servicenow

SCOPED CERTIFIED APPLICATION DESIGN

IBM MaaS 360 Integration

Template version: 4.0

Template effective date: January 11, 2019

Table of Contents

1   Overview

Your Design Document describes the design of your scoped application and will be used throughout the certification process. The document is used internally by ServiceNow only and is not shared with your customers.

To prepare your Design Document, enter a thorough response in each section of this template document. If a section is not applicable, state the reasons clearly.

This document is intended to enable ServiceNow Certification Engineers and Technical Support members to:

- Understand your integration completely
- Identify areas of risk to platform security or platform stability
- Troubleshoot any potential third-party issues

1.1   References

#	Document Identifier	Document Title
[R1]	ID	Add your document references. One line per document

2   Application overview and intended use

Describe, at a high level, what the application does:

The MaaS 360 Integration is used to extract the following mobile device information from a MaaS 360 instance:

1) Asset information
2) User data
3) Incident worthy device events

The integration predominantly uses REST web services to consume the data from the source MaaS 360 instance. Event handling logic integrates with Service-Now.

Describe the business need that the application solves:

This application enables customers to gain visibility into their mobile device assets. It also ensures that they are notified of events of interest for mobile devices while providing a trackable and consistent approach to resolving such events via incident management practices.

Describe each specific customer use case:

1) As an organization, it is desired to have our mobile device asset data included within our centralized Service-Now CMDB.
2) As an organization, it is required to have our mobile device asset data associated with a user who uses the device. This user may or may not have a Service-Now user account.
3) As an organization, it is imperative that we are notified in a consistent manner about mobile device events (security, compliance, etc.). It is also required that these events are tracked and responded to in a manner consistent with our incident management practices.

2.1 Third-party dependencies

List third-party dependencies:

IBM MaaS 360 Service

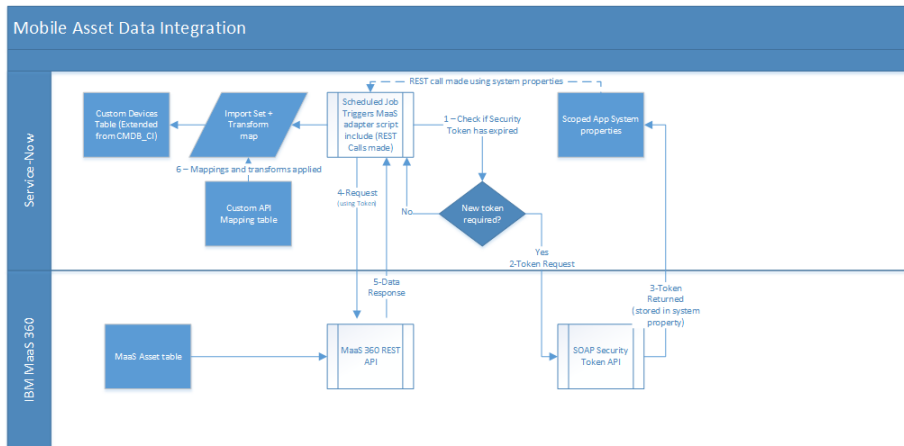IBM MaaS security token registration via MaaS support

3 Software architecture overview

In this section, you describe the top-level software components and their interactions/relationships.

If you have attached a system architecture document, refer to it here:
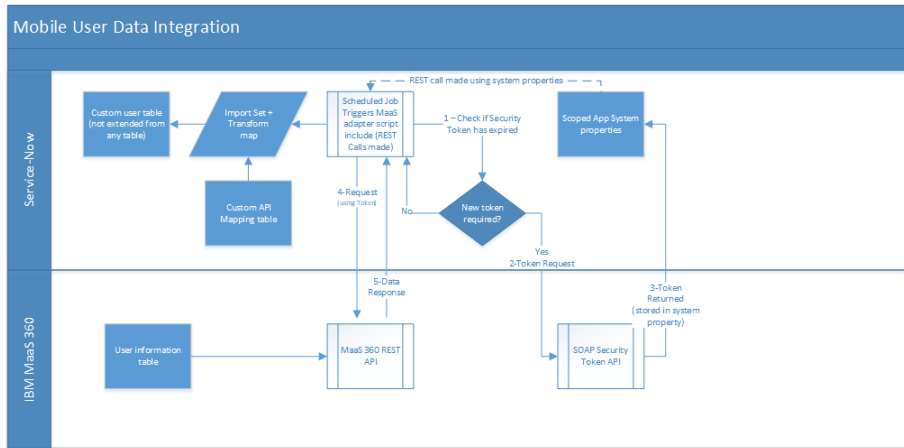
N/A

Attach any UML package diagrams and/or layer diagrams and/or interface diagrams:

Asset Integration step descriptions:

1) As part of the scheduled job execution of the MaaS Adapter script include, a check is completed to determine if the security token has expired. If expired, step 2 + 3 apply.

2) If the security token is expired, perform a SOAP webservice call to MaaS 360 to obtain a new security token.

3) If the security token was expired, MaaS 360 API returns the newly acquired security token, and Service-Now stores that security token in system properties for re-use and check in the next REST calls.

4) REST call is initiated to MaaS 360 REST API using the security token and endpoint stored in the system properties for the application.

5) MaaS 360 returns asset data inserted / updated since the last integration ran.

6) Data is loaded into an import set and transformed in accordance with the custom API mapping table. Data is transformed onto the custom devices table which is extended from CMDB_CI.

Mobile User Data Integration

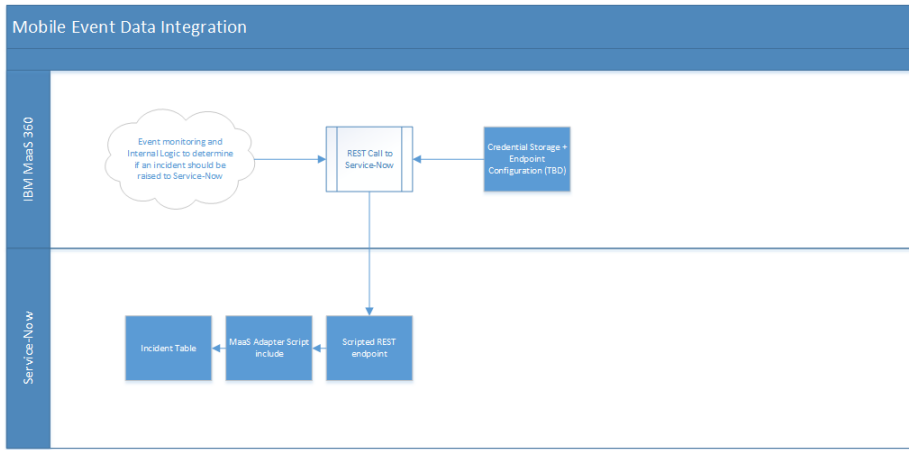User Integration step descriptions:

1) As part of the scheduled job execution of the MaaS Adapter script include, a check is completed to determine if the security token has expired. If expired, step 2 + 3 apply.

2) If the security token is expired, perform a SOAP webservice call to MaaS 360 to obtain a new security token.

3) If the security token was expired, MaaS 360 API returns the newly acquired security token, and Service-Now stores that security token in system properties for re-use and check in the next REST calls.

4) REST call is initiated to MaaS 360 REST API using the security token and endpoint stored in the system properties for the application.

5) MaaS 360 returns user data inserted / updated since the last integration ran.

6) Data is loaded into an import set and transformed in accordance with the custom API mapping table. Data is transformed onto the custom user table which has a reference linkage to the sys_user table, but is not extended from sys_user.

Mobile Event Data Integration

Event Integration step descriptions:

MaaS 360 is a mobile-device monitoring and control suite. Events occurring within MaaS 360 will trigger an event in the form of a webhook that will call a ServiceNow REST endpoint. That event may or may not trigger the creation of an incident ticket. This is controlled through a form within the ServiceNow application.

List the operating systems that the software runs on:
N/A

List any additional external required components (for example, desktop clients, scripts, and so on):
N/A

4   Software design description

Attach class diagrams, collaboration / sequence diagrams, and deployment diagrams to illustrate your description.

If your application imports and/or exports data, specify:

- How often does import/export occur?

Asset + User information IMPORT: Daily @ midnight

Event Information: As necessary per MaaS 360 logic triggers.

- What kind of data?

Mobile device information such as:

- Smartphone, Laptop, Tablet

User ownership data such as:

- Full name, User ID, Domain, Email

Mobile device event data such as:

- emmAccountId
- eventSubType
- eventTimestamp
- emmDeviceId
- emmDeviceName
- ownership
- deviceUserName
- platformName
- deviceType
- osName
- imeiEsn
- installedDate
- lastReportedDate
- deviceStatus
- deviceSubStatus
- udid
- wifiMacAddress
- policyComplianceStatus
- oocReason
- selectiveWipeStatus
- jailbreakStatus

- What considerations did you implement to ensure optimal performance?

Security token caching is implemented to avoid un-necessary calls.

Indexes set up for primary keys on user and asset data in the transform maps.

5   Performance considerations and concerns

- Describe potential performance risks or high-volume transactions that the integration may impose on the platform:

Initial data loads will take time and resources to complete, however the integration going forward from that point will only be running delta transactions of records inserted / updated since the last import. Maas360 also imposes a transaction limit on the number of records passed per day (100,000 records / day).

- Describe the performance metrics of the integration:

N/A

- Describe inbound web services and declare an acceptable threshold of transactions per second: <how many records are created per call and how frequently are the calls made>

Inbound REST integrations are only used to create mobile incidents. The frequency of these transactions will vary based upon conditions within the MaaS 360 mobile environment as well as the size and number of managed devices. Each call will be creating only one record in the incident management table, and these calls are only made in cases where the logic within MaaS 360 determines that the event is worthy of investigation via incident.

- Describe outbound web services and declare an acceptable threshold of transactions per second:<how many records are exported and how frequently>

Outbound REST integrations are used to request, then import asset and user data from MaaS 360. The number of records imported will depend on the size of the company using the application. The integration will be using delta loads whereby only inserted or updated records since the last integration run will be processed. The integrations get triggered daily at midnight based on initial scheduled job execution time.

- Please describe any error handling mechanisms that you have in place:

Application level error trapping and debug logging has been implemented surrounding key code executions through use of try-catch blocks as well as inline debug logging. Logging is implemented as part of the MaaS 360 Adapter script include. Error level trapping is completed at all times, and debug level of error logging is completed if the system property "maas360.debug" is set to true.

- If languages other than English are supported, please list the supported languages here: N/A

- If designed specifically for mobile support, list all devices supported: N/A

- If your application is supported on specific web browsers, list supported browsers here: N/A

6   Security considerations and concerns

- Describe security considerations and concerns:

Access to data will be restricted via security roles. REST calls will be made using security tokens which are cycled on a regular basis as opposed to Username + password authentication.

- List insecure protocols:

N/A

- List all roles:

1) MaaS.user – These users have only access to read information in the devices and users tables.

2) MaaS.admin – These users can change configuration settings for the integration, and see all data pertaining to the integration.

- List all users:
    - Manually created MaaS360 integration user (used by MaaS to integration with Service-now for incident creation from event).
- List any externally accessible services
    - o POST: /api/x_ibmrt_maas360/v1/event

- Sensitive Information Handling:
    - o If your application handles sensitive information (i.e. passwords, PHI, social security #'s, etc.) please outline how you encrypt or otherwise protect this information: N/A
    - o If you are processing financial transactions, please be aware that the credit card information processed cannot be stored within ServiceNow. Please outline how financial transactions are handled: N/A

7   Application components

In this section, identify both newly created artifacts and modifications to base ServiceNow artifacts:

7.1   Components created by the application:

- List all script includes:

MaaS360 Adapter: Houses all functions pertaining to the scoped application. Includes items such as REST call commands, as well as interface activities, and back end data processing functions.

- List all newly defined tables:

x_ibmrt_maas360_devices

x_ibmrt_maas360_users

x_ibmrt_maas360_api_map

Commented [SC6]: Need to confirm with scope pre-fix

Commented [SC7]: Need to confirm with scope pre-fix

Commented [SC8]: Need to confirm with scope pre-fix

- List all business rules:

Register Event: MaaS360 Event[x_ibmrt_maas360_maas360_event]

Commented [SC9]: Need to confirm with scope pre-fix

Set First Discovered: Devices[x_ibmrt_maas360_devices]

Set Import Set Attribute: API Map[x_ibmrt_maas360_api_map]

- List all client Scripts

N/A

- List all applications/modules:

IBM MaaS360 Adapter

- Devices

- Users
- Import Sets
  - o Device imports
  - o User Imports
- Configuration
  - o API Maps
  - o Properties
- List all externally accessible services:

List all properties (including system properties):

- x_ibmrt_maas360.access_key
- x_ibmrt_maas360.app_id
- x_ibmrt_maas360.app_version
- x_ibmrt_maas360.billing_id
- x_ibmrt_maas360.end_point
- x_ibmrt_maas360.logging.verbosity
- x_ibmrt_maas360.password
- x_ibmrt_maas360.platform_id
- x_ibmrt_maas360.token
- x_ibmrt_maas360.token_refreshed_at
- x_ibmrt_maas360.user_name

- Specify the scope(s) used:
  - System Import Sets
  - Configuration Management (CMDB)

- List the integration user & roles created for the integration user authentication (note: the user may need to be created as a part of the installation/configuration process, however please outline the details for this user here):
  - Outbound integrations are authenticated based on the token, token_refreshed, user_name, and password system properties.
  - POST: /api/x_ibmrt_maas360/v1/event for inbound event integration

- Components modified by the integration:
- List all modules:
  - Listed above already
- List all externally accessible services:
  - Listed above already

7.2 Integration components created by the application:
- List any inbound web services: <SOAP, REST, etc.>

- REST – Event integration
- List the target tables of each inbound web service <incident.do, problem.do, etc.>
  - x_ibmrt_maas360_maas360_event
- List all import set tables:

  propertiesximp_tmpl_x_0334_ibm_maas360_api_map
  - x_ibmrt_maas360_user_import
  - x_ibmrt_maas360_device_import
- List all transformation maps:
  - Device import
  - User transform map
  - u_imp_tmpl_x_0334_ibm_maas360_api_map
- List any scheduled jobs for data exports:
  - Update MaaS360 Device List
- List any non-Public API's utilized:

  N/A

8   Future plans

Describe how you envision the application evolving and/or include product roadmaps.

MaaS360 will continue to consult with clients worldwide regarding needs and wishes along with changes to vendor operating systems and devices.   From this MaaS360 will prioritize new functionality and integrate these requirements into the integration.

MaaS360 foresees expansion of devices, changes in enrollment and demand process along with compliance actions that would results in communications to ServiceNow informing admins of change.

MaaS360 also foresee changes to the integration leveraging ServiceNow to create a standard package for application distribution which can be cataloged on ServiceNow, but executed by MaaS360.

9   Service Level Agreement Definition

In this section, you define the Service Level Agreement (SLA) for your customers.

Customers will be instructed to contact the integration provider (your organization) for technical support. If a customer first contacts ServiceNow Customer Support, then ServiceNow Customer Support will isolate the problem and instruct the customer to resolve the issue with your organization.

- **Support Hours of Operation:** (including time zone):[example: 8am - 5pm PST]
  - MaaS360 provides 24 x 7 coverage for Support
- **Support Days of Operation:** [example: Monday - Friday (specify exceptions such as Holidays)]

- MaaS360 provides 24 x 7 coverage for Support
- **Promised Call Response Time:** [example: Within 4 hours of received support request]
  - N/A
- **Promised Call Resolution Time:** [example: Within 5-10 business days of response]
  - N/A until problem is diagnosed
- **Contact Method:** [example: email, phone, website]
  - Email and Phone are primary
- **Contact Details:** [example: 1-800-SUPPORT, support@provider.com, www.support.provider.com]
  -

10 Debugging and troubleshooting

Describe how to debug the integration:

OUTBOUND INTEGRATIONS

1) Change the "x_ibmrt_maas360.debug" system property to true
2) Execute the "Update MaaS360 Device List" scheduled job
3) Open the Application Logs and review log messages from app scope "IBM MaaS360 Adapter"
4) If the debug logs are not identifying the issue, open the import set tables (imp_tmpl_x_ibmrt_maas360_api_map, x_ibmrt_maas360_user_import, or x_ibmrt_maas360_device_import) to determine if the data is being loaded properly into the import set, but not transformed properly

INBOUND INTEGRATIONS

1) Trigger an event in MaaS 360 that should cause an event in ServiceNow to be generated. Observe the Events table in ServiceNow for the generated event.

Describe issues that you have observed and provide troubleshooting tips and workarounds:

N/A

Describe anticipated issues:

- Authentication issues
  - o Username + password mismatch on token security request
  - o Username + password mismatch on INBOUND REST integration for events
- Connectivity issues
  - o Network timeout / loss between instance and MaaS360 environment
- Data volume
  - o Data record count exceeds MaaS360 limits

10.1 Debugging tips:

Describe debugging techniques that may assist Tech Support or the Customer to identify issues.

Commented [SC14]: IBM will need to give us this information I Assume. Unless we've been contracted to support it as well. Scott G. to get from Charlie - 1/2

Commented [AB15R14]:

Commented [SC16]: Will need to confirm once built in vendor instance

Commented [SC17]: Need to confirm with scope prefix

Commented [SC18]: Need to confirm with scope prefix

Commented [SC19]: Need to confirm with scope prefix

Commented [SC20]: TBD

Commented [SC21]: Might be request count instead of record count. Scott G to confirm.

See section 10 response

10.2 Failure modes:

List expected failure modes (for example, third-party server down):

Authentication issues on OUTBOUND integrations (Username + password mismatch on token security request)

- Would show up as errors in the application log under the "IBM MaaS360 Adapter" scope

Authentication issues on INBOUND integrations (Username + password mismatch on INBOUND REST integration for events)

- Would show up as errors in the SECURITY?? Log with message containing ###ENDPOINT NAME###

Connectivity issues (Network timeout / loss between instance and MaaS360 environment)

- Would show up as errors in the application log under the "IBM MaaS360 Adapter" scope

Data volume (Data record count exceeds MaaS360 limits)

- Would show up as errors in the application log under the "IBM MaaS360 Adapter" scope with a return code of HTTP 429 response

END OF DOCUMENT

Commented [SC22]: Will need to confirm once built in vendor instance

Commented [SC23]: Needs confirmation about how this occurs. Per Scott G. hold this item for now - 1/2

Commented [SC24]: Will need to confirm once built in vendor instance

Commented [SC25]: Will need to confirm once built in vendor instance