SOTI

MobiControl v12: Migration to Profiles Guide

December 2014

SOTI

Table of Contents

Introduction

MobiControl v12 redesigns the method by which administrators create and distribute device configurations to managed devices. The new design, referred to as “profiles”, allows administrators to group configurations according to user persona, job role, region, etc. and distribute the configurations as a *profile* to devices that match defined properties.

This *Migration to Profiles Guide* describes the outcome when legacy device configurations are migrated to profiles during the upgrade to MobiControl v12. This document does not cover standard practices for the installation or upgrade of MobiControl environments and assumes that you have basic knowledge, and administrative access to all MobiControl components including the database.

For consultation and/or support of your MobiControl upgrade please **contact** SOTI’s Professional Services and Support teams.

Comparison of Legacy Device Configurations to Profiles

Legacy Device Configurations

Prior to MobiControl v12, device configurations such as Email, WiFi, Authentication Policy, etc. are individually created at a node in the MobiControl device group tree via a contextual “Device Configuration” menu. Upon creation, the configuration is distributed to devices that are members of the selected device group, and child device groups through *inheritance*.

The following conceptual illustration shows an “Authentication Policy” (represented by blue shadding) configured at the root device group “My Company” and is inherited by all child device groups.

Figure 1 - Authentication Policy Created at "My Company"

Where a device configuration is not applicable to child device groups it can optionally be disabled or *overridden* with another configuration of the same type. Using the same device group hierarchy from the previous example, the following illustration represents each override of the authentication configuration with a different shade of blue. In this case the policy was overridden at “Canada” and “USA”.

Figure 2 - Authentication Overridden at Two Child Device Groups

When multiple configuration types are configured, they can each be overridden at different child device groups as demonstrated below.

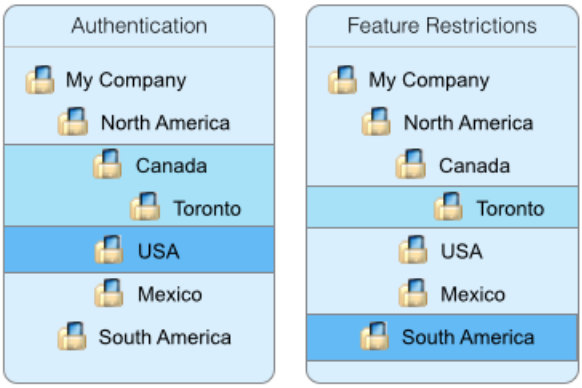

Figure 3 - Multiple Configurations with Unique Overrides

Overview of Profiles

The *device group-centric* approach to device configuration in v11 and earlier provided a simple and effective method of configuring devices organized by a device's group membership. On the other hand, device configurations applied to a device group lacked the context of what devices and associated user actually reside in the group. As a result many MobiControl device group hierarchies would grow to include model-specific device groups to account for model-specific configurations, which could become cumbersome over time.

MobiControl v12 introduces *profiles* to improve device configuration by de-coupling the configuration from the target devices, and provide a distribution method that accounts for device specific, and even user specific, requirements.

Creating a Profile

A profile is a group of configurations that in and of itself represents the needs of a user (a "persona"), or more broadly, common configurations required by a geographical region for example. Administrators may create multiple profiles that are referenced by name and can contain as many or as few configurations as desired; these configurations are referred to as payloads.

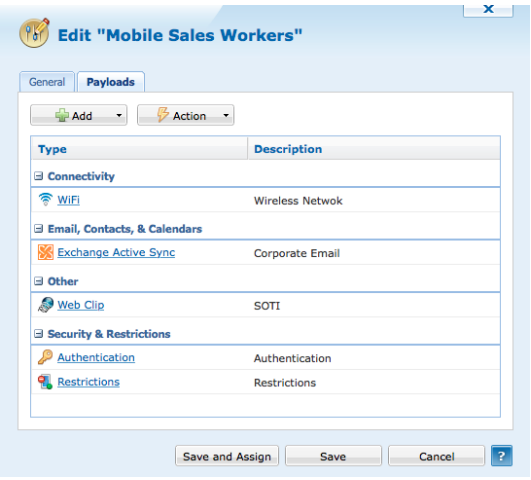

Figure 4 - Example Profile with Multiple Payloads

A profile is created under a new “Profiles” tab at the bottom of the MobiControl Web Console where all profiles can be found listed by name, platform, and other identifying attributes. Profiles can be saved and edited multiple times before being distributed to devices.

	Status	Name	Install Method	Version	Payloads	Assigned Date	Assigned By
	Assigned	Feature Restrictions	Automatic	3	1	2014-12-19 5:55:00 PM	Administrator
	Assigned	Global Authentication Policy	Automatic	1	1	2014-12-16 9:28:06 AM	gwatts
	Assigned	Mobile Sales Workers	Automatic	2	4	2014-12-16 10:58:37 AM	Administrator
	Assigned	Profile Catalog	Automatic	1	1	2014-12-11 5:11:59 PM	MobiControl Administrators

Figure 5 - Profile List

Profile Assignment & Distribution

Using the “Assign” action, MobiControl administrators can define target criteria that will narrow the selection of devices to those matching the defined characteristics. Some of the possible target criteria options include:

- Device group membership
- Devices properties such as model, manufacturer, OS version, encryption status, etc.)
- Custom attributes defined in the web console
- Custom data obtained from the device
- Devices where the associated user is a member of defined LDAP groups

Devices that match the defined target criteria will be assigned the profile, which will then be distributed to devices for installation. The following illustration demonstrates how the profile remains independent until assigned to the target criteria, and in turn devices.

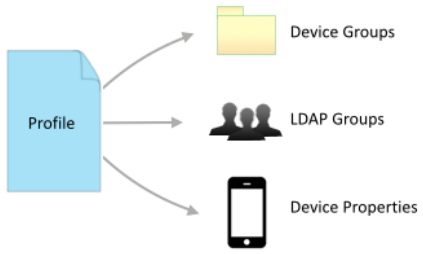

Figure 6 - Profile Assignment to Multiple Target Criteria

Profile Permissions

The standard “Global Permissions” section of MobiControl’s console security architecture provides administrative rights to administrators to “View and Manage” profiles. In addition MobiControl v12 introduces a new access control mechanism where administrative rights can be defined to the profile itself. This allows for even more granular control over which administrators can manage profiles.

Administrators with the “Read” privilege may only view the profile and its assignment, while administrators with the “Read & Write” privilege may edit and assign the profile.

Migration to Profiles

During upgrade to MobiControl v12, all legacy device configurations will be migrated to profiles and will appear under the “Profiles” tab in the web console. Profiles are migrated in such a way that devices remain untouched during and after the upgrade process.

Device Configurations to Profiles

The following logic is used to migrate legacy device configurations to profiles:

Creation

- Device configurations for each platform (iOS, Android, Windows Mobile, etc.) will be migrated independently. In other words profiles, like legacy device configurations, are platform specific.
- Each device configuration type (WiFi, VPN, Email, etc.) will be migrated to a profile containing a single payload with the corresponding configuration.
- Device configurations that contain certificate dependencies will be migrated to a profile with two payloads: the primary configuration, and the dependent certificate configuration.
- A profile will be created each time the configuration was overridden in the device group hierarchy.
- Identical device configurations will be migrated to create a single profile.

Assignment

- Profiles will be assigned to the device group where the legacy device configuration was created excluding any child device groups where the policy was overridden.
- Profiles that were created as a result of identical device configurations will target multiple device groups.

Naming Convention

- Profiles will assume the name of the device configuration type followed by the name of the target device or device group. For example “WiFi > Device Group”.
- Profiles that were created as a result of identical device configurations assume the name of the device configuration type followed by “Multiple Targets”. For example “Email > Multiple Targets”.

Permissions

- All MobiControl administrators that previously had the “Configure Devices/Device Groups” global permission will be granted the “View and Manage” profiles permission.
- The default “MobiControl Administrators” group is granted “Read & Write” access to all profiles.

Execution Status

- iOS profiles will reflect the true installation state of the device configuration reported prior to upgrade.
- Windows Mobile/CE/Desktop and Android Profiles will mark all profiles as “Installed”. Installation status of device configurations for these platforms was not recorded prior to MobiControl v12.

Examples

The following provides a visual representation of the migration logic. With each example, the legacy device configuration is shown on the left and the profiles created as a result of the migration, on the right. The corresponding target device group assignments are shown below the profile.

NOTE:	For the sake of clarity only a single device configuration type is shown in these examples. In a real migration the process is repeated for each device configuration type and any respective overrides.

Device Configuration with Overrides

The following illustration represents the most common migration scenarios where each overridden device configuration is migrated to a profile of its own and the device group assignment criteria set to where the override occurred.

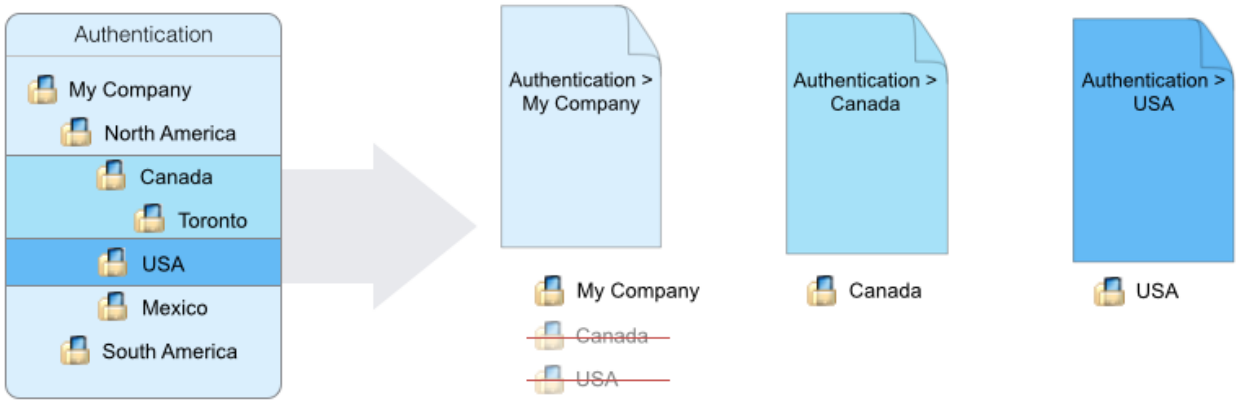

Figure 7 - Migration of Multiple Overridden Configurations

Identical Device Configurations (Merged Profile)

The following example assumes that the same exact authentication configuration policy was defined at both the “USA” and “South America” device groups. In order to reduce the number of profiles the migration process will merge the identical configuration and adjust the target device group assignments accordingly.

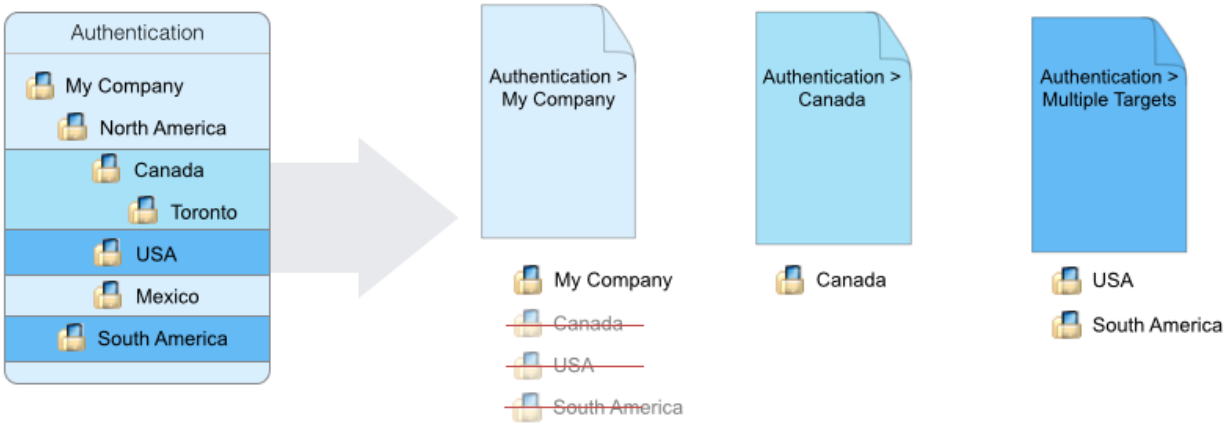

Figure 8 - Migration Resulting in Merged Profile

Pre Upgrade

To ensure the smoothest upgrade experience the following considerations should be taken into account in addition to any standard upgrade practices such as data backups, documentation review, etc.

Optimizing Migration

Profiles allow for more efficient use and re-use of configurations, a feature that was not available in prior versions of MobiControl. As a result, the migration procedure may create more profiles than you otherwise would have created yourself if starting with profiles.

The level of device configuration complexity in your existing MobiControl environment will weigh heavily on the number of profiles created during upgrade. The following factors affect how many profiles will be created:

- Many device-level configurations
- Many “overridden” device configurations on child device groups
- Many *root* device groups

You may take measures to reduce the number of profiles before upgrade by considering the aforementioned factors.

Assessing Migration Outcome

To assess how many profiles will be created, an SQL script is provided that can be run prior to upgrade which will output the number of profiles created for each platform. Use “SQL Management Studio” to run the script against your MobiControl database. The script requires database “Owner” privileges to execute successfully and can be obtained at the following URL:

https://www.soti.net/files/shared/UpgradeV12PreCheck.sql

The MobiControl installer will also provide you with a summary of the migration results where you can choose to proceed or cancel the upgrade before changes are made.

IMPORTANT: Please **contact** SOTI Support to discuss optimizations should any platform migration result in more than 200 profiles.

Staging Upgrade in Pre-production Environments

SOTI strongly encourages the standard IT change control practice of testing upgrades thoroughly in pre-production environments before being transitioned into production. If you

currently do not follow these IT practices with MobiControl please **contact** SOTI's Professional Services and Support Team for consultation before proceeding with your upgrade.

After Upgrade

Having successfully completed the upgrade to MobiControl v12, you are ready to take full advantage of the features profiles has to offer. During the migration process however MobiControl made several decisions that you should review and adjust as necessary.

Permissions

- Review the permissions that are configured on each profile and provide access to the correct administrator. By default "MobiControl Administrators" have been given full read and write access, but if a user is not a member of that group, they will not see any profiles.
- Where device configurations from two or more device groups are merged into a single profile it may target device groups that the original administrators did not have access to. The administrator may be able to see the profile, but not make changes to it.

Profile Consolidation

- The migration procedure will attempt to merge identical configurations into a single profile to reduce the overall number. Slight differences in configurations however will result in multiple profiles. You may wish to consider consolidating these configurations into a fewer profiles while also consolidating multiple configuration types into a single profile to build a person-based profile.

IMPORTANT: Profile consolidation will result in device-level changes. Be sure to plan the consolidation to account for the impact these changes have on the device while also avoiding conflicts between two profiles.