

SOTI[®]

ENTERPRISE MOBILITY MANAGEMENT

Proven Mobility Management

MobiControl v14 Upgrade Guide

OCTOBER 2017

Copyright © 2017 SOTI Inc.

All rights reserved.

This documentation and the software described in this document are furnished under and are subject to the terms of a license agreement or non-disclosure agreement.

Except as expressly set forth in a license agreement, you agree that you shall not reproduce, store or transmit in any form or by any means, electronic, mechanical, or otherwise, all or any part of this document or the software described in this document.

The specification and information regarding the products in this document are subject to change without notice and contains information confidential and proprietary to SOTI. All statements, information, and recommendations in the following documentation are believed to be accurate but are presented without warranty of any kind, expressed or implied. Users must take full responsibility for their application of any products.

In no event shall SOTI Inc. or its affiliates be liable for any indirect, special, consequential, or incidental damages, including without, lost profits or loss or damage to data arising out of the use or inability to use this documentation as recommended, even if SOTI Inc. or its affiliates have been advised of the possibility of such damage.

SOTI Inc. and the SOTI Inc. logo and products are trademarks or registered trademarks of SOTI Inc. and/or its affiliates in Canada and other countries.

Contents

INTRODUCTION	4
UPGRADE CONSIDERATIONS	5
Transition to New Administrative Console	5
Infrastructure Requirements (On-premises Only).....	5
Host Requirements.....	6
Network Requirements.....	6
SQL Permissions	7
End of Life Notices.....	7
Security.....	8
Console Security Permissions	8
Console Security – Conflicting Local and Directory Usernames	9
Communication Security	9
Device Agent Compatibility	10
Remote Control	11
Potential Failures on Upgrade.....	11
Platform Signed Samsung Agents.....	11
SQL Permissions	12

Introduction

MobiControl v14 marks a considerable milestone in an ever-expanding mobile and IoT connected landscape by simplifying day-to-day device administration with a re-designed administrative console, new support for Linux-based devices, and extended integration capabilities to automate further within an organization.

As with any major software release, MobiControl v14 includes a number of technical changes that you must evaluate and plan for prior to a production upgrade. Furthermore, this release contains an element of learning management that, depending on the size of your deployment, should be incorporated into your upgrade plan to successfully adopt the new technology and value provided.

This document serves as an extension to the MobiControl traditional release notes and provides in-depth information about some of the technical differences between the MobiControl v14 release, and earlier versions that may affect your upgrade. SOTI strongly encourages an upgrade approach that incorporates validation and feedback from administrative and device users that may be impacted by the upgrade.

For assistance with upgrade planning, or to schedule the upgrade of your MobiControl Cloud environment please contact SOTI's professional services and support teams:
<https://www.soti.net/about/contact/>

For a complete list of changes included in MobiControl v14 please refer to:
<https://www.soti.net/services/support/release-notes/soti-mobicontrol/>

Upgrade Considerations

The following highlights specific considerations that should be incorporated into your upgrade plan when deploying MobiControl v14. The MobiControl release notes, includes an exhaustive list of changes, while this information provides more depth on areas that may require additional attention or explanation.

This document assumes you are upgrading from v13.3. If you are upgrading from a version of MobiControl earlier than v13.3, you must consider the entire release history from the version you are running.

Transition to New Administrative Console

MobiControl v14 introduces a new administrative console that has been redeveloped from the ground up and is improved both aesthetically and functionally. Despite any visual improvements, the new layout will feel familiar to MobiControl administrators. Devices are still organized on the left with the primary list of devices appearing in the center of the page. The true value of the new console presents itself with in the richness and accessibility of device information, and the simplicity and transparency when interacting with devices.

The MobiControl v14 Administrative Console Transition Guide provides a complete list of improvements and changes to aid in your upgrade planning and any training requirements needed as a result of these improvements. To download this guide, refer to:

<https://www.soti.net/files/shared/MobiControl/MobiControlv14ConsoleTransitionGuide.pdf>

Infrastructure Requirements (On-premises Only)

MobiControl v14 includes a number of new technologies that change both the host and network requirements for MobiControl. If you are a MobiControl Cloud customer you have the advantage of not worrying about these considerations because SOTI provides the infrastructure for your deployment, and the network requirements are not specific to device communication.

Host Requirements

The most substantial infrastructure change in MobiControl v14, is the introduction of a 3rd Windows service called "MobiControl Search". This service is responsible for indexing critical device information to provide the incredible granularity and performance of the improved search feature of the administrative console.

In deployments with MobiControl components distributed across separate hosts, the MobiControl Search service will be installed exclusively on the MobiControl Management Sever. Wherever the Management Server is installed, the following hardware considerations should be taken into account:

- MobiControl Search will store roughly 2% of the total database size on this host. The data will be stored in the MobiControl installation directory, but is only a copy of what is in the database. It can be restored by re-indexing the database if ever lost, but not vice versa.
- MobiControl Search relies heavily on the availability of RAM. Performance of the search in the administrative console will be directly attributed to the availability of this resource on the Management Server. Consider increasing the amount of RAM on this host relative to the size of your device deployment.
- If you monitor the MobiControl services, you should add the MobiControl Search service to the monitoring solution. Should the Search service be offline, not only will no devices appear in the console, but the index consistency will begin to drift from the database. A full synchronization is performed nightly (by default), and can be customized in the MobiControl Search Sync Interval of Global Settings.

In addition to the MobiControl Search Service, the Management Server/Service is now responsible for processing virtual group memberships. This too will increase the load on the Management Server, but ensures better performance on the Deployment Servers, and reduces databases transactions.

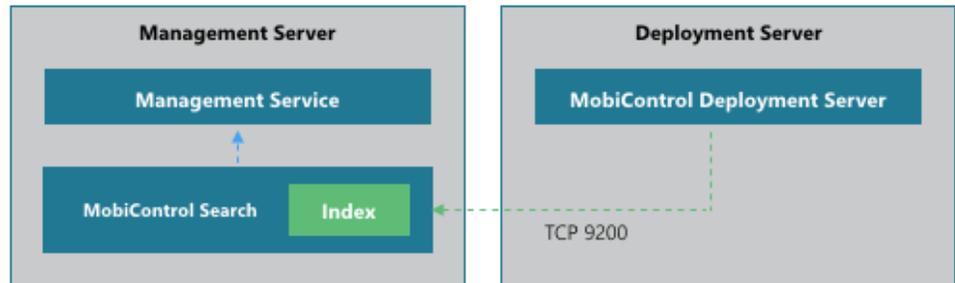
For a complete list of MobiControl system requirements please refer to:

<https://www.soti.net/mc/help/v14.0/en/setup/helpindex.html?helpid=systemreqs>

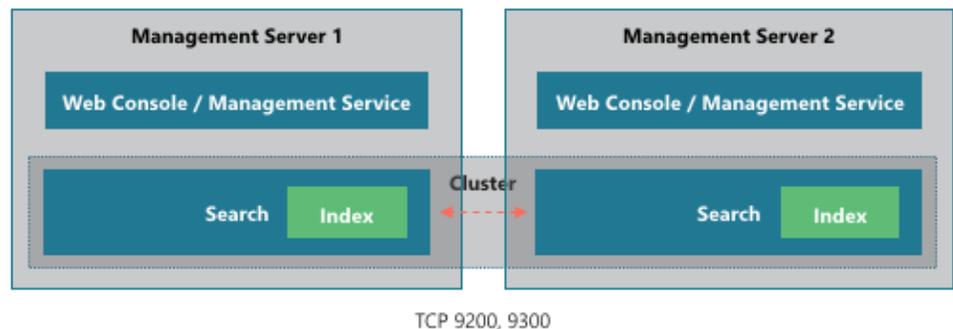
Network Requirements

In distributed MobiControl deployments, the MobiControl Search service changes the communication requirements between the MobiControl Deployment Server and the Management Server. There are no other inbound or outbound network changes with respect to MobiControl v14, and for smaller environments where all services are consolidated on a single host, the following changes do not apply:

- In addition to the existing communication requirements, the Deployment Server and the Management Server must now also communicate over TCP 9200 as illustrated.



- Where multiple Management Servers are deployed both Management Servers must also be able to communicate with each other over TCP 9200 and TCP 9300 in addition to the existing communication requirements.



For a complete list of MobiControl network requirements please refer to:
<https://www.soti.net/mc/help/v14.0/en/setup/helpindex.html?helpid=networkports>

SQL Permissions

SOTI has taken a number of steps to help reduce the privileges the database user must have for MobiControl to operate. As a result, you may wish to re-evaluate the rights provided to this user during regular operation, however refer to **SQL Permissions** for upgrade requirements.

For a complete list of MobiControl SQL permission requirements please refer to:
<https://www.soti.net/mc/help/v14.0/en/setup/helpindex.html?helpid=systemreqs>

End of Life Notices

As of v14, SOTI has ended support of MobiControl deployments installed on Windows Server 2008 and/or those using Microsoft SQL Server 2008 to host the MobiControl database. Upgrading to MobiControl v14 is not expected to fail in these deployments, however you are

strongly encouraged to upgrade to a supported host operating system and database infrastructure prior to upgrade in order to receive support.

Windows Server 2012 or higher, and SQL Server 2014 are the minimum recommended products for deploying MobiControl. Support for Windows Server 2016, and SQL Server 2016 is also provided with MobiControl v14.

SOTI maintains a list of supported versions of 3rd party products MobiControl is dependent upon and attempts to provide you with an estimate for when support will end given a particular product and version. Please refer to:

<https://docs.soti.net/end-of-life-notice/>

Security

Console Security Permissions

MobiControl v14 introduces more granular permissions to support tiered administrative models, most notably for device actions. For example, in prior versions most device actions were bundled under a single "Send Action Commands" permission which resulted in a tradeoff between an administrator not being able to perform any action vs the risk of performing undesired actions. MobiControl v14 solves this challenge by providing an individual permission for each device action, amongst others.

During upgrade the following will occur:

- Administrative users that had the "Send Action Commands" permission will be provided all action permissions except for those actions which had their own permission previously.
- Permissions "Send Scripts", "Send Message", have been moved under the "Send Action Command" parent permission, and are enabled for the user if they had the permission prior to upgrade.
- Administrative users that had the "Manage Devices" permission will be provided the "Edit Custom Attribute Values", "Manage Notes", and "Edit Device User" permissions.

In addition to action permission granularity, a new "Target Group" permission has been introduced for each device group. This permission restricts users from assigning or editing profiles or rules that target device groups they do not have the "Target Group" permission for and allows for more complex workflows for policy distribution.

During upgrade the following will occur:

- Administrative users that had the “View Group” permission on any device group will be given the “Target Group” permission for the respective group.

Given this increased granularity, we strongly encourage you to review your administrative model to identify areas where permissions can be limited before and after upgrade. For clarity, after upgrade these changes do not allow administrators to perform functions they weren't previously authorized to perform, you just now have the option to restrict them further.

Console Security – Conflicting Local and Directory Usernames

In addition to local administrative users, MobiControl provides integration with directory services such as LDAP and SAML-based identify providers for the purpose of authenticating to the administrative console.

Albeit a rare scenario, if a local username conflicted with a directory username, MobiControl previously favored the administrative user that was created in the system first. This could lead to inconsistent behavior and confusion about why some users couldn't login.

With MobiControl v14, local users will always have priority during login. Should a local user conflict with a directory user, the directory user must now prefix their username with their respective domain to login. Should there be no conflict, the directory user does not require the domain prefix.

We recommend that you review this scenario prior to upgrade and identify any users that may have difficulty logging in after upgrade and disseminate the new login procedure.

Communication Security

MobiControl v14 introduces full support for SHA2 certificates for both the MobiControl services and client certificates issued to devices. By default, all new installations will include certificates with a SHA2 signature algorithm while upgraded environments will continue to use the certificates previously bound to the services, no matter the issuer or signature algorithm.

After upgrade, you should consider migrating to SHA2 certificates. While there is no SOTI requirement to do so, not migrating has the following implications:

- As the industry deprecates SHA1 certificates further, web browsers may begin to warn that MobiControl is untrusted despite having trust via the MobiControl root certificate

- Communication with MobiControl components is be considered less secure than the SHA2 alternative

MobiControl v14 also introduces official support for the exclusive use of TLS 1.2. MobiControl leverages the standard communication frameworks provided by Windows to create secure channels of communication with devices. Refer to the following Microsoft KB article on configuring TLS settings:

<https://docs.microsoft.com/en-us/windows-server/security/tls/tls-registry-settings>

IMPORTANT: Changing TLS and/or certificates can have a catastrophic impact in the communication MobiControl establishes with devices. Making changes without guaranteeing device trust can result in losing contact with the device. It is strongly encouraged that you consult the SOTI professional service and support teams for guidance in this matter.

For example, Windows Mobile/CE does not support TLS 1.2, and only some devices support for SHA2. You cannot migrate to these later technologies if the devices don't support them.

MobiControl Cloud customers may request changes to certificate and TLS settings via SOTI Support.

Device Agent Compatibility

MobiControl device agents often receive updates along with the update of the MobiControl server. In MobiControl v14, the following agents must be upgraded in the described manner:

- Android+ if less than v13.3 can be upgraded through the administrative console
- Android devices managed using the "Android Enterprise" (formerly Android for Work) must be running v13.4 or higher. These devices will be upgraded automatically by the Google Play apps store, if they haven't already.
- Windows Mobile/CE if less than v14.0.0 can be upgraded through the administrative console.

If an agent for your particular device manufacturer isn't available after upgrade you can download the latest version via:

<http://www.soti.net/oem>

Remote Control

The "HTML5" remote control console is no longer installed with MobiControl and will not be available after upgrade to MobiControl v14. The equivalent technology however is available when MobiControl is integrated with SOTI Assist whether a SOTI Assist license has been purchase or not.

If you are a MobiControl Cloud customer, SOTI Assist will be installed for you when your environment is upgrade to MobiControl v14.

Whether you deploy MobiControl on your premises, or leverage MobiControl Cloud, you should familiarize yourself with the differences between the "HTML5" remote control, and the SOTI Assist remote control console.

The legacy "plugin-based" remote control is not affected by this change, and is still available after upgrade to MobiControl v14.

For more information about SOTI Assist please refer to:

<http://www.soti.net/products/soti-assist/>

Potential Failures on Upgrade

Platform Signed Samsung Agents

In response to Samsung's deprecation of platform signing, SOTI has provided an administrative action in MobiControl to migrate platform signed device agents to ELM device agents since v11 (May 2014). Official support of Samsung "platform-signed" (non-ELM) agents ended with MobiControl v13.2 (August 2016).

Environments upgrading to v14 will be prevented from proceeding with the installation if devices managed using the platform-signed agent are discovered. An exemption to bypass this check can be provided by SOTI Support, however official support for non-ELM agents is not provided for these environments. Devices should be migrated to ELM prior to upgrade.

To verify if your devices support ELM, the "Supported APIs" property found in the MobiControl administrative console should read "MDMv4" or higher.

To verify whether you have platform-signed agents that would prevent upgrade leverage the "Samsung Platform-Signed Agents" report within MobiControl prior to upgrading.

For more information about ELM, and the ELM migration procedure please refer to:

[Migrating Devices to the ELM Agent](#)

SQL Permissions

During upgrade the MobiControl installer requires a temporary database to perform data migration procedures. Because of this requirement the service user that MobiControl uses to authenticate to the database must have the "sysadmin" rights to create and deploy the database, and later drop it.

Without this permission, the installer will fail to complete the upgrade. This failure is non-destructive in that you can return the system to its previous operational state.

If you are upgrading from a version earlier than v13.3, the MobiControl installer will also create a new database for data archiving purposes, which will also require this permission.

After upgrade, you may restore the service user's rights to the aforementioned permissions.