: `href="itmsservices://?action=downloadmanifest&url=https://@@access_service_host@@/@@ios_app_download_link@@"`
- Android Download link: `href="https://@@access_service_host@@/@@android_app_download_link@@"`

If configuration URL is not added before signing, the app can be configured through a link.

- Container configuration link: `href="bitzerevcconfig://'bmax_config_url':'https://@@access_service_host@@/bmax/configfile.json'"`

> **Note:** The default App Download links are HTTPS but it might not work with Android versions prior to 4.0 if the certificate used for the Mobile Security Access Server is not publicly trusted. To make it work for Android versions prior to 4.0, edit the Android application download link to HTTP instead of HTTPS.

8.6 LDAP Settings

Use this tab to define all sync parameters for Active Directory or Oracle Unified Directory sync. Changes can be sync'd automatically by clicking **Full Sync** or **Incremental Sync**. Otherwise Mobile Security Administrative Console syncs at pre-configured intervals.

- **Directory Type**: is Active Directory or Oracle Unified Directory.
- **Host Name**: is the host name of the Oracle Unified Directory server. This field appears only if the **Directory Type** selected is Oracle Unified Directory.
- **Base dn**: is the distinguished name of the base domain to sync. This field appears only if the **Directory Type** selected is Oracle Unified Directory.
- **Domain Name**: is the Active Directory domain to sync. This field appears only if the **Directory Type** selected is Active Directory
- **Control Group**: is the Active Directory or Oracle Unified Directory group for the approved users that are able to register a Mobile Security Container
- **System Admin Group Name**: is the Active Directory or Oracle Unified Directory group for users with role of Mobile Security Suite Administrative Console System Administrator
- **Company Admin Group Name**: is the Active Directory or Oracle Unified Directory group for users with role of Mobile Security Administrative Console Company Administrator
- **Helpdesk Group Name**: is the Active Directory or Oracle Unified Directory group for users with role of Mobile Security Administrative Console Helpdesk
- **LDAP User Name**: is the username for the account used to sync Active Directory or Oracle Unified Directory.
- **LDAP User Password**: is the password for the account used to sync Active Directory or Oracle Unified Directory.
- **Confirm Password**: is to confirm the above password.
- **Enable/Disable LDAP over SSL**: This is where to specify whether Active Directory or Oracle Unified Directory sync should use secure connection.

> **Note:** Selecting **Enable LDAP over SSL** requires a system restart as this setting requires some environment variables that are not available to scheduled tasks until a restart.

- **Global Catalog Port**: is the port number on which domain controller is listening for global catalog requests. This field appears only if the Directory Type selected is Active Directory.
- **Domain Catalog Port**: is the port number on which domain controller is listening for domain catalog requests.

- **Delete/Disable Users Container Action**: if a user is removed from control group, deleted or disabled in Active Directory or Oracle Unified Directory, action should be either wipe, lock or do nothing. Typically in production the action is wipe, but for some testing environments Do Nothing might be preferred
- **Additional LDAP User Attributes**: if you are using Mobile Security File Manger and need some LDAP attributes to map a user's Home drive, add those attributes here. For example: `homedirectory`, `upn`.

Note: The background task for automatic sync is an incremental sync and only takes changes or updates from the directory. The **Full Sync** button on this page performs a full sync with Active Directory or Oracle Unified Directory, and the **Incremental Sync** button performs incremental sync with Active Directory or Oracle Unified Directory. If a mismatch of users or groups occurs between the directory and the Mobile Security Administrative Console, performing **Full Sync** could resolve the issue.

8.7 Notification Settings

This tab enables you to provide Mobile Security Notification Server configuration details. Initial settings are entered during installation, but you can change them here after installation. The fields are:

- Server URL
- Service user
- Service password
- Confirm password

After initial Mobile Security Notification Server settings have been configured, you can select one of the following tabs to configure settings:

- Exchange Server Settings
- Notification Settings
- APNS Certificate Settings
- Log Level Settings

8.7.1 Exchange Server Settings

This is the tab to configure Exchange server settings. For more information about Exchange, see `http://msdn.microsoft.com`.

- **Exchange domain** is a required field and is exchange server domain name.
- **Heart beat frequency** specifies how frequently exchange server should ping the Mobile Security Notification Server.
- **Exchange server EWS URL** is a required field and specifies the Exchange Web Service URL exposed by exchange server for Mobile Security Notification Server to connect to.
- **Exchange version** specifies the version of the exchange server.
- **Exchange service username** is a required field and specifies which user credential to use to communicate with the exchange server.
- **Exchange service password** and **Confirm password** fields are required and must match

The Mobile Security Notification Server uses Exchange Impersonation required Exchange Web Services API. The service account does not need to have a mailbox account. Instead, it only has an AD account. The configuration is different for exchange 2007 than for exchange 2010.

- Exchange 2007

Create the Service account and then set permissions on both the service account in Exchange and the user accounts in Active Directory or Oracle Unified Directory. This allows the service account to act on behalf of the user accounts.

One permission authorizes the Service Account access to Exchange Impersonation rights on the Client Access Server (CAS). The other is applied to either an AD account or an entire Mailbox database, either on an account-by-account basis, or on the entire mailbox database. It is recommended that the service account be given rights for the entire mailbox database.

Exchange 2007 requires that you apply two permissions to be able to get Exchange Impersonation working:

`oms-Exch-EPI-Impersonation`: This right is applied to the Client Access Server and grants the Service Account permission to function as an Exchange Impersonation account on that CAS.

`oms-Exch-EPI-May-Impersonate`: This right is applied on either a user-by-user basis for each of the users that require impersonation to be enabled, or it can be applied on a mailbox database. In this example `"EWS Proxy"` is the name of the service account used.

```
Add-ADPermission -Identity (Get-ExchangeServer -Identity <your CAS>).DistinguishedName
  -User (Get-User -Identity "EWS Proxy").Identity
  -extendedRight ms-Exch-EPI-Impersonation
```

Set the permissions on each user for which you want to enable Exchange Impersonation on the exchange server.

```
Add-ADPermission -Identity (Get-User -Identity "<User1").DistinguishedName
  -User (Get-User -Identity "EWS Proxy").Identity
  -extendedRight ms-Exch-EPI-May-Impersonate

Add-ADPermission -Identity (Get-User -Identity "User2").DistinguishedName
  -User (Get-User -Identity "EWS Proxy").Identity
  -extendedRight ms-Exch-EPI-May-Impersonate
```

- Exchange 2010

  Exchange 2010 requires that you apply the rights to be able to get Exchange Impersonation working.

  The service account must have management scope of all AD users in control group (for example: Notification Server Users). Configure this scope as follows.

  ```
  New-ManagementScope -Name:"ExchImpersonationScope"
         -RecipientRestrictionFilter {memberofgroup -eq
         "CN=BNS Users,OU=QA,DC=bitzerqa1,DC=com"}
  ```

  Define Assign Role

  ```
  New-ManagementRoleAssignment -Name:"ExchImpersonationRole"
          -Role:ApplicationImpersonation
       -User:"ewsproxy@bitzerqa1.com"
          -CustomRecipientWriteScope:"ExchImpersonationScope"
  ```

8.7.2 Notification Settings

This tab is used for defining notification message format and proxy settings

Include the email sender in the notification message. If **Yes** is selected, sender details are included in the notification message

Include the email subject in the notification message. If **Yes** is selected, subject details are included in the notification message

Use proxy for sending notifications. Selecting **Yes** causes the following four input fields to appear. Use these to specify the proxy details which are used to send notification messages. The proxy server is used to access the internet, if it is configured in your enterprise.

- Proxy host name is a required field and specifies host name of the proxy server
- Proxy host port is a required field and specifies port on which the proxy server listens
- Proxy host username and password are required fields. They specify user name and password which are used to authenticate with the proxy server

8.7.3 APNS Certificate Settings

Use this tab for Apple Push Notifications (APNS) certificate configuration.

The APNS certificate file is mandatory and is used to authenticate the Mobile Security Notification Server with the Apple Push Notification Server. The certificate uploaded here must be trusted by the Apple APNS server to push notifications. More information can be found on the Apple development website: `http://developer.apple.com`

- **APNS certificate name** is mandatory and defaults to the certificate file name uploaded, but can be changed.
- **APNS certificate password** and **confirm password** are mandatory and must match. This password is required to decrypt the APNS certificate file.

8.7.4 Log Level Settings

Use this tab for enabling or disabling debug logging on the Mobile Security Notification Server.

Set **Enable debug logging** to **yes** to produce verbose logging on Mobile Security Notification Server. Mobile Security Notification Server logs are stored in:

`install_dir/BMAX/as/logs/bns*`

8.8 CA Settings

Use this tab for creating new PKI certificate profiles and CA connections. Mobile Security Administrative Console currently supports only connections to Microsoft CA Servers.

To add a new template, select **Add Certificate Profile**, then enter the following information:

- **Cert Authority Type**: Select appropriate CA.
- **CA Authority**: Enter the name of the CA.
- **CA Hostname**: Enter the hostname of the server where CA resides.
- **CA Template**: Enter the name of the cert template to use.
- **Generation**: Select whether the template imported should be a new one or an escrowed cert.

9 Help

Use the Help tab to view the guide. The**?** icon on each page directs you to the correct section of the manual. The entire manual can be downloaded as a zipped PDF.

10 Notes

We consider the following important bits of information useful to reiterate.

- The Search box enables string matching of names of Containers, Groups, Users, Catalogs, and Policies.

- The Add New and Edit screens of all functions are identical. All information entered requires a Save before you leave the screen.
- Clicking Export in Containers gives you a `.csv` file of your containers, which can be viewed in MS Excel™ or any spreadsheet viewer available.
- The Default group cannot be deleted.
- Multiple policies combine if they are Access related (for example: vApp, Time, Geo).
- When you modify or create a new Container, Group, User, Catalog, or Policy, you must click save Save before leaving the page or your work will be lost when you go to another page or refresh the screen.

11 Related Documents

For more information, see the following documents in the Oracle Mobile Security Suite documentation set:

- *Oracle Mobile Security Suite Application Containerization Tool Guide*
- *Oracle Mobile Security Suite Customization and Branding Guide*
- *Oracle Mobile Security Suite Installation Guide*
- *Oracle Mobile Security Suite Release Notes*
- *Oracle Mobile Security Suite Troubleshooting Guide*

12 Documentation Accessibility

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website at http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc.

Access to Oracle Support

Oracle customers have access to electronic support through My Oracle Support. For information, visit http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info or visit http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs if you are hearing impaired.

Oracle Mobile Security Administrative Console Guide, Release 3.0
E51933-01