MobileIron Reporting Database Essentials 2.1.0.0

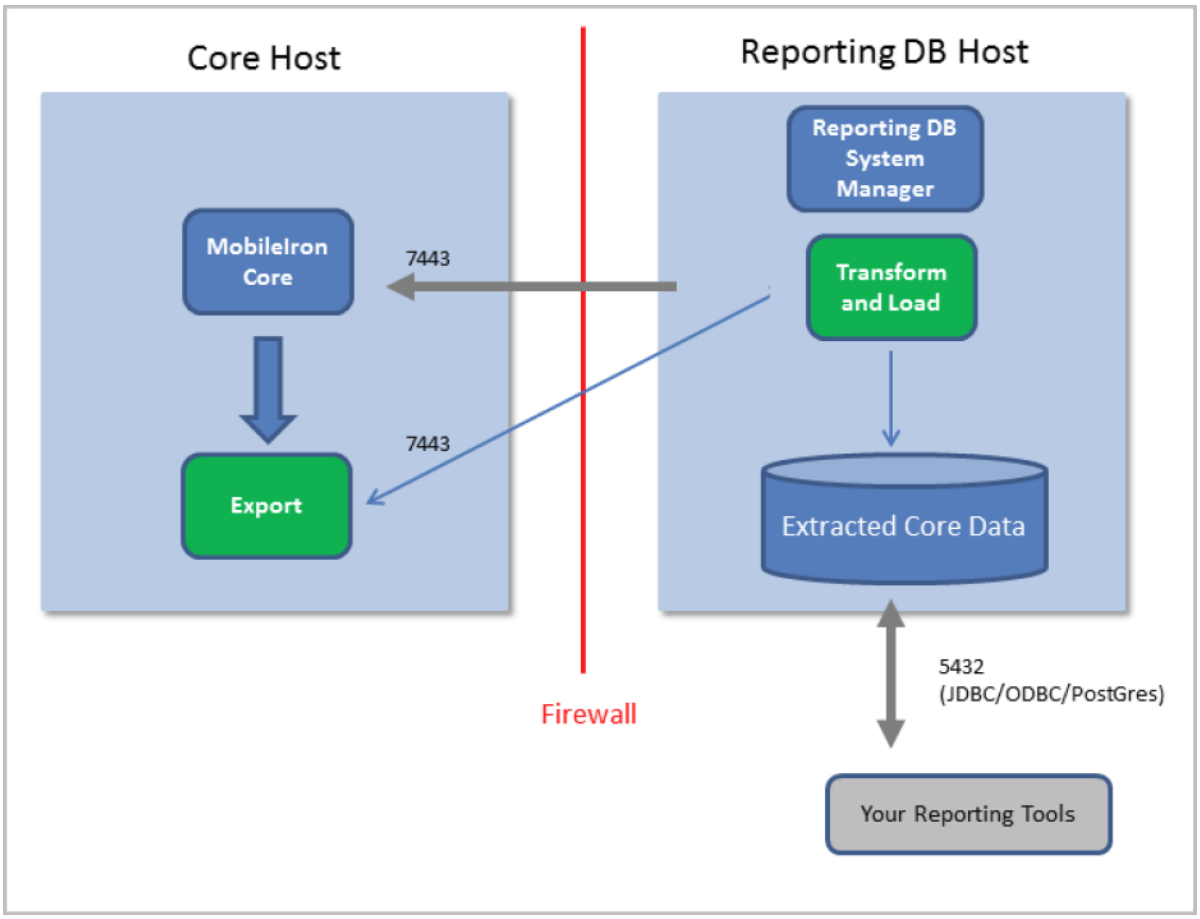
March 10, 2021

Contents

Overview

What is the MobileIron Reporting Database?

MobileIron Reporting Database is a database reporting add-on for MobileIron Core that extracts and houses data from Core in a PostgreSQL database. You use your own reporting tools and basic relational database knowledge to generate reports from the data in the Reporting Database.



Where to get the Reporting Database

The MobileIron Reporting Database ISO is available on:

https://support.mobileiron.com/support/CDL.html

Prerequisites

Software	• An active MobileIron Core system, v7.0 through v9.0 • The MobileIron Reporting Database ISO. • JDBC and/or ODBC client components and drivers for access to the MobileIron Reporting Database, or a database client with a native PostgreSQL connector. • VMware ESX/ESXi 4.x or 5 • Microsoft Hyper-V Server 2008, Microsoft Hyper-V Server 2008 R2, or Microsoft Hyper-V Server 2012
Network	• Port 7443 open between MobileIron Core and the Reporting Database • Port 5432 open between the Reporting Database and your reporting tools
VM Sizing	• To export and house data from a MobileIron Core instance managing 1,000 devices: - **Processor**: 2.53 GHz Quad-core - **Memory**: 8 GB - **Storage**: 80 GB hard drive • To export and house data from a MobileIron Core implementation managing up to 100,000 devices on up to 5 Core instances: - **Processor**: 2.53 GHz Quad-core - **Memory**: 16 GB - **Storage**: 250 GB hard drive
Guest OS	CentOS 4/5/6/7 (64 bit)

Supported upgrade paths

- 1.7.0.0 → 1.8.0.0 → 1.9.0.0 →1.9.1.0 → 2.0.0.0 → 2.1.0.0
- 1.7.0.0 → 1.8.0.0 → 1.8.0.2 → 1.9.1.0 → 2.0.0.0 → 2.1.0.0
- 1.8.0.2 → 1.9.1.0 → 2.0.0.0 → 2.1.0.0
- 1.8.0.0 → 1.9.1.0 → 2.0.0.0 → 2.1.0.0
- 1.9.0.0 → 1.9.1.0 → 2.0.0.0 → 2.1.0.0

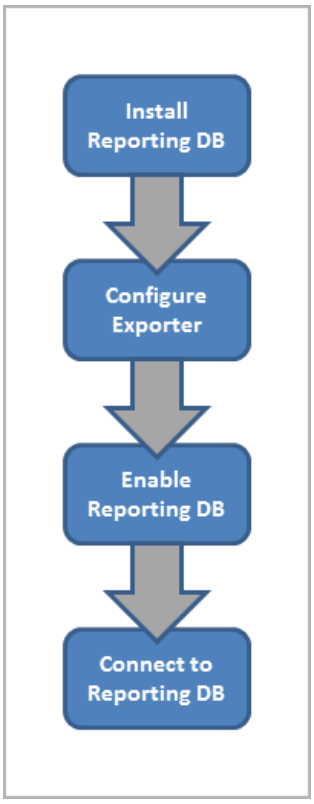
Required information

You need to gather the following information before running the MobileIron Reporting Database installation script:

Item	Description	Values
Licensing agreement information	The company name, contact person name, and contact person email address for the end-user licensing agreement.	
Mobileiron Reporting Database Server IP Address	IP address for portal access.	
External Host- name	Fully-qualified domain name for the Mobileiron Reporting Database. Devices will not connect to MobileIron Reporting Database from the internet, so an internal host-name is acceptable here.	
"enable secret" password	The MobileIron password to be defined for enabling access to Privileged and Configuration modes.	
Administrator User Name	The user name to define for the MobileIron Administrator. Do not use root.	
Administrator Password	The password to set for the MobileIron Administrator. Passwords must have at least 8 characters. Passwords must contain at least 1 alphabetic character. Passwords must contain at least 1 numeric character. Passwords cannot have 4 or more repeating characters. Passwords cannot be the same as the user ID. Password may contain Unicode characters, except for CLI access. Users cannot change a password more than once during a 24 hour period.	
Physical Interface	The physical interface to use on the appliance. Enter a or b. You can configure additional physical interfaces later using the Admin Portal.	
IP Address Netmask	The IP address and netmask of the physical net-	

Item	Description	Values
	work interface.	
Default Gateway	The IP address of the router used to forward traffic to destinations outside of the local network or sub-net.	
Name Server 1, 2, 3	The IP address of a network name server (i.e., DNS server). You must specify at least one name server.	
Remote Shell via SSH?	Specifies whether you want to configure remote shell access via SSH.	
Remote Shell via Telnet?	Specifies whether you want to configure remote access via Telnet.	
NTP Server 1, 2, 3	Specifies the IP address of an optional reliable time source. MobileIron recommends specifying an NTP server. If you do not, you will have the oppor-tunity to set the system clock and date.	

Setup overview

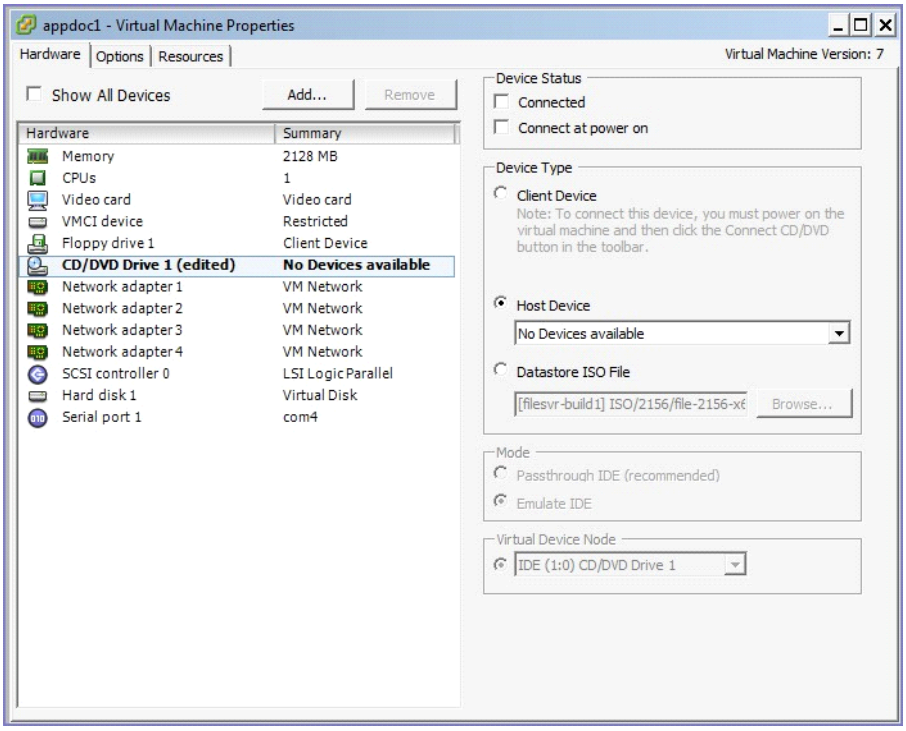

Install Reporting DB
Configure Exporter
Enable Reporting DB
Connect to Reporting DB

Installation, Configuration, and Maintenance

Installing the Reporting Database

To install the MobileIron Reporting Database appliance on VMware:

1. If you have not done so already, create a VM that meets MobileIron's recommended specifications. See Prerequisites for information on VM sizing.
2. Place the ISO distribution in an existing vSphere datastore.
3. In the vSphere Client, select the Edit Settings option for the VM you created.



4. Select **Datastore ISO File**.
5. Click Browse to select the Mobileiron Reporting Database ISO distribution.
6. Make sure the "Connected" and "Connect at power on" options in the Virtual Machine Properties screen are selected.
7. Select **Host Device**.
8. Click **OK**.
9. Power on the VM.
   The VM automatically installs and reloads after a few minutes, and the installation program starts. The following table summarizes the prompts and entries.

	Prompt	What to do
1	**Welcome to the Mobileiron Reporting Database Installation Program** For virtual machine installation, type: **vm-install<ENTER>** For standard physical appliance installation, type: **hw-install<ENTER>** For M2500 series physical appliance installation, type: **hw-m2500-install<ENTER>** **To boot from your hard disk, type:<ENTER>** **Note: System will boot from the local hard disk in 30 seconds if no key is pressed.**	Enter **vm-install**. The package installation process starts and continues for several minutes.
2	**Welcome to the MobileIron Configuration Wizard** **Use the '-' character to move back to the previous field** **Continue with configuration dialog? [yes/no]**	Enter **yes**. Scroll through the displayed license agreement.
3	**Do you accept the End User License Agreement? [yes/no]**	Enter **yes**.
4	Provide the company name, contact person name and email **Company name:**	Enter the company name. **Note:** The company name you enter will serve as the default enterprise name used in SMS and email communication.
5	**Contact person name:**	Enter the name of the member of your organization who will serve as the contact point for MobileIron communications.

	Prompt	What to do
6	`Contact person email:`	Enter the email address for the contact person.
7	`The enable secret is a password used to protect access to privileged EXEC and configuration modes. This password, after entered, becomes encrypted in the configuration.` `Enter enable secret:`	Enter the password to assign. The password must be between 6 and 20 characters.
8	`Enter enable secret (confirm):`	Re-enter the enable secret password.
9	`Administrator User Name:`	Enter the user name you want to assign for the first administrative user. **Do not use** root.
10	`Administrator Password:`	Set the password for the administrator. This password must contain at least 8 characters and include numerals and capital letters.
11	`Administrator Password (confirm):`	Re-enter the administrator password.

12	`Available network interfaces:`
	`GigabitEthernet1`
	`GigabitEthernet2`
	`Select the interface that will be used to connect to the management network.`
		Enter the letter for the physical interface you want to use.

13	`IP Address:`	Enter the IP address that you created for the Mobileiron Reporting Database. It will be associated with the physical interface you selected in the previous step.
14	`Netmask:`	Enter the netmask for use with the IP

	Prompt	What to do
		address you just entered, e.g., 255.255.255.0.
15	`Default Gateway:`	Enter the default network gateway for the Mobileiron Reporting Database.
16	`External Hostname (Fully-Qualified Domain Name):`	Fully-qualified domain name for the Mobileiron Reporting Database. Devices will not connect to MobileIron Reporting Database from the internet, so an internal hostname is OK here.
17	`Name Server 1:`	Enter the IP address of the primary name server to be used by the Mobileiron Reporting Database.
18	`Name Server 2:`	Enter optional secondary and tertiary name servers as preferred Leave the fields blank and press Enter to skip specifying additional name servers.
19	`Enable remote shell access via SSH [yes/NO]:`	Enter **yes** to enable remote access via SSH.
20	`Enable remote shell access via Telnet [yes/NO]:`	If you want to enable Telnet access, enter yes. We recommend that you enter **no**.
21	`Configure NTP? [yes/NO]:`	Enter **yes** to configure an optional reliable time source. We recommend that you configure at least one time source to ensure proper synchronization of time-based tasks.
22	`NTP Server 1:`	If you entered **yes** for configuring a time source, enter the IP address of the primary time source to use. If you specified a time source, you can

	Prompt	What to do
		enter secondary and tertiary time sources. If you do not specify at least one time source, then you have the option to configure the system clock, use HH:MM:SS as the format for the time you enter. Use DD MM YYYY as the format for the date you enter.
23	`The following configuration command script was created: Commit Changes [yes/no]:`	Review the displayed command script and enter **yes**.
24	`Configuration complete.` `Please type 'reload' at the CLI prompt to reboot the system and access the portal.`	Enter **reload**.
25	`System configuration may have been modified. Save? [yes/no]`	Enter **yes**.
26	`Configuration saved. Proceed with reload?`	Enter **yes**. The installation script continues, displaying status on the console. This may take several minutes.
27	`**********` `Mobileiron Reporting Database CLI`	

Managing monitoring the monitor server

You can enable self-monitoring of the RDB server so that MobileIron Monitor can display RDB health information. You can also disable it and check the status.

Enabling monitoring the monitor

1. Login to CLISH.
2. Enter the following commands:
   ```
   configure terminal
   self-monitor enable
   ```

3. Enter yes to confirm.

Disabling monitoring the monitor

To disable Self Monitoring:

1. Login to CLISH.
2. Enter the following command:
   `no self-monitor`
3. Enter yes to confirm.

Checking the status of monitoring the monitor

You can check whether this feature is on or off.

To check the status of monitoring the monitor:

Method 1:

1. Login to CLISH.
2. Enter the following command:
   `show self-monitor`
   The system returns true or false.

Method 2:

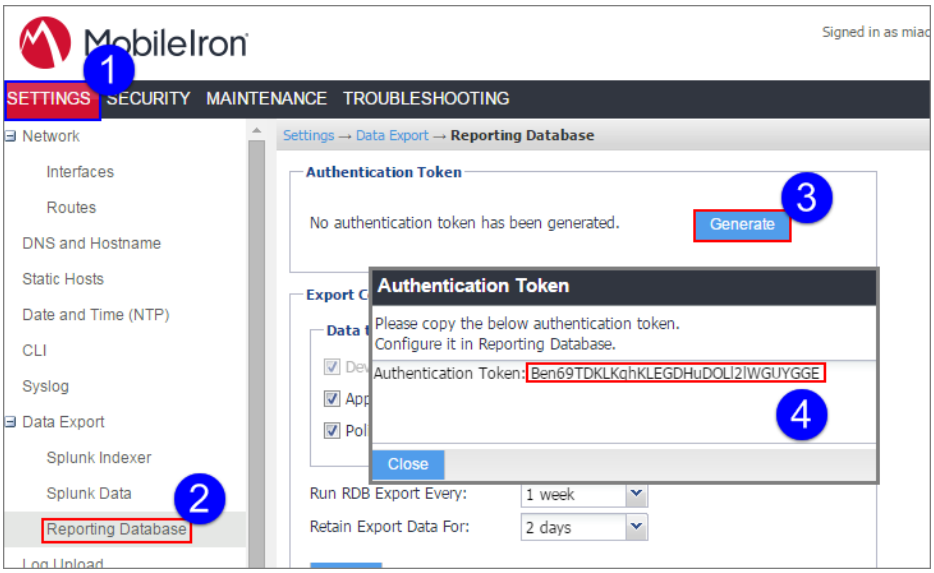
1. Login to CLISH.
2. Enter the following command:
   ```
   configure terminal
   do show self-monitor
   ```
   The system returns true or false.

Configuring the Exporter

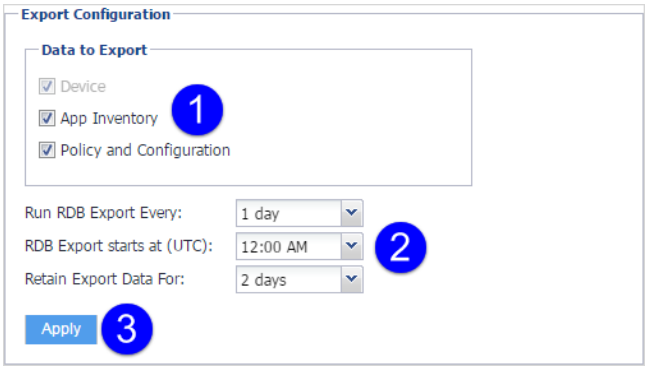
Configuring the Reporting Database Exporter allows the MobileIron Reporting Database to extract the relevant MobileIron Core data.

To configure MobileIron Core to work with the MobileIron Reporting Database system:

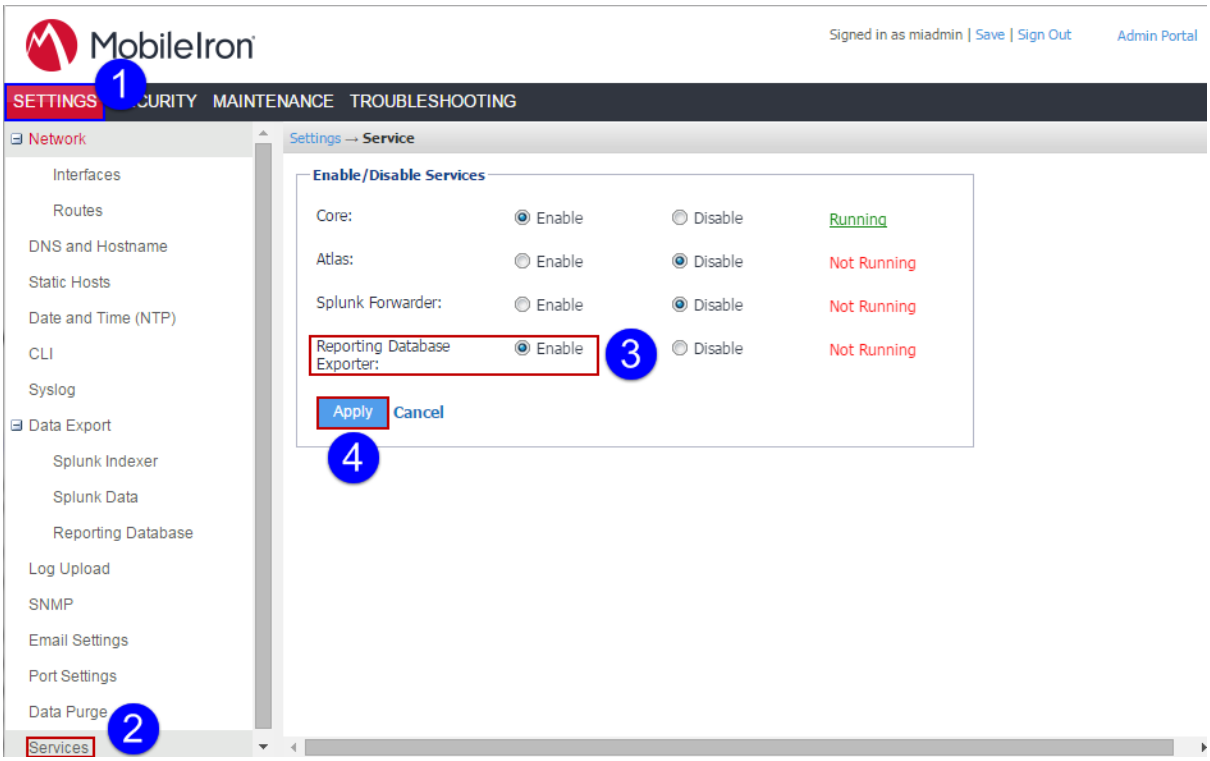
1. In the MobileIron Core System Manager, go to **Settings > Data Export > Reporting Database.**
2. Click **Generate**.
3. Copy the displayed token to the clipboard.
   You will use the authentication token when you configure the Reporting Database.



4. Under **Data to Export**, select or clear data categories to specify the data to export or omit. The **Device** option is required and cannot be cleared.
5. Select a frequency from the **Run RDB Export Every** drop-down.
   Note: You can run the RDB Export on demand without waiting for the next run. Running the RDB export on demand
6. If you selected **1 Week** from the **Run RDB Export Every** drop-down, then select a day to run the RDB export from the **Run RDB Export On** drop-down.
7. Select a time to start the RDB export from the **RDB Export starts at (UTC)** drop-down.
8. Select a retention time from the **Retain Export Data For** drop-down.
9. Click **Apply**.



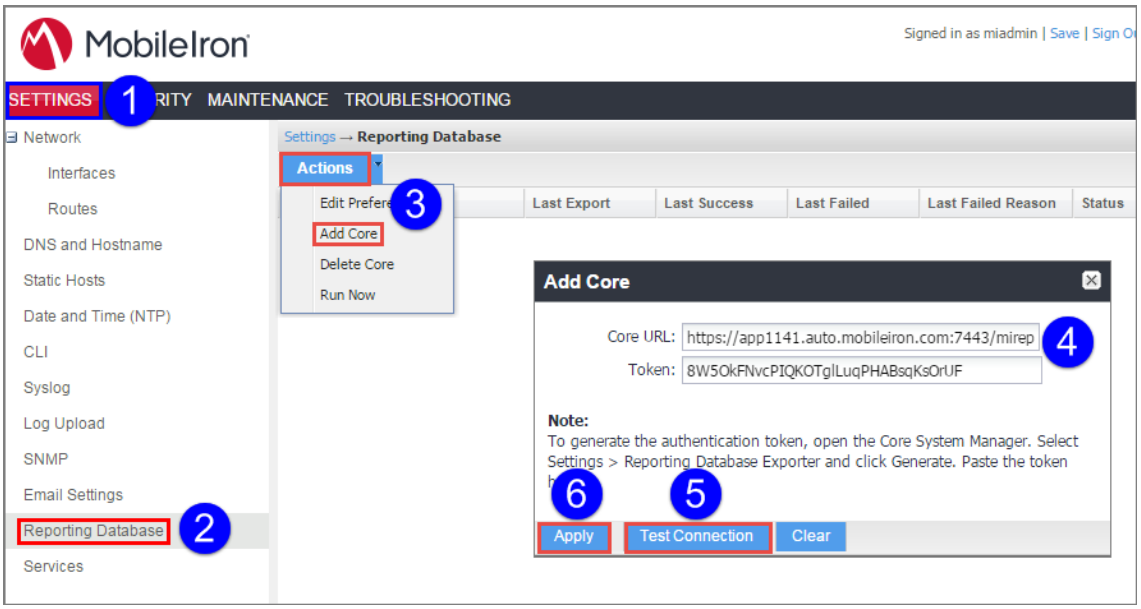
10. Go to **Settings** > **Services**.
11. Select **Enable** for the **Reporting Database Exporter**.
12. Click **Apply**.



Enabling the Reporting Database

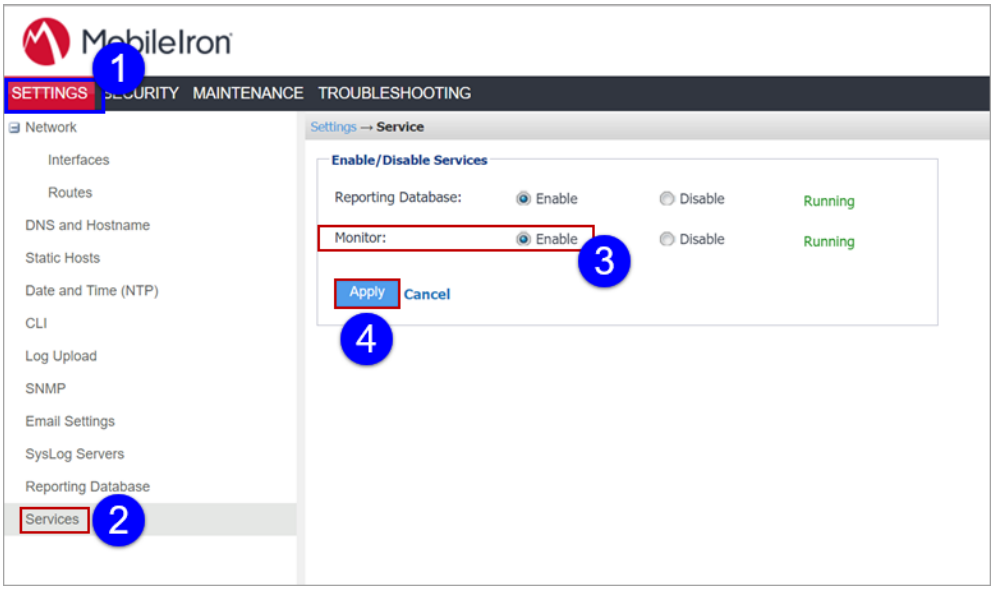
To configure the MobileIron Reporting Database:

1. Log into the MobileIron Reporting Database System Manager at: **https://*<RDB SERVER>*:8443/mics/mics.html**
2. Go to **Settings > Reporting Database > Actions > Add Core.**
3. In the **Core URL field**, enter **https://*<Core host name>*:7443/mireport**.
4. In the **Token** field, paste the token that you copied in Configuring the Exporter.
5. Click **Test Connection** to confirm that the Core instance is reachable.
6. Click **Apply**.



7. Go to **Settings > Services > Reporting Database**.
8. Select **Enable** for **Reporting Database**, and then click **Apply**. If you plan to run MobileIron Monitor, then also select **Enable** for **Monitor**.

NOTE: If you choose to run MobileIron Monitor, check the hardware, software, and server requirements in the *Monitor Configuration Guide*.

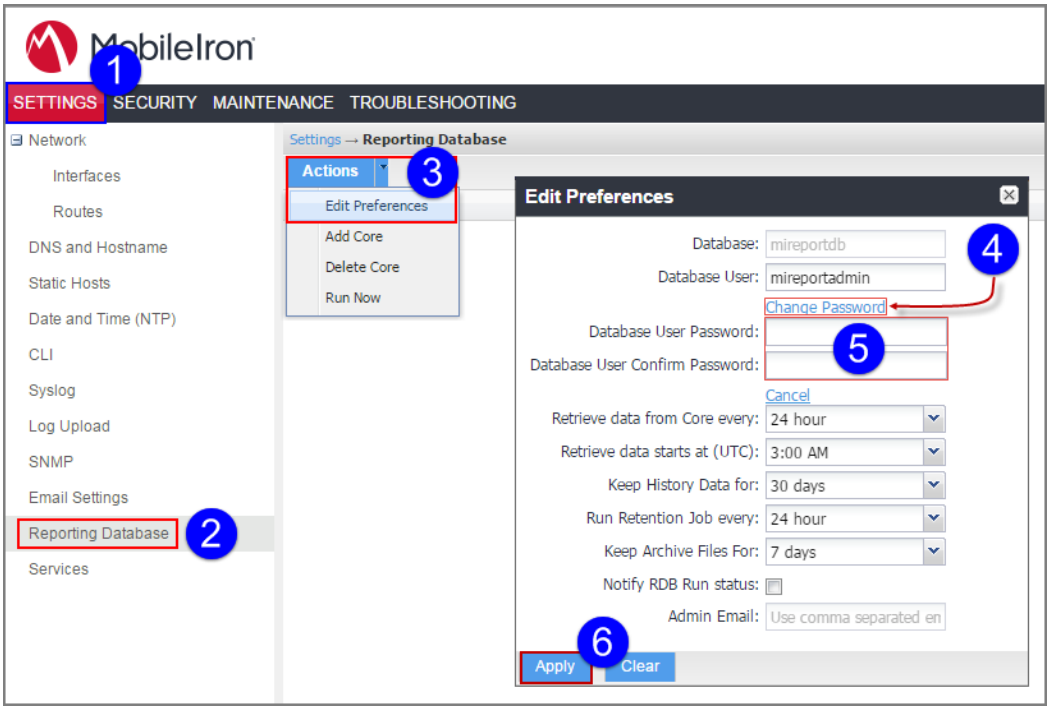


9. Go to **Maintenance > Reboot**.
10. Click **Reboot**.

Changing the database user's password

All MobileIron Reporting Databases have the same default credentials to start. Therefore, we recommend changing the password for the default Reporting Database user:

1. Log into the MobileIron Reporting Database System Manager at: **https://*<RDB SERVER>*:8443/mics/mics.html**
2. Go to **Settings > Reporting Database**
3. Select Actions > Edit Preferences.
4. Click **Change Password**.
5. In the **Database User Password** field, enter the new password you want to set. Enter at least 8 characters.
6. In **Database User Confirm Password** field, re-enter the password.
7. Click **Apply**.



Connecting to the Reporting Database

Confirm your setup by connecting to the Reporting Database. You can use JDBC or ODBC clients, or even non-JDBC/ODBC tools (such as Tableau and Qlickview) that have native connectors to PostgreSQL databases.

The default credentials for Reporting Database access are:

- Database name: mireportdb
- Username: mireportadmin
- Password: MIRDBvuucP787Q#

Consider changing the password. See Changing the database user's password.

Running the RDB export on demand

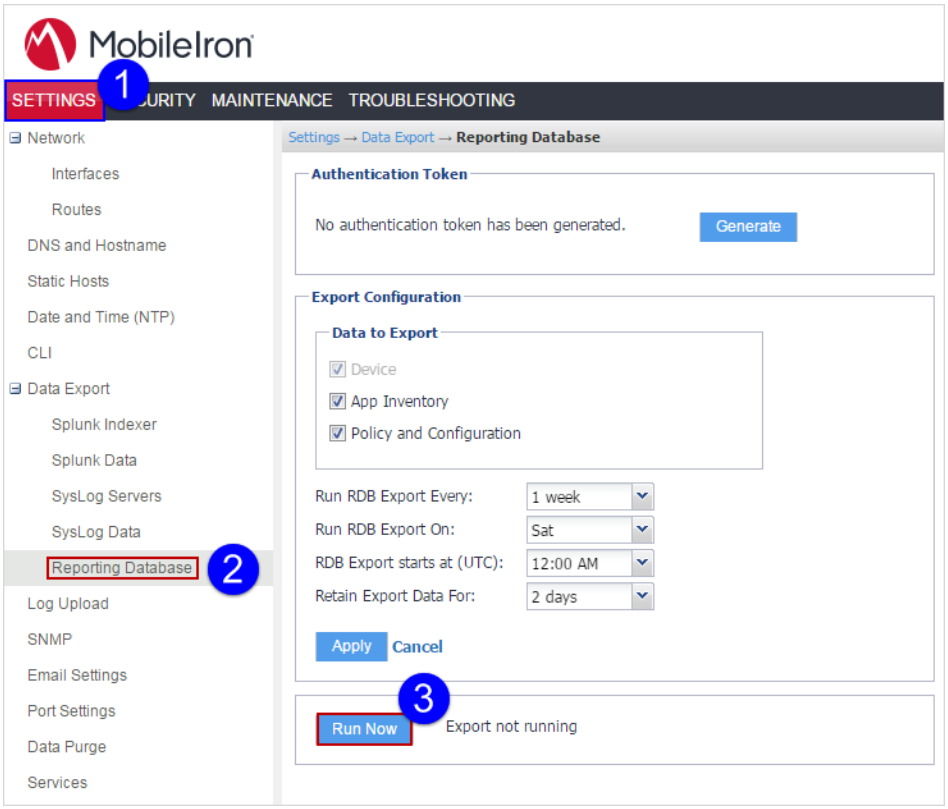
You can run the RDB export on demand without waiting for the interval you specified in step Select a frequency from the Run RDB Export Every drop-down. in the section Configuring the Exporter. This allows you to get data right away in situations where you need to report on data immediately.

You can run the RDB export on demand either from the MobileIron Core System Manager or the MobileIron Reporting Database System Manager.

Running the RDB export on demand from the MobileIron Core System Manager

To run the RDB export on demand from the MobileIron Core System Manager:

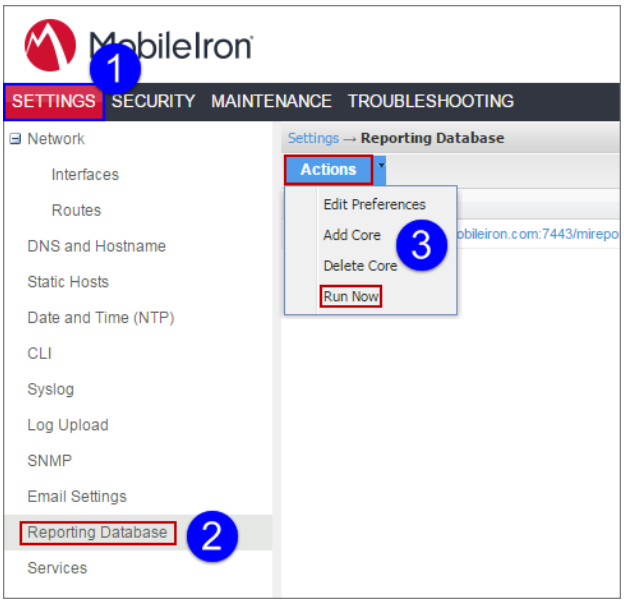
1. In the MobileIron Core System Manager, go to **Settings > Data Export > Reporting Database.**
2. Click **Run Now**.



Running the RDB export on demand from the MobileIron Reporting Database System Manager

To run the RDB export on demand from the MobileIron Reporting Database System Manager:

1. Log into the MobileIron Reporting Database System Manager at:
   https://<*RDB SERVER*>:8443/mics/mics.html
2. Select **Settings > Reporting Database > Actions > Run Now**.



Monitoring system storage

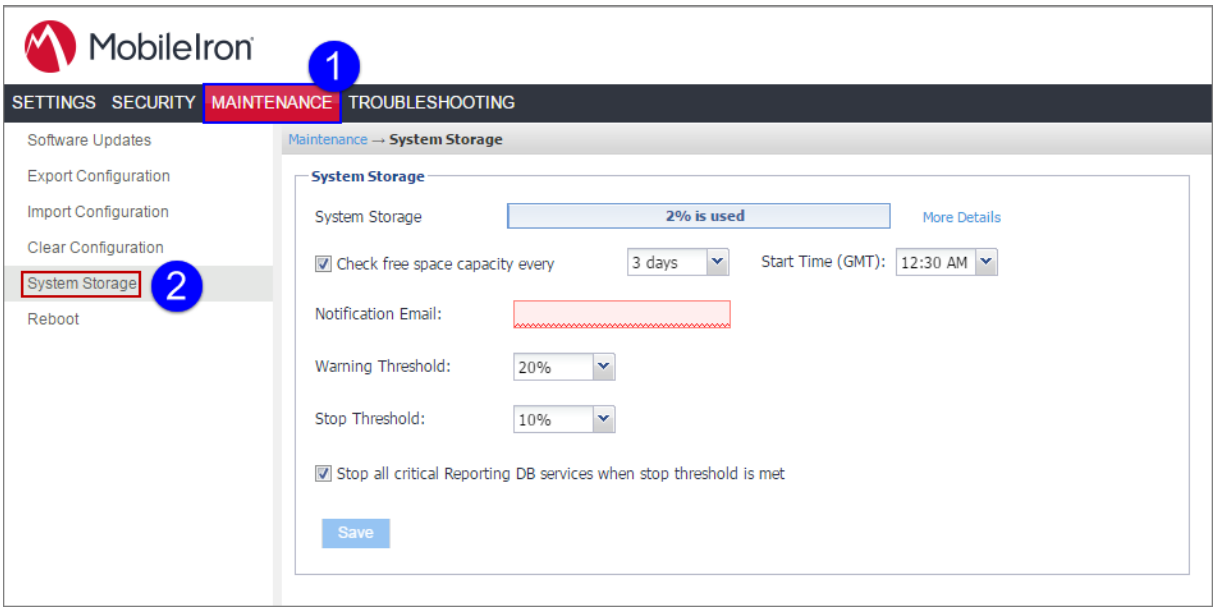
You can configure MobileIron Reporting Database System Manager to send you an email when it detects that its available disk storage space has dropped below thresholds that you define. Specifically:

- When the available space is less than a warning threshold, you receive a warning email.
- When the available space is less than a stop threshold, you receive an email and, after a five minute delay, MobileIron Reporting Database System Manager stops critical services.

Configuring system storage monitoring

To configure system storage monitoring:

1. Log into the MobileIron Reporting Database System Manager at:
   https://<*RDB SERVER*>:8443/mics/mics.html
2. Go to **Maintenance > System Storage.**



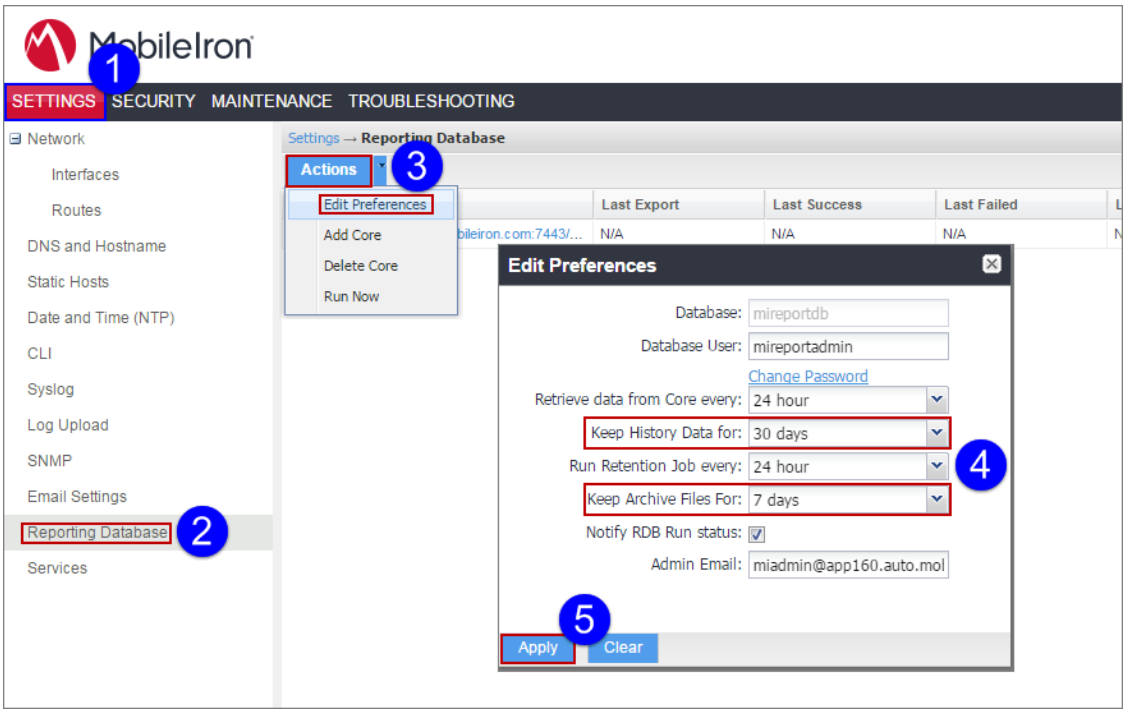
3. Select **Check free space capacity every.**
4. Select how many days between each check.
5. Select the time of day to check.
   Important: The time is GMT (Greenwich Mean Time). Select a time that is during your work hours so that you see the notification emails at a time of day when you can take actions.
6. Enter the email addresses for receiving the notifications. Separate email addresses with commas.
7. Select a **Warning threshold**.
   For example, the default value is 20%, which means an email notification is sent when disk storage availability drops to less than 20% of disk storage capacity.
8. Select a **Stop Threshold**.
   For example, the default value is 10%. When disk storage availability drops to less than the threshold, an email notification is sent when **both** of the following are true:
   - Disk storage availability drops to less than 10% of disk storage capacity.
   - You have selected **Stop all critical Reporting DB services when stop threshold is met**.
9. Select **Stop all critical Reporting DB services when stop threshold is met.**
10. Click **Save**.

Freeing system storage space

To create more free space on the MobileIron Reporting Database server, configure lower values for history and archive retention. You need to wait for the associated scheduled jobs to run to free the disk space.

To create more free space on the MobileIron Reporting Database server:

1. Log into the MobileIron Reporting Database System Manager at:
   https://*<RDB SERVER>*:8443/mics/mics.html
2. Go to **Settings > Reporting Database.**



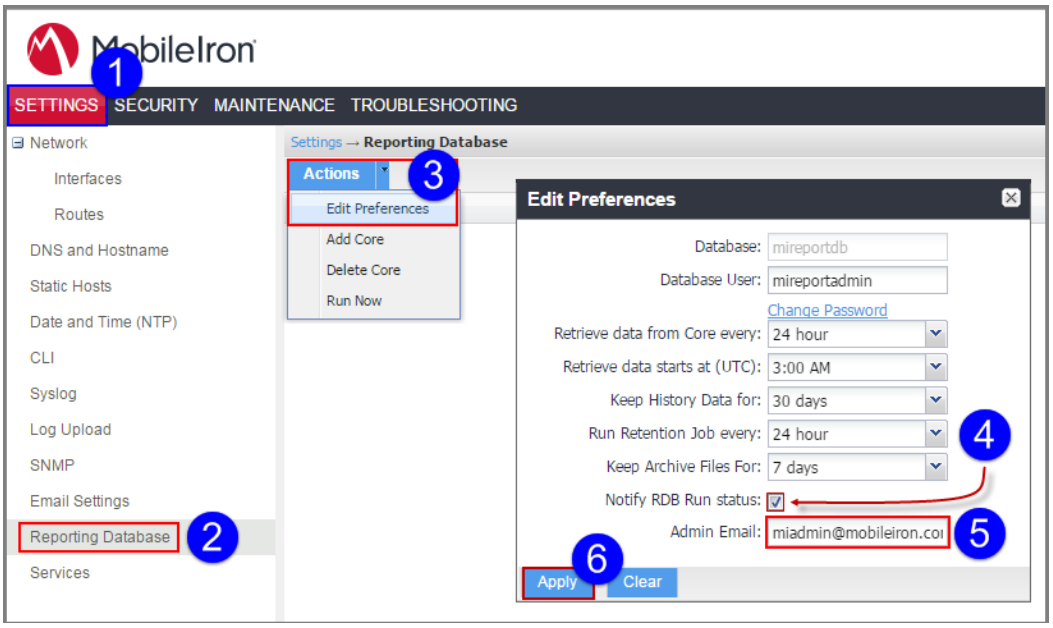
3. Select **Edit Preferences** form the **Actions** drop-down menu.
4. Configure lower values for the **Use the Keep History Data for** and **Keep Archive Files** fields.
5. Click **Apply**.

Sending RDB run status notifications

You can configure the MobileIron Reporting Database to send RDB run status notification emails that contain information about the status of the current RDB run.

To configure RDB run status notification emails:

1. Log into the MobileIron Reporting Database System Manager at:
   https://*<RDB SERVER>*:8443/mics/mics.html
2. Go to **Settings > Reporting Database**
3. Select Actions > Edit Preferences.
4. Place a check mark in the **Notify RDB Run status** box.
5. In **Admin Email** field, enter the email of the admin to receive the RDB run status emails.
6. Click **Apply**.



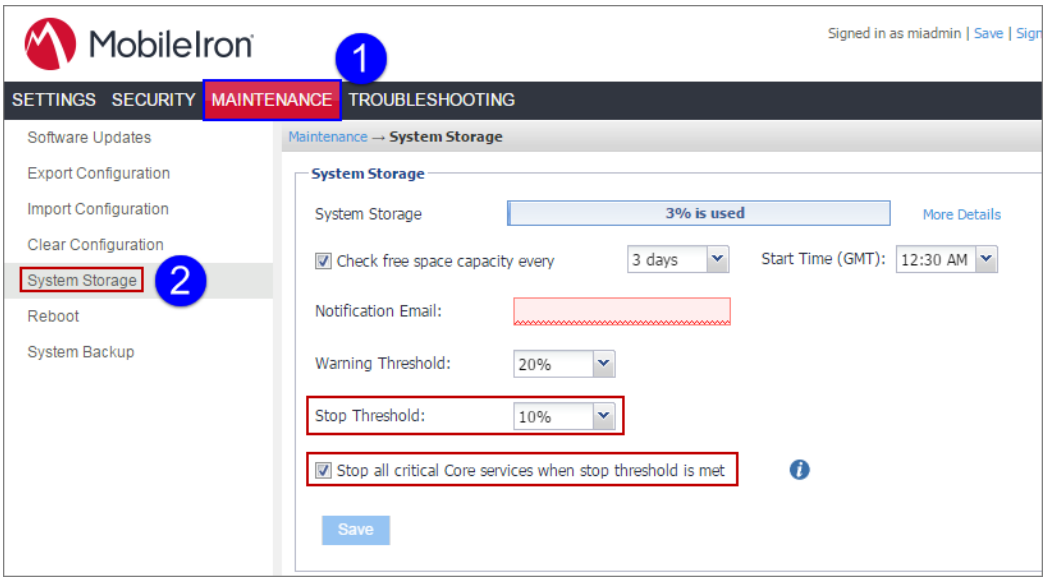
Troubleshooting

RDB export has ceased running at defined intervals

The MobileIron Core system or the MobileIron Reporting Database system may reached its System Storage Stop Threshold, resulting in the stoppage of critical services, including Reporting Database services.

To check the MobileIron Core's System Storage settings:

1. In the MobileIron Core System Manager, go to **Maintenance > System Storage.**
2. Observe the settings in the System Storage pane.



To check the MobileIron Reporting Database System Storage settings, see Monitoring system storage.

Data Dictionary

App inventory: MI_APP_INVENTORY

The MI_APP_INVENTORY table contains a record for each app detected on a registered device.

Name	Data type	Not Null?	Primary key?	Description
etl_run_ts	timestamp	Yes	No	Timestamp at which the ETL process has run
vsp_id	integer	No	No	The identifier of VSP from which this policy got exported
app_id	integer	No	No	Identifier of the application
name	varchar(255)	No	No	Name of the application
bundle	varchar(255)	No	No	Bundle of the app
platform	varchar(1)	No	No	App platform, 'I' - iOS, 'A' - Android
version	varchar(255)	No	No	Version of the app
long_version	varchar(255)	No	No	Long version of the app
short_version	varchar(255)	No	No	short version of the app
created_at	timestamp	No	No	First time this app appeared on the core
modified_at	timestamp	No	No	Last change in status or created timestamp

Configurations: MI_CONFIG table

The MI_CONFIG table contains a record for each configuration defined in MobileIron Core, regardless of whether it has been applied to a device.

Name	Data type	Not Null?	Primary key?	Description
etl_run_ts	timestamp	Yes	No	Timestamp at which the ETL process has run

Name	Data type	Not Null?	Primary key?	Description
vsp_id	integer	No	No	The identifier of VSP from which this policy got exported
config_id	integer	No	No	Identifier of the configuration
config_uuid	varchar(64)	No	No	UUID of the configuration
config_name	varchar(64)	No	No	Name of the configuration
config_type	varchar(64)	No	No	Type of the configuration, SCEP, EXCHANGE, WIFI, CERTIFICATE, VPN, RESTRICTION, WEBCLIP etc.
config_source	varchar(64)	No	No	Source of the configuration, SYSTEM - System created, ADMIN - Admin created
description	varchar(255)	No	No	Configuration description that admin configured
hash	varchar(64)	No	No	Fingerprint of all the associated entries of this configuration
created_at	timestamp	No	No	Date and time at which this configuration is created
version	integer	No	No	Version policy, number of times the configuration got modified
last_modified_at	timestamp	No	No	Last modified date and time
created_by	integer	No	No	The id of the user who created this policy, maps to user_id in mi_user table, if a device is registered to this user. 9000 is the default id for the system created default policies
last_modified_by	integer	No	No	Id of the user who modified the policy

Common device fields: MI_DEVICE table

The set of common device fields in the MI_DEVICE table comprises data from various tables in the VSP database. The MI_DEVICE table is the main/master table that stores all devices.

Name	Data type	Not Null?	Primary key?	Description
etl_run_ts	timestamp without time	Yes	No	The time the snapshot is taken on VSP.

Name	Data type	Not Null?	Primary key?	Description
	zone			
vsp_id	integer	No	No	
device_id	bigint	No	No	VSP device_id. The combination of etl_run_ts + vsp_id + device_id makes the primary key for this table.
device_uuid	character varying(64)	No	No	
battery_level	bigint	No	No	Indicates the device's battery level.
blocked	boolean	No	No	Indicates whether the device is blocked.
blocked_reasons	character varying(256)	No	No	Describes why the device is blocked. See Values for the MI_DEVICE.blocked_reasons, MI_DEVICE.noncompliance_reasons, and MI_DEVICE.quarantined_reasons Fields for more information.
cellular_technology	character varying(255)	No	No	
client_build_date	timestamp without time zone	No	No	
client_id	bigint	No	No	
client_name	character varying(255)	No	No	
client_version	character varying(255)	No	No	
comment	character varying(256)	No	No	
compliant	boolean	No	No	
current_country_code	character varying(255)	No	No	
current_country_name	character varying(255)	No	No	
current_operator_name	character varying(255)	No	No	
current_phone_	character	No	No	

Name	Data type	Not Null?	Primary key?	Description
number	varying(255)			
device_encrypted	boolean	No	No	Device is encrypted
display_size	character varying(255)	No	No	
eas_last_sync_time	timestamp without time zone	No	No	
geographic_ coordinates	character varying(255)	No	No	
geographic_ coordinates_capture_ time	timestamp without time zone	No	No	
home_country_code	character varying(255)	No	No	
home_country_name	character varying(255)	No	No	
home_operator_name	character varying(255)	No	No	
home_phone_number	character varying(255)	No	No	
imei	character varying(255)	No	No	The device's International Mobile Station Equipment Identity.
imsi	character varying(255)	No	No	The device's International mobile Subscriber Identity.
lang_country_id	bigint	No	No	
language	character varying(255)	No	No	
language_id	bigint	No	No	
last_connected_at	timestamp without time zone	No	No	
locale	character varying(255)	No	No	
manufacturer	character	No	No	

Name	Data type	Not Null?	Primary key?	Description
	varying(255)			
mdm_managed	boolean	No	No	
memory_capacity	bigint	No	No	
memory_free	bigint	No	No	
model	character varying(255)	No	No	
modified_at	timestamp	No	No	When device details were modified.
noncompliance_ reasons	character varying(256)	No	No	Describes why the device is non-compliant. See Values for the MI_ DEVICE.blocked_reasons, MI_ DEVICE.noncompliance_reasons, and MI_DEVICE.quarantined_reasons Fields for more information.
os_version	character varying(255)	No	No	
owner	character varying(255)	No	No	Indicates the device's owner. See Values for the MI_DEVICE.owner Field for more information.
pending_device_ passcode	character varying(255)	No	No	
pending_device_ passcode_expiration_ time	timestamp without time zone	No	No	
platform	character varying(255)	No	No	Indicates the device's platform. See Values for the MI_DEVICE.platform Field for more information.
platform_name	character varying(255)	No	No	Indicates the device's platform name. See Values for the MI_ DEVICE.platform_name Field for more information.
processor_ architecture	character varying(255)	No	No	
quarantined	boolean	No	No	
quarantined_action	bigint	No	No	

Name	Data type	Not Null?	Primary key?	Description
quarantined_reasons	character varying(256)	No	No	Describes why the device is quarantined. See Values for the MI_DEVICE.blocked_reasons, MI_DEVICE.noncompliance_reasons, and MI_DEVICE.quarantined_reasons Fields for more information.
registration_date	timestamp without time zone	No	No	
registration_imsi	character varying(255)	No	No	
registration_uuid	character varying(255)	No	No	
retired	boolean	No	No	
roaming	boolean	No	No	
security_state	character varying(255)	No	No	
serial_number	varchar	No	No	
sd_card_encrypted	boolean	No	No	Is the SD card encrypted.
status	character varying(255)	No	No	Indicates the device's status. See Values for the MI_DEVICE.status Field for more information.
storage_capacity	bigint	No	No	
storage_free	bigint	No	No	
wifi_mac_address	character varying(255)	No	No	

Android-only device fields: MI_DEVICE_ANDROID table

The set of Android-only device fields in the MI_DEVICE_ANDROID table comprises only Android-specific device details. It has a one-or-zero to one relationship with the MI_DEVICE table. If a device is not an Android device, the record will not be here.

Name	Data type	Not Null?	Primary key?	Description
etl_run_ts	timestamp without time zone	Yes	No	The time the snapshot is taken on VSP.
vsp_id	integer	No	No	
device_id	bigint	No	No	VSP device_id. The combination of etl_run_ts + vsp_id + device_id makes the primary key for this table.
device_uuid	character varying(64)	No	No	
dpm_encryption_status	varchar	No	No	
admin_activated	boolean	No	No	
board	character varying(255)	No	No	
brand	character varying(255)	No	No	
c2dmtoken	character varying(255)	No	No	
codename	character varying(255)	No	No	
device	character varying(255)	No	No	
device_roaming_flag	boolean	No	No	
incremental	character varying(255)	No	No	
mdm_enabled	boolean	No	No	
media_card_capacity	bigint	No	No	
media_card_free	bigint	No	No	
multi_mdm	boolean	No	No	
os_build_number	character varying(255)	No	No	
platform_flags	character varying(255)	No	No	

Name	Data type	Not Null?	Primary key?	Description
registration_status	varchar	No	No	
security_detail	bigint	No	No	
security_patch	varchar	No	No	
security_reason	varchar	No	No	
usb_debugging	boolean	No	No	

Device app inventory: MI_DEVICE_APP_INVENTORY

The MI_DEVICE_APP_INVENTORY table contains a record for each app/device association, based on the app inventory detected on registered devices.

Name	Data type	Not Null?	Primary key?	Description
etl_run_ts	timestamp	Yes	No	Timestamp at which the ETL process has run
vsp_id	integer	No	No	The identifier of VSP from which this policy got exported
id	integer	No	No	Identifier of this row
client_id	bigint	No	No	Maps to mi_device.client_id
inventory_id	bigint	No	No	maps to mi_app_inventory.app_id
created_at	timestamp	No	No	the association created for the first time on the Core
modified_at	timestamp	No	No	Last change timestamp
status	varchar(64)	No	No	Managed app status

Device configurations: MI_DEVICE_CONFIG table

The MI_DEVICE_CONFIG table contains a record for each device/configuration association.

Name	Data type	Not Null?	Primary key?	Description
etl_run_ts	timestamp	Yes	No	Timestamp at which the ETL process has run

Name	Data type	Not Null?	Primary key?	Description
vsp_id	integer	No	No	The identifier of VSP from which this policy got exported
config_id	integer	No	No	Identifier of the configuration, maps to config_id in mi_config table
device_uuid	varchar(64)	No	No	UUID of the device, maps to device_uuid in mi_device table
status	varchar(1)	No	No	Status of the policy, 'P' - Pending, 'S' - Sent, 'A' - Applied, 'F' - Failed, 'R' - Revoked, 'Q' - Quarantine Revoked, 'U' - Update Pending, 'V' - Update Failed, 'X' - Unknown
last_updated_at	timestamp	No	No	Last change in status or created timestamp

iOS and OS X device fields: MI_DEVICE_IOS table

The set of iOS and OS X device fields in the MI_DEVICE_IOS table comprises iOS and OS X device details. It has a one-or-zero to one relationship with the MI_DEVICE table. If a device is not an iOS device, the record will not be here.

Name	Data type	Not Null?	Primary key?	Description
apns_token	character varying(255)	No	No	
bluetooth_mac	character varying(255)	No	No	
build_version	character varying(255)	No	No	
carrier_settings_version	character varying(255)	No	No	
current_mcc	character varying(255)	No	No	
current_mnc	character varying(255)	No	No	
data_roaming_enabled	boolean	No	No	

Name	Data type	Not Null?	Primary key?	Description
device_id	bigint	No	No	VSP device_id. The combination of etl_run_ts + vsp_id + device_id makes the primary key for this table.
device_name	character varying(255)	No	No	
device_uuid	character varying(64)	No	No	
etl_run_ts	timestamp without time zone	Yes	No	The time the snapshot is taken on VSP.
FDEncryption_Enabled	boolean	No	No	Is full disk encryption enabled.
FDEncryption_ InstitutionalRecoveryKey	boolean	No	No	Does full disk encryption have institutional recovery key.
FDEncryption_ PersonalRecoveryKey	boolean	No	No	Does full disk encryption have personal recovery key.
force_encrypted_backup	boolean	No	No	
hardware_encryption_ caps	bigint	No	No	
ios_background_status	bigint	No	No	
ip_address	character varying(255)	No	No	
iphone_iccid	character varying(255)	No	No	
iphone_mac_address_ en0	character varying(255)	No	No	
iphone_product	character varying(255)	No	No	
iphone_udid	character varying(255)	No	No	
iphone_version	character varying(255)	No	No	
is_mdm_lost_mode_ enabled	varchar	no	no	
is_mdm_service_	varchar	no	no	

Name	Data type	Not Null?	Primary key?	Description
enrolled_device				
it_policy_result	bigint	No	No	
Last_Acknowledged_Lock_PIN	string	no	no	Last acknowledged lock PIN
Last_Acknowledged_Wipe_PIN	string	no	no	Last acknowledged wipe PIN
modem_firmware_version	character varying(255)	No	No	
Organization_Info	string	no	no	Organization information
os_update_status	varchar	no	no	
OSX_UserID	string	no	no	OS X user ID
OSX_UserLongName	string	no	no	OS X users' long name
OSX_UserShortName	string	no	no	OS X user's short name
passcode_is_compliant	boolean	No	No	
passcode_is_compliant_with_profiles	boolean	No	No	
passcode_present	boolean	No	No	
PersonalHotspotEnabled	boolean	No	No	Is the personal hotspot enabled.
product_name	character varying(255)	No	No	
security_reason_code	character varying(255)	No	No	
serial_number	character varying(255)	No	No	
signal_strength	bigint	No	No	
sim_carrier_network	character varying(255)	No	No	
sim_mcc	character varying(255)	No	No	
sim_mnc	character varying(255)	No	No	

Name	Data type	Not Null?	Primary key?	Description
subscriber_carrier_network	character varying(255)	No	No	
supervised	boolean	No	No	
voice_roaming_enabled	boolean	No	No	
vpn_ip_address	character varying(255)	No	No	
vsp_id	integer	No	No	

Device policy fields: MI_DEVICE_POLICY table

The MI_DEVICE_POLICY table contains a record for each device/policy association in MobileIron Core.

Name	Data type	Not Null?	Primary key?	Description
device_uuid	varchar(64)	No	No	UUID of the device, maps to device_uuid in mi_device table
etl_run_ts	timestamp	Yes	No	Timestamp at which the ETL process has run
last_updated_at	timestamp	No	No	Last change in status or created timestamp
policy_id	integer	No	No	Identifier of the policy, maps to policy_id in mi_policy table
status	varchar(1)	No	No	Status of the policy, 'P' - Pending, 'S' - Sent, 'A' - Applied, 'F' - Failed, 'R' - Revoked, 'Q' - Quarantine Revoked, 'U' - Update Pending, 'V' - Update Failed, 'X' - Unknown
vsp_id	integer	No	No	The identifier of VSP from which this policy got exported

Windows Phone and Surface Device fields: MI_DEVICE_WINDOWS_PHONE table

The set of Windows Phone and Surface-only device fields in the MI_DEVICE_WINDOWS_PHONE table comprises Windows Phone and Surface-specific device details. It has a one-or-zero to one relationship with the MI_DEVICE table. If a device is not a Windows Phone or Surface device, the record will not be here.

Name	Data type	Not Null?	Primary key?	Description
etl_run_ts	timestamp without time zone	Yes	No	The time the snapshot is taken on VSP.
vsp_id	integer	No	No	
device_id	bigint	No	No	VSP device_id. The combination of etl_run_ts + vsp_id + device_id makes the primary key for this table.
device_uuid	character varying(64)	No	No	
dm_client_version	double precision	No	No	
wp_cert_renew_ timestamp	timestamp without time zone	No	No	
wp_ent_dm_id	bigint	No	No	
wp_exchange_id	character varying(255)	No	No	
wp_firmware_version	character varying(255)	No	No	
wp_hardware_version	character varying(255)	No	No	
wp_local_time	timestamp without time zone	No	No	
wp_processor_type	bigint	No	No	
wp_signed_ent_dm_id	bigint	No	No	

Policy-related fields: MI_POLICY table

The MI_POLICY table contains the exported details for all MobileIron Core policies, regardless of whether they are currently applied to devices.

Name	Data type	Not Null?	Primary key?	Description
etl_run_ts	timestamp	Yes	No	Timestamp at which the ETL process has

Name	Data type	Not Null?	Primary key?	Description
				run
vsp_id	integer	No	No	The identifier of VSP from which this policy got exported
policy_id	integer	No	No	Identifier of the policy
policy_uuid	varchar(64)	No	No	UUID of the policy
policy_name	varchar(64)	No	No	Name of the policy
priority	integer	No	No	Priority of the policy over other similar type of policies applied to the device
active	varchar(1)	No	No	Whether the policy is active
user_override	varchar(1)	No	No	Always 'f', not used
policy_type	varchar(64)	No	No	Whether it is a DEFAULT policy or ENTERPRISE(Admin created) policy or DEVICE policy
profile_type	varchar(64)	No	No	Type of policy profile, LOCKDOWN, PRIVACY, SECURITY, SYNC, ACTIVESYNC, USER, DOCS, GLOBALHTTPPROXY, SINGLEAPPMODE, KIOSK, APPCONNECT, SAMSUNG_GENERAL, ANDROIDQUICKSETUP
description	varchar(255)	No	No	Policy description that admin configured
hash	varchar(64)	No	No	Fingerprint of all the associated rules of this policy
created_at	timestamp	No	No	Date and time at which this policy is created
version	integer	No	No	Version policy, number of times the policy got modified
last_modified_at	timestamp	No	No	Last modified date and time
created_by	integer	No	No	The id of the user who created this policy, maps to user_id in mi_user table, if a device is registered to this user. 9000 is the default id for the system created default policies
last_modified_by	integer	No	No	Id of the user who modified the policy

User-Related Device Fields: MI_USER

The MI_USER table stores the set of user-related device fields. The MobileIron Reporting Database further separates these fields into common user fields that are stored in this table and LDAP fields that are stored in the MI_USER_LDAP_ATTR and MI_USER_LDAP_GROUP tables.

It has one to one relationship with the MI_DEVICE table, that is, if a user owns three devices, all three devices are stored in the MI_DEVICE table and the user record is stored three times in this MI_USER table, each with a different "device_id" value, but the same values for the other fields.

Common User Fields

Name	Data type	Not Null?	Primary key?	Description
etl_run_ts	timestamp without time zone	Yes	No	
vsp_id	integer	No	No	
device_id	bigint	No	No	
device_uuid	character varying(64)	No	No	
user_id	character varying(128)	No	No	
display_name	character varying(255)	No	No	
email_address	character varying(128)	No	No	
first_name	character varying(128)	No	No	
last_admin_portal_login_time	timestamp without time zone	No	No	
last_name	character varying(128)	No	No	
uuid	character varying(64)	No	No	

Name	Data type	Not Null?	Primary key?	Description
ldap_attr_dn	character varying(640)	No	No	
ldap_dn	character varying(640)	No	No	
ldap_locale	character varying(64)	No	No	
ldap_principal	character varying(128)	No	No	
ldap_upn	character varying(128)	No	No	

LDAP-User Fields

MobileIron Reporting Database further separates LDAP-related fields into sets of basic LDAP-related device fields and groups, described below.

Basic LDAP-User Device Fields: MI_USER_LDAP_ATTR Table

LDAP attributes of the user.

Name	Data type	Not Null?	Primary key?	Description
etl_run_ts	timestamp without time zone	Yes	No	
vsp_id	integer	No	No	
device_id	bigint	No	No	
device_uuid	character varying(64)	No	No	
user_id	character varying(128)	No	No	
attr_name	character varying(255)	No	No	
attr_value	character varying(640)	No	No	

LDAP-Group Device Fields: MI_USER_LDAP_GROUP Table

LDAP groups of the user.

Name	Data type	Not Null?	Primary key?	Description
etl_run_ts	timestamp without time zone	Yes	No	
vsp_id	integer	No	No	
device_id	bigint	No	No	
device_uuid	character varying(64)	No	No	
user_id	character varying(128)	No	No	
dn	character varying(640)	No	No	
name	character varying(128)	No	No	

Value Enumerations

Values for the MI_DEVICE.platform Field

The values for the MI_DEVICE.platform field are:

- Android
- BlackBerry
- iOS
- OS X
- Windows Phone 8

Values for the MI_DEVICE.platform_name Field

The values for the MI_DEVICE.platform_name field are:

Android	AppleTV	BlackBerry	iOS	OS X	Windows
Android 1.6 Android 2.0	AppleTV 7.0	BlackBerry	iOS 4.0 iOS 4.1	OS X 10.7 OS X 10.8	Windows 8.1 Windows Phone

Android	AppleTV	BlackBerry	iOS	OS X	Windows
Android 2.0.1	AppleTV 7.1		iOS 4.2	OS X 10.9	Windows Phone 8
Android 2.1	AppleTV 7.2		iOS 4.3	OS X 10.10	Windows Pro/RT
Android 2.2			iOS 5.0	OS X 10.11	
Android 2.3			iOS 5.1		
Android 3.0			iOS 6.0		
Android 3.1			iOS 6.1		
Android 4.0			iOS 7.0		
Android 4.0.1			iOS 7.1		
Android 4.0.2			iOS 8.0		
Android 4.0.4			iOS 8.1		
Android 4.1			iOS 8.2		
Android 4.2			iOS 8.3		
Android 4.3			iOS 8.4		
Android 4.4			iOS 9.0		
Android 4.4.1					
Android 4.4.2					
Android 4.4.3					
Android 4.4.4					
Android 5.0					
Android 5.0.1					
Android 5.0.2					
Android 5.1					
Android 5.1.1					
Android 6.0					

Values for the MI_DEVICE.status Field

The values for the MI_DEVICE.status field are:

Enum Name	Meaning
ACTIVE	Active
BLOCKED	Blocked
IENROLL_VERIFIED	Enrollment verified

Enum Name	Meaning
IENROLL_INPROGRESS	Enrolling
IENROLL_COMPLETE	Enrolled
INFECTED	Infected
LOST	Lost
RETIRED	Retired
VERIFIED	Verified
VERIFICATION_PENDING	Pending
EXPIRED	Expired
WIPED	Wiped
WIPE_PENDING	Wipe pending
UNKNOWN	Unknown status

Values for the MI_DEVICE.owner Field

The values for the MI_DEVICE.owner field are:

Name	Meaning
COMPANY	Company-owned device
EMPLOYEE	Employee-owned (personal) device

Array Value Enumerations

Values for the MI_DEVICE.blocked_reasons, MI_DEVICE.noncompliance_reasons, and MI_DEVICE.quarantined_reasons Fields

Each of the fields that use these values has an associated field to determine whether any reasons were set or not. For example, if a device is blocked, then the "blocked_reasons" field has a list of reasons, and the "blocked" field is 'true'.

Enum Name	Meaning	Hexadecimal Value
ALLOWED_APP_CONTROL	Allowed app control policy is out of compliance	0x004000

Enum Name	Meaning	Hexadecimal Value
APP_CONTROL	App control policy is out of compliance	0x000040
AUTO_BLOCK	Device is not registered	0x000100
COMPROMISED	Device state is compromised	0x000001
DATA_PROTECTION	Data Protection is not enabled	0x000008
DEVICE_ADMIN_DEACTIVE	Device administrator is deactivated	0x000800
DEVICE_OUT_OF_CONTACT	Phone is out of contact	0x000020
DISALLOWED_APP_CONTROL	Disallowed app control policy is out of compliance	0x001000
EXCHANGE	Exchange-reported	0x000400
HW_VERSION	Hardware revision is not allowed	0x000004
LOGGED_OUT	User logged out	0x008000
MANUAL	Device is manually blocked	0x000200
OS_VERSION	OS version is less than the supported OS version	0x000002
PER_MAILBOX_LIMIT	Device exceeds per mailbox limit	0x000080
POLICY_OUT_OF_DATE	Policy is out of date	0x000010
REQUIRED_APP_CONTROL	Required app control policy is out of compliance	0x002000
UNKNOWN	Unknown reason	0x400000

Example

What follows is an example of how MobileIron Reporting Database creates a value for use in the database. Suppose MobileIron Reporting Database needs to update the compliance column of the **mi_device** table with the COMPROMISED flag and the OS_VERSION flag. Then, the value of compliance would be **COMPROMISED | OS_VERSION**, which is **0x000001 | 0x000002 = 0x000003 = 3**.

History Versus Snapshot Tables

MobileIron Reporting Database snapshots the device information regularly; depending on the export schedule. If run every six hours, then every six hours, MobileIron Reporting Database creates the following set of snapshot tables:

- mi_device (the main one)
- mi_device_ios
- mi_device_android
- mi_device_windows_phone
- mi_user, mi_user_ldap_attr
- mi_user_ldap_group

When MobileIron Reporting Database imports the data, it:

- Replaces the snapshot tables on MobileIron Reporting Database with this latest imported tables from VSP
- Inserts the imported tables to history tables (mi_device_hst, mi_device_android_hst, et cetera). Each snapshot in the history table is distinguished by the etl_run_ts (this is the export run time) column.

For example, if MobileIron Core has 10,000 devices, the snapshot table **mi_device** should only have 10,000 rows (devices), but **mi_device_hst** would contain as many snapshots as MobileIron Reporting Database ever takes. In our example, if MobileIron Reporting Database runs every six hours, after one day, **mi_device_hst** would contain 4 * 10,000 = 40,000 rows. If these settings are in effect for one month, the **mi_device_hst** table would contain 40,000 * 30 days = 1,200,000 rows.

You can use the history tables to create some "stats over time" types of reports:

- Blocked or not compliance devices over time
- Number of devices haven't checked in for the last 4 hours of time"
- Number of devices by their status over time

The history tables do not have many entity relationships to their main tables; **mi_device_hst** is a superset of **mi_device**, **mi_device_ios_hst** is a superset of **mi_device_ios**, et cetera.

When creating your reports, ignore all tables with a “*_stg” suffix and with a number suffix like "*.1".