JP1 Version 11

JP1/IT Desktop Management 2 - Smart Device Manager

3021-3-B61-10(E)

Notices

■ Relevant program products

For details about the applicable OS versions, and the service packs and patches required for JP1/IT Desktop Management 2 - Smart Device Manager, see the *Release Notes*.

P-2A42-7EBL JP1/IT Desktop Management 2 - Smart Device Manager 11-10

JP1/IT Desktop Management 2 - Smart Device Manager consists of the following components:

JP1/IT Desktop Management 2 - Smart Device Manager (Smart Device Manager) (For Windows Server 2016, Windows Server 2012 R2, Windows Server 2012, Windows Server 2008 R2)

JP1/IT Desktop Management 2 - Smart Device Manager (Communication Server) (For Windows Server 2016, Windows Server 2012 R2, Windows Server 2012, Windows Server 2008 R2)

JP1/IT Desktop Management 2 - Smart Device Manager (Messaging Server) (For Windows Server 2016, Windows Server 2012 R2, Windows Server 2012, Windows Server 2008 R2)

JP1/IT Desktop Management 2 - Smart Device Manager (Smart Device Android Agent) (For Android 4.1 or later)

JP1/IT Desktop Management 2 - Smart Device Manager (Smart Device iOS Agent) (For iOS 7.1 or later)

■ Trademarks

HITACHI, JP1, Job Management Partner 1, uCosminexus are either trademarks or registered trademarks of Hitachi, Ltd. in Japan and other countries.

Internet Explorer is either a registered trademark or trademark of Microsoft Corporation in the United States and/or other countries.

Microsoft is either a registered trademark or a trademark of Microsoft Corporation in the United States and/or other countries.

Microsoft Exchange server is a product name of Microsoft Corporation in the U.S. and other countries.

Oracle and Java are registered trademarks of Oracle and/or its affiliates.

RSA and BSAFE are either registered trademarks or trademarks of EMC Corporation in the United States and/or other countries.

Windows is either a registered trademark or a trademark of Microsoft Corporation in the United States and/or other countries.

Windows Server is either a registered trademark or a trademark of Microsoft Corporation in the United States and/or other countries.

Other company and product names mentioned in this document may be the trademarks of their respective owners.

This product includes RSA BSAFE Cryptographic software of EMC Corporation.

This product includes software developed by the Apache Software Foundation (http://www.apache.org/).

This product includes software developed by Ben Laurie for use in the Apache-SSL HTTP server project.

This product includes software developed by IAIK of Graz University of Technology.

Portions of this software were developed at the National Center for Supercomputing Applications (NCSA) at the University of Illinois at Urbana-Champaign.

This product includes software developed by the University of California, Berkeley and its contributors.

This software contains code derived from the RSA Data Security Inc. MD5 Message-Digest Algorithm, including various modifications by Spyglass Inc., Carnegie Mellon University, and Bell Communications Research, Inc (Bellcore).

Regular expression support is provided by the PCRE library package, which is open source software, written by Philip Hazel, and copyright by the University of Cambridge, England. The original software is available from ftp://ftp.csx.cam.ac.uk/pub/software/programming/pcre/

This product includes software developed by Ralf S. Engelschall <rse@engelschall.com> for use in the mod_ssl project (http://www.modssl.org/).

This product includes software developed by the Java Apache Project for use in the Apache JServ servlet engine project (http://java.apache.org/).

This product includes software developed by Daisuke Okajima and Kohsuke Kawaguchi (http://relaxngcc.sf.net/).

This product includes software developed by Andy Clark.

■ Microsoft product screen shots

Microsoft product screen shot(s) reprinted with permission from Microsoft Corporation.

■ Microsoft product name abbreviations

This manual uses the following abbreviations for Microsoft product names.

Abbreviation			Full name or meaning
Exchange			Microsoft(R) Exchange Server
IE	Internet Explorer		Windows(R) Internet Explorer(R)
Windows	Windows Server 2008	Windows Server 2008 R2	Microsoft(R) Windows Server(R) 2008 R2 Datacenter
			Microsoft(R) Windows Server(R) 2008 R2 Enterprise
			Microsoft(R) Windows Server(R) 2008 R2 Standard
	Windows Server 2012	Windows Server 2012	Microsoft(R) Windows Server(R) 2012 Datacenter
			Microsoft(R) Windows Server(R) 2012 Standard

Abbreviation			Full name or meaning
Windows	Windows Server 2012	Windows Server 2012 R2	Microsoft(R) Windows Server(R) 2012 R2 Datacenter
			Microsoft(R) Windows Server(R) 2012 R2 Standard
	Windows Server 2016	Windows Server 2016	Microsoft(R) Windows Server(R) 2016 Datacenter
			Microsoft(R) Windows Server(R) 2016 Standard

■ Restrictions

Information in this document is subject to change without notice and does not represent a commitment on the part of Hitachi. The software described in this manual is furnished according to a license agreement with Hitachi. The license agreement contains all of the terms and conditions governing your use of the software and documentation, including all warranty rights, limitations of liability, and disclaimers of warranty.

Material contained in this document may describe Hitachi products not available or features not available in your country.

No part of this material may be reproduced in any form or by any means without permission in writing from the publisher.

■ Issued

Mar. 2017: 3021-3-B61-10(E)

■ Copyright

Copyright (C) 2016, 2017, Hitachi, Ltd.

Copyright (C) 2016, 2017, Hitachi Solutions, Ltd.

Summary of amendments

The following table lists changes in the manual (3021-3-B61-10(E))

Changes	Location
Pull-distribution functionality was added that allows users to initiate the installation of applications.	*2.6.2*, *4.2*, *4.11*, *9.11*, *9.12*, *9.13*, *9.14*, *15. sdmioutils exportdeliverypermit*, *15. sdmioutils importdeliverypermit*, *15. sdmioutils deletedeliverypermit*, *E.6*
Standard distribution functionality was added that allows the distribution of large applications.	*2.6.2*, *4.9*, *4.10*, *4.12*, *9.1*, *9.2*, *9.3*, *9.5*, *9.6*, *9.7*, *9.9*, *12.1*, *12.2*, *A.2*
The following commands were added: • sdmioutils exportdeliverypermit (exporting settings that define applications as installable by users) • sdmioutils importdeliverypermit (defining applications that can be installed by users) • sdmioutils deletedeliverypermit (deleting settings that define applications as installable by users) • sdmdistributeapp (sending instructions to install applications) • sdmapplyprofile (applying or removing an iOS profile) • sdmgetinvenroty (acquiring inventory information) • sdmexportdistributestatus (outputting application distribution status) • sdmexportinstallapp (outputting installed software information)	*8.6*, *9.6*, *9.7*, *9.9*, *9.11*, *9.12*, *9.13*, *12.3*, *15. Command List*, *15. sdmioutils exportdeliverypermit*, *15. sdmioutils importdeliverypermit*, *15. sdmioutils deletedeliverypermit*, *15. sdmdistributeapp*, *15. sdmapplyprofile*, *15. sdmgetinvenroty*, *15. sdmexportdistributestatus*, *15. sdmexportinstallapp*, *E.6*, *E.7*, *E.8*, *E.9*, *E.10*, *E.11*
Windows Server 2016 was added as a supported OS.	--

In addition to the above changes, minor editorial corrections were made.

Preface

This manual provides an overview of JP1/IT Desktop Management 2 - Smart Device Manager (abbreviated hereafter to *JP1/ITDM2 - SDM*) and describes its features. This manual also explains how to design and build a system, how to use JP1/ITDM2 - SDM, and provides operation examples.

■ Intended readers

This manual is intended for:

- Those who are considering installing JP1/ITDM2 - SDM or who want to design JP1/ITDM2 - SDM systems.
- Those who want to gain an overview of JP1/ITDM2 - SDM products and function details.
- Those who want to build a JP1/ITDM2 - SDM system.
- Those who want to learn how to build JP1/ITDM2 - SDM.
- Those who want to use JP1/ITDM2 - SDM to manage smart devices in the organization.
- Those who want to know how to use and operate JP1/ITDM2 - SDM.

■ Organization of the manual

This manual is organized into the following chapters.

1. Product Overview

This chapter provides an overview of JP1/ITDM2 - SDM, and describes its system components.

2. Features of JP1/ITDM2 - SDM

This chapter explains JP1/ITDM2 - SDM functions.

3. System Configuration

This chapter describes how to build a system.

4. Managing Smart Devices by Using JP1/ITDM2 - SDM

This chapter explains how to operate and utilize JP1/ITDM2 - SDM.

5. Starting and Ending Operations

This chapter explains how to start and end operations in JP1/ITDM2 - SDM.

6. Managing User Accounts

This chapter explains how to manage user accounts.

7. Managing the Security Status

This chapter explains how to manage security of the smart devices in an organization and how to understand the security status.

8. Smart Device Management

This chapter explains how to collect information from smart devices and how to grasp the current status in an organization.

9. Managing Applications

This chapter explains how to manage applications to be distributed to smart devices in an organization.

10. Event Reference

This chapter explains how to reference events that are output by JP1/ITDM2 - SDM.

11. Customizing Settings

This chapter describes the items that can be customized in the Settings module and during setup.

12. Database Management

This chapter explains how to manage a database by using the JP1/ITDM2 - SDM commands.

13. Troubleshooting

This chapter describes the actions to be taken when a problem occurs during operation of JP1/ITDM2 - SDM.

14. GUI Reference

This chapter describes the GUI of JP1/ITDM2 - SDM.

15. Commands

This chapter describes the JP1/ITDM2 - SDM commands.

16. Definition Files

This chapter describes the definition file of JP1/ITDM2-SDM.

17. Messages

This chapter lists the JP1/ITDM2 - SDM messages.

Contents

1 Product Overview

This chapter provides an overview of JP1/ITDM2 - SDM and its system components.

1.1 Product overview

The JP1/ITDM2 - SDM product manages smart device operations and provides security measures.

An increasing number of businesses use smart devices (such as smart phones and tablet PCs) as IT devices, requiring management of such devices in the same way as other IT devices.

JP1/ITDM2 - SDM supports management of smart device operation and security in an organization, and enables unified management of PCs, server devices, and smart devices from JP1/IT Desktop Management 2.

1.1.1 Product benefits

With JP1/ITDM2 - SDM, you can understand the current status of smart devices, ensure compliance with smart device usage guidelines, prevent information leakage if a device is stolen or lost, and distribute applications. JP1/ITDM2 - SDM also provides integrated management of IT assets.

The smart device administrator must manage all smart devices in a manner appropriate for the business goals of the organization. The administrator must also prevent users from using smart devices for non-business purposes, and take preventive measures against leakage of business information from smart devices.

JP1/ITDM2 - SDM supports unified management of smart devices based on the following points:

- Understanding the current status of smart devices
- Ensuring compliance with smart device usage guidelines
- Preventing information leakage if a smart device is stolen or lost
- Distributing applications to smart devices
- Integrated management of IT assets

Understanding the current status of smart devices

Increasing use of smart devices in the organization makes it difficult to know where (and by whom) devices are being used. JP1/ITDM2 - SDM displays a list of smart devices owned by the organization, enabling the administrator to easily understand smart device information. For example, the administrator can easily identify available devices and quickly distribute them as required.

Ensuring compliance with smart device usage guidelines

The smart device administrator must discourage use of smart devices for non-business purposes. JP1/ITDM2 - SDM applies security rules to smart devices in order to notify the administrator of a violation of rules, and to restrict a specific smart device function. For example, allowed phone numbers, Web sites, and applications can be defined in a security policy. If that security policy is applied to smart devices, any use of a disallowed phone number, Web site, or application will be reported to the administrator. In addition, use of smart device cameras can be prohibited if such functionality is not necessary for business purposes.

Preventing information leakage if a smart device is stolen or lost

JP1/ITDM2 - SDM can remotely lock or initialize a lost or stolen device to prevent unauthorized use or information leakage by a third party.

Distributing applications to smart devices

JP1/ITDM2 - SDM provides unified management of applications used for in-company business, and allows for simultaneous distribution of business applications to smart devices. This allows users in the organization to use the same applications, and simplifies the distribution process.

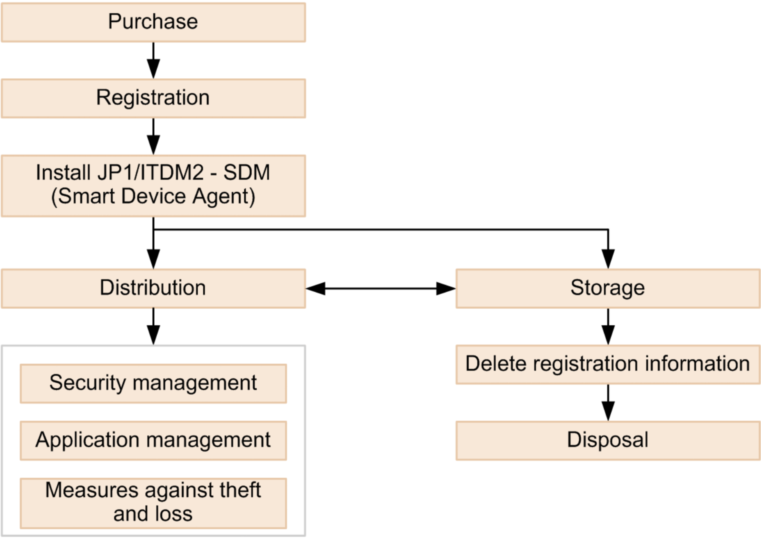
Integrated management of IT assets

Smart device information in JP1/ITDM2 - SDM can be viewed and manipulated from JP1/IT Desktop Management 2. This allows the administrator to manage smart devices in the same way as other IT assets (such as PCs and server devices), by simply using JP1/IT Desktop Management 2.

1.1.2 Flow of smart device management

JP1/IT Desktop Management 2 and JP1/ITDM2 - SDM manages smart devices from their initial purchase to final disposal, within an organization.

The following figure shows the flow from purchase to disposal of a smart device.


Purchase
Registration
Install JP1/ITDM2 - SDM (Smart Device Agent)
Distribution
Storage
Security management
Application management
Measures against theft and loss
Delete registration information
Disposal

When you purchase a smart device, register information about the device in JP1/ITDM2 - SDM. Install JP1/ITDM2 - SDM (Smart Device Agent) on the smart device, and then distribute the smart device to a user. Note that information about smart devices is subject to asset management in JP1/IT Desktop Management 2 in the same way as PCs and other devices.

For distributed smart devices, manage the security status and applications. If a user loses a smart device or if it is stolen, take action such as remotely locking or initializing the device.

If the smart device is currently not being used, change the setting to **Unmanaged**, and then store the smart device. If there is no plan to use the smart device later, delete the registration information from JP1/ITDM2 - SDM, and then dispose of the device.

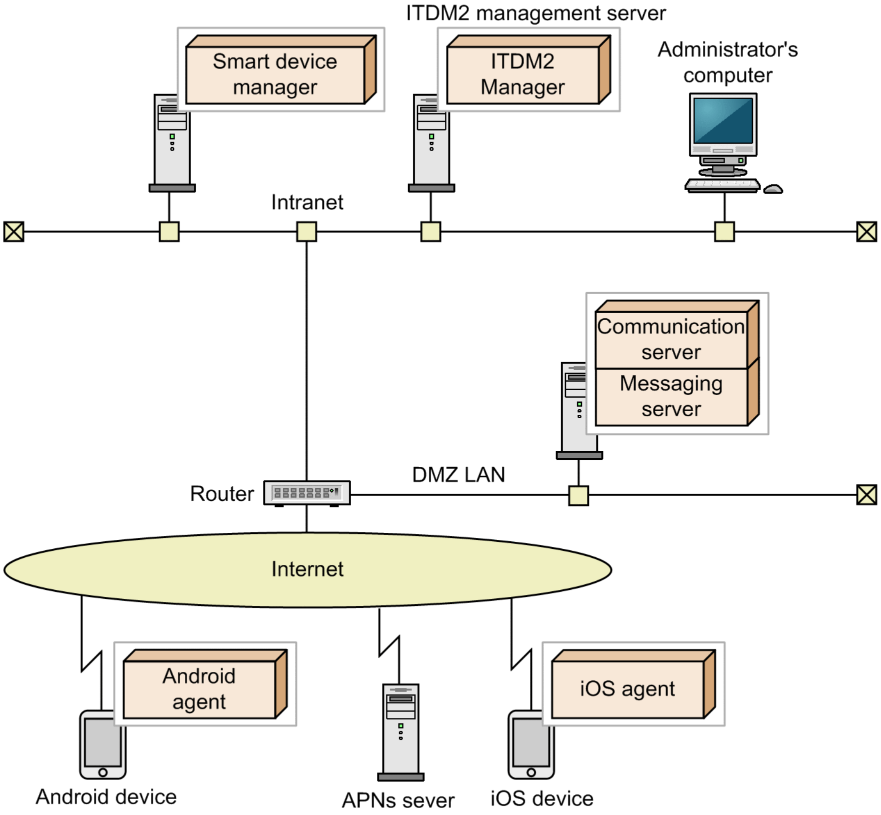
1.2 System components

In this manual, when referring to a system managed by JP1/ITDM2 - SDM, defined names are used for system components such as smart devices and the servers on which JP1/ITDM2 - SDM is installed.

The following table gives definitions used in JP1/ITDM2 - SDM for basic system components.

No.	Component name	Definition
1	Smart device manager	The server on which JP1/ITDM2 - SDM (Smart Device Manager) is installed as a relay system. A database for storing the various information managed by JP1/ITDM2 - SDM is created on the management server. One smart device manager can manage up to 2,000 smart devices.
2	ITDM2 management server	A component that manages IT assets (such as PCs and server devices) and smart devices, in a unified manner
3	Administrator's computer	A computer used by the administrator for on-screen operation of JP1/ITDM2 - SDM. The administrator displays JP1/ITDM2 - SDM program modules from a Web browser. Therefore, JP1/ITDM2 - SDM can be operated on any computer that can access the smart device manager. The smart device manager itself can be used as the administrator's computer.
4	Communication server	A server on which JP1/ITDM2 - SDM (Communication Server) is installed for data communication with smart devices. This server collects inventory information from smart devices and stores it in the database. If an inventory acquisition request, lock or initialization request, or policy application request is sent from the administrator, the communication server requests the smart device to perform processing.
5	Messaging server	A server on which JP1/ITDM2 - SDM (Messaging Server) is installed. This server provides synchronization between an Android device and JP1/ITDM2 - SDM. If an inventory acquisition request, lock or initialization request, or other request is sent from the administrator, this server requests the Android device to connect to the communication server.
6	Android device	An Android device on which JP1/ITDM2 - SDM (Smart Device Android Agent), which monitors and controls the Android device, is installed. The Android device sends smart device information (such as inventory and location information) to JP1/ITDM2 - SDM, and performs processing in response to a lock or initialization request from the administrator.
7	iOS device	An iOS device on which JP1/ITDM2 - SDM (Smart Device iOS Agent), which monitors and controls the iOS device, is installed. The iOS device sends smart device information such as inventory information to JP1/ITDM2 - SDM.
8	APNs server	An Apple server that controls iOS devices. An inventory acquisition request, lock or initialization request or other request from JP1/ITDM2 - SDM to an iOS device is sent via the APNs server.

The following figure shows an example of a basic system configuration consisting of these components and managed by JP1/ITDM2 - SDM.

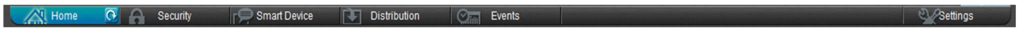


Related Topics

- *3.4 Components of JP1/ITDM2 - SDM*

1.3 Program modules

In JP1/ITDM2 - SDM you can access functions by clicking the buttons at the top and opening a different module.



The operations you can perform in each module are described next.

Home module

In the Home module, you can get an overview of the information managed by JP1/ITDM2 - SDM, presented in panels. From each panel you can navigate to another module to perform a management operation.

Security module

In the Security module, you can view the list of security rules defined for your organization. You can also understand which security rules apply to smart devices.

Smart Device module

In the Smart Device module, you can view the list of smart devices managed by your organization. You can also check hardware information and installed applications for managed smart devices, and perform remote operation on smart devices. This allows you to take action for smart devices that have security problems.

Distribution module

In the Distribution module, you can view the list of applications to be distributed to smart devices. You can also send instructions to distribute and install applications onto, or uninstall applications from, managed smart devices.

Events module

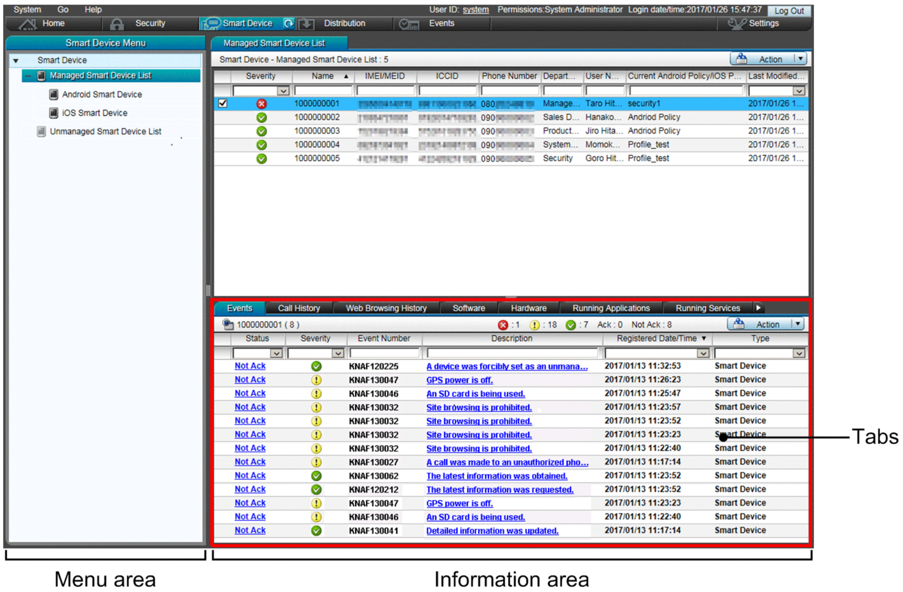
In the Events module, you can check events that occurred during JP1/ITDM2 - SDM operation.

Settings module

In the Settings module, you can customize a variety of JP1/ITDM2 - SDM information, such as user accounts and email notifications.

1.3.1 Basic module layout

The following describes the basic layout of the JP1/ITDM2 - SDM modules and the terminology used for the module components.


System Go Help
Home Security Smart Device Distribution Events Settings
Log Out
Smart Device Menu
Smart Device
Managed Smart Device List
Android Smart Device
iOS Smart Device
Unmanaged Smart Device List
Managed Smart Device List
Action
Events Call History Web Browsing History Software Hardware Running Applications Running Services
Tabs
Menu area
Information area

User ID: system Permissions:System Administrator Login date/time:2017/01/26 15:47:37

Smart Device - Managed Smart Device List : 5

	Severity	Name ▲	IMEI/MEID	ICCID	Phone Number	Depart...	User N...	Current Android Policy/iOS P...	Last Modified...
☑	✗	1000000001	[redacted]	[redacted]	080[redacted]	Manage...	Taro Hit...	security1	2017/01/26 1...
	✓	1000000002	[redacted]	[redacted]	090[redacted]	Sales D...	Hanako...	Andriod Policy	2017/01/26 1...
	✓	1000000003	[redacted]	[redacted]	090[redacted]	Product...	Jiro Hita...	Andriod Policy	2017/01/26 1...
	✓	1000000004	[redacted]	[redacted]	090[redacted]	System...	Momok...	Profile_test	2017/01/26 1...
	✓	1000000005	[redacted]	[redacted]	090[redacted]	Security	Goro Hit...	Profile_test	2017/01/26 1...

1000000001 (8) ✗ : 1 ! : 18 ✓ : 7 Ack : 0 Not Ack : 8

Status	Severity	Event Number	Description	Registered Date/Time ▼	Type
Not Ack	✓	KNAF120225	A device was forcibly set as an unmana...	2017/01/13 11:32:53	Smart Device
Not Ack	!	KNAF130047	GPS power is off.	2017/01/13 11:26:23	Smart Device
Not Ack	!	KNAF130046	An SD card is being used.	2017/01/13 11:25:47	Smart Device
Not Ack	!	KNAF130032	Site browsing is prohibited.	2017/01/13 11:23:57	Smart Device
Not Ack	!	KNAF130032	Site browsing is prohibited.	2017/01/13 11:23:52	Smart Device
Not Ack	!	KNAF130032	Site browsing is prohibited.	2017/01/13 11:23:23	Smart Device
Not Ack	!	KNAF130032	Site browsing is prohibited.	2017/01/13 11:22:40	Smart Device
Not Ack	!	KNAF130027	A call was made to an unauthorized pho...	2017/01/13 11:17:14	Smart Device
Not Ack	✓	KNAF130062	The latest information was obtained.	2017/01/13 11:23:52	Smart Device
Not Ack	✓	KNAF120212	The latest information was requested.	2017/01/13 11:23:52	Smart Device
Not Ack	!	KNAF130047	GPS power is off.	2017/01/13 11:23:23	Smart Device
Not Ack	!	KNAF130046	An SD card is being used.	2017/01/13 11:22:40	Smart Device
Not Ack	✓	KNAF130041	Detailed information was updated.	2017/01/13 11:17:14	Smart Device

Menu area

Menus are specific to the selected module. When you select an item here, corresponding information appears in the information area.

Information area

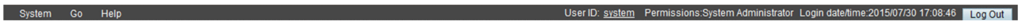
Displays information according to the item selected in the menu area.

Tabs

The tabs in the lower part of the information area show detailed information about any item selected in the upper part of the information area.

Menu bar

The menus at the top of screen are common to all modules.



User ID: system Permissions:System Administrator Login date/time:2015/07/30 17:08:46

System

Logs the user out of JP1/ITDM2 - SDM.

Go

Edits the user account of the logged-in user.

Help

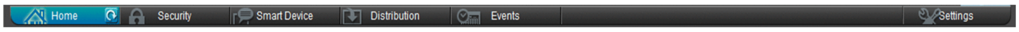
Displays the Help for JP1/ITDM2 - SDM and version information of the product.

Log Out button

Logs the user out of JP1/ITDM2 - SDM. The user ID, permissions, and login date/time for the user account of the logged-in user are displayed on the left of the **Log Out** button. Click the user ID to edit your account information or change your password.

Buttons at the top of the window

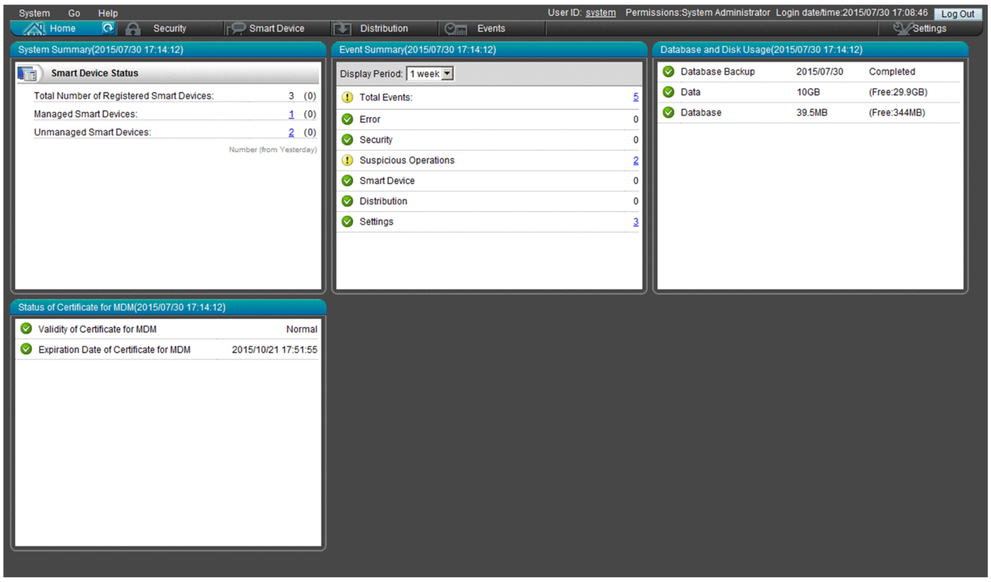
These buttons allow you to access functions by switching to another module.



1.3.2 Working with the Home module

The Home module appears immediately after the user logs in. This module works as the base point of JP1/ITDM2 - SDM operations.

In the Home module, each of the panels presents an overview of information managed by JP1/ITDM2 - SDM. These panels allow you to quickly check the status of information managed by each module.



User ID: system   Permissions:System Administrator   Login date/time:2015/07/30 17:08:46

System Summary(2015/07/30 17:14:12)

Smart Device Status

Total Number of Registered Smart Devices:	3	(0)
Managed Smart Devices:	1	(0)
Unmanaged Smart Devices:	2	(0)

Number (from Yesterday)

Event Summary(2015/07/30 17:14:12)

Display Period: 1 week

Total Events:	5
Error	0
Security	0
Suspicious Operations	2
Smart Device	0
Distribution	0
Settings	3

Database and Disk Usage(2015/07/30 17:14:12)

Database Backup	2015/07/30	Completed
Data	10GB	(Free:29.9GB)
Database	39.5MB	(Free:344MB)

Status of Certificate for MDM(2015/07/30 17:14:12)

Validity of Certificate for MDM	Normal
Expiration Date of Certificate for MDM	2015/10/21 17:51:55

After checking the status, click a button in a module (or a link in a panel) to navigate to another module, and then start management operation.

1.3.3 Working with the Security module

In the Security module, you can create security rules. By applying security rules to smart devices, you can manage the security status and take actions for smart devices that have security problems.

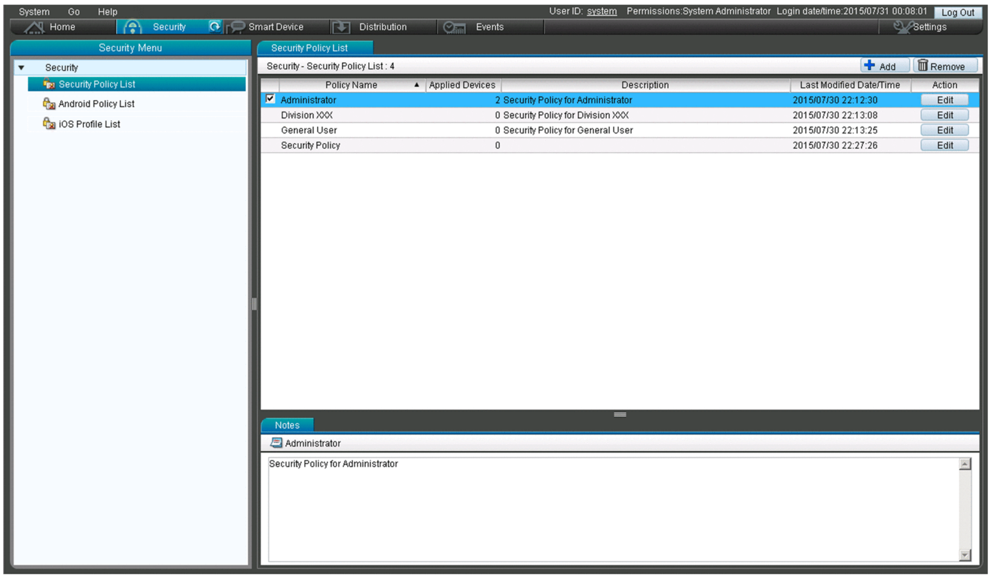
The Security module provides the following views:

- **Security Policy List** view
- **Android Policy List** view
- **iOS Profile List** view

Each view is described next.

Security Policy List view

You can create security policies, which can then be applied to smart devices.



Security - Security Policy List : 4

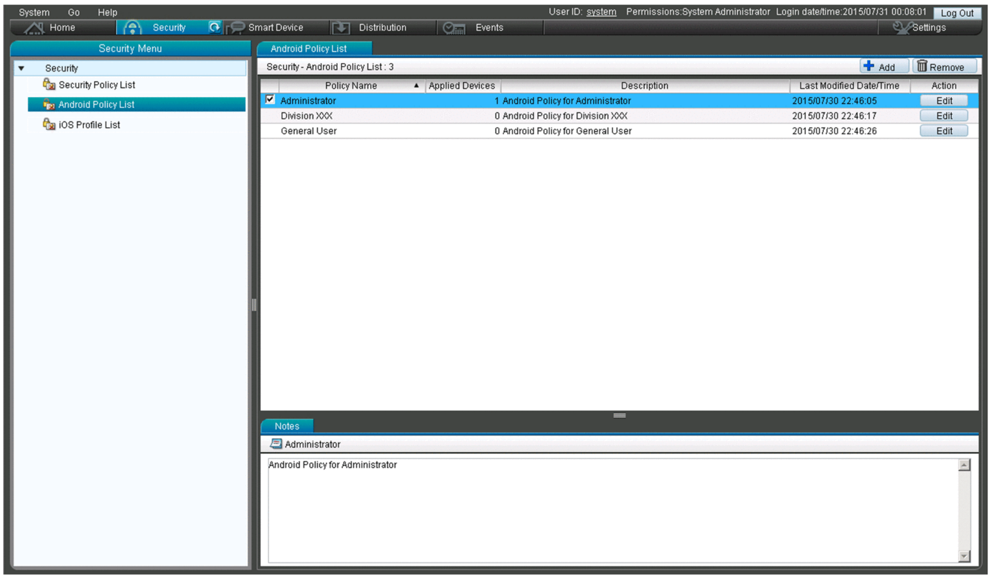
	Policy Name	Applied Devices	Description	Last Modified Date/Time	Action
☑	Administrator	2	Security Policy for Administrator	2015/07/30 22:12:30	Edit
	Division XXX	0	Security Policy for Division XXX	2015/07/30 22:13:08	Edit
	General User	0	Security Policy for General User	2015/07/30 22:13:25	Edit
	Security Policy	0		2015/07/30 22:27:26	Edit

Administrator

Security Policy for Administrator

Android Policy List view

You can create Android policies, which can then be applied to Android devices.



Security - Android Policy List : 3

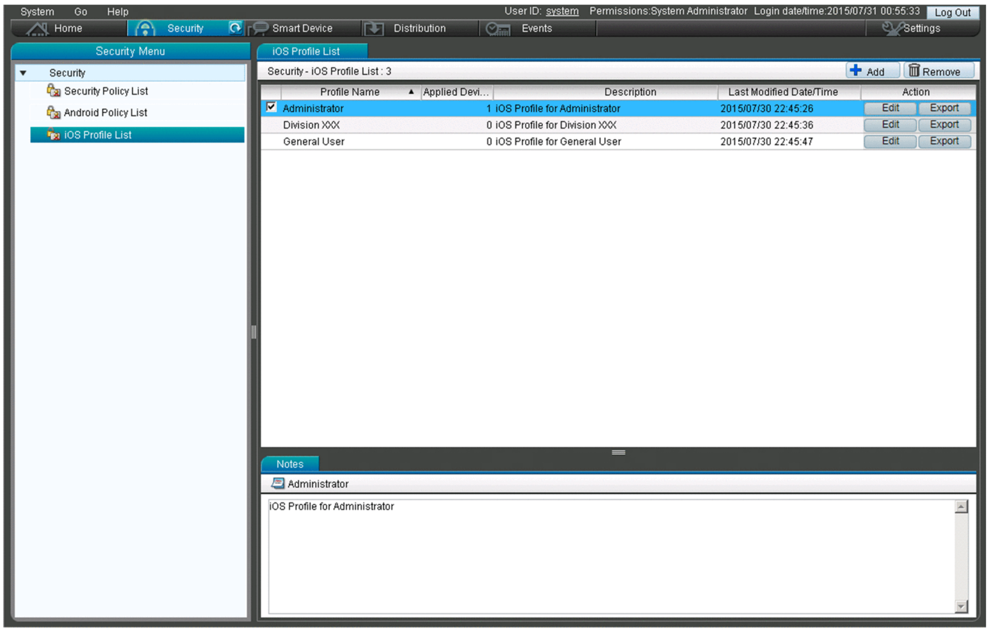
	Policy Name	Applied Devices	Description	Last Modified Date/Time	Action
☑	Administrator	1	Android Policy for Administrator	2015/07/30 22:46:05	Edit
	Division XXX	0	Android Policy for Division XXX	2015/07/30 22:46:17	Edit
	General User	0	Android Policy for General User	2015/07/30 22:46:26	Edit

Administrator

Android Policy for Administrator

iOS Profile List view

You can register iOS profiles, which can then be applied to iOS devices.



Security - iOS Profile List : 3

	Profile Name ▲	Applied Devi...	Description	Last Modified Date/Time	Action
☑	Administrator	1	iOS Profile for Administrator	2015/07/30 22:45:26	Edit Export
	Division XXX	0	iOS Profile for Division XXX	2015/07/30 22:45:36	Edit Export
	General User	0	iOS Profile for General User	2015/07/30 22:45:47	Edit Export

iOS Profile for Administrator

1.3.4 Working with the Smart Device module

In the Smart Device module, you can check or register smart device information, and apply security rules created in the Security module to smart devices. You can also perform remote operations such as locking and initializing smart devices.

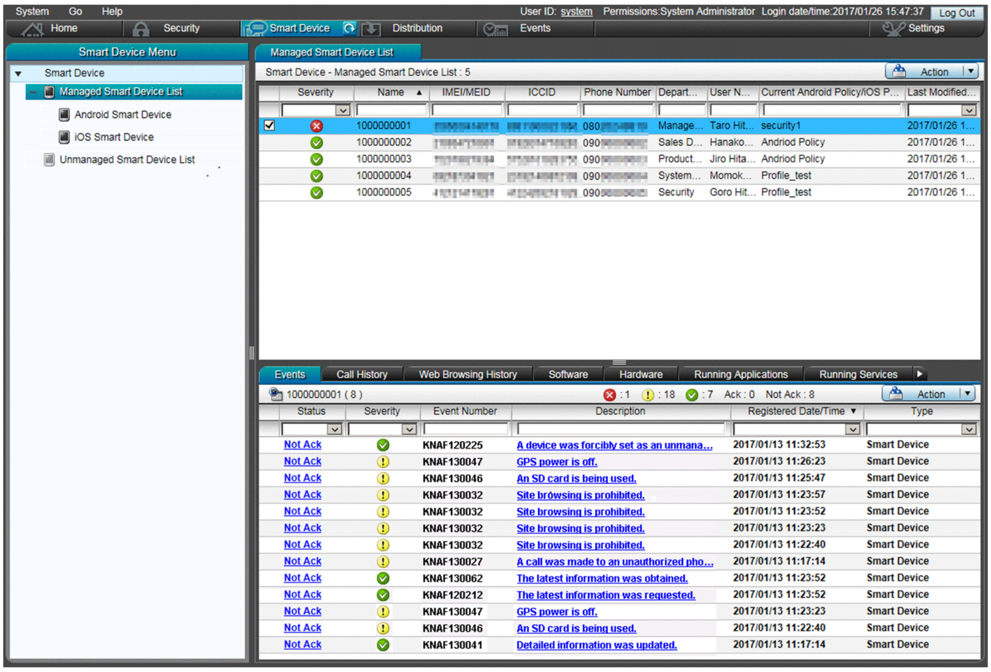
The Smart Device module provides the following views:

- **Managed Smart Device List** view
- **Unmanaged Smart Device List** view

Each view is described next.

Managed Smart Device List view

You can check information about managed smart devices.



Smart Device - Managed Smart Device List : 5

	Severity	Name ▲	IMEI/MEID	ICCID	Phone Number	Depart...	User N...	Current Android Policy/iOS P...	Last Modified...
☑	✗	1000000001	[redacted]	[redacted]	080[redacted]	Manage...	Taro Hit...	security1	2017/01/26 1...
	✓	1000000002	[redacted]	[redacted]	090[redacted]	Sales D...	Hanako...	Andriod Policy	2017/01/26 1...
	✓	1000000003	[redacted]	[redacted]	090[redacted]	Product...	Jiro Hita...	Andriod Policy	2017/01/26 1...
	✓	1000000004	[redacted]	[redacted]	090[redacted]	System...	Momok...	Profile_test	2017/01/26 1...
	✓	1000000005	[redacted]	[redacted]	090[redacted]	Security	Goro Hit...	Profile_test	2017/01/26 1...

1000000001 (8)   ✗ : 1   ! : 18   ✓ : 7   Ack : 0   Not Ack : 8

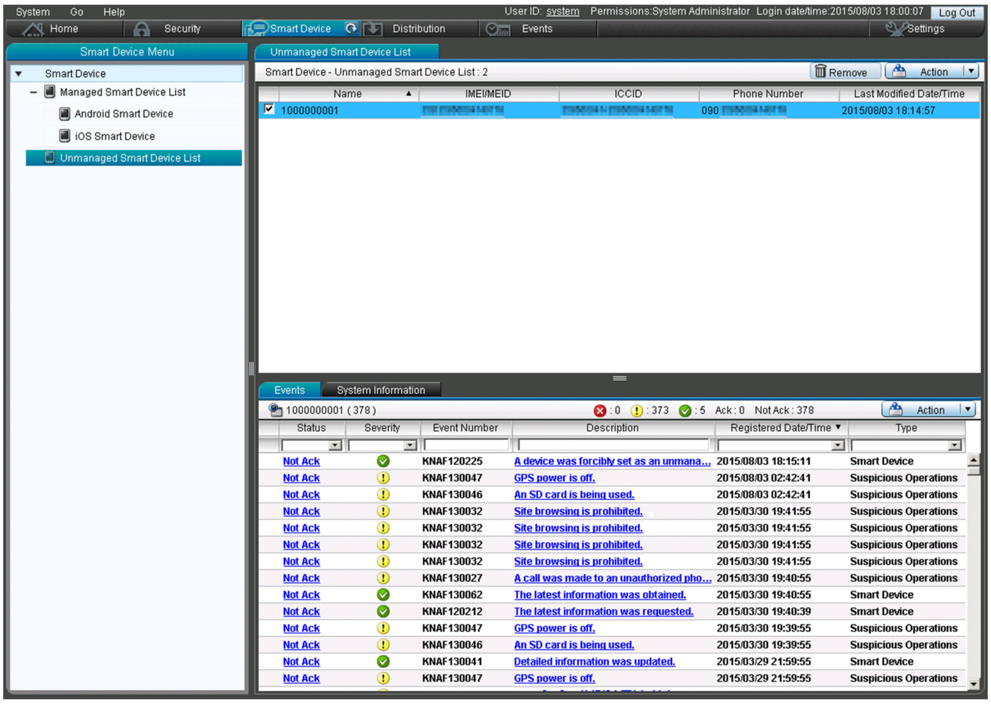
Status	Severity	Event Number	Description	Registered Date/Time ▼	Type
Not Ack	✓	KNAF120225	A device was forcibly set as an unmana...	2017/01/13 11:32:53	Smart Device
Not Ack	!	KNAF130047	GPS power is off.	2017/01/13 11:26:23	Smart Device
Not Ack	!	KNAF130046	An SD card is being used.	2017/01/13 11:25:47	Smart Device
Not Ack	!	KNAF130032	Site browsing is prohibited.	2017/01/13 11:23:57	Smart Device
Not Ack	!	KNAF130032	Site browsing is prohibited.	2017/01/13 11:23:52	Smart Device
Not Ack	!	KNAF130032	Site browsing is prohibited.	2017/01/13 11:23:23	Smart Device
Not Ack	!	KNAF130032	Site browsing is prohibited.	2017/01/13 11:22:40	Smart Device
Not Ack	!	KNAF130027	A call was made to an unauthorized pho...	2017/01/13 11:17:14	Smart Device
Not Ack	✓	KNAF130062	The latest information was obtained.	2017/01/13 11:23:52	Smart Device
Not Ack	✓	KNAF120212	The latest information was requested.	2017/01/13 11:23:52	Smart Device
Not Ack	!	KNAF130047	GPS power is off.	2017/01/13 11:23:23	Smart Device
Not Ack	!	KNAF130046	An SD card is being used.	2017/01/13 11:22:40	Smart Device
Not Ack	✓	KNAF130041	Detailed information was updated.	2017/01/13 11:17:14	Smart Device

In the menu area, select **Android Smart Device** to display a list of Android devices, or select **iOS Smart Device** to display a list of iOS devices.

When you select an item in the upper part of the information area, detailed information about that item is displayed on the tabs in the lower part of the information area. You can check events that have occurred, call history, Web browsing history, software (applications), hardware, running applications, running services, system information, security, and Bluetooth connection information.

Unmanaged Smart Device List view

You can check information about unmanaged smart devices.



Smart Device - Unmanaged Smart Device List : 2

	Name ▲	IMEI/MEID	ICCID	Phone Number	Last Modified Date/Time
☑	1000000001	[redacted]	[redacted]	090 [redacted]	2015/08/03 18:14:57

1000000001 (378)   ✗ : 0   ! : 373   ✓ : 5   Ack : 0   Not Ack : 378

Status	Severity	Event Number	Description	Registered Date/Time ▼	Type
Not Ack	✓	KNAF120225	A device was forcibly set as an unmana...	2015/08/03 18:15:11	Smart Device
Not Ack	!	KNAF130047	GPS power is off.	2015/08/03 02:42:41	Suspicious Operations
Not Ack	!	KNAF130046	An SD card is being used.	2015/08/03 02:42:41	Suspicious Operations
Not Ack	!	KNAF130032	Site browsing is prohibited.	2015/03/30 19:41:55	Suspicious Operations
Not Ack	!	KNAF130032	Site browsing is prohibited.	2015/03/30 19:41:55	Suspicious Operations
Not Ack	!	KNAF130032	Site browsing is prohibited.	2015/03/30 19:41:55	Suspicious Operations
Not Ack	!	KNAF130032	Site browsing is prohibited.	2015/03/30 19:41:55	Suspicious Operations
Not Ack	!	KNAF130027	A call was made to an unauthorized pho...	2015/03/30 19:40:55	Suspicious Operations
Not Ack	✓	KNAF130062	The latest information was obtained.	2015/03/30 19:40:55	Smart Device
Not Ack	✓	KNAF120212	The latest information was requested.	2015/03/30 19:40:39	Smart Device
Not Ack	!	KNAF130047	GPS power is off.	2015/03/30 19:39:55	Suspicious Operations
Not Ack	!	KNAF130046	An SD card is being used.	2015/03/30 19:39:55	Suspicious Operations
Not Ack	✓	KNAF130041	Detailed information was updated.	2015/03/29 21:59:55	Smart Device
Not Ack	!	KNAF130047	GPS power is off.	2015/03/29 21:59:55	Suspicious Operations

Detailed information about the smart device selected in the upper part of the information area is displayed on the tabs in the lower part of the information area. You can check events and system information.

Note that you can set an unmanaged smart device to *Managed* by applying a security policy and an Android policy, or a security policy and an iOS profile, to that smart device.

1.3.5 Working with the Distribution module

In the Distribution module, you can manage applications to be distributed to smart devices. You can also distribute applications to smart devices, and send instructions to smart devices to request the users to install the applications. You can also send instructions to smart devices to request the users to uninstall the distributed applications, and then remove the applications.

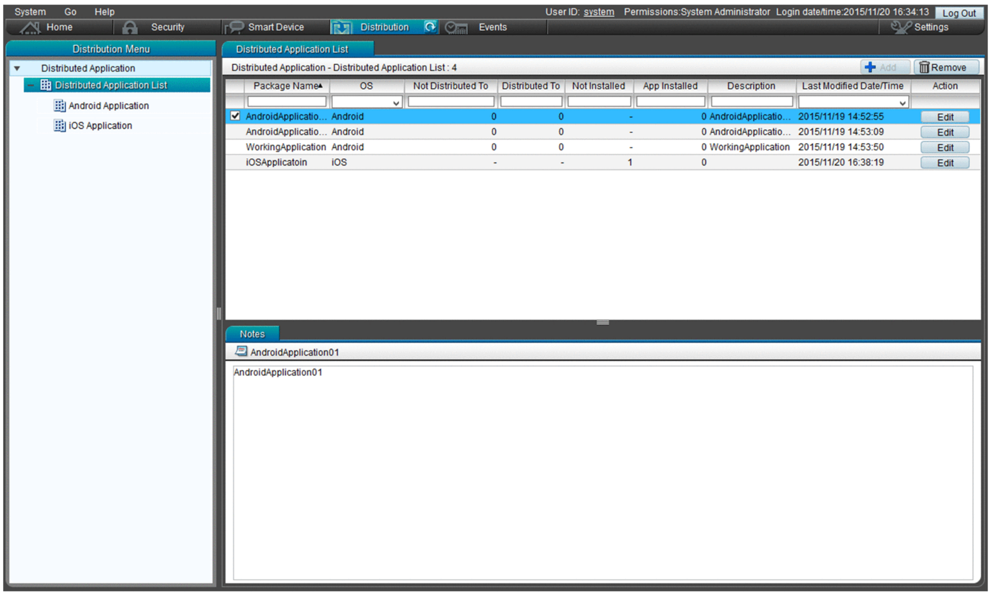
The Distribution module provides the following views:

- **Distributed Application List** view
- **Android Application** view
- **iOS Application** view

Each view is described next.

Distributed Application List view

You can view a list of applications to be distributed to smart devices, and a summary of the distributed applications.



Distributed Application - Distributed Application List : 4

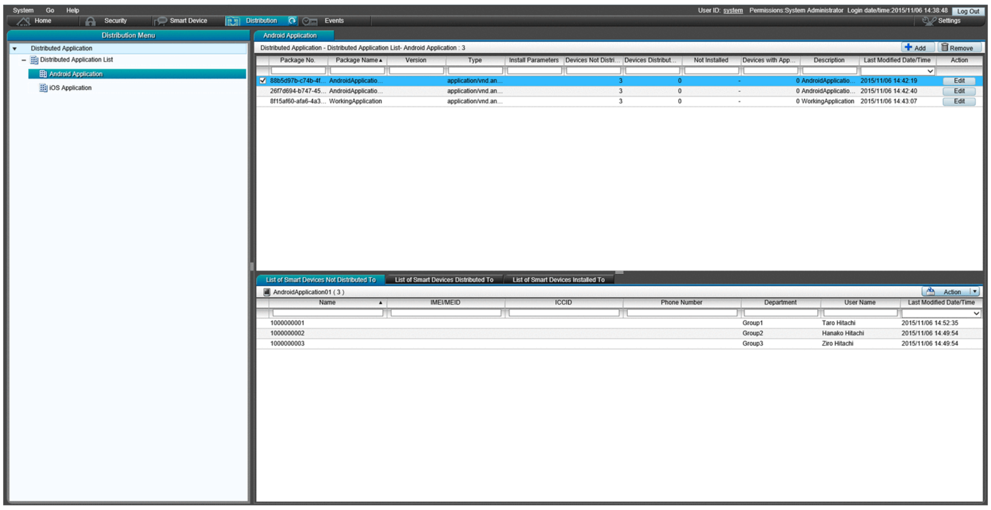
	Package Name▲	OS	Not Distributed To	Distributed To	Not Installed	App Installed	Description	Last Modified Date/Time	Action
☑	AndroidApplicatio...	Android	0	0	-	0	AndroidApplicatio...	2015/11/19 14:52:55	Edit
	AndroidApplicatio...	Android	0	0	-	0	AndroidApplicatio...	2015/11/19 14:53:09	Edit
	WorkingApplication	Android	0	0	-	0	WorkingApplication	2015/11/19 14:53:50	Edit
	iOSApplicatoin	iOS	-	-	1	0		2015/11/20 16:38:19	Edit

AndroidApplication01

AndroidApplication01

Android Application view

You can view a list of Android applications registered in JP1/ITDM2 - SDM.



User ID: system Permissions:System Administrator Login date/time:2015/11/06 14:38:48

Distributed Application - Distributed Application List- Android Application : 3

	Package No.	Package Name▲	Version	Type	Install Parameters	Devices Not Distri...	Devices Distribut...	Not Installed	Devices with App...	Description	Last Modified Date/Time	Action
☑	88b5d97b-c74b-4f...	AndroidApplicatio...		application/vnd.an...		3	0	-	0	AndroidApplicatio...	2015/11/06 14:42:19	Edit
	26f7d694-b747-45...	AndroidApplicatio...		application/vnd.an...		3	0	-	0	AndroidApplicatio...	2015/11/06 14:42:40	Edit
	8f15af60-afa6-4a3...	WorkingApplication		application/vnd.an...		3	0	-	0	WorkingApplication	2015/11/06 14:43:07	Edit

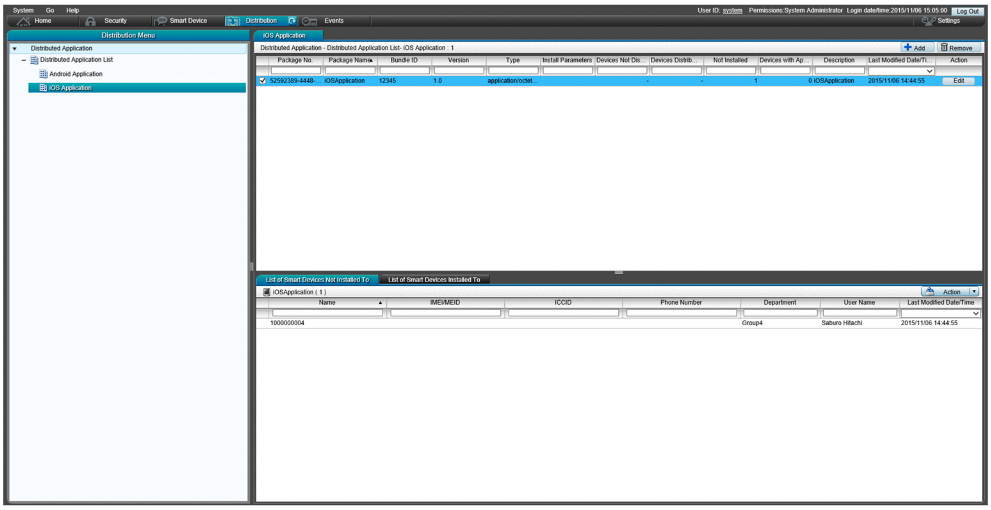
AndroidApplication01 (3)

Name ▲	IMEI/MEID	ICCID	Phone Number	Department	User Name	Last Modified Date/Time
1000000001				Group1	Taro Hitachi	2015/11/06 14:52:35
1000000002				Group2	Hanako Hitachi	2015/11/06 14:49:54
1000000003				Group3	Ziro Hitachi	2015/11/06 14:49:54

When you select an Android application in the upper part of the information area, a list of smart devices is displayed by distribution status in each tab in the lower part. Three types of distribution status are displayed: **Not Distributed**, **Distributed**, and **Installed**. You can also distribute to and remove applications from smart devices, and send instructions to smart devices to request users to install or uninstall applications.

iOS Application view

You can view a list of iOS applications registered in JP1/ITDM2 - SDM.



User ID: system Permissions:System Administrator Login date/time:2015/11/06 15:05:00

Distributed Application - Distributed Application List- iOS Application : 1

	Package No.	Package Name▲	Bundle ID	Version	Type	Install Parameters	Devices Not Dis...	Devices Distrib...	Not Installed	Devices with Ap...	Description	Last Modified Date/Ti...	Action
☑	52592389-4448-...	iOSApplication	12345	1.0	application/octet...		-	-	1	0	iOSApplication	2015/11/06 14:44:55	Edit

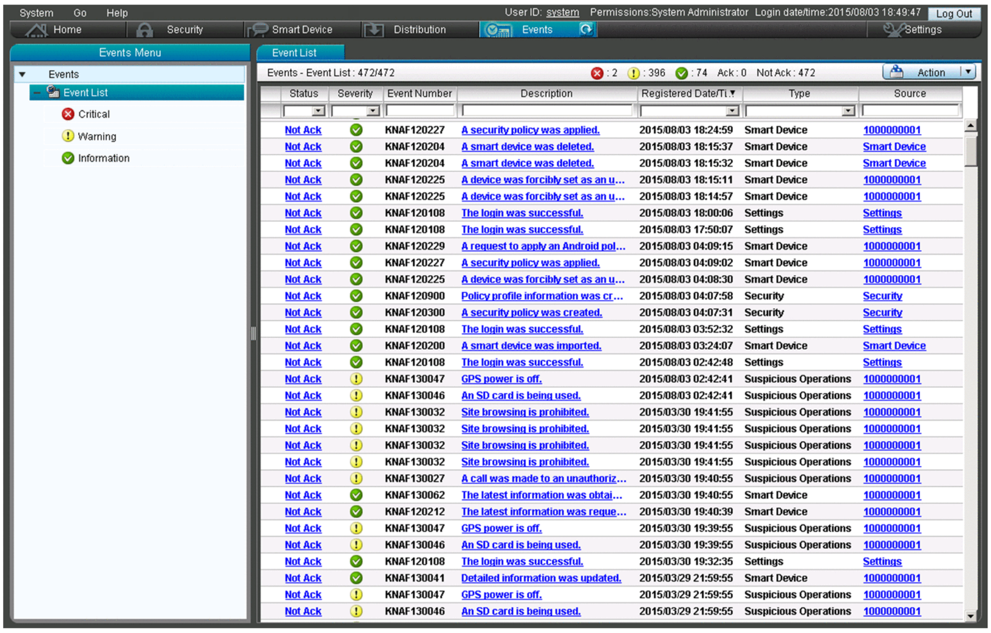
iOSApplication (1)

Name ▲	IMEI/MEID	ICCID	Phone Number	Department	User Name	Last Modified Date/Time
1000000004				Group4	Saburo Hitachi	2015/11/06 14:44:55

When you select an iOS application in the upper part of the information area, a list of smart devices is displayed by distribution status in each tab in the lower part. There are two distribution statuses: not installed and installed. Also, you can send instructions to each smart device to request the user to install applications onto, or uninstall applications from, the device.

1.3.6 Working with the Events module

In the Events module, you can check events that occurred during JP1/ITDM2 - SDM operation. For example, whether a security judgment operation terminated normally is displayed as an event.

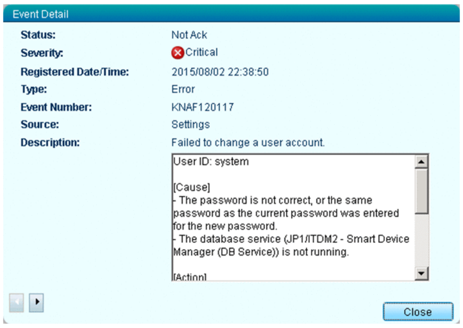


User ID: system Permissions:System Administrator Login date/time:2015/08/03 18:49:47

Events - Event List : 472/472 ✖ : 2 ! : 396 ✓ : 74 Ack : 0 Not Ack : 472

Status	Severity	Event Number	Description	Registered Date/Ti ▼	Type	Source
Not Ack	✓	KNAF120227	A security policy was applied.	2015/08/03 18:24:59	Smart Device	1000000001
Not Ack	✓	KNAF120204	A smart device was deleted.	2015/08/03 18:15:37	Smart Device	Smart Device
Not Ack	✓	KNAF120204	A smart device was deleted.	2015/08/03 18:15:32	Smart Device	Smart Device
Not Ack	✓	KNAF120225	A device was forcibly set as an u...	2015/08/03 18:15:11	Smart Device	1000000001
Not Ack	✓	KNAF120225	A device was forcibly set as an u...	2015/08/03 18:14:57	Smart Device	1000000001
Not Ack	✓	KNAF120108	The login was successful.	2015/08/03 18:00:06	Settings	Settings
Not Ack	✓	KNAF120108	The login was successful.	2015/08/03 17:50:07	Settings	Settings
Not Ack	✓	KNAF120229	A request to apply an Android pol...	2015/08/03 04:09:15	Smart Device	1000000001
Not Ack	✓	KNAF120227	A security policy was applied.	2015/08/03 04:09:02	Smart Device	1000000001
Not Ack	✓	KNAF120225	A device was forcibly set as an u...	2015/08/03 04:08:30	Smart Device	1000000001
Not Ack	✓	KNAF120900	Policy profile information was cr...	2015/08/03 04:07:58	Security	Security
Not Ack	✓	KNAF120300	A security policy was created.	2015/08/03 04:07:31	Security	Security
Not Ack	✓	KNAF120108	The login was successful.	2015/08/03 03:52:32	Settings	Settings
Not Ack	✓	KNAF120200	A smart device was imported.	2015/08/03 03:24:07	Smart Device	Smart Device
Not Ack	✓	KNAF120108	The login was successful.	2015/08/03 02:42:48	Settings	Settings
Not Ack	!	KNAF130047	GPS power is off.	2015/08/03 02:42:41	Suspicious Operations	1000000001
Not Ack	!	KNAF130046	An SD card is being used.	2015/08/03 02:42:41	Suspicious Operations	1000000001
Not Ack	!	KNAF130032	Site browsing is prohibited.	2015/03/30 19:41:55	Suspicious Operations	1000000001
Not Ack	!	KNAF130032	Site browsing is prohibited.	2015/03/30 19:41:55	Suspicious Operations	1000000001
Not Ack	!	KNAF130032	Site browsing is prohibited.	2015/03/30 19:41:55	Suspicious Operations	1000000001
Not Ack	!	KNAF130032	Site browsing is prohibited.	2015/03/30 19:41:55	Suspicious Operations	1000000001
Not Ack	!	KNAF130027	A call was made to an unauthoriz...	2015/03/30 19:40:55	Suspicious Operations	1000000001
Not Ack	✓	KNAF130062	The latest information was obtai...	2015/03/30 19:40:55	Smart Device	1000000001
Not Ack	✓	KNAF120212	The latest information was reque...	2015/03/30 19:40:39	Smart Device	1000000001
Not Ack	!	KNAF130047	GPS power is off.	2015/03/30 19:39:55	Suspicious Operations	1000000001
Not Ack	!	KNAF130046	An SD card is being used.	2015/03/30 19:39:55	Suspicious Operations	1000000001
Not Ack	✓	KNAF120108	The login was successful.	2015/03/30 19:32:35	Settings	Settings
Not Ack	✓	KNAF130041	Detailed information was updated.	2015/03/29 21:59:55	Smart Device	1000000001
Not Ack	!	KNAF130047	GPS power is off.	2015/03/29 21:59:55	Suspicious Operations	1000000001
Not Ack	!	KNAF130046	An SD card is being used.	2015/03/29 21:59:55	Suspicious Operations	1000000001

You can view an event in detail by clicking the link in **Description**.



Status: Not Ack
Severity: ✖Critical
Registered Date/Time: 2015/08/02 22:38:50
Type: Error
Event Number: KNAF120117
Source: Settings
Description: Failed to change a user account.

```
User ID: system

[Cause]
- The password is not correct, or the same
password as the current password was entered
for the new password.
- The database service (JP1/ITDM2 - Smart Device
Manager (DB Service)) is not running.

[Action]
```

Some events require a quick response. Attend to **Critical** events first, followed by **Warning** events. Identify the cause of the event from the event details, and take the appropriate action.

When you have finished dealing with an event, change its status to **Ack**. By changing the event status, you can easily identify whether an event has been resolved.

1.3.7 Working with the Settings module

In the Settings module, you can specify settings required for operating JP1/ITDM2 - SDM, such as user account management and email notification when an event occurs.

The Settings module provides the following views:

User Management

Account Management view

Events

Event Notifications view

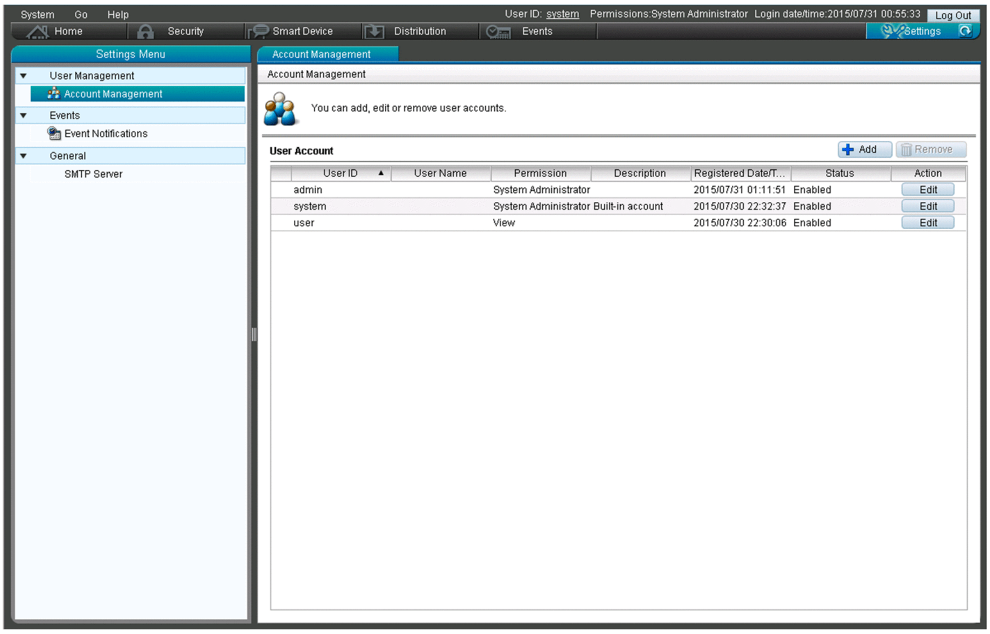
General

SMTP server view

Each view is described next.

Account Management view

You can add, edit, and delete JP1/ITDM2 - SDM user accounts.



Account Management

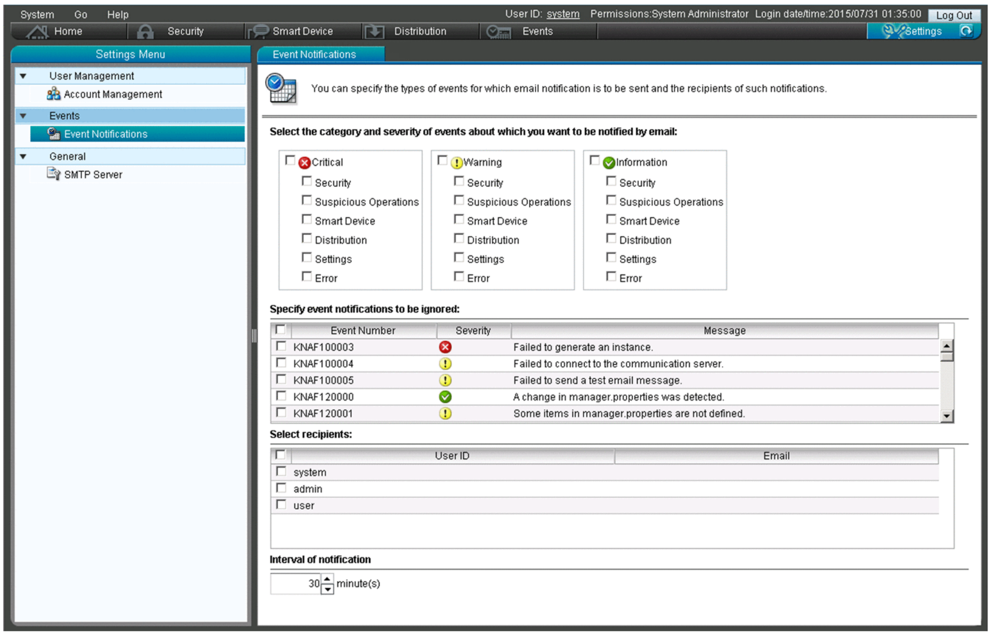
You can add, edit or remove user accounts.

User Account

User ID ▲	User Name	Permission	Description	Registered Date/T...	Status	Action
admin		System Administrator		2015/07/31 01:11:51	Enabled	Edit
system		System Administrator	Built-in account	2015/07/30 22:32:37	Enabled	Edit
user		View		2015/07/30 22:30:06	Enabled	Edit

Event Notifications view

You can specify the severity and type of events for which email notifications will be sent, event notifications to be ignored, and users to which email notification will be sent if a certain event occurs.



You can specify the types of events for which email notification is to be sent and the recipients of such notifications.

Select the category and severity of events about which you want to be notified by email:

□ Critical	□ Warning	□ Information
□ Security	□ Security	□ Security
□ Suspicious Operations	□ Suspicious Operations	□ Suspicious Operations
□ Smart Device	□ Smart Device	□ Smart Device
□ Distribution	□ Distribution	□ Distribution
□ Settings	□ Settings	□ Settings
□ Error	□ Error	□ Error

Specify event notifications to be ignored:

□	Event Number	Severity	Message
□	KNAF100003	✕	Failed to generate an instance.
□	KNAF100004	!	Failed to connect to the communication server.
□	KNAF100005	!	Failed to send a test email message.
□	KNAF120000	✓	A change in manager.properties was detected.
□	KNAF120001	!	Some items in manager.properties are not defined.

Select recipients:

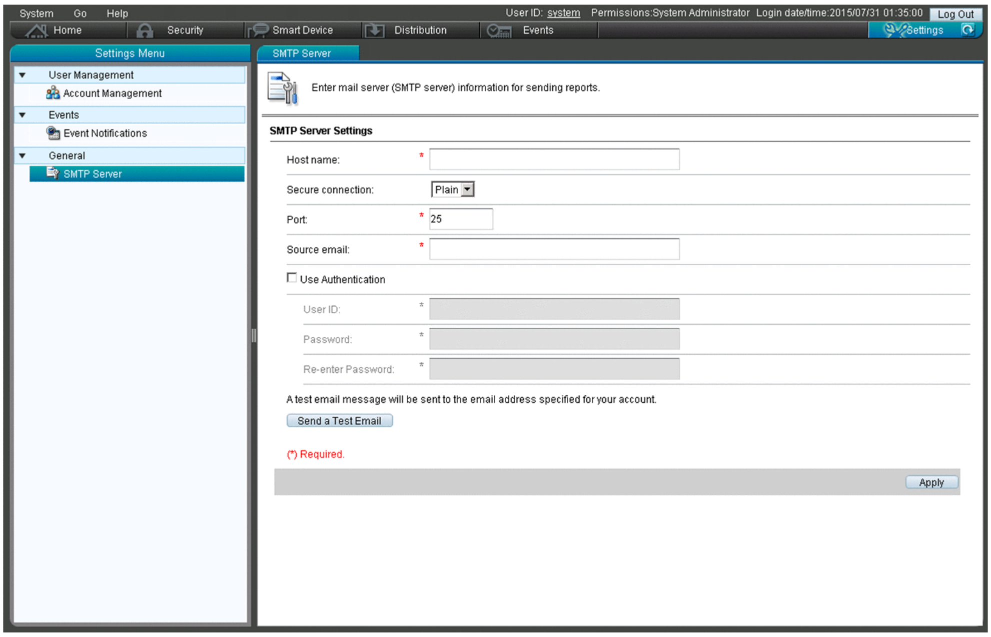
□	User ID	Email
□	system	
□	admin	
□	user	

Interval of notification

30 minute(s)

SMTP server view

You can specify connection information for the mail server when sending an event notification email.



User ID: system Permissions:System Administrator Login date/time:2015/07/31 01:35:00

Enter mail server (SMTP server) information for sending reports.

SMTP Server Settings

Host name: *

Secure connection: Plain

Port: * 25

Source email: *

□ Use Authentication

User ID: *

Password: *

Re-enter Password: *

A test email message will be sent to the email address specified for your account.

(*) Required.

2 Features of JP1/ITDM2 - SDM

This chapter provides details about JP1/ITDM2 - SDM features, such as security management, smart device management, application management, and the event viewer.

2.1 List of features

The following lists and describes JP1/ITDM2 - SDM features.

List of features

No.	Feature	Description
1	System summary	You can check the system summary that contains the following: • Smart device status • Event status • Database status and hard disk usage • Status of certificates for MDM
2	User account management	You can create user accounts appropriate for the role of the JP1/ITDM2 - SDM user.
3	Security management	You can create a security policy for smart devices. You can also create an Android policy or register an iOS profile appropriate for smart devices. You can determine the security status by applying these policies (or profiles) to smart devices.
4	Smart device management	You can check the list of smart devices registered in JP1/ITDM2 - SDM. You can also check detailed device information such as hardware and software information for each smart device. In addition, you can perform remote operation such as locking and initializing smart devices that have security problems.
5	Application management	You can perform unified management of applications to be distributed to smart devices. You can also distribute to, and remove applications from, managed smart devices, and send instructions to smart devices to request users to install or uninstall the applications.
6	Event viewer	You can check events that occurred. Execution results of JP1/ITDM2 - SDM functions can also be displayed as events.

Related Topics

- *2.2 Displaying a system summary*
- *2.3 Managing user accounts*
- *2.4 Managing security*
- *2.5 Managing smart devices*
- *2.6 Managing applications*
- *2.7 Displaying events*

2.2 Displaying a system summary

You can check the status of smart devices registered in JP1/ITDM2 - SDM and the event status. You can also check whether the database is backed up on the smart device manager, check the hard disk usage and free space, and check the status of certificates for MDM.

System Summary panel

Displays summary information for the smart devices registered in JP1/ITDM2 - SDM.

You can check the following information displayed below **Smart Device Status**:

- Total number of registered smart devices, and the difference from the previous day's number of smart devices
- Number of managed smart devices, and the difference from the previous day's number of smart devices
- Number of unmanaged smart devices, and the difference from the previous day's number of smart devices

Click the link on the number of managed or unmanaged smart devices to display the Smart Device module, which allows you to check details about the smart devices.

Event Summary panel

Displays the total number of events that occurred in one week, and the number of events by event type.

If an event whose severity is **Critical** occurred, the ⊗ icon is displayed at the left of the event type. At this time, click the link on the number of events to display the Events module, which allows you to check the contents of events.

You can also change the display period to check the number of events that occur over either a single day, or a three-day period.

Database and Disk Usage panel

You can check the following:

- Whether the database is backed up
- Hard disk usage and free space
- Hard disk usage for the database, and free space

Tip

You can move the database backup folder from a nearly full disk to one with enough free space, or free up disk space by removing data that is no longer needed.

Status of Certificate for MDM panel

You can check the following:

- Validity of the MDM certificate
- Expiration date of the MDM certificate

Related Topics

- *2.5 Managing smart devices*
- *2.7 Displaying events*
- *14.3 Home module*
- *14.5 Smart Device module*
- *14.7 Events module*

2.3 Managing user accounts

If several administrators will be using JP1/ITDM2 - SDM, you can create a user account for each administrator.

You can set the following parameters for user accounts that define the range of operations the user can perform.

Permission

You can set permissions according to the range of operations allowed for a user: for example, a manager who only needs to view information can have permissions different from a system administrator who manages smart devices.

2.3.1 Locking user accounts

If a user fails to log in to JP1/ITDM2 - SDM three consecutive times, the user account is locked. That user cannot log in again until the user account is unlocked.

You can find out whether any accounts are locked by accessing the **Account Management** view in the Settings module from a user account with the system administrator permission. You can then use the same view to unlock the account.

Disabled appears as the **Status** of locked user accounts in the **Account Management** view.

Related Topics

- *2.3.2 User account permissions*
- *6.7 Unlocking a user account*
- *14.8.1 Account Management view*

2.3.2 User account permissions

There are two permissions you can assign to user accounts in JP1/ITDM2 - SDM:

- System administrator permission
  A user with this permission has full access to the features of JP1/ITDM2 - SDM.
- View permission
  A user with this permission is able to view the information managed by JP1/ITDM2 - SDM. Users are assigned view permission by default.

Related Topics

- *2.3.1 Locking user accounts*
- *2.3.3 List of operations that cannot be performed with the view permission*

2.3.3 List of operations that cannot be performed with the view permission

The following describes the operations that cannot be performed by a user account that has been assigned the view permission.

Operations that cannot be performed with the view permission

Operation window		Operation
Security module	**Security Policy List** view	Operations on security policies (adding, editing, and deleting)
		Updating notes about a security policy
	Android Policy List view	Operations on Android policies (adding, editing, and deleting)
		Updating notes about an Android policy
	iOS Profile List view	Operations on iOS profiles (adding and deleting)
		Editing iOS profile information
		Updating notes about an iOS profile
Smart Device module	**Managed Smart Device List** view	The following operations selected from **Action**: • **Update Device Details** • **Initialize Smart Device** • **Lock Smart Device** • **Reset Smart Device Passcode** • **Send Notification** • **Set to Unmanaged** • **Apply Security Policy** • **Apply Android Policy** • **Apply iOS Profile** • **Remove applied iOS Profile** • **Add Smart Device** • **Import Smart Device List**
	Events tab of **Managed Smart Device List** view	The following operations selected from **Action**: • **Set to Confirmed** • **Set to Not Confirmed**
	Call History tab of **Managed Smart Device List** view	The following operations selected from **Action**: • **Set to Confirmed** • **Set to Not Confirmed** • **Allow**
	Web Browsing History tab of **Managed Smart Device List** view	The following operations selected from **Action**: • **Set to Confirmed** • **Set to Not Confirmed** • **Allow** • **Prohibit**
	Software tab of **Managed Smart Device List** view	The following operations selected from **Action**: • **Set to Confirmed** • **Set to Not Confirmed** • **Allow** • **Prohibit**
	Bluetooth Connection Information tab of **Managed Smart Device List** view	The following operations selected from **Action**: • **Set to Confirmed** • **Set to Not Confirmed**
	Unmanaged Smart Device List view	The following operations selected from **Action**: • **Apply Security Policy** • **Apply Android Policy** • **Apply iOS Profile**

Operation window		Operation
Smart Device module	**Unmanaged Smart Device List** view	Deleting smart devices
	Events tab of **Unmanaged Smart Device List** view	The following operations selected from **Action**: • **Set to Confirmed** • **Set to Not Confirmed**
Distribution module	**Distributed Application List** view	Operations on distributed applications (editing and deleting)
		Updating notes about a distributed application
	Android Application view	Operations on Android applications (adding, editing, and deleting)
	List of Smart Devices Not Distributed To tab of **Android Application** view	The following operations selected from **Action**: • **Application Distribution** • **Application Installation**
	List of Smart Devices Distributed To tab of **Android Application** view	The following operations selected from **Action**: • **Application Installation** • **Application Deletion**
	List of Smart Devices Installed To tab of **Android Application** view	The following operations selected from **Action**: • **Application Deletion**
	iOS Application view	Operations on iOS applications (adding, editing, and deleting)
	List of Smart Devices Not Installed To tab of **iOS Application** view	The following operations selected from **Action**: • **Application Installation**
	List of Smart Devices Installed To tab of **iOS Application** view	The following operations selected from **Action**: • **Application Deletion**
Events module	**Event List** view	The following operations selected from **Action**: • **Set to Confirmed** • **Set to Not Confirmed**
Settings module	**Account Management** view	User account management
	Event Notifications view	Setting up event notifications
	SMTP Server view	Setting up the mail server

Related Topics

- *2.3.2 User account permissions*

2.4 Managing security

You can manage smart devices by creating security rules and then applying them to the smart devices.

2.4.1 Types of security rules

There are three types of security rules: Security policy, Android policy, and iOS profile.

Security policy

This is a policy used to monitor the usage of smart devices. Phone numbers, Web sites, and applications can be set for a security policy. JP1/ITDM2 - SDM checks this policy and smart device usage history, and then issues an event if any use that does not comply with the policy is found. The administrator can detect unauthorized use of a smart device by checking the issued event.

Android policy

This is an operation policy that is set for Android devices. An Android policy can specify password rules and restrict use of the camera function.

iOS profile

This is an operation policy that is set for iOS devices. A configuration profile created by using the iPhone Configuration Utility (provided by Apple) can be registered as an iOS profile. An iOS policy can specify passcode rules and restrict use of the camera function.

The following lists the typical functions that can be disabled or monitored by using security rules:

Function	Android device	iOS device
Camera	Can be disabled	Can be disabled
Application installation (using App Store)	Cannot be disabled	Can be disabled
Call history	Can be monitored	Cannot be monitored
Web browsing history	Can be monitored	Cannot be monitored
Application use history	Can be monitored	Cannot be monitored

Legend:

Disable: Specified in an Android policy or iOS profile

Monitor: Specified in a security policy

Related Topics

- *2.4.2 Managing a security policy*
- *2.4.3 Items that can be set for a security policy*
- *2.4.4 Managing an Android policy*
- *2.4.5 Items that can be set for an Android policy*
- *2.4.6 Managing an iOS profile*
- *2.4.7 Items that can be set in an iOS profile*

2.4.2 Managing a security policy

In the **Security Policy List** view of the Security module, create and manage a security policy.

Create a security policy.

Create a security policy based on your organization's security principles. You can create multiple security policies.

Edit a security policy.

If the security trends change or your organization's security principles are changed, edit a security policy.

Security trends change together with changes to smart devices and the network environment. By always incorporating security trends into your organization, you will be able to robustly manage the security status.

Delete a security policy.

Delete security policies that are no longer needed because, for example, the management structure changed or multiple security policies were combined.

Related Topics

- *2.4.3 Items that can be set for a security policy*
- *7.1 Using security policies*

2.4.3 Items that can be set for a security policy

For a security policy, you can set the following items whose use is monitored: phone numbers, Web sites, and applications.

Items that can be set for a security policy

No.	Configuration item	Description
1	**Phone Number**	Set phone numbers to be monitored. If a phone number that is not registered in this list is used, an event is issued to notify the administrator.
2	**Web Site**	Set Web sites to be monitored. If a Web site that is not specified in **Whitelist** or a Web site specified in **Blacklist** is browsed, an event is issued to notify the administrator.
3	**Application**	Set applications to be monitored. If an application that is not specified in **Whitelist** or an application specified in **Blacklist** is installed, an event is issued to notify the administrator. For applications specified in **Whitelist**, you can also specify whether installation is required. If an application that must be installed is not installed, an event is issued to notify the administrator.

Related Topics

- *2.4.2 Managing a security policy*
- *14.4.1 Security Policy List view*

2.4.4 Managing an Android policy

In the **Android Policy List** view of the Security module, create and manage an Android policy.

Create an Android policy.

Create an Android policy based on your organization's security principles. You can create multiple Android policies.

Edit an Android policy.

If your organization's security principles are changed, edit an Android policy.

Delete an Android policy.

Delete Android policies that are no longer needed because, for example, the management structure changed or multiple Android policies were combined.

Related Topics

- *2.4.5 Items that can be set for an Android policy*
- *7.2 Using Android policies*

2.4.5 Items that can be set for an Android policy

For an Android policy, you can set password rules, the time that can elapse before the Android device is automatically locked, and whether the camera can be used.

Items that can be set for an Android policy

No.	Configuration item	Description
1	**Password Complexity**	Set the password complexity as one of the following types: • **1** (Alphabetic password) • **2** (The password requires alphabetic letters and numbers.) • **3** (The password requires alphabetic letters, numbers, and special symbols.) • **4** (Password made of any string) • **5** (Biometrics) The initial value is **1** (Alphabetic password)
2	**Min. Password Length**	Set the number of characters required for the password. This item is valid if **Password Complexity** is not set to **5** (Biometrics). The initial value is **4**. The specifiable values are 4 to 16.
3	**Minimum Number of Alphabetic Characters Required in the Password**	Set the minimum number of alphabetic characters required in the password. This item is valid if **Password Complexity** is set to **3** (The password requires alphabetic letters, numbers, and special symbols.). The initial value is **-** (not limited). The specifiable values are **-** (not limited) and 1 to 4.
4	**Minimum Number of Lowercase Characters Required in the Password**	Set the minimum number of lowercase characters required in the password. This item is valid if **Password Complexity** is set to **3** (The password requires alphabetic letters, numbers, and special symbols.). The initial value is **-** (not limited). The specifiable values are **-** (not limited) and 1 to 4.
5	**Minimum Number of Uppercase Characters Required in the Password**	Set the minimum number of uppercase characters required in the password. This item is valid if **Password Complexity** is set to **3** (The password requires alphabetic letters, numbers, and special symbols.). The initial value is **-** (not limited). The specifiable values are **-** (not limited) and 1 to 4.
6	**Minimum Number of Non-Alphabetic Characters Required in the Password**	Specify the minimum number of non-alphabetic characters required in the password.

No.	Configuration item	Description
6	**Minimum Number of Non-Alphabetic Characters Required in the Password**	This item is valid if **Password Complexity** is set to **3** (The password requires alphabetic letters, numbers, and special symbols.). The initial value is **-** (not limited). The specifiable values are **-** (not limited) and 1 to 4.
7	**Minimum Number of Numerals Required in the Password**	Specify the minimum number of numeric characters required in the password. This item is valid if **Password Complexity** is set to **3** (The password requires alphabetic letters, numbers, and special symbols.). The initial value is **-** (not limited). The specifiable values are **-** (not limited) and 1 to 4.
8	**Minimum Number of Special Characters Required in the Password**	Specify the minimum number of special characters required in the password. This item is valid if **Password Complexity** is set to **3** (The password requires alphabetic letters, numbers, and special symbols.). The initial value is **-** (not limited). The specifiable values are **-** (not limited) and 1 to 4.
9	**Timeout Value Until Password Expires**	Specify the number of days that can elapse before the password must be changed. Specify **0** to disable the function. The initial value is **0** (Disabled). The specifiable values are 0 to 730 (days).
10	**Password History Limit**	This function prevents reuse of the password more than the specified number of times. Specify **0** to disable the function. The initial value is **0** (Disabled). The specifiable values are 0 to 50.
11	**Maximum Number of Retries for Password Failure**	Set the maximum number of retries allowed when the user fails to enter the password. Specify **0** to disable the function. The initial value is **0** (Disabled). The specifiable values are 0 and 4 to 10.
12	**Maximum Value for Inactive Time Lock**	Set the time allowed for idling before the Android device is automatically locked. Specify **0** to disable the function. The initial value is **0** (Disabled). The specifiable values are 0, 1 to 5, 10, and 15 (minutes).
13	**Request for Storage Encryption**	Specify whether to perform encryption for internal storage. If the Android device supports storage encryption, this function is enabled by selecting the check box. This check box is cleared (the function is disabled) by default. You can select the check box to enable the function or clear the check box to disable the function.
14	**Timeout Value for Failed Server Connection**	Specify the maximum amount of time that can elapse before the Android device is initialized if the Android device cannot connect with JP1/ITDM2 - SDM. Select **OFF** to disable the function. The initial setting is **OFF**. You can select **OFF** or **ON**. When **ON** is selected, the specifiable values are 1 to 60 (minutes).
15	**Camera Use Prohibited**	Prohibit use of the camera. This check box is cleared (camera can be used) by default. You can select the check box to prohibit use of the camera, or clear the check box to permit use of the camera.

Important

After a password rule is applied, the rule takes effect the next time the password is changed.

Related Topics

- *2.4.4 Managing an Android policy*
- *14.4.11 Android Policy List view*

2.4.6 Managing an iOS profile

In the **iOS Profile List** view of the Security module, you can manage iOS profiles.

Register an iOS profile.

Use the iPhone Configuration Utility (provided by Apple) to create a configuration profile based on your organization's security principles, and then register that profile as an iOS profile. You can register multiple iOS profiles.

Edit iOS profile information.

Edit the iOS profile name and description.

Export an iOS profile.

If your organization's security principles are changed or a new environment must be created, export the iOS profile as an XML file. You can import the exported file to the iPhone Configuration Utility (provided by Apple) by changing the extension to `.mobileconfig`. If necessary, edit the configuration profile, and then register it again as an iOS profile.

Delete an iOS profiles.

Delete iOS profiles that are no longer needed because, for example, the management structure changed or multiple iOS profiles were combined.

Related Topics

- *2.4.7 Items that can be set in an iOS profile*
- *7.3 Using iOS profiles*

2.4.7 Items that can be set in an iOS profile

In an iOS profile, you can set items of a configuration profile that can be created by using the iPhone Configuration Utility.

To find these items, please visit Apple's website.

Related Topics

- *2.4.6 Managing an iOS profile*

2.5 Managing smart devices

You can register information about smart devices and check the latest information in a list. You can also apply security rules to smart devices and perform remote operations such as locking and initializing smart devices.

2.5.1 Managing managed smart devices

The **Managed Smart Device List** view of the Smart Device module displays a list of managed smart devices. In this view, you can register a smart device, apply security rules, and perform remote operation such as locking or initializing smart devices.

Checking smart device information

In the menu area, select **Android Smart Device** or **iOS Smart Device** to view the list of smart devices for each OS.

When you select a smart device in the list, detailed information is displayed on the tabs in the lower part of the information area. The following describes the information you can check on each tab:

Tab name	Description
Events tab	You can check the list of events that occurred on the smart device. You can set the status of an event to **Ack** or **Not Ack**.
Call History tab	You can check the call history list for the smart device. You can set the status of an entry of the history to **Ack** or **Not Ack**. You can add a phone number in the history to the security policy as an allowed phone number.
Web Browsing History tab	You can check the Web browsing history listing for the smart device. You can set the status of a history entry to **Ack** or **Not Ack**. You can add a Web site in the history to the security policy as an allowed or prohibited Web site.
Software tab	You can check the list of software products (applications) distributed or installed on the smart device. You can set the status of a software product in the list to **Ack** or **Not Ack**. You can also add a software product in the list to the security policy as an allowed or prohibited application.
Hardware tab	You can check hardware information such as the serial number and internal storage capacity of the smart device.
Running Applications tab	You can check the list of applications running on the smart device.
Running Services tab	You can check the list of services running on the smart device.
System Information tab	You can check system information such as the OS information and phone number of the smart device.
Security tab	You can check information including the security policy and Android policy (or iOS profile) applied to the smart device, GPS power status, and the date and time when the smart device was locked last.
Bluetooth Connection Information tab	You can check the smart device connection history using Bluetooth communications. You can set the status of a history entry to **Ack** or **Not Ack**.

Registering smart device information

You can register smart device information including the name, OS type, and security rules. If you create a CSV file containing the smart device information you want to register, you can register the information in a batch by importing that CSV file. You can also export the registered smart device information in a CSV file.

Operations for smart devices

You can perform the following operations for smart devices:

- Acquire the latest information (acquire the latest inventory information from the smart device)
- Initialize the smart device (reset to the factory default settings)
- Lock the smart device
- Change the Android device password
- Resets the iOS device passcode
- Sends messages to an Android device
- Set the smart device to *Unmanaged*
- Apply a security policy
- Apply an Android policy
- Apply an iOS profile
- Remove an applied iOS profile

Related Topics

- *2.5.2 Managing unmanaged smart devices*
- *8. Managing Smart Devices*
- *14.5.1 Managed Smart Device List view*

2.5.2 Managing unmanaged smart devices

The **Unmanaged Smart Device List** view of the Smart Device module displays a list of unmanaged smart devices. In this view, you can apply security rules.

Checking smart device information

When you select a smart device in the list, detailed information is displayed on the tabs in the lower part of the information area. The following describes the information you can check on each tab:

Tab name	Description
Events tab	You can check the list of events that occurred on the smart device. You can set the status of an event to **Ack** or **Not Ack**.
System Information tab	You can check system information such as the OS information and phone number of the smart device.

Operations for smart devices

You can perform the following operations on the smart devices:

- Apply a security policy
- Apply an Android policy
- Apply an iOS profile

Related Topics

- *2.5.1 Managing managed smart devices*
- *8. Managing Smart Devices*
- *14.5.3 Unmanaged Smart Device List view*

2.6 Managing applications

You can manage the applications to be distributed to smart devices.

2.6.1 Managing distributed applications

You can check the registered applications in a list, and edit or remove applications.

In the **Distributed Application List** view of the Distribution module, you can check the list of applications registered by the administrator and check a summary of the status of distribution to smart devices. You can also edit and remove applications.

When you select an application in the list, you can enter the description of the application as a note in the lower part of the information area.

Related Topics

- *2.6.2 About applications to be distributed*
- *2.6.3 Managing Android applications*
- *2.6.4 Managing iOS applications*
- *9. Managing Applications*
- *14.6.1 Distributed Application List view*

2.6.2 About applications to be distributed

Applications can be distributed to smart devices in the following two ways:

- The administrator issues an instruction to install the application, upon which the application is installed on the smart device (Push-distribution).
- The administrator prepares applications in a form that can be installed by the user, and the user downloads and installs only the required applications (Pull-distribution).

The maximum size of applications that can be distributed is as follows:

OS	Maximum application size
Android	100MB
iOS	2GB

Note

When distributing applications, the applications to be distributed are manually placed on the communication server (standard distribution). However, there is another method (simple distribution) that does not require applications to be manually placed on the communication server. With simple distribution, the maximum size of applications that can be distributed is 5 MB for Android, and 50 MB for iOS. Simple distribution is not compatible with pull distribution.

To use simple distribution, you need to modify the environment setting file for smart device manager.

Related Topics

- *16.2 Smart device manager environment setting file (manager.properties)*

2.6.3 Managing Android applications

You can check the list of registered Android applications, and register, edit, or remove them. You can also distribute applications and send instructions to install or uninstall the applications.

The **Android Application** view of the Distribution module shows a list of Android applications and a summary of distribution to Android devices. In this view, you can register Android applications, and edit or delete registered information. You can distribute registered Android applications, remove the distributed applications, and send instructions to install or remove Android applications.

When you select an Android application in the list, a list of smart devices by distribution status is displayed on each tab in the lower part of the information area. The following describes the information you can check on each tab:

Tab name	Description
List of Smart Devices Not Distributed To tab	You can check the list of smart devices to which Android applications have not been distributed. You can distribute Android applications to the displayed smart devices, and send instructions to those smart devices to request users to install applications.
List of Smart Devices Distributed To tab	You can check the list of smart devices to which Android application have been distributed. You can send instructions to the displayed smart devices to request users to install Android applications. You can also remove Android applications from those smart devices.
List of Smart Devices Installed To tab	You can check the list of smart devices on which Android applications are installed. You can send instructions to the displayed smart devices to request users to uninstall Android applications, and then remove the Android applications.

Important

In JP1/ITDM2 - SDM, you can manage Android applications only if the extension of the application file is `.apk`.

Related Topics

- *9. Managing Applications*
- *14.6.2 Android Application view*

2.6.4 Managing iOS applications

You can check the list of registered iOS applications, and register, edit, or remove them. You can also send instructions to install or uninstall the applications.

The **iOS Application** view of the Distribution module shows a list of iOS applications and a summary of distribution to iOS devices. In this view, you can register iOS applications, and edit or delete registered information. You can also send instructions to install or uninstall registered iOS applications.

When you select an iOS application in the list, a list of smart devices by distribution status is displayed on each tab in the lower part of the information area. The following describes the information you can check on each tab:

Tab name	Description
List of Smart Devices Not Installed To tab	You can check the list of smart devices to which iOS applications have not been distributed. You can send instructions to the displayed smart devices to distribute iOS applications and request users to install them.
List of Smart Devices Installed To tab	You can check the list of smart devices on which iOS applications are installed. You can send instructions to the displayed smart devices to request users to uninstall and delete iOS applications.

Important

- In JP1/ITDM2 - SDM, you can manage iOS applications only if the extension of the application file is `.ipa`.
- If you distribute in-house iOS applications for internal use, make sure their use is within the scope of the license defined by the Apple Developer Enterprise Program.

Related Topics

- *9. Managing Applications*
- *14.6.4 iOS Application view*

2.7 Displaying events

An event is output when something that requires a quick response occurs during JP1/ITDM2 - SDM operation. The processing results of each function are also output as events. By checking the displayed events, the administrator can understand what occurred during operation.

2.7.1 Events to be output

Events to be output are classified into three severity types. Periodically check the events, and take action if any problems are found.

Events are classified into three severities depending on the details.

✖ (Critical)

Events that require immediate action. Check the details of the event, and take action immediately.

! (Warning)

Events that require a response but not immediately. Check the details of the event, and take action as necessary.

✓ (Information)

Events regarding the results of system processing. No actions are required.

Some events require immediate action. Check Critical events first and then Warning events. Determine the cause referring to the error message, and take appropriate actions.

Tip

You can specify settings so that the administrator is notified of events when they occur.

Related Topics

- *2.7.2 Event types*
- *2.7.3 Event format*
- *11.1 Specifying settings for event notification*
- *11.2 Setting up mail servers*
- *14.7 Events module*

2.7.2 Event types

The following are types of events to be output:

Event types

No.	Event type	Description
1	**Security**	Events regarding security management, such as a change or application of a security policy, and results of security policy judgments

No.	Event type	Description
2	**Smart Device**	Events regarding smart device management, such as addition or deletion of smart device information
3	**Distribution**	Events regarding distribution, such as distribution of applications to a smart device, and installation of applications
4	**Settings**	Events regarding settings, such as user account management, and email notification of events
5	**Suspicious Operations**	Events regarding suspicious operations, such as use of applications prohibited by a security policy, and a call to a destination prohibited by a security policy
6	**Error**	Events regarding errors that occurred in various functions.

Related Topics

- *2.7.1 Events to be output*
- *2.7.3 Event format*

2.7.3 Event format

The following table describes the format of events to be output.

Event format

No.	Field	Description
1	**Status**	This field shows whether the event was checked. Clicking the field changes the status. • Not Ack • Ack
2	**Severity**	This field shows the severity of the event. One of the following is displayed: • Critical • Warning • Information
3	**Registered Date/Time**	This field shows the date and time the event was registered in the smart device manager.
4	**Type**	This field shows the event type. One of the following is displayed: • Security • Smart Device • Distribution • Settings • Suspicious Operations • Error
5	**Event Number**	This field displays the ID of the event message.
6	**Source**	This field shows information that identifies the target of an event, such as a smart device or security policy. Clicking a link in this field changes the display to the link destination. One of the following is displayed: • **Smart Device Name** (link destination: **Managed Smart Device List** view or **Unmanaged Smart Device List** view) • **Security** (link destination: **Security Policy List** view) • **Distribution** (link destination: **Distributed Application List** view)

No.	Field	Description
6	**Source**	• **Settings** (link destination: Settings module)
7	**Description**	This field displays detailed information about the event.

Related Topics

- *2.7.1 Events to be output*
- *2.7.2 Event types*

3 System Configuration

This chapter describes how to install JP1/ITDM2 - SDM components, set up certificates for SSL communication, and install JP1/ITDM2 - SDM (Smart Device Agent) on a smart device.

3.1 Flow of building a system

To build a system, you set up JP1/ITDM2 - SDM, and then install JP1/ITDM2 - SDM (Smart Device Agent) on each smart device to be managed.

To use JP1/ITDM2 - SDM, set up the smart device manager, communication server, and messaging server, and then install JP1/ITDM2 - SDM (Smart Device Agent) on the smart devices. The following describes the flow of setting up the smart device manager in an intranet environment (basic configuration) and setting up the communication server and messaging server in a DMZ environment.

1. Install JP1/ITDM2 - SDM (Smart Device Manager) on a host in the intranet environment.
   The host on which JP1/ITDM2 - SDM (Smart Device Manager) installed is the smart device manager.
2. Install JP1/ITDM2 - SDM (Communication Server).
   The host on which JP1/ITDM2 - SDM (Communication Server) is installed is the communication server.
3. Install JP1/ITDM2 - SDM (Messaging Server).
   The host on which JP1/ITDM2 - SDM (Messaging Server) is installed is the messaging server.
4. Open the ports on the router and setting up a firewall on each server.
5. Obtain certificates for SSL communication.
6. Set up certificates for SSL communication on the smart device manager.
7. Set up certificates for SSL communication on the communication server.
8. Log in to a program module and then set user account information.
9. Install JP1/ITDM2 - SDM (Smart Device Agent) on a smart device.

> **Important**
>
> To manage iOS devices, the condition shown below must be satisfied. For details, see the information provided by Apple.
>
> - Obtain a license for the Apple Developer Enterprise Program.

Related Topics

- *3.5 Procedure for installing JP1/ITDM2 - SDM (Smart Device Manager)*
- *3.6 Procedure for installing JP1/ITDM2 - SDM (Communication Server)*
- *3.7 Procedure for installing JP1/ITDM2 - SDM (Messaging Server)*
- *3.8 Opening ports on the router and setting up a firewall on each server*
- *3.11 Obtaining certificates for SSL communication*
- *3.12 Setting up certificates for SSL communication on the smart device manager*
- *3.13 Setting up certificates for SSL communication on the communication server*
- *3.14 Flow of installing JP1/ITDM2 - SDM (Smart Device Agent) on a smart device*
- *5.1 Logging in*
- *5.2 Setting user account information*

3.2 Prerequisite OSs

The following lists the prerequisite OSs for JP1/ITDM2 - SDM:

Target	Prerequisite OS
Smart device manager (host on which JP1/ITDM2 - SDM (Smart Device Manager) is installed)	Windows Server 2008 R2
	Windows Server 2012
	Windows Server 2012 R2
	Windows Server 2016
Communication server (host on which JP1/ITDM2 - SDM (Communication Server) is installed)	Windows Server 2008 R2
	Windows Server 2012
	Windows Server 2012 R2
	Windows Server 2016
Messaging server (host on which JP1/ITDM2 - SDM (Messaging Server) is installed)	Windows Server 2008 R2
	Windows Server 2012
	Windows Server 2012 R2
	Windows Server 2016
Smart device on which JP1/ITDM2 - SDM (Smart Device Agent) is installed	Android 4.1
	Android 4.3
	Android 5.0
	Android 6.0
	iOS 7.1
	iOS 8.1
	iOS 8.3
	iOS 8.4
	iOS 9.1
	iOS 9.2
	iOS 9.3
	iOS 10.0
	iOS 10.1
	iOS 10.2

3.3 Prerequisite programs

The prerequisite programs for JP1/ITDM2 - SDM are as follows:

- Internet Explorer 8 or later
- Firefox 24 or later

3.4 Components of JP1/ITDM2 - SDM

JP1/ITDM2 - SDM consists of the following components:

JP1/ITDM2 - SDM (Smart Device Manager)

Installed on a host in the intranet. The host on which JP1/ITDM2 - SDM (Smart Device Manager) is installed is referred to as the smart device manager.

JP1/ITDM2 - SDM (Communication Server)

Installed on a host having a global IP address in DMZ. The host on which JP1/ITDM2 - SDM (Communication Server) is installed is referred to as the communication server.

JP1/ITDM2 - SDM (Messaging Server)

Installed on a host having a global IP address in DMZ. This component can be installed on the same host as the communication server. The host on which JP1/ITDM2 - SDM (Messaging Server) is installed is referred to as the messaging server.

JP1/ITDM2 - SDM (Smart Device Android Agent)

A program installed on an Android device to provide the agent functionality

JP1/ITDM2 - SDM (Smart Device iOS Agent)

A program installed on an iOS device to provide the agent functionality

Related Topics

- *3.5 Procedure for installing JP1/ITDM2 - SDM (Smart Device Manager)*
- *3.6 Procedure for installing JP1/ITDM2 - SDM (Communication Server)*
- *3.7 Procedure for installing JP1/ITDM2 - SDM (Messaging Server)*
- *3.14 Flow of installing JP1/ITDM2 - SDM (Smart Device Agent) on a smart device*

3.5 Procedure for installing JP1/ITDM2 - SDM (Smart Device Manager)

Install JP1/ITDM2 - SDM (Smart Device Manager) on a host in the intranet environment. The host on which JP1/ITDM2 - SDM (Smart Device Manager) is installed is referred to as the smart device manager.

Prerequisites

You must log on to the OS as a user with administrator permissions.

Procedure

1. Insert the media supplied with the product in the CD/DVD drive.

2. In the **Hitachi Integrated Installer** dialog box that opens, select **JP1/IT Desktop Management 2 - Smart Device Manager**, and then click the **Install** button.

3. In the dialog box indicating the start of the installation, click the **Next** button.

4. In the **Permission Agreement** dialog box, check the displayed information, select **I accept the terms in license agreement**, and then click the **Next** button.
   If you do not want to accept the terms in the license agreement, click **Cancel**. The dialog box asking whether you want to cancel the installation of JP1/ITDM2 - SDM appears.
   - Click the **Yes** button to cancel the installation.
   - Click the **No** button to continue the installation.

5. In the **User Registration** dialog box, enter the user name and company name, and then click the **Next** button.

6. In the **Select Server** dialog box, select **Smart device manager**, and then click the **Next** button.

7. In the **Installation type** dialog box, select the installation type, and then click the **Next** button.
   If you choose **quick installation**, go to step 9.

8. In the **Installation folder** dialog box, specify the installation folder, and then click the **Next** button.

> **Important**
>
> To specify the installation folder, use a string that begins with the drive letter and contains only the characters shown below. The path name length must be 42 or fewer characters (bytes), including the backslash (\) at the end.
>
> Alphanumeric characters, underscore (_), period (.), space character, left parenthesis (( ), right parenthesis ( )), and path-delimiter backslash (\ )

9. In the confirmation dialog box for the installation, make sure the information you selected for the installation is correct, and then click the **Install** button.
   Installation starts. If you notice a problem during the installation, click the **Back** button and make the necessary correction.

10. When the installation finishes, click the **Completed** button.
    Installation of JP1/ITDM2 - SDM (Smart Device Manager) is complete. When a message that prompts you to log off appears, log off from JP1/ITDM2 - SDM.

11. Specify the environment setting file for the smart device manager.

12. Restart the `JP1/ITDM2 - Smart Device Manager Server Service` on the smart device manager.

Related Topics

- *3.1 Flow of building a system*
- *16.2 Smart device manager environment setting file (manager.properties)*

3.6 Procedure for installing JP1/ITDM2 - SDM (Communication Server)

Install JP1/ITDM2 - SDM (Communication Server). The host on which JP1/ITDM2 - SDM (Communication Server) is installed is referred to as the communication server.

Prerequisites

- The target host must have a global IP address and must be in DMZ.
- You must log on to the OS as a user with administrator permissions.

Procedure

1. Insert the media supplied with the product in the CD/DVD drive.
2. In the **Hitachi Integrated Installer** dialog box that opens, select **JP1/IT Desktop Management 2 - Smart Device Manager**, and then click the **Install** button.
3. In the dialog box indicating the start of the installation, click the **Next** button.
4. In the **Permission Agreement** dialog box, check the displayed information, select **I accept the terms in license agreement**, and then click the **Next** button.
   If you do not want to accept the terms in the license agreement, click **Cancel**. The dialog box asking whether you want to cancel the installation of JP1/ITDM2 - SDM appears.
   - Click the **Yes** button to cancel the installation.
   - Click the **No** button to continue the installation.
5. In the **User Registration** dialog box, enter the user name and company name, and then click the **Next** button.
6. In the **Select Server** dialog box, select **Communication server**, and then click the **Next** button.
7. In the **Database connects to** dialog box, specify the IP address or domain name, and then click the **Next** button.

   Tip

   You can use the `sdmnetchange` command to change the connection destination address for the database.

8. In the **Installation type** dialog box, select the installation type, and then click the **Next** button.
   If you choose **quick installation**, go to step 10.
9. In the **Installation folder** dialog box, specify the installation folder, and then click the **Next** button.

   Important

   To specify the installation folder, use a string that begins with the drive letter and that contains only the characters shown below. The path name length must be 42 or fewer characters (bytes), including the backslash (\) at the end

   Alphanumeric characters, underscore (_), period (.), space character, left parenthesis (( ), right parenthesis ( )), and path-delimiter backslash (\)

10. In the confirmation dialog box for the installation, make sure the information you selected for the installation is correct, and then click the **Install** button.

Installation starts. If you notice a problem during the installation, click the **Back** button and make the necessary correction.

11. When the installation finishes, click the **Completed** button.

    Installation of JP1/ITDM2 - SDM (Communication Server) is complete. When a message that prompts you to log off appears, log off from JP1/ITDM2 - SDM.

12. To change the operating environment for the communication server, change the communication server environment setting file.

13. If you changed the environment setting file, restart the `JP1/ITDM2 - Smart Device Manager (Communication Server Service)` on the communication server.

> **Note**
>
> When upgrading JP1/ITDM2 - SDM (Communication Server) from a version earlier than 11-10, you need to edit the `httpsd.conf` file.

Related Topics

- *3.1 Flow of building a system*
- *3.19.1 Tasks to perform when upgrading the communication server*
- *15. sdmnetchange (changing the network configuration for the smart device manager or communication server)*
- *16.6 Communication server environment setting file (CommunicationServerEngine.properties)*

3.7 Procedure for installing JP1/ITDM2 - SDM (Messaging Server)

Install JP1/ITDM2 - SDM (Messaging Server). The host on which JP1/ITDM2 - SDM (Messaging Server) is installed is referred to as the messaging server.

Prerequisites

- The target host must have a global IP address and must be in DMZ.
- You must log on to the OS as a user with administrator permissions.

Procedure

1. Insert the media supplied with the product in the CD/DVD drive.

2. In the **Hitachi Integrated Installer** dialog box that opens, select **JP1/IT Desktop Management 2 - Smart Device Manager**, and then click the **Install** button.

3. In the dialog box indicating the start of the installation, click the **Next** button.

4. In the **Permission Agreement** dialog box, check the displayed information, select **I accept the terms in license agreement**, and then click the **Next** button.

   If you do not want to accept the terms in the license agreement, click **Cancel**. The dialog box asking whether you want to cancel the installation of JP1/ITDM2 - SDM appears.

   - Click the **Yes** button to cancel the installation.
   - Click the **No** button to continue the installation.

5. In the **User Registration** dialog box, enter the user name and company name, and then click the **Next** button.

6. In the **Select Server** dialog box, select **Messaging server**, and then click the **Next** button.

7. In the **Installation type** dialog box, select the installation type, and then click the **Next** button.

   If you choose **quick installation**, go to step 9.

8. In the **Installation folder** dialog box, specify the installation folder, and then click the **Next** button.

   > **Important**
   >
   > To specify the installation folder, use a string that begins with the drive letter and that contains only the characters shown below. The path name length must be 42 or fewer characters (bytes), including the backslash (\) at the end.
   >
   > Alphanumeric characters, underscore (_), period (**.**), space character, left parenthesis (( ), right parenthesis ( )), and path-delimiter backslash (\)

9. In the confirmation dialog box for the installation, make sure the information you selected for the installation is correct, and then click the **Install** button.

   Installation starts. If you notice a problem during the installation, click the **Back** button and make the necessary correction.

10. When the installation finishes, click the **Completed** button.

    Installation of JP1/ITDM2 - SDM (Messaging Server) is complete. When a message that prompts you to log off appears, log off from JP1/ITDM2 - SDM.

11. To change the operating environment for the messaging server, change the messaging server environment setting file.

12. If you changed the environment setting file, restart `JP1/ITDM2 - Smart Device Manager (Messaging Server Service)` on the messaging server.

Related Topics

- *3.1 Flow of building a system*
- *16.7 Messaging server setting file (SdMessagingServer.ini)*

3.8 Opening ports on the router and setting up a firewall on each server

You need to open the ports on the router and set up a firewall on each server.

The following shows the port numbers used and the connection direction:

Port number	Connection direction					
	Internet -> DMZ	Internet <- DMZ	DMZ -> Intranet	DMZ <- Intranet	Intranet <- Internet	Intranet -> Internet
26080/tcp	--	--	--	--	Y	--
26055/tcp	Y	--	--	Y	--	--
2195/tcp	--	Y	--	--	--	--
80/tcp	--	Y	--	--	--	--
26079/tcp	Y	--	--	--	--	--
26067/tcp	--	--	Y	--	--	--
26068-26077/tcp	--	--	--	Y	--	--
5223/tcp	--	--	--	--	--	Y

Legend:

Y: Applicable connection direction

--: Inapplicable connection direction

The following describes the port numbers:

- 26080: Port for management modules
- 26055: HTTPS communication port
- 2195: Port for communication with the APNs server. This port is required only for managing iOS devices.
- 80: HTTPS communication port. This port is required only for managing iOS devices.
- 26079: Port for HTTP communication between an Android device and the messaging server.
- 26067: Port for communication between the communication server and the database in the smart device manager (database receiving port)
- 26068-26077: Ports for communication between the communication server and the database in the smart device manager (communication server receiving port)
- 5223: Port for communication between iOS devices and the APNs server. This port is required only for managing iOS devices connected via Wi-Fi.

Related Topics

- *3.1 Flow of building a system*
- *C. Port number list*

3.9 Types of certificates for SSL communication

The following describes the types of certificates required for JP1/ITDM2 - SDM to perform SSL communication.

Certificates for SSL communication required for JP1/ITDM2 - SDM

- Certificates for SSL communication for the communication server
  Obtain the following certificates from a Certificate Authority:
  - Root certificate for SSL communication
  - Server certificate for SSL communication
- Certificates for SSL communication for the smart device manager
  Obtain the following certificates from a Certificate Authority:
  - Root certificate for SSL communication
  - Server certificate for SSL communication
- Certificates for SSL communication for the APNs server (when managing iOS devices)
  To manage iOS devices, the following certificates are required:
  - Root certificate for SSL communication
  - Client certificates for SSL communication (for MDM)
    The file name is `APNsMDMPushDev.p12` in PKCS#12 format

    > **Important**
    >
    > This certificate must be updated every year.

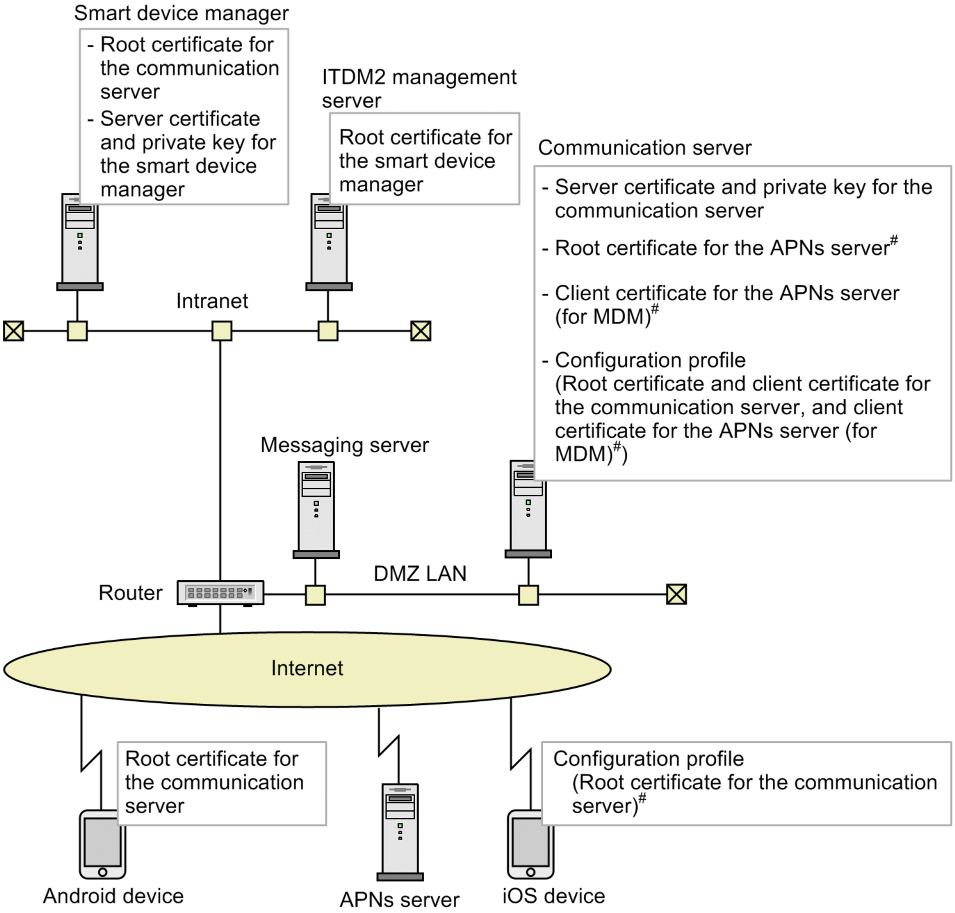
Related Topics

- *3.11 Obtaining certificates for SSL communication*
- *3.12 Setting up certificates for SSL communication on the smart device manager*
- *3.13 Setting up certificates for SSL communication on the communication server*
- *3.14.4 Procedure for setting up the root certificate for SSL communication on the Android device*
- *3.14.5 Procedure for setting root certificates for SSL communication on the iOS device*

3.10 Deployment of certificates for SSL communication

To perform SSL communication using JP1/ITDM2 - SDM, you need to deploy SSL communication certificates on the specified servers or smart devices.

The following figure shows the locations of the certificates for SSL communication:


Smart device manager
- Root certificate for the communication server
- Server certificate and private key for the smart device manager
ITDM2 management server
Root certificate for the smart device manager
Communication server
- Server certificate and private key for the communication server
- Root certificate for the APNs server#
- Client certificate for the APNs server (for MDM)#
- Configuration profile (Root certificate and client certificate for the communication server, and client certificate for the APNs server (for MDM)#)
Intranet
Messaging server
Router
DMZ LAN
Internet
Root certificate for the communication server
Configuration profile (Root certificate for the communication server)#
Android device
APNs server
iOS device

#: Required for managing iOS devices

3.11 Obtaining certificates for SSL communication

The required certificates for SSL communication are different depending on the OS of the smart device.

The following shows the operations for obtaining certificates for SSL communication and when each operation is required:

No.	Operation		Required?
1	Obtain certificates for SSL communication for the communication server.		Required
2	Obtain certificates for SSL communication for the smart device manager.		Required
3	Obtain a root certificate for SSL communication for the APNs server.		Required only for managing iOS devices
4	Obtain a client certificates for SSL communication for the APNs server (for MDM).	Download the MDM certificate request file.	Required only for managing iOS devices
		Create an MDM signed-certificate request file.	
		Create MDM client certificates.	

Related Topics

- *3.1 Flow of building a system*
- *3.11.1 Flow of obtaining certificates for SSL communication for the communication server*
- *3.11.2 Flow of obtaining certificates for SSL communication for the smart device manager*
- *3.11.3 Procedure for obtaining a root certificate for SSL communication for the APNs server (when managing iOS devices)*
- *3.11.4 Flow of obtaining the MDM client certificate for SSL communication for the APNs server (when managing iOS devices)*
- *3.11.5 Procedure for downloading the MDM certificate request file (when managing iOS devices)*
- *3.11.6 Procedure for creating an MDM signed-certificate request file (when managing iOS devices)*
- *3.11.7 Procedure for creating MDM client certificates (when managing iOS devices)*

3.11.1 Flow of obtaining certificates for SSL communication for the communication server

From a Certificate Authority, obtain certificates (root certificate and server certificate) for SSL communication for the communication server.

The flow of obtaining certificates for SSL communication for the communication server is as follows:

1. Create a private key for the Web server (`keygen` command).
   Specify the file containing the created private key for the Web server in the `SSLCertificateKeyFile` directive.
2. Create a Certificate Signing Request (CSR) (`certutil reqgen` command).
3. Display the contents of a Certificate Signing Request (CSR) (`certutil req` command).
   If necessary, check the contents of the Certificate Signing Request (CSR).
4. Send the CSR to the CA.

5. Acquire a certificate from the CA.

> **Tip**
>
> You can use the `certutil cert` command to check the contents of the certificate you obtained.

> **Tip**
>
> In the certificate you obtained, save the part from `-----BEGINCERTIFICATE-----` to `-----END CERTIFICATE----` in another file (`httpsd.pem` file defined in `httpsd.conf` provided as standard). Defining this file for the `SSLCertificateFile` directive enables use of SSL.

Related Topics

- *3.12.1 Procedure for setting up the root certificate for SSL communication for the communication server on the smart device manager*
- *3.13.2 Procedure for setting up server certificates for SSL communication on the communication server*
- *G.1 Creating a private key for the Web server (keygen command)*
- *G.2 Creating a Certificate Signing Request (CSR) (certutil reqgen command)*
- *G.3 Displaying the contents of a Certificate Signing Request (CSR) (certutil req command)*
- *G.4 Displaying certificate contents (certutil cert command)*
- *G.5 Converting the certificate format (certutil cert command)*

3.11.2 Flow of obtaining certificates for SSL communication for the smart device manager

From a Certificate Authority, obtain certificates (root certificate and server certificate) for SSL communication for the smart device manager.

The flow of obtaining certificates for SSL communication for the smart device manager is as follows:

1. Create a private key for the Web server (`keygen` command).
   Specify the file containing the created private key for the Web server in the `SSLCertificateKeyFile` directive.
2. Create a Certificate Signing Request (CSR) (`certutil reqgen` command).
3. Display the contents of a Certificate Signing Request (CSR) (`certutil req` command).
   If necessary, check the contents of the Certificate Signing Request (CSR).
4. Send the CSR to the CA.
5. Acquire a certificate from the CA.

> **Tip**
>
> You can use the `certutil cert` command to check the contents of the certificate you obtained.

Tip

In the certificate you obtained, save the part from `-----BEGINCERTIFICATE-----` to `-----END CERTIFICATE----` in another file (`httpsd.pem` file defined in `httpsd.conf` provided as standard). Defining this file for the `SSLCertificateFile` directive enables use of SSL.

Important

The obtained certificates must also be set up on the JP1/IT Desktop Management 2 management server.

Related Topics

- *3.12.2 Procedure for setting up server certificates for SSL communication on the smart device manager*
- *G.1 Creating a private key for the Web server (keygen command)*
- *G.2 Creating a Certificate Signing Request (CSR) (certutil reqgen command)*
- *G.3 Displaying the contents of a Certificate Signing Request (CSR) (certutil req command)*
- *G.4 Displaying certificate contents (certutil cert command)*
- *G.5 Converting the certificate format (certutil cert command)*

3.11.3 Procedure for obtaining a root certificate for SSL communication for the APNs server (when managing iOS devices)

Because the APNs server uses Entrust server certificates, an Entrust root certificate is required. You need to obtain a root certificate for SSL communication for the APNs server from the Entrust website as described below only when managing iOS devices.

Procedure

1. Access the Entrust website.

2. Select **Personal Use and Secure Server Installation**, and then click the **Download Certificates** button.

3. Click **Root Certificates** to download `entrust_2048_ca.cer`.

Related Topics

- *3.13.1 Procedure for setting up the APNs server's root certificate for SSL communication on the communication server (when managing iOS devices)*

3.11.4 Flow of obtaining the MDM client certificate for SSL communication for the APNs server (when managing iOS devices)

Obtain the MDM client certificate (`APNsMDMPushDev.p12` file) from the iOS Dev Center.

The following shows the flow of obtaining the MDM client certificate, which is required only when managing iOS devices.

1. Download the MDM certificate request file.
2. Create an MDM signed-certificate request file.
3. Create the MDM client certificate.

Related Topics

- *3.11.5 Procedure for downloading the MDM certificate request file (when managing iOS devices)*
- *3.11.6 Procedure for creating an MDM signed-certificate request file (when managing iOS devices)*
- *3.11.7 Procedure for creating MDM client certificates (when managing iOS devices)*
- *3.13.3 Procedure for setting up the APNs server's client certificates for SSL communication on the communication server (when managing iOS devices)*
- *3.13.4 Procedure for creating a configuration profile on the communication server (when managing iOS devices)*

3.11.5 Procedure for downloading the MDM certificate request file (when managing iOS devices)

To create an MDM signed-certificate request file, download the MDM certificate request file (`mdm.cer`). This procedure is required only when managing iOS devices.

Prerequisites

- You must purchase a license for the Apple Developer Enterprise Program.
- You must contact Apple to register as MDM vendor.
- You must perform the procedure on a Mac PC.

Procedure

1. Log in to the iOS Dev Center. From **iOS Developer Program**, click **Certificates, Identifiers & Profiles**.

2. Click **Certificates**.

3. Click the **+ (Add)** button.

4. From **Production**, select **MDM CSR**, and then click the **Continue** button.

5. In the window that explains upload of a certificate request, click the **Continue** button.

6. Use Keychain Access to create a Certificate Signing Request (CSR).
   Specify the following items as certificate information:

   User Email Address

   Enter the email address that was used to register your iOS development license.

   Common Name

   Set any name.

   > **Tip**
   >
   > The name set here will be used when you create an MDM signed-certificate request file.

Request is

Select **Saved to disk**.

Let me specify key pair information

Select this check box.

7. Upload the created CSR (Certificate Signing Request).

8. Download the created MDM certificate request file (`mdm.cer`).

Postrequisites

Create an MDM signed-certificate request file.

Related Topics

- *3.11.4 Flow of obtaining the MDM client certificate for SSL communication for the APNs server (when managing iOS devices)*
- *3.11.6 Procedure for creating an MDM signed-certificate request file (when managing iOS devices)*
- *3.11.7 Procedure for creating MDM client certificates (when managing iOS devices)*

3.11.6 Procedure for creating an MDM signed-certificate request file (when managing iOS devices)

To create MDM client certificates, you need to change the format of the MDM certificate request file, and then create an MDM signed-certificate request file. You need to perform this procedure only when managing iOS devices.

Prerequisites

- You must purchase a license for the Apple Developer Enterprise Program.
- You must contact Apple to register as MDM vendor.
- You must perform the procedure on a Mac PC.
- You must download the MDM certificate request file (`mdm.cer`) in advance.

Procedure

1. Double-click the downloaded MDM certificate request file (`mdm.cer`) to import it to Keychain Access, and then export the file in PKCS#12 format.
   Specify `vendor.p12` as the export file name.

   > **Tip**
   >
   > Set a password when exporting the file. The password set here will be registered in step 6.

2. Obtain the following root certificate and intermediate certificate from Apple:
   - Apple Inc. Root Certificate (AppleIncRootCertificate.cer)
   - WWDR Certificate (AppleWWDRCA.cer)

> **Important**
>
> The name of the root certificate and intermediate certificate might be different. For details, see the information provided by Apple.

3. From the terminal, execute the following commands provided from OS to convert the `cer` files to `pem` format:

```
openssl x509 -inform der -in mdm.cer -out mdm.pem
openssl x509 -inform der -in AppleWWDRCA.cer -out intermediate.pem
openssl x509 -inform der -in AppleIncRootCertificate.cer -out root.pem
```

4. Execute the following commands from the terminal to create a customer certificate request:
   - Create a private key:

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

   - Create the customer certificate request:

```
openssl req -new -key customerPrivateKey.pem -out customer.csr
```

   - Convert the customer certificate request to `der` file format:

```
openssl req -inform pem -outform der -in customer.csr -out customer.der
```

5. Copy the following five created files to the communication server:
   - customer.der
   - vendor.p12
   - mdm.pem
   - intermediate.pem
   - root.pem

6. Execute the following command from the command prompt to create an MDM signed-certificate request file:

```
sdmcreatemdmcertreq -f "folder-storing-files" -o "MDM-signed-certificate-
request-file-output-folder" -a common-name-set-when-creating-the-
certificate-request-file -p password-set-when-exporting-vendor.p12
```

Postrequisites

Create MDM client certificates.

Related Topics

- *3.11.4 Flow of obtaining the MDM client certificate for SSL communication for the APNs server (when managing iOS devices)*
- *3.11.5 Procedure for downloading the MDM certificate request file (when managing iOS devices)*
- *3.11.7 Procedure for creating MDM client certificates (when managing iOS devices)*
- *15. sdmcreatemdmcertreq (creating an MDM signed-certificate request file)*

3.11.7 Procedure for creating MDM client certificates (when managing iOS devices)

Upload the MDM signed-certificate request file to create MDM client certificates. You need to perform this procedure only when managing iOS devices.

Prerequisites

- You must purchase a license for the Apple Developer Enterprise Program.
- You must contact Apple to register as MDM vendor.
- You must perform the procedure below on the Mac computer to which the MDM certificate request file was downloaded or created.
- You must create the MDM signed-certificate request file in advance.

Procedure

1. Log in to Apple Push Certificates Portal.

2. Click the **Create a Certificate** button.

3. Select the check box for accepting the terms of the license agreement, and then click the **Accept** button.

4. Select the `plist_encoded` file to be uploaded, and then click the **Upload** button.
   When the file is uploaded successfully, an MDM certificate file is created.

5. Click the **Download** button to obtain the certificate file (`mdm_vendor.pem`).

6. Click the information icon (Certificate Info), and then confirm the UID of the Subject DN.

> **Tip**
>
> You need the UID when creating a configuration profile communication server in order to distribute client certificates to iOS devices.

7. Execute the following command to create the `APNsMDMPushDev.p12` file from the private key and `pem` file:

```
openssl pkcs12 -export -inkey customerPrivateKey.pem -in mdm_vendor.pem -
out APNsMDMPushDev.p12
```

Related Topics

- *3.11.4 Flow of obtaining the MDM client certificate for SSL communication for the APNs server (when managing iOS devices)*
- *3.11.5 Procedure for downloading the MDM certificate request file (when managing iOS devices)*
- *3.11.6 Procedure for creating an MDM signed-certificate request file (when managing iOS devices)*
- *3.13.4 Procedure for creating a configuration profile on the communication server (when managing iOS devices)*

3.12 Setting up certificates for SSL communication on the smart device manager

This section describes how to set up, on the smart device manager, certificates for SSL communication for the communication server and smart device manager.

3.12.1 Procedure for setting up the root certificate for SSL communication for the communication server on the smart device manager

On the smart device manager, set up the root certificate for SSL communication for the communication server.

Procedure

1. Execute the following command to install the root certificate:

   ```
   "JP1/ITDM2 - SDM (Smart Device Manager)-installation-folder\mgr\uC\jdk\bin\keytool.exe" -importcert -alias alias-name# -file certificate-path -keystore "JP1/ITDM2 - SDM (Smart Device Manager)-installation-folder\mgr\uC\jdk\jre\lib\security\cacerts" -storepass changeit
   ```

   To check the installed root certificate, execute the following command:

   ```
   "JP1/ITDM2 - SDM (Smart Device Manager)-installation-folder\mgr\uC\jdk\bin\keytool.exe" -list -v -storepass changeit -keystore "JP1/ITDM2 - SDM (Smart Device Manager)-installation-folder\mgr\uC\jdk\jre\lib\security\cacerts"
   ```

   To delete the certificate from the keystore, execute the following command:

   ```
   "JP1/ITDM2 - SDM (Smart Device Manager)-installation-folder\mgr\uC\jdk\bin\keytool.exe" -delete -alias alias-name# -keystore "JP1/ITDM2 - SDM (Smart Device Manager)-installation-folder\mgr\uC\jdk\jre\lib\security\cacerts" -storepass changeit
   ```

   #: You can specify any alias name.

   > **Important**
   >
   > If the `keytool.exe` command ends abnormally, the keystore file might be set to **read-only**. In this case, cancel the read-only attribute of the keystore file, and then re-execute the command.
   >
   > The following shows the path to the keystore file and how to cancel the read-only attribute.
   >
   > Keystore file path: "*JP1/ITDM2 - SDM (Smart Device Manager)-installation-folder*`\mgr\uC\jdk\jre\lib\security\cacerts`"
   >
   > 1. Right-click the keystore file, and then select **Properties**.
   > 2. On the **General** tab, clear the **Attributes** check box for **Read-only**.
   > 3. Click **OK**.

Related Topics

- *3.1 Flow of building a system*
- *3.11.1 Flow of obtaining certificates for SSL communication for the communication server*

3.12.2 Procedure for setting up server certificates for SSL communication on the smart device manager

Set up the server certificate for SSL communication and private key on the smart device manager.

Procedure

1. Store the server certificate for SSL communication and private key in the following folder:
   JP1/ITDM2 - SDM (Smart Device Manager)-installation-folder\mgr\uC\httpsd\conf\ssl\server

2. Add the definitions to the `httpsd.conf` file.
   The `httpsd.conf` file is stored in the following location:
   JP1/ITDM2 - SDM (Smart Device Manager)-installation-folder\mgr\uC\httpsd\conf
   Add the following lines and comment out the lines described below.

```
ServerName localhost or host-name

#--Omitted--
Listen 26080
<VirtualHost localhost or host-name:26080>
<Location /jp1itdm2sdm>
     Allow from all
</Location>
</VirtualHost>

Listen 26056
<VirtualHost localhost:26056>
<Location /rest>
     Allow from command
</Location>
</VirtualHost>

#--Uncomment out the following lines--
Listen 26055
<VirtualHost host-name:26055>
    SSLEnable
    SSLProtocol TLSv1 TLSv11 TLSv12
    SSLCertificateFile "JP1/ITDM2 - SDM (Smart Device Manager)-
installation-folder/mgr/uC/httpsd/conf/ssl/server/newcert.pem"
    SSLCertificateKeyFile "JP1/ITDM2 - SDM (Smart Device Manager)-
installation-folder/mgr/uC/httpsd/conf/ssl/server/newkeyRSA.pem"
    #SSLCertificateKeyPassword "JP1/ITDM2 - SDM (Smart Device Manager)-
installation-folder/mgr/uC/httpsd/conf/ssl/server/.keypasswd"
    LoadModule proxy_module modules/mod_proxy.so
    LoadModule proxy_http_module modules/mod_proxy_http.so
    <Location /server01/api/v1.0>
        ProxyPass http://localhost:26057/rest/itdmsdapi
        Allow from all
    </Location>
    <Location /server01/api/version>
        ProxyPass http://localhost:26057/rest/itdmsdapi/version
        Allow from all
    </Location>
</VirtualHost>

Listen 26057
```

```
<VirtualHost localhost:26057>
<Location /rest>
     Allow from all
</Location>
</VirtualHost>
#--End of the change--

Include "JP1/ITDM2 - SDM (Smart Device Manager)-installation-folder/mgr/uC/CC/web/redirector/mod_jk.conf"
```

Legend:

`httpsd.pem`: Server certificate file name (PEM format)

`httpsdkey.pem`: Private key file name (PEM format)

`.keypasswd`: Password file name

> **Important**
>
> If you set a password when creating the private key for the Web server, you need to create a password file by using the `sslpasswd` command, and then set the `SSLCertificateKeyPassword` directive.

Related Topics

- *3.1 Flow of building a system*
- *3.11.2 Flow of obtaining certificates for SSL communication for the smart device manager*
- *G.6 Create a password file (sslpasswd command)*

3.13 Setting up certificates for SSL communication on the communication server

This section describes how to set up, on the communication server, certificates for SSL communication for the communication server and APNs server. This section also describes how to create a configuration profile for distributing client certificates to iOS devices.

3.13.1 Procedure for setting up the APNs server's root certificate for SSL communication on the communication server (when managing iOS devices)

On the communication server, set up the root certificate for SSL communication for the APNs server. You need to perform this procedure only when managing iOS devices.

Procedure

1. Execute the following command to install the root certificate:

   "*JP1/ITDM2 - SDM (Communication Server)-installation-folder*`\cms\uC\jdk\bin\keytool.exe" -importcert -alias` *alias-name*# `-file` *certificate-path* `-keystore "`*JP1/ITDM2 - SDM (Communication Server)-installation-folder*`\cms\uC\jdk\jre\lib\security\cacerts" -storepass changeit`

   To check the installed root certificate, execute the following command:

   "*JP1/ITDM2 - SDM (Communication Server)-installation-folder*`\cms\uC\jdk\bin\keytool.exe" -list -v -storepass changeit -keystore "`*JP1/ITDM2 - SDM (Communication Server)-installation-folder*`\cms\uC\jdk\jre\lib\security\cacerts"`

   To delete the certificate from the keystore, execute the following command:

   "*JP1/ITDM2 - SDM (Communication Server)-installation-folder*`\cms\uC\jdk\bin\keytool.exe" -delete -alias` *alias-name*# `-keystore "`*JP1/ITDM2 - SDM (Communication Server)-installation-folder*`\cms\uC\jdk\jre\lib\security\cacerts" -storepass changeit`

   #: You can specify any alias name.

   > **Important**
   >
   > If the `keytool.exe` command ends abnormally, the keystore file might be set to **read-only**. In this case, cancel the read-only attribute of the keystore file, and then re-execute the command.
   >
   > The following shows the path to the keystore file and how to cancel the read-only attribute.
   >
   > Keystore file path:"*JP1/ITDM2 - SDM (Communication Server)-installation-folder*`\cms\uC\jdk\jre\lib\security\cacerts"`
   >
   > 1. Right-click the keystore file, and then select **Properties**.
   > 2. On the On the **General** tab, clear the **Attributes** check box for **Read-only**.
   > 3. Click **OK**.

Related Topics

- *3.1 Flow of building a system*

- *3.11.3 Procedure for obtaining a root certificate for SSL communication for the APNs server (when managing iOS devices)*

3.13.2 Procedure for setting up server certificates for SSL communication on the communication server

On the communication server, set up the server certificate for SSL communication and private key for the communication server.

Procedure

1. Store the server certificate for SSL communication and private key in the following folder:

   JP1/ITDM2 - SDM (Communication Server)-installation-folder`\cms\uC\httpsd\conf\ssl\server`

2. Add the definitions to the `httpsd.conf` file.

   The `httpsd.conf` file is stored in the following location:

   JP1/ITDM2 - SDM (Communication Server)-installation-folder`\cms\uC\httpsd\conf`

   Add the following lines:

```
ServerName host-name

#--Omitted--
Listen 26055
<VirtualHost host-name:26055>
    SSLEnable
    SSLProtocol TLSv11 TLSv12
    SSLCertificateFile "JP1/ITDM2 - SDM (Communication Server)-
installation-folder/cms/uC/httpsd/conf/ssl/server/newcert.pem"
    SSLCertificateKeyFile "JP1/ITDM2 - SDM (Communication Server)-
installation-folder/cms/uC/httpsd/conf/ssl/server/newkeyRSA.pem"
</VirtualHost>
Include "JP1/ITDM2 - SDM (Communication Server)-installation-
folder/cms/uC/CC/web/redirector/mod_jk.conf"
```

   Legend:

   `httpsd.pem`: Server certificate file name (PEM format)

   `httpsdkey.pem`: Private key file name (PEM format)

   `.keypasswd`: Password file name

   > **Important**
   >
   > If you set a password when creating the private key for the Web server, you need to create a password file by using the `sslpasswd` command, and then set the `SSLCertificateKeyPassword` directive.

3. Restart the `JP1/ITDM2 - Smart Device Manager Web Server` on the communication server.

Related Topics

- *3.1 Flow of building a system*
- *3.11.1 Flow of obtaining certificates for SSL communication for the communication server*

- *G.6 Create a password file (sslpasswd command)*

3.13.3 Procedure for setting up the APNs server's client certificates for SSL communication on the communication server (when managing iOS devices)

On the communication server, store the MDM client certificate and the file containing the password for MDM client certificates. You need to perform this procedure only when managing iOS devices.

Procedure

1. In the following folder on the communication server, store the MDM client certificate (`APNsMDMPushDev.p12` file in PKCS#12 format), and the `password` file containing the password of the MDM client certificate.

   JP1/ITDM2 - SDM (Communication Server)-installation-folder`\cms\conf`

2. Restart the `JP1/ITDM2 - Smart Device Manager (Communication Server Service)` on the communication server.

Related Topics

- *3.1 Flow of building a system*
- *3.11.4 Flow of obtaining the MDM client certificate for SSL communication for the APNs server (when managing iOS devices)*

3.13.4 Procedure for creating a configuration profile on the communication server (when managing iOS devices)

Create a configuration profile on the communication server in order to distribute client certificates to iOS devices. You need to perform this procedure only when managing iOS devices.

(1) Procedure when using the iPhone Configuration Utility

Prerequisites

The following procedure is provided based on the iPhone Configuration Utility version 3.6.

Procedure

1. Install the Apple iPhone Configuration Utility.

2. In the left pane of the window, select **Library**, and then **Configuration Profiles**. Then, click the **New** button at the top of the window.

3. Specify the **General** settings as follows:

Item	Specifiable value
Name	Any
Identifier	Any

Item	Specifiable value
Organization	Any
Description	Any
Consent Message	Any
Security	Select **With Authentication**.
Automatically Remove Profile	Select **Never**.

4. For the **Credentials** setting, select the root certificate used for connecting iOS devices to the communication server. Enter the credential name, and then add the root certificate. (This step is required if the root certificate for the communication server is not installed on an iOS device.)

   Tip

   You can also set root certificates for individual iOS devices.

5. In the **Credentials** settings, select the client certificate (`APNsMDMPushDev.p12`) used by iOS devices to connect to the APNs server. Then, enter the credential name and the password for the certificate, and then add the client certificate.

6. Specify the **Mobile Device Management Settings** information as follows:

Item	Specifiable value
Server URL	https://*communication-server-host-name*:26055/CommunicationServerWeb/ios/server
Check in URL	https://*communication-server-host-name*:26055/CommunicationServerWeb/ios/checkin
Topic	Set the UID in the Subject DN of the MDM certificate created by using the Apple Push Certificates Portal.
Identity	In the list, select the credential name specified in step 5, which is used for connecting to the APNs server.
Sign messages	Select the check box.
Check Out When Removed	Select the check box.
Access Rights	Select all check boxes.
Apple Push Notification Server	Clear the check box.

7. Click the **Export** button at the top of the window, select **Sign Configuration Profile**, and then export the configuration profile.
   For the file name, specify `mdmprofile.mobileconfig`.

8. Store the configuration profile in the following folder on the communication server:
   JP1/ITDM2 - SDM (Communication Server)-installation-folder`\cms\conf`

Related Topics

- *3.1 Flow of building a system*
- *3.11.1 Flow of obtaining certificates for SSL communication for the communication server*
- *3.11.4 Flow of obtaining the MDM client certificate for SSL communication for the APNs server (when managing iOS devices)*
- *3.11.7 Procedure for creating MDM client certificates (when managing iOS devices)*

(2) Procedure when using the configuration profile generation tool

Procedure

1. Start the configuration profile generation tool.

   The configuration profile generation tool is stored in the following location:

```
JP1/ITDM2 - SDM (Communication Server)-installation-folder\cms\bin
\sdmgeneratemobileconf.exe
```

2. Specify the **General** settings as follows:

Item	Description	Required
Name	Display name of the profile	Y
Identifier	Identifier of the profile	Y
Organization	Organization name of the profile	--
Description	Description of the profile	Y
Consent	Message which is shown when the profile is installed.	--
Security	Security options when the profile is deleted. Always: Confirmation on the iOS device is required to delete the profile. Authentication: A password must be entered to delete the profile. None: The profile cannot be deleted.	Y

   Legend:

   Y: Required

   --: Optional

3. For the **Credentials** setting, select the client certificate used by iOS devices to connect to the communication server. Enter the credential name and the password for the certificate, and then add the client certificate.

4. Specify the **Mobile Device Management Settings** information as follows:

Item	Specifiable value	Required
Server URL	https://*communication-server-host-name*:26055/CommunicationServerWeb/ios/server	Y
Check in URL	https://*communication-server-host-name*:26055/CommunicationServerWeb/ios/checkin	Y
Topic	Set the UID in the Subject DN of the MDM certificate created by using the Apple Push Certificates Portal.	Y

   Legend:

   Y: Required

5. Click the **Generate** button, and then export the configuration profile.

   For the file name, specify `mdmprofile.mobileconfig`.

6. Store the configuration profile in the following folder on the communication server:

JP1/ITDM2 - SDM (Communication Server)-installation-folder`\cms\conf`

Related Topics

- *3.1 Flow of building a system*
- *3.11.1 Flow of obtaining certificates for SSL communication for the communication server*
- *3.11.4 Flow of obtaining the MDM client certificate for SSL communication for the APNs server (when managing iOS devices)*
- *3.11.7 Procedure for creating MDM client certificates (when managing iOS devices)*

3.14 Flow of installing JP1/ITDM2 - SDM (Smart Device Agent) on a smart device

The following describes the flow of installing JP1/ITDM2 - SDM (Smart Device Agent) on a smart device used in the organization, and starting the smart device management.

1. Define security principles.
2. Register security rules.
3. Understand the smart devices in your organization.

   Create a smart device management ledger. Based on the ledger information, determine the smart devices to be managed by JP1/ITDM2 - SDM. In addition, obtain registration information of the smart devices.
4. Set up a provisioning.
5. Check the root certificates for SSL communication preinstalled on the smart device.
6. Set the root certificates for SSL communication on the smart device (only when necessary certificates are not preinstalled).
7. Register smart device information in JP1/ITDM2 - SDM.
8. Use JP1/ITDM2 - SDM to set the password for SSL communication with the APNs server.
9. Plan JP1/ITDM2 - SDM (Smart Device Agent) installation.

   Install JP1/ITDM2 - SDM (Smart Device Agent) in either of the following ways:
   - The administrator installs JP1/ITDM2 - SDM (Smart Device Agent), and then distributes it to the user.
   - After distributing the smart device to the user, ask the user to install JP1/ITDM2 - SDM (Smart Device Agent).
10. Install JP1/ITDM2 - SDM (Smart Device Agent) on the smart device.

    The administrator or user installs JP1/ITDM2 - SDM (Smart Device Agent) on the smart device.
11. Confirm that JP1/ITDM2 - SDM (Smart Device Agent) is installed.

    If JP1/ITDM2 - SDM (Smart Device Agent) is installed on the smart device, inventory information is periodically reported to JP1/ITDM2 - SDM. If inventory information has not been sent from the managed smart device for a specified period of time, an event is issued. Therefore, by checking whether an event was issued, you can understand whether JP1/ITDM2 - SDM (Smart Device Agent) is installed on smart device.
12. Send a notification email indicating that JP1/ITDM2 - SDM (Smart Device Agent) must be installed (only for users who have not installed JP1/ITDM2 - SDM (Smart Device Agent).

Related Topics

- *2.4.1 Types of security rules*
- *3.14.1 Defining the organization's security principles*
- *3.14.2 Provisioning settings*
- *3.14.3 Procedure for checking the root certificates for SSL communication preinstalled on the smart device*
- *3.14.4 Procedure for setting up the root certificate for SSL communication on the Android device*
- *3.14.5 Procedure for setting root certificates for SSL communication on the iOS device*
- *3.14.6 Procedure for installing JP1/ITDM2 - SDM (Smart Device Android Agent) on an Android device (using the Android device only)*
- *3.14.7 Procedure for installing JP1/ITDM2 - SDM (Smart Device Android Agent) on an Android device (for a PC)*
- *3.14.8 Procedure for installing JP1/ITDM2 - SDM (Smart Device iOS Agent) on an iOS device*

- *7.1 Using security policies*
- *7.2 Using Android policies*
- *7.3 Using iOS profiles*
- *8.1 Registering smart devices in JP1/ITDM2 - SDM*

3.14.1 Defining the organization's security principles

Define the organization's security principles to manage smart device security.

The following are essential points of security principles to be defined:

- To ensure that hard-to-guess unlock passwords are set for smart devices, create a password policy.
- To restrict users to access phone numbers that are required for jobs, create a list of allowed phone numbers.
- If some applications must be installed or if you want to prohibit use of applications, create a list of required or prohibited applications.
- To permit or prohibit web browsing of some sites, create a list of allowed or prohibited sites.
- To prohibit some smart device functions (such as cameras), create a list of prohibited functions.

These points will differ depending on the group in the organization and contents of work. Cooperate with the security administrators of each department to define security principles applicable to the contents of each job.

We recommend that you understand security trends, and periodically review security principles in order to maintain robust security management.

Related Topics

- *2.4 Managing security*

3.14.2 Provisioning settings

Provisioning information means the configuration information for JP1/ITDM2 - SDM (Smart Device Agent) that runs on the smart device.

The configuration information includes the following:

- URL of the connected communication server
- URL of the connected messaging server
- Inventory data collection interval
- GPS information collection interval
- Battery capacity for sending inventory data in the event of low voltage

The provisioning settings take effect by updating the provisioning information setting file (`provisioning.properties`), and then restarting the service.

Related Topics

- *16.3 Provisioning information setting file (provisioning.properties)*

3.14.3 Procedure for checking the root certificates for SSL communication preinstalled on the smart device

Confirm that the necessary root certificates for SSL communication are preinstalled on the smart device.

Procedure

1. On the smart device, do the following:

   For an iOS device:

   Tap **Settings**, **General**, **About**, and then **Trust Store** to access the Apple's website. In the Apple's website, check the list of root certificates preinstalled on the iOS device.

   For an Android device:

   Confirm the root certificate list. The procedure for displaying the root certificate list depends on the device and OS type. For information about the procedure, contact the manufacturer of your device.

   For Android 4.1.1, the procedure is as follows:

   Tap **Settings**, **Security**, and then **Trusted credentials**. Check the list of root certificates.

Postrequisites

If the necessary root certificate for SSL communication is preinstalled, you do not have to set up a root certificate on the smart device.

If the necessary root certificate for SSL communication is not preinstalled, obtain the certificate, and then set it up on the smart device.

Related Topics

- *3.11.1 Flow of obtaining certificates for SSL communication for the communication server*
- *3.11.3 Procedure for obtaining a root certificate for SSL communication for the APNs server (when managing iOS devices)*
- *3.14.4 Procedure for setting up the root certificate for SSL communication on the Android device*
- *3.14.5 Procedure for setting root certificates for SSL communication on the iOS device*

3.14.4 Procedure for setting up the root certificate for SSL communication on the Android device

On the Android device, install the root certificate for SSL communication for the communication server. You need to perform this procedure only when the root certificate for SSL communication is not installed.

Procedure

1. Save the root certificate file in the internal storage of the device or the root directory of an SD card.

   The extension of the root certificate file is `.cer` or `.crt`.

2. Select whether to install the root certificate from the storage or SD card.

   To install the root certificate from storage:

   Select **Settings**, **Personal**, **Security**, **Credential storage**, and then **Install from device memory**.

   To install the root certificate from an SD card:

   Select **Settings**, **Personal**, **Security**, **Credential storage**, and then **Install from SD card**.

3. Select the root certificate to be installed.

4. Enter the certificate name, and then tap **OK**.
   Installation is complete.

5. Confirm that the certificate has been installed.
   Select **Settings**, **Personal**, **Security**, **Credential storage**, and then **Trusted credentials**. On the **User** tab, confirm that the certificate has been installed.

Related Topics

- *3.14.3 Procedure for checking the root certificates for SSL communication preinstalled on the smart device*

3.14.5 Procedure for setting root certificates for SSL communication on the iOS device

On the iOS device, install the communication server's root certificate for SSL communication and the Root certificate for SSL communication for the APNs server. You need to perform this procedure only when the necessary root certificates for SSL communication are not installed.

Procedure

1. Launch the iPhone Configuration Utility.

2. Tap **Library**, **Configuration Profiles**, and then tap **New**.

3. Tap **Credentials**, and then tap the **Configuration** button in the right pane.

4. Select the root certificate you obtained.

5. Tap **General**, and then enter any values in the **Name** and **Identifier** fields.

6. Under **Devices**, select the device name. Then, tap the **Configuration Profiles** tab, and then tap the **Install** button.

7. In the profile installation window that appears, tap the **Install** button.

8. In the confirmation message dialog box for the installation, tap the **Install** button.

9. In the installation completion window, tap the **Completed** button.

Related Topics

- *3.14.3 Procedure for checking the root certificates for SSL communication preinstalled on the smart device*

3.14.6 Procedure for installing JP1/ITDM2 - SDM (Smart Device Android Agent) on an Android device (using the Android device only)

Install JP1/ITDM2 - SDM (Smart Device Android Agent) (application name: JP1ITDM2SDM) on the Android device, and then set up JP1/ITDM2 - SDM (Smart Device Android Agent). This procedure uses the Android device only.

Procedure

1. Launch the Google Play Store application.

2. Tap the Play Store icon, and then select **My apps**.

3. Select **ALL** as the category.

4. Select JP1/ITDM2 - SDM (Smart Device Android Agent) (application name: JP1ITDM2SDM), and then tap the **Install** button on the application detail page.

   JP1/ITDM2 - SDM (Smart Device Android Agent) is installed.

5. On the Android device, start JP1/ITDM2 - SDM (Smart Device Android Agent).

6. In the Settings window, enter the host name of the connection destination communication server and smart device name, and then tap **OK**.

   For the communication server, enter the host name in *host-name*`:26055` format. For the name, specify the smart device name registered in JP1/ITDM2 - SDM.

   When the server is connected successfully, a dialog box indicating so appears.

7. Tap **OK** in the dialog box.

3.14.7 Procedure for installing JP1/ITDM2 - SDM (Smart Device Android Agent) on an Android device (for a PC)

The following describes how to use a PC to install JP1/ITDM2 - SDM (Smart Device Android Agent) (application name: JP1ITDM2SDM) on the Android device, and then set up JP1/ITDM2 - SDM (Smart Device Android Agent).

Procedure

1. On the PC, access the **My apps** page of Google Play.

2. Select the application, and then display its detail page.

3. Click the **Install** or **Installed** button, and then select the device on which you want to install the application.

4. Click **Install**.

   JP1/ITDM2 - SDM (Smart Device Android Agent) is installed.

5. On the Android device, start JP1/ITDM2 - SDM (Smart Device Android Agent).

6. In the Settings window, enter the host name of the connection destination communication server and smart device name, and then tap **OK**.

   For the communication server, enter the host name in *host-name*`:26055` format. For the name, specify the smart device name registered in JP1/ITDM2 - SDM.

   When the server is connected successfully, a dialog box indicating this fact appears.

7. Tap **OK** in the dialog box.

3.14.8 Procedure for installing JP1/ITDM2 - SDM (Smart Device iOS Agent) on an iOS device

Install JP1/ITDM2 - SDM (Smart Device iOS Agent) (application name: JP1ITDM2SDM) on the iOS device, and then set up JP1/ITDM2 - SDM (Smart Device iOS Agent).

Procedure

1. From the App Store, download and install JP1/ITDM2 - SDM (Smart Device iOS Agent) (application name: JP1ITDM2SDM).

2. On the iOS device, start JP1/ITDM2 - SDM (Smart Device iOS Agent).

3. In the Communication Server Settings window, enter the host name of the connection destination communication server and smart device name, and then tap **OK**.

   For the communication server, enter the host name in *host-name*`:26055` format. For the name, specify the smart device name registered in JP1/ITDM2 - SDM.

   When the server is connected successfully, a dialog box indicating so appears.

4. Tap **OK** in the dialog box.

3.15 Procedure for uninstalling JP1/ITDM2 - SDM from the server

If you want to re-install JP1/ITDM2 - SDM, you must first uninstall JP1/ITDM2 - SDM (Smart Device Manager), and JP1/ITDM2 - SDM (Communication Server) or JP1/ITDM2 - SDM (Messaging Server) from the server.

Prerequisites

- You must log on to the server by using a user account with administrator permissions.
- We recommend that you stop any running JP1/ITDM2 - SDM programs.

Procedure

1. In the Windows Control panel, select **Programs and Features**.
   A dialog box listing programs that can be uninstalled appears.

2. Select the JP/ITDM2 - SDM programs to be uninstalled, and then click the **Uninstall** button.

3. In the dialog box indicating the start of the installation, click the **Next** button.

4. In the **Select Server** dialog box, select the server components to be uninstalled, and then click the **Next** button.

5. In the **Remove the Program** dialog box, click the **Remove** button.
   The selected programs are uninstalled.

6. Remove any files or folders that still exist in the installation folder.

> **Important**
>
> Files and folders that were open during uninstallation are not removed. We recommend that you close the files and folders before starting uninstallation.

Related Topics

- *A. List of folders*

3.16 Procedure for uninstalling JP1/ITDM2 - SDM (Smart Device Android Agent) from the Android device (using the Android device settings menu)

Use the Android device Settings menu to uninstall JP1/ITDM2 - SDM (Smart Device Android Agent) from the Android device.

Procedure

1. In the **Settings** menu, tap **Apps** or **Application manager**.

2. Tap the icon of the JP1/ITDM2 - SDM (Smart Device Android Agent) application (application name: JP1ITDM2SDM).

3. Tap **Uninstall**.
   JP1/ITDM2 - SDM (Smart Device Android Agent) is uninstalled.

3.17 Procedure for uninstalling JP1/ITDM2 - SDM (Smart Device Android Agent) from the Android device (using the Google Play Store application)

Use the Google Play Store application to uninstall JP1/ITDM2 - SDM (Smart Device Android Agent) from the Android device.

Procedure

1. Launch the Google Play Store application.
2. In the Play Store menu, tap **My apps**.
3. Tap the JP1/ITDM2 - SDM (Smart Device Android Agent) application (application name: JP1ITDM2SDM) marked **Installed**, and then tap **Uninstall** on the application detail page.
   JP1/ITDM2 - SDM (Smart Device Android Agent) is uninstalled.

3.18 Procedure for uninstalling JP1/ITDM2 - SDM (Smart Device iOS Agent) from the iOS device

Uninstall JP1/ITDM2 - SDM (Smart Device iOS Agent) from the iOS device.

Procedure

1. Long-press the icon of the JP1/ITDM2 - SDM (Smart Device iOS Agent) application (application name: JP1ITDM2SDM).

2. Tap the × mark that appears at the upper left of the icon.

3. Tap **Remove** to remove the application.
   JP1/ITDM2 - SDM (Smart Device iOS Agent) is uninstalled.

3.19 Tasks required for upgrade installations

This section describes the additional tasks you need to perform as part of an upgrade installation.

3.19.1 Tasks to perform when upgrading the communication server

When performing an upgrade installation of JP1/ITDM2 - SDM (Communication Server) from a version earlier than 11-10, in addition to the usual installation tasks, you need to add definitions to the `httpsd.conf` file.

The httpsd.conf file is stored in the following location:

JP1/ITDM2 - SDM (Communication Server)-installation-folder`\cms\uC\httpsd\conf`

(1) To use standard distribution

In `<VirtualHost localhost:26055>`, add the following (underlined) setting:

```
<VirtualHost localhost:26055>
    SSLEnable
    SSLProtocol TLSv11 TLSv12
    SSLRequiredCiphers DES-CBC3-SHA:AES128-SHA:AES256-SHA
    SSLCertificateFile "C:/Program Files/Hitachi/.../newcert.pem"
    SSLCertificateKeyFile "C:/Program Files/Hitachi/.../newkeyRSA.pem"
    <Location /download/>
         Allow from all
    </Location>
</VirtualHost>
```

(2) To limit the maximum number of simultaneous downloads of distributed applications in standard distribution

Add the following (underlined) setting:

```
LoadModule hws_qos modules/mod_hws_qos.so
QOSCookieServers 0
:
<VirtualHost localhost:26055>
    SSLEnable
    SSLProtocol TLSv11 TLSv12
    SSLRequiredCiphers DES-CBC3-SHA:AES128-SHA:AES256-SHA
    SSLCertificateFile "C:/Program Files/Hitachi/.../newcert.pem"
    SSLCertificateKeyFile "C:/Program Files/Hitachi/.../newkeyRSA.pem"
    <Location /download/>
            Allow from all
            QOSRejectionServers 5
    </Location>
</VirtualHost>
```

(3) To require authentication for standard distribution

Add the following setting:

```
<Directory "JP1/ITDM2 - SDM (Communication Server)-installation-
folder/cms/uC/httpsd/htdocs/download">
    AuthType Basic
    AuthName "realm"
    AuthUserFile "JP1/ITDM2 - SDM (Communication Server)-installation-
folder/cms/conf/htpasswd"
```

```
    Require valid-user
</Directory>
```

Related Topics

- *16.2 Smart device manager environment setting file (manager.properties)*

4 Managing Smart Devices by Using JP1/ITDM2 - SDM

This chapter describes how to use JP1/ITDM2 - SDM: for example, to manage smart devices and to take action if a smart device is lost.

4.1 Remotely operating smart devices

In JP1/ITDM2 - SDM, you can perform operations remotely on smart devices from the Smart Device Manager GUI or by using commands. The operations you can perform remotely include distributing applications, applying security rules, and locking the device.

If you intend to perform remote operations such as distributing applications, applying security rules, and collecting inventory information (including regular collection) on a large number of smart devices, schedule the operations to take place at different times.

Note that the approach to remote operations differs according to the OS of the smart device.

Related Topics

- *4.1.1 Managing Android devices*
- *4.1.2 Managing iOS devices*

4.1.1 Managing Android devices

To perform a remote operation on an Android device from Smart Device Manager, the Android device must be turned on.

If the Android device is not turned on, the operation will fail immediately. In this case, wait a while and then try again.

Note that when distributing applications to Android devices, the operation might fail even if the device is turned on if the user of the device does not perform an operation required on the device side.

Related Topics

- *4.9 Flow of distributing applications to Android devices and instructing installation*

4.1.2 Managing iOS devices

You can perform remote operations on iOS devices from Smart Device Manager even if the iOS device is turned off at the time. However, the operation will fail if the iOS device is not turned on within 24 hours of the request being issued.

When performing remote operations on a large number of iOS devices simultaneously, check the results after 24 hours and repeat the remote operation only for those iOS devices for which the operation failed.

Note that when distributing applications or applying iOS profiles to iOS devices, the operation might fail even if the device is turned on. For example, the operation might fail if the user does not perform an operation required on the device side, or if the iOS device is in a state that does not allow the operation to succeed.

When distributing applications

A dialog appears on the iOS device asking the user for permission to install the application. If the user does not give permission, installation will not take place.

When applying iOS profiles

When applying a profile to an iOS device that is protected by a passcode lock, the iOS device must be unlocked while the profile is being applied.

Related Topics

- *4.10 Flow of sending instructions to iOS devices to install applications*
- *4.13.2 Flow of applying iOS profiles*

4.2 What you can do while JP1/ITDM2 - SDM is running

The following describes what you can do while JP1/ITDM2 - SDM is running:

You can:	Overview
Prepare smart devices	Prepare smart devices to be managed by JP1/ITDM2 - SDM. The preparation procedure differs depending on whether the device is a newly purchased smart device or stored smart devices.
Distribute new smart devices	If you receive a new application to use a smart device, you can distribute the smart device to the user.
Replace smart devices	Replace smart devices in the organization.
Change smart device users	If a user is transferred, another user can inherit the smart device.
Store smart devices	Store a smart device that is not being used because the user was transferred, or smart devices were replaced.
Dispose of smart devices	Dispose of smart devices that are no longer used because of a hardware problem or some other reason.
Distribute applications to Android devices and give instructions on installation	Distribute applications to multiple Android devices at the same time.
Send instructions to iOS devices to request users to install applications	Send instructions to iOS devices (in a batch) to request users to install the applications you want to distribute.
Install applications by a user operation on a smart device	Users can initiate the installation of applications that have been prepared in advance by an administrator.
Remove applications that are no longer needed	Uninstall and remove an application from an Android device when the application is no longer needed.
Manage security rules	Create security rules based on the organization's security principles to manage smart devices. If a user violates security rules, an event is issued so that the administrator can detect the unauthorized use of the smart device.
Take action if a smart device is lost	If a user loses a smart device, lock or initialize that smart device to prevent unauthorized use.
Take action if a user forgets the Android device password or iOS device passcode	If a user forgets an Android device password or iOS device passcode, change the Android device password or reset the iOS device passcode.
Send notifications of events by email	Use email to notify the administrator of events that occur in JP1/ITDM2 - SDM or smart device. The administrator can check JP1/ITDM2 - SDM errors and unauthorized use of the smart device without logging in to the JP1/ITDM2 - SDM program module.
Send messages to Android devices	If there is information that must be reported to Android device users, messages can be sent from JP1/ITDM2 - SDM to Android devices.

Related Topics

- *4.3 Preparing smart devices*
- *4.4 Flow of distributing new smart devices*
- *4.5 Flow of replacing a smart device*
- *4.6 Flow of changing a smart device user*
- *4.7 Flow of storing a smart device*
- *4.8 Flow of disposing of smart devices*
- *4.9 Flow of distributing applications to Android devices and instructing installation*
- *4.10 Flow of sending instructions to iOS devices to install applications*

- *4.11 Flow of user-initiated installation of applications on smart devices*
- *4.12 Flow of removing an application that is no longer needed*
- *4.13 Managing security rules*
- *4.14 Taking action if a smart device is lost*
- *4.15 Taking action if a user forgets the Android device password or iOS device passcode*
- *4.16 Flow of notifying events by email*
- *8.11 Sending messages to Android devices*

4.3 Preparing smart devices

You need to prepare smart devices to be managed and used by JP1/ITDM2 - SDM.

The preparation procedure differs depending on whether you are going to distribute a newly purchased smart device or a smart device already registered in JP1/ITDM2 - SDM.

Related Topics

- *4.3.1 Flow of preparing a newly purchased smart device*
- *4.3.2 Flow of preparing a smart device registered in JP1/ITDM2 - SDM*

4.3.1 Flow of preparing a newly purchased smart device

To use a newly purchased smart device, register it in JP1/ITDM2 - SDM, and then install JP1/ITDM2 - SDM (Smart Device Agent) on the smart device.

The following describes the flow of preparing a new smart device.

1. Check the root certificates for SSL communication preinstalled on the smart device.
2. Set the root certificates for SSL communication on the smart device (only when necessary certificates are not preinstalled).
3. Register the smart device in JP1/ITDM2 - SDM.
   Set the security policy and Android policy (or the security policy and iOS profile) appropriate for the user, and then register the smart device as *Managed*.
4. Install JP1/ITDM2 - SDM (Smart Device Agent) on the smart device.

Related Topics

- *3.14.3 Procedure for checking the root certificates for SSL communication preinstalled on the smart device*
- *3.14.4 Procedure for setting up the root certificate for SSL communication on the Android device*
- *3.14.5 Procedure for setting root certificates for SSL communication on the iOS device*
- *3.14.6 Procedure for installing JP1/ITDM2 - SDM (Smart Device Android Agent) on an Android device (using the Android device only)*
- *3.14.7 Procedure for installing JP1/ITDM2 - SDM (Smart Device Android Agent) on an Android device (for a PC)*
- *3.14.8 Procedure for installing JP1/ITDM2 - SDM (Smart Device iOS Agent) on an iOS device*
- *8.1 Registering smart devices in JP1/ITDM2 - SDM*

4.3.2 Flow of preparing a smart device registered in JP1/ITDM2 - SDM

To use a stored smart device, check the smart device information such as specifications. If the smart device can be used without problems, change the setting from **Unmanaged** to **Managed**, and then install JP1/ITDM2 - SDM (Smart Device Agent) on the smart device.

The following describes the flow of preparing an existing smart device.

1. Check the smart device.

Check the information such as specifications to make sure that the smart device can be used without problems. To view the information to be checked, in the Smart Device module, select **Smart Device**, and then **Unmanaged Smart Device List**.

2. Check the root certificates for SSL communication preinstalled on the smart device.
3. Set the root certificates for SSL communication on the smart device (only when necessary certificates are not preinstalled).
4. Set the smart device to *Managed*.
5. Install JP1/ITDM2 - SDM (Smart Device Agent) on the smart device.

Related Topics

- *3.14.3 Procedure for checking the root certificates for SSL communication preinstalled on the smart device*
- *3.14.4 Procedure for setting up the root certificate for SSL communication on the Android device*
- *3.14.5 Procedure for setting root certificates for SSL communication on the iOS device*
- *3.14.6 Procedure for installing JP1/ITDM2 - SDM (Smart Device Android Agent) on an Android device (using the Android device only)*
- *3.14.7 Procedure for installing JP1/ITDM2 - SDM (Smart Device Android Agent) on an Android device (for a PC)*
- *3.14.8 Procedure for installing JP1/ITDM2 - SDM (Smart Device iOS Agent) on an iOS device*
- *8.3 Setting unmanaged smart devices to Managed*
- *14.5.3 Unmanaged Smart Device List view*

4.4 Flow of distributing new smart devices

If a user submits a new application to use a smart device after the operation, prepare the smart device, and then distribute it to the user.

The following describes the flow of distributing a new smart device.

1. Prepare the smart device.

   > **Tip**
   >
   > You can create a list of smart devices to be distributed, and use it as a check list when distributing smart devices. Create the smart device list by exporting the smart device information to a CSV file.

2. Distribute the smart device to the user.
3. Confirm that the latest inventory information can be collected.

   After distributing the smart device, confirm that the smart device inventory information can be collected to JP1/ITDM2 - SDM. If it cannot be collected, make sure that JP1/ITDM2 - SDM (Smart Device Agent) is installed correctly.

Related Topics

- *4.3 Preparing smart devices*
- *8.2 Exporting a list of smart devices*
- *8.6 Obtaining the latest inventory information from a smart device*

4.5 Flow of replacing a smart device

To replace smart devices in your organization, use JP1/ITDM2 - SDM to find the smart devices to be replaced. Then, collect the smart devices and distribute new ones.

The following describes the flow of replacing smart devices.

1. Identify the smart devices to be replaced.

   In the Smart Device module, select **Smart Device**, and then **Managed Smart Device List**. In the list that appears, check the smart devices that must be replaced. At this time, you can use a filter to narrow down the displayed information.

2. Prepare the smart devices.

   > **Tip**
   >
   > You can create a list of smart devices to be replaced, and use it as a check list when replacing the devices. Create the list by exporting the smart device information to a CSV file.

3. Collect the smart devices.

   > **Tip**
   >
   > Store the collected smart devices if they are to be reused later. Dispose of any that are not to be used.

4. Move the SIM cards of the collected smart devices to the new smart devices to be distributed.

   This step is unnecessary if you are replacing smart devices along with their SIM cards or if SIM cards were not used.

5. Distribute the smart devices to users.

6. Confirm that inventory information can be collected.

   After distributing the smart devices, confirm that the smart device inventory information can be collected to JP1/ITDM2 - SDM. If it cannot be collected, make sure that JP1/ITDM2 - SDM (Smart Device Agent) is installed correctly.

Related Topics

- *4.3 Preparing smart devices*
- *4.7 Flow of storing a smart device*
- *4.8 Flow of disposing of smart devices*
- *8.2 Exporting a list of smart devices*
- *8.6 Obtaining the latest inventory information from a smart device*
- *14.5.1 Managed Smart Device List view*

4.6 Flow of changing a smart device user

For a smart device to be inherited by another user (for example, when the current user is transferred), initialize the smart device, and then re-register it in JP1/ITDM2 - SDM.

The following describes the flow of changing the smart device user.

1. Obtain the required information.
   Obtain the following information required for changing the user:
   - Name
   - User name and department or group before the change
   - User name and department or group after the change
2. Identify the smart device whose user has changed.
   In the Smart Device module, select **Smart Device**, and then **Managed Smart Device List**. In the list that appears, identify the smart device based on the information you obtained. At this time, you can use a filter to narrow down the displayed information.
3. Collect the smart device from the current user.
4. Initialize the collected smart device.
5. Change the smart device to *Unmanaged*.
6. Remove the smart device from JP1/ITDM2 - SDM.
7. Check the root certificates for SSL communication preinstalled on the smart device.
8. Set the root certificates for SSL communication on the smart device (only when necessary certificates are not preinstalled).
9. Register the smart device in JP1/ITDM2 - SDM.
   Set the security policy and Android policy (or the security policy and iOS profile) appropriate for the user, and then register the smart device as *Managed*.
10. Install JP1/ITDM2 - SDM (Smart Device Agent) on the smart device.
11. Distribute the smart device to a new user.
12. Confirm that inventory information can be collected.
    After distributing the smart device, confirm that the smart device inventory information can be collected to JP1/ITDM2 - SDM. If the information cannot be collected, make sure that JP1/ITDM2 - SDM (Smart Device Agent) is installed correctly.

Related Topics

- *3.14.3 Procedure for checking the root certificates for SSL communication preinstalled on the smart device*
- *3.14.4 Procedure for setting up the root certificate for SSL communication on the Android device*
- *3.14.5 Procedure for setting root certificates for SSL communication on the iOS device*
- *3.14.6 Procedure for installing JP1/ITDM2 - SDM (Smart Device Android Agent) on an Android device (using the Android device only)*
- *3.14.7 Procedure for installing JP1/ITDM2 - SDM (Smart Device Android Agent) on an Android device (for a PC)*
- *3.14.8 Procedure for installing JP1/ITDM2 - SDM (Smart Device iOS Agent) on an iOS device*
- *8.1 Registering smart devices in JP1/ITDM2 - SDM*
- *8.3 Setting unmanaged smart devices to Managed*

- *8.4 Setting managed smart devices to Unmanaged*
- *8.5 Removing smart devices from JP1/ITDM2 - SDM*
- *8.7 Resetting a smart device*
- *14.5.1 Managed Smart Device List view*

4.7 Flow of storing a smart device

Initialize and store a smart device that is not being used (when, for example, the current user is transferred, or the smart device is replaced).

The following describes the flow of storing a smart device.

1. Collect the smart device that is not being used.
2. Initialize the collected smart device.

> **Important**
>
> When the smart device is initialized, JP1/ITDM2 - SDM (Smart Device Agent) is removed and the security policy and Android policy (or security policy and iOS profile) settings are discarded.

Related Topics

- *8.7 Resetting a smart device*

4.8 Flow of disposing of smart devices

Dispose of smart devices that are no longer used because of a hardware failure or other reason.

The following describes the flow of disposing of smart devices.

1. Determine the smart devices to be disposed of.

   > **Tip**
   >
   > You can create a list of smart devices to be disposed of and use it as a check list when disposing of smart devices. Create the list by exporting the smart device information to a CSV file.

2. Initialize the smart devices to be disposed of.

   This step is unnecessary if the smart devices have already been initialized.

3. Set the smart devices to *Unmanaged*.

   To set the smart devices to *Unmanaged*, select the **Forcibly set as unmanaged** check box.

   If the smart devices are managed assets in JP1/IT Desktop Management 2, set the device status to *Disposed* in JP1/IT Desktop Management 2.

4. Dispose of the smart devices.

5. Remove the smart devices from JP1/ITDM2 - SDM.

   If the smart devices are managed assets in JP1/IT Desktop Management 2, remove them from JP1/IT Desktop Management 2.

Related Topics

- *8.2 Exporting a list of smart devices*
- *8.4 Setting managed smart devices to Unmanaged*
- *8.5 Removing smart devices from JP1/ITDM2 - SDM*
- *8.7 Resetting a smart device*

4.9 Flow of distributing applications to Android devices and instructing installation

Register applications you want to distribute in JP1/ITDM2 - SDM, and then simultaneously install them to multiple Android devices.

You can also distribute the applications in advance, and send instructions to install them at a later stage.

Because distributing applications can place a load on the network, you need to devise an appropriate distribution plan in advance.

The following describes the flow of distributing and installing applications.

1. Select applications in accordance with the organization's security principles.
2. Devise an application distribution plan.

   When you distribute an application and instructions to install it, the application is distributed without any intervention by the user of the Android device. If you distribute applications to a large number of Android devices simultaneously, the load on the network can increase to the point where it causes a bottleneck. We recommend that you devise a schedule that distributes applications to 50 devices at a time, at 5 minute intervals.

   To check the result of the distribution process, you need to collect inventory information.

   Example

   ```
   01:00 - 03:00  Send instructions to install application.
   22:00 - 24:00  Collect inventory information from distribution-target
   devices.
   ```

3. Register the applications to be distributed in JP1/ITDM2 - SDM.
4. Place the applications to be distributed on the communication server.

   Important

   To confirm that you have placed the applications correctly, try installing them on a test device before distributing the applications or sending instructions to install them.

   If you cannot install the applications, make sure that the correct package names were specified when registering the applications, and that the file names on the communication server are correct.

   Note

   This step is unnecessary if you are using simple distribution.

5. Notify the user to keep their Android device turned on.

   The distribution or installation instruction operation will fail if the Android device is turned off. For this reason, you need to let the user know in advance that their device needs to be turned on.

6. Distribute the applications to Android devices, or instruct users to install the applications.
7. Obtain the inventory information from Android devices.

   As a general rule, collect inventory information about 24 hours after distributing the applications or sending instructions to install them.

8. Check the result of distribution or installation.

Use the **Android Application** view or the `sdmexportdistributestatus` command to check the applications that have been distributed and those that are installed. If distribution or installation has failed on some Android devices, repeat the process for those devices.

Related Topics

- *8.6 Obtaining the latest inventory information from a smart device*
- *9.1 Registering applications to be distributed in JP1/ITDM2 - SDM*
- *9.2 Placing applications to be distributed on the communication server*
- *9.6 Distributing applications to Android devices*
- *9.7 Sending instructions to install applications on Android devices*
- *14.6.2 Android Application view*
- *15. sdmexportdistributestatus (outputting application distribution status)*

4.10 Flow of sending instructions to iOS devices to install applications

Simultaneously install iOS applications developed for internal use on multiple iOS devices.

Installing iOS applications requires intervention by the user of the iOS device. In addition, you need to devise an appropriate distribution plan in advance, because distributing applications can place a load on the network.

> **Important**
>
> Only iOS applications developed for internal use can be distributed by using JP1/ITDM2 - SDM. iOS applications from the App Store cannot be distributed by using JP1/ITDM2 - SDM.

The following describes the flow of installing applications.

1. Select applications in accordance with the organization's security principles.
2. Devise an application distribution plan.

   When you issue instructions to install applications, the applications are distributed after the user of the iOS device gives his or her permission. Because access from a large number of iOS devices can cause network congestion, devise a schedule that staggers the time at which each branch installs the applications.

   Example

   ```
   01:00 - 02:00  Instruct branch A to install the applications.
                  Branch A installs before noon.
   13:00 - 14:00  Instruct branch B to install the applications.
                  Branch B installs after noon.
   22:00 - 24:00  Collect inventory information from distribution-target
   devices.
   ```

   We recommend that installation instructions are issued to approximately 50 iOS devices at a time, about every 5 minutes.
3. Register the applications to be distributed in JP1/ITDM2 - SDM.
4. Place the applications to be distributed on the communication server.

   > **Important**
   >
   > To confirm that you have placed the applications correctly, try installing them on a test device before distributing the applications or sending instructions to install them.
   >
   > If you cannot install the applications, make sure that the correct package names were specified when registering the applications, and that the file names on the communication server are correct.

   > **Note**
   >
   > This step is unnecessary if you are using simple distribution.
5. Send an instruction to the iOS devices to request users to install the applications.
6. Obtain the inventory information from iOS devices.

   As a general rule, collect inventory information about 24 hours after distributing the applications or sending instructions to install them.
7. Check the result of installation.

Use the **iOS Application** view or the `sdmexportdistributestatus` command to check the applications that have been distributed and those that are installed.

If the installation process has not finished within 24 hours of the installation instruction being issued, installation is considered to have failed. Re-issue the installation instruction to the affected iOS devices.

Related Topics

- *8.6 Obtaining the latest inventory information from a smart device*
- *9.1 Registering applications to be distributed in JP1/ITDM2 - SDM*
- *9.2 Placing applications to be distributed on the communication server*
- *9.9 Sending instructions to install applications on iOS devices*
- *14.6.4 iOS Application view*
- *15. sdmexportdistributestatus (outputting application distribution status)*

4.11 Flow of user-initiated installation of applications on smart devices

If you define applications registered in JP1/ITDM2 - SDM as applications that can be installed by users, users can install those applications at any time they choose.

The following describes the flow of user-initiated installation of applications on a smart device:

1. To avoid placing too heavy a load on the network, consider limiting the maximum number of applications that can be downloaded simultaneously.
2. Select applications in accordance with the organization's security principles.
3. Register the applications to be distributed in JP1/ITDM2 - SDM.
4. Place the applications to be distributed on the communication server.

> **Note**
>
> This step is unnecessary if you are using simple distribution.

5. Define applications as installable by users.
6. Notify the users by email or other methods that those applications can be installed.
   Notify the user of the following information:
   - Application name
   - Version
7. The user installs the applications at a time of his or her choosing.

> **Tip**
>
> Use the **iOS Application** view or the `sdmexportdistributestatus` command to check the applications that have been distributed and those that are installed.

8. As needed, use email or other methods to notify users of smart devices without certain software installed that they need to install that software.

Related Topics

- *9.1 Registering applications to be distributed in JP1/ITDM2 - SDM*
- *9.2 Placing applications to be distributed on the communication server*
- *9.11 Managing applications that can be installed by users*
- *9.12 User-initiated installation of applications on Android devices*
- *9.13 User-initiated installation of applications on iOS devices*
- *9.14 Limiting the maximum concurrent downloads of distributed applications*
- *14.6.2 Android Application view*
- *14.6.4 iOS Application view*
- *15. sdmexportdistributestatus (outputting application distribution status)*

4.12 Flow of removing an application that is no longer needed

If a specific application is no longer needed, uninstall and remove it from the smart device, and then remove it from JP1/ITDM2 - SDM.

The following describes the flow of removing an unneeded application from JP1/ITDM2 - SDM.

1. Send instructions to the smart devices to request users to uninstall and remove the application.
2. Remove the distributed application from JP1/ITDM2 - SDM.
3. Remove the applications that are no longer needed.

> **Note**
>
> This step is unnecessary if you are using simple distribution.

Related Topics

- *9.4 Removing applications from JP1/ITDM2 - SDM*
- *9.5 Removing applications that are no longer needed*
- *9.8 Uninstalling distributed applications from Android devices*
- *9.10 Uninstalling distributed applications from iOS devices*

4.13 Managing security rules

Create a security rule based on the organization's security principles and manage smart devices. If a user violates the security rule, a JP1/ITDM2 - SDM event is issued. The administrator can detect unauthorized use of smart devices by checking issued events.

The following describes how to manage security rules.

Register security rules.

Register a security rule based on the organization's security principles. You can register multiple security rules. You can register different security rules for each department or group and for smart devices that require special management.

Apply security rules to smart devices.

Security rules allow the administrator to understand the security status of smart devices, and to restrict the use of smart devices to functions that are for business purposes only.

Edit security rules.

If the organization's security principles are changed, edit the security rules.

Delete security rules.

Delete security rules that are no longer needed because, for example, the management structure changed or security rules were combined.

Related Topics

- *2.4 Managing security*
- *4.13.1 Flow of applying Android policies*
- *4.13.2 Flow of applying iOS profiles*
- *7.1 Using security policies*
- *7.2 Using Android policies*
- *7.3 Using iOS profiles*

4.13.1 Flow of applying Android policies

You can assign an Android policy to an Android device.

The following describes the flow of applying Android policies.

1. Define the contents of Android policies in accordance with the organization's security principles.
2. Add Android policies.
3. Apply Android policies to Android devices.
   We recommend that you apply Android policies to no more than 50 Android devices in one operation.
4. Check the results of applying the Android policies.
   You can find out whether the Android policies were successfully applied by checking the date and time shown for **Date/Time of Android Policy/iOS Profile Application** on the **Security** tab of the Smart Device module. If the new policy has been applied, this date and time will be the date and time at which you performed the operation to apply the Android policies, or later. If you applied Android policies to a large number of Android devices, we recommend that you use the `sdmioutils exportdevice` command to check the results.

If the process of applying Android policies was unsuccessful for some Android devices, repeat the operation for those devices.

Related Topics

- *7.2.1 Adding Android policies*
- *7.2.4 Applying Android policies*
- *15. sdmioutils exportdevice (exporting smart device information)*

4.13.2 Flow of applying iOS profiles

You can apply iOS profiles to multiple iOS devices as a batch.

To apply a profile to an iOS device that is protected by a passcode lock, the iOS device must be unlocked while the profile is being applied.

Although Smart Device Manager will retry the operation periodically, it will take some time for the profiles to be applied to all devices. Ensure ample leeway when planning the application of iOS profiles.

The following describes the flow of applying iOS profiles.

1. Define the contents of iOS profiles in accordance with the organization's security principles.
2. Create iOS profiles using Apple Configurator.
3. Add iOS profiles.
4. Apply iOS profiles to iOS devices.
   We recommend that you apply Android policies to no more than 50 Android devices in one operation.
5. Check the results of applying the iOS profiles.
   You can find out whether the iOS profiles were successfully applied by checking the date and time shown for **Date/Time of Android Policy/iOS Profile Application** on the **Security** tab of the Smart Device module. If the new profile has been applied, this date and time will be the date and time at which you performed the operation to apply the iOS profiles, or later. If you applied iOS profiles to a large number of iOS devices, we recommend that you use the `sdmioutils exportdevice` command to check the results.
   The application process is considered to have failed if the iOS profile is not applied within 24 hours of the instruction being issued. Repeat the operation for those iOS devices for which the application process failed.

Related Topics

- *7.3.1 Adding iOS profiles*
- *7.3.4 Applying iOS profiles*
- *15. sdmioutils exportdevice (exporting smart device information)*

4.14 Taking action if a smart device is lost

You can lock or initialize any lost smart devices. Loss of a smart device used by your organization might result in confidential information on that smart device being leaked. You need to take action if a smart device is lost.

If a smart device is lost, you can do the following:

Lock the lost smart device.

Lock the smart device so that it cannot be used. Apply this method to prevent unauthorized use of the smart device.

Information in the lost smart device is not deleted by simply locking the smart device. It remains possible for a third party to unlock the device and leak information.

Initialize the lost smart device.

Initialize the smart device to the factory default settings. When a smart device is initialized, information in the smart device is also deleted. Apply this method in the following cases:

- The smart device has been lost for a certain period of time.
- Prevention of information leakage has the highest priority.

Related Topics

- *4.14.1 Flow of locking a lost smart device*
- *4.14.2 Flow of initializing a lost smart device*

4.14.1 Flow of locking a lost smart device

If a smart device is lost, you can lock it so that it cannot be used.

The following describes the flow of locking a smart device.

1. Receive a report from a user that the smart device was lost.
   When receiving the report, obtain information, such as the user's name or subscribed phone number, to identify the smart device.
2. Identify the lost smart device.
   In the Smart Device module, select **Smart Device**, and then **Managed Smart Device List**. In the list that appears, identify the smart device based on the information you obtained. At this time, you can use a filter to narrow down the displayed information.
3. Lock the smart device.

Related Topics

- *8.8 Locking a smart device*
- *14.5.1 Managed Smart Device List view*

4.14.2 Flow of initializing a lost smart device

If a smart device is lost, you can initialize it to the factory default settings.

The following describes the flow of initializing a smart device.

1. Receive a report from the user that the smart device was lost.

   When receiving the report, obtain information, such as the user's name or subscribed phone number, to identify the smart device.

2. Identify the lost smart device.

   In the Smart Device module, select **Smart Device**, and then **Managed Smart Device List**. In the list that appears, identify the smart device based on the information you obtained. At this time, you can use a filter to narrow down the displayed information.

3. Initialize the smart device.

Related Topics

- *8.7 Resetting a smart device*
- *14.5.1 Managed Smart Device List view*

4.15 Taking action if a user forgets the Android device password or iOS device passcode

If a user forgets an Android device password or iOS device passcode, the action to be taken differs depending on whether the smart device has been initialized by JP1/ITDM2 - SDM (Smart Device Agent).

If the smart device has not been initialized:

If the user forgets an Android device password or iOS device passcode, the administrator changes the Android device password or resets the iOS device passcode. Then, the administrator instructs the user to set a new Android device password or iOS device passcode.

If the smart device has been initialized:

If the user consecutively enters an incorrect passcode to a smart device, JP1/ITDM2 - SDM (Smart Device Agent) might initialize the smart device. To use the initialized smart device, JP1/ITDM2 - SDM (Smart Device Agent) must be installed again.

Related Topics

- *4.15.1 Flow of changing the Android device password*
- *4.15.2 Flow of resetting the iOS device passcode*
- *4.15.3 Flow of setting the smart device initialized by JP1/ITDM2 - SDM (Smart Device Agent) to Managed*

4.15.1 Flow of changing the Android device password

If a user forgets an Android device password, the administrator changes the Android device password, and then instructs the user to set the Android device password again.

The following describes the flow of changing an Android device password.

1. Receive a report from the user that they forgot the Android device password.

   When receiving the report, obtain information, such as the user's name or subscribed phone number, to identify the Android device.
2. Identify the Android device.

   In the Smart Device module, select **Smart Device**, and then **Managed Smart Device List**. In the list that appears, identify the Android device based on the information you obtained. At this time, you can use a filter to narrow down the displayed information.
3. Change the Android device password.
4. Send the new password to the user whose Android device password was changed, and instruct the user to set the password again.

Related Topics

- *8.9 Changing an Android device password*
- *14.5.1 Managed Smart Device List view*

4.15.2 Flow of resetting the iOS device passcode

If a user forgets an iOS device passcode, the administrator resets the iOS device passcode, and then instructs the user to set the iOS device passcode again.

The following describes the flow of resetting an iOS device passcode.

1. Receive a report from the user that they forgot the iOS device passcode.

   When receiving the report, obtain information, such as the user's name or subscribed phone number, to identify the iOS device.

2. Identify the iOS device.

   In the Smart Device module, select **Smart Device**, and then **Managed Smart Device List**. In the list that appears, identify the iOS device based on the information you obtained. At this time, you can use a filter to narrow down the displayed information.

3. Reset the iOS device passcode.

4. Instruct the user (whose iOS device passcode was reset) to set the passcode again.

Related Topics

- *8.10 Resetting an iOS device passcode*
- *14.5.1 Managed Smart Device List view*

4.15.3 Flow of setting the smart device initialized by JP1/ITDM2 - SDM (Smart Device Agent) to Managed

If a user consecutively enters an incorrect passcode to a smart device, JP1/ITDM2 - SDM (Smart Device Agent) might initialize the smart device. To manage the initialized smart device in JP1/ITDM2 - SDM, the smart device must be set to *Managed* in JP1/ITDM2 - SDM.

The following describes the flow of setting the initialized smart device to *Managed*.

1. Receive a report from the user that the smart device was initialized.

   When receiving the report, obtain information, such as the user's name or subscribed phone number, to identify the smart device.

2. Identify the smart device.

   In the Smart Device module, select **Smart Device**, and then **Managed Smart Device List**. In the list that appears, identify the smart device based on the information you obtained. At this time, you can use a filter to narrow down the displayed information.

3. Check information for the identified smart device.

   Check the user's name and contact address in the smart device information, and then verify the identity of the user.

4. Collect the smart device from the user.

5. Check the root certificates for SSL communication preinstalled on the smart device.

6. Set the root certificates for SSL communication on the smart device (only when necessary certificates are not preinstalled).

7. Install JP1/ITDM2 - SDM (Smart Device Agent) on the smart device.

8. Distribute the smart device to the new user.

9. Confirm that inventory information can be collected.

   After distributing the smart device, confirm that the smart device inventory information can be collected to JP1/ITDM2 - SDM. If it cannot be collected, make sure that JP1/ITDM2 - SDM (Smart Device Agent) is installed correctly.

Related Topics

- *3.14.3 Procedure for checking the root certificates for SSL communication preinstalled on the smart device*
- *3.14.4 Procedure for setting up the root certificate for SSL communication on the Android device*
- *3.14.5 Procedure for setting root certificates for SSL communication on the iOS device*
- *3.14.6 Procedure for installing JP1/ITDM2 - SDM (Smart Device Android Agent) on an Android device (using the Android device only)*
- *3.14.7 Procedure for installing JP1/ITDM2 - SDM (Smart Device Android Agent) on an Android device (for a PC)*
- *3.14.8 Procedure for installing JP1/ITDM2 - SDM (Smart Device iOS Agent) on an iOS device*
- *8.6 Obtaining the latest inventory information from a smart device*
- *14.5.1 Managed Smart Device List view*

4.16 Flow of notifying events by email

You can use email to notify the administrator of events that occurred in JP1/ITDM2 - SDM or a smart device.

The following describes the flow of sending notification of an event by email.

1. Specify settings for event notification.
2. Set up the mail server.
3. Define the event mail format in the event mail format information file.

Related Topics

- *11.1 Specifying settings for event notification*
- *11.2 Setting up mail servers*
- *16.4 Event mail format information file (eventmail.properties)*

5 Starting and Ending Operations

This chapter explains how to start and end operations in JP1/ITDM2 - SDM.

5.1 Logging in

In the Login module, you can log in to JP1/ITDM2 - SDM when your user account is successfully authenticated.

Procedure

1. Enter the following URL into the address bar of your Web browser:
   `http://`*smart-device-manager-IP-address-or-host-name*`:`*port-number-for-connection-from-administrator-computer*#`/jp1itdm2sdm/`

   #: The default port number is `26080`.

   The Login module appears.

2. Enter the user ID and password.

   The default user ID is system. The default password is manager.

3. Click the **Log In** button.

   If you use the default password of the built-in account to log in, the **Change Password** dialog box is displayed. Change the password. Note that the **Change Password** dialog box is also displayed when you use a newly created user account to log in for the first time.

Result

The Home module is displayed if the user account is successfully authenticated.

Tip

A password is valid for 180 days from the setup date. Beginning seven days prior to expiration, when the user logs in, he or she will be prompted to change the password. If you are prompted to do so, change the password. If 180 days have elapsed since the setup date, the **Change Password** dialog box is displayed when you log in.

Important

If a user fails to log in to JP1/ITDM2 - SDM three consecutive times, the user account is locked. The user cannot log in with the locked user account until the user account is unlocked.

Related topics

- *2.3.1 Locking user accounts*
- *5.2 Setting user account information*
- *5.3 Changing the default password*
- *6.7 Unlocking a user account*
- *14.2 Login window*
- *14.2.1 Change Password dialog box*
- *C. Port number list*

5.2 Setting user account information

When you use the built-in account or a newly created user account to log in to JP1/ITDM2 - SDM for the first time, you need to set user account information.

Procedure

1. Click the user ID link on the left of the **Log Out** button.

2. In the dialog box that appears, set information about the logged-in user account, and then click **OK**.

> **Tip**
>
> You can also set user account information by selecting **User Management** and then **Account Management** in the Settings module. In the **Account Management** view, you can also add a new user account.

> **Tip**
>
> After you specify an email address for a user account, notifications of event occurrences can be sent to that email address. We recommend that you specify an email address so that the appropriate person can be made aware of the operating status without having to frequently check the operation window. Note that to receive such notifications, you also need to specify the event notification settings, in addition to the email address.

Related topics

- *6.1 Adding a user account*
- *11.1 Specifying settings for event notification*
- *14.8.1 Account Management view*
- *14.8.3 Edit User Account dialog box*

5.3 Changing the default password

When you use the built-in account or a newly created user account to log in to JP1/ITDM2 - SDM for the first time, you are prompted to change the default password.

Procedure

1. Log in with the built-in account or a new user account.

2. In the dialog box that appears, change the password, and then click **OK**.

> **Important**
>
> Make sure to change the default password to enhance security. After the password is changed, you must use the new password from the next login.

> **Tip**
>
> The password is valid for 180 days from the setup date. Beginning seven days prior to expiration, you will be prompted to change the password when logging in. If you are prompted to do so, change the password. If 180 days have elapsed since the setup date, the **Change Password** dialog box is displayed when you log in.

Related topics

- *5.1 Logging in*
- *14.2.1 Change Password dialog box*

5.4 Logging out

After you have finished performing operations in JP1/ITDM2 - SDM, log out from the operation window.

Procedure

1. Click the Log Out button.
2. In the displayed dialog box, click OK.

> **Tip**
>
> You can also log out by selecting **Log Out** from the **System** menu at the top of the window.

Related topics

- *5.1 Logging in*

6 Managing User Accounts

This chapter describes how to manage user accounts.

6.1 Adding a user account

When multiple persons use JP1/ITDM2 - SDM to manage smart devices, you can add an administrator's user account.

Prerequisites

You must log in by using a user account with the system administrator permission.

Procedure

1. Display the Settings module.
2. In the menu area, select **User Management**, and then **Account Management**.
3. In the information area, click the **Add** button.
4. In the dialog box that appears, enter the user account information, and then click **OK**.

> **Tip**
>
> The functions a user can use vary depending on his or her permissions, so assign adequate permissions to users.

Result

A user account is added and displayed in the **Account Management** view.

Related topics

- *2.3.2 User account permissions*
- *2.3.3 List of operations that cannot be performed with the view permission*
- *14.8.1 Account Management view*
- *14.8.2 Add User Account dialog box*

6.2 Editing your own user account

If you want to change the password or permissions of your user account, you can edit the user account information.

Procedure

1. From the **Go** menu at the top of the window, select **Edit Your Account**.
   Alternatively, click the user ID link on the left of the **Log Out** button.

2. In the dialog box that appears, edit the user account information, and then click **OK**.

Related topics

- *2.3.2 User account permissions*
- *2.3.3 List of operations that cannot be performed with the view permission*
- *6.3 Editing another administrator's user account*
- *14.8.3 Edit User Account dialog box*

6.3 Editing another administrator's user account

You can edit another administrator's user account information such as the password and permissions.

Prerequisites

You must log in by using a user account with the system administrator permission.

Procedure

1. Display the Settings module.
2. In the menu area, select **User Management**, and then **Account Management**.
3. In the information area, click the **Edit** button for the account you want to edit.
4. In the dialog box that appears, enter the user account information, and then click **OK**.

Related topics

- *2.3.2 User account permissions*
- *2.3.3 List of operations that cannot be performed with the view permission*
- *6.2 Editing your own user account*
- *14.8.1 Account Management view*
- *14.8.3 Edit User Account dialog box*

6.4 Removing a user account

You can remove a user account that is no longer used. However, you cannot remove the built-in account or the account of a user who is logged in.

Prerequisites

You must log in by using a user account with the system administrator permission.

Procedure

1. Display the Settings module.
2. In the menu area, select **User Management**, and then **Account Management**.
3. In the information area, select the user account you want to remove, and then click the **Remove** button.
   You can select multiple user accounts.
4. In the dialog box that appears, click **OK**.

Related topics

- *14.8.1 Account Management view*

6.5 Changing your own password

In addition to cases when the **Change Password** dialog box is displayed, you can change the password of your user account if necessary.

Procedure

1. From the **Go** menu at the top of the window, select **Edit Your Account**.
   Alternatively, click the user ID link on the left of the **Log Out** button.

2. In the dialog box that appears, select the **Changes the password** check box.

3. Enter the password in **Password** and **Re-enter Password**, and then click **OK**.

> **Tip**
>
> The password is valid for 180 days from the setup date. Beginning seven days prior to expiration, you will be prompted to change the password when logging in. If you are prompted to do so, change the password. If 180 days have elapsed since the setup date, the **Change Password** dialog box is displayed when you log in.

Related topics

- *6.6 Resetting another administrator's password*
- *14.8.1 Account Management view*
- *14.8.3 Edit User Account dialog box*

6.6 Resetting another administrator's password

If an administrator forgets his or her password, another administrator can reset the password to the default.

Prerequisites

You must log in by using a user account with the system administrator permission.

Procedure

1. Display the Settings module.
2. In the menu area, select **User Management**, and then **Account Management**.
3. In the information area, click the **Edit** button for the user account whose password you want to reset.
4. In the dialog box that appears, select the **Changes the password** check box.
5. Enter the password in **Password** and **Re-enter Password**, and then click **OK**.
   The password is set for the selected user account.
6. Inform the administrator whose password has been reset, of the new password.
   Also inform the administrator that the password needs to be changed after the administrator logs in JP1/ITDM2 - SDM using the reset password.

Related topics

- *6.5 Changing your own password*
- *14.8.1 Account Management view*
- *14.8.3 Edit User Account dialog box*

6.7 Unlocking a user account

A user account is locked if the user fails to log in three consecutive times. You must unlock the account before it can be used.

Prerequisites

You must log in by using a user account with the system administrator permission.

Procedure

1. Display the Settings module.
2. In the menu area, select **User Management**, and then **Account Management**.
3. Click the **Edit** button of the locked user account.
4. In the dialog box that appears, select **Enabled** from **Status**, and then click **OK**.

> **Tip**
>
> If no other administrator has the system administrator permission, restart the JP1/ITDM2 - SDM. The user account is unlocked.

Related topics

- *2.3.1 Locking user accounts*
- *14.8.1 Account Management view*
- *14.8.3 Edit User Account dialog box*

7 Managing the Security Status

This chapter explains how to manage the security of the smart devices in your organization and how to understand the security status.

7.1 Using security policies

Security policies are required to manage the security status of smart devices. For a security policy, you can specify settings to monitor usage of the following: phone numbers, Web sites, and applications. This section describes how to use security policies.

7.1.1 Adding security policies

In the **Security Policy List** view of the Security module, you can add a security policy. By applying the added security policy to smart devices, you can monitor usage of those smart devices.

Prerequisites

You must log in by using a user account with the system administrator permission.

Procedure

1. Display the Security module.
2. In the menu area, select **Security** and then **Security Policy List**.
3. In the information area, click the **Add** button.
4. At the top of the **Add Security Policy** dialog box, enter data in the **Security Policy Name** text box.
5. Under **Security Configuration Items** on the left pane of the **Add Security Policy** dialog box, select **Phone Number**, **Web Site**, or **Application**.
6. Click the **Add** button.
7. In the displayed dialog box, configure the rules settings and then click **OK**.

> **Tip**
>
> You can specify an asterisk (`*`) for **Phone Number** and **URL**. For example, if you enter `1111111*` for **Phone Number**, phone numbers whose first seven digits are `1111111` are monitored. You can also specify an abbreviated dialing number beginning with a sharp sign (#) for **Phone Number**.

8. Repeat steps 5 to 7 for each item you want to set.
9. In the **Add Security Policy** dialog box, click **OK**.

Result

The security policy is added and displayed in the **Security Policy List** view.

Related topics

- *2.4.3 Items that can be set for a security policy*
- *7.1.2 Editing security policies*
- *7.1.3 Removing security policies*
- *7.1.4 Applying security policies*

- *14.4.1 Security Policy List view*
- *14.4.2 Add Security Policy dialog box*

7.1.2 Editing security policies

You can edit security policies if a change occurs with the security policies of your organization or if you want to keep your security policies up to date.

Prerequisites

You must log in by using a user account with the system administrator permission.

Procedure

1. Display the Security module.
2. In the menu area, select **Security** and then **Security Policy List**.
3. In the information area, click the **Edit** button for the security policy that you want to edit.
4. Under **Security Configuration Items** on the left pane of the **Edit Security Policy** dialog box, select **Phone Number**, **Web Site**, or **Application**.
5. In the dialog box that appears, edit the rule.
   - To add a new rule:
     Click the **Add** button. In the dialog box that appears, add a rule, and then click **OK**.
   - To edit an existing rule:
     Click the **Edit** button for the rule you want to edit. In the dialog box that appears, edit the rule, and then click **OK**.
   - To remove an existing rule:
     Select the rule you want to remove, and then click the **Remove** button. In the dialog box that appears, click **OK**. You can select multiple rules.

   > **Tip**
   >
   > You can specify an asterisk (`*`) for **Phone Number** and **URL**. For example, if you enter `1111111*` for **Phone Number**, phone numbers whose first seven digits are `1111111` are monitored. You can also specify an abbreviated dialing number beginning with a sharp sign (`#`) for **Phone Number**.

   > **Tip**
   >
   > You can also add a rule to security policies from **Action** on the **Call History**, **Web Browsing History**, or **Software** tab.
6. Repeat steps 4 and 5 for each item you want to edit.
7. In the **Edit Security Policy** dialog box, click **OK**.

Related topics

- *2.4.3 Items that can be set for a security policy*

- *7.1.1 Adding security policies*
- *7.1.3 Removing security policies*
- *7.1.4 Applying security policies*
- *14.4.1 Security Policy List view*
- *14.4.3 Edit Security Policy dialog box*

7.1.3 Removing security policies

You can remove unneeded security policies if the security policies of your organization are changed or if the number of managed smart devices is reduced.

Prerequisites

- You must log in by using a user account with the system administrator permission.
- You must apply another security policy to smart devices before removing a policy already applied to those devices.

1. Display the Security module.

2. In the menu area, select **Security** and then **Security Policy List**.

3. In the information area, select the security policy you want to remove, and then click the **Remove** button.
   You can select multiple security policies.

4. In the displayed dialog box, click **OK**.

Related topics

- *7.1.1 Adding security policies*
- *7.1.2 Editing security policies*
- *14.4.1 Security Policy List view*

7.1.4 Applying security policies

If you want to monitor usage of smart devices, apply a security policy. The applied policy allows you to understand the status of smart devices, such as unauthorized use.

Prerequisites

You must log in by using a user account with the system administrator permission.

Procedure

1. Display the Smart Device module.

2. In the menu area, select **Smart Device**.

3. In the information area, select the smart device to which you want to apply a security policy.
   You can select multiple smart devices.

Tip

You can use a filter to narrow down the displayed information.

4. From **Action**, select **Apply Security Policy**.

5. In the displayed dialog box, select a security policy and then click **OK**.

Related topics

- *7.1.1 Adding security policies*
- *7.1.2 Editing security policies*
- *14.5.1 Managed Smart Device List view*
- *14.5.3 Unmanaged Smart Device List view*
- *14.5.9 Apply Security Policy dialog box*

7.2 Using Android policies

Android policies are required to manage the security status of Android devices. An Android policy can specify password rules and restrict use of a device's camera function. This section describes how to use Android policies.

7.2.1 Adding Android policies

In the **Android Policy List** view of the Security module, you can add an Android policy. By applying the added Android policy to Android devices, you can monitor usage of the target Android devices.

Prerequisites

You must log in by using a user account with the system administrator permission.

Procedure

1. Display the Security module.

2. In the menu area, select **Security** and then **Android Policy List**.

3. In the information area, click the **Add** button.

4. In the dialog box that appears, specify the rules, and then click **OK**.

Result

The Android policy is added and displayed in the **Android Policy List** view.

Related topics

- *2.4.5 Items that can be set for an Android policy*
- *7.2.2 Editing Android policies*
- *7.2.3 Removing Android policies*
- *7.2.4 Applying Android policies*
- *14.4.11 Android Policy List view*
- *14.4.12 Add Android Policy dialog box*

7.2.2 Editing Android policies

You can edit Android policies if the security policies of your organization are changed or if you want to keep your security policies up to date.

Prerequisites

You must log in by using a user account with the system administrator permission.

Procedure

1. Display the Security module.

2. In the menu area, select **Security** and then **Android Policy List**.

3. In the information area, click the **Edit** button for the Android policy that you want to edit.

4. In the dialog box that appears, edit the rules, and then click **OK**.

Related topics

- *2.4.5 Items that can be set for an Android policy*
- *7.2.1 Adding Android policies*
- *7.2.3 Removing Android policies*
- *7.2.4 Applying Android policies*
- *14.4.11 Android Policy List view*
- *14.4.13 Edit Android Policy dialog box*

7.2.3 Removing Android policies

You can remove Android policies that are no longer required (for example, if the security policies of your organization are changed or the number of managed Android devices is reduced).

Prerequisites

- You must log in by using a user account with the system administrator permission.
- You must apply another Android policy beforehand to the Android devices to which the Android policy to be removed is applied.

Procedure

1. Display the Security module.

2. In the menu area, select **Security** and then **Android Policy List**.

3. In the information area, select the Android policy you want to remove, and then click the **Remove** button.
   You can select multiple Android policies.

4. In the displayed dialog box, click **OK**.

Related topics

- *7.2.1 Adding Android policies*
- *7.2.2 Editing Android policies*
- *14.4.11 Android Policy List view*

7.2.4 Applying Android policies

If you want to monitor usage of Android devices, apply an Android policy. The applied policy allows you to understand the status of Android devices, such as unauthorized use.

Prerequisites

You must log in by using a user account with the system administrator permission.

Procedure

1. Display the Smart Device module.
2. In the menu area, select **Smart Device**.
3. In the information area, select the Android device to which you want to apply an Android policy.
   You can select multiple Android devices.

   > **Tip**
   >
   > You can use a filter to narrow down the displayed information.

4. From **Action**, select **Apply Android Policy**.
5. In the displayed dialog box, select an Android policy and then click **OK**.

Result

On the **Security** tab, **Date/Time of Android Policy/iOS Profile Application** is updated after the policy is applied to the Android device.

Related topics

- *7.2.1 Adding Android policies*
- *7.2.2 Editing Android policies*
- *14.4.11 Android Policy List view*
- *14.5.1 Managed Smart Device List view*
- *14.5.2 Tabs displayed in the Managed Smart Device List view*
- *14.5.3 Unmanaged Smart Device List view*
- *14.5.10 Apply Android Policy dialog box*

7.3 Using iOS profiles

iOS profiles are required to manage the security status of iOS devices. An iOS policy can specify passcode rules and restrict use of the camera function. This section describes how to use iOS profiles.

7.3.1 Adding iOS profiles

In the **iOS Profile List** view of the Security module, you can add an iOS profile. By applying the added iOS profile to iOS devices, you can monitor usage of the target iOS devices.

Prerequisites

- You must log in by using a user account with the system administrator permission.
- You must create a profile by using the iPhone Configuration Utility (provided by Apple) in advance.

Procedure

1. Display the Security module.

2. In the menu area, select **Security** and then **iOS Profile List**.

3. In the information area, click the **Add** button.

4. In the dialog box that appears, specify the profile name and the path to the import file.

5. Click **OK**.

Result

The iOS profile is added and displayed in the **iOS Profile List** view.

Related topics

- *2.4.7 Items that can be set in an iOS profile*
- *7.3.2 Exporting iOS profiles*
- *7.3.3 Removing iOS profiles*
- *7.3.4 Applying iOS profiles*
- *14.4.15 iOS Profile List view*
- *14.4.16 Add iOS Profile dialog box*

7.3.2 Exporting iOS profiles

You can export an iOS profile in XML format.

Procedure

1. Display the Security module.

2. In the menu area, select **Security** and then **iOS Profile List**.

3. In the information area, click the **Export** button for the iOS profile you want to export.

4. In the window that appears, specify the file name and the location to save the file, and then click the **Save** button.

Result

The iOS profile with the specified file name is saved in XML format in the specified location.

> **Tip**
>
> You can import the exported file to the Apple iPhone Configuration Utility by changing the extension to `.mobileconfig`. If necessary, you can edit the configuration profile, and then register it again as an iOS profile.

Related topics

- *7.3.1 Adding iOS profiles*
- *7.3.3 Removing iOS profiles*
- *7.3.4 Applying iOS profiles*
- *14.4.15 iOS Profile List view*

7.3.3 Removing iOS profiles

You can remove iOS profiles that are no longer required (for example, if the security policies of your organization are changed or if the number of managed iOS devices is reduced).

Prerequisites

- You must log in by using a user account with the system administrator permission.
- You must apply another security policy to iOS devices before removing a policy already applied to those devices.

Procedure

1. Display the Security module.

2. In the menu area, select **Security** and then **iOS Profile List**.

3. In the information area, select the iOS profile you want to remove, and then click the **Remove** button.
   You can select multiple iOS profiles.

4. In the displayed dialog box, click **OK**.

Related topics

- *7.3.1 Adding iOS profiles*
- *7.3.2 Exporting iOS profiles*
- *14.4.15 iOS Profile List view*

7.3.4 Applying iOS profiles

If you want to monitor the usage of iOS devices, apply an iOS profile. The applied profile allows you to understand the status of iOS devices, such as unauthorized use.

> **Note**
>
> You can also use the `sdmapplyprofile` command to apply iOS profiles.

Prerequisites

- You must log in by using a user account with the system administrator permission.
- To apply an iOS profile, you must unlock the iOS device.

Procedure

1. Display the Smart Device module.
2. In the menu area, select **Smart Device**.
3. In the information area, select the iOS device to which you want to apply an iOS profile.
   You can select multiple iOS devices.

   > **Tip**
   >
   > You can use a filter to narrow down the displayed information.

4. From **Action**, select **Apply iOS Profile**.
5. In the dialog box that appears, specify the iOS profile, and then click **OK**.

Result

On the **Security** tab, **Date/Time of Android Policy/iOS Profile Application** is updated after the profile is applied to the iOS device.

> **Tip**
>
> You can apply multiple iOS profiles to one iOS device.

> **Important**
>
> To apply an iOS profile, you must unlock the iOS device.

Related topics

- *7.3.1 Adding iOS profiles*
- *7.3.2 Exporting iOS profiles*
- *7.3.3 Removing iOS profiles*
- *14.4.15 iOS Profile List view*
- *14.5.1 Managed Smart Device List view*

- *14.5.2 Tabs displayed in the Managed Smart Device List view*
- *14.5.3 Unmanaged Smart Device List view*
- *14.5.11 Apply iOS Profile dialog box*

7.3.5 Removing applied iOS profiles

If you want to change an applied iOS profile, remove the applied iOS profile.

> **Note**
>
> You can also use the `sdmapplyprofile` command to remove the applied iOS profiles.

Prerequisites

You must log in by using a user account with the system administrator permission.

Procedure

1. Display the Smart Device module.
2. In the menu area, select **Smart Device**.
3. In the information area, select the iOS device to which you want to remove applied an iOS profile.
   You can select multiple iOS devices.

   > **Tip**
   >
   > You can use a filter to narrow down the displayed information.

4. From **Action**, select **Remove Applied iOS Profile**.
5. In the dialog box that appears, specify the iOS profile, and then click **OK**.

Related topics

- *7.3.3 Removing iOS profiles*
- *7.3.4 Applying iOS profiles*
- *14.4.15 iOS Profile List view*
- *14.5.1 Managed Smart Device List view*
- *14.5.2 Tabs displayed in the Managed Smart Device List view*
- *14.5.3 Unmanaged Smart Device List view*

7.3.6 Editing iOS profile information

You can edit the name and description of an iOS profile as needed.

Prerequisites

You must log in by using a user account with the system administrator permission.

Procedure

1. Display the Security module.
2. In the menu area, select **Security** and then **iOS Profile List**.
3. In the information area, click the **Edit** button for the iOS profile that you want to edit.
4. In the dialog box that appears, edit the iOS profile information.
5. Click **OK**.

Result

The updated iOS profile information is displayed in the **iOS Profile List** view.

Related topics

- *2.4.7 Items that can be set in an iOS profile*
- *7.3.1 Adding iOS profiles*
- *7.3.2 Exporting iOS profiles*
- *7.3.3 Removing iOS profiles*
- *7.3.4 Applying iOS profiles*
- *14.4.15 iOS Profile List view*
- *14.4.17 Edit iOS Profile Information dialog box*

8 Managing Smart Devices

This chapter describes how to understand the current smart device status by collecting information from internal smart devices.

8.1 Registering smart devices in JP1/ITDM2 - SDM

Register smart devices you want to manage in JP1/ITDM2 - SDM.

You can register smart devices in the following two ways:

- Manually register smart devices
  Register information about a smart device one by one.
- Register smart devices in a CSV file
  Import a CSV file containing information about multiple smart devices to register them as a batch.

Related topics

- *2.5 Managing smart devices*
- *8.1.1 Manually registering smart devices*
- *8.1.2 Registering smart devices in a CSV file*

8.1.1 Manually registering smart devices

You can manually register information about smart devices, one by one, in JP1/ITDM2 - SDM.

Prerequisites

- You must log in by using a user account with the system administrator permission.
- To register a smart device as a managed device, in advance you must create a security policy and Android policy, or a security policy and iOS profile.
- You must obtain the following information:
  - User name
  - Department to which the user belongs

Procedure

1. Display the Smart Device module.
2. In the menu area, select **Smart Device**, and then **Managed Smart Device List**.
3. From **Action**, select **Add Smart Device**.
4. In the **Add Smart Device** dialog box, enter information about the smart device to be registered.
   Click the **Add** button at the top of the dialog box to add a line in which you can enter smart device information. You can register information about multiple smart devices.

> **Important**
>
> For **Name**, use the following characters only:
>
> - 0 to 9 (ASCII code 0x30 to 0x39)
> - A to Z (ASCII code 0x41 to 0x5a)
> - a to z (ASCII code 0x61 to 0x7a)

- _ (underscore) (ASCII code 0x5f)
- - (hyphen) (ASCII code 0x2d)
- . (period) (ASCII code 0x2e)

Important

If a name that is already registered in JP1/ITDM2 - SDM is entered for **Name**, information about the registered smart device is overwritten.

Tip

In the **Add Smart Device** dialog box, click the **Export** button to output the entered information to a CSV file.

5. Click **OK**.

Result

The smart device is registered in JP1/ITDM2 - SDM. Note that the management status of the smart device varies depending on whether security rules were applied.

- If the smart device is registered with entry of a security policy and Android policy, or with entry of a security policy and iOS profile:
  The smart device is managed, and is displayed in the **Managed Smart Device List** view.
- If the smart device is registered without entry of a security policy and Android policy, or without entry of a security policy and iOS profile:
  The smart device is unmanaged, and is displayed in the **Unmanaged Smart Device List** view.

Related topics

- *8.1.2 Registering smart devices in a CSV file*
- *8.2 Exporting a list of smart devices*
- *8.3 Setting unmanaged smart devices to Managed*
- *14.5.1 Managed Smart Device List view*
- *14.5.3 Unmanaged Smart Device List view*
- *14.5.13 Add Smart Device dialog box*

8.1.2 Registering smart devices in a CSV file

You can import a CSV file containing information about multiple smart devices to register them in a batch.

Prerequisites

- You must log in by using a user account with the system administrator permission.
- You must create a CSV file.
- To register a smart device as a managed device, in advance you must create a security policy and Android policy, or a security policy and iOS profile.

Procedure

1. Display the Smart Device module.
2. In the menu area, select **Smart Device**, and then **Managed Smart Device List**.
3. From **Action**, select **Import Smart Device List**.
4. In the dialog box that appears, select the CSV file containing information about the smart devices, and then click **OK**.

> **Important**
>
> For **Name** to be specified for the CSV file, use the following characters only:
>
> - 0 to 9 (ASCII code 0x30 to 0x39)
> - A to Z (ASCII code 0x41 to 0x5a)
> - a to z (ASCII code 0x61 to 0x7a)
> - _ (underscore) (ASCII code 0x5f)
> - - (hyphen) (ASCII code 0x2d)
> - . (period) (ASCII code 0x2e)

> **Important**
>
> If a name that is already registered in JP1/ITDM2 - SDM is entered for **Name** to be specified for the CSV file, information about the registered smart device is overwritten.

Result

The smart devices are registered in JP1/ITDM2 - SDM. Note that the management status of the smart devices varies depending on whether security rules were applied.

- If the smart devices are registered with an entered security policy and Android policy, or an entered security policy and iOS profile:
  The smart devices are managed, and are displayed in the **Managed Smart Device List** view.
- If the smart devices are registered without a security policy and Android policy, or without a security policy and iOS profile:
  The smart devices are unmanaged, and are displayed in the **Unmanaged Smart Device List** view.

Related topics

- *8.1.1 Manually registering smart devices*
- *8.2 Exporting a list of smart devices*
- *8.3 Setting unmanaged smart devices to Managed*
- *14.5.1 Managed Smart Device List view*
- *14.5.3 Unmanaged Smart Device List view*
- *14.5.13 Add Smart Device dialog box*
- *E. Output Format of Imported and Exported Files*

8.2 Exporting a list of smart devices

You can export information about all smart devices to a CSV file. You can use the CSV file as a check list when, for example, disposing of smart devices.

Procedure

1. Display the Smart Device module.
2. In the menu area, select **Smart Device**, and then **Managed Smart Device List**.
3. From **Action**, select **Export Smart Device List**.
4. In the window that appears, specify the file name and the location to save the file, and then click the **Save** button.

Result

The CSV file is saved with the specified file name in the specified location.

> **Tip**
>
> You can edit and import the exported CSV file.

Related topics

- *8.1.2 Registering smart devices in a CSV file*
- *14.5.1 Managed Smart Device List view*
- *E. Output Format of Imported and Exported Files*

8.3 Setting unmanaged smart devices to Managed

Apply security rules to smart devices registered as unmanaged devices to set them to *Managed*. For the managed smart devices, you can collect device information and check the security status.

If the smart device you are setting to *Managed* has previously been a managed device, first register the unmanaged smart device as a managed device in the smart device manager. Then, on the smart device, enter the settings that allow it to connect to the communication server.

Related topics

- *8.3.1 Setting unmanaged smart devices to Managed in smart device manager*
- *8.3.2 Setting previously managed Android devices to Managed*
- *8.3.3 Setting previously managed iOS devices to Managed*

8.3.1 Setting unmanaged smart devices to Managed in smart device manager

Apply security rules to smart devices registered as unmanaged devices to set them to *Managed*.

Prerequisites

- You must log in by using a user account with the system administrator permission.
- You must add, in advance, a security policy and Android policy, or a security policy and iOS profile.

Procedure

1. Display the Smart Device module.
2. In the menu area, select **Smart Device**, and then **Unmanaged Smart Device List**.
3. Select the smart device to be managed.
   You can select multiple smart devices.
4. From **Action**, select **Apply Security Policy**.
5. In the dialog box that appears, select the security policy to be applied, and then click the **OK** button.
6. From **Action**, select **Apply Android Policy** or **Apply iOS Profile**.
   Depending on the OS type specified when the smart device was registered, you can select **Apply Android Policy** or **Apply iOS Profile**.
7. In the dialog box that appears, select the Android policy or iOS profile to be applied, and then click the **OK** button.

Result

The selected smart devices are now managed, and are displayed in the **Managed Smart Device List** view.

Related topics

- *2.5.1 Managing managed smart devices*
- *8.3.2 Setting previously managed Android devices to Managed*

- *8.3.3 Setting previously managed iOS devices to Managed*
- *8.4 Setting managed smart devices to Unmanaged*
- *14.5.1 Managed Smart Device List view*
- *14.5.3 Unmanaged Smart Device List view*
- *14.5.9 Apply Security Policy dialog box*
- *14.5.10 Apply Android Policy dialog box*
- *14.5.11 Apply iOS Profile dialog box*

8.3.2 Setting previously managed Android devices to Managed

To set to *Managed* an Android device that has been a managed device in the past, you first need to register the unmanaged smart device as a managed device in the smart device manager. Then, on the Android device, you enter the settings that allow it to connect to the communication server.

Procedure

1. On the Android device, start JP1/ITDM2 - SDM (Smart Device Android Agent).

2. Tap **Communication Server**.

3. In the Settings window, enter the host name of the connection destination communication server and smart device name, and then tap **OK**.

   For the communication server, enter the host name in *host-name*:*port-number* (default: `26055`) format. For the name, specify the smart device name registered in JP1/ITDM2 - SDM.

   When the server is connected successfully, a dialog box indicating so appears.

4. Tap **OK** in the dialog box.

Related topics

- *8.4 Setting managed smart devices to Unmanaged*

8.3.3 Setting previously managed iOS devices to Managed

To set to Managed an iOS device that has been a managed device in the past, you first need to register the unmanaged smart device as a managed device in the smart device manager. Then, on the iOS device, you enter the settings that allow it to connect to the communication server.

Procedure

1. On the iOS device, tap **Settings**, **General**, and then **Profile**, and then delete the configuration profiles.

   This step is unnecessary if the configuration profiles have already been deleted.

2. On the iOS device, start JP1/ITDM2 - SDM (Smart Device iOS Agent).

3. Tap **Communication Server**.

4. In the Communication Server Settings window, tap **Delete Communication Server**.

5. In the Delete Communication Server Settings Confirmation window, tap **OK**.

6. Tap **OK** in the confirmation dialog box.

7. In the Communication Server Settings window, enter the host name of the connection destination communication server and the smart device name, and then tap **OK**.

   For the communication server, enter the host name in *host-name*:*port-number* (default: `26055`) format. For the name, specify the smart device name registered in JP1/ITDM2 - SDM.

   When the server is connected successfully, a dialog box indicating so appears.

8. Tap **OK** in the dialog box.

Related topics

- *8.4 Setting managed smart devices to Unmanaged*

8.4 Setting managed smart devices to Unmanaged

For smart devices you no longer need to manage, you can cancel security rules and set those smart devices to *Unmanaged*.

Prerequisites

You must log in by using a user account with the system administrator permission.

Procedure

1. Display the Smart Device module.
2. In the menu area, select **Smart Device**, and then **Managed Smart Device List**.
3. Select the smart device to be unmanaged.
   You can select multiple smart devices.
4. From **Action**, select **Set to Unmanaged**.
5. In the displayed dialog box, click **OK**.

> **Tip**
>
> If you select the **Forcibly set as unmanaged** check box, sets the selected smart device as unmanaged, even if the device cannot be connected with.

Result

The selected smart devices are now unmanaged, and are displayed in the **Unmanaged Smart Device List** view.

Related topics

- *2.5.2 Managing unmanaged smart devices*
- *8.3 Setting unmanaged smart devices to Managed*
- *14.5.1 Managed Smart Device List view*
- *14.5.3 Unmanaged Smart Device List view*
- *14.5.8 Set to Unmanaged dialog box*

8.5 Removing smart devices from JP1/ITDM2 - SDM

You can remove unmanaged smart devices from JP1/ITDM2 - SDM if they are no longer needed (for example, due to a hardware failure or replacement).

Prerequisites

- You must log in by using a user account with the system administrator permission.
- The smart device must be set to *Unmanaged*.
- If necessary, the smart device must be initialized before being removed from JP1/ITDM2 - SDM. A smart device is not initialized by simply removing it from JP1/ITDM2 - SDM.

Procedure

1. Display the Smart Device module.
2. In the menu area, select **Smart Device**, and then **Unmanaged Smart Device List**.
3. Select the smart device to be removed.
   You can select multiple smart devices.
4. Click the **Remove** button.
5. In the displayed dialog box, click **OK**.

Related topics

- *8.7 Resetting a smart device*
- *14.5.3 Unmanaged Smart Device List view*

8.6 Obtaining the latest inventory information from a smart device

You can obtain the latest inventory information from a smart device.

> **Note**
>
> You can also use the `sdmgetinventory` command to collect inventory information.

Prerequisites

You must log in by using a user account with the system administrator permission.

Procedure

1. Display the Smart Device module.
2. In the menu area, select **Smart Device**, and then **Managed Smart Device List**.
3. In the information area, select the smart device from which you want to obtain information.
4. From **Action**, select **Update Device Details**.
5. In the displayed dialog box, click **OK**.

Result

In the **Managed Smart Device List** view, information displayed on the tabs for the selected smart device is updated.

Related topics

- *2.5.1 Managing managed smart devices*
- *14.5.1 Managed Smart Device List view*
- *14.5.2 Tabs displayed in the Managed Smart Device List view*

8.7 Resetting a smart device

When disposing of smart devices, you can initialize them to the factory default settings.

Prerequisites

You must log in by using a user account with the system administrator permission.

Procedure

1. Display the Smart Device module.
2. In the menu area, select **Smart Device**, and then **Managed Smart Device List**.
3. In the information area, select the smart device to be initialized.
   You can select multiple smart devices.
4. From **Action**, select **Initialize Smart Device**.
5. In the displayed dialog box, click **OK**.

> ❗ **Important**
>
> When the smart device is initialized, the installed JP1/ITDM2 - SDM (Smart Device Agent) is removed, and the security policy and Android policy settings, or the security policy and iOS profile settings, are discarded.

Related topics

- *14.5.1 Managed Smart Device List view*
- *14.5.5 Initialize Smart Device dialog box*

8.8 Locking a smart device

You can lock a smart device if, for example, it was lost.

Prerequisites

You must log in by using a user account with the system administrator permission.

Procedure

1. Display the Smart Device module.
2. In the menu area, select **Smart Device**, and then **Managed Smart Device List**.
3. In the information area, select the smart device to be locked.
   You can select multiple smart devices.
4. From **Action**, select **Lock Smart Device**.
5. In the displayed dialog box, click **OK**.

> **Tip**
>
> For Android devices, you can use the **Lock Smart Device** dialog box to lock the device and change the password at the same time.

Related topics

- *8.9 Changing an Android device password*
- *14.5.1 Managed Smart Device List view*
- *14.5.6 Lock Smart Device dialog box*

8.9 Changing an Android device password

If a user forgets an Android device password, you can lock the Android device and change the password.

Prerequisites

You must log in by using a user account with the system administrator permission.

Procedure

1. Display the Smart Device module.
2. In the menu area, select **Smart Device**, **Managed Smart Device List**, and then **Android Smart Device**.
3. In the information area, select the Android device to be locked.
   You can select multiple Android devices.
4. From **Action**, select **Lock Smart Device**.
5. In the **Lock Smart Device** dialog box, select the check box **Change the password used for the lock.**
6. Enter the new password, and then enter it again for confirmation.
7. Click **OK**.
   The Android device is locked and the password is changed.
8. Notify the user to set the password again.

> **Important**
>
> If you select multiple Android devices and change the password, the same password is set for all the selected Android devices. If you want to set different passwords, change the password for each Android device.

Related topics

- *8.10 Resetting an iOS device passcode*
- *14.5.1 Managed Smart Device List view*
- *14.5.6 Lock Smart Device dialog box*

8.10 Resetting an iOS device passcode

If an iOS device user forgets a passcode, you can reset the iOS device passcode.

Prerequisites

You must log in by using a user account with the system administrator permission.

Procedure

1. Display the Smart Device module.

2. In the menu area, select **Smart Device**, **Managed Smart Device List**, and then **iOS Smart Device**.

3. In the information area, select the iOS device of which you want to reset the passcode.
   You can select multiple iOS devices.

4. From **Action**, select **Reset Smart Device Passcode**.

5. In the displayed dialog box, click **OK**.

6. Notify the user to set the passcode again.

Related topics

- *8.9 Changing an Android device password*
- *14.5.1 Managed Smart Device List view*
- *14.5.7 Reset Smart Device Passcode dialog box*

8.11 Sending messages to Android devices

If there is information that must be reported to Android device users, you can send messages from JP1/ITDM2 - SDM to Android devices.

Prerequisites

You must log in by using a user account with the system administrator permission.

Procedure

1. Display the Smart Device module.
2. In the menu area, select **Smart Device**, **Managed Smart Device List**, and then **Android Smart Device**.
3. In the information area, select the Android device to which you want send messages.
   You can select multiple Android devices.
4. From **Action**, select **Send Notification**.
5. In the dialog box that appears, enter the message to be sent.
6. Click **OK**.

Related topics

- *14.5.1 Managed Smart Device List view*
- *14.5.15 Smart Device Message Notification dialog box*

8.12 Collecting smart device log data

You can collect log data output by JP1/ITDM2 - SDM (Smart Device Agent) installed on a smart device.

Procedure

1. On the smart device, start JP1/ITDM2 - SDM (Smart Device Agent) (application name: JP1ITDM2SDM).
2. Tap **Send Log**.

Result

Log data of the smart device is stored in the following file:

JP1/ITDM2 - SDM (Communiation-Server)-installation-folder`\cms\log\agent`
`\`*name*[#1]*_yyyyMMdd_hhmmss*[#2]`.log`

#1: Name of the selected smart device

#2: *yyyy*: year, *MM*: month, *dd*: day, *hh*: hour, *mm*: minute, *ss*: second

Related topics

- *14.5.1 Managed Smart Device List view*
- *F. Storage locations of (and how to obtain) information required for support*

9 Managing Applications

This chapter explains how to manage applications by using JP1/ITDM2 - SDM.

9.1 Registering applications to be distributed in JP1/ITDM2 - SDM

In JP1/ITDM2 - SDM, you can register the applications you want to distribute to smart devices.

> **Important**
>
> If you switch from standard distribution to simple distribution during operation, you will need to re-register all applications.

Prerequisites

- You can register Android applications whose file name extension is `.apk`, and iOS applications whose file name extension is `.ipa`.
- You must log in by using a user account with the system administrator permission.

Procedure

1. Display the Distribution module.
2. In the menu area, select **Android Application** or **iOS Application**.
3. In the information area, click the **Add** button.
4. In the displayed dialog box, type the application information, and then click **OK**.

> **Important**
>
> You cannot specify the following characters for the package name:
>
> <, >, &, |, ^, %

> **Tip**
>
> If you define an application as installable by users, the description of the application to be displayed on the device is the description that you entered in **Description**.
>
> Although a maximum of five lines is allowed in the description of an application to be displayed on devices, the maximum number of characters allowed in the description varies by device type. When entering text in **Description**, we recommend not exceeding 100 characters.

Result

The applications to be distributed are registered in JP1/ITDM2 - SDM, and information for the registered applications is displayed in the Distribution module.

> **Important**
>
> If you distribute in-house iOS applications for internal use, make sure their use is within the scope of the license defined by the Apple Developer Enterprise Program.

Related topics

- *9.2 Placing applications to be distributed on the communication server*

- *9.3 Editing registered application information*
- *9.4 Removing applications from JP1/ITDM2 - SDM*
- *9.6 Distributing applications to Android devices*
- *9.9 Sending instructions to install applications on iOS devices*
- *9.11 Managing applications that can be installed by users*
- *9.12 User-initiated installation of applications on Android devices*
- *9.13 User-initiated installation of applications on iOS devices*
- *14.6.1 Distributed Application List view*
- *14.6.2 Android Application view*
- *14.6.4 iOS Application view*
- *14.6.6 Add Android Application dialog box*
- *14.6.9 Add iOS Application dialog box*

9.2 Placing applications to be distributed on the communication server

After registering applications to be distributed in JP1/ITDM2 - SDM, place those applications on the communication server.

> **Note**
>
> This step is unnecessary if you are using simple distribution.

Prerequisites

- You can deploy Android applications whose file name extension is `.apk`, and iOS applications whose file name extension is `.ipa`.
- The applications to be distributed must be registered in JP1/ITDM2 - SDM in advance.

Procedure

1. Place the applications to be distributed in the following folder on the communication server:

```
JP1/ITDM2 - SDM (Communiation-Server)-installation-folder\cms\uC\httpsd
\htdocs\download
```

2. Rename the application files according to the following conventions:

Application	File name
Android application	*package-name version*`.apk`
iOS application	*package-name version*`.ipa`

package-name

Specify the package name you entered as application information when registering the application in JP1/ITDM2 - SDM.

version

Specify the version number you entered as application information when registering the application in JP1/ITDM2 - SDM.

Example: For an iOS application with the package name `packageA` and the version `1.0`:

```
packageA1.0.ipa
```

Related topics

- *9.1 Registering applications to be distributed in JP1/ITDM2 - SDM*

9.3 Editing registered application information

You can edit information about a registered application.

Prerequisites

You must log in by using a user account with the system administrator permission.

Procedure

1. Display the Distribution module.
2. In the menu area, select **Distributed Application List**.

   > **Tip**
   >
   > After selecting **Android Application** or **iOS Application** in the menu area, you can use the application type to filter the applications to be displayed.

3. In the information area, click the **Edit** button of the application that you want to edit.
4. In the displayed dialog box, edit the application information, and then click **OK**.

   > **Important**
   >
   > If you change the package name when editing application information, you need to make the corresponding change to the application file on the communication server.

   > **Tip**
   >
   > If you define an application as installable by users, the description of the application to be displayed on the device is the description that you entered in **Description**.
   >
   > Although a maximum of five lines is allowed in the description of an application to be displayed on devices, the maximum number of characters allowed in the description varies by device type. When entering text in **Description**, we recommend not exceeding 100 characters.

Related topics

- *9.1 Registering applications to be distributed in JP1/ITDM2 - SDM*
- *9.2 Placing applications to be distributed on the communication server*
- *9.4 Removing applications from JP1/ITDM2 - SDM*
- *9.6 Distributing applications to Android devices*
- *9.9 Sending instructions to install applications on iOS devices*
- *9.11 Managing applications that can be installed by users*
- *9.12 User-initiated installation of applications on Android devices*
- *9.13 User-initiated installation of applications on iOS devices*
- *14.6.1 Distributed Application List view*
- *14.6.2 Android Application view*
- *14.6.4 iOS Application view*

- *14.6.7 Edit Android Application dialog box*
- *14.6.10 Edit iOS Application dialog box*

9.4 Removing applications from JP1/ITDM2 - SDM

If an application is no longer needed, remove it from JP1/ITDM2 - SDM.

Prerequisites

- You must log in by using a user account with the system administrator permission.
- Send an instruction to the smart device (on which the application to be removed has been distributed or installed) to request the user to uninstall the application.

Procedure

1. Display the Distribution module.
2. In the menu area, select **Distributed Application List**.

> **Tip**
>
> After selecting **Android Application** or **iOS Application** in the menu area, you can use the application type to filter the applications to be displayed.

3. In the information area, select the application you want to remove.
4. Click the **Remove** button at the top of the information area.
5. In the displayed dialog box, click **OK**.

Related topics

- *9.1 Registering applications to be distributed in JP1/ITDM2 - SDM*
- *9.3 Editing registered application information*
- *9.5 Removing applications that are no longer needed*
- *9.8 Uninstalling distributed applications from Android devices*
- *9.10 Uninstalling distributed applications from iOS devices*
- *14.6.1 Distributed Application List view*
- *14.6.2 Android Application view*
- *14.6.4 iOS Application view*

9.5 Removing applications that are no longer needed

When an application is no longer needed, remove it from the communication server.

Note

This step is unnecessary if you are using simple distribution.

Prerequisites

- You must have deleted the applications that are no longer needed from JP1/ITDM2 - SDM.
- You must have started the service of the communication server.

Procedure

1. Remove the applications that are no longer needed from the following folder on the communication server:

```
JP1/ITDM2 - SDM (Communiation-Server)-installation-folder\cms\uC\httpsd
\htdocs\download
```

Applications have the following file names:

Application	File name
Android application	*package-name version*`.apk`
iOS application	*package-name version*`.ipa`

Example: For an iOS application with the package name `packageA` and the version `1.0`:

```
packageA1.0.ipa
```

Note

You do not need to restart the service of the communication server after deleting the applications.

Related topics

- *9.8 Uninstalling distributed applications from Android devices*
- *9.10 Uninstalling distributed applications from iOS devices*

9.6 Distributing applications to Android devices

If you want users to install applications as required, distribute the applications to managed Android devices.

> **Note**
>
> You can also use the `sdmdistributeapp` command to distribute applications.

Prerequisites

- You must log in by using a user account with the system administrator permission.
- The applications to be distributed must be registered in JP1/ITDM2 - SDM in advance.
- The applications to be distributed must be placed on the communication server.

Procedure

1. Display the Distribution module.
2. In the menu area, select **Android Application**.
3. In the information area, select the application to be distributed.
4. On the **List of Smart Devices Not Distributed To** tab in the lower part of the information area, select the Android device to which you want to distribute the application.
   You can select multiple Android devices.
5. In the lower part of the information area, select **Action**, and then **Application Distribution**.
6. In the displayed dialog box, click **OK**.

Result

The application is distributed to the selected Android devices. Each user can install the application from the list of distributed applications that are not installed.

After the application is distributed, Android device information is displayed on the **List of Smart Devices Distributed To** tab in the lower part of the information area of the **Android Application** view.

Related topics

- *9.1 Registering applications to be distributed in JP1/ITDM2 - SDM*
- *9.2 Placing applications to be distributed on the communication server*
- *9.3 Editing registered application information*
- *9.7 Sending instructions to install applications on Android devices*
- *14.6.2 Android Application view*

9.7 Sending instructions to install applications on Android devices

You can instruct users to install applications on Android devices. If you send an instruction to a user to install an application that has not been distributed, the application is distributed and then the device displays a request to the user to install the application.

> **Note**
>
> You can also use the `sdmdistributeapp` command to distribute applications and send installation instructions.

Prerequisites

- You must log in by using a user account with the system administrator permission.
- The applications to be distributed must be registered in JP1/ITDM2 - SDM in advance.
- The applications to be distributed must be placed on the communication server.

Procedure

1. Display the Distribution module.
2. In the menu area, select **Android Application**.
3. In the information area, select the application to be installed.
4. Select the Android device on which the application is to be installed.
    - To instruct a user to install a distributed application:
      On the **List of Smart Devices Distributed To** tab in the lower part of the information area, select the Android device on which the application is to be installed. You can select multiple Android devices.
    - To instruct a user to install an application that has not been distributed:
      On the **List of Smart Devices Not Distributed To** tab in the lower part of the information area, select the Android device on which the application is to be installed. You can select multiple Android devices.
5. In the lower part of the information area, select **Action**, and then **Application Installation**.
6. In the displayed dialog box, click **OK**.

Result

The Android device displays a request to install the distributed application.

After the user installs the application, the Android device information appears on the **List of Smart Devices Installed To** tab in the lower part of the information area of the **Android Application** view.

Related topics

- *9.1 Registering applications to be distributed in JP1/ITDM2 - SDM*
- *9.3 Editing registered application information*
- *9.6 Distributing applications to Android devices*
- *14.6.2 Android Application view*

9.8 Uninstalling distributed applications from Android devices

You can send instructions to Android devices to request the user to uninstall distributed or installed applications, and then to delete application data.

Prerequisites

You must log in by using a user account with the system administrator permission.

Procedure

1. Display the Distribution module.
2. In the menu area, select **Android Application**.
3. In the information area, select the application to be uninstalled.
4. In the lower part of the information area, click the **List of Smart Devices Distributed To** or **List of Smart Devices Installed To** tab. Then, select the Android device to which you want to send the instruction to request the user to uninstall the application.

   You can select multiple Android devices.
5. In the lower part of the information area, select **Action**, and then **Application Deletion**.
6. In the displayed dialog box, click **OK**.

Result

If the distributed application is not installed:

> Application data is deleted.

If the distributed application is installed:

> The Android device displays a request to uninstall the application. When the user uninstalls the application, application data is also deleted.

When the application is uninstalled and application data is deleted from the Android device, Android device information appears on the **List of Smart Devices Not Distributed To** tab in the lower part of the information area (**Android Application** view).

Related topics

- *9.6 Distributing applications to Android devices*
- *9.7 Sending instructions to install applications on Android devices*
- *14.6.2 Android Application view*

9.9 Sending instructions to install applications on iOS devices

You can distribute applications to iOS devices, and send instructions to the iOS devices to request users to install those applications.

> **Note**
>
> You can also use the `sdmdistributeapp` command to send installation instructions.

Prerequisites

- You must log in by using a user account with the system administrator permission.
- The applications to be distributed must be registered in JP1/ITDM2 - SDM in advance.
- The applications to be distributed must be placed on the communication server.

Procedure

1. Display the Distribution module.
2. In the menu area, select **iOS Application**.
3. In the information area, select the application to be installed.
4. From the **List of Smart Devices Not Installed To** tab in the bottom of the information area, select the iOS devices in which the application is to be installed.
   You can select multiple iOS devices.
5. In the lower part of the information area, select **Action**, and then **Application Installation**.
6. In the displayed dialog box, click **OK**.

Result

The applications are distributed to the selected iOS devices, and the iOS device displays a request to install the applications.

After a user installs an application, the iOS device information appears on the **List of Smart Devices Installed To** tab in the lower part of the information area of the **iOS Application** view.

Related topics

- *9.1 Registering applications to be distributed in JP1/ITDM2 - SDM*
- *9.2 Placing applications to be distributed on the communication server*
- *9.3 Editing registered application information*
- *14.6.4 iOS Application view*

9.10 Uninstalling distributed applications from iOS devices

You can send an instruction to iOS devices to request the users to uninstall an application.

Prerequisites

You must log in by using a user account with the system administrator permission.

Procedure

1. Display the Distribution module.
2. In the menu area, select **iOS Application**.
3. In the information area, select the application to be uninstalled.
4. In the lower part of the information area, click the **List of Smart Devices Installed To** tab. Then, select the iOS device to which you want to send the instruction to uninstall the application.
   You can select multiple iOS devices.
5. In the lower part of the information area, select **Action**, and then **Application Deletion**.
6. In the displayed dialog box, click **OK**.

Result

The iOS device displays a request to uninstall the application. When the user uninstalls the application, application data is also deleted.

When the application is uninstalled and application data is deleted from the iOS device, iOS device information appears on the **List of Smart Devices Not Installed To** tab in the lower part of the information area (**iOS Application** view).

Related topics

- *9.9 Sending instructions to install applications on iOS devices*
- *14.6.4 iOS Application view*

9.11 Managing applications that can be installed by users

The administrator can manage applications that can be installed by users.

The following table lists the tasks you might perform when managing applications that can be installed by users, and how to perform those tasks:

Task during operation	Procedure
Define new applications as installable by users	1. Register the applications to be distributed in JP1/ITDM2 - SDM. 2. Place the applications to be distributed on the communication server. 3. Execute the `sdmioutils importdeliverypermit -mode all`.
Add applications to be distributed and replace them with new versions	1. Register the applications to be distributed in JP1/ITDM2 - SDM. 2. Place the applications to be distributed on the communication server. 3. Execute the `sdmioutils importdeliverypermit -mode app`.
Stop distribution of old versions of applications and applications that are no longer required	1. Execute the `sdmioutils deletedeliverypermit -mode app`. 2. Place the applications to be distributed on the communication server. 3. Remove the distributed application from JP1/ITDM2 - SDM.
Add smart devices	1. Execute the `sdmioutils importdeliverypermit -mode device`.
Dispose of smart devices	1. Execute the `sdmioutils deletedeliverypermit -mode device`. 2. Set the smart devices to *Unmanaged*.
Check applications that can be installed by users	1. Execute the `sdmioutils exportdeliverypermit`.
Back up and restore applications that can be installed by users	1. Acquire a backup by running the `sdmioutils exportdeliverypermit -mode all` command. 2. Restore the backup by running the `sdmioutils importdeliverypermit -mode all` command.

Tip

Before you use the `sdmioutils importdeliverypermit` command or `sdmioutils deletedeliverypermit` command to change settings, we recommend that you use the `sdmioutils exportdeliverypermit -mode all` command to back up the existing settings.

Result

- *8.4 Setting managed smart devices to Unmanaged*
- *9.1 Registering applications to be distributed in JP1/ITDM2 - SDM*
- *9.2 Placing applications to be distributed on the communication server*
- *9.4 Removing applications from JP1/ITDM2 - SDM*
- *9.5 Removing applications that are no longer needed*
- *15. sdmioutils importdeliverypermit (defining applications that can be installed by users)*
- *15. sdmioutils exportdeliverypermit (exporting settings that define applications as installable by users)*
- *15. sdmioutils deletedeliverypermit(deleting settings that define applications as installable by users)*

9.12 User-initiated installation of applications on Android devices

The user of an Android device can initiate the installation of certain applications.

Prerequisites

- The applications to be distributed must be registered in JP1/ITDM2 - SDM in advance.
- The applications to be distributed must be placed on the communication server.
- The applications that can be installed by users must be defined in advance.

Procedure

1. On the Android device, start JP1/ITDM2 - SDM (Smart Device Android Agent).

2. Tap **Install Applications**.

3. If a confirmation dialog box appears, click **OK**.

4. In the List of Distributed Applications view, tap the application you want to install.

5. Tap **OK** in the confirmation dialog box.
   The application starts to download.

6. Tap **Install** in the confirmation dialog box.

> **Important**
>
> It might take some time for the new installation status to appear in the List of Distributed Applications view.

Related topics

- *9.1 Registering applications to be distributed in JP1/ITDM2 - SDM*
- *9.2 Placing applications to be distributed on the communication server*
- *9.11 Managing applications that can be installed by users*

9.13 User-initiated installation of applications on iOS devices

The user of an iOS device can initiate the installation of certain applications.

Prerequisites

- The applications to be distributed must be registered in JP1/ITDM2 - SDM in advance.
- The applications to be distributed must be placed on the communication server.
- The applications that can be installed by users must be defined in advance.

Procedure

1. On the iOS device, start JP1/ITDM2 - SDM (Smart Device iOS Agent).
2. Tap **Install Applications**.
3. If a confirmation dialog box appears, tap **OK**.
4. In the List of Distributed Applications view, tap the application you want to install.
5. Tap **OK** in the confirmation dialog box.
   The application starts to download.
6. If a confirmation dialog box appears, tap the **Install** button.

> **Important**
>
> It might take some time for the new installation status to appear in the List of Distributed Applications view.

Related topics

- *9.1 Registering applications to be distributed in JP1/ITDM2 - SDM*
- *9.2 Placing applications to be distributed on the communication server*
- *9.11 Managing applications that can be installed by users*

9.14 Limiting the maximum concurrent downloads of distributed applications

When you allow users to initiate the download and installation of applications themselves, considerable load might be placed on the network if multiple smart devices download applications simultaneously, and this can impact other business processes. In these circumstances, you can reduce the load on the network by limiting the maximum number of concurrent downloads.

Procedure

1. On the communication server, open the `httpsd.conf`.

   The `httpsd.conf` file is stored in the following location:

   JP1/ITDM2 - SDM (Communication Server)-installation-folder`\cms\uC\httpsd\conf`

2. Change the value of the `QOSRejectionServers` directive in the `httpsd.conf` file.

   Specify the `QOSRejectionServers` directive as follows:

Location	Directive name	Specifiable range	Description
Inside `<Location /download/>` in `<VirtualHost localhost:26055>`	`QOSRejectionServers`	5 to 49 default: 5 (maximum concurrent downloads: 45)	Specify the maximum concurrent downloads as the value of `50 –` *value-of-QOSRejectionServers*.

   Example

```
Listen 26055
<VirtualHost localhost:26055>
    SSLEnable
    SSLProtocol TLSv11 TLSv12
    SSLRequiredCiphers DES-CBC3-SHA:AES128-SHA:AES256-SHA
    SSLCertificateFile "C:/Program Files/Hitachi/.../newcert.pem"
    SSLCertificateKeyFile "C:/Program Files/Hitachi/.../newkeyRSA.pem"
    <Location /download/>
         Allow from all
         QOSRejectionServers 5
    </Location>
</VirtualHost>
```

3. Restart the `JP1/ITDM2 - Smart Device Manager Web Server` on the communication server.

10 Event Reference

This chapter describes how to reference events that are output by JP1/ITDM2 - SDM.

10.1 Viewing event details

You can view details about events output by JP1/ITDM2 - SDM.

Procedure

1. Display the Events module.
2. In the menu area, select **Events**, and then select the severity of the events you want to display.
3. In the information area, click the link in the **Description** column for the event for which you want to display details.
   Alternatively, select the event for which you want to display details, and then select **Action** and **Show Details,** to open the **Event Detail** dialog box.

Result

Details of the events you have selected are displayed in the **Event Detail** dialog box.

Related topics

- *2.7 Displaying events*
- *14.7.1 Event List view*
- *14.7.2 Event Detail dialog box*

10.2 Exporting event information

You can export information about events that occurred in the past week to a CSV file. The maximum number of records that can be exported is 200,000.

Procedure

1. Display the Events module.
2. From **Action**, select **Export Event List**.
3. In the window that appears, specify the file name and the location to save the file, and then click the **Save** button

Result

The CSV file is saved with the specified file name in the specified location.

Related topics

- *2.7 Displaying events*
- *14.7.1 Event List view*

11 Customizing Settings

This chapter describes items that can be customized in the Settings module.

11.1 Specifying settings for event notification

You can specify settings for mail notification so that when a specific event occurs, you can be notified of the event occurrence via email.

Prerequisites

- You must log in by using a user account with the system administrator permission.
- You must set up the mail server.

Procedure

1. Display the Settings module.
2. In the menu area, select **Events**, and then **Event Notifications**.
3. In the window that appears, select the check boxes for the severity and types of events about which you want to be notified by email, and user IDs of email recipients.

Postrequisites

Use the event mail format information file to define the event email format.

Related topics

- *2.7 Displaying events*
- *11.2 Setting up mail servers*
- *14.8.4 Event Notifications view*
- *16.4 Event mail format information file (eventmail.properties)*

11.2 Setting up mail servers

To receive notification emails about the occurrence of an event, you must specify information about the mail server used by JP1/ITDM2 - SDM to send the email notifications.

Prerequisites

You must log in by using a user account with the system administrator permission.

Procedure

1. Display the Settings module.

2. In the menu area, select **General** and then **SMTP Server**.

3. In the information area, specify the mail server information.
   Click the **Send a Test Email** button to send a test email to the email address set for the user account of a logged-in user. Check if the test mail is sent properly.

4. Click the **Apply** button.

Result

Emails can be sent by using the specified user.

Related topics

- *11.1 Specifying settings for event notification*
- *14.8.5 SMTP Server view*

12 Database Management

This chapter describes how to manage a database.

12.1 Backing up the database

Back up the database before replacing the smart device manager and for restoration in case of a hard disk failure.

> **Important**
>
> In addition to backing up the database, you need to back up the applications placed on the communication server.

Procedure

1. On the communication server, stop the following service from the Windows Services window:
   JP1/ITDM2 - Smart Device Manager Web Server

2. On the communication server, stop the following service from the Windows Services window:
   JP1/ITDM2 - Smart Device Manager (Communication Server Service)

3. On the smart device manager, stop the following service from the Windows Services window:
   JP1/ITDM2 - Smart Device Manager Web Server

4. On the smart device manager, stop the following service from the Windows Services window:
   JP1/ITDM2 - Smart Device Manager Server Service

5. On the smart device manager, start the command prompt, and then change the current directory to the command storage location.

6. On the smart device manager, execute the `sdmexportdb` command.

7. On the smart device manager, start the following service from the Windows Services window:
   JP1/ITDM2 - Smart Device Manager Server Service

8. On the smart device manager, start the following service from the Windows Services window:
   JP1/ITDM2 - Smart Device Manager Web Server

9. On the communication server, start the following service from the Windows Services window:
   JP1/ITDM2 - Smart Device Manager (Communication Server Service)

10. On the communication server, start the following service from the Windows Services window:
    JP1/ITDM2 - Smart Device Manager Web Server

Result

The backup data (that is, the backup of the data) is saved. By default, the backup data is stored in the following folder:

JP1/ITDM2 - SDM (Smart Device Manager)-installation-folder`\mgr\backup`

Related topics

- *9.2 Placing applications to be distributed on the communication server*
- *15. Executing commands*
- *15. sdmexportdb (acquiring backup data)*
- *B.1 List of services*

12.2 Restoring the database

You can restore the database to the status when it was backed up. To restore the database, you need backup data acquired by using the `sdmexportdb` command.

> **Important**
>
> In addition to restoring the database, you need to place the application to be distributed on the communication server.

Procedure

1. On the communication server, stop the following service from the Windows Services window:
   JP1/ITDM2 - Smart Device Manager Web Server
2. On the communication server, stop the following service from the Windows Services window:
   JP1/ITDM2 - Smart Device Manager (Communication Server Service)
3. On the smart device manager, stop the following service from the Windows Services window:
   JP1/ITDM2 - Smart Device Manager Web Server
4. On the smart device manager, stop the following service from the Windows Services window:
   JP1/ITDM2 - Smart Device Manager Server Service
5. Copy the backup data acquired by the `sdmexportdb` command to the smart device manager.
6. On the smart device manager, start the command prompt, and then change the current directory to the command storage location.
7. On the smart device manager, execute the `sdmimportdb` command.
8. On the smart device manager, start the following service from the Windows Services window:
   JP1/ITDM2 - Smart Device Manager Server Service
9. On the smart device manager, start the following service from the Windows Services window:
   JP1/ITDM2 - Smart Device Manager Web Server
10. On the communication server, start the following service from the Windows Services window:
    JP1/ITDM2 - Smart Device Manager (Communication Server Service)
11. On the communication server, start the following service from the Windows Services window:
    JP1/ITDM2 - Smart Device Manager Web Server

Result

The database of JP1/ITDM2 - SDM (Smart Device Manager) is restored to the status when the backup data was acquired.

Related topics

- *9.2 Placing applications to be distributed on the communication server*
- *15. Executing commands*
- *15. sdmimportdb (restoring backup data)*

- *B.1 List of services*

12.3 Changing the connection destination port number for the database

You can change the connection destination port number for the database on the smart device manager.

Prerequisites

You must stop all the JP1/ITDM2 - SDM program modules and all commands.

Procedure

1. On the communication server, stop the following service from the Windows Services window:
   JP1/ITDM2 - Smart Device Manager Web Server

2. On the communication server, stop the following service from the Windows Services window:
   JP1/ITDM2 - Smart Device Manager (Communication Server Service)

3. On the smart device manager, stop the following service from the Windows Services window:
   JP1/ITDM2 - Smart Device Manager Web Server

4. On the smart device manager, stop the following service from the Windows Services window:
   JP1/ITDM2 - Smart Device Manager Server Service

5. On the smart device manager, stop the following service from the Windows Services window:
   JP1/ITDM2 - Smart Device Manager (DB Service)

6. On the smart device manager, use a text editor to open the following file:
   JP1/ITDM2 - SDM (Smart Device Manager)-installation-folder`\db\conf\pdsys`

7. If necessary, change the values of `pd_name_port` and `pd_service_port`.
   Example: Change the underlined part:

   ```
   set pd_name_port = 26066
   set pd_service_port = 26067
   ```

   For `pd_name_port`, set the port number used to connect the smart device manager and its database.

   For `pd_service_port`, set the port number used to connect the communication server and the database of the smart device manager.

8. On the smart device manager, start the following service from the Windows Services window:
   JP1/ITDM2 - Smart Device Manager (DB Service)

9. On the smart device manager, start the command prompt, and then change the current directory to the command storage location.

10. On the smart device manager, execute the `sdmnetchange` command.

    ```
    sdmnetchange -target Manager -port port-number-specified-in-pd_name_port
    ```

11. On the smart device manager, start the following service from the Windows Services window:
    JP1/ITDM2 - Smart Device Manager Server Service

12. On the smart device manager, start the following service from the Windows Services window:
    JP1/ITDM2 - Smart Device Manager Web Server

13. On the communication server, start the command prompt, and then change the current directory to the command storage location.

14. On the communication server, execute the `sdmnetchange` command.

```
sdmnetchange -target Comsrv -port port-number-specified-in-pd_service_port
```

15. On the communication server, start the following service from the Windows Services window:
    JP1/ITDM2 - Smart Device Manager (Communication Server Service)

16. On the communication server, start the following service from the Windows Services window:
    JP1/ITDM2 - Smart Device Manager Web Server

17. On the smart device manager, use a text editor to open the following file:
    JP1/ITDM2 - SDM (Smart Device Manager)-installation-folder`\mgr\conf\sdmdbport.conf`

18. Change the value in the file to the port number you set for `pd_name_port` in step 7.

Result

The connection destination port number for the database is changed.

Related topics

- *15. Executing commands*
- *15. sdmnetchange (changing the network configuration for the smart device manager or communication server)*
- *B.1 List of services*

13 Troubleshooting

This chapter describes the actions to be taken when a problem occurs in JP1/ITDM2 - SDM.

13.1 Troubleshooting procedure on the smart device manager

This section describes the actions to take if a problem occurs during operation of the smart device manager.

Procedure

1. Check the error message.
   Check the error message as follows:
   - Check the error information in the dialog box that was displayed when the error occurred.
   - Check the error information in the output log files.
   - Check the event message in the Home module or in the Events module.
2. Using the error message, check the cause of and workaround for the trouble, and then take action to resolve the problem.
   If necessary, collect log data (troubleshooting information) for the smart device manager.

Related topics

- *10.1 Viewing event details*
- *15. sdmgetlogs (collecting log information)*
- *17. Messages*
- *F. Storage locations of (and how to obtain) information required for support*

13.2 Troubleshooting procedure on a smart device

This section describes the actions to take if a problem occurs during operation of a smart device.

Procedure

1. Check the error message.
   Check the event message in the Home module or in the Events module.

2. Using the error message, check the cause of and workaround for the trouble, and then take action to resolve the problem.
   If necessary, collect smart device log data (troubleshooting information).

Related topics

- *8.12 Collecting smart device log data*
- *10.1 Viewing event details*
- *14.3 Home module*
- *14.7 Events module*
- *17. Messages*

13.3 Actions to be taken when a disk is low on free space

If the amount of free space on the disk that contains the database for JP1/ITDM2 - SDM (Smart Device Manager) is insufficient, new data cannot be added and management with correct information is disabled. To avoid such problems, it is necessary to monitor the free space available on the disk that JP1/ITDM2 - SDM (Smart Device Manager) uses, and to take action when this space runs low.

You can check the free space on the disk that JP1/ITDM2 - SDM (Smart Device Manager) uses from the **Database and Disk Usage** panel in the Home module. If the free space on the disk is becoming low, take action to increase free space.

For example, you can perform the following:

- Delete unnecessary data from the disk.
- If you are using a logical drive, increase its storage capacity by expanding the disk.

If you cannot provide free disk space, replace the smart device manager. You need to back up the database before replacing the smart device manager. After replacing the smart device manager, install JP1/ITDM2 - SDM (Smart Device Manager), and then restore the database from the backup file.

Related topics

- *3.5 Procedure for installing JP1/ITDM2 - SDM (Smart Device Manager)*
- *12.1 Backing up the database*
- *12.2 Restoring the database*
- *14.3.3 Database and Disk Usage panel*

13.4 Troubleshooting for a communication error between servers

This section describes the actions to take if a communication error occurs between servers.

13.4.1 Actions to take if a communication error occurs between the smart device manager and the communication server

The following describes the possible causes and actions to take if a communication error occurs between the smart device manager and the communication server:

Cause	Action
The service of the smart device manager or communication server is stopped.	Start the service of the relevant server from the Windows Services window.
The connection-destination address and port number settings between the smart device manager and communication server are not correct.	Revise the network settings.
The Web server's SSL communication settings on the communication server contain an error.	Revise the SSL communication settings on the communication server.
Other than the above (disconnected cable or hardware failure)	Contact the system administrator.

Related topics

- *3.1 Flow of building a system*
- *3.8 Opening ports on the router and setting up a firewall on each server*
- *3.11 Obtaining certificates for SSL communication*

13.4.2 Actions to take if a communication error occurs between the communication server and the messaging server

The following describes the possible causes and actions to take if a communication error occurs between the communication server and the messaging server:

Cause	Action
The service of the communication server or messaging server is stopped.	Start the service of the relevant server from the Windows Services window.
The connection-destination address and port number settings between the communication server and messaging server are not correct.	Revise the network settings.
Other than the above (disconnected cable or hardware failure)	Contact the system administrator.

Related topics

- *3.8 Opening ports on the router and setting up a firewall on each server*

13.5 Troubleshooting during window operation

The following describes the possible cause and action to take if downloading of the export file does not start when you try to export a list of smart devices or a list of events:

Cause	Action
The **Enable Protected Mode** check box for **Trusted Sites** is cleared in the Internet Explorer settings.	For Internet Explorer 8, specify as follows: • Add the smart device manager to **Trusted sites**. • Change the security level for **Trusted sites**. • Select the **Enable Protected Mode** check box. For details, see the information provided by Microsoft.

13.6 Troubleshooting problems with the database

This section describes the actions to take if a database problem occurs.

13.6.1 Actions to take if a database connection error occurs

The following describes the possible cause and action to take if a database connection error occurs:

Cause	Action
JP1/ITDM2 - Smart Device Manager (DB Service) has stopped or is starting.	• If JP1/ITDM2 - Smart Device Manager (DB Service) has stopped, from the Windows Services window, start JP1/ITDM2 - Smart Device Manager (DB Service). • If JP1/ITDM2 - Smart Device Manager (DB Service) is starting, wait until it has started.

13.6.2 Actions to take if a database access error occurs

The following describes the possible cause and actions to take if a database connection error occurs:

Cause	Action
An access error is caused by database corruption.	Try to restore the database by using the database restore command.

13.6.3 Actions to take if database backup or restoration fails

The following describes the possible causes and actions to take if database backup or restoration fails:

Cause	Action
You do not have permission to access the database storage folder.	Make sure that you have permissions to access the database storage folder. If you do not have the required access permission for the folder, obtain it, and then try to back up or restore the database again.
An I/O error occurred.	Make sure that no disk error occurred. If a disk error occurred, set up the environment again, such as replacing the hard disk.

If the problem cannot be corrected by taking the above actions, collect the backup data of the database and troubleshooting information.

Related topics

- *15. sdmgetlogs (collecting log information)*
- *A.1 Folders created on the smart device manager*

13.7 Troubleshooting regarding installation of applications on iOS devices

This section describes the actions to take if a problem occurs during installation of an application on an iOS device.

13.7.1 Actions to take if installation of an iOS application fails

The following describes the possible causes and actions to take if installation of an iOS application fails.

Cause	Action
Bundle ID is not correct.	Make sure **Bundle ID** is the same as that specified by the application developer when the distribution file was made.
Installation Parameter is not correct.	Check and, if necessary, revise **Installation Parameter**. For details, visit Apple's website.
Apps below **Add / Remove** of **Access Rights** in **Mobile Device Management** is not selected when the configuration profile on the communication server is created by using the Apple iPhone Configuration Utility.	Make sure that **Apps** is selected when you create the configuration profile. Store the profile on the communication server.

13.7.2 Actions to take if the results of the installation of an application do not appear in the iOS Application view

The following describes the possible causes and actions to take if the results of an installation of an application do not appear in the **iOS Application** view.

Cause	Action
The most recent inventory information item is not obtained from the iOS device.	Take either of the following actions: • Click **Update Device Details** from the **Action** menu in the **Managed Smart Device List** view. • Send inventory information from the JP1/ITDM2 - SDM instance (Smart Device Agent) on the iOS device.
Bundle ID or **Version** of the registered iOS application is not correct.	Make sure that **Bundle ID** and **Version** are the same as those which the application developer specified when the distribution file was made.

14 GUI Reference

This chapter describes the windows of JP1/ITDM2 - SDM, buttons, operation menus, and items displayed in windows.

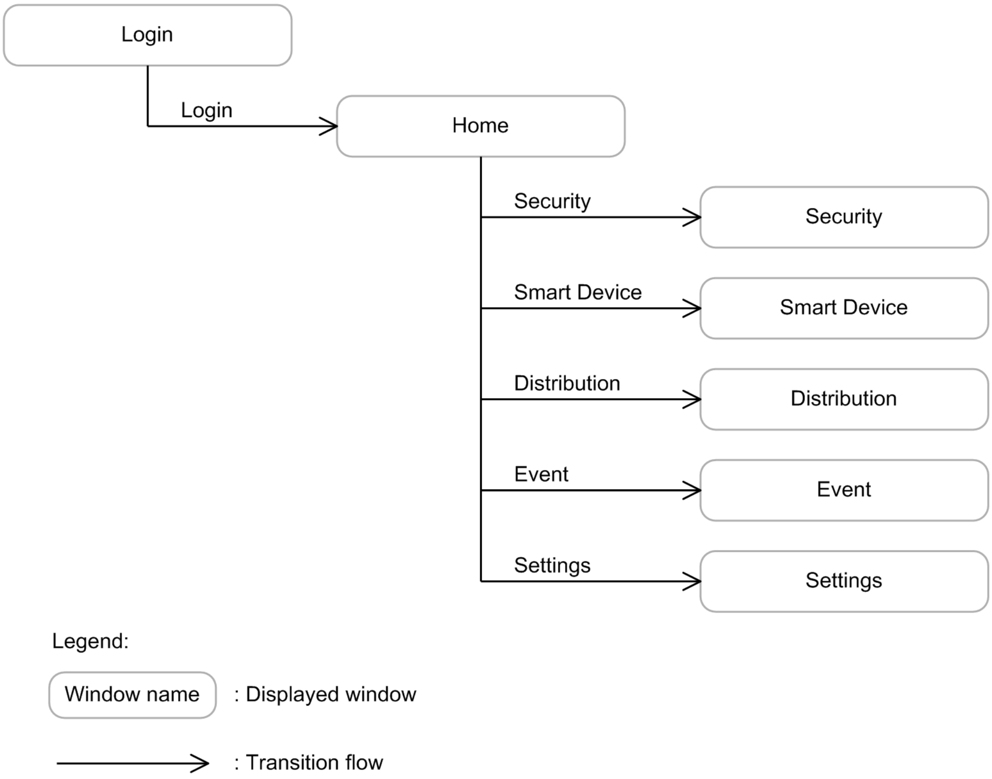
14.1 Window transition diagrams

This section describes window transitions in JP1/ITDM2 - SDM.

14.1.1 Window transitions from the Login window to immediately after the login

The following shows the window transitions from the Login window to immediately after the login.

Window transitions



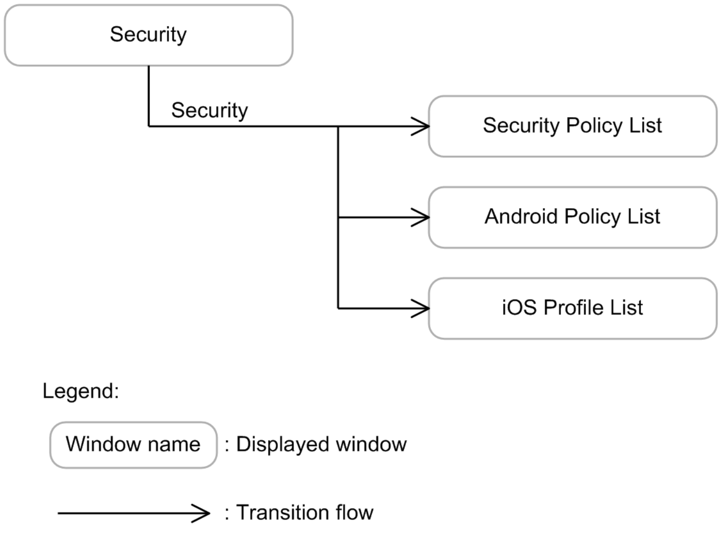
Related Topics

- *14.2 Login window*
- *14.3 Home module*
- *14.4 Security module*
- *14.5 Smart Device module*
- *14.6 Distribution module*
- *14.7 Events module*
- *14.8 Settings module*

14.1.2 Window transitions from the Security module

The following shows the window transitions from the Security module used to manage security rules.

Window transitions



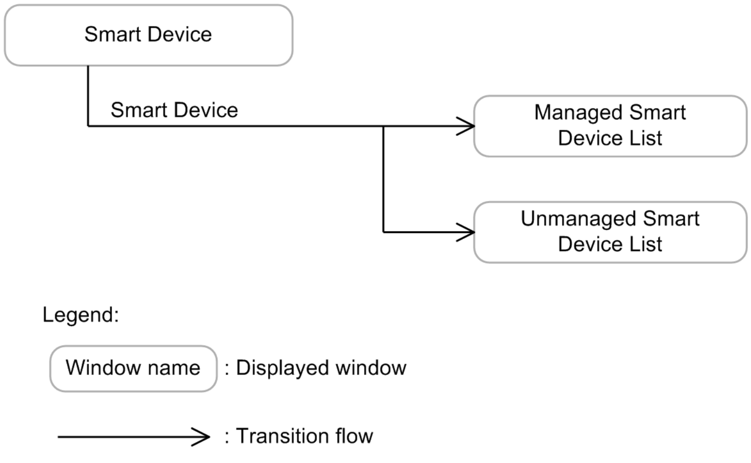
Related Topics

- *14.4 Security module*
- *14.4.1 Security Policy List view*
- *14.4.11 Android Policy List view*
- *14.4.15 iOS Profile List view*

14.1.3 Window transitions from the Smart Device module

The following shows the window transitions from the Smart Device module used to manage smart device information.

Window transitions



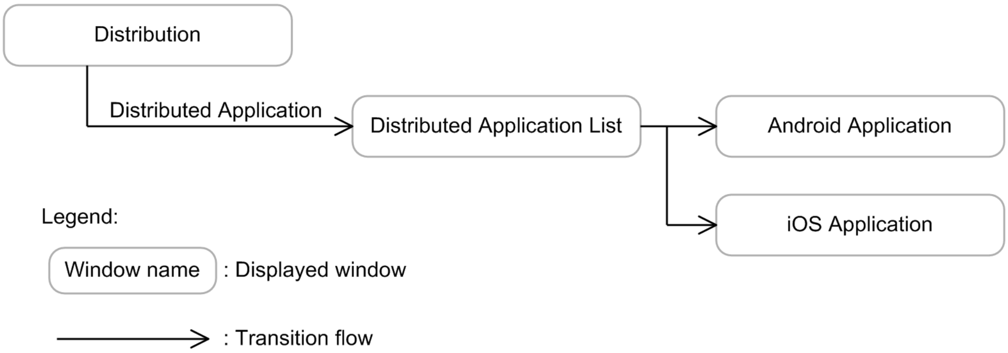
Related Topics

- *14.5 Smart Device module*
- *14.5.1 Managed Smart Device List view*
- *14.5.3 Unmanaged Smart Device List view*

14.1.4 Window transitions from the Distribution module

The following shows the window transitions from the Distribution module used to manage applications to be distributed.

Window transitions



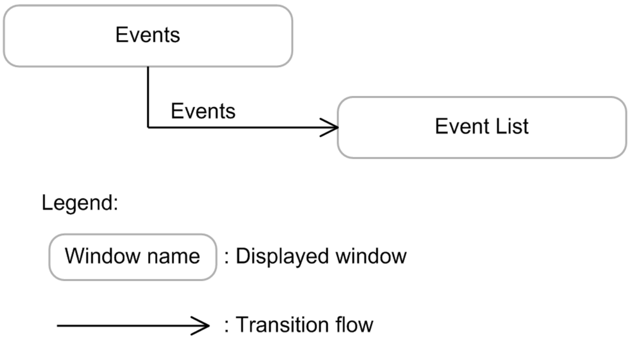
Related Topics

- *14.6 Distribution module*
- *14.6.1 Distributed Application List view*
- *14.6.2 Android Application view*
- *14.6.4 iOS Application view*

14.1.5 Window transitions from the Events module

The following shows the window transitions from the Events module used to check events that occurred during JP1/ITDM2 - SDM operation.

Window transitions



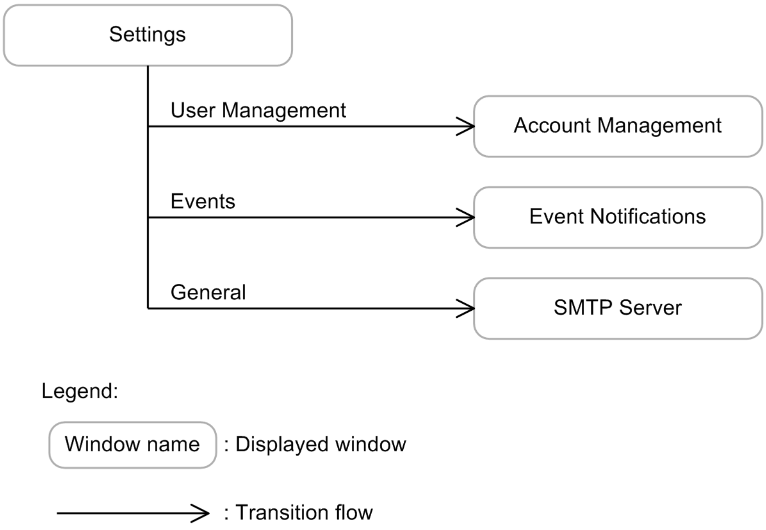
Related Topics

- *14.7 Events module*
- *14.7.1 Event List view*

14.1.6 Window transitions from the Settings module

The following shows the window transitions from the Settings module used to specify settings required for operating JP1/ITDM2 - SDM.

Window transitions



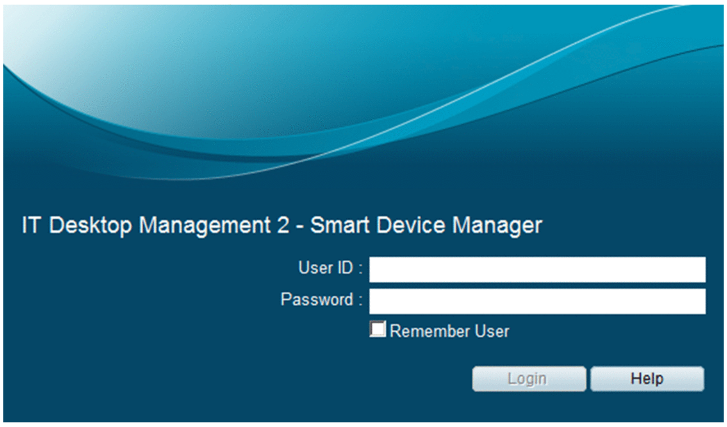
Related Topics

- *14.8 Settings module*
- *14.8.1 Account Management view*
- *14.8.4 Event Notifications view*
- *14.8.5 SMTP Server view*

14.2 Login window

Any user who logs in through the Login window must be authenticated. When authentication is successful, the user can log in to JP1/ITDM2 - SDM. If the built-in account or a newly created user account is used to log in, or if the password has expired, the **Change Password** dialog box is displayed.

Window



Items

The following describes the items displayed in the window.

User ID

Enter the user ID used to log in to JP1/ITDM2 - SDM (Smart Device Manager).

Password

Enter the password for the user name.

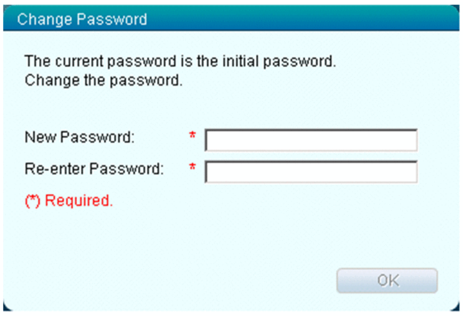
Related Topics

- *14.2.1 Change Password dialog box*

14.2.1 Change Password dialog box

You can use the Change Password dialog box to change the password. If the built-in account or a newly created user account is used to log in, or if the password has expired, the **Change Password** dialog box is displayed.

Window



The current password is the initial password.
Change the password.

Items

The following describes the items displayed in the window.

New Password

Enter a new password.

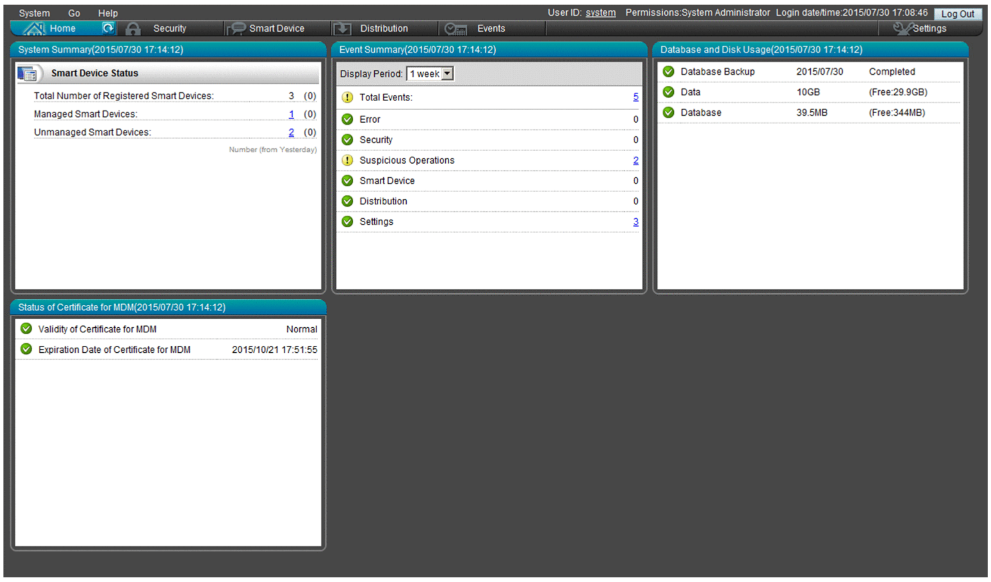
Re-enter Password

Re-enter the password for confirmation.

14.3 Home module

The Home module is the initial module displayed to a user who logs in to JP1/ITDM2 - SDM. This module displays panels that provide an overview of information managed by JP1/ITDM2 - SDM.

Window



User ID: system Permissions:System Administrator Login date/time:2015/07/30 17:08:46

System Summary(2015/07/30 17:14:12)

Smart Device Status

Total Number of Registered Smart Devices:	3	(0)
Managed Smart Devices:	1	(0)
Unmanaged Smart Devices:	2	(0)

Number (from Yesterday)

Event Summary(2015/07/30 17:14:12)

Display Period: 1 week

Total Events:	5
Error	0
Security	0
Suspicious Operations	2
Smart Device	0
Distribution	0
Settings	3

Database and Disk Usage(2015/07/30 17:14:12)

Database Backup	2015/07/30	Completed
Data	10GB	(Free:29.9GB)
Database	39.5MB	(Free:344MB)

Status of Certificate for MDM(2015/07/30 17:14:12)

Validity of Certificate for MDM	Normal
Expiration Date of Certificate for MDM	2015/10/21 17:51:55

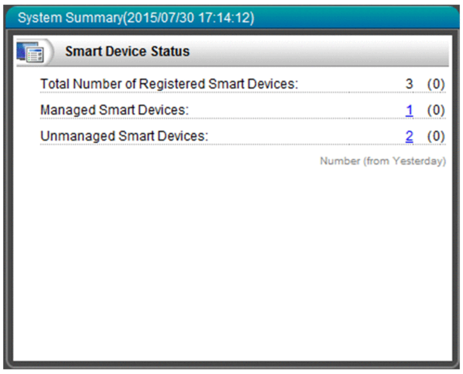
Related Topics

- *14.3.1 System Summary panel*
- *14.3.2 Event Summary panel*
- *14.3.3 Database and Disk Usage panel*
- *14.3.4 Status of Certificate for MDM panel*

14.3.1 System Summary panel

The System Summary panel displays an overview of the statuses of the managed smart devices.

Window



System Summary(2015/07/30 17:14:12)

Smart Device Status

Total Number of Registered Smart Devices:	3	(0)
Managed Smart Devices:	1	(0)
Unmanaged Smart Devices:	2	(0)

Number (from Yesterday)

Items

The following describes the items displayed in the window.

Total Number of Registered Smart Devices

Displays the total number of smart devices registered in JP1/ITDM2 - SDM, and the difference from the previous day's number of smart devices.

Managed Smart Devices

Displays the number of managed smart devices, and the difference from the previous day's number of smart devices. If the current number of smart devices is one or more, clicking the link on the number displays the Smart Device module, in which you can check detailed information about managed smart devices.

Unmanaged Smart Devices

Displays the number of unmanaged smart devices, and the difference from the previous day's number of smart devices. If the current number of smart devices is one or more, clicking the link on the number displays the Smart Device module, in which you can check detailed information about unmanaged smart devices.

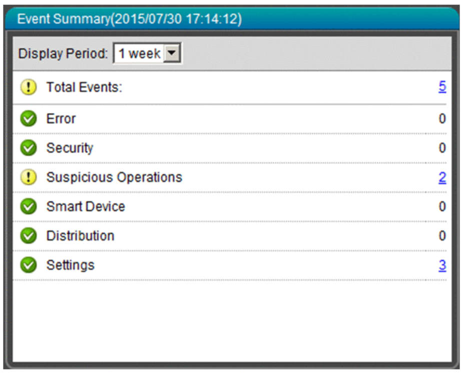
Related Topics

- *14.5 Smart Device module*

14.3.2 Event Summary panel

The **Event Summary** panel displays the total number of events that occurred in the specified display period, and the number of events by event type.

Window



Event Summary(2015/07/30 17:14:12)

Display Period: 1 week

!	Total Events:	5
✓	Error	0
✓	Security	0
!	Suspicious Operations	2
✓	Smart Device	0
✓	Distribution	0
✓	Settings	3

Clicking the link on the number of events displays the Events module, in which you can check the contents of events.

Items

The following describes the items displayed in the window.

Display Period

Changes the event display period.

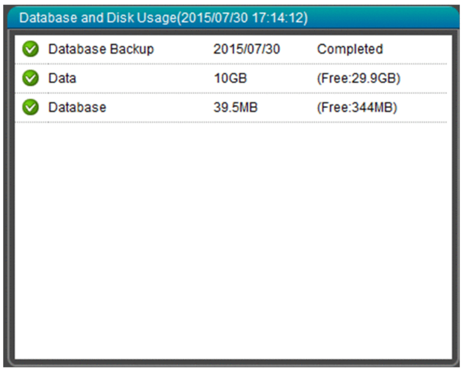
Related Topics

- *14.7 Events module*

14.3.3 Database and Disk Usage panel

In the **Database and Disk Usage** panel, you can check database-related information, including the database backup status and free space on the hard disk.

Window



Database and Disk Usage(2015/07/30 17:14:12)

✓	Database Backup	2015/07/30	Completed
✓	Data	10GB	(Free:29.9GB)
✓	Database	39.5MB	(Free:344MB)

Items

The following describes the items displayed in the window.

Database Backup

Displays the date when the database was backed up, and the backup status.

Data

Displays the hard disk usage and free space.

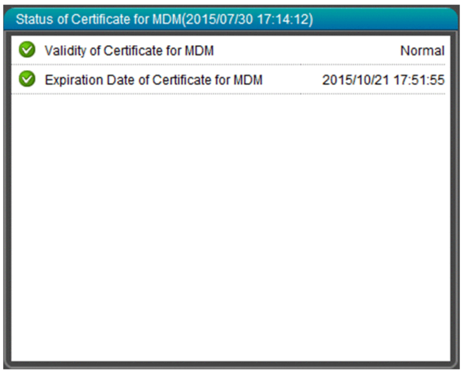
Database

Displays the hard disk usage for the database, and free space.

14.3.4 Status of Certificate for MDM panel

In the **Status of Certificate for MDM** panel, you can check information about the expiration dates of certificates and the validity of a certificate.

Window



Status of Certificate for MDM(2015/07/30 17:14:12)

✓	Validity of Certificate for MDM	Normal
✓	Expiration Date of Certificate for MDM	2015/10/21 17:51:55

Items

The following describes the items displayed in the window.

Validity of Certificate for MDM

Displays the validity of the certificate for MDM.

The following describes the displayed information:

Information	Description
Not Used	The certificate is not set.
Normal	The certificate is set (normal).
Invalid	The certificate is set (invalid).

Expiration date of Certificate for MDM

Displays the expiration date of the certificate for MDM.

The following describes the displayed information:

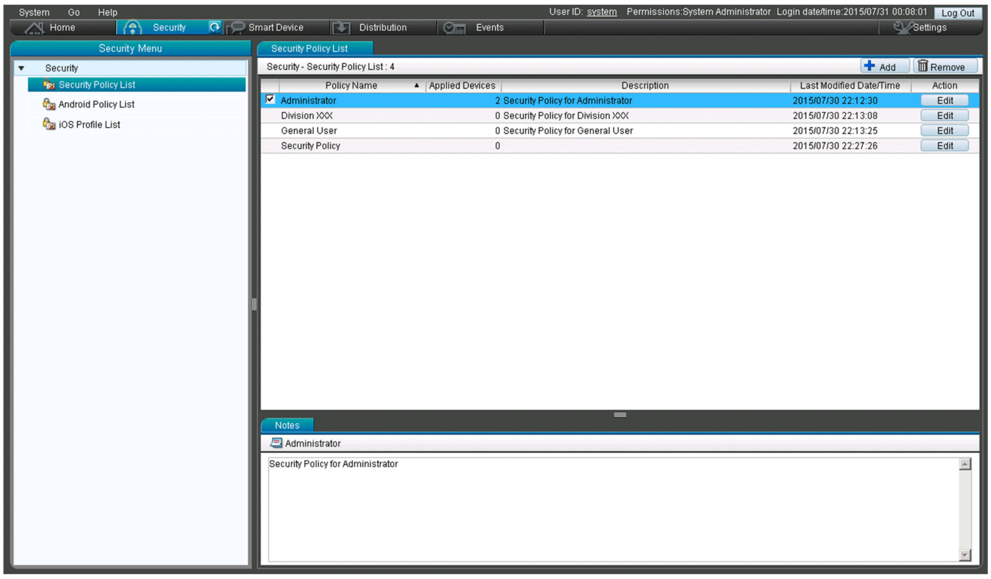
Information	Description
hyphen (-)	The certificate for MDM is not set.
yyyy/*MM*/*dd* *hh*:*mm*:*ss*# (Date/Time)	The certificate for MDM is set.
✖ (Critical)	Expired
! (Warning)	One month before expiration
✓ (Information)	Within the valid period, or the certificate for MDM is not set.

# *yyyy*: year, *MM*: month, *dd*: day, *hh*: hour, *mm*: minute, *ss*: second

14.4 Security module

In the Security module, you can manage security rules provided in JP1/ITDM2 - SDM.

Window



User ID: system Permissions:System Administrator Login date/time:2015/07/31 00:08:01

Security - Security Policy List : 4

	Policy Name	Applied Devices	Description	Last Modified Date/Time	Action
☑	Administrator	2	Security Policy for Administrator	2015/07/30 22:12:30	Edit
	Division XXX	0	Security Policy for Division XXX	2015/07/30 22:13:08	Edit
	General User	0	Security Policy for General User	2015/07/30 22:13:25	Edit
	Security Policy	0		2015/07/30 22:27:26	Edit

Administrator

Security Policy for Administrator

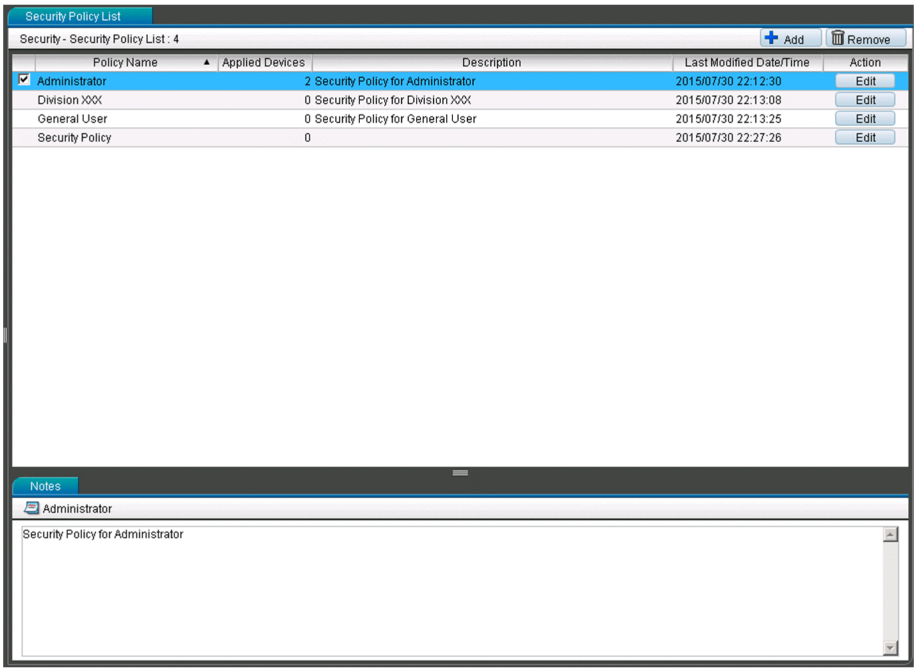
Related Topics

- *14.4.1 Security Policy List view*
- *14.4.11 Android Policy List view*
- *14.4.15 iOS Profile List view*

14.4.1 Security Policy List view

The **Security Policy List** view displays a list of created security policies. This view can also be used to add, edit, or remove security policies.

Window



Security - Security Policy List : 4

	Policy Name ▲	Applied Devices	Description	Last Modified Date/Time	Action
☑	Administrator	2	Security Policy for Administrator	2015/07/30 22:12:30	Edit
	Division XXX	0	Security Policy for Division XXX	2015/07/30 22:13:08	Edit
	General User	0	Security Policy for General User	2015/07/30 22:13:25	Edit
	Security Policy	0		2015/07/30 22:27:26	Edit

Administrator

Security Policy for Administrator

Items

The following describes the items displayed in the window.

Add button

Adds a new security policy.

Remove button

Removes the selected security policy.

Edit button (**Browse** button)

Edits the selected security policy.

If you have logged in by using an account with the view permission, the **Browse** button is displayed, which allows you to check the contents of the selected security policy.

Notes tab

The description of the selected security policy is displayed in the lower part of the information area. If you have logged in by using an account with the system administrator permission, you can edit this description.

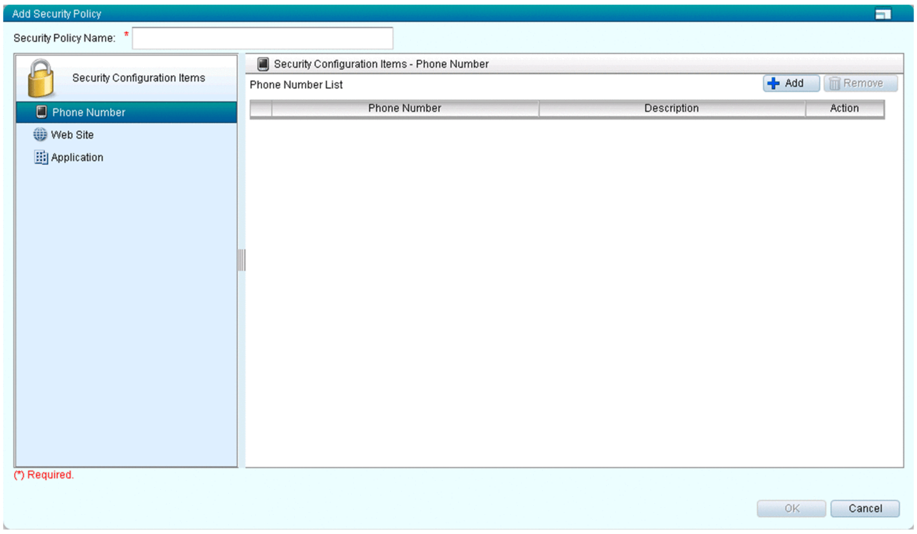
Related Topics

- *14.4.2 Add Security Policy dialog box*
- *14.4.3 Edit Security Policy dialog box*
- *14.4.4 View Security Policy dialog box*

14.4.2 Add Security Policy dialog box

The **Add Security Policy** dialog box allows you to add a new security policy.

Window



Items

The following describes the security configuration items.

Phone Number

Sets the phone numbers allowed for use. If a phone number not registered in the phone number list is used for a smart device, an event is issued to notify the administrator.

Web Site

Sets the Web sites for which browsing is allowed or prohibited. If a Web site for which browsing is prohibited is viewed on a smart device, an event is issued to notify the administrator.

Application

Allows or prohibits the use of applications. If an application for which use is prohibited is used on a smart device, an event is issued to notify the administrator.

You can specify whether installing applications for which use is allowed is required or optional. If an application that must be installed is not, an event is issued to notify the administrator.

The following describes the item and buttons displayed in the window.

Security Policy Name

Enter the name of a security policy.

Add button

Adds a security configuration item, such as a phone number.

Remove button

Removes the selected item, such as a phone number.

Edit button

Edits the selected item, such as a phone number.

Related Topics

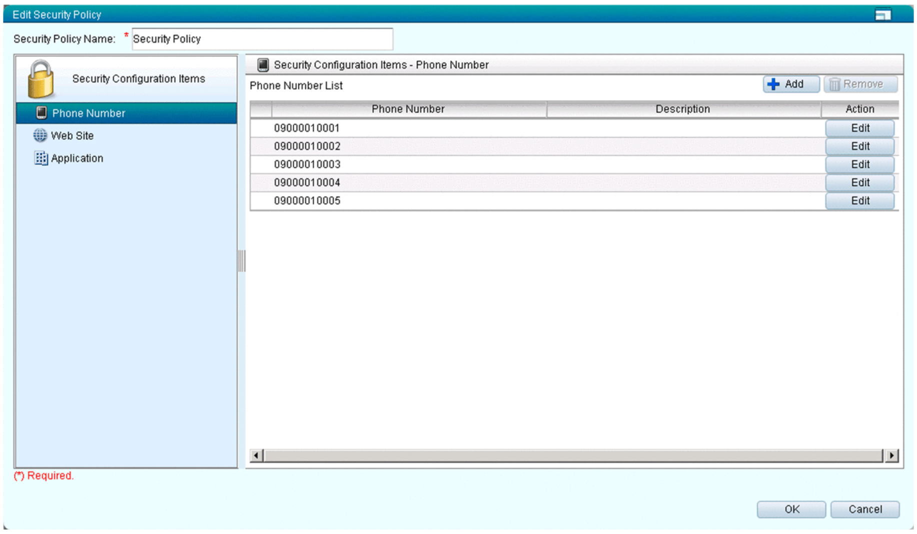
- *14.4.5 Add Phone Number dialog box*
- *14.4.6 Edit Phone Number dialog box*
- *14.4.7 Add Web Site dialog box*

- *14.4.8 Edit Web Site dialog box*
- *14.4.9 Add Application dialog box*
- *14.4.10 Edit Application dialog box*

14.4.3 Edit Security Policy dialog box

The **Edit Security Policy** dialog box allows you to edit a created security policy.

Window



Edit Security Policy

Security Policy Name: * Security Policy

Security Configuration Items

- Phone Number
- Web Site
- Application

Security Configuration Items - Phone Number

Phone Number List

Add Remove

Phone Number	Description	Action
09000010001		Edit
09000010002		Edit
09000010003		Edit
09000010004		Edit
09000010005		Edit

(*) Required.

OK Cancel

Items

The following describes the security configuration items.

Phone Number

Sets the phone numbers allowed for use. If a phone number not registered in the phone number list is used for a smart device, an event is issued to notify the administrator.

Web Site

Sets the Web sites for which browsing is allowed or prohibited. If a Web site for which browsing is prohibited is viewed on a smart device, an event is issued to notify the administrator.

Application

Allows or prohibits the use of applications. If an application for which use is prohibited is used on a smart device, an event is issued to notify the administrator.

You can specify whether installing applications for which use is allowed is required or optional. If an application that must be installed is not, an event is issued to notify the administrator.

The following describes the item and buttons displayed in the window.

Security Policy Name

Enter the name of a security policy.

Add button

Adds a security configuration item, such as a phone number.

Remove button

Removes the selected item, such as a phone number.

Edit button

Edits the selected item, such as a phone number.

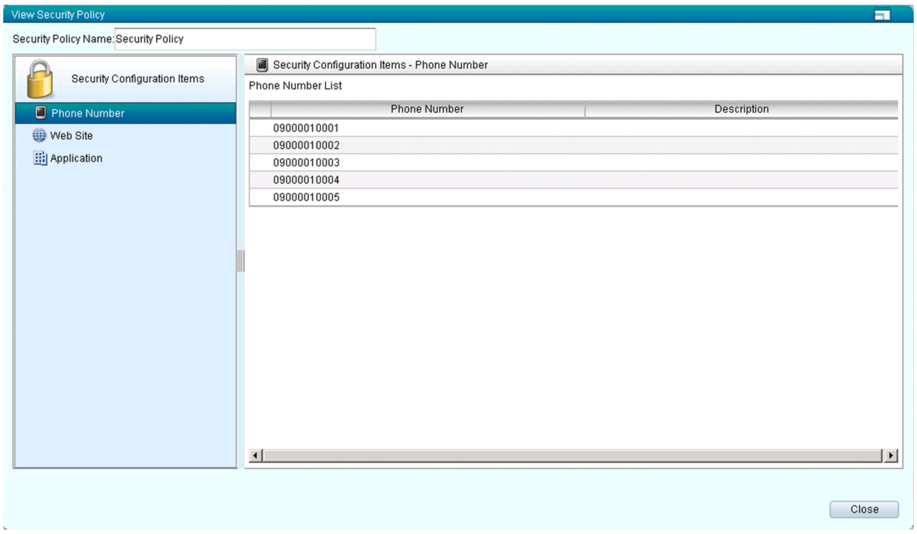
Related Topics

- *14.4.5 Add Phone Number dialog box*
- *14.4.6 Edit Phone Number dialog box*
- *14.4.7 Add Web Site dialog box*
- *14.4.8 Edit Web Site dialog box*
- *14.4.9 Add Application dialog box*
- *14.4.10 Edit Application dialog box*

14.4.4 View Security Policy dialog box

The **View Security Policy** dialog box allows you to check the contents of a security policy.

Window



View Security Policy

Security Policy Name: Security Policy

Security Configuration Items - Phone Number

Phone Number List

Phone Number	Description
09000010001	
09000010002	
09000010003	
09000010004	
09000010005	

Items

The following describes the security configuration items.

Phone Number

Displays a list of the phone numbers allowed for use. If a phone number not registered in the phone number list is used for a smart device, an event is issued to notify the administrator.

Web Site

Displays a list of the Web sites for which browsing is allowed or prohibited. If a Web site for which browsing is prohibited is viewed on a smart device, an event is issued to notify the administrator.

Application

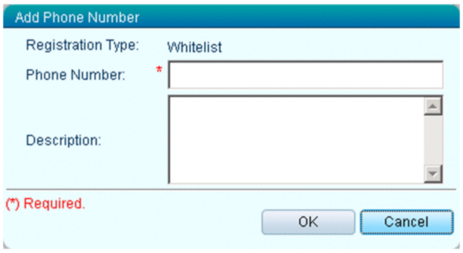
Displays a list of the applications allowed or prohibited for use. If an application for which use is prohibited is used on a smart device, an event is issued to notify the administrator.

You can specify whether installing applications for which use is allowed is required or optional. If an application that must be installed is not, an event is issued to notify the administrator.

14.4.5 Add Phone Number dialog box

The **Add Phone Number** dialog box allows you to add a phone number to which calls are allowed.

Window



Add Phone Number

Registration Type: Whitelist

Phone Number: *

Description:

(*) Required.

Items

The following describes the items displayed in the window.

Phone Number

Enter the phone number to which calls are allowed for smart devices.

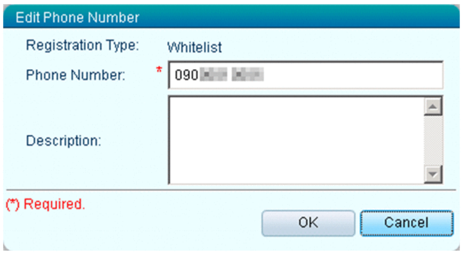
Description

Enter a description about the phone number. Enter information, such as the user name and purpose of the phone number, to make policy management easier.

14.4.6 Edit Phone Number dialog box

The **Edit Phone Number** dialog box allows you to edit a phone number to which calls are allowed.

Window



Edit Phone Number

Registration Type: Whitelist

Phone Number: * 090[redacted]

Description:

(*) Required.

Items

The following describes the items displayed in the window.

Phone Number

Edits a registered phone number.

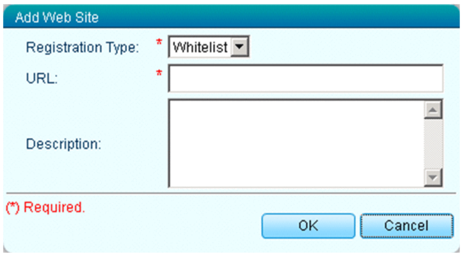
Description

Edit the description about the phone number. Enter information, such as the user name and purpose of the phone number, to make policy management easier.

14.4.7 Add Web Site dialog box

The **Add Web Site** dialog box allows you to add a Web site for which browsing is allowed or prohibited.

Window



Add Web Site

Registration Type: * Whitelist

URL: *

Description:

(*) Required.

Items

The following describes the items displayed in the window.

Registration Type

Select whether to allow or prohibit browsing of the Web site to be registered. Select **Whitelist** to allow browsing. Select **Blacklist** to prohibit browsing.

URL

Enter the URL of the Web site for which browsing is to be allowed or prohibited.

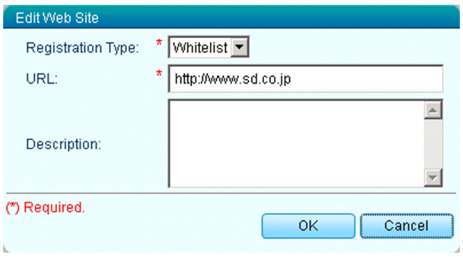
Description

Enter a description about the Web site to be registered. Enter information, such as the site name and purpose, to make policy management easier.

14.4.8 Edit Web Site dialog box

The **Edit Web Site** dialog box allows you to edit a Web site for which browsing is to be allowed or prohibited.

Window



Edit Web Site

Registration Type: * Whitelist

URL: * http://www.sd.co.jp

Description:

(*) Required.

Items

The following describes the items displayed in the window.

Registration Type

Select whether to allow or prohibit browsing of the Web site to be registered. Select **Whitelist** to allow browsing. Select **Blacklist** to prohibit browsing.

URL

Edit the URL of the Web site for which you want to allow or prohibit browsing.

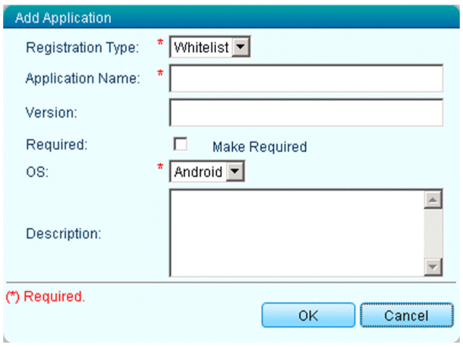
Description

Edit the description about the Web site to be registered. Enter information, such as the site name and purpose, to make policy management easier.

14.4.9 Add Application dialog box

The **Add Application** dialog box allows you to add an application for which usage is to be allowed or prohibited. You can also specify whether installation of an allowed application is required.

Window



Add Application

Registration Type: * Whitelist

Application Name: *

Version:

Required: □ Make Required

OS: * Android

Description:

(*) Required.

Items

The following describes the items displayed in the window.

Registration Type

Select whether to allow or prohibit use of the application to be registered. Select **Whitelist** to allow use of the application. Select **Blacklist** to prohibit use of the application.

Application Name

Enter the name of the application for which usage is to be allowed or prohibited.

Version

Enter the version of the application for which usage is to be allowed or prohibited.

Enter an asterisk (*) if you want to allow or prohibit all versions of the application.

Required

Specify whether installation of the allowed application is required or optional. To specify that installation is required, select the **Required** check box.

OS

Specify the OS for the application for which usage is to be allowed or prohibited.

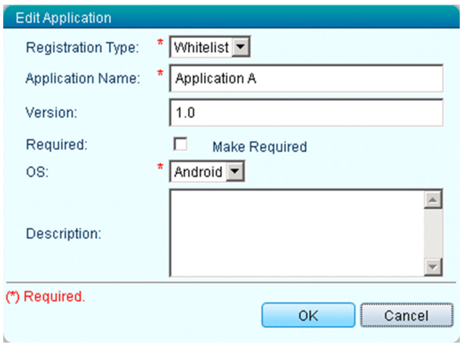
Description

Enter a description about the application to be registered. Enter information, such as the purpose of the application, to make application management easier.

14.4.10 Edit Application dialog box

The **Edit Application** dialog box allows you to edit an application for which usage is to be allowed or prohibited. You can also specify whether installation of the allowed application is required.

Window



Edit Application

Registration Type: * Whitelist

Application Name: * Application A

Version: 1.0

Required: □ Make Required

OS: * Android

Description:

(*) Required.

Items

The following describes the items displayed in the window.

Registration Type

Select whether to allow or prohibit use of the application to be registered. Select **Whitelist** to allow use of the application. Select **Blacklist** to prohibit use of the application.

Application Name

Edit the name of the application for which usage is to be allowed or prohibited.

Version

Edit the version of the application for which usage is to be allowed or prohibited.

Required

Specify whether installation of the allowed application is required or optional. To specify that installation is required, select the **Required** check box.

OS

Specify the OS for the application for which usage is to be allowed or prohibited.

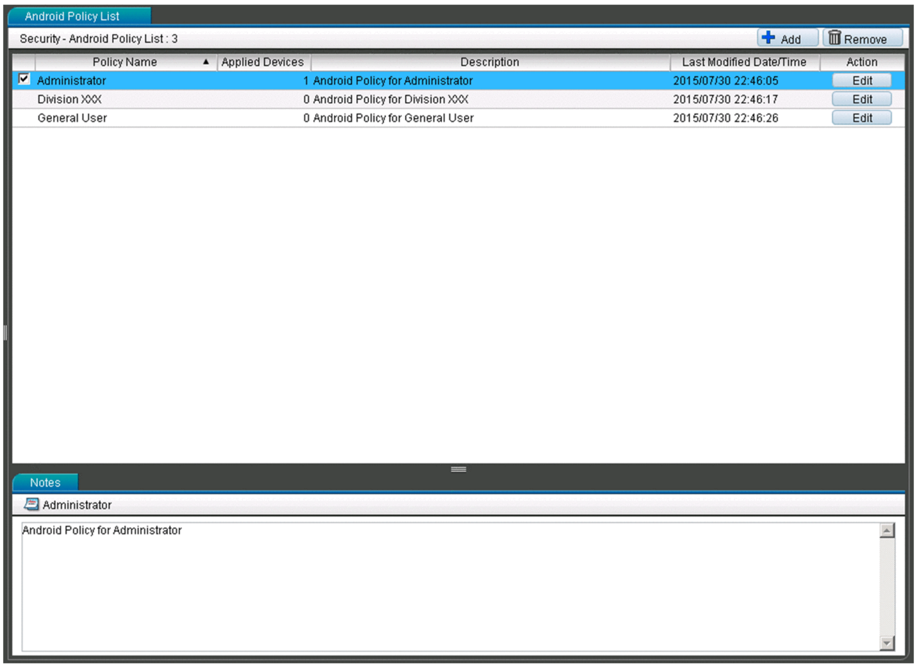
Description

Edit the description about the application to be registered. Enter information, such as the purpose of the application, to make application management easier.

14.4.11 Android Policy List view

The **Android Policy List** view displays a list of created Android policies. This view can also be used to add, edit, or remove Android policies.

Window



Security - Android Policy List : 3

	Policy Name	Applied Devices	Description	Last Modified Date/Time	Action
☑	Administrator	1	Android Policy for Administrator	2015/07/30 22:46:05	Edit
	Division XXX	0	Android Policy for Division XXX	2015/07/30 22:46:17	Edit
	General User	0	Android Policy for General User	2015/07/30 22:46:26	Edit

Administrator

Android Policy for Administrator

Items

The following describes the buttons and tab displayed in the window.

Add button

Adds a new Android policy.

Remove button

Removes the selected Android policy.

Edit button (**Browse** button)

Edits the selected Android policy.

If you have logged in by using an account with the view permission, the **Browse** button is displayed, which allows you to check the contents of the selected Android policy.

Notes tab

The description of the selected Android policy is displayed in the lower part of the information area. If you have logged in by using an account with the system administrator permission, you can edit this description.

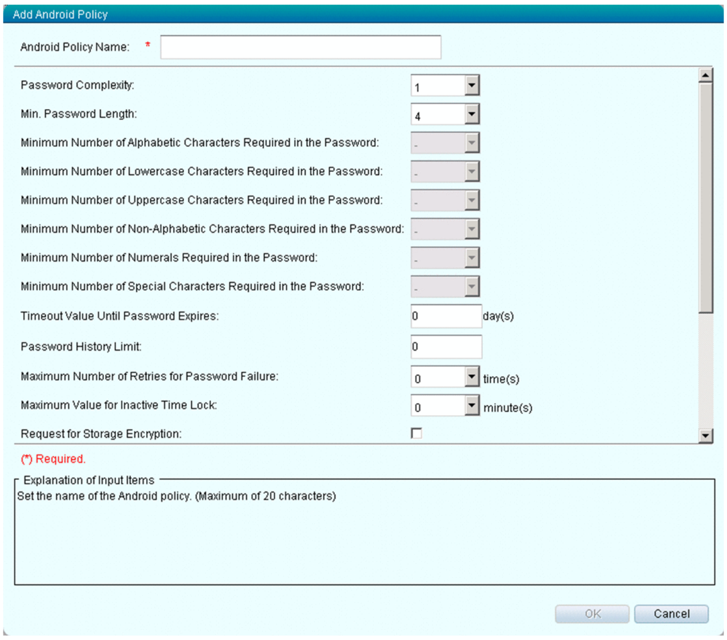
Related Topics

- *14.4.12 Add Android Policy dialog box*
- *14.4.13 Edit Android Policy dialog box*
- *14.4.14 View Android Policy dialog box*

14.4.12 Add Android Policy dialog box

The **Add Android Policy** dialog box allows you to add a new Android policy.

Window



Add Android Policy

Android Policy Name: *

Password Complexity: 1

Min. Password Length: 4

Minimum Number of Alphabetic Characters Required in the Password: -

Minimum Number of Lowercase Characters Required in the Password: -

Minimum Number of Uppercase Characters Required in the Password: -

Minimum Number of Non-Alphabetic Characters Required in the Password: -

Minimum Number of Numerals Required in the Password: -

Minimum Number of Special Characters Required in the Password: -

Timeout Value Until Password Expires: 0 day(s)

Password History Limit: 0

Maximum Number of Retries for Password Failure: 0 time(s)

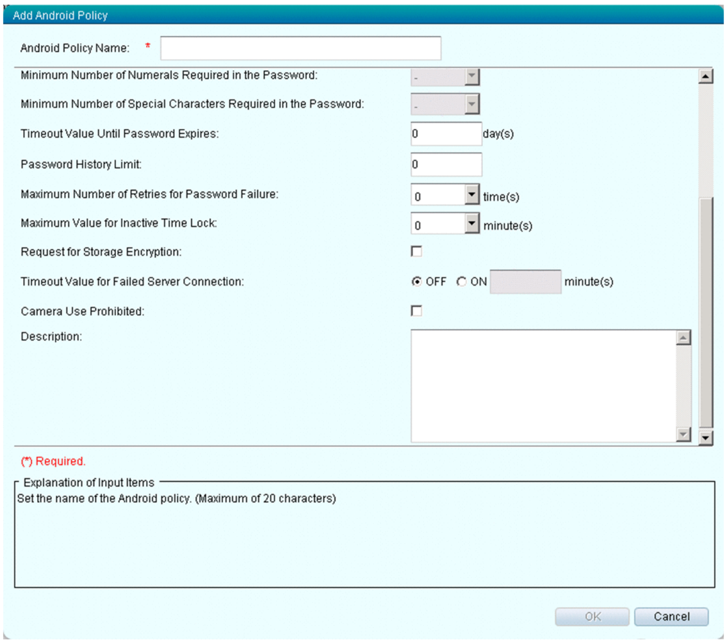
Maximum Value for Inactive Time Lock: 0 minute(s)

Request for Storage Encryption: □

(*) Required.

Explanation of Input Items

Set the name of the Android policy. (Maximum of 20 characters)



Add Android Policy

Android Policy Name: *

Minimum Number of Numerals Required in the Password: -

Minimum Number of Special Characters Required in the Password: -

Timeout Value Until Password Expires: 0 day(s)

Password History Limit: 0

Maximum Number of Retries for Password Failure: 0 time(s)

Maximum Value for Inactive Time Lock: 0 minute(s)

Request for Storage Encryption: □

Timeout Value for Failed Server Connection: ● OFF ○ ON minute(s)

Camera Use Prohibited: □

Description:

(*) Required.

Explanation of Input Items

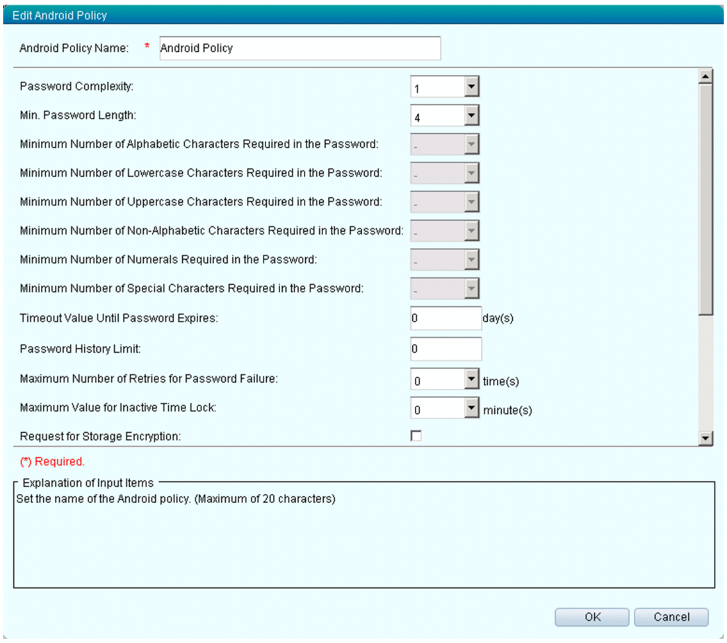
Set the name of the Android policy. (Maximum of 20 characters)

If you select an item, the description of the selected item appears in the **Description** field.

14.4.13 Edit Android Policy dialog box

The **Edit Android Policy** dialog box allows you to change a created Android policy.

Window



Edit Android Policy

Android Policy Name: * Android Policy

Password Complexity: 1

Min. Password Length: 4

Minimum Number of Alphabetic Characters Required in the Password: -

Minimum Number of Lowercase Characters Required in the Password: -

Minimum Number of Uppercase Characters Required in the Password: -

Minimum Number of Non-Alphabetic Characters Required in the Password: -

Minimum Number of Numerals Required in the Password: -

Minimum Number of Special Characters Required in the Password: -

Timeout Value Until Password Expires: 0 day(s)

Password History Limit: 0

Maximum Number of Retries for Password Failure: 0 time(s)

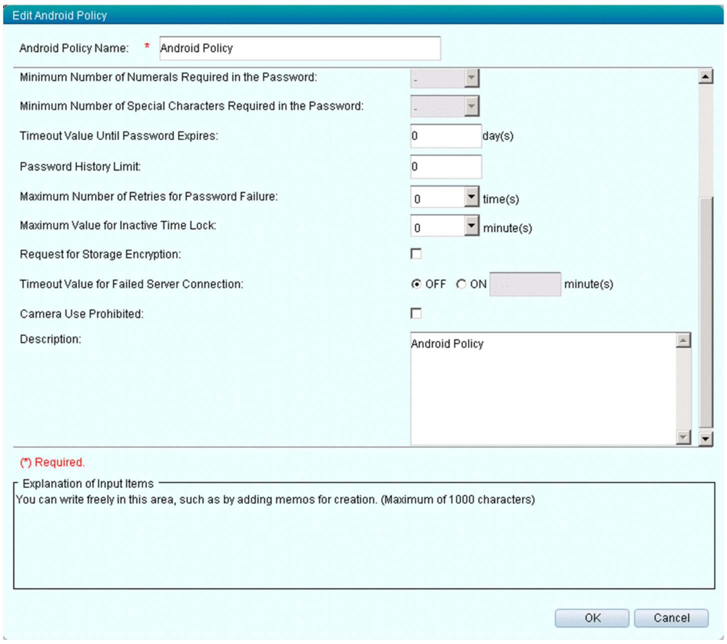
Maximum Value for Inactive Time Lock: 0 minute(s)

Request for Storage Encryption: □

(*) Required.

Explanation of Input Items

Set the name of the Android policy. (Maximum of 20 characters)



Edit Android Policy

Android Policy Name: * Android Policy

Minimum Number of Numerals Required in the Password: -

Minimum Number of Special Characters Required in the Password: -

Timeout Value Until Password Expires: 0 day(s)

Password History Limit: 0

Maximum Number of Retries for Password Failure: 0 time(s)

Maximum Value for Inactive Time Lock: 0 minute(s)

Request for Storage Encryption: □

Timeout Value for Failed Server Connection: ● OFF ○ ON minute(s)

Camera Use Prohibited: □

Description: Android Policy

(*) Required.

Explanation of Input Items

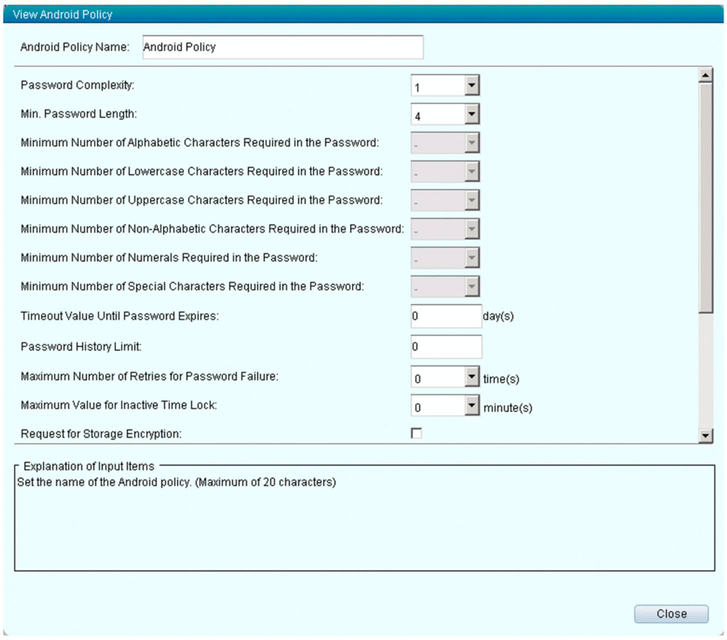
You can write freely in this area, such as by adding memos for creation. (Maximum of 1000 characters)

If you select an item, the description of the selected item appears in the **Description** field.

14.4.14 View Android Policy dialog box

The **View Android Policy** dialog box allows you to check the contents of an Android policy.

Window



View Android Policy

Android Policy Name: Android Policy

Password Complexity: 1

Min. Password Length: 4

Minimum Number of Alphabetic Characters Required in the Password: -

Minimum Number of Lowercase Characters Required in the Password: -

Minimum Number of Uppercase Characters Required in the Password: -

Minimum Number of Non-Alphabetic Characters Required in the Password: -

Minimum Number of Numerals Required in the Password: -

Minimum Number of Special Characters Required in the Password: -

Timeout Value Until Password Expires: 0 day(s)

Password History Limit: 0

Maximum Number of Retries for Password Failure: 0 time(s)

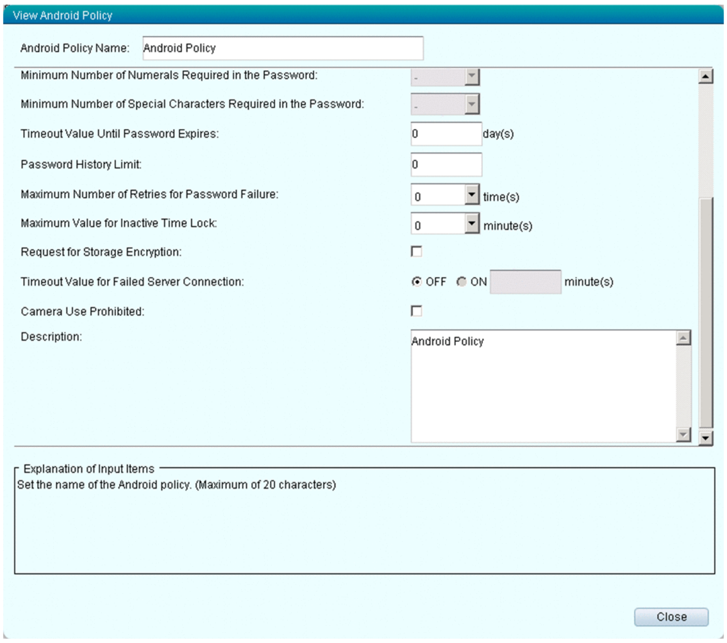
Maximum Value for Inactive Time Lock: 0 minute(s)

Request for Storage Encryption: □

Explanation of Input Items

Set the name of the Android policy. (Maximum of 20 characters)

Close



View Android Policy

Android Policy Name: Android Policy

Minimum Number of Numerals Required in the Password: -

Minimum Number of Special Characters Required in the Password: -

Timeout Value Until Password Expires: 0 day(s)

Password History Limit: 0

Maximum Number of Retries for Password Failure: 0 time(s)

Maximum Value for Inactive Time Lock: 0 minute(s)

Request for Storage Encryption: □

Timeout Value for Failed Server Connection: ● OFF ○ ON minute(s)

Camera Use Prohibited: □

Description: Android Policy

Explanation of Input Items

Set the name of the Android policy. (Maximum of 20 characters)

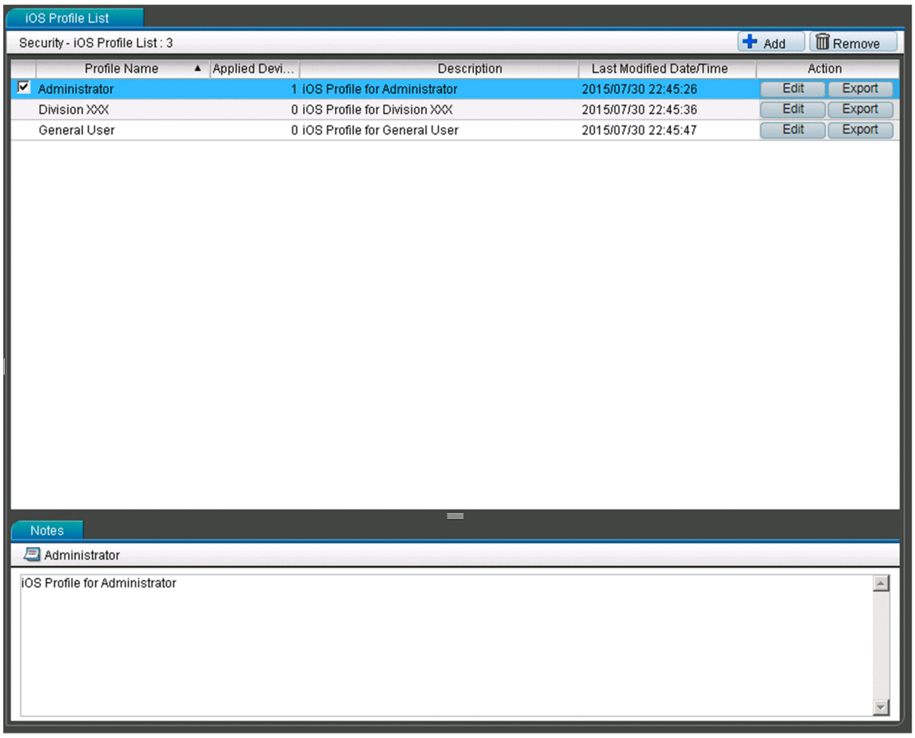
Close

If you select an item, the description of the selected item appears in the **Description** field.

14.4.15 iOS Profile List view

The **iOS Profile List** view displays a list of created iOS profiles. This view can also be used to add, edit, remove, or export iOS profiles.

Window



Security - iOS Profile List : 3

	Profile Name ▲	Applied Devi...	Description	Last Modified Date/Time	Action
☑	Administrator	1	iOS Profile for Administrator	2015/07/30 22:45:26	Edit Export
	Division XXX	0	iOS Profile for Division XXX	2015/07/30 22:45:36	Edit Export
	General User	0	iOS Profile for General User	2015/07/30 22:45:47	Edit Export

Administrator

iOS Profile for Administrator

Items

The following describes the buttons and tab displayed in the window.

Add button

Adds a new iOS profile.

Remove button

Removes the selected iOS profile.

Edit button

Edits the information of the selected iOS profile.

Export button

Exports the contents of the selected iOS profile.

Notes tab

The description of the selected iOS profile is displayed in the lower part of the information area. If you have logged in by using an account with the system administrator permission, you can edit this description.

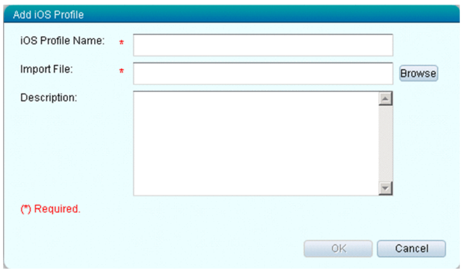
Related Topics

- *14.4.16 Add iOS Profile dialog box*
- *14.4.17 Edit iOS Profile Information dialog box*

14.4.16 Add iOS Profile dialog box

The **Add iOS Profile** dialog box allows you to load a configuration profile created by using the iPhone Configuration Utility, and then add it as an iOS profile.

Window



Items

The following describes the security configuration items.

iOS Profile Name

Enter the iOS profile name.

Import File

Click the **Browse** button, and then specify the configuration profile created by using the iPhone Configuration Utility.

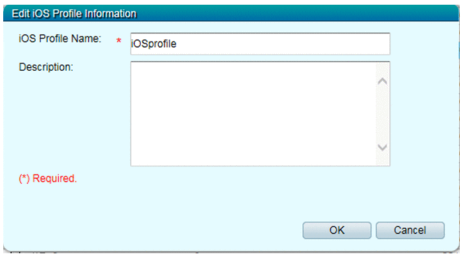
Description

Enter supplementary information for the iOS profile to be added. Enter information, such as the purpose of the iOS profile, to make iOS profile management easier.

14.4.17 Edit iOS Profile Information dialog box

The **Edit iOS profile information** dialog box allows you to edit information about the iOS profile you created.

Window



iOS Profile Name: * iOSprofile

Items

The following describes the security configuration items.

iOS Profile Name

Edit the iOS profile name.

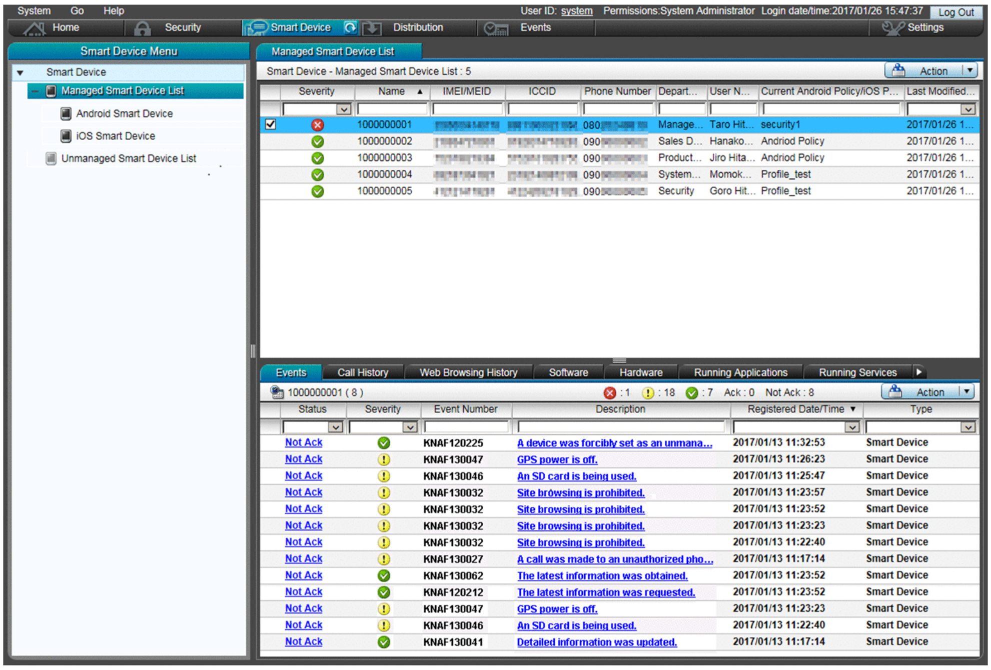
Description

Edit supplementary information about the iOS profile.

14.5 Smart Device module

In the Smart Device module, you can manage smart device information. You can also apply security rules to smart devices, and lock or initialize smart devices.

Window



Smart Device - Managed Smart Device List : 5

	Severity	Name ▲	IMEI/MEID	ICCID	Phone Number	Depart...	User N...	Current Android Policy/iOS P...	Last Modified...
☑	✖	1000000001	[redacted]	[redacted]	080[redacted]	Manage...	Taro Hit...	security1	2017/01/26 1...
	✓	1000000002	[redacted]	[redacted]	090[redacted]	Sales D...	Hanako...	Andriod Policy	2017/01/26 1...
	✓	1000000003	[redacted]	[redacted]	090[redacted]	Product...	Jiro Hita...	Andriod Policy	2017/01/26 1...
	✓	1000000004	[redacted]	[redacted]	090[redacted]	System...	Momok...	Profile_test	2017/01/26 1...
	✓	1000000005	[redacted]	[redacted]	090[redacted]	Security	Goro Hit...	Profile_test	2017/01/26 1...

1000000001 (8) ✖ : 1 ! : 18 ✓ : 7 Ack : 0 Not Ack : 8

Status	Severity	Event Number	Description	Registered Date/Time ▼	Type
Not Ack	✓	KNAF120225	A device was forcibly set as an unmana...	2017/01/13 11:32:53	Smart Device
Not Ack	!	KNAF130047	GPS power is off.	2017/01/13 11:26:23	Smart Device
Not Ack	!	KNAF130046	An SD card is being used.	2017/01/13 11:25:47	Smart Device
Not Ack	!	KNAF130032	Site browsing is prohibited.	2017/01/13 11:23:57	Smart Device
Not Ack	!	KNAF130032	Site browsing is prohibited.	2017/01/13 11:23:52	Smart Device
Not Ack	!	KNAF130032	Site browsing is prohibited.	2017/01/13 11:23:23	Smart Device
Not Ack	!	KNAF130032	Site browsing is prohibited.	2017/01/13 11:22:40	Smart Device
Not Ack	!	KNAF130027	A call was made to an unauthorized pho...	2017/01/13 11:17:14	Smart Device
Not Ack	✓	KNAF130062	The latest information was obtained.	2017/01/13 11:23:52	Smart Device
Not Ack	✓	KNAF120212	The latest information was requested.	2017/01/13 11:23:52	Smart Device
Not Ack	!	KNAF130047	GPS power is off.	2017/01/13 11:23:23	Smart Device
Not Ack	!	KNAF130046	An SD card is being used.	2017/01/13 11:22:40	Smart Device
Not Ack	✓	KNAF130041	Detailed information was updated.	2017/01/13 11:17:14	Smart Device

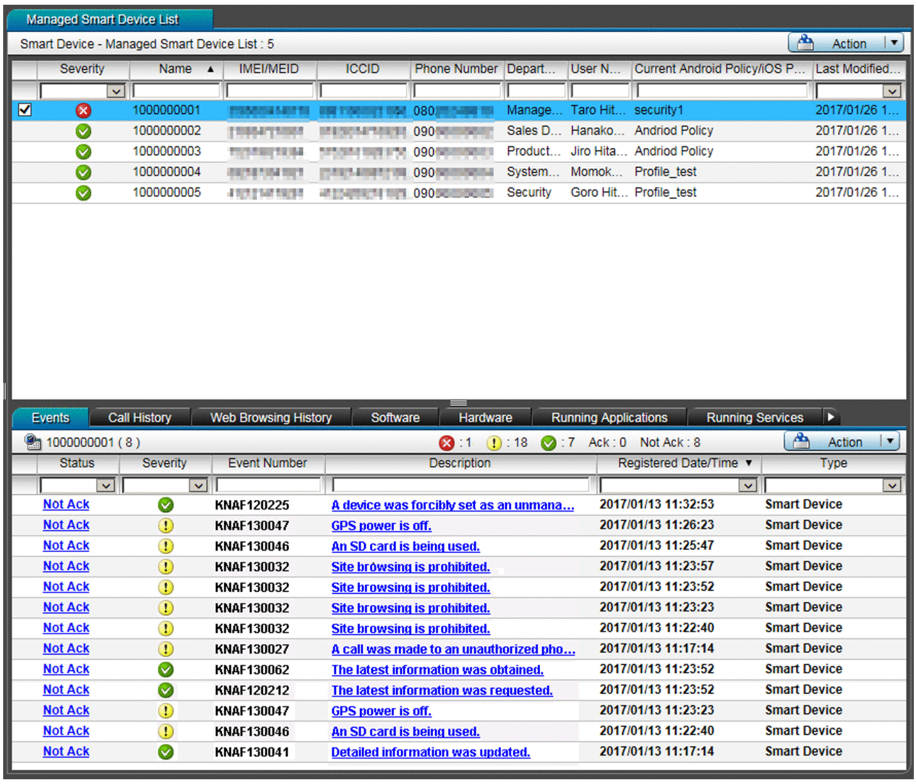
Related Topics

- *14.5.1 Managed Smart Device List view*
- *14.5.3 Unmanaged Smart Device List view*

14.5.1 Managed Smart Device List view

The **Managed Smart Device List** view displays a list of managed smart devices. You can register and remove smart devices, and apply security rules. In the menu area, you can also select **Android Smart Device** or **iOS Smart Device** to check a list of smart devices by OS.

Window



Smart Device - Managed Smart Device List : 5

	Severity	Name ▲	IMEI/MEID	ICCID	Phone Number	Depart...	User N...	Current Android Policy/iOS P...	Last Modified...
☑	☒	1000000001	[redacted]	[redacted]	080[redacted]	Manage...	Taro Hit...	security1	2017/01/26 1...
	✓	1000000002	[redacted]	[redacted]	090[redacted]	Sales D...	Hanako...	Andriod Policy	2017/01/26 1...
	✓	1000000003	[redacted]	[redacted]	090[redacted]	Product...	Jiro Hita...	Andriod Policy	2017/01/26 1...
	✓	1000000004	[redacted]	[redacted]	090[redacted]	System...	Momok...	Profile_test	2017/01/26 1...
	✓	1000000005	[redacted]	[redacted]	090[redacted]	Security	Goro Hit...	Profile_test	2017/01/26 1...

1000000001 (8) ☒ : 1 ! : 18 ✓ : 7 Ack : 0 Not Ack : 8

Status	Severity	Event Number	Description	Registered Date/Time ▼	Type
Not Ack	✓	KNAF120225	A device was forcibly set as an unmana...	2017/01/13 11:32:53	Smart Device
Not Ack	!	KNAF130047	GPS power is off.	2017/01/13 11:26:23	Smart Device
Not Ack	!	KNAF130046	An SD card is being used.	2017/01/13 11:25:47	Smart Device
Not Ack	!	KNAF130032	Site browsing is prohibited.	2017/01/13 11:23:57	Smart Device
Not Ack	!	KNAF130032	Site browsing is prohibited.	2017/01/13 11:23:52	Smart Device
Not Ack	!	KNAF130032	Site browsing is prohibited.	2017/01/13 11:23:23	Smart Device
Not Ack	!	KNAF130032	Site browsing is prohibited.	2017/01/13 11:22:40	Smart Device
Not Ack	!	KNAF130027	A call was made to an unauthorized pho...	2017/01/13 11:17:14	Smart Device
Not Ack	✓	KNAF130062	The latest information was obtained.	2017/01/13 11:23:52	Smart Device
Not Ack	✓	KNAF120212	The latest information was requested.	2017/01/13 11:23:52	Smart Device
Not Ack	!	KNAF130047	GPS power is off.	2017/01/13 11:23:23	Smart Device
Not Ack	!	KNAF130046	An SD card is being used.	2017/01/13 11:22:40	Smart Device
Not Ack	✓	KNAF130041	Detailed information was updated.	2017/01/13 11:17:14	Smart Device

> **Tip**
>
> You can use a filter to narrow down the displayed information. The data entered in the filter text box is used for prefix filtering.

Items

The following describes the **Action** menu items.

Update Device Details

Obtains the latest inventory information from the selected smart device. You can select multiple smart devices.

Initialize Smart Device

Initializes the selected smart device. You can select multiple smart devices.

Lock Smart Device

Locks the selected smart device. You can select multiple smart devices.

Reset Smart Device Passcode

Resets the passcode of the selected iOS device. You can select multiple iOS devices.

Send Notification

Sends messages to the selected Android device. You can select multiple Android devices.

Set to Unmanaged

Sets the selected smart device to **Unmanaged**. You can select multiple smart devices.

Apply Security Policy

Applies a security policy to the selected smart device. You can select multiple smart devices.

Apply Android Policy

Applies an Android policy to the selected Android device. You can select multiple Android devices.

Apply iOS Profile

Applies an iOS profile to the selected iOS device. You can select multiple iOS devices.

Remove Applied iOS Profile

Removes an iOS profile from the selected iOS device. You can select multiple iOS devices.

Add Smart Device

Registers new smart device information.

Import Smart Device List

Imports smart device information from a CSV file.

Export Smart Device List

Exports a list of smart devices displayed in the **Managed Smart Device List** view to a CSV file.

Related Topics

- *14.5.2 Tabs displayed in the Managed Smart Device List view*
- *14.5.5 Initialize Smart Device dialog box*
- *14.5.6 Lock Smart Device dialog box*
- *14.5.7 Reset Smart Device Passcode dialog box*
- *14.5.8 Set to Unmanaged dialog box*
- *14.5.9 Apply Security Policy dialog box*
- *14.5.10 Apply Android Policy dialog box*
- *14.5.11 Apply iOS Profile dialog box*
- *14.5.12 Remove Applied iOS Profile dialog box*
- *14.5.13 Add Smart Device dialog box*
- *14.5.14 Import Smart Device List dialog box*
- *14.5.15 Smart Device Message Notification dialog box*
- *H. Inventory information list*

14.5.2 Tabs displayed in the Managed Smart Device List view

On the tabs displayed in the **Managed Smart Device List** view, you can check the event list and call history for a smart device selected in the information area.

Tip

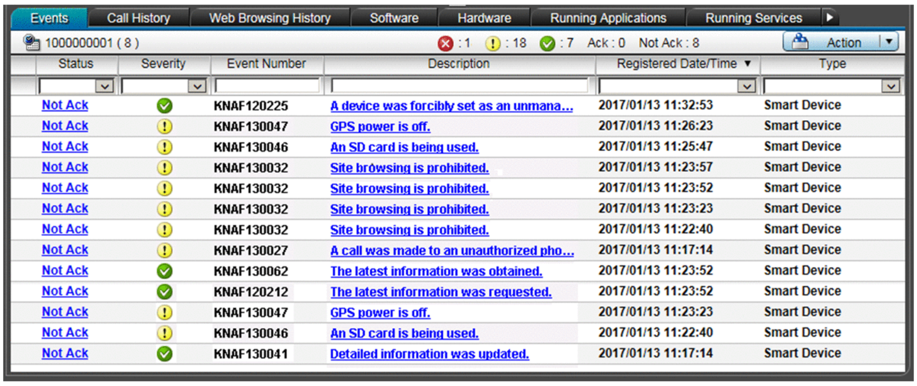
You can use a filter to narrow down the displayed information. The data entered in the filter text box is used for prefix filtering.

The following describes the tabs displayed in the window.

Events tab

Displays a list of events that occurred on the selected smart device. You can perform the following operations for events that occurred:

- Click a link displayed in the **Status** column to change the status of an event.
- Click a link displayed in the **Description** column to check details of an event.



1000000001 (8)   ✕ : 1   ! : 18   ✓ : 7   Ack : 0   Not Ack : 8

Status	Severity	Event Number	Description	Registered Date/Time ▼	Type
Not Ack	✓	KNAF120225	A device was forcibly set as an unmana...	2017/01/13 11:32:53	Smart Device
Not Ack	!	KNAF130047	GPS power is off.	2017/01/13 11:26:23	Smart Device
Not Ack	!	KNAF130046	An SD card is being used.	2017/01/13 11:25:47	Smart Device
Not Ack	!	KNAF130032	Site browsing is prohibited.	2017/01/13 11:23:57	Smart Device
Not Ack	!	KNAF130032	Site browsing is prohibited.	2017/01/13 11:23:52	Smart Device
Not Ack	!	KNAF130032	Site browsing is prohibited.	2017/01/13 11:23:23	Smart Device
Not Ack	!	KNAF130032	Site browsing is prohibited.	2017/01/13 11:22:40	Smart Device
Not Ack	!	KNAF130027	A call was made to an unauthorized pho...	2017/01/13 11:17:14	Smart Device
Not Ack	✓	KNAF130062	The latest information was obtained.	2017/01/13 11:23:52	Smart Device
Not Ack	✓	KNAF120212	The latest information was requested.	2017/01/13 11:23:52	Smart Device
Not Ack	!	KNAF130047	GPS power is off.	2017/01/13 11:23:23	Smart Device
Not Ack	!	KNAF130046	An SD card is being used.	2017/01/13 11:22:40	Smart Device
Not Ack	✓	KNAF130041	Detailed information was updated.	2017/01/13 11:17:14	Smart Device

The following describes the **Action** menu items.

Set to Confirmed

Sets the status of the selected event to **Ack**.

Set to Not Confirmed

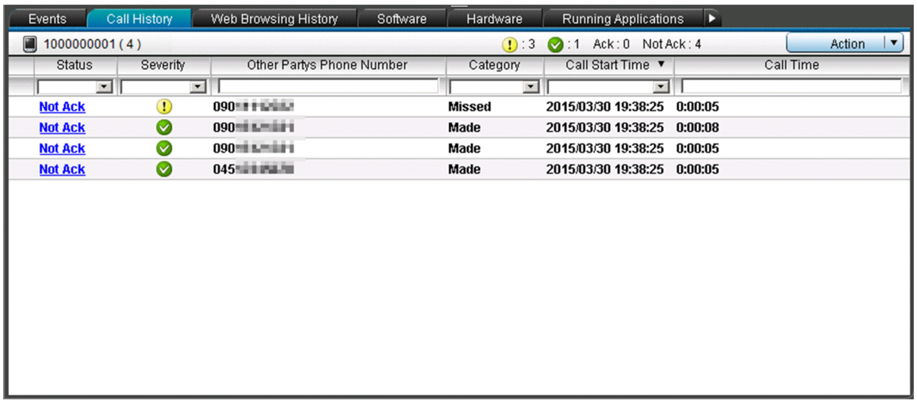
Sets the status of the selected event to **Not Ack**.

Show Details

Displays details about the selected event.

Call History tab

Displays the call history for the selected smart device. You can change the status of an entry in the history by clicking the link displayed in the **Status** column. You can also register phone numbers displayed in the history as allowed phone numbers in the security policy applied to the smart device.



1000000001 (4)   ! : 3   ✓ : 1   Ack : 0   Not Ack : 4

Status	Severity	Other Partys Phone Number	Category	Call Start Time ▼	Call Time
Not Ack	!	090[redacted]	Missed	2015/03/30 19:38:25	0:00:05
Not Ack	✓	090[redacted]	Made	2015/03/30 19:38:25	0:00:08
Not Ack	✓	090[redacted]	Made	2015/03/30 19:38:25	0:00:05
Not Ack	✓	045[redacted]	Made	2015/03/30 19:38:25	0:00:05

The following describes the **Action** menu items.

Set to Confirmed

Sets the status of the selected entry to **Ack**.

Set to Not Confirmed

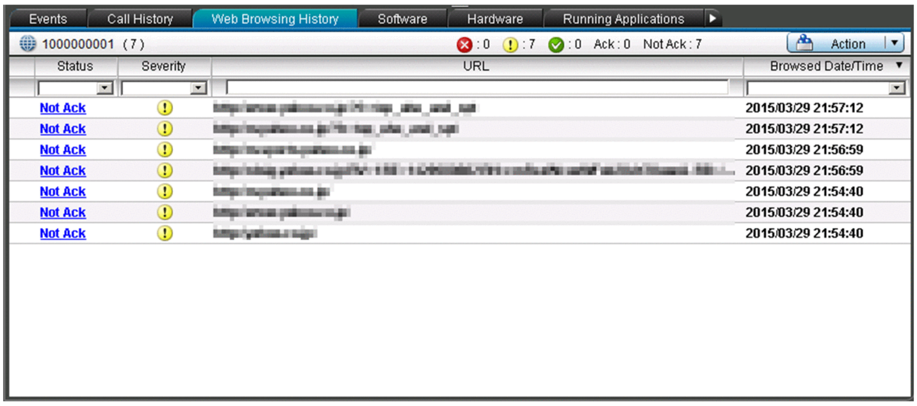
Sets the status of the selected entry to **Not Ack**.

Allow

Registers the selected phone number as an allowed phone number in the security policy applied to the smart device.

Web Browsing History tab

Displays the Web browsing history for the selected smart device. You can change the status of an entry in the history by clicking the link displayed in the **Status** column. You can also register URLs displayed in the history (as **Whitelist** or **Blacklist**) in the security policy applied to the smart device.



1000000001 (7) ✖ : 0 ! : 7 ✓ : 0 Ack : 0 Not Ack : 7

Status	Severity	URL	Browsed Date/Time
Not Ack	!	[redacted]	2015/03/29 21:57:12
Not Ack	!	[redacted]	2015/03/29 21:57:12
Not Ack	!	[redacted]	2015/03/29 21:56:59
Not Ack	!	[redacted]	2015/03/29 21:56:59
Not Ack	!	[redacted]	2015/03/29 21:54:40
Not Ack	!	[redacted]	2015/03/29 21:54:40
Not Ack	!	[redacted]	2015/03/29 21:54:40

The following describes the **Action** menu items.

Set to Confirmed

Sets the status of the selected entry to **Ack**.

Set to Not Confirmed

Sets the status of the selected entry to **Not Ack**.

Allow

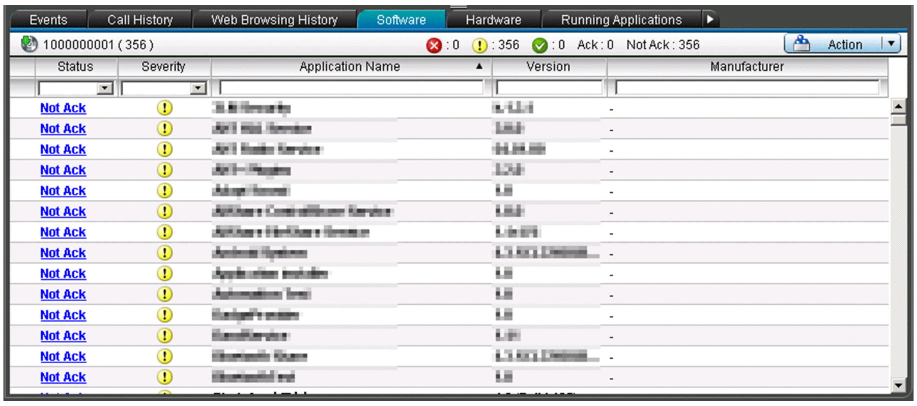
Registers the URL selected in the Web browsing history as **Whitelist** in the security policy applied to the smart device.

Prohibit

Registers the URL selected in the Web browsing history as **Blacklist** in the security policy applied to the smart device.

Software tab

Displays the applications distributed to or installed on the selected smart device. You can change the status of an application by clicking the link displayed in the **Status** column. You can also register applications displayed in the list (as **Whitelist** or **Blacklist**) to the security policy applied to the smart device.



1000000001 (356) ✖ : 0 ! : 356 ✓ : 0 Ack : 0 Not Ack : 356

Status	Severity	Application Name ▲	Version	Manufacturer
Not Ack	!	[redacted]	[redacted]	-
Not Ack	!	[redacted]	[redacted]	-
Not Ack	!	[redacted]	[redacted]	-
Not Ack	!	[redacted]	[redacted]	-
Not Ack	!	[redacted]	[redacted]	-
Not Ack	!	[redacted]	[redacted]	-
Not Ack	!	[redacted]	[redacted]	-
Not Ack	!	[redacted]	[redacted]	-
Not Ack	!	[redacted]	[redacted]	-
Not Ack	!	[redacted]	[redacted]	-
Not Ack	!	[redacted]	[redacted]	-
Not Ack	!	[redacted]	[redacted]	-
Not Ack	!	[redacted]	[redacted]	-
Not Ack	!	[redacted]	[redacted]	-

The following describes the **Action** menu items.

Set to Confirmed

Sets the status of the selected application to **Ack**.

Set to Not Confirmed

Sets the status of the selected application to **Not Ack**.

Allow

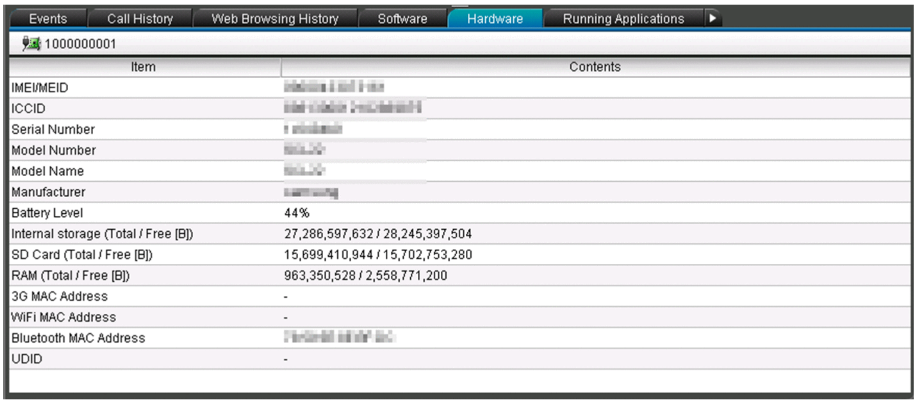
Registers the selected application as **Whitelist** in the security policy applied to the smart device.

Prohibit

Registers the selected application as **Blacklist** in the security policy applied to the smart device.

Hardware tab

Displays hardware-related information, such as the serial number and internal storage capacity, of the selected smart device.

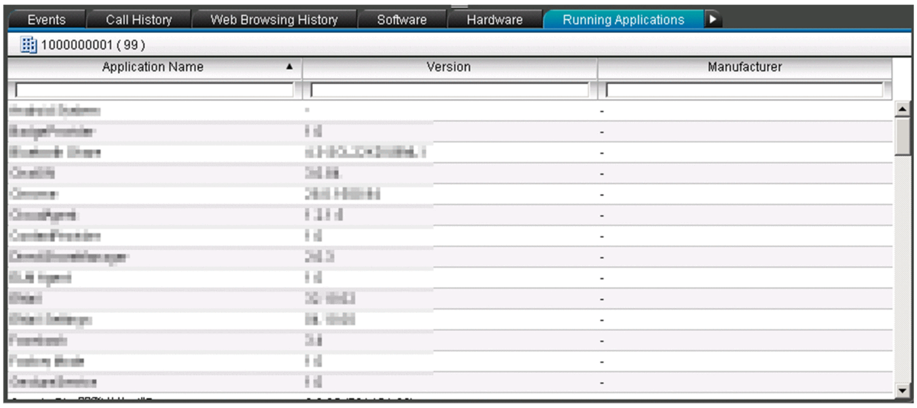


1000000001

Item	Contents
IMEI/MEID	[redacted]
ICCID	[redacted]
Serial Number	[redacted]
Model Number	[redacted]
Model Name	[redacted]
Manufacturer	[redacted]
Battery Level	44%
Internal storage (Total / Free [B])	27,286,597,632 / 28,245,397,504
SD Card (Total / Free [B])	15,699,410,944 / 15,702,753,280
RAM (Total / Free [B])	963,350,528 / 2,558,771,200
3G MAC Address	-
WiFi MAC Address	-
Bluetooth MAC Address	[redacted]
UDID	-

Running Applications tab

Displays a list of applications running on the selected smart device.

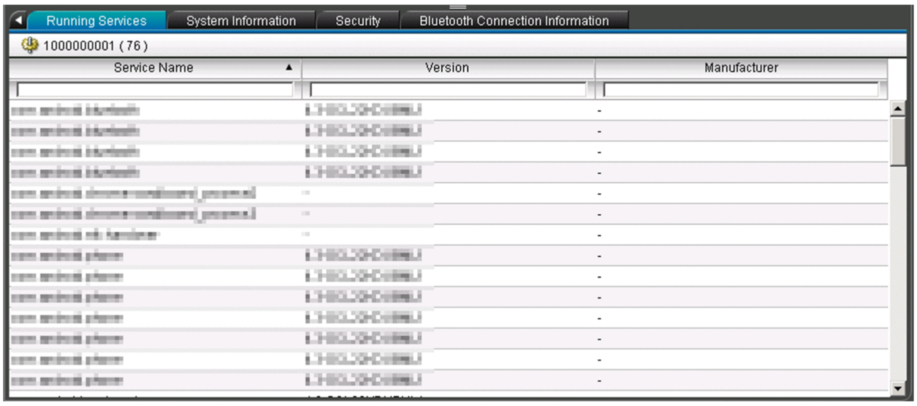


1000000001 (99)

Application Name ▲	Version	Manufacturer
[redacted]	[redacted]	-
[redacted]	[redacted]	-
[redacted]	[redacted]	-
[redacted]	[redacted]	-
[redacted]	[redacted]	-
[redacted]	[redacted]	-
[redacted]	[redacted]	-
[redacted]	[redacted]	-
[redacted]	[redacted]	-
[redacted]	[redacted]	-
[redacted]	[redacted]	-
[redacted]	[redacted]	-
[redacted]	[redacted]	-
[redacted]	[redacted]	-

Running Services tab

Displays a list of services running on the selected smart device.



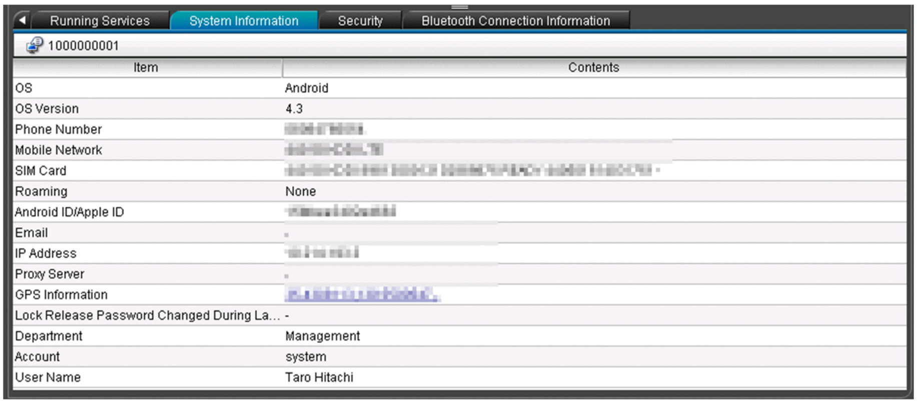
1000000001 (76)

Service Name	Version	Manufacturer
[illegible]	[illegible]	-
[illegible]	[illegible]	-
[illegible]	[illegible]	-
[illegible]	[illegible]	-
[illegible]	-	-
[illegible]	-	-
[illegible]	-	-
[illegible]	[illegible]	-
[illegible]	[illegible]	-
[illegible]	[illegible]	-
[illegible]	[illegible]	-
[illegible]	[illegible]	-
[illegible]	[illegible]	-
[illegible]	[illegible]	-

System Information tab

Displays system-related information, such as the OS information and phone number, of the selected smart device.

You can click the link for **GPS Information** to check the location of the smart device on a map site.

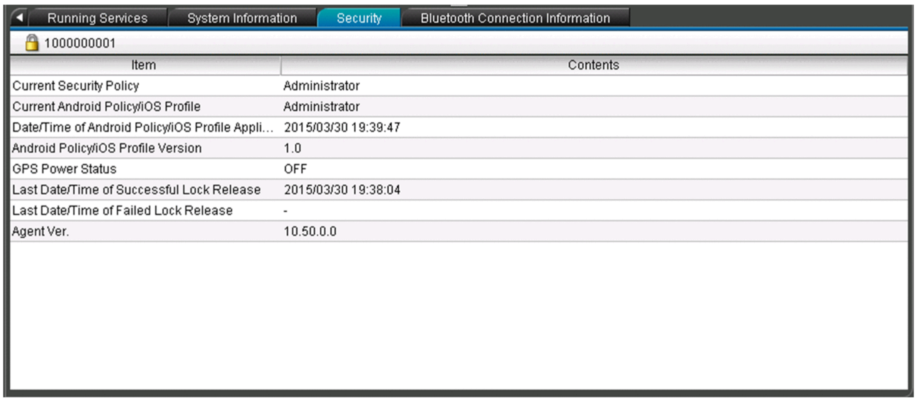


1000000001

Item	Contents
OS	Android
OS Version	4.3
Phone Number	[illegible]
Mobile Network	[illegible]
SIM Card	[illegible]
Roaming	None
Android ID/Apple ID	[illegible]
Email	-
IP Address	[illegible]
Proxy Server	-
GPS Information	[illegible]
Lock Release Password Changed During La...	-
Department	Management
Account	system
User Name	Taro Hitachi

Security tab

Displays security-related information, such as the security rules applied to the selected smart device, GPS power status, and the date and time when the smart device was locked last.

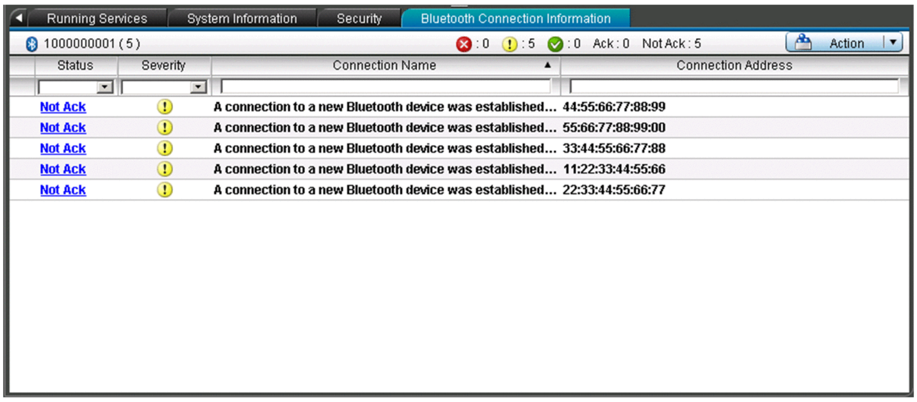


1000000001

Item	Contents
Current Security Policy	Administrator
Current Android Policy/iOS Profile	Administrator
Date/Time of Android Policy/iOS Profile Appli...	2015/03/30 19:39:47
Android Policy/iOS Profile Version	1.0
GPS Power Status	OFF
Last Date/Time of Successful Lock Release	2015/03/30 19:38:04
Last Date/Time of Failed Lock Release	-
Agent Ver.	10.50.0.0

Bluetooth Connection Information tab

Displays the Bluetooth connection history of the selected smart device. You can change the status of an entry in the connection history by clicking the link displayed in the **Status** column.


Running Services
System Information
Security
Bluetooth Connection Information
1000000001 (5)
ⓧ : 0 ⚠ : 5 ✓ : 0 Ack : 0 Not Ack : 5
Action ▼

Status	Severity	Connection Name ▲	Connection Address
Not Ack	⚠	A connection to a new Bluetooth device was established...	44:55:66:77:88:99
Not Ack	⚠	A connection to a new Bluetooth device was established...	55:66:77:88:99:00
Not Ack	⚠	A connection to a new Bluetooth device was established...	33:44:55:66:77:88
Not Ack	⚠	A connection to a new Bluetooth device was established...	11:22:33:44:55:66
Not Ack	⚠	A connection to a new Bluetooth device was established...	22:33:44:55:66:77

The following describes the **Action** menu items.

Set to Confirmed

Sets the status of the selected entry of the Bluetooth connection information to **Ack**.

Set to Not Confirmed

Sets the status of the selected entry of the Bluetooth connection information to **Not Ack**.

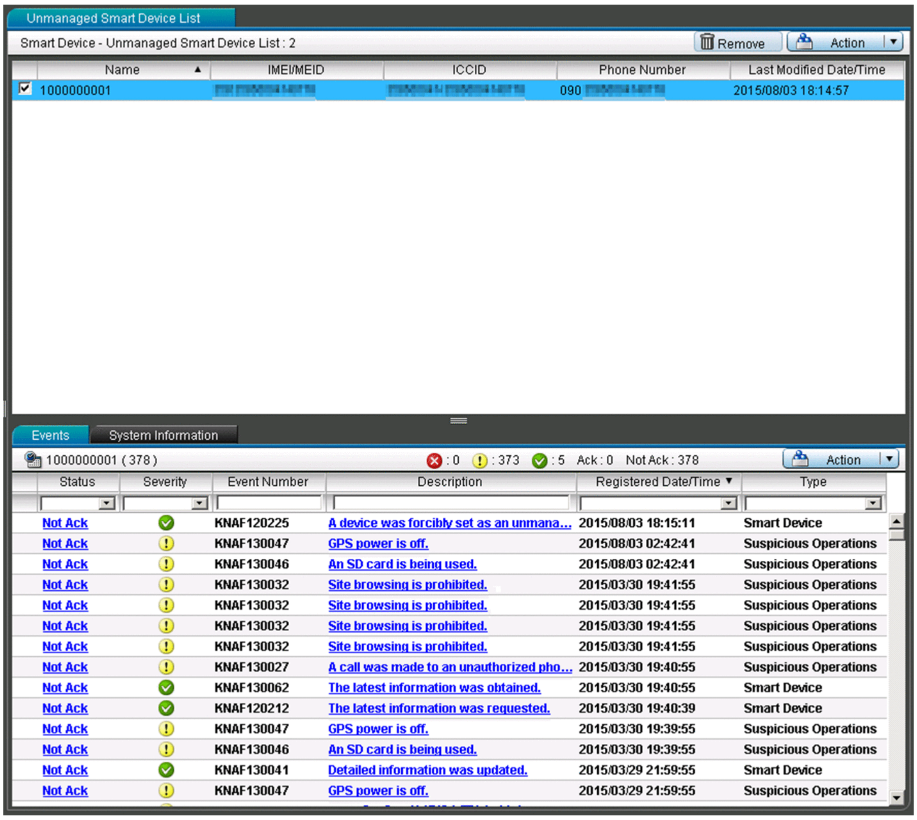
Related Topics

- *H. Inventory information list*

14.5.3 Unmanaged Smart Device List view

The **Unmanaged Smart Device List** view displays a list of unmanaged smart devices. You can remove smart devices or apply security rules to manage smart devices.

Window



Smart Device - Unmanaged Smart Device List : 2

	Name ▲	IMEI/MEID	ICCID	Phone Number	Last Modified Date/Time
☑	1000000001	[redacted]	[redacted]	090 [redacted]	2015/08/03 18:14:57

1000000001 (378) ✕ : 0 ! : 373 ✓ : 5 Ack : 0 Not Ack : 378

Status	Severity	Event Number	Description	Registered Date/Time ▼	Type
Not Ack	✓	KNAF120225	A device was forcibly set as an unmana...	2015/08/03 18:15:11	Smart Device
Not Ack	!	KNAF130047	GPS power is off.	2015/08/03 02:42:41	Suspicious Operations
Not Ack	!	KNAF130046	An SD card is being used.	2015/08/03 02:42:41	Suspicious Operations
Not Ack	!	KNAF130032	Site browsing is prohibited.	2015/03/30 19:41:55	Suspicious Operations
Not Ack	!	KNAF130032	Site browsing is prohibited.	2015/03/30 19:41:55	Suspicious Operations
Not Ack	!	KNAF130032	Site browsing is prohibited.	2015/03/30 19:41:55	Suspicious Operations
Not Ack	!	KNAF130032	Site browsing is prohibited.	2015/03/30 19:41:55	Suspicious Operations
Not Ack	!	KNAF130027	A call was made to an unauthorized pho...	2015/03/30 19:40:55	Suspicious Operations
Not Ack	✓	KNAF130062	The latest information was obtained.	2015/03/30 19:40:55	Smart Device
Not Ack	✓	KNAF120212	The latest information was requested.	2015/03/30 19:40:39	Smart Device
Not Ack	!	KNAF130047	GPS power is off.	2015/03/30 19:39:55	Suspicious Operations
Not Ack	!	KNAF130046	An SD card is being used.	2015/03/30 19:39:55	Suspicious Operations
Not Ack	✓	KNAF130041	Detailed information was updated.	2015/03/29 21:59:55	Smart Device
Not Ack	!	KNAF130047	GPS power is off.	2015/03/29 21:59:55	Suspicious Operations

Tip

You can use a filter to narrow down the displayed information. The data entered in the filter text box is used for prefix filtering.

Items

The following describes the button displayed in the window.

Remove button

Removes the selected smart device from JP1/ITDM2 - SDM.

The following describes the **Action** menu items.

Apply Security Policy

Applies a security policy to the selected smart device. You can select multiple smart devices.

Apply Android Policy

Applies an Android policy to the selected Android device. You can select multiple Android devices.

Apply iOS Profile

Applies an iOS profile to the selected iOS device. You can select multiple iOS devices.

Related Topics

- *14.5.4 Tabs displayed in the Unmanaged Smart Device List view*
- *14.5.9 Apply Security Policy dialog box*
- *14.5.10 Apply Android Policy dialog box*

- *14.5.11 Apply iOS Profile dialog box*
- *H. Inventory information list*

14.5.4 Tabs displayed in the Unmanaged Smart Device List view

On the tabs displayed in the **Unmanaged Smart Device List** view, you can check the event list and system information for the smart device selected in the information area.

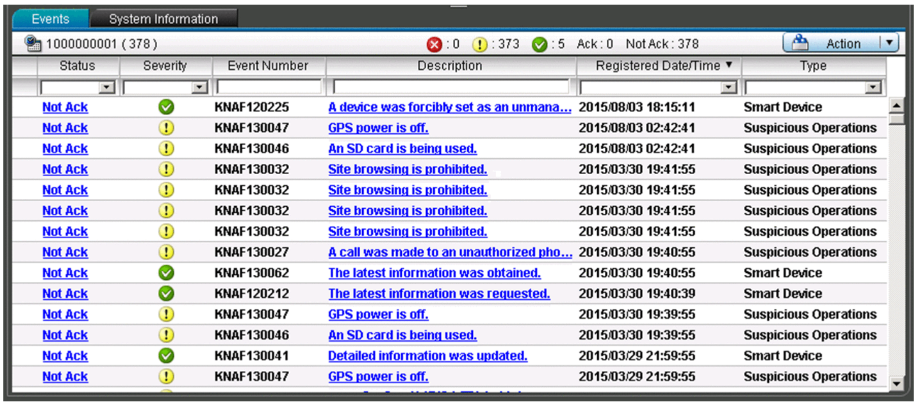
Tip

You can use a filter to narrow down the displayed information. The data entered in the filter text box is used for prefix filtering.

The following describes the tabs displayed in the window.

Events tab

Displays a list of events that occurred on the selected smart device. You can change the status of an event by clicking the link displayed in the **Status** column.



Status	Severity	Event Number	Description	Registered Date/Time ▼	Type
Not Ack	✓	KNAF120225	A device was forcibly set as an unmana...	2015/08/03 18:15:11	Smart Device
Not Ack	!	KNAF130047	GPS power is off.	2015/08/03 02:42:41	Suspicious Operations
Not Ack	!	KNAF130046	An SD card is being used.	2015/08/03 02:42:41	Suspicious Operations
Not Ack	!	KNAF130032	Site browsing is prohibited.	2015/03/30 19:41:55	Suspicious Operations
Not Ack	!	KNAF130032	Site browsing is prohibited.	2015/03/30 19:41:55	Suspicious Operations
Not Ack	!	KNAF130032	Site browsing is prohibited.	2015/03/30 19:41:55	Suspicious Operations
Not Ack	!	KNAF130032	Site browsing is prohibited.	2015/03/30 19:41:55	Suspicious Operations
Not Ack	!	KNAF130027	A call was made to an unauthorized pho...	2015/03/30 19:40:55	Suspicious Operations
Not Ack	✓	KNAF130062	The latest information was obtained.	2015/03/30 19:40:55	Smart Device
Not Ack	✓	KNAF120212	The latest information was requested.	2015/03/30 19:40:39	Smart Device
Not Ack	!	KNAF130047	GPS power is off.	2015/03/30 19:39:55	Suspicious Operations
Not Ack	!	KNAF130046	An SD card is being used.	2015/03/30 19:39:55	Suspicious Operations
Not Ack	✓	KNAF130041	Detailed information was updated.	2015/03/29 21:59:55	Smart Device
Not Ack	!	KNAF130047	GPS power is off.	2015/03/29 21:59:55	Suspicious Operations

The following describes the **Action** menu items.

Set to Confirmed

Sets the status of the selected event to **Ack**.

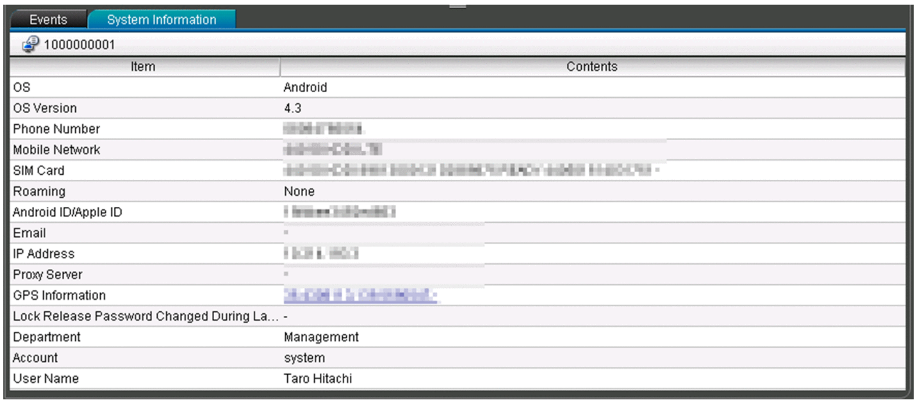
Set to Not Confirmed

Sets the status of the selected event to **Not Ack**.

System Information tab

Displays system-related information, such as the OS information and phone number, of the selected smart device.

You can click the link for **GPS Information** to check the location of the smart device on a map site.



1000000001

Item	Contents
OS	Android
OS Version	4.3
Phone Number	[redacted]
Mobile Network	[redacted]
SIM Card	[redacted]
Roaming	None
Android ID/Apple ID	[redacted]
Email	-
IP Address	[redacted]
Proxy Server	-
GPS Information	[redacted]
Lock Release Password Changed During La...	-
Department	Management
Account	system
User Name	Taro Hitachi

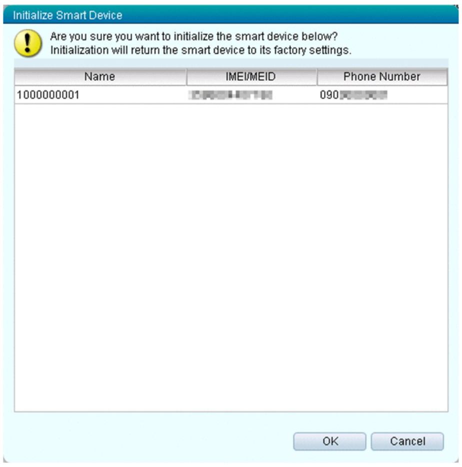
Related Topics

- *H. Inventory information list*

14.5.5 Initialize Smart Device dialog box

The **Initialize Smart Device** dialog box allows you to initialize the displayed smart device to the factory default settings.

Window



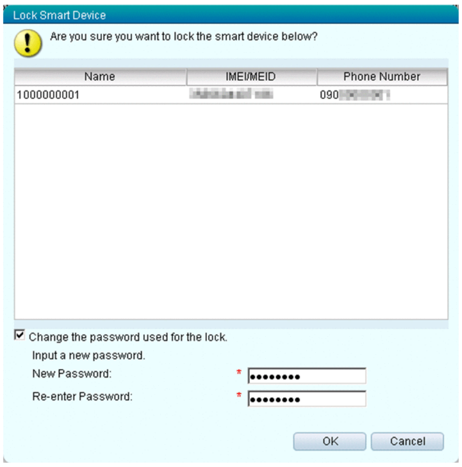
Are you sure you want to initialize the smart device below?
Initialization will return the smart device to its factory settings.

Name	IMEI/MEID	Phone Number
1000000001	[redacted]	090[redacted]

14.5.6 Lock Smart Device dialog box

The **Lock Smart Device** dialog box allows you to lock the displayed smart device. For Android devices, you can also change the password.

Window



Lock Smart Device

Are you sure you want to lock the smart device below?

Name	IMEI/MEID	Phone Number
1000000001	[redacted]	090[redacted]

☑ Change the password used for the lock.

Input a new password.

New Password: * ••••••••

Re-enter Password: * ••••••••

Items

The following describes the items displayed in the window.

Change the password used for the lock.

Select this check box if you want to change the password when locking an Android device. If this check box is selected, data can be entered for **New Password** and **Re-enter Password**.

> **Important**
>
> For iOS devices, the password does not change, even if you select the check box **Change the password used for the lock.**, and then enter a password.

New Password

Enter a new password.

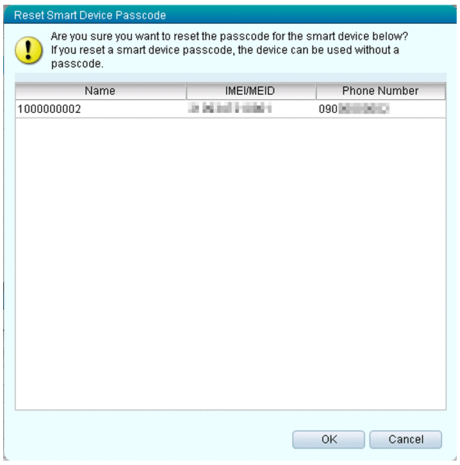
Re-enter Password

Re-enter the password for confirmation.

14.5.7 Reset Smart Device Passcode dialog box

The **Reset Smart Device Passcode** dialog box allows you to reset the passcode of the displayed iOS device.

Window



Reset Smart Device Passcode

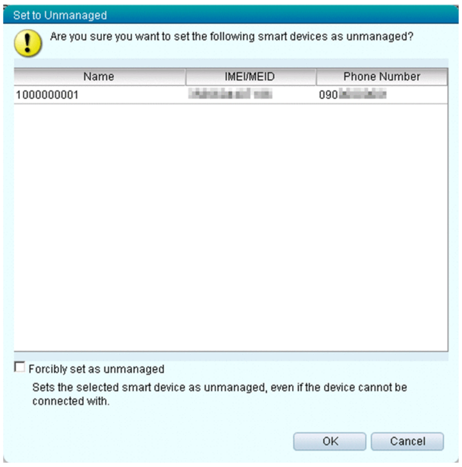
Are you sure you want to reset the passcode for the smart device below? If you reset a smart device passcode, the device can be used without a passcode.

Name	IMEI/MEID	Phone Number
1000000002	[redacted]	090[redacted]

14.5.8 Set to Unmanaged dialog box

The **Set to Unmanaged** dialog box allows you to cancel the security rules applied to the displayed smart device, and set the device to **Unmanaged**.

Window



Set to Unmanaged

Are you sure you want to set the following smart devices as unmanaged?

Name	IMEI/MEID	Phone Number
1000000001	[redacted]	090[redacted]

□ Forcibly set as unmanaged

Sets the selected smart device as unmanaged, even if the device cannot be connected with.

Items

The following describes the items displayed in the window.

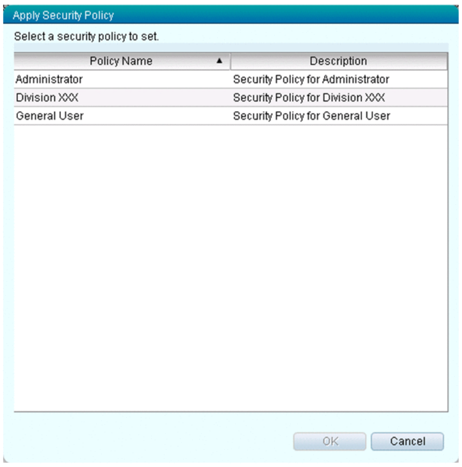
Forcibly set as unmanaged

Select this check box if you want to forcibly set the smart device to **Unmanaged**, even if it cannot be connected.

14.5.9 Apply Security Policy dialog box

The **Apply Security Policy** dialog box allows you to apply a security policy to smart devices.

Window



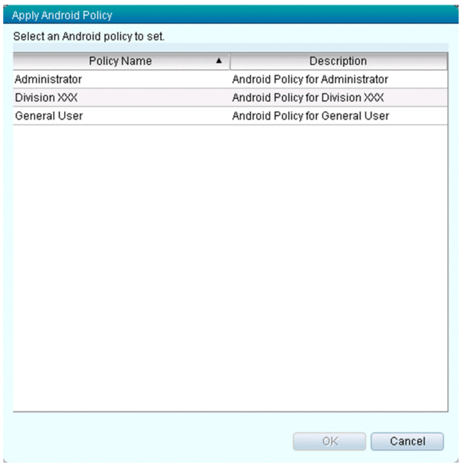
Select a security policy to set.

Policy Name ▲	Description
Administrator	Security Policy for Administrator
Division XXX	Security Policy for Division XXX
General User	Security Policy for General User

14.5.10 Apply Android Policy dialog box

The **Apply Android Policy** dialog box allows you to apply an Android policy to Android devices.

Window



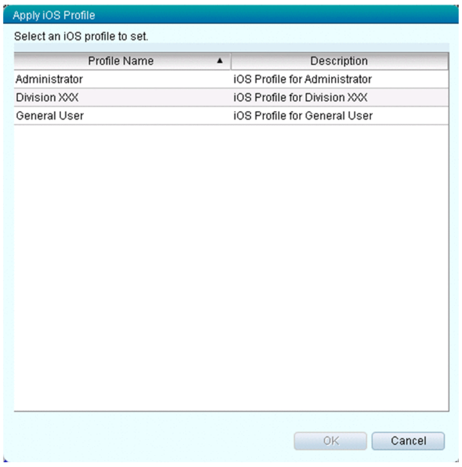
Select an Android policy to set.

Policy Name ▲	Description
Administrator	Android Policy for Administrator
Division XXX	Android Policy for Division XXX
General User	Android Policy for General User

14.5.11 Apply iOS Profile dialog box

The **Apply iOS Profile** dialog box allows you to apply an iOS profile to iOS devices.

Window



Apply iOS Profile

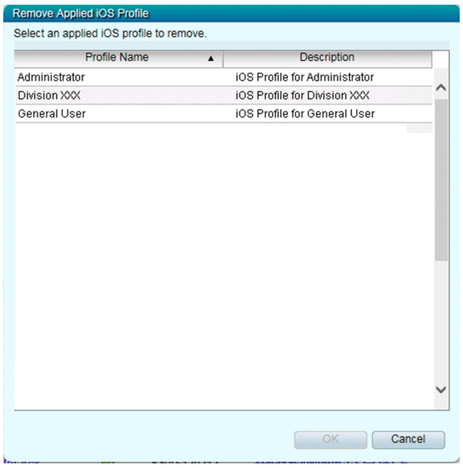
Select an iOS profile to set.

Profile Name	Description
Administrator	iOS Profile for Administrator
Division XXX	iOS Profile for Division XXX
General User	iOS Profile for General User

14.5.12 Remove Applied iOS Profile dialog box

In the Remove Applied iOS Profile dialog box, you can remove iOS profiles applied to iOS devices.

Window



Remove Applied iOS Profile

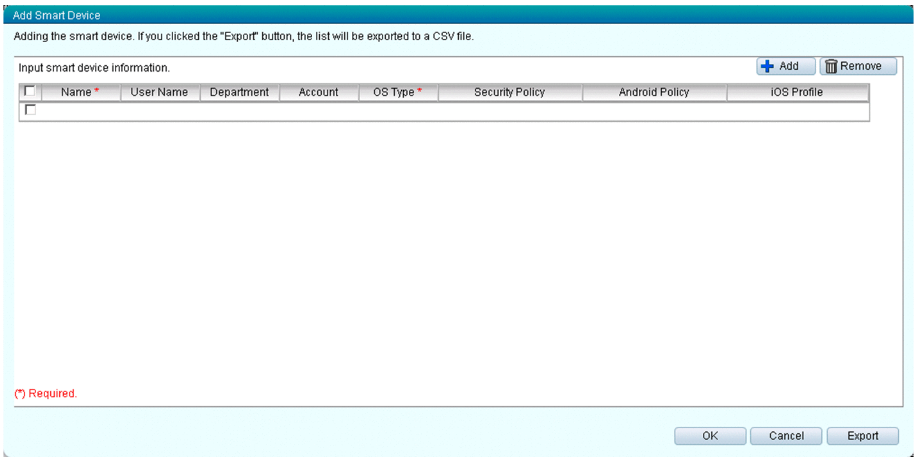
Select an applied iOS profile to remove.

Profile Name	Description
Administrator	iOS Profile for Administrator
Division XXX	iOS Profile for Division XXX
General User	iOS Profile for General User

14.5.13 Add Smart Device dialog box

The **Add Smart Device** dialog box allows you to add smart devices to be managed in JP1/ITDM2 - SDM.

Window



Add Smart Device

Adding the smart device. If you clicked the "Export" button, the list will be exported to a CSV file.

Input smart device information.

□	Name *	User Name	Department	Account	OS Type *	Security Policy	Android Policy	iOS Profile
□								

(*) Required.

Items

The following describes the buttons displayed in the window.

Add button

Adds a line in which you can enter smart device information.

Remove button

Removes the selected line. You can select multiple lines.

Export button

Outputs the entered information to a CSV file.

The following describes the items for smart device information.

Name

Enter a name, such as an asset management number.

User Name

Enter the user name.

Department

Enter the department to which the user belongs.

Account

Enter information, such as an employee ID and email address.

OS Type

Select the OS type.

Security Policy

Select the security policy to be applied.

Android Policy

Select the Android policy to be applied.

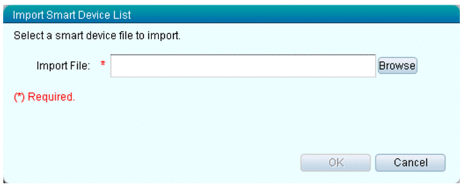
iOS Profile

Select the iOS profile to be applied.

14.5.14 Import Smart Device List dialog box

The **Import Smart Device List** dialog box allows you to import a CSV file containing information about multiple smart devices to register them as a batch in JP1/ITDM2 - SDM.

Window



Import Smart Device List

Select a smart device file to import.

Import File: *

(*) Required.

Items

The following describes the items displayed in the window.

Import File

Click the **Browse** button, and then specify a CSV file containing smart device information.

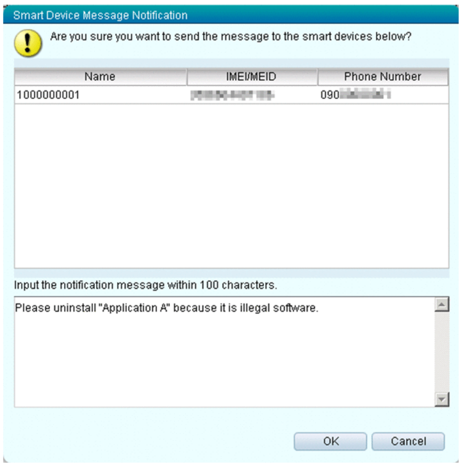
Related Topics

- *E. Output Format of Imported and Exported Files*

14.5.15 Smart Device Message Notification dialog box

The **Smart Device Message Notification** dialog box allows you to send a message to the displayed Android device.

Window



Smart Device Message Notification

Are you sure you want to send the message to the smart devices below?

Name	IMEI/MEID	Phone Number
1000000001	[redacted]	090[redacted]

Input the notification message within 100 characters.

Please uninstall "Application A" because it is illegal software.

Items

The following describes the items displayed in the window.

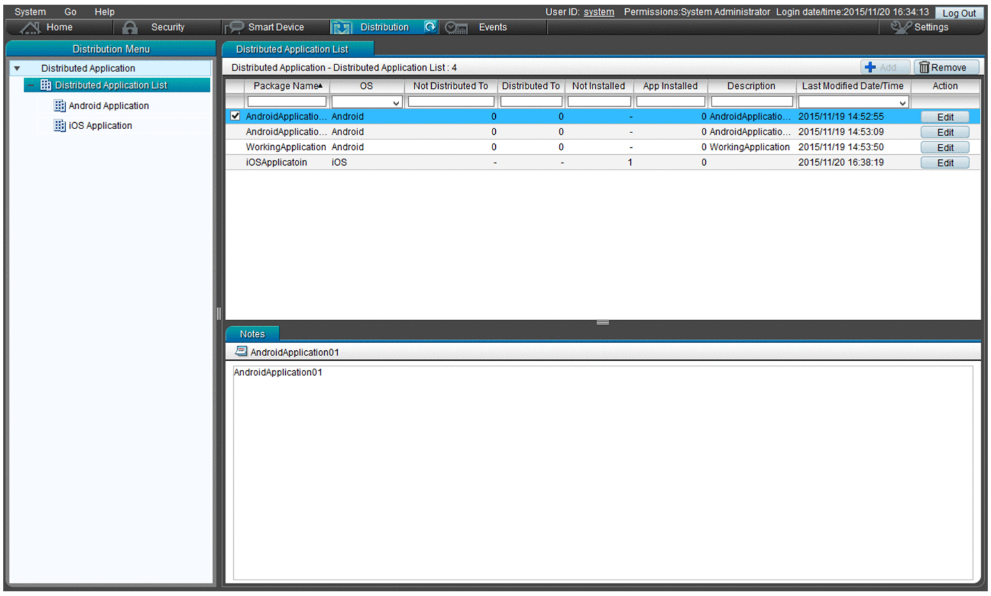
Input the notification message within 100 characters.

Enter the message you want to send to the Android device.

14.6 Distribution module

In the Distribution module, you can manage applications to be distributed by JP1/ITDM2 - SDM. You can also add applications to be distributed, and instruct installation.

Window



Distributed Application - Distributed Application List : 4

	Package Name▲	OS	Not Distributed To	Distributed To	Not Installed	App Installed	Description	Last Modified Date/Time	Action
☑	AndroidApplicatio...	Android	0	0	-	0	AndroidApplicatio...	2015/11/19 14:52:55	Edit
	AndroidApplicatio...	Android	0	0	-	0	AndroidApplicatio...	2015/11/19 14:53:09	Edit
	WorkingApplication	Android	0	0	-	0	WorkingApplication	2015/11/19 14:53:50	Edit
	iOSApplicatoin	iOS	-	-	1	0		2015/11/20 16:38:19	Edit

AndroidApplication01

AndroidApplication01

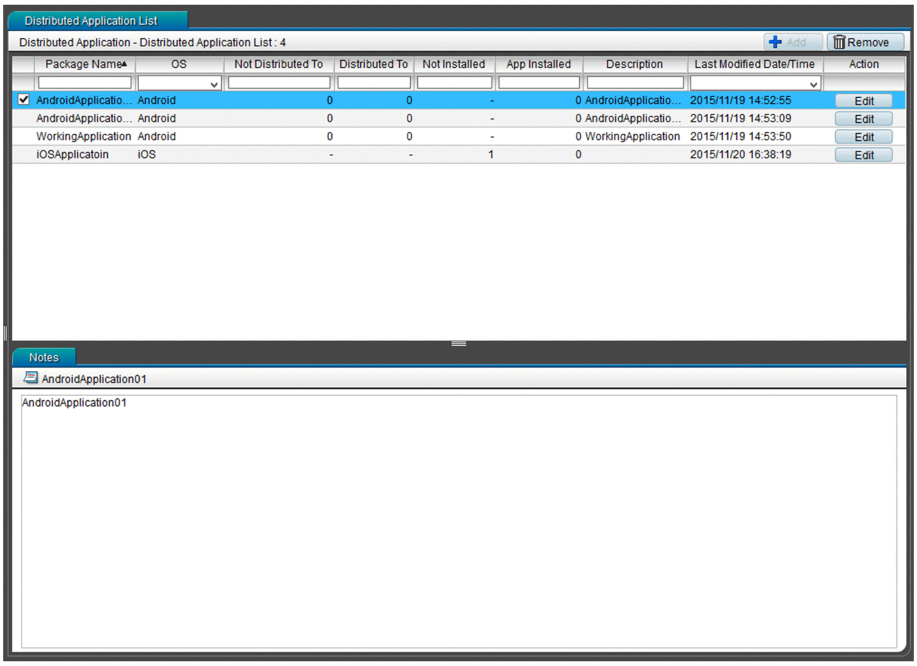
Related Topics

- *14.6.1 Distributed Application List view*
- *14.6.2 Android Application view*
- *14.6.4 iOS Application view*

14.6.1 Distributed Application List view

The **Distributed Application List** view displays a list of registered applications. This view can also be used to edit or remove applications.

Window



Distributed Application - Distributed Application List : 4

	Package Name	OS	Not Distributed To	Distributed To	Not Installed	App Installed	Description	Last Modified Date/Time	Action
☑	AndroidApplicatio...	Android	0	0	-	0	AndroidApplicatio...	2015/11/19 14:52:55	Edit
	AndroidApplicatio...	Android	0	0	-	0	AndroidApplicatio...	2015/11/19 14:53:09	Edit
	WorkingApplication	Android	0	0	-	0	WorkingApplication	2015/11/19 14:53:50	Edit
	iOSApplicatoin	iOS	-	-	1	0		2015/11/20 16:38:19	Edit

AndroidApplication01

AndroidApplication01

Tip

You can use a filter to narrow down the displayed information. The data entered in the filter text box is used for prefix filtering.

Items

The following describes the buttons and tab displayed in the window.

Remove button

Removes the selected application.

Edit button (**Browse** button)

Edits the selected application.

If you have logged in by using an account with the view permission, the **Browse** button is displayed, which allows you to check the contents of the selected application.

Notes tab

The description of the selected application is displayed in the lower part of the information area. If you have logged in by using an account with the system administrator permission, you can edit this description.

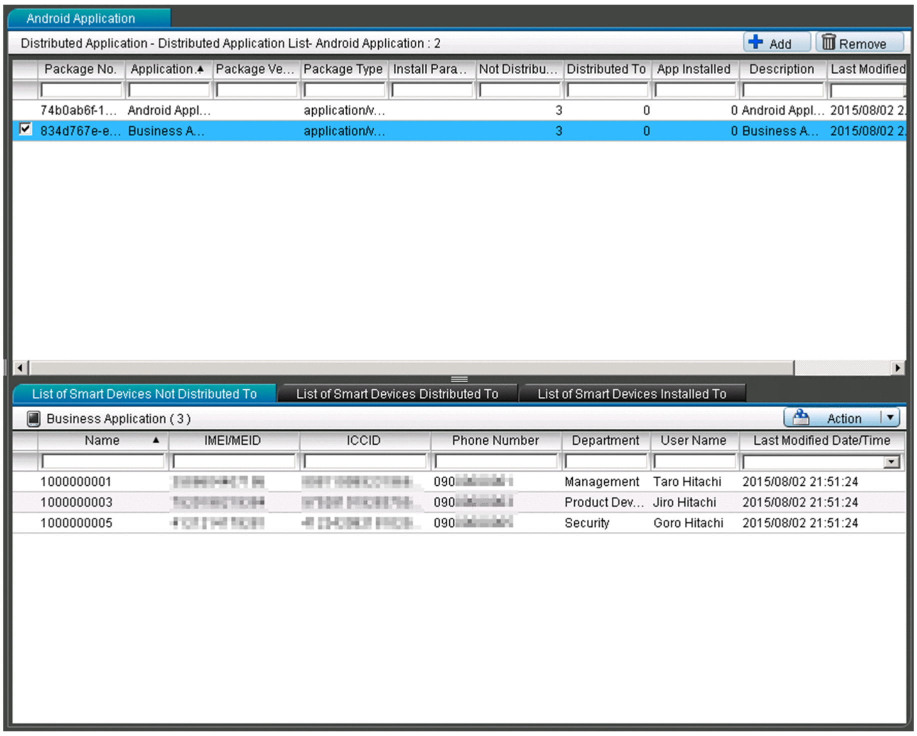
Related Topics

- *14.6.7 Edit Android Application dialog box*
- *14.6.8 View Android Application dialog box*
- *14.6.10 Edit iOS Application dialog box*
- *14.6.11 View iOS Application dialog box*

14.6.2 Android Application view

The **Android Application** view displays a list of registered Android applications. This view can also be used to add, edit, or remove applications.

Window



Android Application
Add
Remove
List of Smart Devices Not Distributed To
List of Smart Devices Distributed To
List of Smart Devices Installed To
Action

Distributed Application - Distributed Application List- Android Application : 2

	Package No.	Application ▲	Package Ve…	Package Type	Install Para…	Not Distribu…	Distributed To	App Installed	Description	Last Modified
	74b0ab6f-1…	Android Appl…		application/v…		3	0	0	Android Appl…	2015/08/02 2…
☑	834d767e-e…	Business A…		application/v…		3	0	0	Business A…	2015/08/02 2…

Business Application (3)

Name ▲	IMEI/MEID	ICCID	Phone Number	Department	User Name	Last Modified Date/Time
1000000001	[redacted]	[redacted]	090[redacted]	Management	Taro Hitachi	2015/08/02 21:51:24
1000000003	[redacted]	[redacted]	090[redacted]	Product Dev…	Jiro Hitachi	2015/08/02 21:51:24
1000000005	[redacted]	[redacted]	090[redacted]	Security	Goro Hitachi	2015/08/02 21:51:24

> **Tip**
>
> You can use a filter to narrow down the displayed information. The data entered in the filter text box is used for prefix filtering.

Items

The following describes the buttons displayed in the window.

Add button

Adds a new Android application.

Remove button

Removes the selected Android application.

Edit button (**Browse** button)

Edits the selected Android application.

If you have logged in by using an account with the view permission, the **Browse** button is displayed, which allows you to check the contents of the selected Android application.

Related Topics

- *14.6.3 Tabs displayed in the Android Application view*
- *14.6.6 Add Android Application dialog box*
- *14.6.7 Edit Android Application dialog box*

- *14.6.8 View Android Application dialog box*

14.6.3 Tabs displayed in the Android Application view

On the tabs displayed in the **Android Application** view, you can check the distribution and installation status of the Android application selected in the information area.

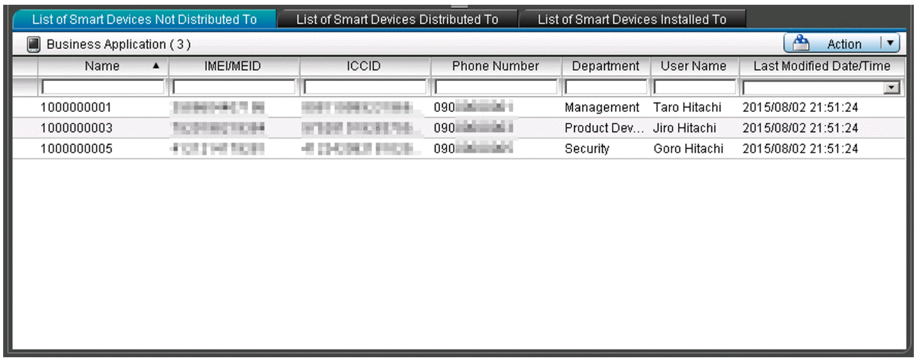
Tip

You can use a filter to narrow down the displayed information. The data entered in the filter text box is used for prefix filtering.

The following describes the tabs displayed in the window.

List of Smart Devices Not Distributed To tab

Displays information for the smart devices to which the selected Android application is not distributed.


List of Smart Devices Not Distributed To
List of Smart Devices Distributed To
List of Smart Devices Installed To
Business Application (3)
Action

Name ▲	IMEI/MEID	ICCID	Phone Number	Department	User Name	Last Modified Date/Time
1000000001	[redacted]	[redacted]	090[redacted]	Management	Taro Hitachi	2015/08/02 21:51:24
1000000003	[redacted]	[redacted]	090[redacted]	Product Dev...	Jiro Hitachi	2015/08/02 21:51:24
1000000005	[redacted]	[redacted]	090[redacted]	Security	Goro Hitachi	2015/08/02 21:51:24

The following describes the **Action** menu items.

Application Distribution

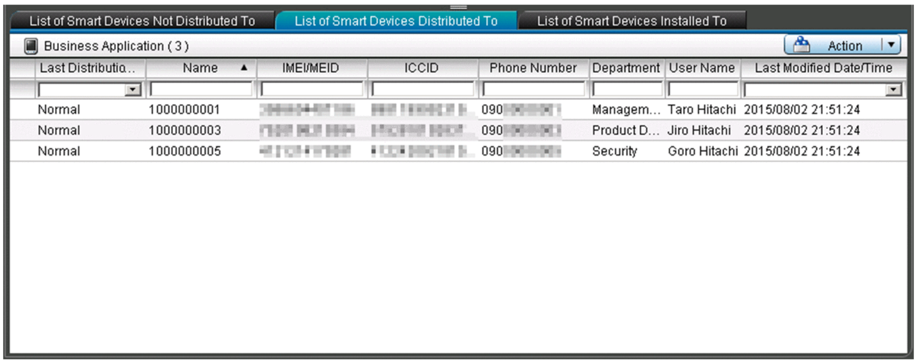
Distributes the Android application to the selected Android devices.

Application Installation

Distributes the Android application to the selected Android devices, and then instructs the installation.

List of Smart Devices Distributed To tab

Displays information for the smart devices to which the selected Android application is distributed.


List of Smart Devices Not Distributed To
List of Smart Devices Distributed To
List of Smart Devices Installed To
Business Application (3)
Action

Last Distributio...	Name ▲	IMEI/MEID	ICCID	Phone Number	Department	User Name	Last Modified Date/Time
Normal	1000000001	[redacted]	[redacted]	090[redacted]	Managem...	Taro Hitachi	2015/08/02 21:51:24
Normal	1000000003	[redacted]	[redacted]	090[redacted]	Product D...	Jiro Hitachi	2015/08/02 21:51:24
Normal	1000000005	[redacted]	[redacted]	090[redacted]	Security	Goro Hitachi	2015/08/02 21:51:24

The following describes the **Action** menu items.

Application Installation

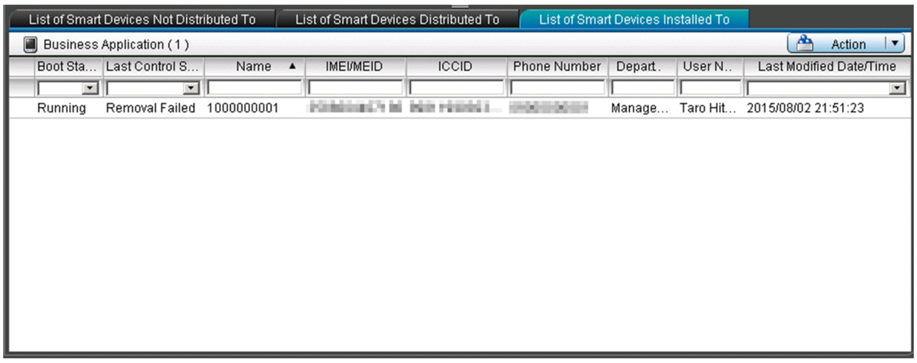
Instructs the selected smart devices to install the Android application.

Application Deletion

Instructs the selected smart devices to uninstall the Android application, and then removes the distributed Android application.

List of Smart Devices Installed To tab

Displays information about the smart devices on which the selected Android application is installed.


List of Smart Devices Not Distributed To
List of Smart Devices Distributed To
List of Smart Devices Installed To
Business Application (1)
Action

Boot Sta...	Last Control S...	Name ▲	IMEI/MEID	ICCID	Phone Number	Depart...	User N...	Last Modified Date/Time
Running	Removal Failed	1000000001	[redacted]	[redacted]	[redacted]	Manage...	Taro Hit...	2015/08/02 21:51:23

The following describes the **Action** menu items.

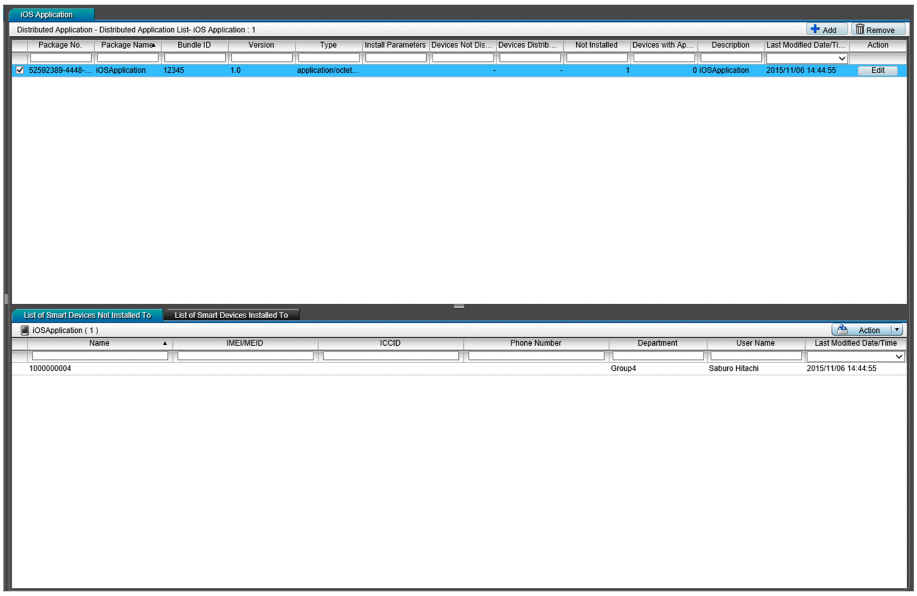
Application Deletion

Instructs the selected smart devices to uninstall the Android application, and then removes the distributed Android application.

14.6.4 iOS Application view

The **iOS Application** view displays a list of registered iOS applications. This view can also be used to add, edit, or remove applications.

Window


iOS Application
Add
Remove
List of Smart Devices Not Installed To
List of Smart Devices Installed To
Action

Distributed Application - Distributed Application List- iOS Application : 1

	Package No.	Package Name▲	Bundle ID	Version	Type	Install Parameters	Devices Not Dis...	Devices Distrib...	Not Installed	Devices with Ap...	Description	Last Modified Date/Ti...	Action
☑	52592389-4448-...	iOSApplication	12345	1.0	application/octet...		-	-	1	0	iOSApplication	2015/11/06 14:44:55	Edit

iOSApplication (1)

Name ▲	IMEI/MEID	ICCID	Phone Number	Department	User Name	Last Modified Date/Time
1000000004				Group4	Saburo Hitachi	2015/11/06 14:44:55

Tip

You can use a filter to narrow down the displayed information. The data entered in the filter text box is used for prefix filtering.

Items

The following describes the buttons displayed in the window.

Add button

Adds a new iOS application.

Remove button

Removes the selected iOS application.

Edit button (**Browse** button)

Edits the selected iOS application.

If you have logged in by using an account with the view permission, the **Browse** button is displayed, which allows you to check the contents of the selected iOS application.

Related Topics

- *14.6.5 Tabs displayed in the iOS Application view*
- *14.6.9 Add iOS Application dialog box*
- *14.6.10 Edit iOS Application dialog box*
- *14.6.11 View iOS Application dialog box*

14.6.5 Tabs displayed in the iOS Application view

On the tabs displayed in the **iOS Application** view, you can check the installation status of the iOS application selected in the information area.

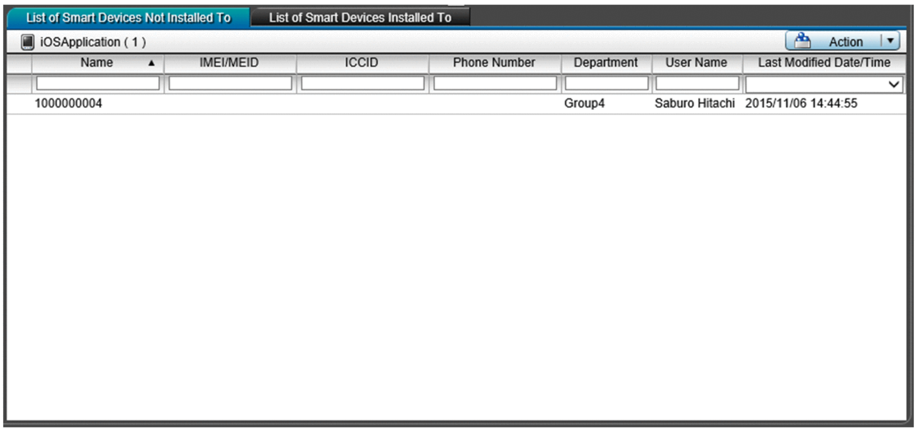
Tip

You can use a filter to narrow down the displayed information. The data entered in the filter text box is used for prefix filtering.

The following describes the tabs displayed in the window.

List of Smart Devices Not Installed To tab

Displays information for the smart devices to which the selected iOS application is not installed.


List of Smart Devices Not Installed To
List of Smart Devices Installed To
iOSApplication (1)
Action

Name	IMEI/MEID	ICCID	Phone Number	Department	User Name	Last Modified Date/Time
1000000004				Group4	Saburo Hitachi	2015/11/06 14:44:55

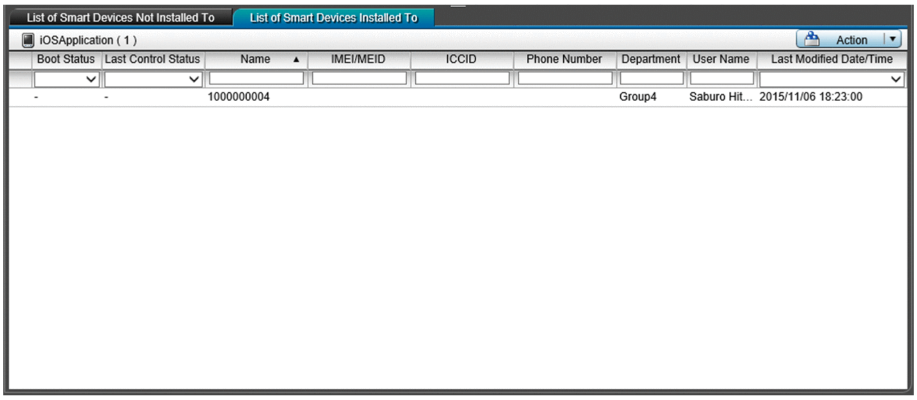
The following describes the **Action** menu items.

Application Installation

Distributes the iOS application to the selected smart devices, and then instructs the installation.

List of Smart Devices Installed To tab

Displays information about the smart devices on which the selected iOS application is installed.


List of Smart Devices Not Installed To
List of Smart Devices Installed To
iOSApplication (1)
Action

Boot Status	Last Control Status	Name	IMEI/MEID	ICCID	Phone Number	Department	User Name	Last Modified Date/Time
-	-	1000000004				Group4	Saburo Hit...	2015/11/06 18:23:00

The following describes the **Action** menu items.

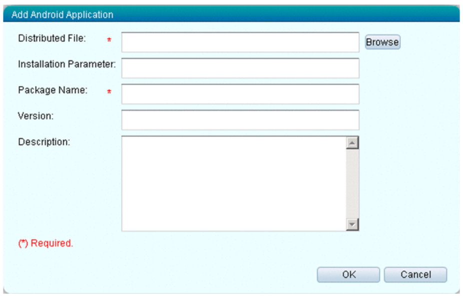
Application Deletion

Instructs the selected smart devices to uninstall the iOS application, and then removes the distributed iOS application.

14.6.6 Add Android Application dialog box

The **Add Android Application** dialog box allows you to register an Android application to be distributed in JP1/ITDM2 - SDM.

Window



Items

The following describes the items displayed in the window.

Distributed File

Click the **Browse** button, and then specify the Android application to be registered.

Installation Parameter

Enter the parameters used for installation.

Package Name

Enter the Android application name. You cannot specify the following characters:

<, >, &, |, ^, %

Version

Enter the package version of the Android application.

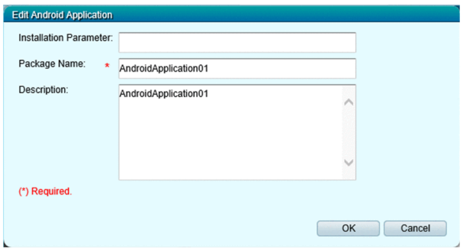
Description

Enter a description about the Android application to be registered. Enter information, such as the purpose of the Android application, to make Android application management easier.

14.6.7 Edit Android Application dialog box

The **Edit Android Application** dialog box allows you to edit a registered Android application.

Window



Package Name: AndroidApplication01

Description: AndroidApplication01

Items

The following describes the items displayed in the window.

Installation Parameter

Enter the parameters used for installation.

Package Name

Enter the Android application name. You cannot specify the following characters:

<, >, &, |, ^, %

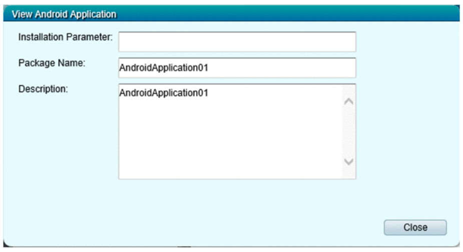
Description

Enter a description about the Android application. Enter information, such as the purpose of the Android application, to make Android application management easier.

14.6.8 View Android Application dialog box

The **View Android Application** dialog box allows you to check the contents of a registered Android application.

Window



View Android Application

Installation Parameter:

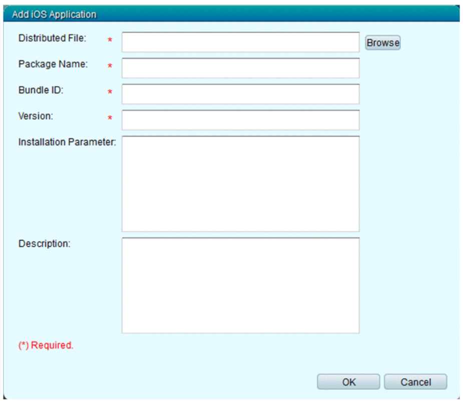
Package Name: AndroidApplication01

Description: AndroidApplication01

14.6.9 Add iOS Application dialog box

The **Add iOS Application** dialog box allows you to register an iOS application to be distributed in JP1/ITDM2 - SDM.

Window



Add iOS Application

Distributed File: *

Package Name: *

Bundle ID: *

Version: *

Installation Parameter:

Description:

(*) Required.

Items

The following describes the items displayed in the window.

Distributed File

Click the **Browse** button, and then specify the iOS application to be registered.

Package Name

Enter the iOS application name. You cannot specify the following characters:

<, >, &, |, ^, %

Bundle ID

Enter the bundle ID of the iOS application.

Version

Enter the package version of the iOS application.

Installation Parameter

Enter the installation parameters of the iOS application.

The specifiable options are shown below. For details, please visit Apple's website.

- Management flag option
- App Install option
- Managed App Configuration and Feedback option
- Managed Application Attributes Queries App Attribute option

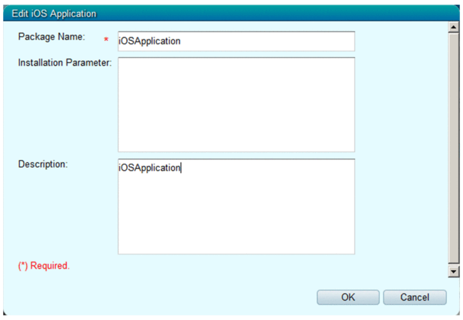
Description

Enter a description about the iOS application to be registered. Enter information, such as the purpose of the iOS application, to make iOS application management easier.

14.6.10 Edit iOS Application dialog box

The **Edit iOS Application** dialog box allows you to edit a registered iOS application.

Window



Package Name: * iOSApplication

Description: iOSApplication

Items

The following describes the items displayed in the window.

Package Name

Enter the iOS application name. You cannot specify the following characters:

<, >, &, |, ^, %

Installation Parameter

Enter the installation parameters of the iOS application.

The specifiable options are shown below. For details, please visit Apple's website.

- Management flag option
- App Install option
- Managed App Configuration and Feedback option
- Managed Application Attributes Queries App Attribute option

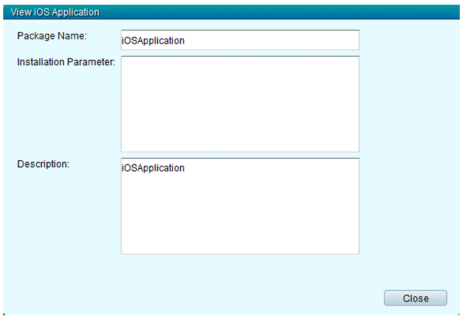
Description

Enter a description about the iOS application. Enter information, such as the purpose of the iOS application, to make iOS application management easier.

14.6.11 View iOS Application dialog box

The **View iOS Application** dialog box allows you to check the contents of a registered iOS application.

Window



View iOS Application

Package Name: iOSApplication

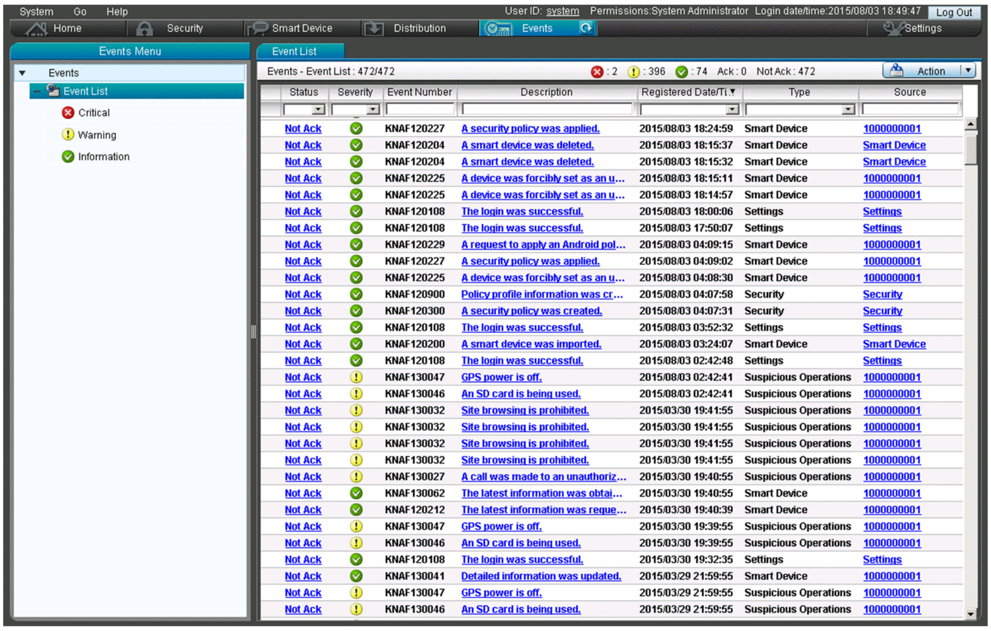
Installation Parameter:

Description: iOSApplication

14.7 Events module

In the Event module, you can check events that occurred during JP1/ITDM2 - SDM operation. You can also check event details and export an event list to a CSV file.

Window



User ID: system Permissions:System Administrator Login date/time:2015/08/03 18:49:47

Events - Event List : 472/472 ✕ : 2 ! : 396 ✓ : 74 Ack : 0 Not Ack : 472

Status	Severity	Event Number	Description	Registered Date/Ti	Type	Source
Not Ack	✓	KNAF120227	A security policy was applied.	2015/08/03 18:24:59	Smart Device	1000000001
Not Ack	✓	KNAF120204	A smart device was deleted.	2015/08/03 18:15:37	Smart Device	Smart Device
Not Ack	✓	KNAF120204	A smart device was deleted.	2015/08/03 18:15:32	Smart Device	Smart Device
Not Ack	✓	KNAF120225	A device was forcibly set as an u...	2015/08/03 18:15:11	Smart Device	1000000001
Not Ack	✓	KNAF120225	A device was forcibly set as an u...	2015/08/03 18:14:57	Smart Device	1000000001
Not Ack	✓	KNAF120108	The login was successful.	2015/08/03 18:00:06	Settings	Settings
Not Ack	✓	KNAF120108	The login was successful.	2015/08/03 17:50:07	Settings	Settings
Not Ack	✓	KNAF120229	A request to apply an Android pol...	2015/08/03 04:09:15	Smart Device	1000000001
Not Ack	✓	KNAF120227	A security policy was applied.	2015/08/03 04:09:02	Smart Device	1000000001
Not Ack	✓	KNAF120225	A device was forcibly set as an u...	2015/08/03 04:08:30	Smart Device	1000000001
Not Ack	✓	KNAF120900	Policy profile information was cr...	2015/08/03 04:07:58	Security	Security
Not Ack	✓	KNAF120300	A security policy was created.	2015/08/03 04:07:31	Security	Security
Not Ack	✓	KNAF120108	The login was successful.	2015/08/03 03:52:32	Settings	Settings
Not Ack	✓	KNAF120200	A smart device was imported.	2015/08/03 03:24:07	Smart Device	Smart Device
Not Ack	✓	KNAF120108	The login was successful.	2015/08/03 02:42:48	Settings	Settings
Not Ack	!	KNAF130047	GPS power is off.	2015/08/03 02:42:41	Suspicious Operations	1000000001
Not Ack	!	KNAF130046	An SD card is being used.	2015/08/03 02:42:41	Suspicious Operations	1000000001
Not Ack	!	KNAF130032	Site browsing is prohibited.	2015/03/30 19:41:55	Suspicious Operations	1000000001
Not Ack	!	KNAF130032	Site browsing is prohibited.	2015/03/30 19:41:55	Suspicious Operations	1000000001
Not Ack	!	KNAF130032	Site browsing is prohibited.	2015/03/30 19:41:55	Suspicious Operations	1000000001
Not Ack	!	KNAF130032	Site browsing is prohibited.	2015/03/30 19:41:55	Suspicious Operations	1000000001
Not Ack	!	KNAF130027	A call was made to an unauthoriz...	2015/03/30 19:40:55	Suspicious Operations	1000000001
Not Ack	✓	KNAF130062	The latest information was obtai...	2015/03/30 19:40:55	Smart Device	1000000001
Not Ack	✓	KNAF120212	The latest information was reque...	2015/03/30 19:40:39	Smart Device	1000000001
Not Ack	!	KNAF130047	GPS power is off.	2015/03/30 19:39:55	Suspicious Operations	1000000001
Not Ack	!	KNAF130046	An SD card is being used.	2015/03/30 19:39:55	Suspicious Operations	1000000001
Not Ack	✓	KNAF120108	The login was successful.	2015/03/30 19:32:35	Settings	Settings
Not Ack	✓	KNAF130041	Detailed information was updated.	2015/03/29 21:59:55	Smart Device	1000000001
Not Ack	!	KNAF130047	GPS power is off.	2015/03/29 21:59:55	Suspicious Operations	1000000001
Not Ack	!	KNAF130046	An SD card is being used.	2015/03/29 21:59:55	Suspicious Operations	1000000001

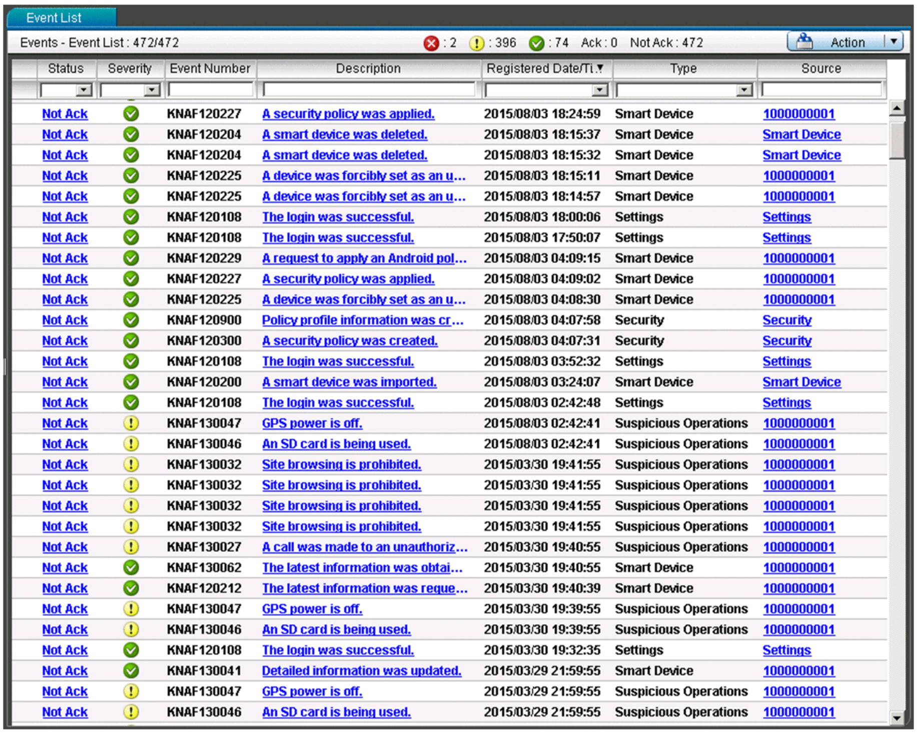
Related Topics

- *14.7.1 Event List view*

14.7.1 Event List view

The **Event List** view displays events that occurred during JP1/ITDM2 - SDM operation. You can check details about the events that occurred, and export an event list to a CSV file.

Window



Events - Event List : 472/472 ✖ : 2 ! : 396 ✓ : 74 Ack : 0 Not Ack : 472

Status	Severity	Event Number	Description	Registered Date/Ti...	Type	Source
Not Ack	✓	KNAF120227	A security policy was applied.	2015/08/03 18:24:59	Smart Device	1000000001
Not Ack	✓	KNAF120204	A smart device was deleted.	2015/08/03 18:15:37	Smart Device	Smart Device
Not Ack	✓	KNAF120204	A smart device was deleted.	2015/08/03 18:15:32	Smart Device	Smart Device
Not Ack	✓	KNAF120225	A device was forcibly set as an u...	2015/08/03 18:15:11	Smart Device	1000000001
Not Ack	✓	KNAF120225	A device was forcibly set as an u...	2015/08/03 18:14:57	Smart Device	1000000001
Not Ack	✓	KNAF120108	The login was successful.	2015/08/03 18:00:06	Settings	Settings
Not Ack	✓	KNAF120108	The login was successful.	2015/08/03 17:50:07	Settings	Settings
Not Ack	✓	KNAF120229	A request to apply an Android pol...	2015/08/03 04:09:15	Smart Device	1000000001
Not Ack	✓	KNAF120227	A security policy was applied.	2015/08/03 04:09:02	Smart Device	1000000001
Not Ack	✓	KNAF120225	A device was forcibly set as an u...	2015/08/03 04:08:30	Smart Device	1000000001
Not Ack	✓	KNAF120900	Policy profile information was cr...	2015/08/03 04:07:58	Security	Security
Not Ack	✓	KNAF120300	A security policy was created.	2015/08/03 04:07:31	Security	Security
Not Ack	✓	KNAF120108	The login was successful.	2015/08/03 03:52:32	Settings	Settings
Not Ack	✓	KNAF120200	A smart device was imported.	2015/08/03 03:24:07	Smart Device	Smart Device
Not Ack	✓	KNAF120108	The login was successful.	2015/08/03 02:42:48	Settings	Settings
Not Ack	!	KNAF130047	GPS power is off.	2015/08/03 02:42:41	Suspicious Operations	1000000001
Not Ack	!	KNAF130046	An SD card is being used.	2015/08/03 02:42:41	Suspicious Operations	1000000001
Not Ack	!	KNAF130032	Site browsing is prohibited.	2015/03/30 19:41:55	Suspicious Operations	1000000001
Not Ack	!	KNAF130032	Site browsing is prohibited.	2015/03/30 19:41:55	Suspicious Operations	1000000001
Not Ack	!	KNAF130032	Site browsing is prohibited.	2015/03/30 19:41:55	Suspicious Operations	1000000001
Not Ack	!	KNAF130032	Site browsing is prohibited.	2015/03/30 19:41:55	Suspicious Operations	1000000001
Not Ack	!	KNAF130027	A call was made to an unauthoriz...	2015/03/30 19:40:55	Suspicious Operations	1000000001
Not Ack	✓	KNAF130062	The latest information was obtai...	2015/03/30 19:40:55	Smart Device	1000000001
Not Ack	✓	KNAF120212	The latest information was reque...	2015/03/30 19:40:39	Smart Device	1000000001
Not Ack	!	KNAF130047	GPS power is off.	2015/03/30 19:39:55	Suspicious Operations	1000000001
Not Ack	!	KNAF130046	An SD card is being used.	2015/03/30 19:39:55	Suspicious Operations	1000000001
Not Ack	✓	KNAF120108	The login was successful.	2015/03/30 19:32:35	Settings	Settings
Not Ack	✓	KNAF130041	Detailed information was updated.	2015/03/29 21:59:55	Smart Device	1000000001
Not Ack	!	KNAF130047	GPS power is off.	2015/03/29 21:59:55	Suspicious Operations	1000000001
Not Ack	!	KNAF130046	An SD card is being used.	2015/03/29 21:59:55	Suspicious Operations	1000000001

Tip

You can use a filter to narrow down the displayed information. The data entered in the filter text box is used for prefix filtering.

You can perform the following operations for events that occurred:

- Click a link displayed in the **Status** column to change the status of an event.
- Click a link displayed in the **Description** column to check details of an event.
- Click a link displayed in the **Source** column to display the window in which an event occurred.
- Export an event list to a CSV file.

Items

The following describes the **Action** menu items.

Show Details

Displays details about the selected event.

Display Source Information

Displays the window, such as the Smart Device module or Settings module, in which the selected event occurred.

Set to Confirmed

Sets the status of the selected event to **Ack**.

Set to Not Confirmed

Sets the status of the selected event to **Not Ack**.

Export Event List

Exports the displayed event list to a CSV file.

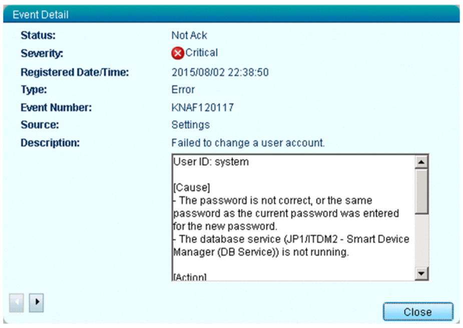
Related Topics

- *14.7.2 Event Detail dialog box*

14.7.2 Event Detail dialog box

The **Event Detail** dialog box can be used to check details of an event.

Window



Status:	Not Ack
Severity:	✖Critical
Registered Date/Time:	2015/08/02 22:38:50
Type:	Error
Event Number:	KNAF120117
Source:	Settings
Description:	Failed to change a user account.

```
User ID: system

[Cause]
- The password is not correct, or the same
password as the current password was entered
for the new password.
- The database service (JP1/ITDM2 - Smart Device
Manager (DB Service)) is not running.

[Action]
```

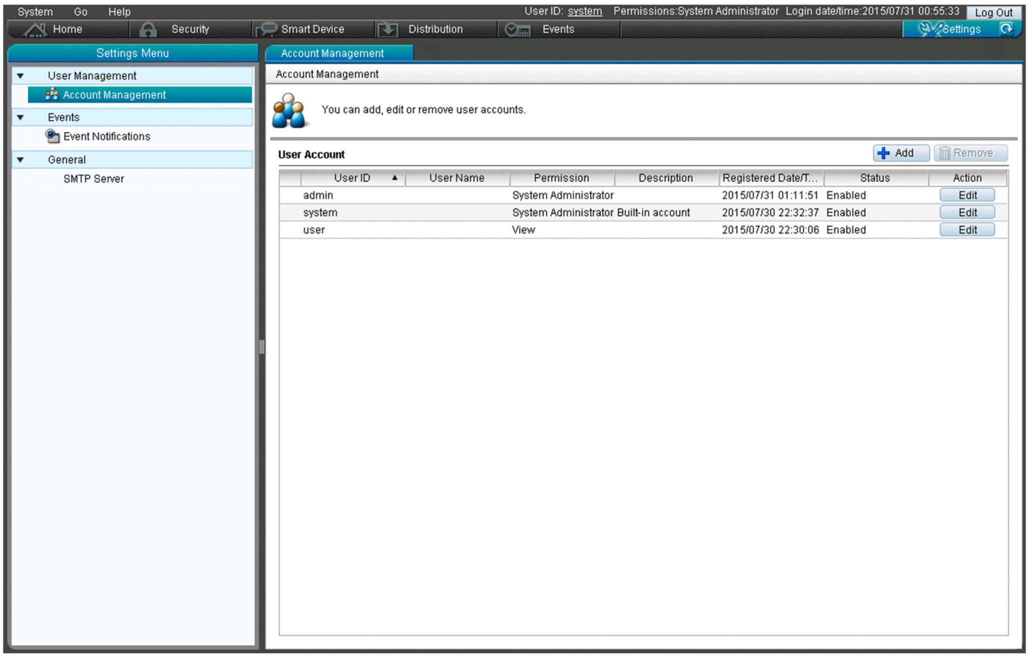
If a high-severity event occurs, use this dialog box to check the details of the event, and take appropriate measures.

You can also click ◀ or ▶ to switch to the previous or next event without closing the dialog box.

14.8 Settings module

In the Settings module, you can specify settings required for operating JP1/ITDM2 - SDM, such as settings for user account management and for email notifications.

Window



You can add, edit or remove user accounts.

User ID ▲	User Name	Permission	Description	Registered Date/T...	Status	Action
admin		System Administrator		2015/07/31 01:11:51	Enabled	Edit
system		System Administrator	Built-in account	2015/07/30 22:32:37	Enabled	Edit
user		View		2015/07/30 22:30:06	Enabled	Edit

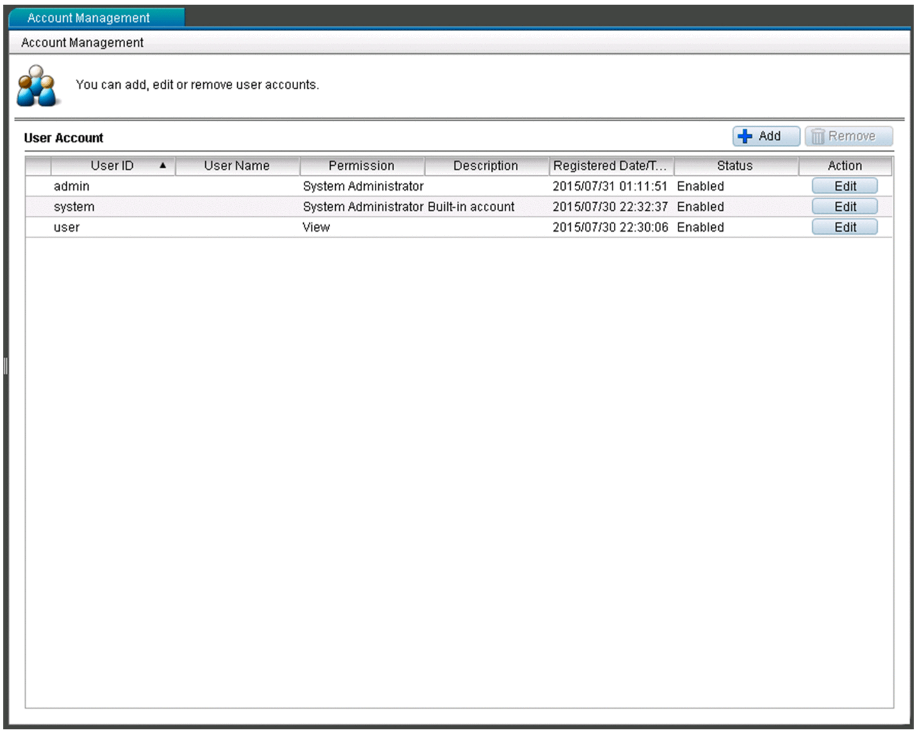
Related Topics

- *14.8.1 Account Management view*
- *14.8.4 Event Notifications view*
- *14.8.5 SMTP Server view*

14.8.1 Account Management view

The **Account Management** view displays a list of registered user accounts. This view can also be used to add, edit, or remove user accounts.

Window



Account Management

Account Management

You can add, edit or remove user accounts.

User Account

User ID ▲	User Name	Permission	Description	Registered Date/T...	Status	Action
admin		System Administrator		2015/07/31 01:11:51	Enabled	Edit
system		System Administrator	Built-in account	2015/07/30 22:32:37	Enabled	Edit
user		View		2015/07/30 22:30:06	Enabled	Edit

Items

The following describes the buttons displayed in the window.

Add button

Adds a new user account.

Remove button

Removes the selected user account. The built-in account or logged-in user account cannot be removed, even if selected.

Edit button

Edits the selected user account.

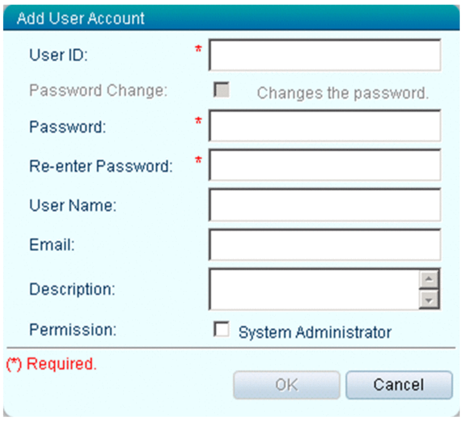
Related Topics

- *14.8.2 Add User Account dialog box*
- *14.8.3 Edit User Account dialog box*

14.8.2 Add User Account dialog box

The **Add User Account** dialog box allows you to register a user account in JP1/ITDM2 - SDM.

Window



Items

The following describes the items displayed in the window.

User ID

Enter the user ID used to log in to JP1/ITDM2 - SDM.

Password

Enter the password for the user ID to be added for login.

Re-enter Password

Re-enter the password for confirmation.

User Name

Enter the user name.

Email

Enter the email address of the user to be added.

Event notification emails are sent to the email address specified here.

Description

Enter a description about the user account to be added. Enter information, such as the purpose of the user account, to make account management easier.

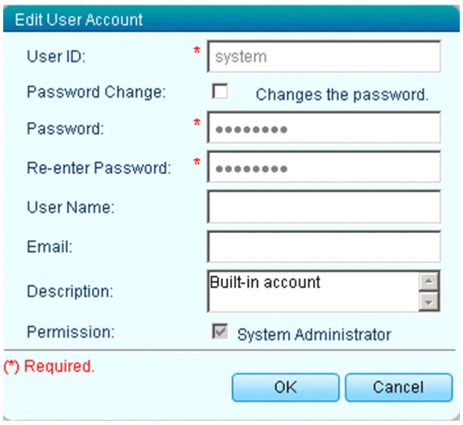
Permission

Select this check box to assign the system administrator permission to the user account. If this check box is not selected, only the view permission is assigned.

14.8.3 Edit User Account dialog box

The **Edit User Account** dialog box allows you to edit registered user account information.

Window



Edit User Account

User ID: * system

Password Change: □ Changes the password.

Password: * ••••••••

Re-enter Password: * ••••••••

User Name:

Email:

Description: Built-in account

Permission: ☑ System Administrator

(*) Required.

Items

The following describes the items displayed in the window.

User ID

Displays the user ID used to log in to JP1/ITDM2 - SDM. This item cannot be edited.

Password

Enter the password for login by using the added user ID.

Re-enter Password

Re-enter the password for confirmation.

User Name

Enter the user name.

Email

Enter the email address.

Event notification emails are sent to the email address specified here.

Description

Enter a description about the user account. Enter information, such as the purpose of the user account, to make account management easier.

Permission

Select this check box to assign the system administrator permission to the user account. If this check box is not selected, only the view permission is assigned.

Status

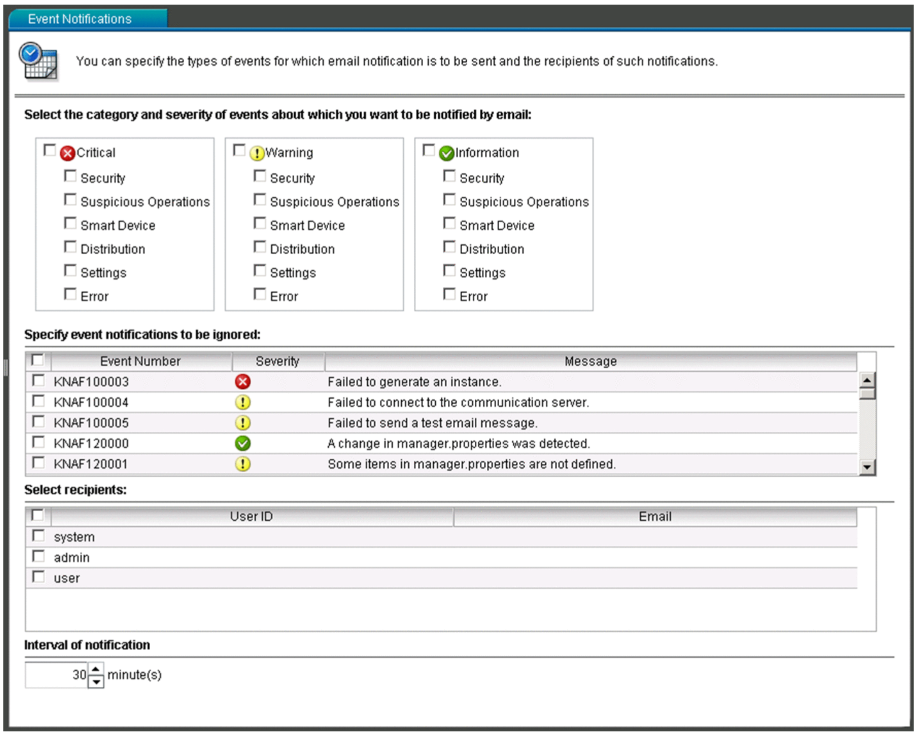
This item is displayed if the user account being edited is locked.

If you have logged in by using an account with the system administrator permission, you can unlock the user account. After the user account is unlocked, the user can use that user account to log in.

14.8.4 Event Notifications view

The **Event Notifications** can be used to specify which events are automatically notified via email.

Window



Event Notifications

You can specify the types of events for which email notification is to be sent and the recipients of such notifications.

Select the category and severity of events about which you want to be notified by email:

□ ✖ Critical	□ ! Warning	□ ✓ Information
□ Security	□ Security	□ Security
□ Suspicious Operations	□ Suspicious Operations	□ Suspicious Operations
□ Smart Device	□ Smart Device	□ Smart Device
□ Distribution	□ Distribution	□ Distribution
□ Settings	□ Settings	□ Settings
□ Error	□ Error	□ Error

Specify event notifications to be ignored:

□	Event Number	Severity	Message
□	KNAF100003	✖	Failed to generate an instance.
□	KNAF100004	!	Failed to connect to the communication server.
□	KNAF100005	!	Failed to send a test email message.
□	KNAF120000	✓	A change in manager.properties was detected.
□	KNAF120001	!	Some items in manager.properties are not defined.

Select recipients:

□	User ID	Email
□	system	
□	admin	
□	user	

Interval of notification

30 minute(s)

Items

The following describes the items displayed in the window.

Select the category and severity of events about which you want to be notified by email:

Select the check boxes for the severity and types of events for which you want to send notification emails.

Specify event notifications to be ignored:

Select the check boxes for the events for which you do not want to send notification emails. To select all events, select the check box at the left end of the title line.

Select recipients:

Select the check boxes for the user accounts to which you want to send event notification emails. To select all user accounts, select the check box at the left end of the title line.

Interval of notification

Set the interval for event notifications.

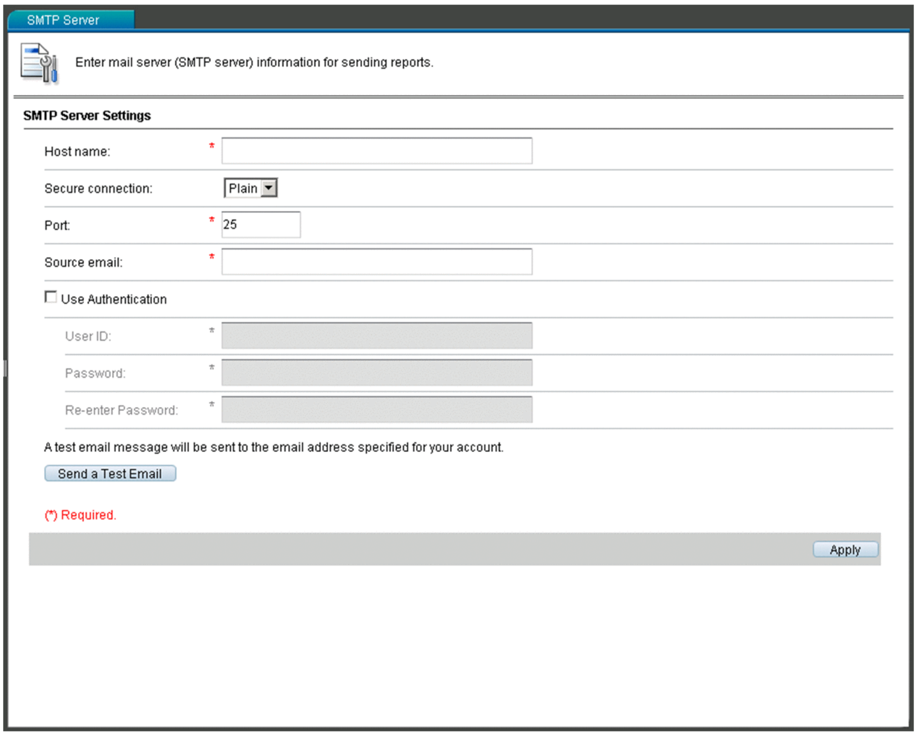
Related Topics

- *2.7.2 Event types*

14.8.5 SMTP Server view

The **SMTP Server** view can be used to set up the mail server (SMTP server) used to send event notifications by email, and send a test email.

Window


SMTP Server

Enter mail server (SMTP server) information for sending reports.

SMTP Server Settings

Host name: *

Secure connection: Plain

Port: * 25

Source email: *

□ Use Authentication

User ID: *

Password: *

Re-enter Password: *

A test email message will be sent to the email address specified for your account.

(*) Required.

Items

The following describes the items and buttons displayed in the window.

Host name

Enter the host name of the SMTP server.

Secure connection

Select the security protection used for communication with the SMTP server.

> **Important**
>
> To use SSL or TLS, you need to import the CA root certificate to the environment in which the smart device manager is running.

Port

Enter the port number of the SMTP server.

Source email

Specify the source email address of event notification emails.

Use Authentication

Select this check box if you use SMTP authentication.

User ID

Enter a user ID if you use SMTP authentication.

Password

Enter the password for the user ID if you use SMTP authentication.

Re-enter Password

Re-enter the password for confirmation.

Send a Test Email button

Sends a test email to the email address of the logged-in user.

Apply button

Applies the specified settings.

Related Topics

- *3.12 Setting up certificates for SSL communication on the smart device manager*
- *14.8.4 Event Notifications view*

15 Commands

This chapter describes JP1/ITDM2 - SDM commands.

Command description format

The description of each command consists of eight items, including the functionality, format (syntax), and arguments. The following table shows how the commands are described.

Command description format

No.	Item	Description
1	Functionality	This subsection describes the command functionality.
2	Format	This subsection describes the format of the command.
3	Arguments	This subsection describes the arguments for the command.
4	Storage location	This subsection describes the storage location for the command.
5	Execution permissions	This subsection describes the permissions required to execute the command.
6	Notes	This subsection provides notes on execution of the command.
7	Return values	This subsection describes the return values of the command.
8	Example	This subsection provides an example of usage of the command.

Executing commands

To execute JP1/ITDM2 - SDM commands, you can use the Windows command prompt. The following describes how to execute a command.

Executing commands

1. Open the Windows command prompt.
2. Change the current directory to the command storage location.
   The command is stored in the following locations:

Server type	Storage location
Smart device manager	*JP1/ITDM2 - SDM (Smart Device Manager)-installation-folder*`\mgr\bin`
Communication server	*JP1/ITDM2 - SDM (Communication Server)-installation-folder*`\cms\bin`
Messaging server	*JP1/ITDM2 - SDM (Messaging Server)-installation-folder*`\mss\bin`

3. Enter the command that you want to execute.

Command List

The following table shows the list of available commands in JP1/ITDM2 - SDM.

Command List

No.	Command name	Functionality	Server where the command is executed
1	sdmexportdb	Acquires data owned by the smart device manager for backup purposes.	Smart device manager
2	sdmimportdb	Restores data owned by the smart device manager to the state at the last backup point.	Smart device manager
3	sdmioutils exportdevice	Exports smart device information.	Smart device manager
4	sdmioutils importdevice	Imports smart device information.	Smart device manager
5	sdmioutils exportpolicy	Exports security policy settings.	Smart device manager
6	sdmioutils importpolicy	Imports security policy settings.	Smart device manager
7	sdmioutils exportsdpolicy	Exports Android policy or iOS profile information.	Smart device manager
8	sdmioutils importsdpolicy	Imports Android policy or iOS profile information.	Smart device manager
9	sdmioutils exportdeliveryapp	Exports application distribution information.	Smart device manager
10	sdmioutils importdeliveryapp	Imports application distribution information.	Smart device manager
11	sdmioutils exportdeliverypermit	Exports settings that define applications as installable by users.	Smart device manager
12	sdmioutils importdeliverypermit	Defines applications as installable by users.	Smart device manager
13	sdmioutils deletedeliverypermit	Deletes settings that define applications as installable by users.	Smart device manager
14	sdmdistributeapp	Distributes applications to smart devices and sends instructions to install them.	Smart device manager
15	sdmapplyprofile	Applies an iOS profile to an iOS device, or removes an iOS profile from an iOS device.	Smart device manager
16	sdmgetinventory	Acquires the latest inventory information from smart devices.	Smart device manager
17	sdmexportdistributestatus	Outputs the distribution status of an application.	Smart device manager
18	sdmexportinstallapp	Outputs information about installed software for all smart devices.	Smart device manager
19	sdmnetchange	Changes the network configuration for the smart device manager or communication server.	• Smart device manager • Communication server
20	sdmcreatemdmcertreq	Creates an MDM signed-certificate request file when iOS devices are managed.	• Smart device manager • Communication server
21	sdmgetlogs	Collects log information on the smart device manager, communication server, JP1/ITDM2 - SDM (Smart Device Agent), or messaging server.	• Smart device manager • Communication server • Messaging server

Related Topics

- *15. sdmexportdb (acquiring backup data)*

- *15. sdmimportdb (restoring backup data)*
- *15. sdmioutils exportdevice (exporting smart device information)*
- *15. sdmioutils importdevice (importing smart device information)*
- *15. sdmioutils exportpolicy (exporting security policy settings)*
- *15. sdmioutils importpolicy (importing security policy settings)*
- *15. sdmioutils exportsdpolicy (exporting Android policy information or iOS profile information)*
- *15. sdmioutils importsdpolicy (importing Android policy information or iOS profile information)*
- *15. sdmioutils exportdeliveryapp (exporting distributed application information)*
- *15. sdmioutils importdeliveryapp (importing distributed application information)*
- *15. sdmioutils exportdeliverypermit (exporting settings that define applications as installable by users)*
- *15. sdmioutils importdeliverypermit (defining applications that can be installed by users)*
- *15. sdmioutils deletedeliverypermit (deleting settings that define applications as installable by users)*
- *15. sdmdistributeapp (sending instructions to install applications)*
- *15. sdmapplyprofile (applying or removing an iOS profile)*
- *15. sdmgetinventory (acquiring inventory information)*
- *15. sdmexportdistributestatus (outputting application distribution status)*
- *15. sdmexportinstallapp (outputting installed software information)*
- *15. sdmnetchange (changing the network configuration for the smart device manager or communication server)*
- *15. sdmcreatemdmcertreq (creating an MDM signed-certificate request file)*
- *15. sdmgetlogs (collecting log information)*

sdmexportdb (acquiring backup data)

This command is used to export data on the smart device manager for backup purposes.

Functionality

This command exports data on the smart device manager for backup purposes. The acquired backup can be used for data restoration in the event of a failure.

When you execute this command, a new backup storage folder is created with the name of *yyyyMMddhhmmss*# under the backup folder you specify in the argument. The backup file will be created in this folder.

# *yyyy*: year, *MM*: month, *dd*: day, *hh*: hours, *mm*: minutes, *ss*: seconds

Format

```
sdmexportdb[ -f backup-folder]
```

Arguments

-f *backup-folder*

Specify the absolute path to the backup storage folder. Only the folders in local drive can be specified. The size of the backup file varies depending on the operational environment and how long JP1/ITDM2 - SDM has been used. Make sure to keep enough free space for the disk drive in which the backup folder resides. The amount of space required is greater than the sum of the size of the database folder and the data folders that are already taking up capacity.

To specify a path containing a space, enclose the strings with double quotation marks (").

Make sure that the path length of the backup folder is 165 or fewer characters (bytes), including the backup file name.

You can use half-width alphanumeric characters, white space, and the following special characters:

#, (,), hyphen (-), period (.), @, underscore (_), and path-delimiter backslash (\)

If this argument is specified, the following backup folder is used:

folder-specified-in-argument\yyyyMMddhhmmss

If this argument is omitted, backup files are stored in the following default backup folder:

JP1/ITDM2 - SDM (Smart Device Manager)-installation-folder\mgr\backup\yyyyMMddhhmmss

Storage location

JP1/ITDM2 - SDM (Smart Device Manager)-installation-folder`\mgr\bin`

Execution permissions

Administrator permissions (this command is executed from the administrator's console if the Windows UAC function is enabled)

Notes

- To execute this command, the smart device manager and communication server must be stopped.
- To execute this command, the database service on the smart device manager must be running.
- Multiple instances of this command cannot be executed simultaneously.

- This command cannot be executed simultaneously with any of the following commands:
  - `sdmimportdb`
  - Commands beginning with `sdmioutils`

Return values

Return value	Description
0	The command finished normally.
11	The format for specifying the command arguments is invalid. Alternatively, the length of the folder name specified for the command argument exceeds the upper limit.
12	You do not have the permissions to execute this command.
13	The specified server is not correct, or the operating environment of JP1/ITDM2 - SDM (Smart Device Manager) is invalid.
14	The file does not exist, or you do not have permission to access it.
15	A file access error occurred, or the disk does not have sufficient capacity.
16	The specified folder does not exist.
17	An access error for the specified folder occurred.
18	Another command is being executed.
24	An attempt to create a backup file failed.
30	The database cannot be accessed.
150	Other error occurred.
253	The service has not started.

Example

The following shows an example of using the command to acquire backup data to `C:\tmp\backup`.

```
sdmexportdb -f C:\tmp\backup
```

Related Topics

- *15. Executing commands*
- *15. sdmimportdb (restoring backup data)*

sdmimportdb (restoring backup data)

This command restores data owned by the smart device manager to the state at the last backup point.

Functionality

This command restores data owned by the smart device manager to the state of the last backup point in case a disk failure occurs. To restore data, a backup file acquired with the `sdmexportdb` command is used.

Execute this command on the smart device manager.

Format

```
sdmimportdb[ -f backup-folder]
```

Arguments

-f *backup-folder*

Specify the absolute path to the folder in which the backup file of the target restore point resides. The path must contain the folder name *yyyyMMddhhmmss* that is created in the backup folder by the `sdmexportdb` command. Only a folder in a local drive can be specified.

To specify a path containing a space, enclose the strings with double quotation marks (").

Make sure that the path length of the backup folder is 165 or fewer characters (bytes), including the backup file name.

Half-width alphanumeric characters, white space, and the following special characters are allowed:

#, (,), -(hyphen),.(period), @, _, and path-delimiter backslash (\)

When this argument is specified, the backup folder specified in the argument is used.

When this argument is omitted, the most up-to-date backup folder available under the path below is chosen by name.

JP1/ITDM2 - SDM (Smart Device Manager)-installation-folder\mgr\backup

Example:

If the following backup folders are under the path, the `\20140101060000` folder is used to restore data:

```
\20140101000000
\20140101060000
```

Storage location

JP1/ITDM2 - SDM (Smart Device Manager)-installation-folder`\mgr\bin`

Execution permissions

Administrator permissions (this command is executed from the administrator's console if the Windows UAC function is enabled)

Notes

- To execute this command, the smart device manager and communication server must be stopped.
- To execute this command, the database service on the smart device manager must be running.
- Multiple instances of this command cannot be executed simultaneously.
- This command cannot be executed simultaneously with any of the following commands:

- `sdmexportdb`
- Commands beginning with `sdmioutils`

Return values

Return value	Description
0	The command finished normally.
11	The format for specifying the command arguments is invalid. Alternatively, the length of the folder name specified for the command argument exceeds the upper limit.
12	You do not have the permissions to execute this command.
13	The specified server is not correct, or the operating environment of JP1/ITDM2 - SDM (Smart Device Manager) is invalid.
14	The file does not exist, or you do not have permission to access it.
15	A file access error occurred, or the disk does not have sufficient capacity.
16	The specified folder does not exist.
17	An access error for the specified folder occurred.
18	Another command is being executed.
25	An attempt to restore the database failed.
30	The database cannot be accessed.
150	Other error occurred.
253	The service has not started.

Example

The following shows an example of using the command to restore data from a backup acquired at 2:30:00 on January 1, 2014 (backup folder: `C:\tmp\backup\20140101023000`).

```
sdmimportdb -f C:\tmp\backup\20140101023000
```

Related Topics

- *15. Executing commands*
- *15. sdmexportdb (acquiring backup data)*

sdmioutils exportdevice (exporting smart device information)

This command exports smart device information in CSV format.

Functionality

This command exports smart device information to the specified file in CSV format.

Execute this command on the smart device manager.

Format

```
sdmioutils exportdevice -export export-file-name[ -encoding character-
encoding][ -s]
```

Arguments

-export *export-file-name*

Specify the absolute path (within 259 bytes) of the CSV file to export.

-encoding *character-encoding*

Specify the character encoding of the file to be exported. If you do not specify this argument, the character encoding is set to UTF-8.

The following types of character encoding can be specified.

- `ISO-8859-1`
- `UTF-8`
- `UTF-16`

-s

Overwrites the file even if a file with the same file name already exists at the export destination. If you do not specify this argument and a file with the same file name already exists, an overwrite confirmation message appears. In this case, the system cancels the output or overwrites the file according to the administrator's reply.

Storage location

JP1/ITDM2 - SDM (Smart Device Manager)-installation-folder`\mgr\bin`

Execution permissions

Administrator permissions (this command is executed from the administrator's console if the Windows UAC function is enabled)

Notes

- To execute this command, the smart device manager must be running.
- To execute this command, the database service on the smart device manager must be running.
- Multiple instances of this command cannot be executed simultaneously.
- This command cannot be executed simultaneously with any of the following commands:
    - `sdmexportdb`
    - `sdmimportdb`

Return values

Return value	Description
0	The command finished normally.
11	The format for specifying the command arguments is invalid. Alternatively, the length of the file name specified for the command argument exceeds the upper limit.
12	You do not have the permissions to execute this command.
13	The specified server is not correct, or the operating environment of JP1/ITDM2 - SDM (Smart Device Manager) is invalid.
14	The file does not exist, or you do not have permission to access it.
15	A file access error occurred, or the disk does not have sufficient capacity.
18	Another command is being executed.
30	The database cannot be accessed.
40	Command execution was interrupted.
150	Other error occurred.
253	The service has not started.

Example

The following shows an example of using the command to export smart device information to `C:\temp\smartdevice.csv`.

```
sdmioutils exportdevice -export C:\temp\smartdevice.csv -encoding UTF-8 -s
```

Related Topics

- *15. Executing commands*
- *15. sdmioutils importdevice (importing smart device information)*
- *E.1 Format of exported or imported smart device list CSV file*

sdmioutils importdevice (importing smart device information)

This command imports smart device information using a CSV file.

Functionality

This command imports smart device information using a CSV file.

Execute this command on the smart device manager.

Format

```
sdmioutils importdevice -import import-file-name[ -encoding character-
encoding]
```

Arguments

-import *import-file-name*

Specify the absolute path (within 259 bytes) of the CSV file to import.

-encoding *character-encoding*

Specify the character encoding of the file to be imported. If you do not specify this argument, the character encoding is set to UTF-8.

The following types of character encoding can be specified.

- `ISO-8859-1`
- `UTF-8`
- `UTF-16`

Storage location

JP1/ITDM2 - SDM (Smart Device Manager)-installation-folder`\mgr\bin`

Execution permissions

Administrator permissions (this command is executed from the administrator's console if the Windows UAC function is enabled)

Notes

- To execute this command, the smart device manager must be running.
- To execute this command, the database service on the smart device manager must be running.
- Multiple instances of this command cannot be executed simultaneously.
- This command cannot be executed simultaneously with any of the following commands:
  - `sdmexportdb`
  - `sdmimportdb`

Return values

Return value	Description
0	The command finished normally.
11	The format for specifying the command arguments is invalid. Alternatively, the length of the file name specified for the command argument exceeds the upper limit.
12	You do not have the permissions to execute this command.
13	The specified server is not correct, or the operating environment of JP1/ITDM2 - SDM (Smart Device Manager) is invalid.
14	The file does not exist, or you do not have permission to access it.
15	A file access error occurred, or the disk does not have sufficient capacity.
18	Another command is being executed.
30	The database cannot be accessed.
40	Command execution was interrupted.
150	Other error occurred.
253	The service has not started.

Example

The following shows an example of using the command to import the smart device information defined in the CSV file `C:\temp\smartdevice.csv`.

```
sdmioutils importdevice -import C:\temp\smartdevice.csv -encoding UTF-8
```

Related Topics

- *15. Executing commands*
- *15. sdmioutils exportdevice (exporting smart device information)*
- *E.1 Format of exported or imported smart device list CSV file*

sdmioutils exportpolicy (exporting security policy settings)

This command exports security policy settings in XML format.

Functionality

This command exports security policy settings to the specified file in XML format.

For an environment with multiple JP1/ITDM2 - SDM systems configured, this command enables security policy settings created on one smart device manager to be reused on another smart device manager.

Execute this command on the smart device manager.

Format

```
sdmioutils exportpolicy -export export-file-name -name security-policy-
name[ -s]
```

Arguments

-export *export-file-name*

Specify the absolute path (within 259 bytes) of the XML file to export.

-name *security-policy-name*

Specify a security policy name to export.

-s

Overwrites the file even if a file with the same file name already exists at the export destination. If this argument is not specified and a file with the same file name already exists, an overwrite confirmation message appears. In this case, the system cancels the output or overwrites the file according to the administrator's reply.

Storage location

JP1/ITDM2 - SDM (Smart Device Manager)-installation-folder`\mgr\bin`

Execution permissions

Administrator permissions (this command is executed from the administrator's console if the Windows UAC function is enabled)

Notes

- To execute this command, the smart device manager must be running.
- To execute this command, the database service on the smart device manager must be running.
- Multiple instances of this command cannot be executed simultaneously.
- This command cannot be executed simultaneously with any of the following commands:
    - `sdmexportdb`
    - `sdmimportdb`

Return values

Return value	Description
0	The command finished normally.
11	The format for specifying the command arguments is invalid. Alternatively, the length of the file name specified for the command argument exceeds the upper limit.
12	You do not have the permissions to execute this command.
13	The specified server is not correct, or the operating environment of JP1/ITDM2 - SDM (Smart Device Manager) is invalid.
14	The file does not exist, or you do not have permission to access it.
15	A file access error occurred, or the disk does not have sufficient capacity.
18	Another command is being executed.
20	The specified security policy does not exist.
30	The database cannot be accessed.
40	Command execution was interrupted.
150	Other error occurred.
253	The service has not started.

Example

The following shows an example of using the command to export the security policy settings `Development Department policy` to `C:\temp\exportpolicy.xml`.

```
sdmioutils exportpolicy -export C:\temp\exportpolicy.xml -name Development
Department policy -s
```

Related Topics

- *15. Executing commands*
- *15. sdmioutils importpolicy (importing security policy settings)*
- *E.3 Format of an exported security policy list XML file*

sdmioutils importpolicy (importing security policy settings)

This command imports previously exported security policy settings.

Functionality

This command imports previously exported security policy settings.

For an environment with multiple JP1/ITDM2 - SDM systems configured, this command enables security policy settings created on one smart device manager to be reused on another smart device manager.

Execute this command on the smart device manager.

Format

```
sdmioutils importpolicy -import import-file-name[ -name security-policy-
name]
```

Arguments

-import *import-file-name*

Specify the absolute path (within 259 bytes) of the XML file to import.

-name *security-policy-name*

Specify a security policy name to import. If this argument is omitted, the security policy name defined in XML is registered. If the specified security policy name already exists, registration fails.

Storage location

JP1/ITDM2 - SDM (Smart Device Manager)-installation-folder`\mgr\bin`

Execution permissions

Administrator permissions (this command is executed from the administrator's console if the Windows UAC function is enabled)

Notes

- To execute this command, the smart device manager must be running.
- To execute this command, the database service on the smart device manager must be running.
- Multiple instances of this command cannot be executed simultaneously.
- This command cannot be executed simultaneously with any of the following commands:
  - `sdmexportdb`
  - `sdmimportdb`

Return values

Return value	Description
0	The command finished normally.
11	The format for specifying the command arguments is invalid. Alternatively, the length of the file name specified for the command argument exceeds the upper limit.

Return value	Description
12	You do not have the permissions to execute this command.
13	The specified server is not correct, or the operating environment of JP1/ITDM2 - SDM (Smart Device Manager) is invalid.
14	The file does not exist, or you do not have permission to access it.
15	A file access error occurred, or the disk does not have sufficient capacity.
18	Another command is being executed.
22	The specified security policy already exists.
30	The database cannot be accessed.
40	Command execution was interrupted.
150	Other error occurred.
253	The service has not started.

Example

The following shows an example of using the command to import the security policy settings in `exportpolicy.xml` (security policy name: `Development Department policy`) that was exported to `C:\temp\`.

```
sdmioutils importpolicy -import C:\temp\exportpolicy.xml -name Development
Department policy
```

Related Topics

- *15. Executing commands*
- *15. sdmioutils exportpolicy (exporting security policy settings)*
- *E.3 Format of an exported security policy list XML file*

sdmioutils exportsdpolicy (exporting Android policy information or iOS profile information)

This command exports Android policy or iOS profile information in XML format.

Functionality

This command exports Android policy or iOS profile information to the specified file in XML format.

For an environment with multiple JP1/ITDM2 - SDM systems configured, this command enables Android policy or iOS profile created on one smart device manager to be reused on another smart device manager.

Execute this command on the smart device manager.

Format

```
sdmioutils exportsdpolicy -export export-file-name -name Android-policy-
name-or-iOS-profile-name -policytype policy-type[ -s]
```

Arguments

-export *export-file-name*

Specify the absolute path (within 259 bytes) of the XML file to export.

-name *Android-policy-name-or-iOS-profile-name*

Specify an Android policy name or iOS profile name to export.

-policytype *policy-type*

Specify the type of policy to export.

The following policy types can be specified:

`0`: iOS profile

`1`: Android policy

-s

Overwrites the file even if a security policy with the same file name already exists. If this argument is not specified and a security policy with the same file name already exists, an overwrite confirmation message appears. In this case, the system cancels the input or overwrites the file according to the administrator's reply.

Storage location

JP1/ITDM2 - SDM (Smart Device Manager)-installation-folder`\mgr\bin`

Execution permissions

Administrator permissions (this command is executed from the administrator's console if the Windows UAC function is enabled)

Notes

- To execute this command, the smart device manager must be running.
- To execute this command, the database service on the smart device manager must be running.
- Multiple instances of this command cannot be executed simultaneously.

- This command cannot be executed simultaneously with any of the following commands:
    - `sdmexportdb`
    - `sdmimportdb`

Return values

Return value	Description
0	The command finished normally.
11	The format for specifying the command arguments is invalid. Alternatively, the length of the file name specified for the command argument exceeds the upper limit.
12	You do not have the permissions to execute this command.
13	The specified server is not correct, or the operating environment of JP1/ITDM2 - SDM (Smart Device Manager) is invalid.
14	The file does not exist, or you do not have permission to access it.
15	A file access error occurred, or the disk does not have sufficient capacity.
18	Another command is being executed.
20	The specified Android policy or iOS profile does not exist.
30	The database cannot be accessed.
40	Command execution was interrupted.
150	Other error occurred.
253	The service has not started.

Example

The following shows an example of using the command to export `Development Department policy` to `C:\temp\exportsdpolicy.xml`.

```
sdmioutils exportsdpolicy -export C:\temp\exportsdpolicy.xml -name
Development Department policy -policytype 0 -s
```

Related Topics

- *15. Executing commands*
- *15. sdmioutils importsdpolicy (importing Android policy information or iOS profile information)*
- *E.4 Format of an exported smart device security policy (Android policy or iOS profile) XML file*

sdmioutils importsdpolicy (importing Android policy information or iOS profile information)

This command imports previously exported Android policy or iOS profile.

Functionality

This command imports previously exported Android policy or iOS profile.

For an environment with multiple JP1/ITDM2 - SDM systems configured, this command enables Android policy or iOS profile created on one smart device manager to be reused on another smart device manager.

Execute this command on the smart device manager.

Format

```
sdmioutils importsdpolicy -import import-file-name[ -name Android-policy-
name-or-iOS-profile-name]
```

Arguments

-import *import-file-name*

Specify the absolute path (within 259 bytes) of the XML file to import.

-name *Android-policy-name-or-iOS-profile-name*

Specify an Android policy name or iOS profile name to import. If this argument is omitted, the Android policy or iOS profile name defined in XML is registered. If the specified name already exists, registration fails.

Storage location

JP1/ITDM2 - SDM (Smart Device Manager)-installation-folder`\mgr\bin`

Execution permissions

Administrator permissions (this command is executed from the administrator's console if the Windows UAC function is enabled)

Notes

- To execute this command, the smart device manager must be running.
- To execute this command, the database service on the smart device manager must be running.
- Multiple instances of this command cannot be executed simultaneously.
- This command cannot be executed simultaneously with any of the following commands:
    - `sdmexportdb`
    - `sdmimportdb`

Return values

Return value	Description
0	The command finished normally.

Return value	Description
11	The format for specifying the command arguments is invalid. Alternatively, the length of the file name specified for the command argument exceeds the upper limit.
12	You do not have the permissions to execute this command.
13	The specified server is not correct, or the operating environment of JP1/ITDM2 - SDM (Smart Device Manager) is invalid.
14	The file does not exist, or you do not have permission to access it.
15	A file access error occurred, or the disk does not have sufficient capacity.
18	Another command is being executed.
22	The specified Android policy or iOS profile already exists.
30	The database cannot be accessed.
40	Command execution was interrupted.
150	Other error occurred.
253	The service has not started.

Example

The following shows an example of using the command to import `Development Department policy` exported to `C:\temp\exportsdpolicy.xml`.

```
sdmioutils importsdpolicy -import C:\temp\exportsdpolicy.xml -name
Development Department policy
```

Related Topics

- *15. Executing commands*
- *15. sdmioutils exportsdpolicy (exporting Android policy information or iOS profile information)*
- *E.4 Format of an exported smart device security policy (Android policy or iOS profile) XML file*

sdmioutils exportdeliveryapp (exporting distributed application information)

This command exports application distribution information in XML format.

Functionality

This command exports application distribution information to the specified file in CSV format.

If multiple JP1/ITDM2 - SDM systems are configured, this command allows application distribution information created on a smart device manager to be reused on another smart device manager.

> **Important**
>
> To reuse application distribution information on another smart device manager, you need to manually copy the applications that were placed on the communication server.

Execute this command on the smart device manager.

Format

```
sdmioutils exportdeliveryapp -export export-file-name -name application-
name [ -version version] -ostype OS-type[ -s]
```

Arguments

-export *export-file-name*

Specify the absolute path (within 259 bytes) of the XML file to export.

-name *application-name*

Specify the name of the application to be exported.

-version *version*

Specify the version of the application to be exported.

If you want to export an iOS application, you must specify a version.

-ostype *OS-type*

Specify the OS type of the application to be exported.

The following OS types can be specified:

`0`: iOS

`1`: Android

-s

Overwrites the file even if a security policy with the same file name already exists. If this argument is not specified and a security policy with the same file name already exists, an overwrite confirmation message appears. In this case, the system cancels the input or overwrites the file according to the administrator's reply.

Storage location

JP1/ITDM2 - SDM (Smart Device Manager)-installation-folder`\mgr\bin`

Execution permissions

Administrator permissions (this command is executed from the administrator's console if the Windows UAC function is enabled)

Notes

- To execute this command, the smart device manager must be running.
- To execute this command, the database service on the smart device manager must be running.
- Multiple instances of this command cannot be executed simultaneously.
- This command cannot be executed simultaneously with any of the following commands:
    - `sdmexportdb`
    - `sdmimportdb`

Return values

Return value	Description
0	The command finished normally.
11	The format for specifying the command arguments is invalid. Alternatively, the length of the file name specified for the command argument exceeds the upper limit.
12	You do not have the permissions to execute this command.
13	The specified server is not correct, or the operating environment of JP1/ITDM2 - SDM (Smart Device Manager) is invalid.
14	The file does not exist, or you do not have permission to access it.
15	A file access error occurred, or the disk does not have sufficient capacity.
18	Another command is being executed.
21	The specified application does not exist.
30	The database cannot be accessed.
40	Command execution was interrupted.
150	Other error occurred.
253	The service has not started.

Example

The following shows an example of using the command to export the application distribution information `Security applications` to `C:\temp\exportdeliveryapp.xml`.

```
sdmioutils exportdeliveryapp -export C:\temp\exportdeliveryapp.xml -name
Security applications -ostype 0 -s
```

Related Topics

- *15. Executing commands*
- *15. sdmioutils importdeliveryapp (importing distributed application information)*
- *E.5 Format of an exported distributed-application XML file*

sdmioutils importdeliveryapp (importing distributed application information)

This command imports previously exported application distribution information.

Functionality

This command imports previously exported application distribution information.

If multiple JP1/ITDM2 - SDM systems are configured, this command allows application distribution information created on a smart device manager to be reused on another smart device manager.

> **Important**
>
> To reuse application distribution information on another smart device manager, you need to manually copy the applications that were placed on the communication server.

Execute this command on the smart device manager.

Format

```
sdmioutils importdeliveryapp -import import-file-name[ -name application-
name]
```

Arguments

-import *import-file-name*

Specify the absolute path (within 259 bytes) of the XML file to import.

-name *application-name*

Specify an application name to import. If this argument is omitted, the application name defined in XML is registered. If the specified application name already exists, registration fails.

Storage location

JP1/ITDM2 - SDM (Smart Device Manager)-installation-folder`\mgr\bin`

Execution permissions

Administrator permissions (this command is executed from the administrator's console if the Windows UAC function is enabled)

Notes

- To execute this command, the smart device manager must be running.
- To execute this command, the database service on the smart device manager must be running.
- Multiple instances of this command cannot be executed simultaneously.
- This command cannot be executed simultaneously with any of the following commands:
  - `sdmexportdb`
  - `sdmimportdb`

Return values

Return value	Description
0	The command finished normally.
11	The format for specifying the command arguments is invalid. Alternatively, the length of the file name specified for the command argument exceeds the upper limit.
12	You do not have the permissions to execute this command.
13	The specified server is not correct, or the operating environment of JP1/ITDM2 - SDM (Smart Device Manager) is invalid.
14	The file does not exist, or you do not have permission to access it.
15	A file access error occurred, or the disk does not have sufficient capacity.
18	Another command is being executed.
23	The specified application already exists.
30	The database cannot be accessed.
40	Command execution was interrupted.
150	Other error occurred.
253	The service has not started.

Example

The following shows an example of using the command to import the application distribution information (application name: `Security applications`) exported to `C:\temp\exportdeliveryapp.xml`.

```
sdmioutils importdeliveryapp -import C:\temp\exportdeliveryapp.xml -name
Security applications
```

Related Topics

- *15. Executing commands*
- *15. sdmioutils exportdeliveryapp (exporting distributed application information)*
- *E.5 Format of an exported distributed-application XML file*

sdmioutils exportdeliverypermit (exporting settings that define applications as installable by users)

This command is used to export the settings that define applications as installable by users. The settings are exported in CSV format.

Functionality

This command exports the settings that define applications as installable by users to a distribution permission definition file.

The information exported by this command depends on the value specified for `-mode`. The following table describes the information exported for each value of `-mode`:

Value specified for -mode	Exported information
`all`	Information about all applications that can be installed by users
`app`	Information about the smart devices to which a specific application can be distributed
`device`	Information about the applications that can be distributed to a specific smart device

Execute this command on the smart device manager.

Format 1

```
sdmioutils exportdeliverypermit -export distribution-permission-definition-
file -mode all[ -encoding character-encoding][ -s]
```

Format 2

```
sdmioutils exportdeliverypermit -export distribution-permission-definition-
file -mode {app | device} -name name -ostype OS-type[ -encoding character-
encoding][ -s]
```

Arguments

-export *distribution-permission-definition-file*

Specify the absolute path (within 259 bytes) of the distribution permission definition file to which to export the settings for applications that can be installed by users.

-mode {all | app | device}

Specify the export mode.

`all`

Exports information about all applications that can be installed by users.

`app`

Exports information about the smart devices to which a specific application can be distributed.

`device`

Exports Information about the applications that can be distributed to a specific smart device.

-name *name*

Specify the name of the application or smart device for which to output information.

-ostype *OS-type*

Specify the OS type of the application to be exported.

The following OS types can be specified:

`0`: Android

`1`: iOS

-encoding *character-encoding*

Specify the character encoding of the file to be exported. If you do not specify this argument, the character encoding is set to UTF-8.

The following types of character encoding can be specified.

- `ISO-8859-1`
- `UTF-8`
- `UTF-16`

-s

Overwrites the file even if a file with the same file name already exists at the export destination. If you do not specify this argument and a file with the same file name already exists, an overwrite confirmation message appears. In this case, the system cancels the output or overwrites the file according to the administrator's reply.

Storage location

JP1/ITDM2 - SDM (Smart Device Manager)-installation-folder`\mgr\bin`

Execution permissions

Administrator permissions (this command is executed from the administrator's console if the Windows UAC function is enabled)

Notes

- To execute this command, the smart device manager must be running.
- To execute this command, the database service on the smart device manager must be running.
- Multiple instances of this command cannot be executed simultaneously.
- This command cannot be executed simultaneously with any of the following commands:
  - `sdmexportdb`
  - `sdmimportdb`

Return values

Return value	Description
0	The command finished normally.
11	The format for specifying the command arguments is invalid. Alternatively, the length of the file name specified for the command argument exceeds the upper limit.
12	You do not have the permissions to execute this command.
13	The specified server is not correct, or the operating environment of JP1/ITDM2 - SDM (Smart Device Manager) is invalid.
14	The file does not exist, or you do not have permission to access it.
15	A file access error occurred, or the disk does not have sufficient capacity.

Return value	Description
18	Another command is being executed.
21	The specified application does not exist.
29	The specified device does not exist.
30	The database cannot be accessed.
40	Command execution was interrupted.
150	Other error occurred.
253	The service has not started.

Example 1

The following shows an example of using the command to export information for all applications that can be installed by users to the file `C:\temp\exportdeliverypermit.csv`.

```
sdmioutils exportdeliverypermit -export C:\temp\exportdeliverypermit.csv -
mode all -s
```

Example 2

The following shows an example of using the command to export information about the smart devices to which the iOS application `application01` can be distributed, to the file `C:\temp\exportdeliverypermit.csv`.

```
sdmioutils exportdeliverypermit -export C:\temp\exportdeliverypermit.csv -
mode app -name application01 -ostype 1 -s
```

Example 3

The following shows an example of using the command to export information about the applications that can be distributed to the iOS device `smartdevice01`, to the file `C:\temp\exportdeliverypermit.csv`.

```
sdmioutils exportdeliverypermit -export C:\temp\exportdeliverypermit.csv -
mode device -name smartdevice01 -ostype 1 -s
```

Related Topics

- *15. Executing commands*
- *15. sdmioutils importdeliverypermit (defining applications that can be installed by users)*
- *15. sdmioutils deletedeliverypermit (deleting settings that define applications as installable by users)*
- *E.6 Format of a distribution permission definition file*

sdmioutils importdeliverypermit (defining applications that can be installed by users)

This command defines applications that can be installed by users.

Functionality

This command imports a distribution permission definition file, and defines the applications that can be installed by users based on the contents of the file.

The information set by this command depends on the value specified for `-mode`. The following table describes the information set for each value of `-mode`:

Value specified for -mode	Settings
`all`	All information in the distribution permission definition file pertaining to applications that can be installed by users is set.
`app`	Permission to distribute the specified application is granted for the smart devices specified in the distribution permission definition file.
`device`	Permission to distribute the applications in the distribution permission definition file is granted for the specified smart device.

Execute this command on the smart device manager.

Format 1

```
sdmioutils importdeliverypermit -import distribution-permission-definition-
file -mode all [ -encoding character-encoding]
```

Format 2

```
sdmioutils importdeliverypermit -import distribution-permission-definition-
file -mode app -name name -version version -ostype OS-type[ -encoding
character-encoding]
```

Format 3

```
sdmioutils importdeliverypermit -import distribution-permission-definition-
file -mode device -name name -ostype OS-type[ -encoding character-encoding]
```

Arguments

-inport *distribution-permission-definition-file*

Specify the absolute path (within 259 bytes) of the distribution permission definition file that lists the applications that can be installed by users.

-mode {all | app | device}

Specify the import mode.

`all`

All information in the distribution permission definition file pertaining to applications that can be installed by users is set.

`app`

Permission to distribute the specified application is granted for the smart devices specified in the distribution permission definition file.

`device`

Permission to distribute the applications in the distribution permission definition file is granted for the specified smart device.

-name *name*

Specify the name of the application or smart device.

-version *version*

Specify the version of the application. You can only specify this argument when `app` is specified for `-mode`.

-ostype *OS-type*

Specify the OS type of the application to be imported.

The following OS types can be specified:

`0`: Android

`1`: iOS

-encoding *character-encoding*

Specify the character encoding of the file to be imported. If you do not specify this argument, the character encoding is set to UTF-8.

- `ISO-8859-1`
- `UTF-8`
- `UTF-16`

Storage location

JP1/ITDM2 - SDM (Smart Device Manager)-installation-folder`\mgr\bin`

Execution permissions

Administrator permissions (this command is executed from the administrator's console if the Windows UAC function is enabled)

Notes

- To execute this command, the smart device manager must be running.
- To execute this command, the database service on the smart device manager must be running.
- Multiple instances of this command cannot be executed simultaneously.
- This command cannot be executed simultaneously with any of the following commands:
  - `sdmexportdb`
  - `sdmimportdb`

Return values

Return value	Description
0	The command finished normally.

Return value	Description
11	The format for specifying the command arguments is invalid. Alternatively, the length of the file name specified for the command argument exceeds the upper limit.
12	You do not have the permissions to execute this command.
13	The specified server is not correct, or the operating environment of JP1/ITDM2 - SDM (Smart Device Manager) is invalid.
14	The file does not exist, or you do not have permission to access it.
15	A file access error occurred, or the disk does not have sufficient capacity.
18	Another command is being executed.
21	The specified application does not exist.
27	The format of the file is invalid.
28	A specified application or smart device was not found.
29	The specified device does not exist.
30	The database cannot be accessed.
40	Command execution was interrupted.
150	Other error occurred.
253	The service has not started.

Example 1

The following shows an example of using the command to set information for all applications that can be installed by users (distribution permission definition file: `C:\temp\exportdeliverypermit.csv`#).

```
sdmioutils importdeliverypermit -import C:\temp\exportdeliverypermit.csv -
mode all
```

# The contents of the `C:\temp\exportdeliverypermit.csv` file are as follows:

```
OS type,Application name,Version,Distribution permission type,Device name
Android,app2,v1,0,device4
Android,app2,v1,0,device5
Android,app3,v1,0,device5
iOS,app1,v1,0,device1
iOS,app1,v1,0,device2
iOS,app1,v1,0,device3
```

Example 2

The following shows an example of using the command to permit distribution of the iOS application `application01` (version `1.00`) (distribution permission definition file: `C:\temp\exportdeliverypermit.csv`#).

```
sdmioutils importdeliverypermit -import C:\temp\exportdeliverypermit.csv -
mode app -name application01 -version 1.00 -ostype 1
```

# The contents of the `C:\temp\exportdeliverypermit.csv` file are as follows:

```
Distribution permission type,Device name
0,device1
```

```
0,device2
0,device3
```

Example 3

The following shows an example of using the command to permit distribution of applications to the iOS device `smartdevice01` (distribution permission definition file: `C:\temp\exportdeliverypermit.csv`#).

```
sdmioutils importdeliverypermit -import C:\temp\exportdeliverypermit.csv -
mode device -name smartdevice01 -ostype 1
```

# The contents of the `C:\temp\exportdeliverypermit.csv` file are as follows:

```
Application name,Version
app1,v1
app2,v1
app3,v1
```

Related Topics

- *15. Executing commands*
- *15. sdmioutils exportdeliverypermit (exporting settings that define applications as installable by users)*
- *15. sdmioutils deletedeliverypermit (deleting settings that define applications as installable by users)*
- *E.6 Format of a distribution permission definition file*

sdmioutils deletedeliverypermit (deleting settings that define applications as installable by users)

This command deletes the settings that define applications as installable by users.

Functionality

This command deletes the settings that define applications as installable by users.

Execute this command on the smart device manager.

Format 1

```
sdmioutils deletedeliverypermit -mode all
```

Format 2

```
sdmioutils deletedeliverypermit -mode app -name name -version version -
ostype OS-type
```

Format 3

```
sdmioutils deletedeliverypermit -mode device -name name -ostype OS-type
```

Arguments

-mode {all | app | device}

Specify the delete mode.

`all`

Deletes information for all applications that can be installed by users.

`app`

Deletes distribution permission for the specified application.

`device`

Deletes distribution permission for the specified device.

-name *name*

Specify the name of the application or smart device.

-version *version*

Specify the version of the application. You can only specify this argument when `app` is specified for `-mode`.

-ostype *OS-type*

Specify the OS type of the application to be deleted.

The following OS types can be specified:

`0`: Android

`1`: iOS

Storage location

JP1/ITDM2 - SDM (Smart Device Manager)-installation-folder`\mgr\bin`

Execution permissions

Administrator permissions (this command is executed from the administrator's console if the Windows UAC function is enabled)

Notes

- To execute this command, the smart device manager must be running.
- To execute this command, the database service on the smart device manager must be running.
- Multiple instances of this command cannot be executed simultaneously.
- This command cannot be executed simultaneously with any of the following commands:
    - `sdmexportdb`
    - `sdmimportdb`

Return values

Return value	Description
0	The command finished normally.
11	The format for specifying the command arguments is invalid. Alternatively, the length of the file name specified for the command argument exceeds the upper limit.
12	You do not have the permissions to execute this command.
13	The specified server is not correct, or the operating environment of JP1/ITDM2 - SDM (Smart Device Manager) is invalid.
14	The file does not exist, or you do not have permission to access it.
15	A file access error occurred, or the disk does not have sufficient capacity.
18	Another command is being executed.
21	The specified application does not exist.
29	The specified device does not exist.
30	The database cannot be accessed.
40	Command execution was interrupted.
150	Other error occurred.
253	The service has not started.

Example 1

The following shows an example of using the command to delete information for all applications that can be installed by users.

```
sdmioutils deletedeliverypermit -mode all
```

Example 2

The following shows an example of using the command to delete distribution permission for the iOS application `application01` (version `1.00`).

```
sdmioutils deletedeliverypermit -mode app -name application01 -version 1.00
-ostype 1
```

Example 3

The following shows an example of using the command to delete distribution permission for the iOS device `smartdevice01`.

```
sdmioutils deletedeliverypermit -mode device -name smartdevice01 -ostype 1
```

Related Topics

- *15. Executing commands*
- *15. sdmioutils exportdeliverypermit (exporting settings that define applications as installable by users)*
- *15. sdmioutils importdeliverypermit (defining applications that can be installed by users)*

sdmdistributeapp (sending instructions to install applications)

This command distributes applications to smart devices and sends a request to users to install those applications.

Functionality

This command distributes applications to smart devices specified in an application distribution information file, and sends instructions to install those applications.

Format

```
sdmdistributeapp -file application-distribution-information-file
```

Arguments

-file *application-distribution-information-file*

Specify an application distribution information file that lists the applications to distribute and the smart devices to which to distribute those applications, as an absolute path of 259 or fewer bytes.

The character encoding of the application distribution information file is UTF-8.

Storage location

JP1/ITDM2 - SDM (Smart Device Manager)-installation-folder`\mgr\bin`

Execution permissions

Administrator permissions (this command is executed from the administrator's console if the Windows UAC function is enabled)

Notes

- To execute this command, the smart device manager and the service of the communication server must be running.
- In the case of an Android application, if the application distribution information file defines distribution and installation, application distribution will take place first. If the application distribution information file defines distribution and installation for the same application, installation of the application will take place and the distribution request will be ignored.

  If an installation request is specified for an application that has already been distributed, the application is installed without being redistributed.
- If the application distribution information file specifies a non-existent application or smart device, the command terminates abnormally.
- If an identical line appears more than once in application distribution information file, the corresponding application distribution and issuing of installation instructions takes place only once.

Return values

Return value	Description
0	The command finished normally.
11	The format for specifying the command arguments is invalid. Alternatively, the length of the file name specified for the command argument exceeds the upper limit.
12	You do not have the permissions to execute this command.

Return value	Description
13	The specified server is not correct, or the operating environment of JP1/ITDM2 - SDM (Smart Device Manager) is invalid.
14	The file does not exist, or you do not have permission to access it.
27	The format of the file is invalid.
28	A specified application or smart device was not found.
150	Other error occurred.
253	The service has not started.

Example

The following shows an example of using the command to distribute the applications specified in the application distribution information file `C:\temp\distributeapp.csv`# to the smart devices specified in the file, and issue the corresponding installation instructions.

```
sdmdistributeapp -file C:\temp\distributeapp.csv
```

#: The contents of the `C:\temp\distributeapp.csv` file are as follows:

```
Operation,OS type,Distributed application,Version,Smart device name
install,iOS,ApplicationA,1.0,Device1
install,iOS,ApplicationA,1.0,Device2
install,iOS,ApplicationA,1.0,Device3
install,iOS,ApplicationB,1.0,Device1
install,iOS,ApplicationB,1.0,Device2
```

Related Topics

- *15. Executing commands*
- *E.7 Format of an application distribution information file*

sdmapplyprofile (applying or removing an iOS profile)

This command applies an iOS profile to an iOS device, or removes an iOS profile that has been applied to an iOS device.

Functionality

This command issues iOS profile application requests or removal requests to iOS devices specified in an iOS profile information file.

Format

```
sdmapplyprofile -file iOS-profile-information-file
```

Arguments

-file *iOS-profile-information-file*

Specify an iOS profile information file that lists the iOS devices to which to apply and from which to remove iOS profiles, as an absolute path of 259 or fewer bytes.

The character encoding of the iOS profile information file is UTF-8.

Storage location

JP1/ITDM2 - SDM (Smart Device Manager)-installation-folder`\mgr\bin`

Execution permissions

Administrator permissions (this command is executed from the administrator's console if the Windows UAC function is enabled)

Notes

- To execute this command, the smart device manager and the service of the communication server must be running.
- The command applies and removes iOS profiles in the order in which they appear in the iOS profile information file. If an attempt to apply or remove an iOS profile fails, processing continues with the next line and the command still terminates normally.
- If you attempt to remove the only iOS profile that is applied to a particular iOS device, the command will fail to remove the iOS profile. However, the command will still terminate normally.

Return values

Return value	Description
0	The command finished normally.
11	The format for specifying the command arguments is invalid. Alternatively, the length of the file name specified for the command argument exceeds the upper limit.
12	You do not have the permissions to execute this command.
13	The specified server is not correct, or the operating environment of JP1/ITDM2 - SDM (Smart Device Manager) is invalid.
14	The file does not exist, or you do not have permission to access it.
27	The format of the file is invalid.
28	A specified application or smart device was not found.

Return value	Description
30	The database cannot be accessed.
150	Other error occurred.
253	The service has not started.

Example

The following shows an example of using the command to apply iOS profiles to the iOS devices specified in the iOS profile information file `C:\temp\profile.csv`#.

```
sdmapplyprofile -file C:\temp\profile.csv
```

#: The contents of the `C:\temp\profile.csv` file are as follows:

```
Operation,Profile name,Device name,Comment
apply,profile_A,Device1,
apply,profile_A,Device2,
```

Related Topics

- *15. Executing commands*
- *E.8 Format of an iOS profile information file*

sdmgetinventory (acquiring inventory information)

This command acquires the latest inventory information from smart devices.

Functionality

This command issues inventory acquisition requests to smart devices whose inventory is to be collected, as specified in a device information file.

Format

```
sdmgetinventory -file device-information-file
```

Arguments

-file *device-information-file*

Specify a device information file that contains device information for devices whose inventory information is to be collected, as an absolute path of 259 or fewer bytes.

The character encoding of the device information file is UTF-8.

Storage location

JP1/ITDM2 - SDM (Smart Device Manager)-installation-folder`\mgr\bin`

Execution permissions

Administrator permissions (this command is executed from the administrator's console if the Windows UAC function is enabled)

Notes

- To execute this command, the smart device manager and the service of the communication server must be running.
- The command acquires inventory information in the order in which the devices are specified in the device information file. If an attempt to acquire inventory information fails, processing continues with the next line and the command still terminates normally.

Return values

Return value	Description
0	The command finished normally.
11	The format for specifying the command arguments is invalid. Alternatively, the length of the file name specified for the command argument exceeds the upper limit.
12	You do not have the permissions to execute this command.
13	The specified server is not correct, or the operating environment of JP1/ITDM2 - SDM (Smart Device Manager) is invalid.
14	The file does not exist, or you do not have permission to access it.
27	The format of the file is invalid.
28	A specified application or smart device was not found.
30	The database cannot be accessed.

Return value	Description
150	Other error occurred.
253	The service has not started.

Example

The following shows an example of using the command to acquire inventory information for the smart devices specified in the device information file `C:\temp\dev_info.csv`#.

```
sdmgetinventory -file C:\temp\dev_info.csv
```

#: The contents of the `C:\temp\dev_info.csv` file are as follows:

```
Inventory type,Device name,Comment
All,Device1,
All,Device2,
All,Device3,
```

Related Topics

- *15. Executing commands*
- *E.9 Format of a device information file*

sdmexportdistributestatus (outputting application distribution status)

This command outputs the distribution status of an application to a file.

Functionality

This command outputs the distribution status of an application to a distribution status output file.

The following table lists the distribution statuses that can be output for an application.

In iOS:

Distribution status	Description	Remarks
Not installed	An instruction to install the application has not been issued. Alternatively, the application has been uninstalled.	--
Installed	Inventory information indicating that installation is complete has been acquired from the smart device.	--
Installation requested	The installation instruction was issued successfully, and distribution is pending.	Because smart device manager cannot detect when an error has occurred on a smart device, installation might have failed despite this status. If the status has not changed to *Installed* by a certain time (24 hours), issue the installation instruction again.
Installing	The application is distributing.	
Installation request failed	An attempt to issue an installation instruction has failed.	Installation has failed. Issue the installation instruction again.
Installation failed	Installation has failed on the smart device.	
Uninstallation requested	The uninstallation instruction was issued successfully, and uninstallation is pending.	Because smart device manager cannot detect when an error has occurred on a smart device, uninstallation might have failed despite this status. If the status has not changed to *Not installed* by a certain time (24 hours), issue the uninstallation instruction again.
Uninstallation request failed	An attempt to issue an uninstallation instruction has failed.	Uninstallation has failed. Issue the uninstallation instruction again.
Uninstallation failed	Uninstallation has failed on the smart device.	

In Android:

Item	Distribution status	Description	Remarks
Distribute Status	Not distributed	The application has not been distributed.	--
	Distributed	The application has been distributed.	--
Last Distribute Control Status	Normal	The application has been distributed or deleted normally.	--
	Deletion failed	An attempt to delete the distributed application has failed on the smart device.	The distributed application could not be deleted. Try deleting the application again.
	Deletion requested	The request to delete the distributed application was issued successfully.	If the status has not changed to *Not distributed* by a certain time (24 hours), try deleting the application again.

Item	Distribution status	Description	Remarks
Last Distribute Control Status	Distribution requested	The request to distribute the application was issued successfully.	If the status has not changed to *Distributed* or *Distribution failed* by a certain time (24 hours), try distributing the application again.
	Distribution failed	Distribution of the application has failed.	Distribution of the application has failed. Try distributing the application again.
Last Installation Control Status	Not installed	The application has not been installed.	--
	Installed	The application has been installed.	--
	Installation failed	Installation has failed on the smart device.	Installation has failed. Issue the installation instruction again.
	Uninstallation failed	Uninstallation has failed on the smart device.	Uninstallation has failed. Issue the uninstallation instruction again.

Format

```
sdmexportdistributestatus -os OS-type -package package-name[ -version
version] -file distribution-status-output-file
```

Arguments

-os *OS-type*

Specify the OS type.

The following OS types can be specified:

0: Android

1: iOS

-package *package-name*

Specify the package name of the application whose distribution status you want to output. You cannot specify the following characters:

<, >, &, |, ^, %

-version *version*

Specify the version of the application whose distribution status you want to output. If you omit this argument, the command outputs the distribution status for all versions of the application. You cannot specify the following characters:

<, >, &, |, ^, %

-file *distribution-status-output-file*

Specify the name of the distribution status output file to which to output the distribution status of the application, as an absolute path of 259 or fewer bytes.

Storage location

JP1/ITDM2 - SDM (Smart Device Manager)-installation-folder\mgr\bin

Execution permissions

Administrator permissions (this command is executed from the administrator's console if the Windows UAC function is enabled)

Notes

- To execute this command, the smart device manager must be running.
- To execute this command, the database service on the smart device manager must be running.

Examples

- The following shows an example of using the command to output the distribution status of an application (package name: `PackageA`, version: `1.0`) to the distribution status output file `C:\temp\PacA_0100_DB.csv`:

  ```
  sdmexportdistributestatus -package PackageA -version 1.0 -file C:\temp
  \PacA_0100_DB.csv
  ```

- The following shows an example of using the command to output the distribution status of an application (package name: `PackageA`, version: All versions) to the distribution status output file `C:\temp\PacA_all_DB.csv`:

  ```
  sdmexportdistributestatus -package PackageA -file C:\temp\PacA_all_DB.csv
  ```

Related Topics

- *15. Executing commands*
- *E.10 Format of a distribution status output file*

sdmexportinstallapp (outputting installed software information)

This command outputs information about the software installed on all smart devices to a file.

Functionality

This command outputs information about software installed on all smart devices to an installed software information output file.

Format

```
sdmexportinstallapp -file installed-software-information-output-file
```

Arguments

-file *installed-software-information-output-file*

Specify the file name of the installed software information output file to which to output information about installed software on all smart devices, as an absolute path of 259 or fewer bytes.

Storage location

JP1/ITDM2 - SDM (Smart Device Manager)-installation-folder`\mgr\bin`

Execution permissions

Administrator permissions (this command is executed from the administrator's console if the Windows UAC function is enabled)

Notes

- To execute this command, the smart device manager must be running.
- To execute this command, the database service on the smart device manager must be running.

Example

The following shows an example of using the command to output installed software information for all smart devices to the installed software information output file `C:\temp\installsoft_inf.csv`:

```
sdmexportinstallapp -file C:\temp\installsoft_inf.csv
```

Related Topics

- *15. Executing commands*
- *E.11 Format of a installed software information output file*

sdmnetchange (changing the network configuration for the smart device manager or communication server)

This command changes the connection destination address and port number set on the smart device manager or communication server.

Functionality

This command changes the connection destination address and port number set on the smart device manager or communication server.

Execute this command on the target smart device manager or communication server.

Format 1

```
sdmnetchange -target Manager -port port-number
```

Format 2

```
sdmnetchange -target Comsrv {-db database-address | -port port-number | -db
database-address -port port-number}
```

Arguments

-target {Manager | Comsrv}

Specify the name of the target server.

`Manager`: For the smart device manager

`Comsrv`: For the communication server

-db *database-address*

Specify this argument to change the database address (connection destination IP address). You can specify this argument only when the target server is the communication server.

-port *port-number*

Specify this argument to change the connection destination port number for the database. You must specify this argument if the target server is the smart device manager.

Note that the port number to be specified differs depending on whether the target server is the smart device manager or the communication server. If the target server is the smart device manager, specify the port number of the smart device manager. If the target server is the communication server, specify the port number of the communication server.

Storage location

In JP1/ITDM2 - SDM (Smart Device Manager):

JP1/ITDM2 - SDM (Smart Device Manager)-installation-folder`\mgr\bin`

In JP1/ITDM2 - SDM (Communication Server):

JP1/ITDM2 - SDM (Communication Server)-installation-folder`\cms\bin`

Execution permissions

Administrator permissions (this command is executed from the administrator's console if the Windows UAC function is enabled)

Notes

- Before executing this command, stop the following services, but do not stop the database service.

  On the smart device manager:

  - JP1/ITDM2 - Smart Device Manager Server Service
  - JP1/ITDM2 - Smart Device Manager Web Server

  On the communication server:

  - JP1/ITDM2 - Smart Device Manager (Communication Server Service)
  - JP1/ITDM2 - Smart Device Manager Web Server

  After executing this command, restart the above services.
- Multiple instances of this command cannot be executed simultaneously.

Return values

Return value	Description
0	The command finished normally.
11	The format for specifying the command arguments is invalid.
12	You do not have the permissions to execute this command.
13	The specified server is not correct, or the operating environment of JP1/ITDM2 - SDM (Smart Device Manager) is invalid.
14	The file does not exist, or you do not have permission to access it.
18	Another command is being executed.
64	Failed to open the XML file.
66	Failed to stop the JP1/ITDM2 - Smart Device Manager Server Service.
67	Failed to start the JP1/ITDM2 - Smart Device Manager Server Service.
68	Failed to stop the JP1/ITDM2 - Smart Device Manager (Communication Server Service).
69	Failed to start the JP1/ITDM2 - Smart Device Manager (Communication Server Service).
70	The alias name is not correct.
71	The password is not correct.
80	JP1/ITDM2 - Smart Device Manager Server Service is running. Stop the service in the Windows Services window, and then re-execute the command.
81	JP1/ITDM2 - Smart Device Manager (Communication Server Service) is running. Stop the service in the Windows Services window, and re-execute the command.
150	Other error occurred.

Example

- The following shows an example of using the command to change the connection destination port number for the database on the smart device manager.

```
sdmnetchange -target Manager -port 32000
```

- The following shows an example of using the command to change the connection destination address and port number for the database on the communication server.

```
sdmnetchange -target Comsrv -db 192.168.1.13 -port 32001
```

Related Topics

- *12.3 Changing the connection destination port number for the database*
- *15. Executing commands*

sdmcreatemdmcertreq (creating an MDM signed-certificate request file)

This command creates an MDM signed-certificate request file when managing iOS devices.

Functionality

This command creates an MDM signed-certificate request file. Use this command when managing iOS devices. The name of the file created by this command is `plist_encoded` (or `plist.xml` if `-x` is specified).

Execute this command on the smart device manager or the communication server.

Format

```
sdmcreatemdmcertreq -a alias-name -p password -f name-of-folder-for-storing-
signature-files[ -o file-destination][ -x]
```

Arguments

-a *alias-name*

Specify the alias name (within 260 bytes) that was specified when the MDM certificate request file was created.

-p *password*

Specify the password (within 260 bytes) that was specified when the MDM certificate request file was created.

-f *name-of-folder-for-storing-signature-files*

Specify the absolute path (within 260 bytes) to the folder that stores a file used to sign the MDM certificate request file.

-o *file-destination*

Specify the absolute path (within 260 bytes) to the output destination of the MDM signed-certificate request file.

-x

Specify this argument to output the MDM signed-certificate request file in XML (non-encoded) format.

Storage location

JP1/ITDM2 - SDM (Smart Device Manager)-installation-folder`\mgr\bin`

Execution permissions

Administrator permissions (this command is executed from the administrator's console if the Windows UAC function is enabled)

Notes

Multiple instances of this command cannot be executed simultaneously.

Return values

Return value	Description
0	The command finished normally.
11	The format for specifying the command arguments is invalid.
14	The file does not exist, or you do not have permission to access it.

Return value	Description
15	A file access error occurred, or the disk does not have sufficient capacity.
18	Another command is being executed.
70	The alias name is not correct.
71	The password is not correct.
150	Other error occurred.

Example

- The following shows an example of using the command to create the MDM signed-certificate request file (`plist_encoded`).

```
sdmcreatemdmcertreq -a mdmalias -p mdmpass -f C:\work -o C:\temp
```

- The following shows an example of using the command to output the created MDM signed-certificate request file in XML format (`plist.xml`).

```
sdmcreatemdmcertreq -a mdmalias -p mdmpass -f C:\work -o C:\temp -x
```

Related Topics

- *3.11.4 Flow of obtaining the MDM client certificate for SSL communication for the APNs server (when managing iOS devices)*
- *3.11.5 Procedure for downloading the MDM certificate request file (when managing iOS devices)*
- *3.11.6 Procedure for creating an MDM signed-certificate request file (when managing iOS devices)*
- *15. Executing commands*

sdmgetlogs (collecting log information)

This command collects log information compressed in zip format for the smart device manager, communication server, JP1/ITDM2 - SDM (Smart Device Agent), or messaging server.

Functionality

This command collects log information compressed in zip format for the smart device manager, communication server, JP1/ITDM2 - SDM (Smart Device Agent), or messaging server.

Execute this command on the server for which you want to collect log information. To collect log data for JP1/ITDM2 - SDM (Smart Device Agent), execute the command on the communication server.

The following table lists the output file names:

Collection target	file name
Smart device manager	tsinfo_manager.zip
Communication server	tsinfo_comsrv.zip
JP1/ITDM2 - SDM (Smart Device Agent)	tsinfo_agent.zip
Messaging server	tsinfo_msgsrv.zip

Format

```
sdmgetlogs -target log-collection-target[ -f output-folder]
```

Arguments

-target *log-collection-target*

Specify the log collection target as follows:

Collection target	Specification
Smart device manager	`Manager`
Communication server	`Comsrv`
JP1/ITDM2 - SDM (Smart Device Agent)	`Agent`
Messaging server	`Msgsrv`

-f *output-folder*

Specify the absolute path (within 161 bytes) to the output destination of the collected log information.

If this argument is omitted, log information will be output to one of the following folders created by the command:

Collection target	Output folder if this argument is omitted
Smart device manager	*JP1/ITDM2 - SDM (Smart Device Manager)-installation-folder*\mgr\troubleshoot
Communication server	*JP1/ITDM2 - SDM (Communication Server)-installation-folder*\cms\troubleshoot
JP1/ITDM2 - SDM (Smart Device Agent)	*JP1/ITDM2 - SDM (Communication Server)-installation-folder*\cms\troubleshoot
Messaging server	*JP1/ITDM2 - SDM (Messaging Server)-installation-folder*\mss\troubleshoot

Storage location

The command is stored in the following locations:

Collection target	Storage location
Smart device manager	*JP1/ITDM2 - SDM (Smart Device Manager)-installation-folder*`\mgr\bin`
Communication server	*JP1/ITDM2 - SDM (Communication Server)-installation-folder*`\cms\bin`
JP1/ITDM2 - SDM (Smart Device Agent)	*JP1/ITDM2 - SDM (Communication Server)-installation-folder*`\cms\bin`
Messaging server	*JP1/ITDM2 - SDM (Messaging Server)-installation-folder*`\mss\bin`

Execution permissions

Administrator permissions (this command is executed from the administrator's console if the Windows UAC function is enabled)

Notes

- To collect log information for JP1/ITDM2 - SDM (Smart Device Agent), you must send log information from JP1/ITDM2 - SDM (Smart Device Agent) to the communication server before executing the command.
- Multiple instances of this command cannot be executed simultaneously.

Return values

Return value	Description
0	The command finished normally.
11	The format for specifying the command arguments is invalid. Alternatively, the length of the folder name specified for the command argument exceeds the upper limit.
12	You do not have the permissions to execute this command.
13	The specified server is not correct, or the operating environment of JP1/ITDM2 - SDM (Smart Device Manager) is invalid.
14	The folder does not exist, or you do not have permission to access it.
15	A file access error occurred, or the disk does not have sufficient capacity.
18	Another command is being executed.
150	Other error occurred.

Example

- The following shows an example of using the command to output log information for the smart device manager to the `C:\work` folder.

```
sdmgetlogs -target Manager -f C:\work
```

- The following shows an example of using the command to output log information for the communication server to the `C:\work` folder.

```
sdmgetlogs -target Comsrv -f C:\work
```

- The following shows an example of using the command to output log information for JP1/ITDM2 - SDM (Smart Device Agent) to the `C:\work` folder on the communication server.

```
sdmgetlogs -target Agent -f C:\work
```

- The following shows an example of using the command to output log information for the messaging server to the `C:\work` folder.

```
sdmgetlogs -target Msgsrv -f C:\work
```

Related Topics

- *8.12 Collecting smart device log data*
- *15. Executing commands*

16 Definition Files

This chapter describes the JP1/ITDM2 - SDM definition files.

16.1 Definition file list

The following table lists the JP1/ITDM2 - SDM definition files.

Definition file list

Server	Definition file	File name	Description
Smart device manager	Smart device manager environment setting file	manager.properties	Environment settings file for the smart device manager
	Provisioning information setting file	provisioning.properties	Provisioning information settings file for the smart device
	Event mail format information file	eventmail.properties	Format information file for event emails
	Test mail format information file	testmail.properties	Format information file for test emails
Communication server	Communication server environment setting file	CommunicationServerEngine .properties	Environment settings file for the communication server
Messaging server	Messaging server setting file	SdMessagingServer.ini	Environment settings file for the messaging server

Important

To change a definition file and apply settings, you must restart the server on which the definition server is stored.

Related Topics

- *16.2 Smart device manager environment setting file (manager.properties)*
- *16.3 Provisioning information setting file (provisioning.properties)*
- *16.4 Event mail format information file (eventmail.properties)*
- *16.5 Test mail format information file (testmail.properties)*
- *16.6 Communication server environment setting file (CommunicationServerEngine.properties)*
- *16.7 Messaging server setting file (SdMessagingServer.ini)*

16.2 Smart device manager environment setting file (manager.properties)

This file specifies the operating environment for the smart device manager.

Format

```
callhistory=call-history-storage-period
webhistory=Web-browsing-history-storage-period
apphistory=application-use-history-storage-period
gpsevent=whether-to-issue-GPS-power-off-event
gpsmapview=map-site-linkage-for-GPS-information-display
sdcardevent=whether-to-issue-SD-card-use-event
bluetoothevent=whether-to-issue-Bluetooth-connection-event
bluetoothalertlevel=alert-level-of-Bluetooth-connection-event
simevent=whether-to-issue-SIM-card-change-event
unlockevent=number-of-days-until-event-is-issued-before-next-unlock
unconectedevent=event-issuing-period-if-inventory-data-collection-is-
incomplete
callhistory.securityinterval=call-history-security-check-interval
webhistory.securityinterval=Web-browsing-history-security-check-interval
application.securityinterval=application-security-check-interval
bluetooth.securityinterval=Bluetooth-history-security-check-interval
baseinfo.securityinterval=basic-information-security-check-interval
communicationserverurl=communication-server-address
detail.debug.log.mode=detailed-trace-log-output-mode
distribute.mode = distribution-type
distribute.auth = whether-to-authenticate-access
```

Setting items

The following describes the setting items and specifiable values for the smart device manager environment setting file:

Setting item	Description	Specifiable value	Initial value
callhistory	Specify the call history storage period.	1 to 365 (in days)	120
webhistory	Specify the period to store the Web browsing history.	1 to 365 (in days)	120
apphistory	Specify the period to store the application use history.	1 to 365 (in days)	120
gpsevent	Specify whether to issue an event when GPS power is turned off.	true Issues an event. false Does not issue an event.	true
gpsmapview	Specify whether to link the map site when GPS information is displayed.	true Links the map site. false Does not link the map site.	true
sdcardevent	Specify whether to issue an event when an SD card is used.	true Issues an event.	true

Setting item	Description	Specifiable value	Initial value
sdcardevent	Specify whether to issue an event when an SD card is used.	false Does not issue an event.	true
bluetoothevent	Specify whether to issue an event when a Bluetooth connection is established.	true Issues an event. false Does not issue an event.	true
bluetoothalertlevel	Set the alert level of an event that is issued when a Bluetooth connection is established.	0 Critical 1 Warning 2 Information	0
simevent	Specify whether to issue an event when a SIM card is changed.	true Issues an event. false Does not issue an event.	true
unlockevent	Specify whether to issue an event before the lock is released the next time. If an event is to be issued, specify the number of days until the event is issued.	0 Does not issue an event. 1 to 7 Number of days until the event is issued	1
unconectedevent	Specify the period during which an event is issued if inventory data collection is incomplete.	1 to 7 (in days)	1
callhistory.securityinterval	Specify the security check interval for the call history.	1 to 86400 (in minutes)	1440
webhistory.securityinterval	Specify the security check interval for the Web browsing history.	1 to 86400 (in minutes)	1440
application.securityinterval	Specify the security check interval for applications.	1 to 86400 (in minutes)	1440
bluetooth.securityinterval	Specify the security check interval for the Bluetooth history.	1 to 86400 (in minutes)	1440
baseinfo.securityinterval	Specify the security check interval for basic information.	1 to 86400 (in minutes)	1440
communicationserverurl	Specify the address of the communication server to which the smart device manager is connected. This item must be specified.	*host-name*:*port-number* *host-name* Host name of the communication server (FQDN format)	None

Setting item	Description	Specifiable value	Initial value
communicationserverurl	Specify the address of the communication server to which the smart device manager is connected. This item must be specified.	*port-number*#1 The communication server HTTPS port number for SSL communication (default: 26055)	None
detail.debug.log.mode	Set the detailed trace log output mode.	0 Disabled 1 Enabled	0
distribute.mode#2	Set the distribution method for applications.	0 Simple distribution 1 Standard distribution	1
distribute.auth#2	Set whether to require authentication when using standard distribution.#3	0 Do not require authentication 1 Require authentication	1

#1

This port number must be the same as the port number specified in the `httpsd.conf` file for the communication server.

#2

If a value other than `0` or `1` is specified or this item is omitted, `0` is assumed.

#3

If access authentication is unnecessary, comment out the following line in the httpsd.conf file on the JP1/ITDM2 - SDM communication server. Then, restart the `JP1/ITDM2 - Smart Device Manager Web Server` on the communication server.

```
<Directory "JP1/ITDM2 - SDM (Communication Server)-installation-folder/cms/uC/httpsd/htdocs/download">
    AuthType Basic
    AuthName "realm"
    AuthUserFile "JP1/ITDM2 - SDM (Communication Server)-installation-folder/cms/conf/htpasswd"
    Require valid-user
</Directory>
```

Example

```
callhistory=120
webhistory=120
apphistory=120
gpsevent=true
gpsmapview=true
sdcardevent=true
bluetoothevent=true
bluetoothalertlevel=1
simevent=true
unlockevent=1
unconectedevent=1
callhistory.securityinterval=30
```

```
webhistory.securityinterval=30
application.securityinterval=30
bluetooth.securityinterval=30
baseinfo.securityinterval=30
communicationserverurl=xxxxxxx.xxxxxxx.co.jp:26055
detail.debug.log.mode = 1
distribute.mode = 1
distribute.auth = 1
```

16.3 Provisioning information setting file (provisioning.properties)

This file specifies the provisioning information for JP1/ITDM2 - SDM (Smart Device Agent) that runs on a smart device.

Format

```
communicationserveraddress=connection-destination-communication-server-
address
messagingseverurl=connection-destination-message-server-address
inventoryinterval=inventory-data-collection-interval
gpsinterval=GPS-information-collection-interval
lowbattery=battery-capacity-to-send-inventory-data-at-low-voltage
```

Setting items

The following describes the setting items and specifiable values for the provisioning information setting file:

Setting item	Description	Specifiable value	Initial value
communicationserveraddress	Specify the address of the connection destination communication server. This item must be specified.	*host-name*:*port-number* *host-name* Host name of the communication server (FQDN format) *port-number*#1 The communication server HTTPS port number for SSL communication (default: 26055)	None
messagingseverurl	Specify the address of the connection destination messaging server (for Android only). This item must be specified.	*host-name*:*port-number* *host-name* Host name of the messaging server (FQDN format) *port-number*#2 The messaging server HTTP port number for communication (default: 26079)	None
inventoryinterval	Specify the inventory data collection interval.	0 to 24 (in hours) #3	24
gpsinterval	Specify the GPS information collection interval.	1 to 24 (in hours)	24
lowbattery	Specify the battery level for sending inventory data in the event of low voltage. You can specify multiple values separated by commas. Example: `15,10,5`	1 to 100 (%)	5

#1

This port number must be the same as the port number specified in the `httpsd.conf` file for the communication server.

#2

This port number must be the same as the port number to be set for HttpPort in the messaging server setting file (`SdMessagingServer.ini`).

#3

If 0 is specified, inventory data will not be collected.

If the number of managed devices reaches or exceeds 1,000, the collection of inventory data might take more than an hour. For this reason, set 2 or a greater value.

Example

```
communicationserveraddress=xxxxxxx.xxxxxxx.co.jp:26055
messagingseverurl=xxxxxxx.xxxxxxx.co.jp:26079
inventoryinterval=24
gpsinterval=24
lowbattery=10,5
```

Related Topics

- *16.7 Messaging server setting file (SdMessagingServer.ini)*

16.4 Event mail format information file (eventmail.properties)

This file specifies the event email format.

Format

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE properties SYSTEM "http://java.sun.com/dtd/properties.dtd">
<properties>
<comment>Event mail properties</comment>

<!-- Mail subject -->
<entry key="mail_subject">mail-subject</entry>

<!-- Mail header -->
<!--
Create data by replacing the following parameter characters enclosed in
curly brackets { } with the corresponding data:

{EVENT_COUNT}           : Number of events
 -->
<entry key="mailheader">mail-header</entry>


<!-- Mail footer -->
<entry key="mailfooter">mail-footer</entry>


<!-- Mail format -->
<!--
Create data by replacing the following parameter characters enclosed in
curly brackets { } with the corresponding data:

{STATUS}                : Whether the event is checked
{ALERT_LEVEL}           : Severity
{MESSAGE_ID}            : Event number
{MESSAGE_CONTENT}       : Event description
{NOTE}                  : Detailed information for the event
{EVENT_DATE}            : Date and time when the event was registered
{MESSAGE_TYPE}          : Event type
{EVENT_ORIGIN}          : Source of the event
 -->
<entry key="mailformat">mail-format</entry>
</properties>
```

Setting items

The following describes the setting items of the event email format information file:

Setting item	Description
mail_subject	Specify the email subject name.
mailheader	Specify the email header.
mailfooter	Specify the email footer.
mailformat	Specify the email text.

The table below lists the parameter characters you can use to specify event email. The parameter characters used in the file are replaced with the corresponding data when an email is sent.

Parameter character	Description
{EVENT_COUNT}	Number of events
{STATUS}	Whether the event is checked
{ALERT_LEVEL}	Severity
{MESSAGE_ID}	Event number
{MESSAGE_CONTENT}	Event description
{NOTE}	Detailed information for the event
{EVENT_DATE}	Date and time when the event was registered
{MESSAGE_TYPE}	Event type
{EVENT_ORIGIN}	Source of the event

Example

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE properties SYSTEM "http://java.sun.com/dtd/properties.dtd">
<properties>
<comment>Event mail properties</comment>

<!-- Mail subject -->
<entry key="mail_subject">Event Mail Information</entry>

<!-- Mail header -->
<!--
Create data by replacing the following parameter characters enclosed in
curly brackets { } with the corresponding data.


{EVENT_COUNT}           : Number of events
 -->
<entry key="mailheader"><![CDATA[Number of events: {EVENT_COUNT}]]></entry>


<!-- Mail footer -->
<entry key="mailfooter"><![CDATA[
////////////////////////////////////
* Company: XXXXXXX
* Address: XXXXXXXXX X-X-X
* MAIL: XXXXXX@XXX.XX.XX
* TEL: XXX-XXXX-XXXX
////////////////////////////////////
]]></entry>


<!-- Mail format -->
<!--
Create data by replacing the following parameter characters enclosed in
curly brackets { } with the corresponding data.

{STATUS}                : Whether the event is checked
```

```
{ALERT_LEVEL}            : Severity
{MESSAGE_ID}             : Event number
{MESSAGE_CONTENT}        : Event description
{NOTE}                   : Detailed information for the event
{EVENT_DATE}             : Date and time when the event was registered
{MESSAGE_TYPE}           : Event type
{EVENT_ORIGIN}           : Source of the event
 -->
<entry key="mailformat"><![CDATA[
Whether the event is checked              : {STATUS}
Severity                                  : {ALERT_LEVEL}
Event number                              : {MESSAGE_ID}
Event description                         : {MESSAGE_CONTENT}
Detailed information for the event        : {NOTE}
Date and time when the event was registered : {EVENT_DATE}
Event type                                : {MESSAGE_TYPE}
Source of the event                       : {EVENT_ORIGIN}
]]></entry>
</properties>
```

16.5 Test mail format information file (testmail.properties)

This file specifies the test email format.

Format

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE properties SYSTEM "http://java.sun.com/dtd/properties.dtd">
<properties>
<comment>Event mail properties</comment>

<!-- Mail subject -->
<entry key="mail_subject">mail-subject</entry>

<!-- Mail header -->
<entry key="mailheader">mail-header</entry>


<!-- Mail footer -->
<entry key="mailfooter">mail-footer</entry>

</properties>
```

Setting items

The following describes the setting items of the test mail format information file:

Setting item	Description
mail_subject	Specify the email subject name.
mailheader	Specify the email header.
mailfooter	Specify the email footer.

Example

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE properties SYSTEM "http://java.sun.com/dtd/properties.dtd">
<properties>
<comment>Event mail properties</comment>

<!-- Mail subject -->
<entry key="mail_subject">JP1/ITDM2 - SDM Test mail</entry>

<!-- Mail header -->
<entry key="mailheader"><![CDATA[Confirm email transmission]]></entry>


<!-- Mail footer -->
<entry key="mailfooter"><![CDATA[--message end--]]></entry>

</properties>
```

16.6 Communication server environment setting file (CommunicationServerEngine.properties)

This file specifies the operating environment for the communication server.

Format

```
messaging.server.address = messaging-server-connection-destination-address
messaging.server.port = messaging-server-connection-destination-port-number
request.timeout.time = request-timeout-time
semaphore.wait.timeout.time = semaphore-allocation-timeout-time
ios.battery.inventory.timeout.time = iOS-device-battery-information-
collection-interval
detail.debug.log.mode = detailed-trace-log-output-mode
communication.server.address = communication-sarver-address
ios.request.getinventory.timeout.time = iOS-collect-inventory-request-
timeout-time
ios.request.wipe.timeout.time = iOS-initialization-request-timeout-time
ios.request.lock.timeout.time = iOS-lock-request-timeout-time
ios.request.clearpasscode.timeout.time = iOS-reset-passcode-request-timeout-
time
ios.request.installappli.timeout.time = iOS-application-installation-
request-timeout-time
ios.request.uninstallappli.timeout.time = iOS-application-deletion-request-
timeout-time
ios.request.unmanage.timeout.time = iOS-set-to-unmanaged-request-timeout-
time
ios.request.applyprofile.timeout.time = iOS-apply-profile-request-timeout-
time
ios.request.removeprofile.timeout.time = iOS-remove-profile-request-timeout-
time
ios.inventory.collect.run.mode = iOS-device-inventory-collection-method
ios.inventory.collect.run.time = iOS device-inventory-collection-time
```

Setting items

The following describes the setting items and specifiable values for the communication server environment setting file:

Setting item	Description	Specifiable value	Initial value
messaging.server.address	Specify the connection destination address for the messaging server. This item must be specified.	IPv4 address	localhost
messaging.server.port	Specify the connection destination port number for the messaging server. This item must be specified.	1 to 65535	26078
request.timeout.time	Specify the request timeout time.	0 to 60 (in minutes)	5
semaphore.wait.timeout.time	Specify the semaphore allocation timeout time.	0 to 60 (in minutes)	5
ios.battery.inventory.timeout.time	Specify the interval for collecting iOS device battery information.	0, 60 to 1440 (in minutes)#1	0

Setting item	Description	Specifiable value	Initial value
detail.debug.log.mode	Specify the detailed trace log output mode.	0 Disabled 1 Enabled	0
communication.server.address	Specify the address of the communication server. Required to specify when you deliver applications to iOS.	*host-name***:***port-number* *host-name* Host name of the communication server (FQDN format) *port-number*#2 The communication server HTTPS port number for SSL communication (When no port number is specified, port 443 is used.)	None
ios.request.getinventory.timeout.time	Specify the timeout value of the request of inventory collection for iOS devices.	0 to 10080 (in minutes)#3	1440
ios.request.wipe.timeout.time	Specify the timeout value of the wipe request for iOS devices.	0 to 10080 (in minutes)#3	1440
ios.request.lock.timeout.time	Specify the timeout value of the lock request for iOS devices.	0 to 10080 (in minutes)#3	1440
ios.request.clearpasscode.timeout.time	Specify the timeout value of the passcode reset request for iOS devices.	0 to 10080 (in minutes)#3	1440
ios.request.installappli.timeout.time	Specify the timeout value of the request of application installation on iOS devices.	0 to 10080 (in minutes)#3	4320
ios.request.uninstallappli.timeout.time	Specify the timeout value of the request of application uninstallation on iOS devices.	0 to 10080 (in minutes)#3	4320
ios.request.unmanage.timeout.time	Specify the timeout value of the unmanage request for iOS devices.	0 to 10080 (in minutes)#3	1440
ios.request.applyprofile.timeout.time	Specify the timeout value of the request of applying profiles to iOS devices.	0 to 10080 (in minutes)#3	1440
ios.request.removeprofile.timeout.time	Specify the timeout value of the request of removing profiles in iOS devices.	0 to 10080 (in minutes)#3	1440
ios.inventory.collect.run.mode	Specify the method of collecting inventory information from iOS devices.	time Collecting inventory	time

Setting item	Description	Specifiable value	Initial value
ios.inventory.collect.run.mode	Specify the method of collecting inventory information from iOS devices.	information at the specified time. interval Collecting inventory information at the specified interval. none No execution of collecting inventory information.	time
ios.inventory.collect.run.time	Specify the time for collecting inventory information when you define the `ios.inventory.collect.run.mode` as `time`.#4	hh:mm When you specify multiple time, comma delimited.#5	04:00

#1

When specified 0, checking batteries for iOS devices will not be executed.

#2

This port number must be the same as the port number specified in the `httpsd.conf` file.

#3

If you specify `0`, this operation will not time out.

#4

Recommended that the collection be executed once a day and avoid to overlap between other tasks and execcution time.

#5

When specifying multiple time, each time's differences must be over one hour. Collection will not take place at collection times that occur less than one hour after another collection time.

Example

```
messaging.server.address = localhost
messaging.server.port = 9000
request.timeout.time = 5
semaphore.wait.timeout.time = 5
ios.battery.inventory.timeout.time = 60
detail.debug.log.mode = 0
communication.server.address = xxxxxxx.xxxxxxx.co.jp:26055
ios.request.getinventory.timeout.time = 1440
ios.request.wipe.timeout.time = 1440
ios.request.lock.timeout.time = 1440
ios.request.clearpasscode.timeout.time = 1440
ios.request.installappli.timeout.time = 4320
ios.request.uninstallappli.timeout.time = 4320
ios.request.unmanage.timeout.time = 1440
ios.request.applyprofile.timeout.time = 1440
ios.request.removeprofile.timeout.time = 1440
ios.inventory.collect.run.mode = time
ios.inventory.collect.run.time = 04:00
```

16.7 Messaging server setting file (SdMessagingServer.ini)

This file specifies the operating environment for the messaging server.

Format

```
[MessagingServer]
HttpPort=Android-device-listen-port-number
HttpAddress=Android-device-listen-IP-address
HttpKeepConnectTime=Android-device-Comet-connection-keep-time
HttpClosePendingTime=Android-device-reconnection-wait-time
HttpMaxConnection=maximum-number-of-Comet-connections-with-Android-devices
ManagePort=communication-server-listen-port-number
ManageAddress=communication-server-listen-IP-address
```

Setting items

The following describes the setting items and specifiable values for the messaging server setting file:

Setting item	Description	Specifiable value	Initial value
HttpPort	Specify the listen port number used for establishing TCP connections with Android devices. To change the initial value, if you omit the specification or specify a null string, listen port number `80` is used. Therefore, you must specify this item.	1 to 65535	26079
HttpAddress	Specify the listen IP address used for establishing TCP connections with Android devices. If you omit the specification or specify a null string, all IP addresses on the local computer are listened.	IPv4 address	None
HttpKeepConnectTime	Specify the time (in seconds) to maintain a Comet connection with an Android device. A connection that exceeds the specified time is disconnected, and then is reconnected with JP1/ITDM2 - SDM (Smart Device Android Agent).	1 or more (no upper limit; in seconds)	86400
HttpClosePendingTime	Specify the time to wait for a reconnection from the Android device from which a Comet connection was disconnected.	0 to 3600 (in minutes)	60
HttpMaxConnection	Specify the maximum number of simultaneous Comet connections with Android devices. If a connection request exceeding the specified value is issued, a connection is disconnected immediately after being established.	1 to 30000	10000
ManagePort	Specify the listen port number used for establishing TCP connections with the communication server. To change the initial value, if you omit the specification or specify a null string, listen	1 to 65535	26078

Setting item	Description	Specifiable value	Initial value
ManagePort	port number 9000 is used. Therefore, you must specify this item.	1 to 65535	26078
ManageAddress	Specify the listen IP address used for establishing TCP connections with the communication server. If you omit the specification or specify a null string, all IP addresses on the local computer are listened.	IPv4 address	None

Example

```
[MessagingServer]
HttpPort=26079
HttpAddress=xxx.xxx.xxx.xxx
HttpKeepConnectTime=86400
HttpClosePendingTime=60
HttpMaxConnection=10000
ManagePort=26078
ManageAddress=xxx.xxx.xxx.xxx
```

17 Messages

This chapter lists and describes messages output by JP1/ITDM2 - SDM.

17.1 Message format

JP1/ITDM2 - SDM messages consist of a message ID, message type, and message text.

The following shows the format of message IDs and message types, and the meanings of the constituent parts of a message.

Format: KNAF*pnnnnn*-*m*

KNAF

Indicate a message output from JP1/ITDM2 - SDM.

p

Indicates the component that output the message. The following table shows the correspondence between the numbers and the components:

Number	Component
0	Installer
1	Smart device manager
2	Communication server
3	Messaging server
4	JP1/ITDM2 - SDM (Smart Device Android Agent)
5	JP1/ITDM2 - SDM (Smart Device iOS Agent)
6	Command

nnnnn

Indicates the message number.

m

Indicates the message type. The following are the message types:

Message code	Type	Description
E	Error	Processing could not continue because an error occurred.
W	Warning	A warning was output, and processing continued. See the warning message to determine whether there is a problem.
I	Information	Processing ended successfully.

17.2 JP1/ITDM2 - SDM (Smart Device Manager) messages output as events

Some JP1/ITDM2 - SDM (Smart Device Manager) messages are output as events, and others are not.

JP1/ITDM2 - SDM (Smart Device Manager) messages output as events

Message ID	Output as event
KNAF100003-E	Y
KNAF100004-W	Y
KNAF100005-W	Y
KNAF120000-I	Y
KNAF120001-W	Y
KNAF120002-W	Y
KNAF120100-I	Y
KNAF120101-E	Y
KNAF120102-I	Y
KNAF120103-E	Y
KNAF120105-E	Y
KNAF120107-E	Y
KNAF120108-I	Y
KNAF120109-W	Y
KNAF120111-E	Y
KNAF120113-E	Y
KNAF120114-W	Y
KNAF120115-W	Y
KNAF120116-I	Y
KNAF120117-E	Y
KNAF120118-I	Y
KNAF120119-I	Y
KNAF120200-I	Y
KNAF120201-E	Y
KNAF120203-E	Y
KNAF120204-I	Y
KNAF120205-E	Y
KNAF120207-E	Y
KNAF120209-E	Y
KNAF120211-E	Y

Message ID	Output as event
KNAF120212-I	Y
KNAF120213-W	Y
KNAF120214-I	Y
KNAF120215-W	Y
KNAF120216-I	Y
KNAF120217-W	Y
KNAF120218-I	Y
KNAF120219-W	Y
KNAF120220-I	Y
KNAF120221-W	Y
KNAF120222-I	Y
KNAF120223-W	Y
KNAF120224-I	Y
KNAF120225-I	Y
KNAF120226-W	Y
KNAF120227-I	Y
KNAF120228-W	Y
KNAF120229-I	Y
KNAF120230-W	Y
KNAF120231-I	Y
KNAF120232-W	Y
KNAF120233-I	Y
KNAF120234-W	Y
KNAF120300-I	Y
KNAF120301-E	Y
KNAF120302-I	Y
KNAF120303-E	Y
KNAF120305-E	Y
KNAF120307-E	Y
KNAF120309-E	Y
KNAF120310-I	Y
KNAF120311-E	Y
KNAF120312-I	Y
KNAF120313-E	Y
KNAF120315-E	Y

Message ID	Output as event
KNAF120317-E	Y
KNAF120318-I	Y
KNAF120319-E	Y
KNAF120320-I	Y
KNAF120321-E	Y
KNAF120323-E	Y
KNAF120325-E	Y
KNAF120326-I	Y
KNAF120327-E	Y
KNAF120328-I	Y
KNAF120329-E	Y
KNAF120331-E	Y
KNAF120332-I	Y
KNAF120333-E	Y
KNAF120401-E	Y
KNAF120403-E	Y
KNAF120405-E	Y
KNAF120407-E	Y
KNAF120409-E	Y
KNAF120411-E	Y
KNAF120501-E	Y
KNAF120503-E	Y
KNAF120505-E	Y
KNAF120507-E	Y
KNAF120509-E	Y
KNAF120511-E	Y
KNAF120513-E	Y
KNAF120515-E	Y
KNAF120517-E	Y
KNAF120519-E	Y
KNAF120521-E	Y
KNAF120523-E	Y
KNAF120524-E	Y
KNAF120526-E	Y
KNAF120528-E	Y

Message ID	Output as event
KNAF120530-E	Y
KNAF120531-E	Y
KNAF120533-E	Y
KNAF120535-E	Y
KNAF120537-E	Y
KNAF120539-E	Y
KNAF120541-E	Y
KNAF120543-E	Y
KNAF120545-E	Y
KNAF120547-E	Y
KNAF120600-I	Y
KNAF120601-E	Y
KNAF120602-I	Y
KNAF120603-E	Y
KNAF120607-E	Y
KNAF120700-I	Y
KNAF120701-E	Y
KNAF120702-I	Y
KNAF120703-E	Y
KNAF120707-E	Y
KNAF120900-I	Y
KNAF120901-E	Y
KNAF120902-I	Y
KNAF120903-E	Y
KNAF120907-E	Y
KNAF120908-I	Y
KNAF120909-E	Y
KNAF121000-I	Y
KNAF121001-E	Y
KNAF121003-E	Y
KNAF121005-E	Y
KNAF121006-I	Y
KNAF121007-E	Y
KNAF121009-E	Y
KNAF121011-E	Y

Message ID	Output as event
KNAF121013-E	Y
KNAF121015-E	Y
KNAF121017-E	Y
KNAF121019-E	Y
KNAF121021-E	Y
KNAF121023-E	Y
KNAF121024-I	Y
KNAF121025-E	Y
KNAF121026-I	Y
KNAF121027-E	Y
KNAF121028-I	Y
KNAF121029-E	Y
KNAF121030-I	Y
KNAF121031-E	Y
KNAF121033-E	Y
KNAF121034-W	Y
KNAF121035-W	Y
KNAF121038-I	Y
KNAF121039-W	Y
KNAF121040-W	Y
KNAF121045-I	Y
KNAF121046-E	Y
KNAF121047-E	Y
KNAF121048-E	Y
KNAF121049-I	Y
KNAF121050-E	Y
KNAF121051-E	Y
KNAF121052-I	Y
KNAF121053-E	Y
KNAF121054-E	Y
KNAF130000-I	Y
KNAF130001-E	Y
KNAF130002-I	Y
KNAF130003-E	Y
KNAF130004-I	Y

Message ID	Output as event
KNAF130005-E	Y
KNAF130008-I	Y
KNAF130009-E	Y
KNAF130012-I	Y
KNAF130013-E	Y
KNAF130016-I	Y
KNAF130017-E	Y
KNAF130018-I	Y
KNAF130019-W	Y
KNAF130024-I	Y
KNAF130025-E	Y
KNAF130026-I	Y
KNAF130027-W	Y
KNAF130028-I	Y
KNAF130029-W	Y
KNAF130030-W	Y
KNAF130031-I	Y
KNAF130032-W	Y
KNAF130033-W	Y
KNAF130037-I	Y
KNAF130038-I	Y
KNAF130039-W	Y
KNAF130040-I	Y
KNAF130041-I	Y
KNAF130043-W	Y
KNAF130044-W	Y
KNAF130045-W	Y
KNAF130046-W	Y
KNAF130047-W	Y
KNAF130048-W	Y
KNAF130051-W	Y
KNAF130056-I	Y
KNAF130057-E	Y
KNAF130060-I	Y
KNAF130061-W	Y

Message ID	Output as event
KNAF130062-I	Y
KNAF130063-W	Y
KNAF130064-W	Y
KNAF130065-I	Y
KNAF130066-W	Y
KNAF130067-I	Y
KNAF130068-W	Y
KNAF130069-I	Y
KNAF130070-W	Y
KNAF130071-I	Y
KNAF130072-W	Y
KNAF130073-I	Y
KNAF130074-W	Y
KNAF130075-I	Y
KNAF130076-W	Y
KNAF130077-I	Y
KNAF130078-W	Y
KNAF130079-W	Y
KNAF130080-W	Y
KNAF130081-W	Y
KNAF130082-W	Y
KNAF130083-W	Y
KNAF130084-W	Y
KNAF130086-W	Y
KNAF130087-W	Y
KNAF130088-W	Y
KNAF130089-W	Y
KNAF130090-W	Y
KNAF130091-W	Y
KNAF190001-I	--
KNAF190002-I	--
KNAF190003-I	--
KNAF190004-E	--
KNAF190005-E	--
KNAF190006-I	--

Message ID	Output as event
KNAF190007-I	--
KNAF190008-E	--
KNAF190009-E	--

Legend:

Y: Output

---: Not output

17.3 List of JP1/ITDM2 - SDM (Smart Device Manager) messages

The following lists and describes JP1/ITDM2 - SDM (Smart Device Manager) messages.

KNAF100003-E

Failed to generate an instance. *error-description* (*instance-name*)

[Cause] The system failed to generate an instance.

[Action] Continues the process.

[Workaround] Collect troubleshooting information, and then contact customer support.

KNAF100004-W

Failed to connect to the communication server.

[Cause] The system failed to connect to the communication server.

[Action] Cancels the connection.

[Workaround] Verify that the communication server is running.

Verify that the communicationserverurl value in the file manager.properties is configured properly.

Verify that the root certificate required for connection is specified.

KNAF100005-W

Failed to send a test email message.

[Cause] The system failed to send a test email message.

[Action] Cancels email notification.

[Workaround] Check and, if necessary, revise the settings in the file testmail.properties, or verify that the destination SMTP server is specified properly.

KNAF120000-I

A change in manager.properties was detected. *key-of-the-changed-value*:[*value-before-the-change*]->[*value-after-the-change*]

KNAF120001-W

Some items in manager.properties are not defined.

item-name

[Cause] Some required definition items in manager.properties are not defined.

[Action] Cancels the execution.

[Workaround] Add necessary definitions, and then restart the service (JP1/ITDM2 - Smart Device Manager Server Service).

KNAF120002-W

The definition file contains incorrect settings. *file-name*: *item-name*

[Cause] Items in the definition file have incorrect values.

[Action] Discards the settings in the definition file and continues the processing.

[Workaround] Check and, if necessary, revise the settings in the definition file, and then restart the service (JP1/ITDM2 - Smart Device Manager Server Service).

KNAF120100-I

A user account was created. User ID = *user-ID*

KNAF120101-E

Failed to create a user account. User ID = *user-ID*

[Cause] The database service (JP1/ITDM2 - Smart Device Manager (DB Service)) is not running.

[Action] Cancels the execution.

[Workaround] Start the database service (JP1/ITDM2 - Smart Device Manager (DB Service)), and then restart the service (JP1/ITDM2 - Smart Device Manager Server Service).

If the problem persists, collect troubleshooting information, and then contact customer support.

KNAF120102-I

A user account was deleted. User ID = *user-ID*

KNAF120103-E

Failed to delete a user account. User ID = *user-ID*

[Cause] The database service (JP1/ITDM2 - Smart Device Manager (DB Service)) is not running.

[Action] Cancels the execution.

[Workaround] Start the database service (JP1/ITDM2 - Smart Device Manager (DB Service)), and then restart the service (JP1/ITDM2 - Smart Device Manager Server Service).

If the problem persists, collect troubleshooting information, and then contact customer support.

KNAF120105-E

Failed to obtain the number of user accounts.

[Cause] The database service (JP1/ITDM2 - Smart Device Manager (DB Service)) is not running.

[Action] Cancels the execution.

[Workaround] Start the database service (JP1/ITDM2 - Smart Device Manager (DB Service)), and then restart the service (JP1/ITDM2 - Smart Device Manager Server Service).

If the problem persists, collect troubleshooting information, and then contact customer support.

KNAF120107-E

Failed to obtain user account information.

[Cause] The database service (JP1/ITDM2 - Smart Device Manager (DB Service)) is not running.

[Action] Cancels the execution.

[Workaround] Start the database service (JP1/ITDM2 - Smart Device Manager (DB Service)), and then restart the service (JP1/ITDM2 - Smart Device Manager Server Service).

If the problem persists, collect troubleshooting information, and then contact customer support.

KNAF120108-I

The login was successful. User ID = *user-ID*

KNAF120109-W

The login failed. User ID = *user-ID*

[Cause]

- The user ID or password is not correct.

- The database service (JP1/ITDM2 - Smart Device Manager (DB Service)) is not running.

[Action] Cancels the execution.

[Workaround]

- Enter the correct user ID and password, and then try logging in again.

- Start the database service (JP1/ITDM2 - Smart Device Manager (DB Service)), and then restart the service (JP1/ITDM2 - Smart Device Manager Server Service).

If the problem persists, collect troubleshooting information, and then contact customer support.

KNAF120111-E

Failed to obtain role information. User ID = *user-ID*

[Cause] The database service (JP1/ITDM2 - Smart Device Manager (DB Service)) is not running.

[Action] Cancels the execution.

[Workaround] Start the database service (JP1/ITDM2 - Smart Device Manager (DB Service)), and then restart the service (JP1/ITDM2 - Smart Device Manager Server Service).

If the problem persists, collect troubleshooting information, and then contact customer support.

KNAF120113-E

Failed to obtain the list of user accounts.

[Cause] The database service (JP1/ITDM2 - Smart Device Manager (DB Service)) is not running.

[Action] Cancels the execution.

[Workaround] Start the database service (JP1/ITDM2 - Smart Device Manager (DB Service)), and then restart the service (JP1/ITDM2 - Smart Device Manager Server Service).

If the problem persists, collect troubleshooting information, and then contact customer support.

KNAF120114-W

Multiple attempts to log in failed.

[Cause] The specified maximum number of login attempts was exceeded.

[Action] Cancels the execution.

[Workaround] Enter the correct user ID and password, or contact and ask the administrator to create a user.

KNAF120115-W

A user account was locked. User ID = *user-ID*

[Cause] The user account was locked.

[Action] Cancels the execution.

[Workaround] Contact and ask a user with administrator privileges to unlock the locked user account.

If all users with administrator privileges are locked, restart the service (JP1/ITDM2 - Smart Device Manager Server Service) to unlock the users.

KNAF120116-I

A user account was changed. User ID = *user-ID*

KNAF120117-E

Failed to change a user account. User ID = *user-ID*

[Cause]

- The password is not correct, or the same password as the current password was entered for the new password.
- The database service (JP1/ITDM2 - Smart Device Manager (DB Service)) is not running.

[Action] Cancels the execution.

[Workaround]

- Specify the correct password, or provide a new password different from the current one.
- Start the database service (JP1/ITDM2 - Smart Device Manager (DB Service)), and then restart the service (JP1/ITDM2 - Smart Device Manager Server Service).

If the problem persists, collect troubleshooting information, and then contact customer support.

KNAF120118-I

A user account was unlocked. User ID = *user-ID*

KNAF120119-I

You have logged out. User ID = *user-ID*

KNAF120200-I

A smart device was imported.

KNAF120201-E

Failed to import a smart device. Error line number: *line-number*

[Cause] The system failed to import smart device information.

[Action] Cancels the execution.

[Workaround] Remove the error that occurred at the line for the specified number in the file, and then retry the import.

If the problem persists, collect troubleshooting information, and then contact customer support.

KNAF120203-E

Failed to export smart device information. *error-description*

[Cause] The system failed to export smart device information.

[Action] Cancels the execution.

[Workaround] Start the database service (JP1/ITDM2 - Smart Device Manager (DB Service)), and then restart the service (JP1/ITDM2 - Smart Device Manager Server Service).

If the problem persists, collect troubleshooting information, and then contact customer support.

KNAF120204-I

A smart device was deleted. *name*

KNAF120205-E

Failed to delete a smart device. *name*

[Cause] The database service (JP1/ITDM2 - Smart Device Manager (DB Service)) is not running.

[Action] Cancels the execution.

[Workaround] Start the database service (JP1/ITDM2 - Smart Device Manager (DB Service)), and then restart the service (JP1/ITDM2 - Smart Device Manager Server Service).

If the problem persists, collect troubleshooting information, and then contact customer support.

KNAF120207-E

Failed to obtain the number of smart devices.

[Cause] The database service (JP1/ITDM2 - Smart Device Manager (DB Service)) is not running.

[Action] Cancels the execution.

[Workaround] Start the database service (JP1/ITDM2 - Smart Device Manager (DB Service)), and then restart the service (JP1/ITDM2 - Smart Device Manager Server Service).

If the problem persists, collect troubleshooting information, and then contact customer support.

KNAF120209-E

Failed to obtain the differences from the previous day.

[Cause] The database service (JP1/ITDM2 - Smart Device Manager (DB Service)) is not running.

[Action] Cancels the execution.

[Workaround] Start the database service (JP1/ITDM2 - Smart Device Manager (DB Service)), and then restart the service (JP1/ITDM2 - Smart Device Manager Server Service).

If the problem persists, collect troubleshooting information, and then contact customer support.

KNAF120211-E

Failed to obtain smart device information.

[Cause] The database service (JP1/ITDM2 - Smart Device Manager (DB Service)) is not running.

[Action] Cancels the execution.

[Workaround] Start the database service (JP1/ITDM2 - Smart Device Manager (DB Service)), and then restart the service (JP1/ITDM2 - Smart Device Manager Server Service).

If the problem persists, collect troubleshooting information, and then contact customer support.

KNAF120212-I

The latest information was requested.

KNAF120213-W

Failed to request the latest information.

[Cause] The system failed to collect the latest information.

[Action] Cancels the execution.

[Workaround] Make sure that the target smart device is connected to the network. If the smart device is out of the service range or is not connected via Wi-Fi, the system cannot access the device.

KNAF120214-I

An initialization request was made.

KNAF120215-W

An initialization request failed.

[Cause] An initialization request failed.

[Action] Cancels the execution.

[Workaround] Make sure that the target smart device is connected to the network. If the smart device is out of the service range or is not connected via Wi-Fi, the system cannot access the device.

KNAF120216-I

A device was instructed to lock itself.

KNAF120217-W

Failed to instruct a device to lock itself.

[Cause] Lock instructions failed.

[Action] Cancels the execution.

[Workaround] Make sure that the target smart device is connected to the network. If the smart device is out of the service range or is not connected via Wi-Fi, the system cannot access the device.

KNAF120218-I

A device was instructed to lock itself and to update its password.

KNAF120219-W

Failed to instruct a device to lock itself and to update its password.

[Cause] The system failed to instruct a device to lock itself and to update its password.

[Action] Cancels the execution.

[Workaround] Make sure that the target smart device is connected to the network. If the smart device is out of the service range or is not connected via Wi-Fi, the system cannot access the device.

KNAF120220-I

A device was instructed to reset its passcode.

KNAF120221-W

Failed to instruct a device to reset its passcode.

[Cause] The system failed to instruct a device to reset its passcode.

[Action] Cancels the execution.

[Workaround] Make sure that the target smart device is connected to the network. If the smart device is out of the service range or is not connected via Wi-Fi, the system cannot access the device.

KNAF120222-I

Logs were requested.

KNAF120223-W

Failed to request logs.

[Cause] The system failed to request logs.

[Action] Cancels the execution.

[Workaround] Make sure that the target smart device is connected to the network. If the smart device is out of the service range or is not connected via Wi-Fi, the system cannot access the device.

KNAF120224-I

A device was set as an unmanaged device.

KNAF120225-I

A device was forcibly set as an unmanaged device.

KNAF120226-W

Failed to set a device as an unmanaged device.

[Cause] The system failed to set a device as an unmanaged device.

[Action] Cancels the execution.

[Workaround] Make sure that the target smart device is connected to the network. If the smart device is out of service range or is not connected via Wi-Fi, the system cannot access the device. If the system cannot access the smart device because it failed or was lost, select the "Forcibly set to unmanaged" check box.

KNAF120227-I

A security policy was applied. Policy name: *policy-name*

KNAF120228-W

Failed to apply a security policy. Policy name: *policy-name*

[Cause] The system failed to apply a security policy.

[Action] Cancels the execution.

[Workaround] Make sure that the target smart device is connected to the network. If the smart device is out of the service range or is not connected via Wi-Fi, the system cannot access the device.

KNAF120229-I

A request to apply an Android policy was made. Policy name: *policy-name*

KNAF120230-W

A request to apply an Android policy failed. Policy name: *policy-name*

[Cause] The system failed to apply an Android policy.

[Action] Cancels the execution.

[Workaround] Make sure that the target smart device is connected to the network. If the smart device is out of the service range or is not connected via Wi-Fi, the system cannot access the device.

KNAF120231-I

A request to apply an iOS profile was made. Profile name: *profile-name*

KNAF120232-W

A request to apply an iOS profile failed. Profile name: *profile-name*

[Cause] The system failed to apply an iOS profile.

[Action] Cancels the execution.

[Workaround] Make sure that the target smart device is connected to the network. If the smart device is out of the service range or is not connected via Wi-Fi, the system cannot access the device.

KNAF120233-I

A message was sent.

KNAF120234-W

Failed to send a message.

[Cause] A message transfer failed.

[Action] Cancels the execution.

[Workaround] Make sure that the target smart device is connected to the network. If the smart device is out of the service range or is not connected via Wi-Fi, the system cannot access the device.

KNAF120300-I

A security policy was created. Policy name: *policy-name*

KNAF120301-E

Failed to create a security policy. Policy name: *policy-name*

[Cause] The database service (JP1/ITDM2 - Smart Device Manager (DB Service)) is not running.

[Action] Cancels the execution.

[Workaround] Start the database service (JP1/ITDM2 - Smart Device Manager (DB Service)), and then restart the service (JP1/ITDM2 - Smart Device Manager Server Service).

If the problem persists, collect troubleshooting information, and then contact customer support.

KNAF120302-I

A security policy was removed. Policy name: *policy-name*

KNAF120303-E

Failed to remove a security policy. Policy name: *policy-name*

[Cause] The database service (JP1/ITDM2 - Smart Device Manager (DB Service)) is not running.

[Action] Cancels the execution.

[Workaround] Start the database service (JP1/ITDM2 - Smart Device Manager (DB Service)), and then restart the service (JP1/ITDM2 - Smart Device Manager Server Service).

If the problem persists, collect troubleshooting information, and then contact customer support.

KNAF120305-E

Failed to obtain security policy information.

[Cause] The database service (JP1/ITDM2 - Smart Device Manager (DB Service)) is not running.

[Action] Cancels the execution.

[Workaround] Start the database service (JP1/ITDM2 - Smart Device Manager (DB Service)), and then restart the service (JP1/ITDM2 - Smart Device Manager Server Service).

If the problem persists, collect troubleshooting information, and then contact customer support.

KNAF120307-E

Failed to obtain the number of security policies.

[Cause] The database service (JP1/ITDM2 - Smart Device Manager (DB Service)) is not running.

[Action] Cancels the execution.

[Workaround] Start the database service (JP1/ITDM2 - Smart Device Manager (DB Service)), and then restart the service (JP1/ITDM2 - Smart Device Manager Server Service).

If the problem persists, collect troubleshooting information, and then contact customer support.

KNAF120309-E

Failed to obtain the phone number list in a security policy.

[Cause] The database service (JP1/ITDM2 - Smart Device Manager (DB Service)) is not running.

[Action] Cancels the execution.

[Workaround] Start the database service (JP1/ITDM2 - Smart Device Manager (DB Service)), and then restart the service (JP1/ITDM2 - Smart Device Manager Server Service).

If the problem persists, collect troubleshooting information, and then contact customer support.

KNAF120310-I

A phone number was added to a security policy or changed in a security policy.

KNAF120311-E

Failed to add a phone number to a security policy or change it in a security policy.

[Cause] The database service (JP1/ITDM2 - Smart Device Manager (DB Service)) is not running.

[Action] Cancels the execution.

[Workaround] Start the database service (JP1/ITDM2 - Smart Device Manager (DB Service)), and then restart the service (JP1/ITDM2 - Smart Device Manager Server Service).

If the problem persists, collect troubleshooting information, and then contact customer support.

KNAF120312-I

A phone number was removed from a security policy.

KNAF120313-E

Failed to remove a phone number from a security policy.

[Cause] The database service (JP1/ITDM2 - Smart Device Manager (DB Service)) is not running.

[Action] Cancels the execution.

[Workaround] Start the database service (JP1/ITDM2 - Smart Device Manager (DB Service)), and then restart the service (JP1/ITDM2 - Smart Device Manager Server Service).

If the problem persists, collect troubleshooting information, and then contact customer support.

KNAF120315-E

Failed to obtain the number of registered phone numbers in a security policy.

[Cause] The database service (JP1/ITDM2 - Smart Device Manager (DB Service)) is not running.

[Action] Cancels the execution.

[Workaround] Start the database service (JP1/ITDM2 - Smart Device Manager (DB Service)), and then restart the service (JP1/ITDM2 - Smart Device Manager Server Service).

If the problem persists, collect troubleshooting information, and then contact customer support.

KNAF120317-E

Failed to obtain the URL list in a security policy.

[Cause] The database service (JP1/ITDM2 - Smart Device Manager (DB Service)) is not running.

[Action] Cancels the execution.

[Workaround] Start the database service (JP1/ITDM2 - Smart Device Manager (DB Service)), and then restart the service (JP1/ITDM2 - Smart Device Manager Server Service).

If the problem persists, collect troubleshooting information, and then contact customer support.

KNAF120318-I

A URL was added to, or changed in, a security policy.

KNAF120319-E

Failed to add a URL to a security policy, or failed to change it in a security policy.

[Cause] The database service (JP1/ITDM2 - Smart Device Manager (DB Service)) is not running.

[Action] Cancels the execution.

[Workaround] Start the database service (JP1/ITDM2 - Smart Device Manager (DB Service)), and then restart the service (JP1/ITDM2 - Smart Device Manager Server Service).

If the problem persists, collect troubleshooting information, and then contact customer support.

KNAF120320-I

A URL was removed from a security policy.

KNAF120321-E

Failed to remove a URL from a security policy.

[Cause] The database service (JP1/ITDM2 - Smart Device Manager (DB Service)) is not running.

[Action] Cancels the execution.

[Workaround] Start the database service (JP1/ITDM2 - Smart Device Manager (DB Service)), and then restart the service (JP1/ITDM2 - Smart Device Manager Server Service).

If the problem persists, collect troubleshooting information, and then contact customer support.

KNAF120323-E

Failed to obtain the number of registered URLs in a security policy.

[Cause] The database service (JP1/ITDM2 - Smart Device Manager (DB Service)) is not running.

[Action] Cancels the execution.

[Workaround] Start the database service (JP1/ITDM2 - Smart Device Manager (DB Service)), and then restart the service (JP1/ITDM2 - Smart Device Manager Server Service).

If the problem persists, collect troubleshooting information, and then contact customer support.

KNAF120325-E

Failed to obtain the application list in a security policy.

[Cause] The database service (JP1/ITDM2 - Smart Device Manager (DB Service)) is not running.

[Action] Cancels the execution.

[Workaround] Start the database service (JP1/ITDM2 - Smart Device Manager (DB Service)), and then restart the service (JP1/ITDM2 - Smart Device Manager Server Service).

If the problem persists, collect troubleshooting information, and then contact customer support.

KNAF120326-I

An application was added to, or changed in, a security policy.

KNAF120327-E

Failed to add an application to, or failed to change an application in, a security policy.

[Cause] The database service (JP1/ITDM2 - Smart Device Manager (DB Service)) is not running.

[Action] Cancels the execution.

[Workaround] Start the database service (JP1/ITDM2 - Smart Device Manager (DB Service)), and then restart the service (JP1/ITDM2 - Smart Device Manager Server Service).

If the problem persists, collect troubleshooting information, and then contact customer support.

KNAF120328-I

An application was removed from a security policy.

KNAF120329-E

Failed to remove an application from a security policy.

[Cause] The database service (JP1/ITDM2 - Smart Device Manager (DB Service)) is not running.

[Action] Cancels the execution.

[Workaround] Start the database service (JP1/ITDM2 - Smart Device Manager (DB Service)), and then restart the service (JP1/ITDM2 - Smart Device Manager Server Service).

If the problem persists, collect troubleshooting information, and then contact customer support.

KNAF120331-E

Failed to obtain the number of registered applications in a security policy.

[Cause] The database service (JP1/ITDM2 - Smart Device Manager (DB Service)) is not running.

[Action] Cancels the execution.

[Workaround] Start the database service (JP1/ITDM2 - Smart Device Manager (DB Service)), and then restart the service (JP1/ITDM2 - Smart Device Manager Server Service).

If the problem persists, collect troubleshooting information, and then contact customer support.

KNAF120332-I

A security policy was changed.

KNAF120333-E

Failed to change a security policy.

[Cause] The database service (JP1/ITDM2 - Smart Device Manager (DB Service)) is not running.

[Action] Cancels the execution.

[Workaround] Start the database service (JP1/ITDM2 - Smart Device Manager (DB Service)), and then restart the service (JP1/ITDM2 - Smart Device Manager Server Service).

If the problem persists, collect troubleshooting information, and then contact customer support.

KNAF120401-E

An event was deleted.

[Cause] The database service (JP1/ITDM2 - Smart Device Manager (DB Service)) is not running.

[Action] Cancels the execution.

[Workaround] Start the database service (JP1/ITDM2 - Smart Device Manager (DB Service)), and then restart the service (JP1/ITDM2 - Smart Device Manager Server Service).

If the problem persists, collect troubleshooting information, and then contact customer support.

KNAF120403-E

Failed to export a list of events.

[Cause] The database service (JP1/ITDM2 - Smart Device Manager (DB Service)) is not running.

[Action] Cancels the execution.

[Workaround] Start the database service (JP1/ITDM2 - Smart Device Manager (DB Service)), and then restart the service (JP1/ITDM2 - Smart Device Manager Server Service).

If the problem persists, collect troubleshooting information, and then contact customer support.

KNAF120405-E

Failed to obtain the number of events.

[Cause] The database service (JP1/ITDM2 - Smart Device Manager (DB Service)) is not running.

[Action] Cancels the execution.

[Workaround] Start the database service (JP1/ITDM2 - Smart Device Manager (DB Service)), and then restart the service (JP1/ITDM2 - Smart Device Manager Server Service).

If the problem persists, collect troubleshooting information, and then contact customer support.

KNAF120407-E

Failed to obtain a list of event information.

[Cause] The database service (JP1/ITDM2 - Smart Device Manager (DB Service)) is not running.

[Action] Cancels the execution.

[Workaround] Start the database service (JP1/ITDM2 - Smart Device Manager (DB Service)), and then restart the service (JP1/ITDM2 - Smart Device Manager Server Service).

If the problem persists, collect troubleshooting information, and then contact customer support.

KNAF120409-E

Failed to add or change event information.

[Cause] The database service (JP1/ITDM2 - Smart Device Manager (DB Service)) is not running.

[Action] Cancels the execution.

[Workaround] Start the database service (JP1/ITDM2 - Smart Device Manager (DB Service)), and then restart the service (JP1/ITDM2 - Smart Device Manager Server Service).

If the problem persists, collect troubleshooting information, and then contact customer support.

KNAF120411-E

Failed to obtain an alert level.

[Cause] The database service (JP1/ITDM2 - Smart Device Manager (DB Service)) is not running.

[Action] Cancels the execution.

[Workaround] Start the database service (JP1/ITDM2 - Smart Device Manager (DB Service)), and then restart the service (JP1/ITDM2 - Smart Device Manager Server Service).

If the problem persists, collect troubleshooting information, and then contact customer support.

KNAF120501-E

Failed to update inventory information.

[Cause] The database service (JP1/ITDM2 - Smart Device Manager (DB Service)) is not running.

[Action] Cancels the execution.

[Workaround] Start the database service (JP1/ITDM2 - Smart Device Manager (DB Service)), and then restart the service (JP1/ITDM2 - Smart Device Manager Server Service).

If the problem persists, collect troubleshooting information, and then contact customer support.

KNAF120503-E

Failed to delete inventory information.

[Cause] The database service (JP1/ITDM2 - Smart Device Manager (DB Service)) is not running.

[Action] Cancels the execution.

[Workaround] Start the database service (JP1/ITDM2 - Smart Device Manager (DB Service)), and then restart the service (JP1/ITDM2 - Smart Device Manager Server Service).

If the problem persists, collect troubleshooting information, and then contact customer support.

KNAF120505-E

Failed to update call history information.

[Cause] The database service (JP1/ITDM2 - Smart Device Manager (DB Service)) is not running.

[Action] Cancels the execution.

[Workaround] Start the database service (JP1/ITDM2 - Smart Device Manager (DB Service)), and then restart the service (JP1/ITDM2 - Smart Device Manager Server Service).

If the problem persists, collect troubleshooting information, and then contact customer support.

KNAF120507-E

Failed to obtain call history information.

[Cause] The database service (JP1/ITDM2 - Smart Device Manager (DB Service)) is not running.

[Action] Cancels the execution.

[Workaround] Start the database service (JP1/ITDM2 - Smart Device Manager (DB Service)), and then restart the service (JP1/ITDM2 - Smart Device Manager Server Service).

If the problem persists, collect troubleshooting information, and then contact customer support.

KNAF120509-E

Failed to obtain the number of records of call history information.

[Cause] The database service (JP1/ITDM2 - Smart Device Manager (DB Service)) is not running.

[Action] Cancels the execution.

[Workaround] Start the database service (JP1/ITDM2 - Smart Device Manager (DB Service)), and then restart the service (JP1/ITDM2 - Smart Device Manager Server Service).

If the problem persists, collect troubleshooting information, and then contact customer support.

KNAF120511-E

Failed to update URL browsing history information.

[Cause] The database service (JP1/ITDM2 - Smart Device Manager (DB Service)) is not running.

[Action] Cancels the execution.

[Workaround] Start the database service (JP1/ITDM2 - Smart Device Manager (DB Service)), and then restart the service (JP1/ITDM2 - Smart Device Manager Server Service).

If the problem persists, collect troubleshooting information, and then contact customer support.

KNAF120513-E

Failed to obtain URL browsing history information.

[Cause] The database service (JP1/ITDM2 - Smart Device Manager (DB Service)) is not running.

[Action] Cancels the execution.

[Workaround] Start the database service (JP1/ITDM2 - Smart Device Manager (DB Service)), and then restart the service (JP1/ITDM2 - Smart Device Manager Server Service).

If the problem persists, collect troubleshooting information, and then contact customer support.

KNAF120515-E

Failed to obtain the number of records of URL browsing history.

[Cause] The database service (JP1/ITDM2 - Smart Device Manager (DB Service)) is not running.

[Action] Cancels the execution.

[Workaround] Start the database service (JP1/ITDM2 - Smart Device Manager (DB Service)), and then restart the service (JP1/ITDM2 - Smart Device Manager Server Service).

If the problem persists, collect troubleshooting information, and then contact customer support.

KNAF120517-E

Failed to create information about installed applications.

[Cause] The database service (JP1/ITDM2 - Smart Device Manager (DB Service)) is not running.

[Action] Cancels the execution.

[Workaround] Start the database service (JP1/ITDM2 - Smart Device Manager (DB Service)), and then restart the service (JP1/ITDM2 - Smart Device Manager Server Service).

If the problem persists, collect troubleshooting information, and then contact customer support.

KNAF120519-E

Failed to obtain the number of records of information about installed applications.

[Cause] The database service (JP1/ITDM2 - Smart Device Manager (DB Service)) is not running.

[Action] Cancels the execution.

[Workaround] Start the database service (JP1/ITDM2 - Smart Device Manager (DB Service)), and then restart the service (JP1/ITDM2 - Smart Device Manager Server Service).

If the problem persists, collect troubleshooting information, and then contact customer support.

KNAF120521-E

Failed to obtain a list of information about installed applications.

[Cause] The database service (JP1/ITDM2 - Smart Device Manager (DB Service)) is not running.

[Action] Cancels the execution.

[Workaround] Start the database service (JP1/ITDM2 - Smart Device Manager (DB Service)), and then restart the service (JP1/ITDM2 - Smart Device Manager Server Service).

If the problem persists, collect troubleshooting information, and then contact customer support.

KNAF120523-E

Failed to create information about running applications.

[Cause] The database service (JP1/ITDM2 - Smart Device Manager (DB Service)) is not running.

[Action] Cancels the execution.

[Workaround] Start the database service (JP1/ITDM2 - Smart Device Manager (DB Service)), and then restart the service (JP1/ITDM2 - Smart Device Manager Server Service).

If the problem persists, collect troubleshooting information, and then contact customer support.

KNAF120524-E

Failed to delete information about running applications.

[Cause] The database service (JP1/ITDM2 - Smart Device Manager (DB Service)) is not running.

[Action] Cancels the execution.

[Workaround] Start the database service (JP1/ITDM2 - Smart Device Manager (DB Service)), and then restart the service (JP1/ITDM2 - Smart Device Manager Server Service).

If the problem persists, collect troubleshooting information, and then contact customer support.

KNAF120526-E

Failed to obtain the number of records of information about running applications.

[Cause] The database service (JP1/ITDM2 - Smart Device Manager (DB Service)) is not running.

[Action] Cancels the execution.

[Workaround] Start the database service (JP1/ITDM2 - Smart Device Manager (DB Service)), and then restart the service (JP1/ITDM2 - Smart Device Manager Server Service).

If the problem persists, collect troubleshooting information, and then contact customer support.

KNAF120528-E

Failed to obtain a list of information about running applications.

[Cause] The database service (JP1/ITDM2 - Smart Device Manager (DB Service)) is not running.

[Action] Cancels the execution.

[Workaround] Start the database service (JP1/ITDM2 - Smart Device Manager (DB Service)), and then restart the service (JP1/ITDM2 - Smart Device Manager Server Service).

If the problem persists, collect troubleshooting information, and then contact customer support.

KNAF120530-E

Failed to create information about running services.

[Cause] The database service (JP1/ITDM2 - Smart Device Manager (DB Service)) is not running.

[Action] Cancels the execution.

[Workaround] Start the database service (JP1/ITDM2 - Smart Device Manager (DB Service)), and then restart the service (JP1/ITDM2 - Smart Device Manager Server Service).

If the problem persists, collect troubleshooting information, and then contact customer support.

KNAF120531-E

Failed to delete information about running services.

[Cause] The database service (JP1/ITDM2 - Smart Device Manager (DB Service)) is not running.

[Action] Cancels the execution.

[Workaround] Start the database service (JP1/ITDM2 - Smart Device Manager (DB Service)), and then restart the service (JP1/ITDM2 - Smart Device Manager Server Service).

If the problem persists, collect troubleshooting information, and then contact customer support.

KNAF120533-E

Failed to obtain the number of records of information about running services.

[Cause] The database service (JP1/ITDM2 - Smart Device Manager (DB Service)) is not running.

[Action] Cancels the execution.

[Workaround] Start the database service (JP1/ITDM2 - Smart Device Manager (DB Service)), and then restart the service (JP1/ITDM2 - Smart Device Manager Server Service).

If the problem persists, collect troubleshooting information, and then contact customer support.

KNAF120535-E

Failed to obtain a list of information about running services.

[Cause] The database service (JP1/ITDM2 - Smart Device Manager (DB Service)) is not running.

[Action] Cancels the execution.

[Workaround] Start the database service (JP1/ITDM2 - Smart Device Manager (DB Service)), and then restart the service (JP1/ITDM2 - Smart Device Manager Server Service).

If the problem persists, collect troubleshooting information, and then contact customer support.

KNAF120537-E

Failed to create GPS history information.

[Cause] The database service (JP1/ITDM2 - Smart Device Manager (DB Service)) is not running.

[Action] Cancels the execution.

[Workaround] Start the database service (JP1/ITDM2 - Smart Device Manager (DB Service)), and then restart the service (JP1/ITDM2 - Smart Device Manager Server Service).

If the problem persists, collect troubleshooting information, and then contact customer support.

KNAF120539-E

Failed to obtain the number of records of GPS history information.

[Cause] The database service (JP1/ITDM2 - Smart Device Manager (DB Service)) is not running.

[Action] Cancels the execution.

[Workaround] Start the database service (JP1/ITDM2 - Smart Device Manager (DB Service)), and then restart the service (JP1/ITDM2 - Smart Device Manager Server Service).

If the problem persists, collect troubleshooting information, and then contact customer support.

KNAF120541-E

Failed to obtain a list of GPS history information.

[Cause] The database service (JP1/ITDM2 - Smart Device Manager (DB Service)) is not running.

[Action] Cancels the execution.

[Workaround] Start the database service (JP1/ITDM2 - Smart Device Manager (DB Service)), and then restart the service (JP1/ITDM2 - Smart Device Manager Server Service).

If the problem persists, collect troubleshooting information, and then contact customer support.

KNAF120543-E

Failed to create Bluetooth history information.

[Cause] The database service (JP1/ITDM2 - Smart Device Manager (DB Service)) is not running.

[Action] Cancels the execution.

[Workaround] Start the database service (JP1/ITDM2 - Smart Device Manager (DB Service)), and then restart the service (JP1/ITDM2 - Smart Device Manager Server Service).

If the problem persists, collect troubleshooting information, and then contact customer support.

KNAF120545-E

Failed to obtain the number of records of Bluetooth history information.

[Cause] The database service (JP1/ITDM2 - Smart Device Manager (DB Service)) is not running.

[Action] Cancels the execution.

[Workaround] Start the database service (JP1/ITDM2 - Smart Device Manager (DB Service)), and then restart the service (JP1/ITDM2 - Smart Device Manager Server Service).

If the problem persists, collect troubleshooting information, and then contact customer support.

KNAF120547-E

Failed to obtain a list of Bluetooth history information.

[Cause] The database service (JP1/ITDM2 - Smart Device Manager (DB Service)) is not running.

[Action] Cancels the execution.

[Workaround] Start the database service (JP1/ITDM2 - Smart Device Manager (DB Service)), and then restart the service (JP1/ITDM2 - Smart Device Manager Server Service).

If the problem persists, collect troubleshooting information, and then contact customer support.

KNAF120600-I

Provisioning information for Android was created.

KNAF120601-E

Failed to create provisioning information for Android.

[Cause] The database service (JP1/ITDM2 - Smart Device Manager (DB Service)) is not running.

[Action] Cancels the execution.

[Workaround] Start the database service (JP1/ITDM2 - Smart Device Manager (DB Service)), and then restart the service (JP1/ITDM2 - Smart Device Manager Server Service).

If the problem persists, collect troubleshooting information, and then contact customer support.

KNAF120602-I

Provisioning information for Android was deleted.

KNAF120603-E

Failed to delete provisioning information for Android.

[Cause] The database service (JP1/ITDM2 - Smart Device Manager (DB Service)) is not running.

[Action] Cancels the execution.

[Workaround] Start the database service (JP1/ITDM2 - Smart Device Manager (DB Service)), and then restart the service (JP1/ITDM2 - Smart Device Manager Server Service).

If the problem persists, collect troubleshooting information, and then contact customer support.

KNAF120607-E

Failed to obtain a list of provisioning information for Android.

[Cause] The database service (JP1/ITDM2 - Smart Device Manager (DB Service)) is not running.

[Action] Cancels the execution.

[Workaround] Start the database service (JP1/ITDM2 - Smart Device Manager (DB Service)), and then restart the service (JP1/ITDM2 - Smart Device Manager Server Service).

If the problem persists, collect troubleshooting information, and then contact customer support.

KNAF120700-I

Provisioning information for iOS was created.

KNAF120701-E

Failed to create provisioning information for iOS.

[Cause] The database service (JP1/ITDM2 - Smart Device Manager (DB Service)) is not running.

[Action] Cancels the execution.

[Workaround] Start the database service (JP1/ITDM2 - Smart Device Manager (DB Service)), and then restart the service (JP1/ITDM2 - Smart Device Manager Server Service).

If the problem persists, collect troubleshooting information, and then contact customer support.

KNAF120702-I

Provisioning information for iOS was deleted.

KNAF120703-E

Failed to delete provisioning information for iOS.

[Cause] The database service (JP1/ITDM2 - Smart Device Manager (DB Service)) is not running.

[Action] Cancels the execution.

[Workaround] Start the database service (JP1/ITDM2 - Smart Device Manager (DB Service)), and then restart the service (JP1/ITDM2 - Smart Device Manager Server Service).

If the problem persists, collect troubleshooting information, and then contact customer support.

KNAF120707-E

Failed to obtain a list of provisioning information for iOS.

[Cause] The database service (JP1/ITDM2 - Smart Device Manager (DB Service)) is not running.

[Action] Cancels the execution.

[Workaround] Start the database service (JP1/ITDM2 - Smart Device Manager (DB Service)), and then restart the service (JP1/ITDM2 - Smart Device Manager Server Service).

If the problem persists, collect troubleshooting information, and then contact customer support.

KNAF120900-I

Policy profile information was created.

KNAF120901-E

Failed to create policy profile information.

[Cause] The database service (JP1/ITDM2 - Smart Device Manager (DB Service)) is not running.

[Action] Cancels the execution.

[Workaround] Start the database service (JP1/ITDM2 - Smart Device Manager (DB Service)), and then restart the service (JP1/ITDM2 - Smart Device Manager Server Service).

If the problem persists, collect troubleshooting information, and then contact customer support.

KNAF120902-I

Policy profile information was deleted.

KNAF120903-E

Failed to delete policy profile information.

[Cause] The database service (JP1/ITDM2 - Smart Device Manager (DB Service)) is not running.

[Action] Cancels the execution.

[Workaround] Start the database service (JP1/ITDM2 - Smart Device Manager (DB Service)), and then restart the service (JP1/ITDM2 - Smart Device Manager Server Service).

If the problem persists, collect troubleshooting information, and then contact customer support.

KNAF120907-E

Failed to obtain a list of policy profile information.

[Cause] The database service (JP1/ITDM2 - Smart Device Manager (DB Service)) is not running.

[Action] Cancels the execution.

[Workaround] Start the database service (JP1/ITDM2 - Smart Device Manager (DB Service)), and then restart the service (JP1/ITDM2 - Smart Device Manager Server Service).

If the problem persists, collect troubleshooting information, and then contact customer support.

KNAF120908-I

Policy profile information was changed.

KNAF120909-E

Failed to change policy profile information.

[Cause] The database service (JP1/ITDM2 - Smart Device Manager (DB Service)) is not running.

[Action] Cancels the execution.

[Workaround] Start the database service (JP1/ITDM2 - Smart Device Manager (DB Service)), and then restart the service (JP1/ITDM2 - Smart Device Manager Server Service).

If the problem persists, collect troubleshooting information, and then contact customer support.

KNAF121000-I

A distributed application was removed. Application name: *application-name*

KNAF121001-E

Failed to remove a distributed application. Application name: *application-name*

[Cause] The database service (JP1/ITDM2 - Smart Device Manager (DB Service)) is not running.

[Action] Cancels the execution.

[Workaround] Start the database service (JP1/ITDM2 - Smart Device Manager (DB Service)), and then restart the service (JP1/ITDM2 - Smart Device Manager Server Service).

If the problem persists, collect troubleshooting information, and then contact customer support.

KNAF121003-E

Failed to obtain the number of distributed applications.

[Cause] The database service (JP1/ITDM2 - Smart Device Manager (DB Service)) is not running.

[Action] Cancels the execution.

[Workaround] Start the database service (JP1/ITDM2 - Smart Device Manager (DB Service)), and then restart the service (JP1/ITDM2 - Smart Device Manager Server Service).

If the problem persists, collect troubleshooting information, and then contact customer support.

KNAF121005-E

Failed to obtain distributed application information.

[Cause] The database service (JP1/ITDM2 - Smart Device Manager (DB Service)) is not running.

[Action] Cancels the execution.

[Workaround] Start the database service (JP1/ITDM2 - Smart Device Manager (DB Service)), and then restart the service (JP1/ITDM2 - Smart Device Manager Server Service).

If the problem persists, collect troubleshooting information, and then contact customer support.

KNAF121006-I

A distributed application was added. Application name: *application-name*

KNAF121007-E

Failed to add a distributed application. Application name: *application-name*

[Cause] The database service (JP1/ITDM2 - Smart Device Manager (DB Service)) is not running.

[Action] Cancels the execution.

[Workaround] Start the database service (JP1/ITDM2 - Smart Device Manager (DB Service)), and then restart the service (JP1/ITDM2 - Smart Device Manager Server Service).

If the problem persists, collect troubleshooting information, and then contact customer support.

KNAF121009-E

Failed to delete the state of a distributed application. *application-name*

[Cause] The database service (JP1/ITDM2 - Smart Device Manager (DB Service)) is not running.

[Action] Cancels the execution.

[Workaround] Start the database service (JP1/ITDM2 - Smart Device Manager (DB Service)), and then restart the service (JP1/ITDM2 - Smart Device Manager Server Service).

If the problem persists, collect troubleshooting information, and then contact customer support.

KNAF121011-E

Failed to obtain the number of states of distributed applications.

[Cause] The database service (JP1/ITDM2 - Smart Device Manager (DB Service)) is not running.

[Action] Cancels the execution.

[Workaround] Start the database service (JP1/ITDM2 - Smart Device Manager (DB Service)), and then restart the service (JP1/ITDM2 - Smart Device Manager Server Service).

If the problem persists, collect troubleshooting information, and then contact customer support.

KNAF121013-E

Failed to obtain state information about a distributed application.

[Cause] The database service (JP1/ITDM2 - Smart Device Manager (DB Service)) is not running.

[Action] Cancels the execution.

[Workaround] Start the database service (JP1/ITDM2 - Smart Device Manager (DB Service)), and then restart the service (JP1/ITDM2 - Smart Device Manager Server Service).

If the problem persists, collect troubleshooting information, and then contact customer support.

KNAF121015-E

Failed to add the state information about a distributed application. *application-name*

[Cause] The database service (JP1/ITDM2 - Smart Device Manager (DB Service)) is not running.

[Action] Cancels the execution.

[Workaround] Start the database service (JP1/ITDM2 - Smart Device Manager (DB Service)), and then restart the service (JP1/ITDM2 - Smart Device Manager Server Service).

If the problem persists, collect troubleshooting information, and then contact customer support.

KNAF121017-E

Failed to delete application data. Application name: *application-name*

[Cause] The database service (JP1/ITDM2 - Smart Device Manager (DB Service)) is not running.

[Action] Cancels the execution.

[Workaround] Start the database service (JP1/ITDM2 - Smart Device Manager (DB Service)), and then restart the service (JP1/ITDM2 - Smart Device Manager Server Service).

If the problem persists, collect troubleshooting information, and then contact customer support.

KNAF121019-E

Failed to obtain the number of application data records.

[Cause] The database service (JP1/ITDM2 - Smart Device Manager (DB Service)) is not running.

[Action] Cancels the execution.

[Workaround] Start the database service (JP1/ITDM2 - Smart Device Manager (DB Service)), and then restart the service (JP1/ITDM2 - Smart Device Manager Server Service).

If the problem persists, collect troubleshooting information, and then contact customer support.

KNAF121021-E

Failed to obtain application data information.

[Cause] The database service (JP1/ITDM2 - Smart Device Manager (DB Service)) is not running.

[Action] Cancels the execution.

[Workaround] Start the database service (JP1/ITDM2 - Smart Device Manager (DB Service)), and then restart the service (JP1/ITDM2 - Smart Device Manager Server Service).

If the problem persists, collect troubleshooting information, and then contact customer support.

KNAF121023-E

Failed to register application data information. Application name: *application-name*

[Cause] The database service (JP1/ITDM2 - Smart Device Manager (DB Service)) is not running.

[Action] Cancels the execution.

[Workaround] Start the database service (JP1/ITDM2 - Smart Device Manager (DB Service)), and then restart the service (JP1/ITDM2 - Smart Device Manager Server Service).

If the problem persists, collect troubleshooting information, and then contact customer support.

KNAF121024-I

An application was distributed.

KNAF121025-E

Failed to distribute an application.

[Cause] The database service (JP1/ITDM2 - Smart Device Manager (DB Service)) is not running.

[Action] Cancels the execution.

[Workaround] Start the database service (JP1/ITDM2 - Smart Device Manager (DB Service)), and then restart the service (JP1/ITDM2 - Smart Device Manager Server Service).

If the problem persists, collect troubleshooting information, and then contact customer support.

KNAF121026-I

A request to install an application was made.

KNAF121027-E

A request to install an application failed.

[Cause] The database service (JP1/ITDM2 - Smart Device Manager (DB Service)) is not running.

[Action] Cancels the execution.

[Workaround] Start the database service (JP1/ITDM2 - Smart Device Manager (DB Service)), and then restart the service (JP1/ITDM2 - Smart Device Manager Server Service).

If the problem persists, collect troubleshooting information, and then contact customer support.

KNAF121028-I

A request to remove an application was made.

KNAF121029-E

A request to remove an application failed.

[Cause] The database service (JP1/ITDM2 - Smart Device Manager (DB Service)) is not running.

[Action] Cancels the execution.

[Workaround] Start the database service (JP1/ITDM2 - Smart Device Manager (DB Service)), and then restart the service (JP1/ITDM2 - Smart Device Manager Server Service).

If the problem persists, collect troubleshooting information, and then contact customer support.

KNAF121030-I

A distributed application was changed.

KNAF121031-E

Failed to register a distributed application.

[Cause] The database service (JP1/ITDM2 - Smart Device Manager (DB Service)) is not running.

[Action] Cancels the execution.

[Workaround] Start the database service (JP1/ITDM2 - Smart Device Manager (DB Service)), and then restart the service (JP1/ITDM2 - Smart Device Manager Server Service).

If the problem persists, collect troubleshooting information, and then contact customer support.

KNAF121033-E

Failed to change the state information about a distributed application.

[Cause] The database service (JP1/ITDM2 - Smart Device Manager (DB Service)) is not running.

[Action] Cancels the execution.

[Workaround] Start the database service (JP1/ITDM2 - Smart Device Manager (DB Service)), and then restart the service (JP1/ITDM2 - Smart Device Manager Server Service).

If the problem persists, collect troubleshooting information, and then contact customer support.

KNAF121034-W

Failed to install an application.

[Cause] The device sends error an message.

[Action] Cancels the execution.

[Workaround] Refer the error message from the device.

KNAF121035-W

Failed to remove an application.

[Cause] The device sends error an message.

[Action] Cancels the execution.

[Workaround] Refer the error message from the device.

KNAF121038-I

A request to remove an applied iOS profile was made. Profile name: *profile-name*

KNAF121039-W

A request to remove an applied iOS profile failed. Profile name: *profile-name*

[Cause] The database service (JP1/ITDM2 - Smart Device Manager (DB Service)) is not running.

[Action] Cancels the execution.

[Workaround] Start the database service (JP1/ITDM2 - Smart Device Manager (DB Service)), and then restart the service (JP1/ITDM2 - Smart Device Manager Server Service).

If the problem persists, collect troubleshooting information, and then contact customer support.

KNAF121040-W

A request to remove an applied iOS profile was not made. Profile name: *profile-name*

[Cause] Only 1 iOS profile is being applied to the device.

[Action] Cancels the execution.

[Workaround] Retry after applying 2 or more iOS profiles to the device.

KNAF121045-I

The sdmioutils importdeliverypermit command finished successfully. *distribution-permission-definition-file-path number-of-lines*

KNAF121046-E

An error occurred during execution of the sdmioutils importdeliverypermit command. *distribution-permission-definition-file-path error-line-number*

[Cause] The format of the distribution permission definition file is invalid.

[Action] Cancels the execution.

[Workaround] Eliminate the cause of the error in the specified row in the file, and execute the sdmioutils importdeliverypermit command again.

If the problem persists, contact customer service, and be prepared to collect and provide troubleshooting information.

KNAF121047-E

An error occurred during execution of the sdmioutils importdeliverypermit command. *distribution-permission-definition-file-path error-line-number distributed-application-name*(*version*)*-or-distribution-permission-target-name*

[Cause] The application or the target allowed to be distributed specified either in the distribution permission definition file or for the command argument cannot be found.

[Action] Cancels the execution.

[Workaround] Eliminate the cause of the error, and execute the sdmioutils importdeliverypermit command again.

If the problem persists, contact customer service, and be prepared to collect and provide troubleshooting information.

KNAF121048-E

An error occurred during execution of the sdmioutils importdeliverypermit command. *distribution-permission-definition-file-path*

[Cause] The database service (JP1/ITDM2 - Smart Device Manager (DB Service)) is not running.

[Action] Cancels the execution.

[Workaround] Start the database service (JP1/ITDM2 - Smart Device Manager (DB Service)), and then restart the service (JP1/ITDM2 - Smart Device Manager Server Service).

If the problem persists, collect troubleshooting information, and then contact customer support.

KNAF121049-I

The sdmioutils exportdeliverypermit command finished successfully. *distribution-permission-definition-file-path number-of-lines*

KNAF121050-E

An error occurred during execution of the sdmioutils exportdeliverypermit command. *distribution-permission-definition-file-path*

[Cause] The database service (JP1/ITDM2 - Smart Device Manager (DB Service)) is not running.

[Action] Cancels the execution.

[Workaround] Start the database service (JP1/ITDM2 - Smart Device Manager (DB Service)), and then restart the service (JP1/ITDM2 - Smart Device Manager Server Service).

If the problem persists, collect troubleshooting information, and then contact customer support.

KNAF121051-E

An error occurred during execution of the sdmioutils exportdeliverypermit command. *distribution-permission-definition-file-path distributed-application-name*(*version*)*-or-distribution-permission-target-name*

[Cause] The application or the target allowed to be distributed specified for the command argument cannot be found.

[Action] Cancels the execution.

[Workaround] Eliminate the cause of the error, and execute the sdmioutils exportdeliverypermit command again.

If the problem persists, contact customer service, and be prepared to collect and provide troubleshooting information.

KNAF121052-I

The sdmioutils deletedeliverypermit command finished successfully. *number-of-lines*

KNAF121053-E

An error occurred during execution of the sdmioutils deletedeliverypermit command. *distribution-permission-definition-file-path error-line-number distributed-application-name*(*version*)*-or-distribution-permission-target-name*

[Cause] The application or the target allowed to be distributed specified for the command argument cannot be found.

[Action] Cancels the execution.

[Workaround] Eliminate the cause of the error, and execute the sdmioutils deletedeliverypermit command again.

If the problem persists, contact customer service, and be prepared to collect and provide troubleshooting information.

KNAF121054-E

An error occurred during execution of the sdmioutils deletedeliverypermit command.

[Cause] The database service (JP1/ITDM2 - Smart Device Manager (DB Service)) is not running.

[Action] Cancels the execution.

[Workaround] Start the database service (JP1/ITDM2 - Smart Device Manager (DB Service)), and then restart the service (JP1/ITDM2 - Smart Device Manager Server Service).

If the problem persists, collect troubleshooting information, and then contact customer support.

KNAF130000-I

Detailed information was updated.

KNAF130001-E

Failed to update detailed information.

[Cause] The system failed to update detailed information.

[Action] Continues the process.

[Workaround] Collect troubleshooting information, and then contact customer support.

KNAF130002-I

Bluetooth connection information was updated.

KNAF130003-E

Failed to update Bluetooth connection information.

[Cause] The system failed to update Bluetooth connection information.

[Action] Continues the process.

[Workaround] Collect troubleshooting information, and then contact customer support.

KNAF130004-I

Security of the call history was validated.

KNAF130005-E

Failed to validate the security of the call history.

[Cause] The system failed to validate the security of the call history.

[Action] Continues the process.

[Workaround] Collect troubleshooting information, and then contact customer support.

KNAF130008-I

Security of application information was validated.

KNAF130009-E

Failed to validate the security of application information.

[Cause] The system failed to validate the security of application information.

[Action] Continues the process.

[Workaround] Collect troubleshooting information, and then contact customer support.

KNAF130012-I

Security of the Web browsing history was validated.

KNAF130013-E

Failed to validate the security of the Web browsing history.
[Cause] The system failed to validate the security of the Web browsing history.
[Action] Continues the process.
[Workaround] Collect troubleshooting information, and then contact customer support.

KNAF130016-I

Information for which the retention period expired was deleted.

KNAF130017-E

Failed to delete information for which the retention period expired.
[Cause] The system failed to delete information for which the retention period expired.
[Action] Continues the process.
[Workaround] Collect troubleshooting information, and then contact customer support.

KNAF130018-I

The severity management table was updated.

KNAF130019-W

Failed to update the severity management table.
[Cause] The system failed to update the severity management table.
[Action] Continues the process.
[Workaround] Collect troubleshooting information, and then contact customer support.

KNAF130024-I

The security policy of detailed information was validated.

KNAF130025-E

Failed to validate the security policy of detailed information.
[Cause] The system failed to validate the security policy of detailed information.
[Action] Continues the process.
[Workaround] Collect troubleshooting information, and then contact customer support.

KNAF130026-I

A call was made to an authorized phone number. Phone number: *phone-number*

KNAF130027-W

A call was made to an unauthorized phone number. Phone number: *phone-number*
[Cause] A violation was found during the validation of the security policy.
[Action] Continues the process.

[Workaround] Take action according to the applicable security policy.

KNAF130028-I

Installation is allowed. Application name: *application-name*

KNAF130029-W

Installation is prohibited. Application name: *application-name*

[Cause] A violation was found during the validation of the security policy.

[Action] Continues the process.

[Workaround] Take action according to the applicable security policy.

KNAF130030-W

An application which is not in the security list has been installed. Application name: *application-name*

[Cause] A violation was found during the validation of the security policy.

[Action] Continues the process.

[Workaround] Take action according to the applicable security policy.

KNAF130031-I

Site browsing is allowed. URL: *URL*

KNAF130032-W

Site browsing is prohibited. URL: *URL*

[Cause] A violation was found during the validation of the security policy.

[Action] Continues the process.

[Workaround] Take action according to the applicable security policy.

KNAF130033-W

You are browsing a website which is not in the security list.

[Cause] A violation was found during the validation of the security policy.

[Action] Continues the process.

[Workaround] Take action according to the applicable security policy.

KNAF130037-I

An application was installed.

KNAF130038-I

An application was uninstalled.

KNAF130039-W

A connection to a new Bluetooth device was established. Device name: *device-name*

[Cause] A violation was found during the validation of the security policy.
[Action] Continues the process.
[Workaround] Take action according to the applicable security policy.

KNAF130040-I

A connection to a Bluetooth device was removed. Device name: *device-name*

KNAF130041-I

Detailed information was updated.

KNAF130043-W

IMEI/MEID information was changed. Changed from: *changed-from* Changed to: *changed-to*
[Cause] A violation was found during the validation of the security policy.
[Action] Continues the process.
[Workaround] Take action according to the applicable security policy.

KNAF130044-W

OS version information was changed. Changed from: *changed-from* Changed to: *changed-to*
[Cause] A violation was found during the validation of the security policy.
[Action] Continues the process.
[Workaround] Take action according to the applicable security policy.

KNAF130045-W

ICCID information was changed. Changed from: *changed-from* Changed to: *changed-to*
[Cause] A violation was found during the validation of the security policy.
[Action] Continues the process.
[Workaround] Take action according to the applicable security policy.

KNAF130046-W

An SD card is being used.
[Cause] A violation was found during the validation of the security policy.
[Action] Continues the process.
[Workaround] Take action according to the applicable security policy.

KNAF130047-W

GPS power is off.
[Cause] A violation was found during the validation of the security policy.
[Action] Continues the process.
[Workaround] Take action according to the applicable security policy.

KNAF130048-W

The device remains locked for a certain period of time.

[Cause] A violation was found during the validation of the security policy.

[Action] Continues the process.

[Workaround] Take action according to the applicable security policy.

KNAF130051-W

A required application is not installed. Application name: *application-name*

[Cause] A violation was found during the validation of the security policy.

[Action] Continues the process.

[Workaround] Take action according to the applicable security policy.

KNAF130056-I

The number of managed smart devices was updated.

KNAF130057-E

Failed to update the number of managed smart devices.

[Cause] The system failed to update the number of managed smart devices.

[Action] Continues the process.

[Workaround] Collect troubleshooting information, and then contact customer support.

KNAF130060-I

An email notification of event information was sent.

KNAF130061-W

Failed to send an email notification of event information.

[Cause] The system failed to send an email notification of event information.

[Action] Continues the process.

[Workaround] Collect troubleshooting information, and then contact customer support.

KNAF130062-I

The latest information was obtained.

KNAF130063-W

Failed to obtain the latest information.

[Cause] The system failed to obtain the latest information.

[Action] Continues the process.

[Workaround] The request might have failed because the smart device was out of service range or has no Wi-Fi connection. Wait a while, and then try again.

KNAF130064-W

Initialization failed.

[Cause] Initialization processing failed.

[Action] Continues the process.

[Workaround] The request might have failed because the smart device was out of service range or has no Wi-Fi connection. Wait a while, and then try again.

KNAF130065-I

The device was locked.

KNAF130066-W

Failed to lock a device.

[Cause] The system failed to lock a device.

[Action] Continues the process.

[Workaround] The request might have failed because the smart device was out of service range or has no Wi-Fi connection. Wait a while, and then try again.

KNAF130067-I

A passcode was reset.

KNAF130068-W

Failed to reset a passcode.

[Cause] The system failed to reset a passcode.

[Action] Continues the process.

[Workaround] The request might have failed because the smart device was out of service range or has no Wi-Fi connection. Wait a while, and then try again.

KNAF130069-I

The log was obtained.

KNAF130070-W

Failed to obtain the log.

[Cause] The system failed to obtain the log.

[Action] Continues the process.

[Workaround] The request might have failed because the smart device was out of service range or has no Wi-Fi connection. Wait a while, and then try again.

KNAF130071-I

A device was set as an unmanaged device.

KNAF130072-W

Failed to set a device as an unmanaged device.

[Cause] The system failed to set a device as an unmanaged device.

[Action] Continues the process.

[Workaround] The request might have failed because the smart device was out of service range or has no Wi-Fi connection. Wait a while, and then try again.

KNAF130073-I

An Android policy was applied.

KNAF130074-W

Failed to apply an Android policy.

[Cause] The system failed to apply an Android policy.

[Action] Continues the process.

[Workaround] The request might have failed because the smart device was out of service range or has no Wi-Fi connection. Wait a while, and then try again.

KNAF130075-I

An iOS profile was applied.

KNAF130076-W

Failed to apply an iOS profile.

[Cause] The system failed to apply an iOS profile.

[Action] Continues the process.

[Workaround] The request might have failed because the smart device was out of service range or has no Wi-Fi connection. Wait a while, and then try again.

KNAF130077-I

An applied iOS profile was removed.

KNAF130078-W

Failed to remove an applied iOS profile.

[Cause] The system failed to remove an applied iOS profile.The possible reasons are:

(1) The smart device is out of service area, or the request failed due to WiFi disconnecting.

[Action] Continues the process.

[Workaround] Wait a while, and then try again.

KNAF130079-W

Failed to install an application.

[Cause] The system failed to install an application.

[Action] Cancels the execution.

[Workaround] The request might have failed because the smart device was out of service range or has no Wi-Fi connection. Wait a while, and then try again.

KNAF130080-W

Failed to remove an application.

[Cause] The system failed to remove an application.

[Action] Cancels the execution.

[Workaround] The request might have failed because the smart device was out of service range or has no Wi-Fi connection. Wait a while, and then try again.

KNAF130081-W

A requeest to obtain the latest information failed with timeout.

[Cause] The request time-outed because the smart device is out of service area, or the communition failed due to WiFi disconnecting.

[Action] Continues the process.

[Workaround] Confirm a power status or an network status of the smart device, and then try again.

KNAF130082-W

A request to Initialize a device failed with timeout.

[Cause] The request time-outed because the smart device is out of service area, or the communition failed due to WiFi disconnecting.

[Action] Continues the process.

[Workaround] Confirm a power status or an network status of the smart device, and then try again.

KNAF130083-W

A request to lock a device failed with timeout.

[Cause] The request time-outed because the smart device is out of service area, or the communition failed due to WiFi disconnecting.

[Action] Continues the process.

[Workaround] Confirm a power status or an network status of the smart device, and then try again.

KNAF130084-W

A request to reset a passcode failed with timeout.

[Cause] The request time-outed because the smart device is out of service area, or the communition failed due to WiFi disconnecting.

[Action] Continues the process.

[Workaround] Confirm a power status or an network status of the smart device, and then try again.

KNAF130086-W

A request to set a device as an unmanaged device failed with timeout.

[Cause] The request time-outed because the smart device is out of service area, or the communition failed due to WiFi disconnecting.

[Action] Continues the process.

[Workaround] Confirm a power status or an network status of the smart device, and then try again.

KNAF130087-W

A request to apply an iOS profile failed with timeout.

[Cause] The request time-outed because the smart device is out of service area, or the communition failed due to WiFi disconnecting.

[Action] Continues the process.

[Workaround] Confirm a power status or an network status of the smart device, and then try again.

KNAF130088-W

A request to remove an applied iOS profile failed with timeout.

[Cause] The request time-outed because the smart device is out of service area, or the communition failed due to WiFi disconnecting.

[Action] Continues the process.

[Workaround] Confirm a power status or an network status of the smart device, and then try again.

KNAF130089-W

A request to install an application failed with timeout.

[Cause] The request time-outed because the smart device is out of service area, or the communition failed due to WiFi disconnecting.

[Action] Continues the process.

[Workaround] Confirm a power status or an network status of the smart device, and then try again.

KNAF130090-W

A request to remove an application failed with timeout.

[Cause] The request time-outed because the smart device is out of service area, or the communition failed due to WiFi disconnecting.

[Action] Continues the process.

[Workaround] Confirm a power status or an network status of the smart device, and then try again.

KNAF130091-W

Failed to remove an applied iOS profile, because the specified iOS profile does not exist in the smart device. Profile Name: *profile-name*

[Cause] The system failed to remove an applied iOS profile. The possible reasons are:

(1) The iOS profile name is not same as the display name of the imported profile.

(2) The specified iOS profile is not being applied to the smart device.

[Action] Continues the process.

[Workaround] Make sure that the iOS Profile name shown on the iOS Profile List view is coincident with the name field in the file you imported.

Please correct the iOS Profile name on the iOS Profile List view if the name is not coincident. Delete the iOS Profile you applied as 'Android Policy/iOS Profile' on the Managed Smart Device List when it was deleted in the smart device.

KNAF190001-I

The JP1/ITDM2 - Smart Device Manager Server Service service will now start.

KNAF190002-I

The JP1/ITDM2 - Smart Device Manager Server Service service will now stop.

KNAF190003-I

The system will now stop.

KNAF190004-E

A system error occurred. (*message-description*)
[Cause] A system error occurred.
[Action] Stops the service.
[Workaround] Collect troubleshooting information, and then contact customer support.

KNAF190005-E

Failed to start the JP1/ITDM2 - Smart Device Manager Server Service service.
[Cause] Service startup failed.
[Action] Stops the service.
[Workaround] Collect troubleshooting information, and then contact customer support.

KNAF190006-I

The JP1/ITDM2 - Smart Device Manager Server Service service was registered.

KNAF190007-I

The JP1/ITDM2 - Smart Device Manager Server Service service was removed.

KNAF190008-E

Failed to register the JP1/ITDM2 - Smart Device Manager Server Service service.
[Cause] Registration of the service to Windows services failed.
[Action] Cancels installation.
[Workaround] Collect troubleshooting information, and then contact customer support.

KNAF190009-E

Failed to remove the JP1/ITDM2 - Smart Device Manager Server Service service.
[Cause] Removal of the service from Windows services failed.
[Action] Cancels uninstallation.
[Workaround] Collect troubleshooting information, and then contact customer support.

17.4 List of JP1/ITDM2 - SDM (Messaging Server) messages

The following lists and describes JP1/ITDM2 - SDM (Messaging Server) messages.

KNAF300001-I

The JP1/ITDM2 - Smart Device Manager (Messaging Server Service) service will now start.

KNAF300002-I

The JP1/ITDM2 - Smart Device Manager (Messaging Server Service) service will now stop.

KNAF300003-I

The system will now stop.

KNAF300004-E

A system error occurred. (*message-description*)
[Cause] A system error occurred.
[Action] Stops the service.
[Workaround] Collect troubleshooting information, and then contact customer support.

KNAF300005-E

Failed to start the JP1/ITDM2 - Smart Device Manager (Messaging Server Service) service.
[Cause] Service startup failed.
[Action] Stops the service.
[Workaround] Collect the troubleshooting information, and then contact customer support.

KNAF300006-I

The JP1/ITDM2 - Smart Device Manager (Messaging Server Service) service was registered.

KNAF300007-I

The JP1/ITDM2 - Smart Device Manager (Messaging Server Service) service was removed.

KNAF300008-E

Failed to register the JP1/ITDM2 - Smart Device Manager (Messaging Server Service) service.
[Cause] Registration of the service to Windows services failed.
[Action] Cancels installation.
[Workaround] Collect troubleshooting information, and then contact customer support.

KNAF300009-E

Failed to remove the JP1/ITDM2 - Smart Device Manager (Messaging Server Service) service.
[Cause] Removal of the service from Windows services failed.

[Action] Cancels uninstallation.

[Workaround] Collect troubleshooting information, and then contact customer support.

KNAF300201-E

The server address is invalid.

[Cause] Either the communication server defined in the configuration file or the address on standby for connection from the agent is invalid.

[Action] Stops the service.

[Workaround] Make sure the values defined in the configuration file are correct. If the problem persists, collect the troubleshooting information, and then contact customer support.

KNAF300202-E

An error occurred in the communication with the smart device agent. (*WinSock-error-code*)

[Cause] An error occurred in the communication with the smart device agent.

[Action] Continues the process.

[Workaround] Collect troubleshooting information, and then contact customer support.

KNAF300203-I

Standby for the server port started. (IP address = *IP-address*, port number: *port-number*)

KNAF300204-I

Standby for the server port ended. (IP address = *IP-address*, port number: *port-number*)

KNAF300205-I

Connection with the smart device agent will now start. (IP address = *IP-address*, port number: *port-number*)

KNAF300206-I

Connection with the smart device agent is freed (*device-ID*).

KNAF300207-E

The length of the received data exceeded the maximum size. (*socket-ID*)

[Cause] The length of the received data exceeded the maximum size.

[Action] Continues the process.

[Workaround] Collect troubleshooting information, and then contact customer support.

KNAF300208-E

The maximum number of simultaneous connections was exceeded.

[Cause] The number of simultaneous connections with the smart device agent was exceeded.

[Action] Continues the process.

[Workaround] Make sure the values defined in the configuration file are correct. If the problem persists, collect the troubleshooting information, and then contact customer support.

KNAF300209-E

An error occurred in the communication with the communication server. (*WinSock-error-code*)

[Cause] An error occurred in the communication with the communication server.

[Action] Continues the process.

[Workaround] Collect troubleshooting information, and then contact customer support.

KNAF300210-E

An error occurred in the server socket. (*WinSock-error-code*)

[Cause] A communication error occurred.

[Action] Stops the service when an error occurred in the starting process, but in other case continues process.

[Workaround] Make sure the values defined in the configuration file are correct. If the problem persists, collect the troubleshooting information, and then contact customer support.

KNAF300211-W

The smart device agent to which data was to be sent (*device-ID*) has already been disconnected.

[Cause] The smart device agent is not connected.

[Action] Continues the process.

[Workaround] Check the boot status and communication status of the smart device agent.

KNAF300212-I

Connection to the smart device agent (*device-ID*) was established.

KNAF300213-E

Failed to read the configuration file (*file-name*).

[Cause] Failed to get a path of the configuration file.

[Action] Continues the process.

[Workaround] Collect the troubleshooting information, and then contact customer support.

KNAF300214-W

The smart device agent for which processing was requested (*device-ID*) is not connected.

[Cause] The smart device agent is not connected.

[Action] Continues the process.

[Workaround] Check the boot status and communication status of the smart device agent.

KNAF300215-I

A request for connection with the smart device agent (*device-ID*) will now be sent.

KNAF300216-I

A request for log transmission from the smart device agent (*device-ID*) will now be sent.

KNAF300217-E

Failed to request processing from the smart device agent.

[Cause] An error occurred in the communication with the smart device agent.

[Action] Continues the process.

[Workaround] Check the boot status and communication status of the smart device agent.

KNAF300218-I

A message notification will now be sent to the smart device agent (*device-ID*).

17.5 List of command messages

The following lists and describes command messages.

KNAF600001-I

The command ended normally. (command = *command-name*)

KNAF600002-E

The command ended abnormally. (command = *command-name*, return value = *return-value*)

[Cause] The command ended abnormally.

[Action] Cancels the execution.

[Workaround] Check the return value of the command and take appropriate action, and then re-execute the command.

Appendixes

A. List of folders

This appendix describes the folders that are created during installation of components.

A.1 Folders created on the smart device manager

The following tables list and describe the folders that are created on the smart device manager during installation of JP1/ITDM2 - SDM (Smart Device Manager).

Folders created during installation of JP1/ITDM2 - SDM (Smart Device Manager)

Folder name	Description
JP1/ITDM2 - SDM (Smart Device Manager)-installation-folder	JP1/ITDM2 - SDM (Smart Device Manager) data folder Default: `%Program Files%\Hitachi\jp1itdm2sdm`
`%WINDIR%\Temp\SDMINST`	Folder for log files which are output during installation

Folders created under the installation folder

Folder name	Description
`log\`	Folder for log files which are output during installation
`mgr\`	Root folder for the smart device manager
`mgr\bin`	Executable file folder
`mgr\backup`	Default backup folder
`mgr\conf\`	Environment definition file folder
`mgr\Database\`#	JP1/ITDM2 - SDM (Smart Device Manager) data folder
`mgr\db\`	Database installation folder
`mgr\log\`	Trace log folder
`mgr\temp`	Temporary data folder
`mgr\troubleshoot\`	Default troubleshooting information folder
`mgr\uC\`	Application server installation folder

#: This folder is created when a new installation of JP1/ITDM2 - Smart Device Manager version 11-00 or later is performed. This folder is not created when JP1/ITDM2 - Smart Device Manager is upgraded from 10-50 to 11-00 or later.

Folders created during installation of JP1/ITDM2 - SDM (Smart Device Manager) (other than the installation folder)

Folder name	Description
`%Program Files%\Hitachi\HNTRLib2\`	Trace library installation folder
All-User-profile-application-data-folder`\Hitachi\jp1itdm2sdm\Database\`#	JP1/ITDM2 - SDM (Smart Device Manager) data folder
program-menu-of-the-system`\JP1_IT Desktop Management2 - Smart Device Manager`	Program folder

#: This folder is created when JP1/ITDM2 - Smart Device Manager is upgraded from 10-50 to 11-00 or later. This folder is not created when a new installation of JP1/ITDM2 - Smart Device Manager version 11-00 or later is performed.

A.2 Folders created on the communication server

The following tables list and describe the folders that are created on the communication server during installation of JP1/ITDM2 - SDM (Communication Server).

Folders created during installation of JP1/ITDM2 - SDM (Communication Server)

Folder name	Description
JP1/ITDM2 - SDM (Communication Server)-installation-folder	JP1/ITDM2 - SDM (Communication Server) data folder. Default: `%Program Files%\Hitachi\jp1itdm2sdm`
`%WINDIR%\Temp\SDMINST`	Folder for log files which are output during installation

Folders created under the installation folder

Folder name	Description
`log\`	Folder for log files which are output during installation
`cms\`	Root folder for the communication server
`cms\bin`	Executable file folder
`cms\conf\`	Environment definition file folder
`cms\log\`	Trace log folder
`cms\troubleshoot\`	Default troubleshooting information folder
`cms\uC\`	Application server installation folder
`cms\uC\httpsd\htdocs\download\`	Folder for applications to be distributed

A.3 Folders created on the messaging server

The following tables list and describe the folders that are created on the messaging server during installation of JP1/ITDM2 - SDM (Messaging Server).

Folders created during installation of JP1/ITDM2 - SDM (Messaging Server)

Folder name	Description
JP1/ITDM2 - SDM (Messaging Server)-installation-folder	JP1/ITDM2 - SDM (Messaging Server) data folder. Default: `%Program Files%\Hitachi\jp1itdm2sdm`
`%WINDIR%\Temp\SDMINST`	Folder for log files which are output during installation

Folders created under the installation folder

Folder name	Description
`log\`	Folder for log files which are output during installation
`mss\`	Root folder for the messaging server
`mss\bin\`	Executable file folder
`mss\conf\`	Environment definition file folder
`mss\log\`	Trace log folder

Folder name	Description
`mss\troubleshoot\`	Default troubleshooting information folder

B. List of services and processes

This appendix describes the services and processes of JP1/ITDM2 - SDM.

B.1 List of services

For each server, this section shows JP1/ITDM2 - SDM service names, corresponding service process names, and service descriptions, and indicates whether a service starts automatically.

Smart device manager

Service name	Service display name	Service process name	Description	Automatic startup of the service
JP1_ITDM2_SDM_MGRSVR	JP1/ITDM2 - Smart Device Manager Server Service	*JP1/ITDM2 - SDM (Smart Device Manager)-installation-folder*`\mgr\bin\SdManagerServer.exe`	Smart device manager service	Yes
HiRDBEmbeddedEdition_IS1	JP1/ITDM2 - Smart Device Manager (DB Service)	*JP1/ITDM2 - SDM (Smart Device Manager)-installation-folder*`\mgr\db\BIN\pdservice.exe`	Smart device manager database service	Yes
JP1_ITDM2_SDM_WEBSVR	JP1/ITDM2 - Smart Device Manager Web Server	*JP1/ITDM2 - SDM (Smart Device Manager)-installation-folder*`\mgr\uC\httpsd\httpsd.exe`	Web server service	Yes

Legend:

Yes: The service starts automatically

Communication server

Service name	Service display name	Service process name	Description	Automatic startup of the service
JP1_ITDM2_SDM_COMSVR	JP1/ITDM2 - Smart Device Manager (Communication Server Service)	*JP1/ITDM2 - SDM (Communication Server)-installation-folder*`\cms\bin\SdCommunicationServer.exe`	Communication server service	Yes
JP1_ITDM2_SDM_WEBSVR	JP1/ITDM2 - Smart Device Manager Web Server	*JP1/ITDM2 - SDM (Communication Server)-installation-folder*`\cms\uC\httpsd\httpsd.exe`	Web server service	No

Legend:

Yes: The service starts automatically

No: Does not start automatically

Messaging server

Service name	Service display name	Service process name	Description	Automatic startup of the service
JP1_ITDM2_SDM_MSGSVR	JP1/ITDM2 - Smart Device Manager (Messaging Server Service)	*JP1/ITDM2 - SDM (Messaging Server)-installation-folder*`\mss\bin\SdMessagingServer.exe`	Messaging server service	Yes

Legend:

Yes: The service starts automatically

B.2 List of processes

This section lists and describes the functions of JP1/ITDM2 - SDM processes for each server.

Smart device manager

Process name	Function	Whether the process is resident
cjstartsv.exe	Application server process	Yes
SdManagerServer.exe	Service process	Yes
pd*xxx*.exe#	Database processes	Yes
httpsd.exe	Web server function process	Yes

Legend:

Yes: The process is resident.

#: *xxx* is a character string that contains 3 to 8 characters.

Communication server

Process name	Function	Whether the process is resident
cjstartsv.exe	Application server process	Yes
SdCommunicationServer.exe	Service process	Yes
httpsd.exe	Web server function process	Yes

Legend:

Yes: The process is resident.

Messaging server

Process name	Function	Whether the process is resident
SdMessagingServer.exe	Service process	Yes

Legend:

Yes: The process is resident.

C. Port number list

This appendix lists and describes the port numbers used in JP1/ITDM2 - SDM for each server.

Smart device manager

Port number	Connection direction	Connected to [port number]	Protocol	Use
26080	<-	Administrator's computer [ephemeral]	TCP	Used for communication from the administrator's computer to the smart device manager for operating and viewing program modules
26055	<-	ITDM2 management server	TCP	Hitachi Web Server HTTPS port used for SSL communication with the ITDM2 management server
26056	<-	Smart device manager [ephemeral]	TCP	Used to receive requests for internal communication when the `sdmioutils` command is executed
26057	<-	ITDM2 management server	TCP	Used for HTTP communication with the ITDM2 management server
26065	<-	Smart device manager [ephemeral]	TCP	Used by J2EE applications in the smart device manager to receive RMI registry requests
26053	<-	Smart device manager [ephemeral]	TCP	Used by J2EE applications in the smart device manager to receive requests from the in-process HTTP server
26052	<-	Smart device manager [ephemeral]	TCP	Used for management communication by J2EE applications in the smart device manager
26066	<-	Smart device manager or ITDM2 management server [ephemeral]	TCP	Used for communication with the database configured in the smart device manager
26067	<-	Communication server [26068-26077]	TCP	Used for communication with the database configured in the smart device manager

Communication server

Port number	Connection direction	Connected to [port number]	Protocol	Use
26055	<-	Smart device manager [ephemeral]	TCP	Hitachi Web Server HTTPS port number for SSL communication
	<-	JP1/ITDM2 - SDM (Smart Device Android Agent) [ephemeral]	TCP	
	<-	JP1/ITDM2 - SDM (Smart Device iOS Agent) [ephemeral]	TCP	
26065	<-	Communication server [ephemeral]	TCP	Used by J2EE applications in the communication server to receive RMI registry requests

Port number	Connection direction	Connected to [port number]	Protocol	Use
26053	<-	Communication server [ephemeral]	TCP	Used by J2EE applications in the communication server to receive requests from the Web server (redirector)
26052	<-	Communication server [ephemeral]	TCP	Used for management communication by J2EE applications in the communication server
26068-26077	<-	Smart device manager [26067]	TCP	Used for communication with the database configured in the smart device manager

Messaging server

Port number	Connection direction	Connected to [port number]	Protocol	Use
26078	<-	Communication server [ephemeral]	TCP	Used to send requests from the communication server to the messaging server
26079	<-	JP1/ITDM2 - SDM (Smart Device Android Agent) [ephemeral]	TCP	Used for Comet connection with JP1/ITDM2 - SDM (Smart Device Android Agent)

D. Lists of parameters

This appendix describes the parameters for each setting.

D.1 User account parameters

The following table lists and describes the parameters in the **Account Management** view.

User account parameters

Item	Description	Specifiable values	Default
User ID	Specify the user ID of the user account used to log in to JP1/ITDM2 - SDM (Smart Device Manager)	Character string of 8-50 half-width characters[#1]	(Blank)
Password	Specify the password for the user ID.	Character string of 8-20 half-width characters[#1] [#2]	(Blank)
Re-enter Password	Enter the password again.	Character string of 8-20 half-width characters[#1] [#2]	(Blank)
User Name	Specify the user account name.	Character string of 20 or fewer full- or half-width characters	(Blank)
Email	Specify the email address of the user account user.	Email character string of 100 or fewer characters	(Blank)
Description	Enter a description of the user account.	Character string of 1,000 or fewer half-width characters	(Blank)
Permission	Specify whether to assign the system administrator permission to the user account.	Selected The system administrator permission is assigned. Not selected The system administrator permission is not assigned.	Not selected
Status	The user account can be unlocked if it has been locked.	• **Enabled** • **Disabled**	**Disabled**[#3]

#1: You can use ASCII characters other than ASCII control characters.

#2: To change the password, specify a character string that is different from the current password.

#3: Displayed only when the user account has been locked.

D.2 Event notification parameters

The following tables list and describe the parameters in the **Event Notifications** view.

Select the category and severity of events about which you want to be notified by email:

Item	Description	Specifiable values	Default
Critical	Select the check box to send notification emails for all types of events whose severity is **Critical**.	Selected Event notification emails are sent.	Not selected

Item	Description	Specifiable values	Default
Warning	Select the check box to send notification emails for all types of events whose severity is **Warning**.	Not selected Event notification emails are not sent.	Not selected
Information	Select the check box to send notification emails for all types of events whose severity is **Information**.		
Security	Select the check box to send notification emails for events related to security management, such as a change or allocation of a security policy, and results of security policy judgment.	Selected Notification emails for the selected events. Not selected Event notification emails are not sent.	Not selected
Suspicious Operations	Select the check box to send notification emails for events related to suspicious operations, such as the detection of a call to a disallowed phone number, or browsing of a disallowed Web site.		
Smart Device	Select the check box to send notification emails for events related to smart devices, such as addition and removal of smart devices.		
Distribution	Select the check box to send notification emails for events related to distribution, such as addition and removal of distributed applications, and distribution of applications.		
Settings	Select the check box to send notification emails for events related to settings, such as user account management and event notification settings.		
Error	Set events related to errors that occur in functions.		

Specify event notifications to be ignored:

Item	Description	Specifiable values	Default
Event Number	Select the check box for the event number for which you do not want to send notification email.	Selected The event is not notified. Not selected The event is notified.	Not selected

Select recipients:

Item	Description	Specifiable values	Default
User ID	Select the check box for the user ID to which you want to send event notification emails. If an email address is not set, use the **Edit User Account** dialog box to set the email address.	Selected Event notification emails are sent to the user. Not selected Event notification emails are not sent to the user.	Not selected

Interval of notification

Item	Description	Specifiable values	Default
Interval of notification (minutes)	Specify the interval (minutes) at which notification emails are sent.	1 to 1440	30

Related Topics

- *6.3 Editing another administrator's user account*

D.3 Mail server parameters

The following table lists and describes the parameters in the **SMTP Server** view.

Mail server parameters

Item	Description	Specifiable values	Default
Host name	Enter the host name of the SMTP server.	The host name of the SMTP server	(Blank)
Secure connection	Select the security protection used for communication with the SMTP server.	• Plain • SSL • TLS	Plain
Port	Specify the port number of the SMTP sever.	1 to 65535	25
Source email	Specify the source email address of notification emails.	Email character string	(Blank)
Use Authentication	Select to use the user authentication function (SMTP Authentication) on the SMTP server.	Selected SMTP authentication is used. Not selected SMTP authentication is not used.	Not selected
User ID	Enter the user ID used for user authentication.	User ID used for user authentication	(Blank)
Password	Specify the password for the user ID.	Password for the user ID	(Blank)
Re-enter Password	Enter the password again for confirmation.	Password for confirmation	(Blank)

E. Output Format of Imported and Exported Files

This appendix describes the output format of imported or exported files.

E.1 Format of exported or imported smart device list CSV file

The following table describes the format of an exported or imported smart device list CSV file.

Format of an exported or imported smart device list CSV file

Item[#1]	Description	Specifiable values	Maximum number of bytes[#2]	Imported?
Name	Name such as an asset management number	--	128	Y
OS	OS information acquired from the smart device	0: iOS 1: Android	1	Y
IMEI/MEID	IMEI/MEID acquired from the smart device	15 digits	15	N
Phone number	Phone number of the smart device from which the information is acquired	Maximum of 20 characters Only numbers can be specified, excluding a hyphen (-).	20	N
Status	Management status in the product	0: Unmanaged 1: Managed	1	N
Current security policy	Name of the security policy applied to the smart device	--	36	Y[#3]
Current Android policy/iOS profile[#6]	Android policy or iOS profile currently applied to the smart device	--	809	Y[#3]
Department	Department to which the user belongs	--	128	Y[#4]
Account	Account of the user	--	128	Y[#4]
User name	Name of the user	--	128	Y[#4]
Last modified date/Time	Date and time that the information was last modified due to registration of a smart device or import of smart device information	*yyyy*/*MM*/*dd hh*:*mm*:*ss*[#5]	19	N
Manufacturer	Manufacturer name acquired from the smart device	--	256	N
Model number	Model number acquired from the smart device	--	256	N
Protocol version	Protocol version of the product	--	64	N
Language	Language setting acquired from the smart device	Maximum of 20 characters	80	N

Item[#1]	Description	Specifiable values	Maximum number of bytes[#2]	Imported?
Product name	Product name acquired from the smart device	Maximum of 10 characters Android iOS	40	N
Model name	Model name acquired from the smart device	--	256	N
Serial number	Serial number acquired from the smart device	--	256	N
OS version	OS version acquired from the smart device	--	32	N
OEM name	OEM name acquired from the smart device	--	64	N
Firmware version	Firmware version acquired from the smart device	--	64	N
Software version	Software version acquired from the smart device	--	64	N
Mobile network country code	Mobile network country code acquired from the smart device	Maximum of 10 characters	40	N
Mobile network operator code	Mobile network operator code acquired from the smart device	Maximum of 20 characters	80	N
Mobile network operator name	Mobile network operator name acquired from the smart device	Maximum of 20 characters	80	N
Mobile network type	Mobile network type acquired from the smart device	Maximum of 20 characters	80	N
SIM card country code	SIM card country code acquired from the smart device	Maximum of 10 characters	40	N
SIM card operator code	SIM card operator code acquired from the smart device	Maximum of 20 characters	80	N
SIM card operator name	SIM card operator name acquired from the smart device	--	256	N
ICCID	ICCID acquired from the smart device	19 digits	19	N
SIM status code	SIM status code acquired from the smart device	--	64	N
IMSI	IMSI acquired from the smart device	15 digits	15	N
User name	User name acquired from the smart device	Maximum of 20 characters	80	N
Roaming	Roaming information acquired from the smart device	0: Normal 1: Roaming	1	N

Item[#1]	Description	Specifiable values	Maximum number of bytes[#2]	Imported?
Android ID/Apple ID	Android ID or Apple ID acquired from the smart device	--	256	N
Email	Email address acquired from the smart device	--	256	N
Password (set or not set)	Password (set or not set) acquired from the smart device	0: Not set 1: Set	1	N
Internal storage (Total / Free [B])	Internal storage information acquired from the smart device	--	64	N
SD Card (Total / Free [B])	SD card information acquired from the smart device	--	64	N
RAM (Total / Free [B])	RAM information acquired from the smart device	--	64	N
Date/Time of Android policy/iOS profile application[#6]	Date and time that the Android policy or iOS profile was applied to the smart device	*yyyy*/*MM*/*dd* *hh*:*mm*:*ss*[#5]	199	N
Android policy/iOS profile version[#6]	Version of the Android policy or iOS profile that was applied to the smart device	Maximum of 5 characters	59	N
Date/time of device details update	Last date and time that the inventory information was collected	*yyyy*/*MM*/*dd* *hh*:*mm*:*ss*[#5]	19	N
Battery Level	Battery level acquired from the smart device	--	4	N
3G MAC Address	3G MAC address acquired from the smart device	--	64	N
WiFi MAC Address	WiFi MAC address acquired from the smart device	--	64	N
Bluetooth MAC Address	Bluetooth MAC address acquired from the smart device	--	64	N
UDID	UDID acquired from the smart device	--	40	N
IP Address	IP address acquired from the smart device	--	64	N
Proxy Server	Proxy server acquired from the smart device	--	256	N
GPS Information	GPS information acquired from the smart device	--	128	N
Lock Release Password Changed During Last Lock	Unlock password that was changed the last time the lock was set	--	10	N

Item[#1]	Description	Specifiable values	Maximum number of bytes[#2]	Imported?
GPS Power Status	GPS power status acquired from the smart device	--	3	N
Last Date/Time of Successful Lock Release	Date and time that the last unlock was successful	--	19	N
Last Date/Time of Failed Lock Release	Date and time that the last unlock failed	--	19	N
Agent Ver.	Agent version of this product	--	128	N

Legend:

Y: Imported

N: Not imported

--: Any value

#1: The first line of the CSV file does not contain item information.

#2: The maximum number of bytes if UTF-8 or UTF-16 is specified for the character encoding. For half-width alphanumeric characters and symbols, one character is counted as one byte. For other characters, one character is counted as four bytes.

#3: If this item is not specified, the smart device is registered as an unmanaged device.

#4: Although this is an optional item, we recommend that you specify a value.

#5: *yyyy*: year, *MM*: month, *dd*: day, *hh*: hour, *mm*: minute, *ss*: second

#6: If an information item includes multiple values, the values are delimited by semicolons (;).

Related Topics

- *15. sdmioutils exportdevice (exporting smart device information)*
- *15. sdmioutils importdevice (importing smart device information)*

E.2 Format of an exported event list CSV file

The following table describes the format of an exported event list CSV file.

Format of an exported event list CSV file

Item[#1]	Description	Output format	Maximum number of bytes[#2]
Severity	The severity is output.	0: Information 1: Warning 2: Critical	1
Registered Date/Time	The registration date and time is output.	*yyyy/MM/dd hh:mm:ss*[#3]	19
Source	The source of the event is output.	• Smart Device • *smart-device-name* • Security • Distribution • Settings	128
Description	The event description is output.	A character string of 1,024 characters plus the number of embedded characters is output.	4,096 characters + *number-of-embedded characters* **x** 4
Event Number	The event number is output.	The message for event output is displayed.	10

Item#1	Description	Output format	Maximum number of bytes#2
Type	The event type is output.	0: Security 1: Suspicious Operations 2: Smart Device 3: Distribution 4: Settings 5: Error	1
Details	Event details are output.	A character string of 1,024 characters plus the number of embedded characters is output.	4,096 characters + *number-of-embedded characters* **x** 4
Status	The check status is output.	0: Not Ack 1: Ack	1

#1: The first line of the CSV file does not contain item information.

#2: The maximum number of bytes if UTF-8 or UTF-16 is specified for the character encoding. For half-width alphanumeric characters and symbols, one character is counted as one byte. For other characters, one character is counted as four bytes.

#3: *yyyy*: year, *MM*: month, *dd*: day, *hh*: hour, *mm*: minute, *ss*: second

Related Topics

- *10.2 Exporting event information*
- *17.2 JP1/ITDM2 - SDM (Smart Device Manager) messages output as events*

E.3 Format of an exported security policy list XML file

The following describes the format of an exported security policy list XML file.

Example of an exported security policy list XML file

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<policy name="General">
    <note>Description in the note</note>
    <phones number="09000010001">
        <note>Customer A</note>
    </phones>
    <apps name="In-house application">
        <version>1.0</version>
        <alerttype>0</alerttype>
        <installtype>1</installtype>
        <os>1</os>
        <note>For in-house information access</note>
    </apps>
    <urls name="http://www.xyz.co.jp">
        <alerttype>0</alerttype>
        <note>Search site</note>
    </urls>
</policy>
```

Important

Do not edit the exported file.

Format of an exported security policy list XML file

Element name	Description	Type	Value output format	Maximum number of bytes#
policy	Security policy root element	!	N	0
name	Security policy name	@	A maximum of 20 characters	80
note	Description of the security policy	!	A maximum of 1,000 characters	4000
phones	Phone number list root element	-	N	0
phone	Phone number information root element	+	N	0
number	Phone number	@	• A maximum of 20 characters • A hyphen (-) is not included. • Only numbers are output.	20
note	Description of the phone number	!	A maximum of 1,000 characters	4000
apps	Application list root element	-	N	0
app	Application information	+	N	0
name	Application name	@	A maximum of 100 characters	400
version	Application version	!	A maximum of 100 characters	400
alerttype	Alert type	!	0: Allowed 1: Prohibited	1
installtype	Installation type	!	0: Installation allowed 1: Installation required	1
os	OS type	!	0: iOS 1: Android	1
note	Application description	!	A maximum of 1000 characters	4000
urls	Web site list root element	-	N	0
url	Web site information	+	N	0
name	URL	@	A maximum of 200 characters	800
alerttype	Alert type	!	0: Allowed 1: Prohibited	1
note	URL description	!	A maximum of 1000 characters	4000

Legend:

N: No value is output.

@: Attribute value of the element

!: Required

-: Optional

+: One or more repetitions

#: The maximum number of bytes if UTF-8 or UTF-16 is specified for the character encoding. For half-width alphanumeric characters and symbols, one character is counted as one byte. For other characters, one character is counted as four bytes.

Related Topics

- *15. sdmioutils exportpolicy (exporting security policy settings)*
- *15. sdmioutils importpolicy (importing security policy settings)*

E.4 Format of an exported smart device security policy (Android policy or iOS profile) XML file

The following describes the format of an exported smart device security policy (Android policy or iOS profile) XML file.

Example of an exported smart device security policy (Android policy or iOS profile) XML file

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<sdmpolicy name="General">
    <os>0</os>
    <policy>Android-policy-or-iOS-profile</policy>
    <note>Description</note>
</sdmpolicy>
```

Important

Do not edit the exported file.

Format of an exported smart device security policy (Android policy or iOS profile) XML file

Element name	Description	Type	Value output format	Maximum number of bytes#
sdmpolicy	Root element of the Android policy or iOS profile	!	N	0
name	Android policy name or iOS profile name	@	A maximum of 20 characters	80
os	OS type	!	0: iOS 1: Android	1
policy	Android policy or iOS profile	!	<![CDATA[*XML-data-for-Android-policy-or-iOS profile*]]>	32000
note	Description of the Android policy or iOS profile	!	A maximum of 1,000 characters	4000

Legend:

N: No value is output.

@: Attribute value of the element

!: Required

#: The maximum number of bytes if UTF-8 or UTF-16 is specified for the character encoding. For half-width alphanumeric characters and symbols, one character is counted as one byte. For other characters, one character is counted as four bytes.

Related Topics

- *15. sdmioutils exportsdpolicy (exporting Android policy information or iOS profile information)*
- *15. sdmioutils importsdpolicy (importing Android policy information or iOS profile information)*

E.5 Format of an exported distributed-application XML file

The following describes the format of an exported distributed-application XML file.

Example of an exported distributed-application XML file

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<delivery name="Sample application">
    <os>OS type</os>
    <identifier>Bundle ID</identifier>
    <version>Package version</version>
    <description>Description</description>
    <binary>distributed-application-package</binary>
    <installparam>installParam</installparam>
    <mime>package-type</mime>
    <pkg_no>package-No.</pkg_no>
    <pkg_id>package-ID</pkg_id>
</delivery>
```

Important

Do not edit the exported file.

Format of an exported distributed-application XML file

Element name	Description	Type	Value output format	Maximum number of bytes[#1]
delivery	Distributed application root element	!	N	0
name	Distributed application name	@	A maximum of 100 characters	400
os	OS type	-[#2]	0: iOS 1: Android	1
identifier	Bundle ID	In Android - In iOS !	In Android N In iOS A maximum of 256 characters	In Android 0 In iOS 1024
version	Package version	In Android - In iOS !	A maximum of 100 characters	400
description	Description	!	A maximum of 1000 characters	4000
binary	Distributed application package	!	Binary value	Package size
installparam	Install Parameters	-	In Android A maximum of 256 characters In iOS A maximum of 1000 characters	In Android 1024 In iOS 4000

Element name	Description	Type	Value output format	Maximum number of bytes#1
mime	Package type	!	A maximum of 256 characters	1024
pkg_no	Package No.	!	UUID value	36
pkg_id	Package ID	!	UUID value	36

Legend:

N: No value is output.

@: Attribute value of the element

-: Optional

#1: The maximum number of bytes if UTF-8 or UTF-16 is specified for the character encoding. For half-width alphanumeric characters and symbols, one character is counted as one byte. For other characters, one character is counted as four bytes.

#2: If you import an exported distributed-application XML file for which the OS type is not defined, the OS type is assumed to be Android.

Related Topics

- *15. sdmioutils exportdeliveryapp (exporting distributed application information)*
- *15. sdmioutils importdeliveryapp (importing distributed application information)*

E.6 Format of a distribution permission definition file

The following describes the format of a distribution permission definition file (CSV format).

Example of a distribution permission definition file (when import mode is `all` or when exporting)

```
OS type,Application name,Version,Distribution permission type,Device name
Android,app2,v1,0,device4
Android,app2,v1,0,device5
Android,app3,v1,0,device5
iOS,app1,v1,0,device1
iOS,app1,v1,0,device2
iOS,app1,v1,0,device3
```

Example of a distribution permission definition file (when import mode is `app`)

```
Distribution permission type,Device name
0,device1
0,device2
0,device3
```

Example of a distribution permission definition file (when import mode is `device`)

```
Application name,Version
app1,v1
app2,v1
app3,v1
```

Format of a distribution permission definition file

Column number	Item	Description	Import mode			Export
			all	app	device	
1	OS type	Specify the OS type. • iOS • Android	R	D	D	O
2	Application name	Specify the name of the application.	R	D	R	O
3	Version	Specify the version of the application.	R	D	R	O
4	Distribution permission type	Fixed as `0`.	R	R	D	O
5	Device name	Specify the name of the smart device.	R	R	D	O

Legend:

R: Required

D: Disused

O: Output

Conventions for distribution permission definition file

- The first line is a title line, with data specified on the second and subsequent lines.
- As the last line, enter a linefeed character.
- Specify the file contents in ISO-8859-1, UTF-8 or UTF-16 encoding.

Related Topics

- *15. sdmioutils exportdeliverypermit (exporting settings that define applications as installable by users)*
- *15. sdmioutils importdeliverypermit (defining applications that can be installed by users)*

E.7 Format of an application distribution information file

The following describes the format of an application distribution information file (CSV format).

Example of an application distribution information file

```
Operation,OS type,Distributed application,Version,Smart device name
install,iOS,ApplicationA,1.0,Device1
install,iOS,ApplicationA,1.0,Device2
install,iOS,ApplicationA,1.0,Device3
install,iOS,ApplicationB,1.0,Device1
install,iOS,ApplicationB,1.0,Device2
```

Format of an application distribution information file

Column number	Item	Specifiable values
1	Operation	Specify installation or distribution. • install

Column number	Item	Specifiable values
1	Operation	• distribute#
2	OS type	Specify the OS type of the smart device. • iOS • Android
3	Distributed application	Specify the name of the distributed application.
4	Version	Specify the version of the distributed application.
5	Smart device name	Specify the name of the smart device on which to install the application.
6	Comment	Specify a comment. If you do not wish to specify a comment, you can also omit the comma after the fifth column.

#: You can only specify `Android`.

Conventions for application distribution information files

- The first line is a title line, with data specified on the second and subsequent lines.
- As the last line, enter a linefeed character.
- Specify the file contents in UTF-8 (with BOM) encoding.

Related Topics

- *15. sdmdistributeapp (sending instructions to install applications)*

E.8 Format of an iOS profile information file

The following describes the format of an iOS profile information file (CSV format).

Example of an iOS profile information file

```
Operation,Profile name,Device name,Comment
apply,ProfileA,Device1
apply,ProfileA,Device2
```

Format of an iOS profile information file

Column number	Item	Specifiable values
1	Operation	Specify whether to apply or remove the iOS profile: apply: Apply the profile remove: Remove the profile
2	Profile name	Specify the name of the iOS profile to apply or remove.
3	Device name	Specify the device name of the smart device to which the iOS profile is to be applied, or from which it is to be removed.
4	Comment	Specify a comment. If you do not wish to specify a comment, you can also omit the comma after the fifth column.

Conventions for iOS profile information files

- The first line is a title line, with data specified on the second and subsequent lines.
- As the last line, enter a linefeed character.
- Specify the file contents in UTF-8 (with BOM) encoding.
- Do not specify `apply` and `remove` operations in the same iOS profile information file.

Related Topics

- *15. sdmapplyprofile (applying or removing an iOS profile)*

E.9 Format of a device information file

The following describes the format of a device information file (CSV format).

Example of a device information file

```
Inventory type,Device name,Comment
All,Device1
All,Device2
All,Device3
```

Format of a device information file

Column number	Item	Specifiable values
1	Inventory type	Fixed as `All`.
2	Device name	Specify the name of the smart device for which to acquire inventory information.
3	Comment	Specify a comment. If you do not wish to specify a comment, you can also omit the comma after the fifth column.

Conventions for device information files

- The first line is a title line, with data specified on the second and subsequent lines.
- As the last line, enter a linefeed character.
- Specify the file contents in UTF-8 encoding.

Related Topics

- *15. sdmgetinventory (acquiring inventory information)*

E.10 Format of a distribution status output file

The following describes the format of a distribution status output file (CSV format).

Example of a distribution status output file (for iOS)

When `-version` is specified:

```
Name,Status,Package name,Version
"Device1","0","PackageA","1.0"
"Device2","1","PackageA","1.0"
"Device3","4","PackageA","1.0"
"Device4","3","PackageA","1.0"
"Device5","3","PackageA","1.0"
"Device6","1","PackageA","1.0"
```

When `-version` is omitted:

```
Name,Status,Package name,Version
"Device1","0","PackageA","1.0"
"Device1","0","PackageA","1.5"
"Device1","1","PackageA","2.0"
"Device2","1","PackageA","1.0"
"Device2","1","PackageA","1.5"
"Device2","0","PackageA","2.0"
"Device3","4","PackageA","1.0"
"Device3","0","PackageA","1.5"
"Device3","0","PackageA","2.0"
```

Example of a distribution status output file (for Android)

When `-version` is specified:

```
Name,Distribute Status,Last Distribute Control Status,Last Installation
Control Status,Package name,Version
"Device 1","0","0","9","Package A","1.0"
"Device 2","1","0","0","Package A","1.0"
"Device 3","1","0","2","Package A","1.0"
"Device 4","1","1","9","Package A","1.0"
"Device 5","0","3","9","Package A","1.0"
"Device 6","0","4","9","Package A","1.0"
```

When `-version` is omitted:

```
Name,Distribute Status,Last Distribute Control Status,Last Installation
Control Status,Package name,Version
"Device 1","0","0","9","Package A","1.0"
"Device 1","0","0","9","Package A","1.5"
"Device 1","1","0","0","Package A","2.0"
"Device 2","0","0","9","Package A","1.0"
"Device 2","1","3","9","Package A","1.5"
"Device 2","0","0","9","Package A","2.0"
"Device 3","0","0","9","Package A","1.0"
"Device 3","0","0","9","Package A","1.5"
"Device 3","1","0","2","Package A","2.0"
```

Format of a distribution status output file (for iOS)

Column number	Item	Output information
1	Name	The name of the smart device, such as an asset management number.

Column number	Item	Output information
2	Status	0: Not installed 1: Installed 3: Installation requested 4: Installation request failed 5: Installation failed 6: Installing 13: Uninstallation requested 14: Uninstallation request failed 15: Uninstallation failed
3	Package name	The package name of the application
4	Version	The version of the application

Format of a distribution status output file (for Android)

Column number	Item	Output information
1	Name	The name of the smart device, such as an asset management number.
2	Distribute Status	0: Not distributed 1: Distributed
3	Last Distribution Control Status	0: Normal 1: Removal failed 2: Removing 3: Distributing 4: Distribution failed
4	Last Installation Control Status	0: Normal 1: Uninstallation failed 2: Installation failed 9: Not installed
5	Package name	The package name of the application
6	Version	The version of the application

Explanation of the output values in a distribution status output file

- The character encoding is UTF-8.
- The file contents are sorted in order of smart device name. If you did not specify the `-version` command argument, the file contents are sorted using the name as the first sort key and the version as the second sort key.
- Information is only output for managed smart devices.

Related Topics

- *15. sdmexportdistributestatus (outputting application distribution status)*

E.11 Format of a installed software information output file

The following describes the format of an installed software information output file (CSV format).

Example of an installed software information output file

```
Name,Application name,Version
"Device1","ApplicationA","1.0"
"Device1","ApplicationB","2.0"
"Device1","ApplicationC","3.0"
"Device2","ApplicationB","2.0"
"Device2","ApplicationD","1.5"
"Device3","ApplicationB","2.0"
```

Format of an installed software information output file

Column number	Item	Output information
1	Name	The name of the smart device, such as an asset management number.
2	Application name	The name of the application
3	Version	The version of the application

Explanation of the output values in an installed software information output file

- The character encoding is UTF-8.
- The file contents are sorted using the name as the first sort key, the application name as the second sort key, and the version as the third sort key.
- Information is only output for managed smart devices.

Related Topics

- *15. sdmexportinstallapp (outputting installed software information)*

F. Storage locations of (and how to obtain) information required for support

The table below shows the storage locations of information required for support if the `sdmgetlogs` command cannot be used in a user environment, and how to obtain such information. Notify users of the storage locations and how to collect the information.

Storage locations or how to collect information required for support

Information	Description	Storage location or how to obtain information
Smart device manager information	JP1/ITDM2 - SDM (Smart Device Manager) log	File stored in the following folder: *JP1/ITDM2 - SDM (Smart Device Manager)-installation-folder*`\mgr\log`
	JP1/ITDM2 - SDM (Smart Device Manager) environment setting file	File stored in the following folder: *JP1/ITDM2 - SDM (Smart Device Manager)-installation-folder*`\mgr\conf`
	Files in the `uC` folder for JP1/ITDM2 - SDM (Smart Device Manager)	Files stored in the following folder: *JP1/ITDM2 - SDM (Smart Device Manager)-installation-folder*`\mgr\uC`
	Files in the `db` folder for JP1/ITDM2 - SDM (Smart Device Manager)	Files stored in the following folder: *JP1/ITDM2 - SDM (Smart Device Manager)-installation-folder*`\mgr\db`
Communication server information	JP1/ITDM2 - SDM (Communication Server) log	File stored in the following folder: *JP1/ITDM2 - SDM (Communication Server)-installation-folder*`\cms\log`
	JP1/ITDM2 - SDM (Communication Server) environment setting file	File stored in the following folder: *JP1/ITDM2 - SDM (Communication Server)-installation-folder*`\cms\conf`
	Files in the `uC` folder for JP1/ITDM2 - SDM (Communication Server)	Files stored in the following folder: *JP1/ITDM2 - SDM (Communication Server)-installation-folder*`\cms\uC`
Messaging server information	JP1/ITDM2 - SDM (Messaging Server) log	File stored in the following folder: *JP1/ITDM2 - SDM (Messaging Server)-installation-folder* `\mss\log`
	JP1/ITDM2 - SDM (Messaging Server) environment setting file	Following file: *JP1/ITDM2 - SDM (Messaging Server)-installation-folder* `\mss\conf\SdMessagingServer.ini`
JP1/ITDM2 - SDM (Smart Device Android Agent) information	JP1/ITDM2 - SDM (Smart Device Android Agent) log	Collect log data from the smart device, and then obtain the file stored in the following folder: *JP1/ITDM2 - SDM (Communication Server)-installation-folder*`\cms\log\agent` `\`*name_yyyyMMdd_hhmmss*#`.log`
JP1/ITDM2 - SDM (Smart Device iOS Agent) information	JP1/ITDM2 - SDM (Smart Device iOS Agent) log	Collect log data from the smart device, and then obtain the file stored in the following folder: J*JP1/ITDM2 - SDM (Communication Server)-installation-folder*`\cms\log\agent` `\`*name_yyyyMMdd_hhmmss*#`.log`

#: *yyyy*: year, *MM*: month, *dd*: day, *hh*: hour, *mm*: minute, *ss*: second

Tip

Information might not be obtainable, depending on the user's environment. In such cases, collect information as much as possible.

G. Commands used to acquire certificates for SSL communication

The following describes the commands used to acquire certificates for SSL communication.

The commands are stored in the following folders:

- *JP1/ITDM2 - SDM (Smart Device Manager)-installation-folder*`\mgr\uC\httpsd\sbin`
- *JP1/ITDM2 - SDM (Communication Server)-installation-folder*`\cms\uC\httpsd\sbin`

G.1 Creating a private key for the Web server (keygen command)

This section describes how to use the `keygen` command to create a private key for the Web server. The created Web server private key file is specified in the SSLCertificateKeyFile directive.

Format

```
keygen -rand file-name [encryption-type] -out key-file [-bits bit-length]
```

Arguments

-rand *file-name*

Specify any file to be used for random number generation. You must specify an appropriate file whose size is large enough for the random number generation (for example, `C:\WINNT\NOTEPAD.EXE`).

encryption-type

Specify the encryption type when encrypting the private key. If you specify this parameter, you will be requested to enter a password when creating the private key. The password must be no more than 64 characters long.

When creating the Certificate Signing Request (CSR) and starting the Web server, you will also be requested to enter the password. Note that you can skip the password entry for Web server startup. The following encryption types can be specified:

- -des
  The Data Encryption Standard (DES) is selected as the encryption type.
- -des3
  Triple DES is selected as the encryption type. This parameter does not affect the encryption type used in the communication between the Web server and the Web browser.

-out *key-file*

Specify the file to which the Web server private key is output.

-bits *bit-length*

Specify the bit length of the Web server private key. The following bit length can be specified:

- 512
- 1024
- 2048
- 4096

If this argument is omitted, `1024` is assumed.

Example

To create the httpsdkey.pem Web server private key:

```
keygen -rand C:\WINNT\NOTEPAD.EXE -out httpsdkey.pem -bits 1024
```

Related Topics

- *G.2 Creating a Certificate Signing Request (CSR) (certutil reqgen command)*
- *G.6 Create a password file (sslpasswd command)*

G.2 Creating a Certificate Signing Request (CSR) (certutil reqgen command)

This section describes how to use the certutil reqgen command to create a Certificate Signing Request (CSR). The created CSR file is submitted to the CA, which then issues the signed certificate. The CSR is created in the format conforming to PKCS #10.

Format

```
certutil reqgen [-sign signature-algorithm] -key key-file -out CSR-file
```

Arguments

-sign *signature-algorithm*

Specify the signature algorithm used when the CSR is created. The following signature algorithms can be specified:

- MD5
  `md5WithRSAEncryption` is used.
- SHA1
  `sha1WithRSAEncryption` is used.
- SHA224
  `sha224WithRSAEncryption` is used.
- SHA256
  `sha256WithRSAEncryption` is used.
- SHA384
  `sha384WithRSAEncryption` is used.
- SHA512
  `sha512WithRSAEncryption` is used.

If this argument is omitted, `SHA1` is assumed.

-key *key-file*

Specify the Web server private key file. Specify the private key file created by using the `keygen` command.

-out *CSR-file*

Specify the file to which the created CSR is output.

Example

To create a Certificate Signing Request (CSR) by using the Web server private key file `httpsdkey.pem`, specify as follows:

```
certutil reqgen -sign SHA1 -key httpsdkey.pem -out httpsd.csr
```

If you have set a password when creating the private key for the Web server, you are prompted to enter the password. For the items to be set, follow the instructions from the CA to which you submit the Certificate Signing Request (CSR).

G.3 Displaying the contents of a Certificate Signing Request (CSR) (certutil req command)

This section explains how to display the contents of a Certificate Signing Request (CSR).

Format

```
certutil req -in CSR-file -text
```

Arguments

-in *CSR-file*

Specify the CSR file to be displayed.

Example

To display the CSR file `httpsd.csr`, specify as follows:

```
certutil req -in httpsd.csr -text
```

G.4 Displaying certificate contents (certutil cert command)

This subsection explains how to display the contents of a certificate file. The following command displays the part of the certificate file that begins with -----BEGIN CERTIFICATE----- and ends with -----END CERTIFICATE----.

Format

```
certutil cert -in certificate-file -text
```

Arguments

-in *certificate-file*

Specify the certificate file to be displayed.

Example

To display the certificate file `httpsd.pem`, specify as follows:

```
certutil cert -in httpsd.pem -text
```

G.5 Converting the certificate format (certutil cert command)

This section explains how to convert the certificate format. Use this functionality as necessary.

Format

```
certutil cert -inform input-format -outform output-format -in input-file -
out output-file
```

Arguments

-inform *input-format*

Specify the input format of the certificate file before conversion. The following input formats can be specified:

- DER
- PEM

If this argument is omitted, `PEM` is assumed.

-outform *output-format*

Specify the input format of the certificate file after conversion. The following input formats can be specified:

- DER
- PEM

If this argument is omitted, `PEM` is assumed.

-in *input-file*

Specify the certificate file before conversion.

-out *output-file*

Specify the certificate file after conversion.

G.6 Create a password file (sslpasswd command)

If you want to omit the password input when starting the Web server, create a password file.

When you use the server private key protected by a password, you can save the password in advance in a file and set the directive to omit the password input when restarting the server. This procedure is described below. Note that the following procedure is required when you use the server private key protected by password:

1. Create a server private key with a password by using the `keygen` command.
2. Create a password file by the `sslpasswd` command.
3. Set the SSLCertificateKeyPassword directive that specifies the created password file together with the SSLCertificateKeyFile directive that specifies the server private key file in the `httpsd.conf`.
4. Start or restart the server.

> **Important**
>
> You need to take care when protecting the password file items. Set the directory permissions and the file permissions to prevent other users from accessing the storage directory of the server private key, and also prevent them from accessing the storage directory of the password file.

Format

```
sslpasswd server-private-key-file-name password-file-name
```

Arguments

server-private-key-file-name

Specify the password protected server private key. Specify the private key file created by using the `keygen` command.

password-file-name

Specify the name of the file that outputs password.

> **Important**
>
> You cannot specify an existing file name as the password file name.

Example

To create a password file `keypasswd`, specify as follows:

```
sslpasswd httpsdkey.pem .keypasswd
```

Related Topics

- *G.1 Creating a private key for the Web server (keygen command)*

H. Inventory information list

The following table describes inventory information that can be collected in JP1/ITDM2 - SDM.

Inventory information list

Category	Item	Description	iOS	Android
Smart Device List view	**Severity**	The highest severity of events for the smart device	Y	Y
	Name	Name such as an asset management number	Y	Y
	IMEI/MEID	IMEI/MEID acquired from the smart device	Y	Y
	ICCID	ICCID acquired from the smart device	Y	Y
	Phone Number	Phone number of the smart device from which the information is acquired	Y	Y
	Department	Department to which the user belongs	Y	Y
	User Name	Name of the user	Y	Y
	Last Modified Date/Time	Date and time that the information was last modified due to registration of a smart device or import of smart device information	Y	Y
Events tab	**Status**	Check status of the event	Y	Y
	Severity	Severity of the event	Y	Y
	Event Number	Event number	Y	Y
	Description	Event description	Y	Y
	Registered Date/ Time	Date and time that the event was registered	Y	Y
	Type	Event type	Y	Y
Call History tab	**Status**	Check status of the call history	N	Y
	Severity	Severity of the call history	N	Y
	Other Party's Phone Number	Other party's phone number acquired from the smart device	N	Y
	Category	Call category (**Made**, **Received**, **Missed**, **Unidentified**, or **Blocked**) acquired from the smart device	N	Y
	Call Start Time	Call start time acquired from the smart device	N	Y
	Call Time	Call time acquired from the smart device	N	Y
Web Browsing History tab	**Status**	Check status of the Web browsing history	N	Y
	Severity	Severity of the Web browsing history	N	Y

Category	Item	Description	iOS	Android
Web Browsing History tab	**URL**	Browsed URL acquired from the smart device	N	Y
	Browsed Date/ Time	Browsed date and time acquired from the smart device	N	Y
Software tab	**Status**	Software check status	Y	Y
	Severity	Severity of the software	Y	Y
	Application name	Name of the application installed on the smart device	Y	Y
	Version	Application version	Y	Y
	Manufacturer	Application manufacturer	Y	Y
Hardware tab	**IMEI/MEID**	IMEI/MEID acquired from the smart device	Y	Y
	ICCID	ICCID acquired from the smart device	Y	Y
	Serial Number	Serial number acquired from the smart device	Y	Y
	Model Number	Model number acquired from the smart device	Y	Y
	Model Name	Model name acquired from the smart device	Y	Y
	Manufacturer	Manufacturer name acquired from the smart device	Y	Y
	Battery Level	Battery level acquired from the smart device	Y	Y
	Internal storage (Total / Free [B])	Internal storage information acquired from the smart device	Y	Y
	SD Card (Total / Free [B])	SD card information acquired from the smart device	N	Y
	RAM (Total / Free [B])	RAM information acquired from the smart device	N	Y
	3G MAC Address	3G MAC address acquired from the smart device	N	Y
	WiFi MAC Address	WiFi MAC address acquired from the smart device	Y	Y
	Bluetooth MAC Address	Bluetooth MAC address acquired from the smart device	Y	Y
	UDID	UDID acquired from the smart device	Y	N
Running Applications tab	**Application name**	Name of the running application acquired from the smart device	N	Y
	Version	Application version	N	Y
	Manufacturer	Application manufacturer	N	Y
Running Services tab	**Service Name**	Name of the running service acquired from the smart device	N	Y
	Version	Service version	N	Y

Category	Item	Description	iOS	Android
Running Services tab	**Manufacturer**	Service manufacturer	N	Y
System Information tab	**OS**	OS information acquired from the smart device	Y	Y
	OS Version	OS version acquired from the smart device	Y	Y
	Phone Number	Phone number acquired from the smart device	Y	Y
	Mobile Network	Mobile network information acquired from the smart device	Y	Y
	SIM Card	SIM card information acquired from the smart device	Y	Y
	Roaming	Roaming information acquired from the smart device	Y	Y
	Android ID/ Apple ID	Android ID or Apple ID acquired from the smart device	N	Y
	Email	Email address acquired from the smart device	Y	Y
	IP Address	IP address acquired from the smart device	Y#	Y
	Proxy Server	Proxy server acquired from the smart device	Y	Y
	GPS Information	GPS information acquired from the smart device	N	Y
	Lock Release Password Changed During Last Lock	Unlock password that was changed the last time the lock was set	N	Y
	Department	Department to which the user belongs	Y	Y
	Account	Account of the user	Y	Y
	User Name	Name of the user	Y	Y
Security tab	**Current Security Policy**	Name of the security policy applied to the smart device	Y	Y
	Current Android Policy/iOS Profile	Android policy or iOS profile currently applied to the smart device	Y	Y
	Date/Time of Android Policy/iOS Profile Application	Date and time that the Android policy or iOS profile was applied to the smart device	Y	Y
	Android Policy/iOS Profile Version	Version of the Android policy or iOS profile that was applied to the smart device	Y	Y
	GPS Power Status	GPS power status acquired from the smart device	Y#	Y

Category	Item	Description	iOS	Android
Security tab	**Last Date/Time of Successful Lock Release**	Date and time that the last unlock was successful	N	Y
	Last Date/Time of Failed Lock Release	Date and time that the last unlock failed	N	Y
	Agent Ver.	Agent version of this product	Y	Y
Bluetooth Connection Information tab	**Status**	Check status of Bluetooth connection information	N	Y
	Severity	Severity of Bluetooth connection information	N	Y
	Connection Name	Bluetooth connection name acquired from the smart device	N	Y
	Connection Address	Bluetooth connection address acquired from the smart device	N	Y

Legend:

Y: Can be acquired

N: Cannot be acquired

#: Inventory data about a smart device will be collected only when the user taps **Send Inventory**.

I. Version Changes

The following describes the changes in each version.

I.1 Changes in version 11-10

The following change was made in version 11-10:

- Pull-distribution functionality was added that allows users to initiate the installation of applications.
- Standard distribution functionality was added that allows the distribution of large applications.
- The following commands were added:
  - sdmioutils exportdeliverypermit (exporting settings that define applications as installable by users)
  - sdmioutils importdeliverypermit (defining applications that can be installed by users)
  - sdmioutils deletedeliverypermit (deleting settings that define applications as installable by users)
  - sdmdistributeapp (sending instructions to install applications)
  - sdmapplyprofile (applying or removing an iOS profile)
  - sdmgetinvenroty (acquiring inventory information)
  - sdmexportdistributestatus (outputting application distribution status)
  - sdmexportinstallapp (outputting installed software information)
- Windows Server 2016 was added as a supported OS.

I.2 Changes in version 11-00

The following change was made in version 11-00:

- You can now distribute iOS applications to iOS devices.
- A function for setting the time at which inventory data is to be collected from iOS devices was added. In addition, the default collection time was changed.
- Information items that can be exported by exporting the smart device list were added.
- Detailed information about events on the **Events** tab can now be checked in the **Managed Device List** view.
- A function that periodically resends requests to iOS devices that do not respond was added.
- The default values of the following items were changed to 1440 minutes:
  - ios.request.getinventory.timeout.time
  - ios.request.wipe.timeout.time
  - ios.request.lock.timeout.time
  - ios.request.clearpasscode.timeout.time
  - ios.request.unmanage.timeout.time
  - ios.request.applyprofile.timeout.time
  - ios.request.removeprofile.timeout.time

- By using the MDM system linkage function of JP1/IT Desktop Management 2, the following information can now be collected:
  - Model number (Android)
  - Manufacturer name (iOS)
  - Serial number (Android)
  - Passcode settings (Android)
- Information about iOS profiles can now be edited.
- The following functions can now be disabled: periodic collection of inventory data and checking the batteries of smart devices.
- A configuration profile generation tool for iOS devices is now available.
- The following function is now supported: checking whether specific versions of applications listed in a security policy are installed.
- Request timeout functions for iOS devices are now supported.
- Applied iOS profiles can now be removed.
- You can now manage information about multiple iOS profiles.
- If a user attempts to apply an iOS profile to a locked iOS device, the attempt will no longer immediately fail. Instead, the attempt will be retried for a maximum period of 24 hours.
- Windows Server 2008 is no longer supported. (Windows Server 2008 R2 is still supported.)

J. Reference Material for This Manual

This appendix provides reference information, including various conventions, for this manual.

J.1 Related publications

This manual is part of a related set of manuals. The manuals in the set are listed below (with the manual numbers):

- *JP1 Version 11 Asset and Distribution Management: Getting Started* (3021-3-B51(E))
- *JP1 Version 11 JP1/IT Desktop Management 2 Overview and System Design Guide* (3021-3-B52(E))
- *JP1 Version 11 JP1/IT Desktop Management 2 Configuration Guide* (3021-3-B53(E))
- *JP1 Version 11 JP1/IT Desktop Management 2 Administration Guide* (3021-3-B54(E))
- *JP1 Version 11 JP1/IT Desktop Management 2 Distribution Function Administration Guide* (3021-3-B55(E))
- *JP1 Version 11 JP1/IT Desktop Management 2 - Asset Console Configuration and Administration Guide* (3021-3-B56(E))
- *JP1 Version 11 JP1/IT Desktop Management 2 - Asset Console Creating an Access Definition File Guide* (3021-3-B57(E))
- *JP1 Version 11 JP1/IT Desktop Management 2 Messages* (3021-3-B58(E))
- *JP1 Version 11 JP1/IT Desktop Management 2 - Agent Description and User's Guide (For UNIX Systems)* (3021-3-B58(E))

J.2 Conventions: Fonts

The following table explains the text formatting conventions used in this manual:

Text formatting	Convention
Bold	Bold characters indicate text in a window, other than the window title. Such text includes menus, menu options, buttons, radio box options, or explanatory labels. For example: • From the **File** menu, choose **Open**. • Click the **Cancel** button. • In the **Enter name** entry box, type your name.
Italic	Italic characters indicate a placeholder for some actual text to be provided by the user or system. For example: • Write the command as follows: `copy` *source-file* *target-file* • The following message appears: `A file was not found. (file =` *file-name*`)` Italic characters are also used for emphasis. For example: • Do *not* delete the configuration file.
`Monospace`	Monospace characters indicate text that the user enters without change, or text (such as messages) output by the system. For example: • At the prompt, enter `dir`. • Use the `send` command to send mail. • The following message is displayed: `The password is incorrect.`

J.3 Conventions: Symbols

The following table explains the symbols used in this manual:

Symbol	Convention
`|`	In syntax explanations, a vertical bar separates multiple items, and has the meaning of OR. For example: `A|B|C` means `A`, or `B`, or `C`.
`{ }`	In syntax explanations, curly brackets indicate that only one of the enclosed items is to be selected. For example: `{A|B|C}` means only one of A, or B, or C.
`[ ]`	In syntax explanations, square brackets indicate that the enclosed item or items are optional. For example: `[A]` means that you can specify `A` or nothing. `[B|C]` means that you can specify `B`, or `C`, or nothing.

J.4 Conventions: Abbreviations for product names

This manual uses the following abbreviations for product names:

Abbreviation			Full name or meaning
Firefox			Firefox(R)
JP1/ITDM2 - SDM	JP1/ITDM2 - SDM (Smart Device Agent)	JP1/ITDM2 - SDM (Smart Device Android Agent)	JP1/IT Desktop Management 2 - Smart Device Manager (Smart Device Android Agent)
		JP1/ITDM2 - SDM (Smart Device iOS Agent)	JP1/IT Desktop Management 2 - Smart Device Manager (Smart Device iOS Agent)
	JP1/ITDM2 - SDM (Smart Device Manager)		JP1/IT Desktop Management 2 - Smart Device Manager (Smart Device Manager)
	JP1/ITDM2 - SDM (Communication Server)		JP1/IT Desktop Management 2 - Smart Device Manager (Communication Server)
	JP1/ITDM2 - SDM (Messaging Server)		JP1/IT Desktop Management 2 - Smart Device Manager (Messaging Server)

J.5 Conventions: Acronyms

This manual uses the following acronyms:

Acronym	Full name or meaning
APNs	Apple Push Notification Service
CD	Compact Disc
CPU	Central Processing Unit
CSV	Comma Separated Values
DB	Database
DMZ	DeMilitarized Zone
DVD	Digital Versatile Disk

Acronym	Full name or meaning
HTTP	Hyper Text Transfer Protocol
HTTPS	Hyper Text Transfer Protocol Secure
ICCID	Integrated Circuit Card ID
IMEI	International Mobile Equipment Identity
IMSI	International Mobile Subscriber Identity
ID	IDentification
IP	Internet Protocol
IT	Information Technology
LAN	Local Area Network
MAC	Media Access Control
MDM	Mobile Device Management
OEM	Original Equipment Manufacturer
OMA-DM	Open Mobile Alliance Device Management
OS	Operating System
PC	Personal Computer
RAM	Random Access Memory
SD	Secure Digital
SIM	Subscriber Identity Module
SSL	Secure Socket Layer
Subject DN	Subject Distinguished Name
TCP	Transmission Control Protocol
TLS	Transport Layer Security
UAC	User Account Control
UDID	Unique Device IDentifier
URL	Uniform Resource Locator
USB	Universal Serial Bus
UUID	Universally Unique IDentifier
VPN	Virtual Private Network
WWW	World Wide Web
XML	Extensible Markup Language

J.6 Conventions: KB, MB, GB, and TB

This manual uses the following conventions:

- 1 KB (kilobyte) is 1,024 bytes.

- 1 MB (megabyte) is $1{,}024^2$ bytes.
- 1 GB (gigabyte) is $1{,}024^3$ bytes.
- 1 TB (terabyte) is $1{,}024^4$ bytes.

J.7 About Help

JP1/ITDM2 - SDM comes with an HTML manual that you can read in a Web browser.

You can view the help by selecting **Help** and then **IT Desktop Management2 - Smart Device Manager Help** in the JP1/ITDM2 - SDM operation window.

K. Glossary

administrator's computer

The computer a JP1/ITDM2 - SDM administrator uses to log in to JP1/ITDM2 - SDM.

Android policy

A policy used in JP1/ITDM2 - SDM to batch specify Android device functionality and usage guidelines. This policy is set on the smart device manager, and then applied to managed smart devices.

APNs

Abbreviation of *Apple Push Notification Service*, which is provided by Apple.

Comet

A technology used when making Web applications. Comet technology allows a server to hold a request from a client, without giving an immediate response, and then send a response when an event occurs on the server.

Comet connection

In JP1/ITDM2 - SDM, Comet technology is used as a means of implementing requests to Android terminals. A Comet connection indicates an HTTP connection that uses Comet technology for the connection between an Android device and JP1/ITDM2 - SDM.

communication server

A computer on which JP1/ITDM2 - SDM (Communication Server) is installed.

configuration profile

An XML file containing device and security policies, VPN configuration information, Wi-Fi settings, APN settings, Exchange account settings, email settings, and certificates that allow enterprise system operations from iPhones and iPads. You can create a configuration profile by using the iPhone Configuration Utility provided by Apple.

initialize

The act of initializing (wiping) a smart device to the factory default settings. This operation is used to prevent unauthorized use by third parties if a smart device is lost or stolen.

iOS profile

A policy used in JP1/ITDM2 - SDM to batch specify iOS device functionality and usage guidelines. This policy is set on the smart device manager, and then applied to managed smart devices. A configuration profile that is created in advance by using the iPhone Configuration Utility configuration is used as an iOS profile in JP1/ITDM2 - SDM.

iPhone Configuration Utility

A tool, provided by Apple, for creating configuration profiles. In addition to creating configuration profiles, you can use this tool to install a configuration profile on a smart device.

JP1/IT Desktop Management 2

A system that manages IT assets from device management, security management, and asset management perspectives.

JP1/ITDM2 - SDM (Communication Server)

A JP1/ITDM2 - SDM program that provides communication server functionality

JP1/ITDM2 - SDM (Messaging Server)

A program that provides the Comet function with Android devices

JP1/ITDM2 - SDM (Smart Device Agent)

The generic name for JP1/ITDM2 - SDM (Smart Device Android Agent) and JP1/ITDM2 - SDM (Smart Device iOS Agent)

JP1/ITDM2 - SDM (Smart Device Android Agent)

A JP1/ITDM2 - SDM program that provides agent functionality for Android devices

JP1/ITDM2 - SDM (Smart Device iOS Agent)

A JP1/ITDM2 - SDM program that provides agent functionality for iOS devices

JP1/ITDM2 - SDM (Smart Device Manager)

A JP1/ITDM2 - SDM program that provides server functionality

lock

The act of remotely disabling a smart device. This operation is used to prevent unauthorized third parties from using a smart device that was lost or stolen.

menu area

An area that appears in the left side of the operation window. The menu displayed in this area depends on the selected module. Select a menu item to display the corresponding information in the information area on the right side of the operation window.

messaging server

A computer on which JP1/ITDM2 - SDM (Messaging Server) is installed.

OMA-DM

An abbreviation of *Open Mobile Alliance (OMA) Device Management (DM)*, which is a device management protocol defined by the Open Mobile Alliance, which promotes standardization of mobile-related applications. OMA-DM provides functionality such as provisioning, device setup, and software upgrading.

OMA-DM Client

An OMA-DM client program that is deployed on an Android device

passcode

A password used to unlock an iOS device

provisioning

A function that automatically changes settings such as the connection destination URL and inventory data collection interval for JP1/ITDM2 - SDM (Smart Device Agent) running on a smart device managed by JP1/ITDM2 - SDM

security policy

A policy used to monitor the usage of smart devices in JP1/ITDM2 - SDM. Phone numbers, Web sites, and applications to be monitored can be set as criteria for evaluating the risk level of smart devices. A security policy is set on the smart device manager and then applied to managed smart devices.

security rule

The generic name of the following three rules for managing smart devices:

- Security policy
- Android policy
- iOS profile

severity

Three types of severity (**Critical**, **Warning**, and **Information**) are displayed for events output during JP1/ITDM2 - SDM operation by an administrator, and for events output as a result of security policy verification.

smart device

A small, portable terminal device such as a smartphone, tablet PC, or PDA.

smart device manager

A computer on which JP1/ITDM2 - SDM (Smart Device Manager) is installed.

system administrator permission

One of the permissions assignable when a user account is created in JP1/ITDM2 - SDM. A user with this permission has full access to the management features of JP1/ITDM2 - SDM.

view permission

One of the permissions assignable when a user account is created in JP1/ITDM2 - SDM. A user with this permission can view modules other than the Settings module, but cannot add new information or change existing settings.

Index

Hitachi, Ltd.

6-6, Marunouchi 1-chome, Chiyoda-ku, Tokyo, 100–8280 Japan