IT Security Procedural Guide: Mulesoft Application Programming Interface (API) Security Process CIO-IT Security-20-108

Initial Release

September 18, 2020

Office of the Chief Information Security Officer

VERSION HISTORY/CHANGE RECORD

Change Number	Person Posting Change	Change	Reason for Change	Page Number of Change
		Initial Release – September 18, 2020		
N/A	ISE	New guide created.	Provide guidance regarding the Mulesoft API Management System.	N/A

Approval

IT Security Procedural Guide: Mulesoft Application Programming Interface (API) Security Process, CIO-IT Security 20-108, Initial Release, is hereby approved for distribution.

X DocuSigned by:
Bo Berlas
FD717926161544F...

Bo Berlas
GSA Chief Information Security Officer

Contact: GSA Office of the Chief Information Security Officer (OCISO), Security Engineering Division (ISE) at SecEng@gsa.gov.

Table of Contents

Note: It may be necessary to copy and paste hyperlinks in this document (Right-Click, Select Copy Hyperlink) directly into a web browser rather than using Ctrl-Click to access them within the document.

1 Introduction

This procedural guide provides an overview of the process by which General Services Administration (GSA) customers can seek and obtain approval for Application Programming Interface (API) use cases within the Mulesoft API Management System. This process leverages the inherent flexibility in the application of security controls noted in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision 4, "*Security and Privacy Controls for Federal Information Systems and Organizations,*" and NIST SP 800-37, Revision 2, "*Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy.*" It also leverages and operationalizes the guidance from CIO-IT Security-19-93, "*Application Programming Interface (API) Security"* for the Mulesoft API Platform.

APIs provide system solution architects and developers an effective, efficient, and secure method for interconnecting systems, consuming data from another system, and publishing updates to destination systems at a machine level with predictability and no direct user interaction. Both modern and legacy systems can be connected together based on current requirements, irrespective of their on premise or cloud location.

1.1 Purpose

The purpose of this guide is to define the process for GSA Federal employees and contractors with IT security responsibilities to implement a secure Mulesoft API. This guide identifies the key activities for submitting a proposed Mulesoft API for security review.

1.2 Scope

GSA authorizes the use of APIs based on GSA's API standards and CIO-IT Security-19-93. This guide only implements those standards and guidance for APIs managed through the Mulesoft Anypoint Platform. This guide DOES NOT apply to all APIs at GSA. It is tailored to the specific use of the Mulesoft API service offering.

2 API Key Terminology

All key terms for APIs are defined in CIO-IT Security-19-93.

Mulesoft – A software product, platform, and Federal Information Security Modernization Act (FISMA) system (Mulesoft Anypoint Platform) that serves as an API gateway for several GSA systems and implements GSA security, process, and policy requirements on behalf of GSA API customers.

3 Mulesoft API Roles and Responsibilities

3.1 Authorizing Officials (AOs)

AOs have the overall responsibility of accepting risk for systems under their purview and updating their authorization packages to incorporate approved Mulesoft APIs, as applicable.

3.2 System Owners (SOs)

SOs approve access for Mulesoft APIs to their systems for the purposes defined in the GSA API Security Package. SOs are also responsible for verifying the System Security Plans (SSPs) for their systems are updated as described in Section 6.2.2.

3.3 Mulesoft API Owners

API Owners are responsible for the Mulesoft API on the business side. They have multiple responsibilities:

- Liaising with the Mulesoft API Developer, System Owners of the systems the Mulesoft API will connect with, the Privacy Office, and the Security Team.
- Completing the Mulesoft API Attributes Questionnaire required for the security review. The questionnaire is available on the IT Security Forms and Aids page.
- When adding a use case for an existing API, Mulesoft API owners prepare and submit an amended Security Package to include an updated PTA/PIA and updated SSP for their current FISMA Information System.

3.4 Mulesoft API Developer

The Mulesoft API Developer is the in-house person, group, or contractor engaged to code the Mulesoft API. As part of the process, the developer collaborates with the Mulesoft API Owner on the Mulesoft API Security Package.

3.5 Information Systems Security Officer (ISSO)

The ISSO is the focal point in getting Mulesoft APIs through the approval process and appropriately reviewed. Additionally, the ISSO is responsible for assisting the Mulesoft API Developers with recommendations for changes required for successful approval. The ISSO works with the Mulesoft API Owner and the Mulesoft API Developer to ensure the Mulesoft API Attributes Questionnaire is complete and accurate. The ISSO also works with the Mulesoft API Owner as well as the Privacy Office to complete a Privacy Threshold Assessment (PTA).

The ISSO tracks all Mulesoft APIs, manages the approval workflows and status, and makes recommendations for approvals of submitted Mulesoft APIs. The ISSO updates the Mulesoft API tracking sheet as Mulesoft APIs are approved.

3.6 Information Systems Security Manager (ISSM)

The ISSM is the final approval authority for all Mulesoft APIs, but may delegate approval authority for Mulesoft APIs to Mulesoft ISSOs at their discretion. The ISSM reviews the Mulesoft API Attributes Questionnaire and artifacts after they have been compiled by the ISSO and relays their concurrence that the security measures have been met, and that the Mulesoft API is allowed to operate in accordance with this guide. If the ISSM does not concur, feedback is provided on why they do not concur.

3.7 Mulesoft Admin

System administrators for the Mulesoft Platform oversee the information system the Mulesoft APIs connect through. They assist Mulesoft API Owners in the troubleshooting of Mulesoft APIs and other performance and execution issues.

3.8 Chief Privacy Officer (CPO)

GSA's Privacy Office is the final approval authority for the Privacy Threshold Assessment (PTA) and Privacy Impact Assessment (PIA) (if required) to be included in the Mulesoft API security package. GSA's CPO signs all final privacy documentation.

4 Mulesoft API Operational Environment

The Mulesoft operational environment is described in the Mulesoft Anypoint Platform's SSP.

5 General API Security

The following sections describe general processes and requirements that must be applied to all APIs in use within the Mulesoft Platform.

5.1 Mulesoft API Authorizations/Access Approval

5.1.1 Authorization

The Mulesoft API Authorization Policy of a given Mulesoft API must be documented in the Mulesoft API Security Package as part of the Mulesoft API Attributes Questionnaire. Access controls can be leveraged from the Mulesoft Anypoint Platform but must still be documented in the Mulesoft API Security Package. The authorization process which defines the requirements for all APIs is defined in CIO-IT Security 19-93.

5.1.2 Mulesoft API Security Package

The Security Package consists of all the information needed to approve an API for Production use. At a minimum, the Security Package will include the API Attributes Questionnaire, PTA, all evidence and artifacts required to support the assertions made in the API Attributes Questionnaire, and links to the SSPs for the applications that consume the API. The evidence may be a screenshot, XML file, Process Design Document, configuration outputs, log data, or code snippets that demonstrate the proof of a claim made by the submitter.

Additionally, it is at the discretion of the ISSM to request and receive any additional evidence or answers to additional questions. All such additional inquiries and responses will be made part of the Security Package.

Each Security Package is linked and maintained from a central inventory sheet. Access to the sheet is approved by the Mulesoft ISSM.

Once a Mulesoft API is approved and an additional application seeks to use it, an update to the Mulesoft API Security Package and questionnaire must be made. Following the details of any existing entries, the API attributes questions must be replicated and answered for the new application. Original validation evidence may be reused at the discretion of the ISSM, but updates to the corresponding consuming application's SSP must be made in all cases.

Initial use case API submissions must include a technical point of contact (POC), preferably an assigned System Administrator, for the destination application that Mulesoft is making available for the API. It is the duty of this POC to validate and provide evidence of the data access levels and assigned permissions for all accounts used by the API (i.e., what database tables the API will be able to read, write, delete, etc.). Principles of least privilege will be followed and validated by the ISSM.

5.1.3 Authentication

There are multiple methods of API authentication supported by Mulesoft and available to Mulesoft API Developers and each are thoroughly described in CIO-IT Security 19-93.

OAuth 2.0, HTTP Authentication, Digital Certificates, SAML, and HMAC are all currently available. Note, this guide is not a governing document and authorized authentication methods are governed and defined in CIO-IT Security 19-93. Each method comes with additional considerations and requirements. Mulesoft API Owners must ensure that the Mulesoft API Security Package clearly demonstrates which API Authentication method(s) are in use and how the guidelines identified in CIO-IT Security 19-93 have been met. The Mulesoft ISSO will evaluate the Mulesoft API Security Package against these guidelines.

5.2 API Activity Logging

To ensure API actions can be properly monitored, Mulesoft logs all API activity. Mulesoft API logs must be reviewed monthly by the Mulesoft API Owner. This review provides assurance there is a capability to provide a complete audit trail of activities, including data needed to identify abnormal spikes in activity, access of specific systems, and use of privileged accounts.

5.3 API Clients Approval in IT Standards Profile

APIs must be developed using software approved in GSA's official IT Standards Profile. The GSA IT Standards Profile process is used to maintain a listing of all software technologies and applications that have been acquired and approved for use at GSA. The Security Review of any new Mulesoft API applications shall ensure encryption meets GSA standards.

6 GSA Mulesoft API Security Methodology

6.1 Development of Mulesoft APIs

This section describes the process for developing, testing, obtaining approval to deploy, and operate Mulesoft APIs at GSA.

All changes to Mulesoft APIs are managed by resubmitting the Mulesoft API through the approval process. However, the submission package should specify all the changes made to the Mulesoft API to support a faster review by the ISSO and ISSM. Any new connections made to new information systems (requiring System Owner approval and SSP updates) are considered changes in this context.

6.1.1 Development of the API in a Test Environment

To begin development, members of the business lines meet with the Mulesoft API developer to go over the requirements of the Mulesoft API. Then, the developer prepares the Mulesoft API for testing in the Mulesoft test environment and test environments of the system(s) the Mulesoft API will be connecting to.

When the business representatives determine that the Mulesoft API satisfies their needs in the test environment, a member of the development team prepares screenshots and other evidence needed for the Mulesoft API Attributes Questionnaire as part of the Mulesoft API Security Package. This evidence is shared with the ISSO and Privacy Office to begin the approval process.

The requirements to obtain approval on the Mulesoft APIs are outlined in the following sections. Additionally, any major changes that occur to a particular Mulesoft API after already receiving an approval will require a new security review.

6.2 Approval Process for Mulesoft APIs

The requirements to obtain approval on the Mulesoft APIs are outlined in the following sections. Additionally, any major changes that occur to a particular Mulesoft API after already receiving an approval will require a new security review.

6.2.1 Completion of API Attributes Questionnaire

The Mulesoft API Owner along with the Mulesoft API Developer will work to complete the Mulesoft API Attributes Questionnaire. Once complete, the Mulesoft API Attributes Questionnaire is used to determine if the Mulesoft API has implemented all of the prescriptive guidelines described in CIO-IT Security-19-93. This determination is performed by the Mulesoft API ISSO. If any concerns are raised by the ISSO, they must be addressed before the Mulesoft API is permitted to move out of testing. At this time, the ISSO will also review the other evidence and that has been provided by the Mulesoft API Owner and likewise any concerns that arise must be addressed.

Notice for requested exceptions to standard security requirements:

Many of the required application specific security configurations (see Appendix B) needed for each API are provided at the Enterprise level, are inherited by all APIs on the platform, and are not optional. However, if an exception to the standard security posture and controls is required, an exception can be requested using the API Security Questionnaire. The ISSO will coordinate additional reviews by the ISSM and the Security Engineering Division (ISE) for any requested exceptions. Exceptions must be reviewed in relation to:

- A validated business need
- Acceptance of the level of risk introduced
- Risk mitigations to ameliorate additional risk

Any exceptions and evidence supporting the exceptions must be added to the Security Package. Explicit concurrence by the ISSM and ISE are required.

6.2.2 Update to SSPs

The Mulesoft API Owner must inform and collaborate with the Systems Owners and ISSOs of FISMA systems affected by a given Mulesoft API. Updated SSPs MUST be presented and linked through the Security Package and validated by the ISSM/ISSO prior to Mulesoft API approval and promotion to production.

Updates include affected SSP sections identified in Appendix A. Updates include descriptions; diagrams; data flows; ports, protocols, and services; and accounts/user-types. Appendix A also describes the procedure for the review and possible updates to security control implementation statements. These updates and reviews are required of all API submissions, without regard to FISMA systems, FIPS-199 risk determination, or API Questionnaire Risk Calculation.

6.2.3 Submit Mulesoft API Security Package for Review by Mulesoft API ISSO

Prepare the evidence, Mulesoft API Attributes Questionnaire, testing results, confirmations of consent from affected System Owners, screenshots, and data flow diagrams, and provide to the Mulesoft API ISSO.

6.2.4 Timeline for Review

Upon receipt of the Mulesoft API Security Package, the Mulesoft ISSO and ISSM target a timeframe of 3-5 business days to complete the review of the package and come to a determination on its suitability for promotion to production. This timeframe encompasses the time from submission of a complete package to the security team to notification of determination. Incomplete security packages do not start the review period.

6.2.5 Mulesoft API ISSO review

The Mulesoft API ISSO reviews all artifacts and makes a determination on the Mulesoft API's suitability for promotion to production. Upon receipt of the package, the Mulesoft API ISSO enters the Mulesoft API into the Mulesoft API tracking inventory and records the necessary information. If all information is presented and complete and meets with the ISSOs concurrence

of adherence to the Mulesoft API Security Requirements, this Process Guide, and the IT Security 19-93 guide, the Mulesoft API may be promoted to production and used according to the Change Process, the Mulesoft ATO, and the Annual Review requirements.

6.2.6 Mulesoft API Promotion

After review and with ISSO recommendation, the ISSM is the final approval authority, and the Mulesoft API is promoted from testing to production and begins operation. The Mulesoft API ISSO notifies the Mulesoft API Owner that production use of the Mulesoft API is authorized.

6.2.7 Mulesoft API Annual Review

The individually approved Mulesoft API Security Package becomes part of a larger singular enterprise wide Mulesoft API ATO. All individual Mulesoft API Security Packages will expire at once in correspondence with the expiration of the GSA Mulesoft API ATO and each will require an annual review to become operable with the issuance of the new Mulesoft API ATO. The individual Mulesoft API Owners must annually submit to the Mulesoft API ISSO a validation with evidence that nothing has changed and attest to the ongoing need for the Mulesoft API's business operation.

Appendix A: Updating SSPs Regarding Mulesoft API Interaction

SSP Required Updates

All Mulesoft APIs interact with at least two FISMA information systems. The FISMA system's SSPs **must** be updated in the following ways:

1. Update the SSP to add the interaction with Mulesoft APIs as part of the System Description in **Section 9, General System Description.** This section must include a listing of all Mulesoft APIs that interact with the system and a reference/link to the Mulesoft API(s.)

2. **Section 10.5, Data Flow (and Figure 10-1).** Include the data flows associated with Mulesoft APIs.

3. **Section 10.6, Ports, Protocols, and Services (and Table 10-4)**, should include ports/protocols/services used by the Mulesoft API, if any, and include Mulesoft API use in the purpose column. If an existing port, protocol, or service is used, add Mulesoft API use in the purpose statement.

4. All sections which enumerate users must be updated to include the accounts used by, and in support of the API.

NIST SP 800-53 Security Controls. The following security controls are to include information about Mulesoft APIs, when API-specific actions, attribution, or interaction can be ascertained.

While the updates above are required, some security control implementation statements may need to be updated as well. All of the following controls must be reviewed regardless of FISMA Risk rating and without respect to the results of the Risk Calculator. Determinations of the need for updates are at the discretion of the ISSOs of the impacted FISMA systems, but those decisions are reviewed by the ISSO and ISSM of the Mulesoft API Platform and are part of the Mulesoft API approval process.

The security controls in Table A-1 may need to be updated in the SSPs of API connected FISMA information systems to include information about Mulesoft APIs, when API-specific actions, attribution, or interaction can be ascertained. This table is provided as a guide to help ISSOs quickly identify the controls that must be reviewed. Updates are only required when the API impacts the control. It is not the intention to force the need for unnecessary updates with no real impact or value. Only make control updates when the API interacts with the control.

Table A-1: Control Implementations Requiring REVIEW by ISSOs/System Owners

NIST Control	Instructions for Control Implementation
AC-2: Account Management	Review for impact and make a determination on the inclusion of the usage of Mulesoft APIs. If accounts used by Mulesoft APIs are managed differently than other accounts on the

	system explain how they are managed.
AC-6: Least Privilege	Review for impact and make a determination on the inclusion of the usage of Mulesoft APIs. If access privileges of any Mulesoft APIs are different, then describe how privileges are handled.
AC-6(2): Least Privilege | Non-Privileged Access For Nonsecurity Functions	Review for impact and make a determination on the inclusion of usage of Mulesoft APIs. If access privileges of any Mulesoft APIs are different, then describe how privileges are handled.
AC-6(5): Least Privilege | Privileged Accounts	Review for impact and make a determination on the inclusion of the usage of Mulesoft APIs. If access privileges of any Mulesoft APIs are different, then describe how privileges are handled.
AC-6(10): Least Privilege | Prohibit Non-Privileged Users From Executing Privileged Functions.	Review for impact and make a determination on the inclusion of the usage of Mulesoft APIs. If access privileges of any Mulesoft APIs are different, then describe how privileges are handled.
AU-2: Audit Events	Review for impact and make a determination on the inclusion of the usage of APIs. Ensure that API calls are included in the auditable events and that appropriate activity logs are created.
IA-2: Identification And Authentication (Organizational Users)	Review for impact and make a determination on the inclusion of the usage of Mulesoft APIs. Describe the methods of Authentication in use by the Mulesoft API.
IA-2(1): Identification And Authentication (Organizational Users) | Network Access To Privileged Accounts	Review for impact and make a determination on the inclusion of the usage of Mulesoft APIs. Describe the methods of Authentication in use by the Mulesoft API. If Mulesoft APIs have or use privileged accounts, describe how MFA is implemented.
IA-2(2): Identification And Authentication (Organizational Users) | Network Access To Non-Privileged Accounts	If Mulesoft APIs have or use non-privileged accounts, describe how MFA is supported.
IA-5: Authenticator Management (c) Ensuring that authenticators have sufficient strength of mechanism for their intended use; (g) Changing/refreshing authenticators [Assignment: organization-defined time period by authenticator type]; (h) Protecting authenticator content from unauthorized disclosure and modification; (j) Changing authenticators for group/role accounts when membership to those accounts changes.	Describe how the authenticators used by Mulesoft APIs are managed, especially with regard to the conditions under which they are changed. This control must be updated to describe the authentication of API accounts if different from authentication of other accounts.
SC-8: Transmission Confidentiality and Integrity	Update to identify if Mulesoft APIs are using existing transmission means or additional transmission means have been established for Mulesoft APIs. Ensure web service connections are secured.
SC-8(1): Transmission Confidentiality and Integrity | Cryptographic or Alternate Physical Protection	Update to identify if Mulesoft APIs are using existing transmission means or additional transmission means have been established for Mulesoft APIs. Ensure web service connections are secured.

Appendix B: Security Controls and Configurations Provided by the Platform

The controls and configuration in Table B-1 are automatically applied to every Mulesoft API. Requested exceptions to these configurations are requested as part of the Security Package as described above.

Table B-1: Platform Security Controls and Configuration Information

Inherited Security Controls	Summary	Returned Status Codes	Input Fields	Values	Description
Rate Limiting	Specifies the maximum value for the number of messages processed per time period, and rejects any messages beyond the maximum. Applies rate limiting to all API calls, regardless of the source.	None	**Identifier**	gold	For each identifier value, the set of Limits defined in the policy will be enforced independently (i.e., #[attributes.queryParams['identifier']]).
			Limits		Pairs of maximum quota allowed and time window.
			# of Reqs	10000	Unit
			Time Period	1	
			Time Unit	DAYS	DAYS, HOURS, etc.,
Client ID Enforcement	The Client ID Enforcement policy restricts access to a protected resource by allowing requests only from registered client applications. The policy ensures that the client credentials sent on each request have been approved to consume the API.	401 - Unauthorized or invalid client application credentials 500 - Bad response from authorization server, or WSDL SOAP Fault error	**Credentials origin**		Origin of the Client ID and Client Secret credentials.
			Client ID Expression		Mule Expression to be used to extract the Client ID from API requests
			Client Secret Expression		Mule Expression to be used to extract the Client Secret from API requests
JSON threat protection	Protects against malicious JSON in API requests.	400 - Bad Request	**Maximum Container Depth**	3	Specifies the maximum allowed nested depth. JSON allows you to nest the containers (object and array) in any order to any depth
			Maximum String Value Length	256	Specifies the maximum length allowed for a string value

Inherited Security Controls	Summary	Returned Status Codes	Input Fields	Values	Description
			Maximum Object Entry Name Length	256	Specifies the maximum string length allowed for an object's entry name
			Maximum Object Entry Count	100	Specifies the maximum number of entries allowed in an object
			Maximum Array Element Count	100	Specifies the maximum number of elements allowed in an array
XML threat protection	Protects against malicious XML in API requests.	400 - Bad Request	**Maximum Node Depth**	3	Specifies the maximum node depth allowed in the XML.
			Maximum Attribute Count Per Element	25	Specifies the maximum number of attributes allowed for any element. Note that attributes used for defining namespaces are not counted.
			Maximum Child Count	25	Specifies a limit on the maximum number of children allowed for any element in the XML document.
			Maximum Text Length	512	Specifies a limit on the maximum length, in characters, of any text nodes present in the XML document.
			Maximum Attribute Length	25	Specifies a limit on the maximum length, in characters, of any attributes for any element in the XML document.
			Maximum Comment Length	256	Specifies a limit on the maximum number of comment characters in the XML document.
IP Blacklist	The IP Blacklist policy controls access to a configured API endpoint from a single IP address or a range of IP addresses.	403 - IP is rejected	**IP expression**		Mule Expression for extracting the IP address from this API request (e.g., #[attributes.headers['x-forwarded-for']]).

Inherited Security Controls	Summary	Returned Status Codes	Input Fields	Values	Description
			Blacklist		List of IP addresses denied from API access. You can add one or several IP addresses separated by comma or define a range (e.g., 192.168.0.1/16).
CORS	CORS (Cross-origin resource sharing) is a standard mechanism that allows JavaScript XMLHttpRequest (XHR) calls executed in a web page to interact with resources from non-origin domains. CORS is a commonly implemented solution to the "same-origin policy" that is enforced by all browsers.		**Origins**		Origin of the Client ID and Client Secret credentials.
			Access control max age		Indicates how long the results of a preflight request can be cached (in seconds)
			Methods		Mule Expression to be used to extract the Client Secret from API requests
			Headers		Comma separated list of request headers allowed to be sent to this API
			Exposed headers		Comma separated list of response headers clients of this API can access
Salesforce IP Whitelist Policy	Limits all service calls to a defined set of IP addresses.	403 - IP is rejected	**IP expression**		Mule Expression for extracting the IP address from this API request (e.g., #[attributes.headers['x-forwarded-for']]).
			Whitelist		Limited list of IP addresses allowed API access. You can add one or several IP addresses separated by comma or define a range (e.g., 192.168.0.1/16).
Spike Control	Control spikes in traffic by limiting the number of messages processed by an API. If the number is exceeded, the request will be queued for retry according to configuration. Uses a sliding window algorithm, ensuring that no more than the configured maximum requests are processed in the last X milliseconds (X being the configured time period). Applies spike control to all API calls, regardless of the source.	429 - Too many requests Request is rejected after a specified number of reattempts. The number of requests exceeded the configured limit.	**Number of Reqs**	10	Maximum quota allowed per time window.
			Time Period	100	Window's size in milliseconds.
			Delay Time in Milliseconds	499	Amount of time requested will be delayed before retrying (delaying is a CPU intensive process).
			Delay Attempts	1	The maximum number of times the policy will try to process the request if there is no quota available (delaying is a CPU intensive process).
			Queuing Limit	5	The maximum number of concurrent requests that can be waiting to be retried.

The following security control is optional and can be applied by the ISSM as an additional risk mitigation at their discretion.

Additional Security Controls	Summary	Returned Status Codes	Input Fields	Values	Description
GSA IP Whitelist Policy	Limits all service calls to a defined set of IP addresses.	403 - IP is rejected	**IP expression**		Mule Expression for extracting the IP address from this API request (e.g., #[attributes.headers['x-forwarded-for']]).
			Whitelist		Limited list of IP addresses allowed API access. You can add one or several IP addresses separated by comma or define a range (e.g., 192.168.0.1/16).