Intel® Endpoint Management Assistant (Intel® EMA)

API Guide

Rev. 1.14.2

February 2025

Doc. No.: , Rev.: 1.14.2

Legal Disclaimer

Intel technologies may require enabled hardware, software or service activation.

No product or component can be absolutely secure.

Your costs and results may vary.

No license (express or implied, by estoppel or otherwise) to any intellectual property rights is granted by this document.

Intel disclaims all express and implied warranties, including without limitation, the implied warranties of merchantability, fitness for a particular purpose, and non-infringement, as well as any warranty arising from course of performance, course of dealing, or usage in trade.

The products and services described may contain defects or errors known as errata which may cause deviations from published specifications. Current characterized errata are available on request.

Intel technologies' features and benefits depend on system configuration and may require enabled hardware, software or service activation. Performance varies depending on system configuration. No computer system can be absolutely secure. Intel does not assume any liability for lost or stolen data or systems or any damages resulting from such losses. Check with your system manufacturer or retailer or learn more at

http://www.intel.com/technology/vpro.

Contents

Figures

Tables

Revision History

Revision Number	Description	Release Date
1.14.0	Revision update only	August 2024
1.14.2	Revision update only	February 2025

1.0 Introduction

Intel® Endpoint Management Assistant (Intel® EMA) is a software application that provides an easy way to manage Intel vPro® platform-based devices in the cloud, both inside and outside the firewall. Intel® EMA is designed to make Intel® AMT easy to configure and use so that IT can manage devices equipped with Intel vPro platform technology without disrupting workflow. This in turn simplifies client management and can help reduce management costs for IT organizations.

Intel® EMA and its management console offer IT a sophisticated and flexible management solution by providing the ability to remotely and securely connect Intel AMT devices over the cloud. Benefits include:

- Intel® EMA can configure and use Intel AMT on Intel vPro platforms for out-of-band, hardware-level management
- Intel® EMA can manage systems using its software-based agent, while the OS is running, on non-Intel vPro® platforms or on Intel vPro® platforms where Intel AMT is not activated.
- Intel® EMA can be installed on premises or in the cloud.
- You can use Intel® EMA's built-in user interface or call Intel® EMA functionality from APIs

This document provides general information for developers about the Intel® EMA Application Programming Interface (API). Detailed information about individual API URIs (such as descriptions and parameters) are available in online format and can be displayed from the installed Intel® EMA application itself. After installing Intel® EMA, the online HTML-based version of the API documentation is accessible from a browser at https://<your_ema_url>/swagger.

In addition, the online HTML-based API documentation is available for download without installing Intel® EMA:

1. Go to https://www.intel.com/content/www/us/en/support/articles/000055621/software/manageability-products.html).
2. Click **Detailed HTML API Documentation** to download.
3. Open the downloaded file Vxswagger.html in a browser (Chrome works best), where "x" is the current released API version.

Code samples on how to use the API are available in the folder [Intel® EMA installation package folder] \Samples.

IMPORTANT

These samples should *never* be hosted in a production environment.

For hosting in a test environment for development purposes, copy the Samples folder to the Intel® EMA website root folder (e.g., C:\inetpub\wwwroot\).

NOTE

The version 9 (v9) APIs have been removed from this release of Intel® EMA. The version 10 (v10) APIs will be removed in the next release of the Intel® EMA API. Please upgrade any custom integration code you have created to use a new API version. We recommend, you always update to the latest API version as soon as possible as older versions will be removed upon subsequent updates. If desired, you can use the "latest" API path (for example, GET /api/latest/802_1XSetups) to ensure you are always calling the latest API version in your code.

2.0 Authentication and Authorization

Authentication and authorization are commonly understood terms for a framework that executes access control to ensure a secure environment and effective network management.

Auth Grant Types:

The Intel® EMA API offers two types of grants for token requests:

- Password – typical token for individual end users
- Client Credentials – used for non-interactive applications (such as a CLI, a daemon, or a service) where the token is issued to the application itself instead of an end user.

Windows Domain Authentication:

In addition to oAuth grant types, Intel® EMA also offers the option to use Windows domain authentication to obtain a bearer token. For details, see Access Tokens in the online API details file vXswagger.html at https://www.intel.com/content/www/us/en/support/articles/000055621/software/manageability-products.html.

Azure AD Authentication:

And Intel® EMA offers Azure AD authentication, which uses the "Microsoft identity platform and OAuth 2.0 authorization" flow. See the link below:

https://learn.microsoft.com/en-us/azure/active-directory/develop/v2-oauth2-auth-code-flow

2.1 Authentication

All requests made to the Intel® EMA REST API are met with a bearer token challenge. The token can be obtained via the OAuth2 Resource Owner Password Credentials flow in the token path **https://<your_ema_url>/api/token**.

To obtain a token, generate an HTTPS POST request to the token path using the following parameters (depending on your grant type) in the message body:

- grant_type: value can be either password or client_credentials,
- username: the resource owner's username (only for Password grant)
- password: the resource owner's password (only for Password grant)
- client_id: the Client Credentials client ID (only for Client Credentials grant)
- client_secret: the Client Credentials secret passphrase (only for Client Credentials grant)

IMPORTANT

This token has a preset expiration: a default of 60 minutes for Password grants, and a minimum of 60 minutes for Client Credentials grants (expiration is user configured, see Client Credentials API online documentation). During that time, the token can be used to make API calls. Ensure this token is protected, similarly to a username and password.

The following example illustrates a curl command line tool using HTTPS POST to obtain a bearer token via the HTTPS POST, replacing the placeholder values <in brackets>:

For Password grant:

```
$ curl -k -d
"grant_type=password&username=<user@yourdomain.com>&password=<password>" https://
<your_ema_url>/api/token
```

For Client Credentials grant:

```
$ curl -k -d
"grant_type=client_credentials&client_id=<Guid>&client_secret=<passphrase>"
https://<your_ema_url>/api/token
```

To use the bearer token to access an Intel® EMA Uniform Resource Identifier (URI), set the token in the request header as depicted in the following example with curl:

```
curl -H "Authorization: Bearer <token> " https://<your_ema_url>/api/v3/<endpoint>
```

2.2 Azure AD Authentication

NOTE

Azure AD authentication requires the Azure AD setup procedure that is documented in the installation prerequisites section of the Intel® EMA Server Installation and Maintenance Guide. .

Currently, Azure AD user login is supported only for direct interactions with the Intel® EMA web interface.

On Intel® EMA instances configured to use Azure AD authentication, it is not possible for external applications or scripts to retrieve a token for an Azure AD user using the REST API.

API integrations implementing authentication via Client Credentials will work on all Intel® EMA instances, including those configured to use Azure AD login. API actions available to Client Credentials are limited. See the online API documentation on any Intel® EMA instance at https://<your_ema_url>/swagger for details.

API integrations implementing user login via Password and/or Windows Domain authentication will continue to work with Intel® EMA instances configured to use those authentication methods.

2.3 Authorization

To use the REST API, callers must be in a specific role required by the URI. Role-based security supports authorization by making authorization decisions based on the user's identity or role membership.

The authorization process determines whether a specific user or client application has the necessary permissions to enforce specific commands or operations.

For Password grants, these permissions are based on user roles. A role is a set of principles that are under the same umbrella of privileges, security-wise. Thus, in the case of Intel® EMA, the system uses role membership to determine whether a user is authorized to perform a requested action.

For Password grants, these roles are:

- **Global Administrator:** This role performs user management, tenant management, and server management. The Global Administrator does not perform endpoint management and does not (and cannot) belong to any endpoint group. The Global Administrator's control spans all tenants in a single Intel® EMA server installation instance.Tenant Administrator: This role is specific to a particular tenant and can perform all operations (user management, endpoint management, Intel AMT Discovery) under that tenant. Therefore, the Tenant Administrator does not (and cannot) belong to any user group in its tenant. A Tenant Administrator user cannot manage a Global Administrator user.
- **Account Manager:** This role is specific to a particular tenant, and can perform user management only. However, an Account Manager cannot manage users with higher-level roles (e.g., a Tenant Administrator or Global Administrator). Account Managers cannot perform endpoint management, and therefore cannot belong to any user group.
- **Endpoint Group Creator:** This role is specific to a particular tenant. It can perform endpoint management, as well as create new endpoint groups and manage Intel AMT Profiles. An Endpoint Group Creator can be a member of multiple user groups and can manage all groups to which they belong. Endpoint Group Creators cannot perform user management. However, they can see the list of all user groups and the list of all Endpoint Group Creators and Endpoint Group Users in that tenant (i.e., user roles in that tenant that are equal or lower in the user role hierarchy; they cannot see Account Managers, Tenant Administrators, or Global Administrators).
- **Endpoint Group User:** This role is specific to a particular tenant, and can perform endpoint management only. Endpoint Group Users can be members of multiple user groups, but they cannot perform user management, and can only view their own user information.

  Refer the Intel® EMA Administration and Usage Guide document for further information about the user roles.

  For Client Credentials grants, such permissions are based on "scope," not "role". A client application's scope determines what that application can do within Intel® EMA. In this release, there is only one supported scope:

- **Endpoint management:** can manage (any In Band or Out-of-Band operation) and provision any endpoint within a given Tenant, regardless of which user groups or endpoint groups to which the endpoint belongs.

Authorization enables you to make more granular choices when it comes to granting access to specific resources. There are authorization filters that are triggered before an action is requested to verify if the requesting user has the necessary privileges to perform the action. If the request is not authorized, the filter returns an error message and the action is not executed.

3.0 Troubleshooting

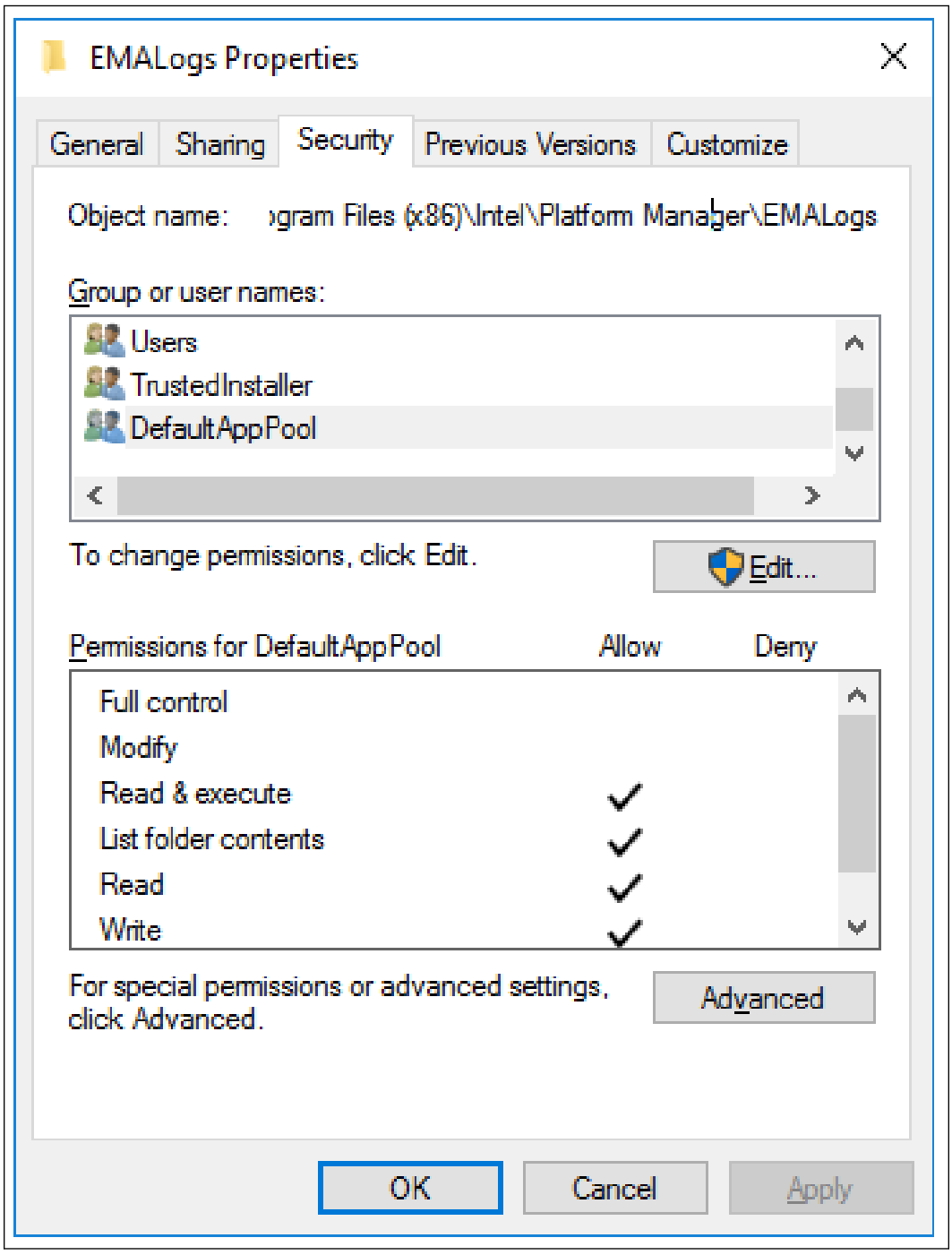
The Intel® EMA Server uses the NLog to log Intel® EMA API errors and debug information. The configuration file is located in **c:\inetpub\wwwroot\NLog.config**.

The default directory where the troubleshooting logs are written is **C:\Program Files (x86)\Intel\Platform Manager\EMALogs**.

Troubleshooting logs are written in the subdirectory EmaWebApiLogs within, which is a directory for each tenant.

For this release, the write permission to **C:\Program Files (x86)\Intel\Platform Manager\EMALogs must be configured for the system account IIS AppPool \DefaultAppPool**

Figure 1. EMALogs Properties



4.0 HTTP Status Codes

The Intel® EMA API uses HTTP status codes that generally follow REST conventions where 2xx indicates success, 4xx indicates client errors, and 5xx indicates server errors. The following error codes are commonly used in the Intel® EMA API.

- **200 OK**: Successful request with content returned.
- **204 No Content**: Successful request with no content returned.
- **400 Bad Request**: bad request from the client.
- **401 Unauthorized:** the client is not authenticated.
- **403 Forbidden:** the client does not have the correct permissions to access the resource.
- **404 Not Found:** the requested resource is not found.
- **405 Method Not Allowed:** the requested method is not supported by the resource.
- **409 Conflict:** the request could not be completed do to a conflict with the current state of the resource.
- **415 Unsupported Media Type:** the resource does not support the media type from the request.
- **500 Internal Server Error:** the server encountered an unexpected error.

In some cases the error messages will be returned as the Intel® EMA API Extended Errors in following format:

```
{
  "Message":  {
    "ExtendedCode": string,
    "ExtendedMessage": "string"
   }
}
```

4.1 400 Bad Request Errors

The following is a table listing the Intel® EMA API Extended Errors for error code 400.

Extended Code	Error Type	Extended Message
1000	OFFSET_PARAMETER_INVALID_400	Offset parameter is invalid
1001	PAGESIZE_PARAMETER_INVALID_400	pageSize parameter is invalid
1002	POWERSTATE_PARAMETER_INVALID_400	powerState parameter is invalid
1003	CONNECTIONSTATE_PARAMETER_INVALID_400	connectionState parameter is invalid
1004	STARTDATE_PARAMETER_INVALID_400	startDate parameter is invalid
1005	ENDDATE_PARAMETER_INVALID_400	endDate parameter is invalid

continued...

Extended Code	Error Type	Extended Message
1006	ENABLED_PARAMETER_INVALID_400	enabled parameter is invalid
1007	TENANTID_PARAMETER_INVALID_400	tenantId parameter is invalid
1008	ROLEID_PARAMETER_INVALID_400	roleId parameter is invalid
1009	SEARCHTYPE_PARAMETER_INVALID_400	searchType parameter is invalid
1010	SEARCHVALUE_PARAMETER_INVALID_400	searchValue parameter is invalid
1011	SEARCH_PARAMETERS_INVALID_400	both search parameters are required
1012	UPDATE_PARAMETERS_INVALID_400	update parameters are required
1013	ENDPOINTGROUPID_PARAMETER_INVALID_400	endpointGroupId parameter is invliad
1014	USERGROUP_DISSOCIATION_INVALID_400	userGroup parameter is invalid
1015	IP_ADDRESS_INVALID_400	IP address is invalid
1016	START_IP_ADDRESS_INVALID_400	Start IP address is invalid
1017	END_IP_ADDRESS_INVALID_400	End IP address is invalid
1018	SUBNETMASK_INVALID_400	Subnetmask is invalid
1019	AMT_NOT_SUPPORTED_400	Endpoint does not have Intel AMT support
1020	AMT_FW_INVALID_400	Endpoint Intel ME version is invalid for Intel AMT provisioning
1021	AMT_ONLY_EITHER_TLS_OR_CIRA_CAN_BE_SELECTED_400	Only either TLS or CIRA can be selected for Intel AMT provisioning
1022	AMT_USB_PROVISIONING_NOT_SUPPORTED_400	Endpoint does not support Intel AMT provisioning using USB
1023	AMT_HBP_PROVISIONING_NOT_SUPPORTED_400	Endpoint does not support Intel AMT host based provisioning
1024	AMT_PKI_PROVISIONING_NOT_SUPPORTED_400	Endpoint does not support Intel AMT PKI certificate based provisioning
1025	AMT_PROVISIONING_CERT_HASH_TYPE_UNKNOWN_400	Intel AMT provisioning certificate hash type is unknown
1026	AMT_CIRA_NOT_SUPPORTED_400	Endpoint does not support CIRA
1027	CURRENT_PASSWORD_CANNOT_BE_NULL_OR_EMPTY_400	Current password cannot be null or empty
1028	CALLERID_PARAMETER_INVALID_400	callerId parameter is invalid
1029	WIFISETUP_ENABLED_BUT_NO_WIFISETUPID_SELECTED_400	Wi-Fi Connection Setup enabled, but no WifiSetupId selected
1030	WIFISETUP_NOT_ENABLED_BUT_WIFISETUPID_SELECTED_400	Wi-Fi Connection Setup not enabled, but WifiSetupId(s) selected
1031	ENDPOINTGROUP_AMTPROFILEID_NOT_EXISTS_400	Cannot update Endpoint Group since AmtProfile ID not exists

continued...

Extended Code	Error Type	Extended Message
1032	PASSWORD_RESET_FAILED_DUE_TO_BAD_CREDENTIALS_400	Password reset failed due to bad credentials
1033	WIFISETUP_IDS_NOT_IN_DATABASE_400	WiFiSetupIds(s) associated with Intel AMT Profile were not found in the Database
1034	MODEL_CANNOT_BE_NULL_400	Model cannot be null
1035	CALLER_NOT_PERMITTED_TO_CREATE_USER_HAVING_SELECTED_ROLE_400	Caller not permitted to create a new user with selected role
1036	CALLER_NOT_PERMITTED_TO_CREATE_USER_WITH_SELECTED_TENANTID_400	Caller not permitted to create a new user with a different tenant
1037	CALLER_NOT_PERMITTED_TO_CREATE_USER_WITHOUT_TENANTID_400	Caller not permitted to create a new user without a tenant
1038	CALLER_NOT_PERMITTED_TO_UPDATE_USER_WITH_SELECTED_ROLE_ID_400	Caller not permitted to update user with selected role
1039	NAME_ONLY_ONE_PER_REQUEST_400	Only one name per request allowed
1040	PASSWORD_ONLY_ONE_PER_REQUEST_400	Only one password per request allowed
1041	FILE_ONLY_ONE_PER_REQUEST_400	Only one file per request allowed
1042	FILE_INVALID_400	Uploaded file is invalid
1043	CERTIFICATE_NAME_INVALID_400	Certificate name is invalid
1044	CERTIFICATE_PASSWORD_INVALID_400	Certificate password is invalid
1045	CERTIFICATE_IMPORT_FAILED_400	Certificate import failed. Please check that the .PFX file and password are valid
1046	UPLOADED_FILE_NOT_AMT_PROVISIONING_CERTIFICATE_400	Uploaded file is not an Intel AMT provisioning certificate
1047	CERTIFICATE_ID_INVALID_400	Certificate ID is invalid
1048	CERTIFICATE_IS_NOT_FOR_AMT_PROVISIONING_400	Certificate is not for Intel AMT provisioning
1049	AMTSETUPID_SPECIFIED_IN_REQUEST_IS_INVALID_400	The AmtSetupId specified in the request is invalid
1050	AMTPROFILE_ID_INVALID_400	Intel AMT Profile ID is invalid
1051	CERTIFICATE_HAS_EXPIRED_400	Certificate has expired
1052	CIRA_INTRANET_SUFFIX_INVALID_400	CIRA Intranet Suffix is invalid
1053	CIRA_LIMIT_EXCEEDED	CIRA Proxies limit exceeded
1054	CREATE_DISABLED_USER_NOT_ALLOWED_400	Creating new user with enabled set to false is not permitted
1055	_802_1X_SETUP_ROOT_CERTIFICATE_REQUIRED_400	A root certificate is required for the specified authentication protocol
1056	_802_1X_SETUP_CLIENT_CERTIFICATE_REQUIRED_400	A client certificate is required for the specified authentication protocol

continued...

Extended Code	Error Type	Extended Message
1057	_802_1X_SETUP_INVALID_CONFIGURATION_SETTINGS_REQUIRED_400	Invalid configuration settings for certificate (required), please review
1058	_802_1X_SETUP_INVALID_CONFIGURATION_SETTINGS_400	Invalid configuration settings for certificate, please review
1059	_802_1X_SETUP_PSK_PARAMETER_INVALID_400	The field PSK is not a valid OctetString
1060	_802_1X_SETUP_PROTECTED_ACCESS_CREDENTIAL_PARAMETER_INVALID_400	The field ProtectedAccessCredential is not a valid OctetString
1061	_802_1X_SETUP_SERVER_CERTIFICATE_NAME_COMPARISON_OPTION_INVALID_400	The field ServerCertificateNameComparisonOption is not a valid number
1062	MAX_FILE_SIZE_EXCEEDED_400	The file size exceeds the maximum allowed
1063	ENDPOINTS_LIST_CANNOT_BE_EMPTY_400	Endpoints list cannot be empty
1064	_802_1X_SETUP_PROTOCOL_INVALID_400	The authentication protocol is not supported.
1065	AMT_GLOBALLY_DISABLED_400	Intel AMT in Endpoint is globally disabled and cannot be provisioned.
1066	MEBX_PASS_CHANGE_HBP_NOT_SUPPORTED_400	Intel MEBx password change is not supported during Host Based Provisioning
1067	_802_1X_SETUP_SERVER_CERTIFICATE_DESIGNATEDCN_COMMONNAME_MISMATCH_400	Invalid DesignatedCN, it is not part of the CommonNames.
1068	_802_1X_SETUP_INVALID_ROOT_CERTIFICATE_400	Root certificate is not valid or does not exist.
1069	_802_1X_SETUP_INVALID_CLIENT_CERTIFICATE_400	Client certificate is not valid or does not exist.
1070	_802_1X_SETUP_INVALID_COMMON_NAMES_400	Invalid or empty CommonNames.
1071	HOSTNAME_PARAMETER_INVALID_400	Input HostName parameter is invalid.
1072	ENDPOINT_NOT_ROUTABLE_400	Endpoint is not routable.
1073	BAD_PROVISIONING_STATE_400	Endpoint provisioning state is not correct.
1074	POWER_OP_NOT_SUPPORTED_400	Power operation sent is not supported.
1075	INVALID_AMT_CREDENTIAL_TYPE_400	Input Intel AMT credential type is invalid.
1076	INVALID_USERNAME_FORMAT_400	Invalid username format.
1083	INVALID_CLIENT_CREDENTIALS_UPDATE_400	A client credentials account cannot be updated using this method. Please update the account using the Client Credentials API.
1084	_802_1X_INVALID_SECURITY_GROUP_LENGTH_400	Invalid length for security group.
1085	_802_1X_MAX_SECURITY_GROUPS_NUMBER_EXCEEDED_400	Maximum number of security groups exceeded.
1091	START_OPERATION_FAILED_400	Failed to start remote secure erase.
1092	FEATURE_NOT_SUPPORTED_ON_ENDPOINT_400	The feature is not supported on the Endpoint.

continued...

Extended Code	Error Type	Extended Message
1093	_802_1X_DESIGNATED_SUBJECT_NOT_SUPPORTED_400	Selected designated subject common name is not supported.
2031	USER_DELETING_CLIENT_CREDENTIALS_400	A client credentials account cannot be deleted using this method. Please delete the account using the Client Credentials API.
3002	RESOURCEID_ON_PATH_AND_MODEL_DO_NOT_MATCH_400	Resource Id value on the path to the controller and Resource Id in the input model do not match
3003	ENDPOINTID_PARAMETER_INVALID_400	Input endpoint Id parameter is invalid
3004	USERGROUPID_PARAMETER_INVALID_400	Input endpoint Id parameter is invalid
3005	TENANTID_OF_REQUESTED_ROLE_AND_TARGET_USER_DO_NOT_MATCH_400	TenantId of requested role and target user do not match
3008	MAC_ADDRESS_INVALID_400	MAC address is invalid or does not exist
3009	IP_RANGE_INVALID_400	End IP Address cannot be lower than Start IP Address
3011	INVALID_PASSWORD_FORMAT_400	Invalid password format
3012	UPN_IS_NOT_IN_DOMAIN_400	UPN used is not registered in this domain
3017	MANUAL_USER_LOCKING_NOT_SUPPORTED_400	Manually locking user is not currently supported
3018	POWER_OP_NOT_SUPPORTED_IN_FW_400	Endpoint does not support the power operation sent
4004	USER_CONSENT_NOT_REQUIRED_400	User consent is not required.
4005	USER_CONSENT_INVALID_DISPLAY_400	This display is not supported by AMT.
4007	USER_CONSENT_CODE_INVALID_400	User consent code is invalid.
4010	RESUMABLE_ID_INVALID_400	Resumable ID is invalid.
4011	USBRIMAGE_ID_INVALID_400	USBR image ID is invalid.
4012	USER_ID_INVALID_400	User ID is invalid.
4013	WIFISETUP_ID_INVALID	WiFi ID is invalid.
4014	_802_1X_SETUP_ID_INVALID_400	802.1x Setup ID is invalid.
4015	CLIENT_CREDENTIALS_ID_INVALID_400	Client credentials ID is invalid.
4017	MODEL_PYRITEPSID_CANNOT_BE_EMPTY_400	Pyrite PSID cannot be empty.
4018	MODEL_SSDMASTERPASSWORD_CANNOT_BE_EMPTY_400	SSD Master password cannot be empty.
4019	RPE_FAILED_400	Failed to start remote platform erase.
4020	ADMINPASSWORD_NOT_REQUIRED_400	Do not provide Admin Password if Random Admin Password option is selected.
4021	BOOTOPTION_NOT_FOUND_400	OCR Boot option cannot be found in Intel AMT.
4023	ENDPOINTADOPTION_ENDPOINTGROUP_AUTOSETUP_NOT_FOUND_400	The endpoint group of the target endpoint does not have AutoSetup enabled.
4024	ENDPOINTADOPTION_AMTSETUP_ALREADY_EXISTS_400	The target endpoint is already provisioned by EMA.
4025	_802_1X_SETUP_ID_DOESNT_EXIST_400	The 802.1x setup Id does not exist in the database.

continued...

Extended Code	Error Type	Extended Message
4026	_802_1X_SETUP_ORGANIZATIONUNIT_CONFLICT_400	All specified 802.1x related profiles (wired + any wireless) must have matching Organization Unit configuration.
4027	DISALLOWED_PASSWORD_USED_400	Password is on the disallowed list. Please choose a different password.
4028	ALARM_NOT_FOUND_400	Alarm cannot be found in endpoint
4029	DATETIME_UTC_FORMAT_INVALID_400	DateTime format is not a valid UTC format
4032	AMT_ALARM_CLOCK_STARTTIME_INVALID_400	The start time for the Intel AMT alarm clock is invalid.
4033	SCOPE_PARAMETER_INVALID_400	The value of the scope parameter for creating a client credentials account is invalid.

4.2 401 Method Not Allowed Errors

The following is a table listing the Intel® EMA API Extended Errors for error code 401.

Table 1. 401 Intel® EMA API Extended Errors

Extended Code	Error Type	Extended Message
4000	UNAUTHORIZED_USER_NOT_REGISTERED_401	User is not registered in Intel® EMA system
4001	INVALID_USERNAME_OR_PASSWORD_401	The user name or password may be incorrect, or the account may be locked.

4.3 403 Forbidden Errors

The following is a table listing the Intel® EMA API Extended Errors for error code 403.

Table 2. 403 Intel® EMA API Extended Errors

Extended Code	Error Type	Extended Message
3006	USER_LOCKED_OR_DELETED_403	The user is locked or doesn't exist
3015	AMT_PROVISION_RECORD_RETRIEVE_FORBIDDEN	User has insufficient rights to retrieve Intel AMT credentials
3019	POWER_OP_NOT_ALLOWED_403	Endpoint is not allowed to execute this power operation
3023	POWER_OP_USER_FORBIDDEN_403	User not allowed to execute power operations

continued...

Extended Code	Error Type	Extended Message
4003	USBR_STOP_SESSION_NOT_ALLOWED_403	User is not allowed to stop the USB-R session on the Endpoint.
4022	ENDPOINTADOPTION_CALLER_INVALID_403	The caller does not have Execute right for the target endpoint.
	CALLER_NOT_PERMITTED_TO_CREATE_TOTP_OTHERUSER_403	The caller is not permitted to create Totp enrollment for other user.

4.4 404 Not Found Errors

The following is a table listing the Intel® EMA API Extended Errors for error code 404.

Table 3. 404 Intel® EMA API Extended Errors

Extended Code	Error Type	Extended Message
3013	AMT_PROVISION_RECORD_NOT_FOUND	Intel AMT Provisioning Record does not exist in database
3014	UNABLE_TO_RETRIEVE_AMT_PROVISION_RECORD	Intel AMT Provisioning Record does not exist in database
3016	ENDPOINTID_RECORD_NOT_FOUND	Endpoint record does not exist in database
3025	UNABLE_TO_RETRIEVE_MEBX_PASSWORD	Intel MEBx password doesn't exist in the database
4008	FILE_NOT_ON_DISK_404	File is not on the disk.

4.5 405 Method Not Allowed Error

The following is a table listing the Intel® EMA API Extended Errors for error code 405.

Table 4. 405 Intel® EMA API Extended Errors

Extended Code	Error Type	Extended Message
3010	METHOD_NOT_ALLOWED_WRONG_AUTH_MODE_405	Method not allowed due to current authentication mode
4034	METHOD_NOT_ALLOWED_DEPRECATED_API_VERSION_405	Method not allowed, please use latest version.

4.6 409 Conflict Errors

The following is a table listing the Intel® EMA API Extended Errors for error code 409.

Table 5. 409 Extended Intel® EMA API Errors

Extended Code	Error Type	Extended Message
2001	USER_GROUP_NAME_CONFLICT_409	UserGroup.Name already exists
2002	ENDPOINT_GROUP_NAME_CONFLICT_409	EndpointGroup.Name already exists
2003	USER_NAME_CONFLICT_409	User.Name already exists
2004	TENANT_NAME_CONFLICT_409	Tenant.Name already exists
2005	USER_GROUP_TO_ENDPOINT_GROUP_CONFLICT_409	UserGroup and EndpointGroup are already associated
2006	AMT_NOT_PROVISIONED_UNPROVISIONING_NOT_POSSIBLE_409	Unprovision is not possible since endpoint is not provisioned
2007	AMT_ALREADY_PROVISIONED_409	Intel AMT is already provisioned
2008	WIFISETUP_NAME_CONFLICT_409	WiFiSetup.SetupName already exists
2009	AMTPROFILE_NAME_CONFLICT_409	AMTProfile.Name already exists
2010	AMTPROFILE_STILL_LINKED_TO_ENDPOINTGROUP_CONFLICT_409	Cannot delete Intel AMT Profile since it is still linked to at least one Endpoint Group
2011	WIFISETUP_STILL_LINKED_TO_AMTPROFILE_CONFLICT_409	still linked to Intel AMT Profile
2012	REQUEST_NOT_POSSIBLE_TCPRELAY_DISABLED_IN_POLICY_409	Request is not possible because TCPRELAY is disabled in the Policy Group
2013	AMTCERTIFICATE_PART_OF_ANOTHER_CHAIN_409	Intel AMT certificate could not be deleted, since it is part of another Intel AMT Certificate Chain
2014	AMTCERTIFICATE_IN_USE_BY_PROFILE_409	Intel AMT certificate could not be deleted, since it is use in an Intel AMT Profile for provisioning
2015	CERTIFICATE_THUMBPRINT_ALREADY_EXISTS_409	since its thumbprint already exists in the database
2016	CERTIFICATE_NAME_ALREADY_EXISTS_409	name is already in use
2017	_802_1X_SETUP_NAME_CONFLICT_409	802_1XSetup.SetupName already exists
2018	_802_1X_SETUP_ID_CONFLICT_409	SetupId in model and from request don't match
2019	_802_1X_SETUP_STILL_LINKED_TO_WIFISETUP_CONFLICT_409	still linked to WiFi Seup
2020	_802_1X_SETUP_STILL_LINKED_TO_AMTPROFILE_CONFLICT_409	Cannot delete 802.1x Setup since it is still linked to Intel AMT Profile
2021	AMTPROFILE_STILL_LINKED_TO_INTELAMTSETUP_CONFLICT_409	it is still linked to at least one Intel AMT Setup record
2022	FW_NOT_READY_409	Endpoint is not ready to execute this operation yet, please wait and retry.
2023	AMT_CONNECTION_CONFLICT_409	problem.

continued...

Extended Code	Error Type	Extended Message
2024	AMT_PROVISION_STATE_CONFLICT_409	Intel AMT must be in post-provisioning state.
2025	ENDPOINT_NOT_ROUTABLE_CONFLICT_409	Endpoint must be CIRA connected or have neighbors.
2026	CIRA_CANT_USE_STATIC_IP_409	CIRA Setup doesn't allow profiles with Static IP.
2027	REALM_CONFLICT_409	Different realm reported by Endpoint, operation cancelled
2028	CLIENT_CREDENTIALS_TENANT_CONFLICT_409	A Client Credentials account already exists for this tenant.
2029	FILENAME_NOT_UNIQUE_409	File name has already been taken.
4006	USER_CONSENT_ALREADY_STARTED_409	User consent already started.
4030	NUMBER_OF_AMT_ALARM_CLOCK_LIMIT_REACHED_409	Number of Alarm clocks set per endpoint cannot be more than 5.
4031	AMT_ALARM_CLOCK_NAME_NOT_UNIQUE_409	Name of Alarm clocks per endpoint should be unique.
4035	TOTP_ENROLLMENT_ALREADY_EXISTS_409	User is already enrolled in Totp.

4.7 415 Unsupported Media Type Errors

The following is a table listing the Intel® EMA API Extended Errors for error code 415.

Table 6. 415 Intel® EMA API Extended Errors

Extended Code	Error Type	Extended Message
3000	BAD_MEDIA_ONLY_TEXT_FILE_ACCEPTED_415	Only the text file is accepted.

4.8 500 Internal Server Errors

The following is a table listing the Intel® EMA API Extended Errors for error code 500.

Table 7. 500 Intel® EMA API Extended Errors

Extended Code	Error Type	Extended Message
4009	NO_WRITE_ACCESS_TO_DIRECTORY_500	Intel® EMA doesn't have write access to the directory.
4036	TOTP_ENROLLMENT_ONLY_SUPPORTS_NORMAL_AUTH_501	Totp enrollment is only supported in Normal Authentication mode.