SEL Configuration API Instruction Manual

Introduction

The SEL Configuration API is an application programming interface (API) that you can use to access the protection, security, and communications device configuration data stored in the AcSELERATOR® Database. The database is managed by either Device Manager in AcSELERATOR QuickSet® SEL-5030 Software or SEL-5037 Grid Configurator.

The API is deployed as a representational state transfer (RESTful) web service running as a Windows service. The RESTful web service is a de facto standard that you can access through client applications by using most programming languages.

This instruction manual explains how to install and configure the API. Once the API is installed and configured, you can use the API Programmer's Reference and examples to learn how to access the API from your client application.

System Requirements

➤ The API must be installed on the same computer as the AcSELERATOR Database that it will service.

➤ The AcSELERATOR Database must be at a version compatible with the version of the API that you are installing. Contact Technical Support for version compatibility information. To identify the currently installed version, use the API **GET sca/database_information** endpoint.

➤ The API is only supported on Windows 10 x64 and Windows Server 2016 x64 operating systems. You must have .NET Framework 4.7.2 installed on the computer.

Installing the SEL Configuration API

Install the API by running the installer, which is available on the SEL website.

Ensure that the service account has the following permissions:

➤ Read and write access to the following folder and its subfolders: %ProgramData%\SEL\SCA\Service

➤ Run As Service. You do not have to explicitly grant this permission; the operating system grants this permission when you start the service with the new account.

Obtain the following permission for the service account when you use the SEL Configuration API to perform database backups or restores and TEAM services are installed locally:

➤ Start and Stop Windows Services

NOTE
To ensure application of appropriate permissions to dependent files, run the installer program again to change the service account under which SEL Configuration API runs.

After completing the installation, verify that the API installed correctly by entering the following URL in a web browser that is running on the same computer:

http://localhost:5231

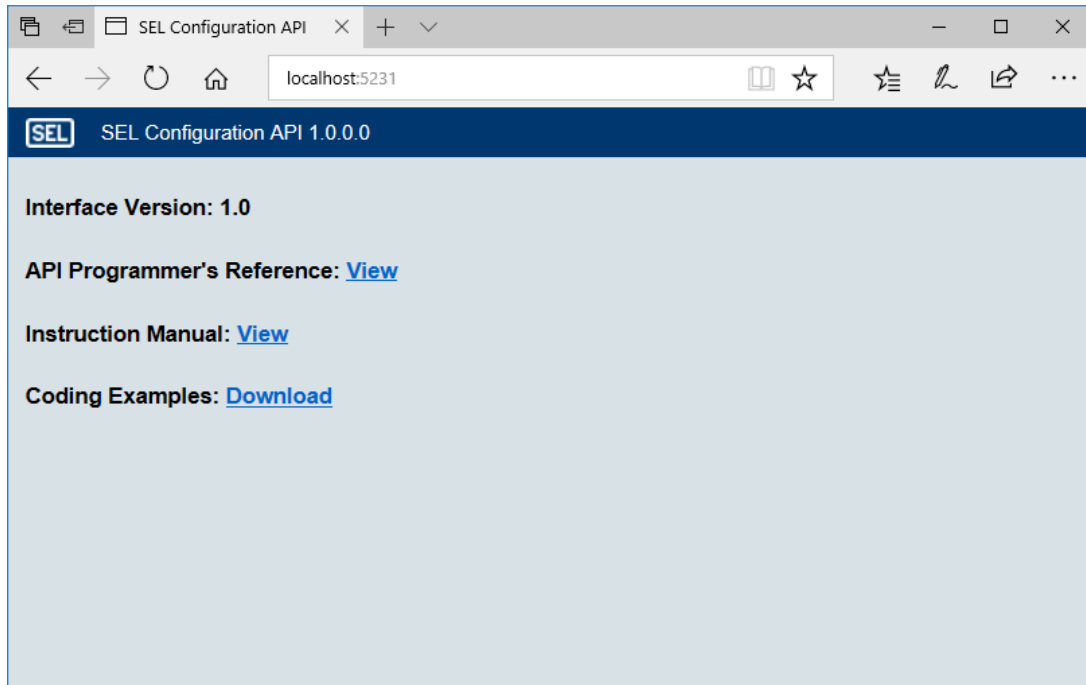If the API is installed correctly, you will see the home page, as shown in *Figure 1*.

Figure 1   API Home Page

API Accessibility

When installed, the API uses the HTTP protocol and only accepts local connections from the same computer.

When configured with a certificate, the service uses the more secure HTTPS protocol. An API license is required for the service to accept remote connections from other computers.

Configuring the SEL Configuration API

Service Account

The API is installed to run under the Local Service account, as indicated in *Figure 2*. You can use the Services control panel applet to configure the service to run under a local or domain account.
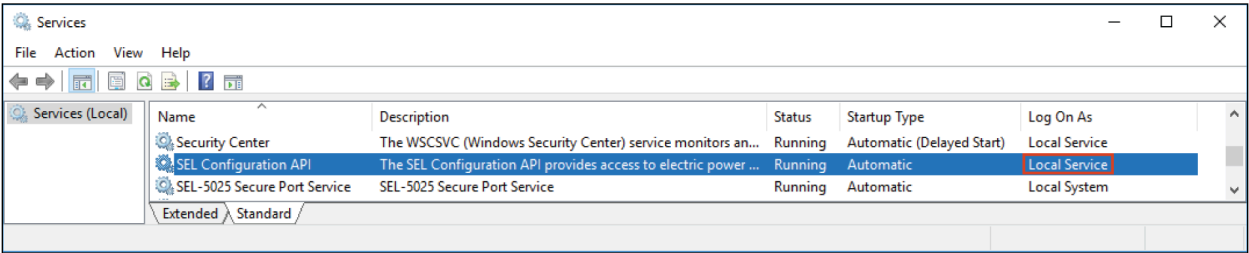
Figure 2   Services Control Panel

The service account must have the following permissions.

➤ Read and write access to the following folder and its subfolders:

%ProgramData%\SEL\SCA\Service

➤ Run As Service. You do not have to explicitly grant this permission; the operating system grants this permission when you start the service with the new account.

Restart the service after configuring the service account.

Service Configuration

Use the SEL Configuration API Setup utility to change the configuration of the API. This utility can be found under the SEL Applications folder in the Start menu.

When first started, the utility displays the default configuration from the installation, as shown in *Figure 3*.
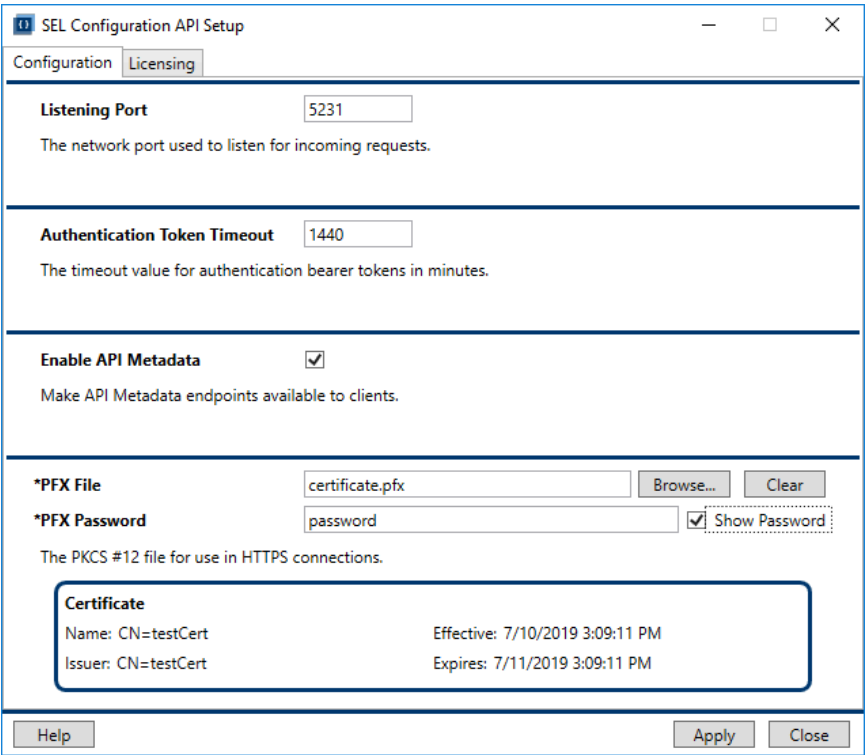

Figure 3   Default Configuration

Update the configuration as needed for your environment, and select Apply to save the new configuration. The API uses the new configuration after the API restarts. Note that your configuration may vary between a system used to develop and test an application and a production system.

Listening Port

The listening port is used to receive incoming requests. Ensure the assigned port is not in use by another application.

>**Default:** 5231

>**Valid values:** 1–65535

Authentication Token Timeout

The Authentication Token Timeout setting is the time-out value (in minutes) for an authentication bearer token returned by the service when an application logs in to the API. Your client application must provide the token on subsequent API requests.

The API reports an authentication error if an expired token is provided on a request, requiring that the client application log in again.

Adjust the token expiration time-out to suit the needs of your application.

>**Default:** 1440 minutes (24 hours)

>**Valid values:** 1–525,600 minutes (365 days)

Enable API Metadata

The Enable API Metadata configuration setting makes API metadata endpoints available to clients. These endpoints provide development and testing features that are disabled by default to prevent their misuse in a production environment. See the API Programmer's Reference for more information on using these endpoints.

>**Default:** False

>**Valid values:** False, True

PFX File

The PFX File setting can be used to configure a PKCS #12 certificate file, which allows the API to use the HTTPS protocol and accept connections from other computers.

Work with your Information Services department to determine your requirements, and obtain a certificate if needed.

>**Default:** Not configured

>**Valid values:** File path and password for a valid PKCS #12 certificate file (see *Figure 4*). PFX files with an empty password are not supported.

Figure 4   Specify Certificate

Licensing the SEL Configuration API

A license is required to use the API remotely from other computers. To purchase an SEL Configuration API SEL-5231 Software license file, contact your local SEL sales representative. Once you have purchased a license, perform the following steps as necessary for software licensing:

➤ *Internet Activate on page 5*

➤ *Internet Deactivate on page 7*

➤ *Manual Activate on page 9*

➤ *Manual Deactivate on page 13*

Internet Activate

Step 1.   Open the SEL Configuration API Setup utility.

Step 2.   Select the **Licensing** tab.

Step 3.   From the Licensing tab, select **Internet Activate**.
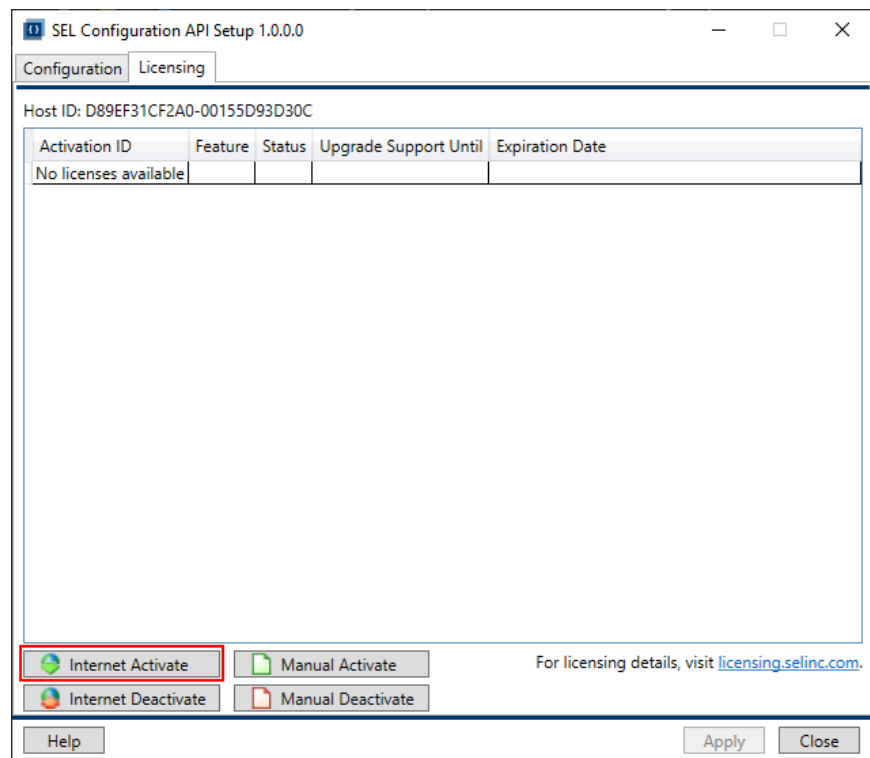
Figure 5   Internet Activate

Step 4. At the Enter Activation ID window, enter the Activation ID you received when you purchased your license.
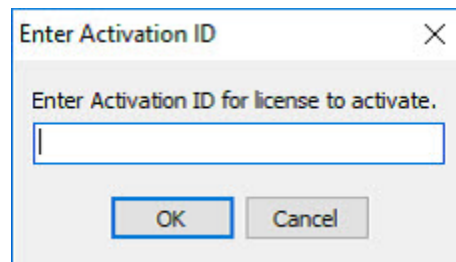

Figure 6   Enter Activation ID

Step 5. Select **OK**. When you successfully activate your license, the License Information window displays your active license information.
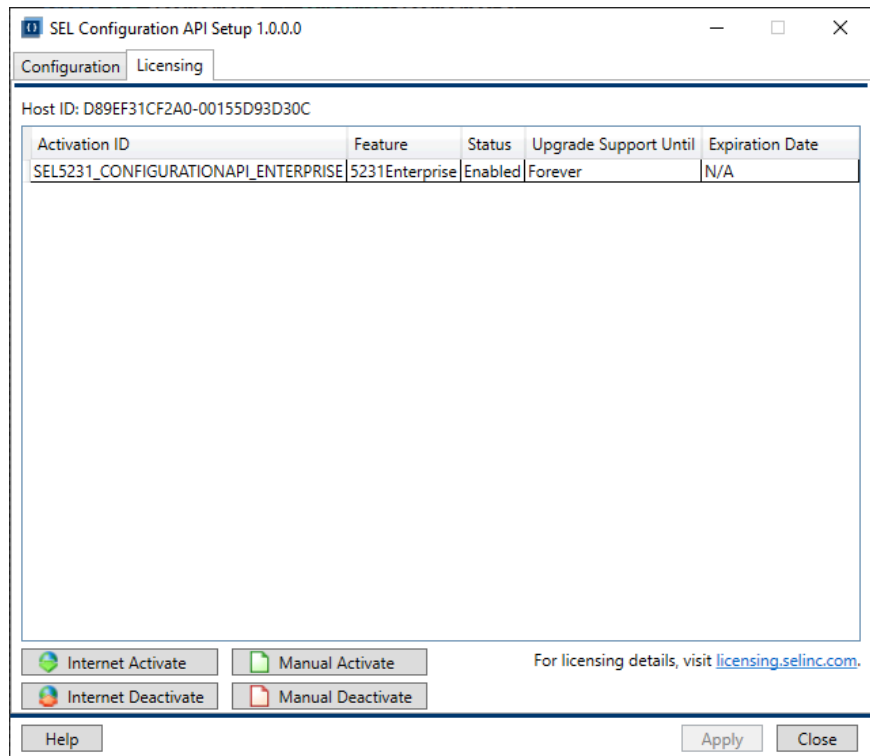
Figure 7   Available Licenses

Internet Deactivate

Step 1.   Open the SEL Configuration API Setup utility.

Step 2.   Select the **Licensing** tab.

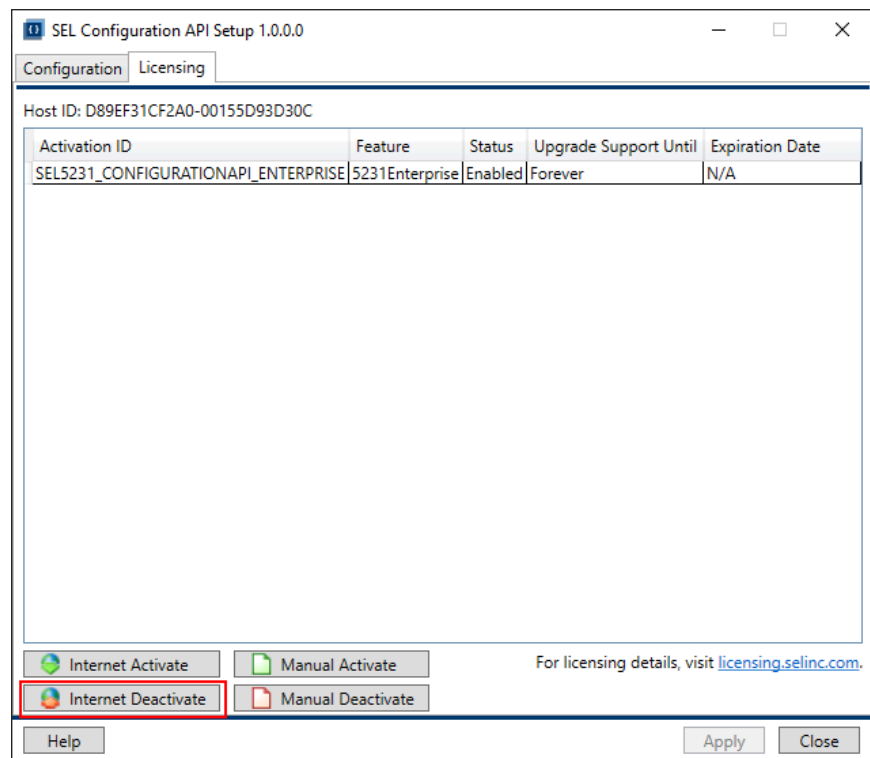Step 3.   From the Licensing tab, select **Internet Deactivate**.

Figure 8   Internet Deactivate

Step 4.   From the Enter Activation ID window, enter the Activation ID you intend to deactivate.
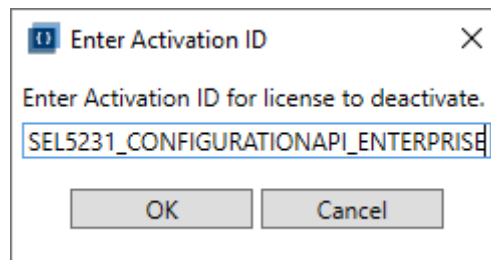

Figure 9   Verify Activation ID

Step 5.   Select **OK**. When you successfully deactivate your license, the License Information window no longer displays your active license for the deactivated Activation ID.
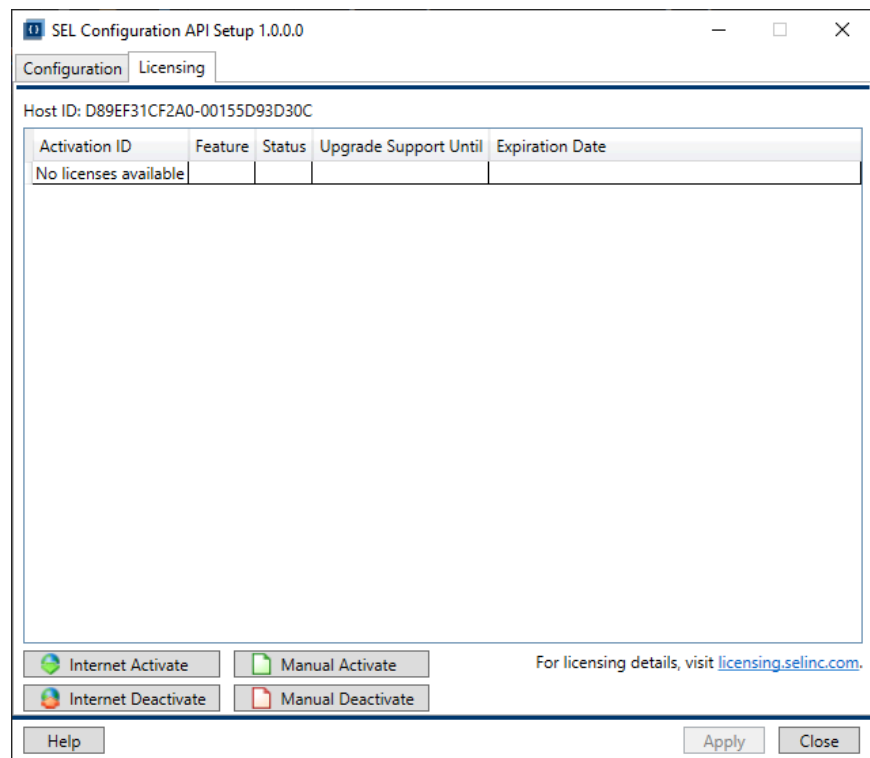
Figure 10   No Licenses Available

Step 6.   Select **Close**.

Manual Activate

Step 1.   Open the SEL Configuration API Setup utility.

Step 2.   Select the **Licensing** tab.

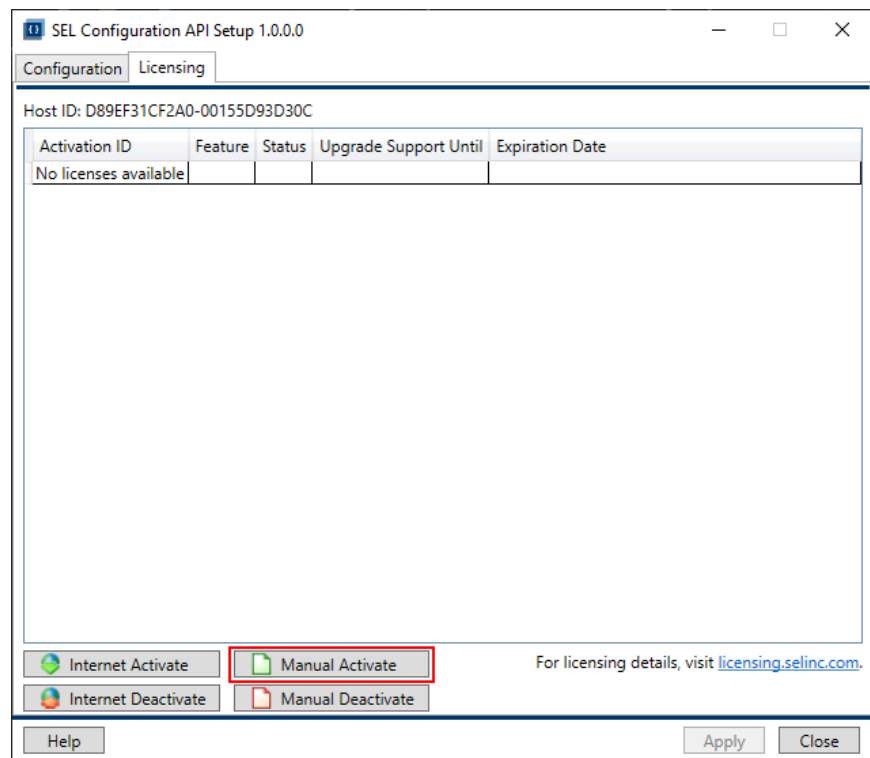Step 3.   From the Licensing tab, select **Manual Activate**.

Figure 11   Manual Activate

Step 4.   From the Manual Activate window, select **Generate Capability Request File**.
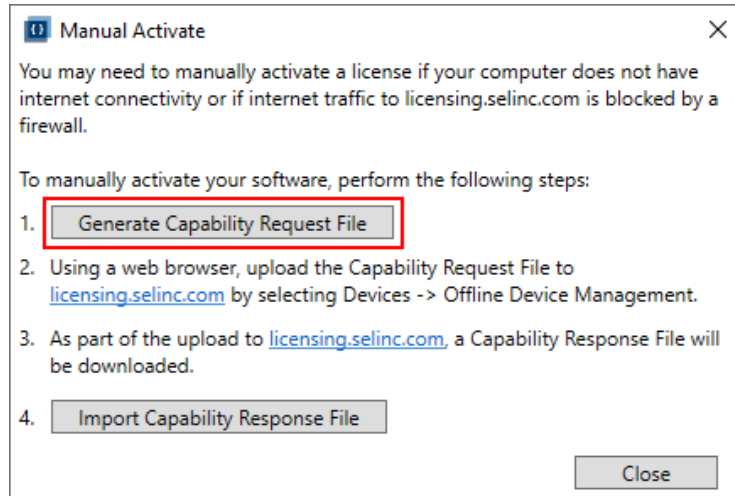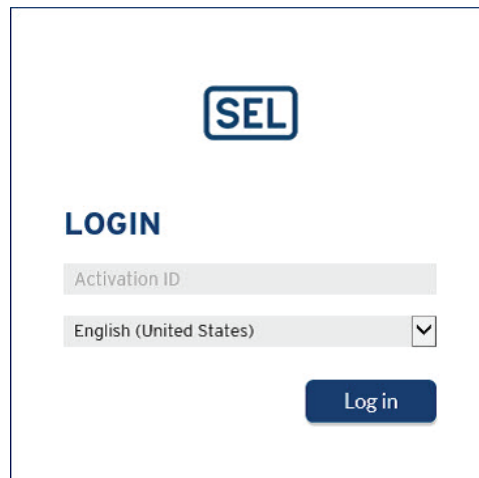

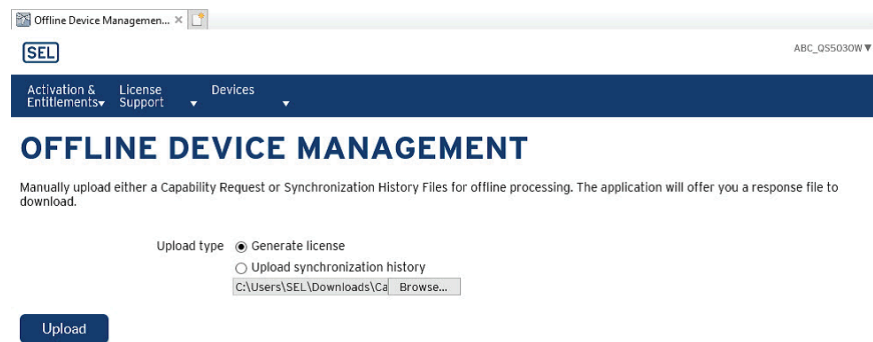**Figure 12   Generate Capability Request File for Manual Activation**

Step 5.   Save the Capability Request File to a thumb drive or a network drive that can be accessed by a separate computer that has internet access, or email the Capability Request File to SEL.

Step 6.   At the Enter Activation ID prompt, enter the Activation ID you received when you purchased your license and select **OK**.

Step 7.   Select **OK** on the confirmation message that indicates the file was successfully created.

Step 8.   From a computer that has internet access, go to licensing.selinc.com and log in with the Activation ID you are activating.

Figure 13   Log In With Activation ID
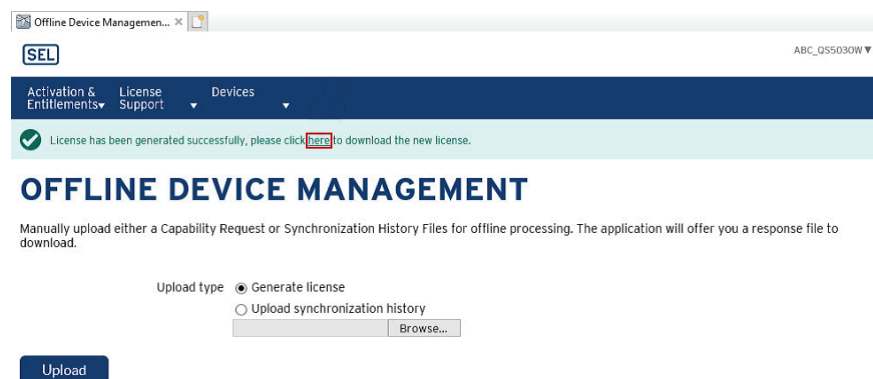
Step 9.   From the License & Delivery Portal page, select the **Devices** tab and select **Offline Device Management**.

Step 10.   From the Offline Device Management page, select **Browse** and the Capability Request File generated in *Step 4*.

Step 11.   Select **Upload**.

Figure 14   Upload Capability Request

Step 12.   Select the link highlighted in *Figure 15* to download the Capability Response File.

Figure 15   Link to Download Capability Response File

Step 13.   Select **Save**.

Do you want to open or save **capabilityResponse.bin** (4.75 KB) from **selinc.com**?   Open   Save   ▾   Cancel   ✕

Figure 16   Save the Request File

Step 14. With the Capability Response File saved in *Step 13*, return to the computer where the SEL Configuration API license is being activated.

Step 15. From the Manual Activate form, select **Import Capability Response File**.
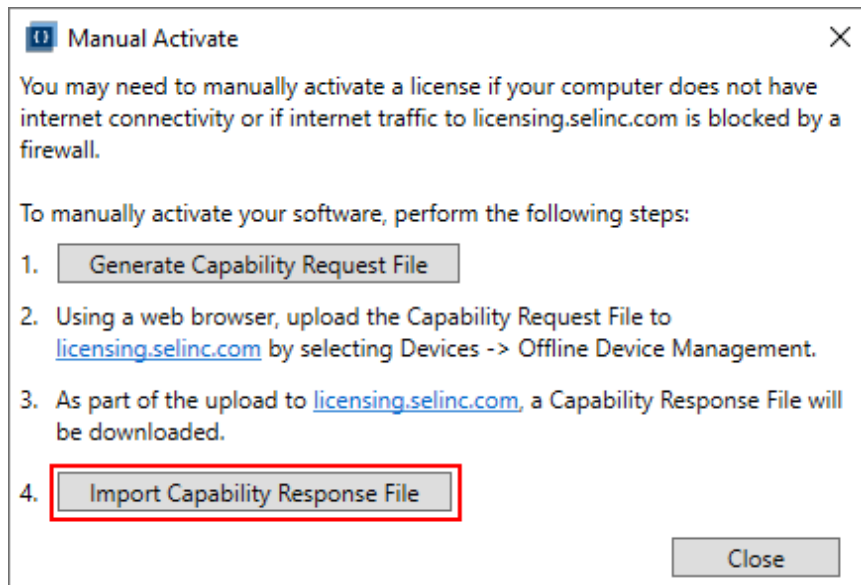
Figure 17   Import Capability Response File

Step 16. Navigate to the location of the Capability Response File created in *Step 13* and select **Open**.

Step 17. Select **OK** on the confirmation message that indicates the file was successfully imported.
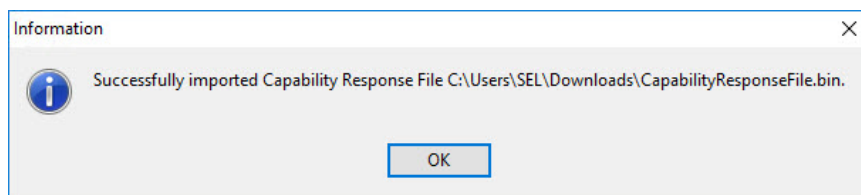
Figure 18   Confirmation Message

Step 18. Select **Close** on the Manual Activate form. The License Information screen now displays the activated license for SEL Configuration API.
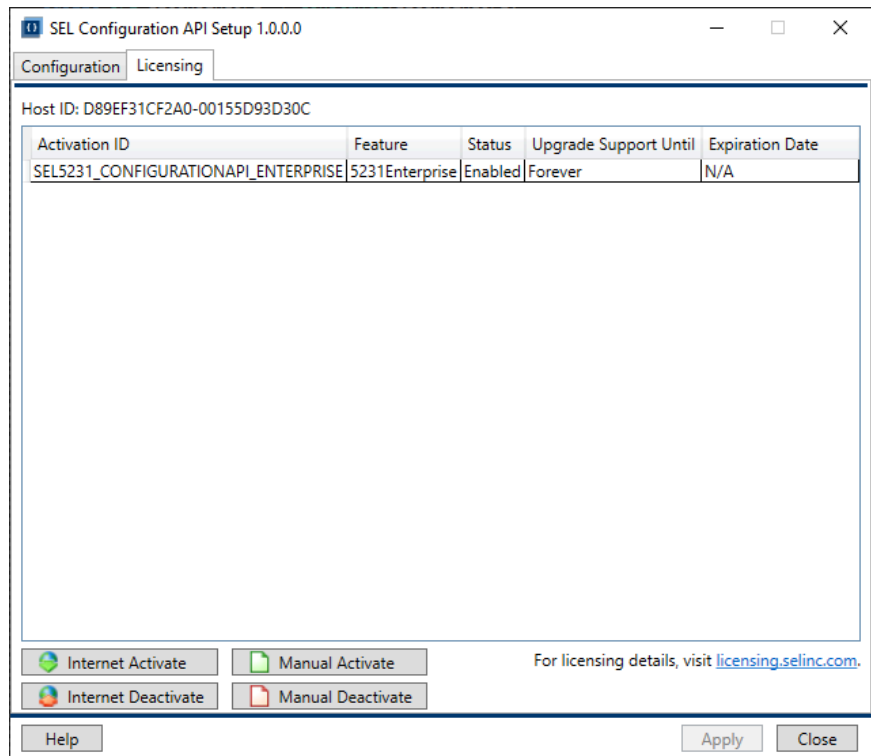
Figure 19   Activated License

Step 19. Select **Close**.

Manual Deactivate

Step 1.   Open the SEL Configuration API Setup utility.

Step 2.   Select the **Licensing** tab.

Step 3.   From the Licensing tab, select **Manual Deactivate**.
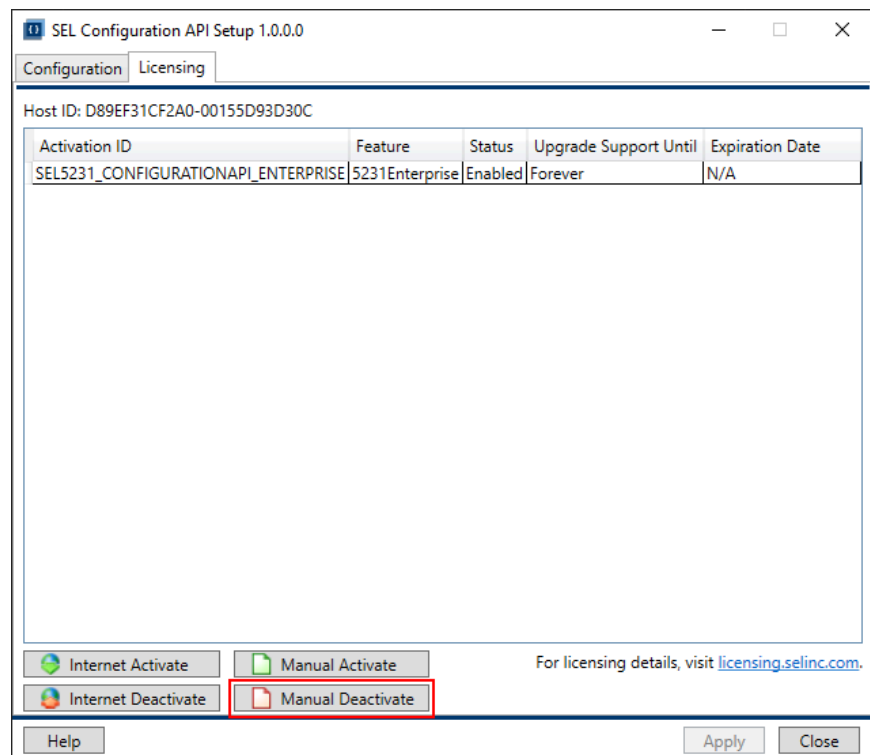
Figure 20   Manual Deactivate

> Step 4. From the Manual Deactivate screen, select **Generate Capability Request File**.
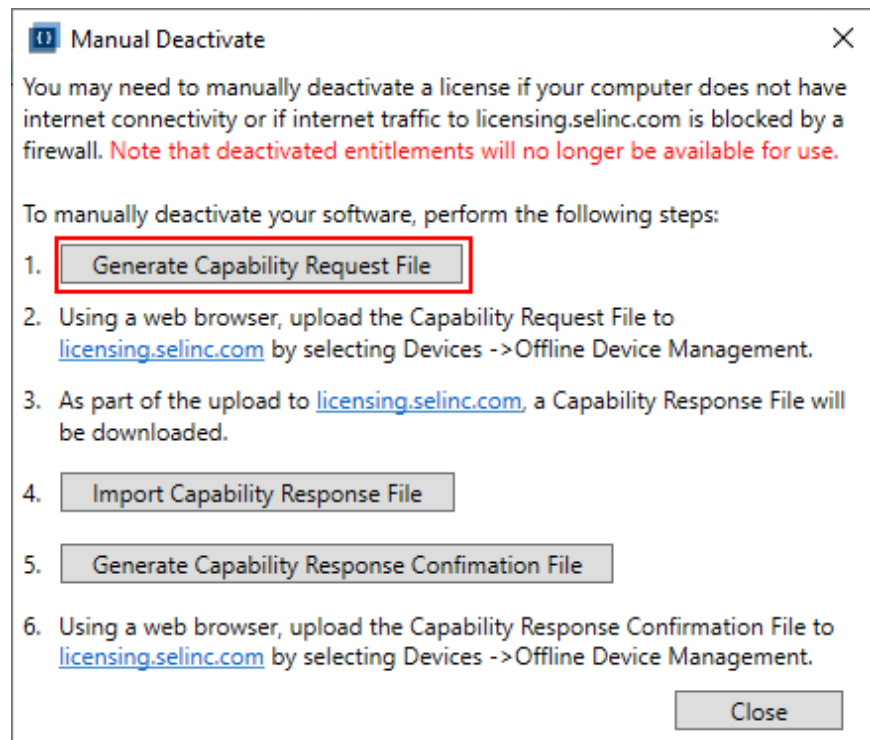
Figure 21   Generate Capability Request File for Manual Deactivation

Step 5.   Save the Capability Request File to a thumb drive or a network drive that can be accessed by a separate computer that has internet access, or email the Capability Request File to SEL.

Step 6.   Verify that the value populated in the Enter Activation ID window is the Activation ID that you intend to deactivate. Select **OK**.

Step 7.   Select **OK** on the confirmation message that indicates the file was successfully created.

Step 8.   From a computer that has internet access, go to https://licensing.selinc.com and sign in with the Activation ID you are deactivating.

Step 9.   From the License & Delivery Portal page, select the **Devices** tab and select **Offline Device Management**.

Step 10.   From the Upload Capability Request page, select **Browse** and select the Capability Request File generated in *Step 4*. Select **Upload**.

Step 11.   Select the link highlighted in *Figure 22* to download the Capability Response file.
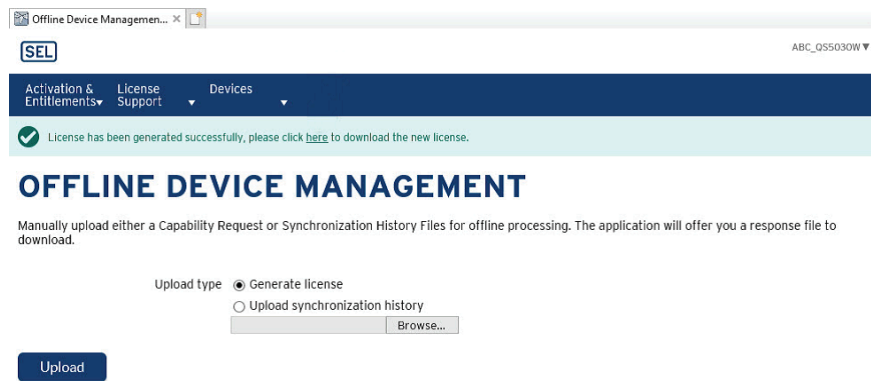
Figure 22   Link to Download Capability Response File

Step 12.   Select **Save** on the message similar to *Figure 23*.

**Figure 23   Save the Capability Request File**

Step 13.   With the Capability Response File saved in *Step 12*, return to the computer where the SEL Configuration API license is being deactivated.

Step 14.   From the Manual Deactivate form, select **Import Capability Response File**.
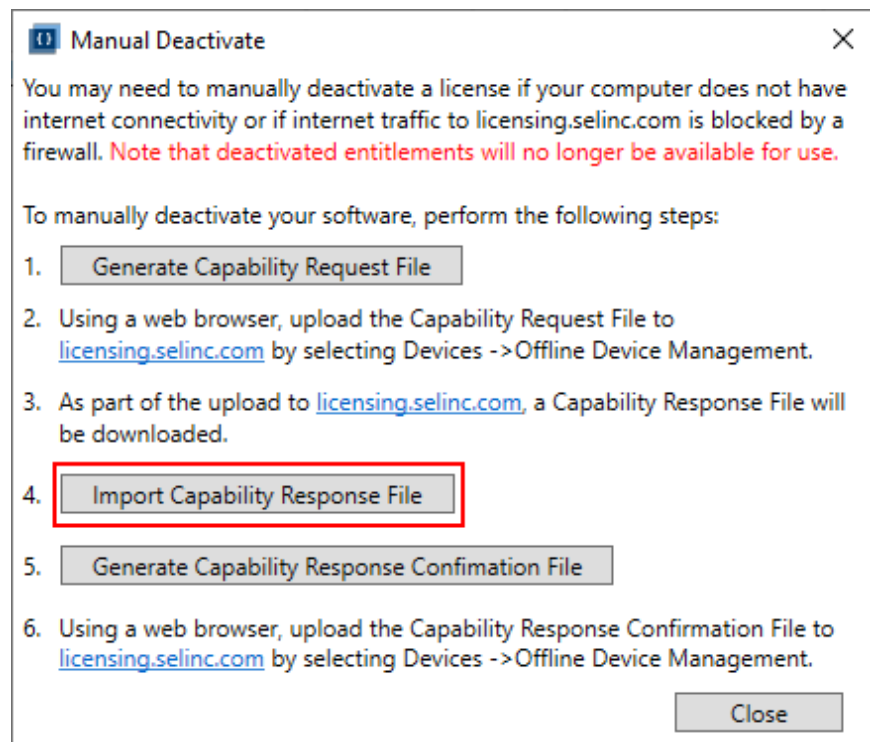
Figure 24   Import Capability Response File

Step 15. Browse to the location of the Capability Response File created in *Step 12* and select **Open**.

Step 16. Select **OK** on the confirmation message that indicates the file was successfully imported.

Step 17. From the Manual Deactivate screen, select **Generate Capability Response Confirmation File**.
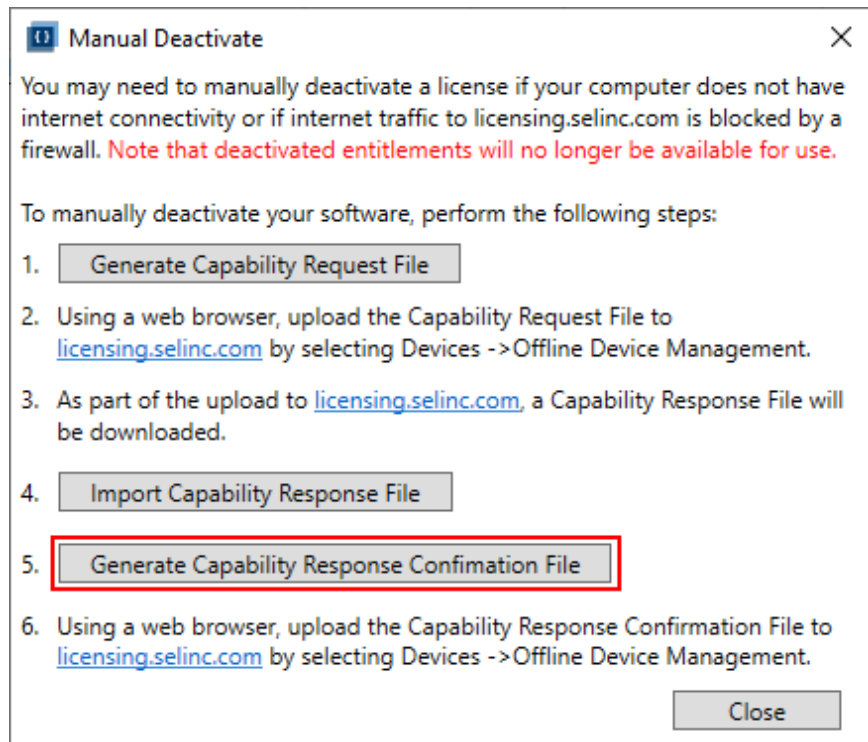
Figure 25   Generate Capability Response Confirmation File

Step 18. Provide a name and location for the Capability Response Confirmation File and select **Save**.

Step 19. Select **OK** on the confirmation message that indicates the file was successfully created. Do not close the Manual Deactivate form.

Step 20. From a computer that has internet access, go to *licensing.selinc.com* and log in with the Activation ID you are deactivating.

Step 21. From the License & Delivery Portal page, select the **Devices** tab and select **Offline Device Management**.

Step 22. From the Upload Capability Request page, select **Browse**, select the Capability Response Confirmation File generated in *Step 18*, and select **Upload**. After you upload the confirmation file, the FlexNet software generates another response file. This additional response file is not required and does not need to be downloaded.

Step 23. Select **Close** on the Manual Deactivate form. The Activation ID that was deactivated no longer shows in the License Information screen.
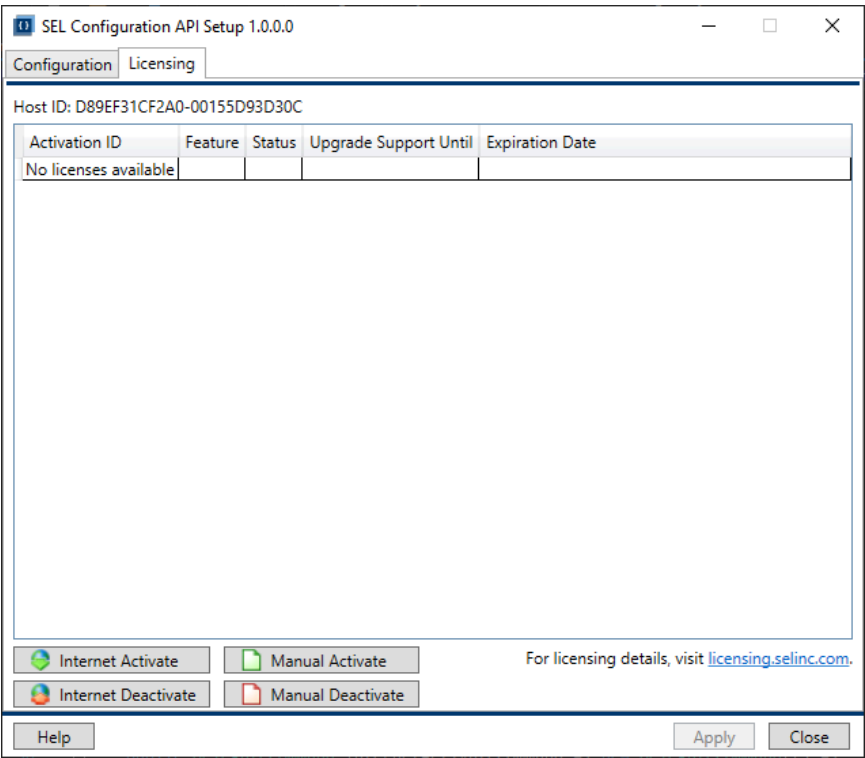
Figure 26   Deactivated Activation ID

Step 24. Select **Close**.

Appendix A: Software and Manual Versions

Software

The date code at the bottom of each page of this manual reflects the creation or revision date.

Table 1 lists the software versions, description of modifications, and the date code corresponding to the software version. The table lists the most recent software version first.

Descriptions marked as "[Breaking]" require an API client to be updated to maintain related API capabilities because the previous functionality has been altered or removed. A breaking change will always result in an incremented major version number.

Starting with revisions published after March 1, 2022, changes that address security vulnerabilities are marked with "[Cybersecurity]". Other improvements to cybersecurity functionality that should be evaluated for potential cybersecurity importance are marked with "[Cybersecurity Enhancement]".

Table 1   Software Revision History

Software Version Number	Summary of Revisions	Manual Date Code
3.4.x.x	➤ Increased the maximum database size supported by database backup and restore operations.	20250205
3.3.x.x	➤ [Cybersecurity Enhancement] Updated third-party components to ensure continuity of support.	20240807

Software Version Number	Summary of Revisions	Manual Date Code
3.2.x.x	➤ Added support for folder type operations.	20240605
3.1.x.x	➤ [Cybersecurity] Addressed a security vulnerability that could allow an authenticated attacker to execute arbitrary code when the computer starts. ➤ Addressed an issue in which certain licensing failures could prevent unlicensed application functionality.	20231222
3.0.x.x	➤ [Cybersecurity] Addressed an issue in which the script resources could be managed by users without the "Manage script" permission. ➤ [Cybersecurity] Addressed an issue in which device password values could be included in event logs under some configurations. ➤ [Cybersecurity] Addressed an input data validation issue in the asset node clone operation. ➤ [Cybersecurity Enhancement] Addressed an issue in which login bearer tokens would not recognize permission changes to the user made after the token's creation. ➤ [Cybersecurity Enhancement], [Breaking] User Permission "SCA Access" added. API endpoint access will now require "SCA Access" user permission instead of "Log on" user permission. Note that existing users with "Log on" permissions will automatically have "SCA Access" after upgrading. ➤ [Breaking] Changed value "name" to "username" on the UserDto type. ➤ [Breaking] The OpenApiGet endpoint now defaults output to the OpenApi 3.0.1 specification. ➤ [Breaking] WorkflowGetDto now returns a single WorkflowDto instead of a list. Additionally, the WorkflowDto field "id" has been removed. ➤ Added support for user and group management operations. ➤ Added support for device and folder document operations. ➤ Added support for device and folder custom attribute operations. ➤ Added support for device application operations. ➤ Added support for device firmware backup record operations. ➤ Added support for modifying device setting version metadata. ➤ Added support for titled password read operations. ➤ Added support for import and export endpoint variants to communicate data as a byte stream for improved communication for potentially large amounts of data. ➤ Added support for modifying application LDAP configuration. ➤ Added support for additional settings workflow operations. ➤ Asset Node Import and Merge operations will now return a ResourceChangeRecord for device configuration working copies added or modified by the operation.	20230925
2.4.x.x	➤ [Cybersecurity] Addressed an elevation of privilege vulnerability when installed with SEL-5037 Grid Configurator Admin install.	20230328
2.3.x.x	➤ Improved performance of the GetDeviceList endpoint. ➤ [Cybersecurity Enhancement] Updated to support PostgreSQL version 14.5. ➤ [Cybersecurity Enhancement] Added *Appendix B: Cybersecurity Features*.	20221107
2.2.x.x	➤ [Cybersecurity] Improved security of stored data by encryption using a unique key generated when the database is installed. ➤ [Cybersecurity] Added the ability to provide a password for database backup and restore operations. ➤ [Cybersecurity] Updated the installer to protect against maliciously placed files.	20220628
2.1.x.x	➤ Addressed an infrequent timing issue that could cause multiple simultaneous LDAP authentication requests to fail.	20220314

Software Version Number	Summary of Revisions	Manual Date Code
2.0.x.x	➤ [Breaking] Updated the "svn" integer parameter for operations that write device settings to the API. The parameter has been replaced with a new "settings_version" string parameter. The provided value will still be ignored for a value retrieved from settings content for most SEL devices. ➤ Added new API operations to handle device settings as raw byte content. ➤ Added support for settings management of non-SEL provided and third-party device types. ➤ Adjusted the Asset Node Export operation to give settings working copy data as raw byte content. ➤ Added additional validation to device settings data provided to the API. ➤ Increased maximum allowed request size from 30 MB to 500 MB. ➤ Increased timeout on application start to connect to the ACSELERATOR Database. ➤ Addressed an issue preventing the import of GE device types. ➤ Addressed an issue where settings groups or files could be incorrectly named when saving and returning settings. ➤ Adjusted necessary permissions required for database backup configuration operations.	20211029
1.4.x.x	➤ Added support for changing the device type of an existing device. ➤ Added the device type of the settings to the data returned when obtaining device settings from the API. ➤ Added a PowerShell coding example for retrieving support data from the API. ➤ Deprecated the SVN parameter from operations for writing device settings to the API. The SVN is now retrieved from the settings content. An SVN value may still be provided when executing these operations but that value will be ignored. ➤ Addressed an issue where the introduction section was missing from the API documentation.	20210716
1.3.x.x	➤ Added database backup and restore operations. ➤ Added to audited operation responses a changed attributes property that provides a list of properties that changed. ➤ Added support for obtaining and setting device password scripts. ➤ Added enable_radius_authentication and who_are_you_response to the device nameplate properties. ➤ Added a custom OpenAPI endpoint for improved compatibility with some code generation tools. ➤ Added script management operations. ➤ Added support for obtaining user account information. ➤ Added support for obtaining workflow information.	20201218
1.2.x.x	➤ Added support for Windows Server 2012 and Windows Server 2019. ➤ Added Audit API operations that allow access to a record of certain resource changes made over time. ➤ Added IsManaged and InService to the Device nameplate properties. ➤ Addressed an issue where the API returned null instead of an empty string for some Asset Node, Device, and Settings-related properties with no value. ➤ Addressed an issue where Asset Node deletions using the API were not being reflected in the Device Manager Connection Explorer. ➤ Addressed an issue with processing that could allow unauthorized access to the API.	20200922

Software Version Number	Summary of Revisions	Manual Date Code
1.1.x.x	➤ Added read-only access to the custom attributes of devices and folders. ➤ Added the Asset Node Merge operation that updates existing assets and adds missing assets from an asset inventory. ➤ Added support for managing device permissions. The Right Post operation grants a specific device permission to a user group. The Rights Delete operation revokes a set of device permissions. ➤ Added support for using HTTPS local host connections without requiring a license entitlement. ➤ Added the ability to use the internet to activate licenses. ➤ Corrected an issue where passing a null value as a device password should have resulted in the password not being changed but instead resulted in setting the password to an empty string.	20200127
1.0.x.x	➤ Initial version.	20190906

Instruction Manual

The date code at the bottom of each page of this manual reflects the creation or revision date.

Table 2 lists the instruction manual versions and revision descriptions. The most recent instruction manual version is listed first.

Table 2   Instruction Manual Revision History

Date Code	Summary of Revisions
20250205	➤ Updated for software version 3.4.x.x.
20240807	➤ Updated for software version 3.3.x.x.
20240605	➤ Updated for software version 3.2.x.x.
20231222	➤ [Cybersecurity] Updated for software version 3.1.x.x.
20230925	➤ Updated for software version 3.0.x.x.
20230328	➤ Updated for software version 2.4.x.x.
20221107	➤ Updated for software version 2.3.x.x. ➤ Added *Appendix B: Cybersecurity Features*.
20220628	➤ Updated for software version 2.2.x.x.
20220314	➤ Updated for software version 2.1.x.x.
20211112	➤ Updated for software version 2.0.x.x.
20210716	➤ Updated for software version 1.4.x.x.
20201218	➤ Added support for SEL Configuration API script and user account operations in *SEL Configuration API*. ➤ Updated for software version 1.3.x.x.
20200922	➤ Updated *API Accessibility*. ➤ Updated for software version 1.2.x.x.
20200127	➤ Updated for software version 1.1.x.x.
20190906	➤ Initial version.

Appendix B: Cybersecurity Features

Introduction and Security Environment

The SEL Configuration API is designed to run within regularly patched operating systems with strong user accounts and firewalls enabled. No internet connection is required to use the SEL Configuration API.

Version Information

To identify the currently installed version, use the SEL Configuration API **GET sca/service_information** endpoint. *Appendix A: Software and Manual Versions on page 18* contains a list of the SEL Configuration API releases and descriptions of each software update.

Commissioning and Decommissioning

Commissioning

The SEL Configuration API uses the following characteristics during installation to configure its operation.

Installation Characteristics

Data Protection

The ACSELERATOR Database backups generated by the SEL Configuration API are encrypted by using AES-256 encryption. See *Backup and Restore on page 23* for additional information.

Accounts

The SEL Configuration API uses the ACSELERATOR Database, a PostgreSQL database for storing device settings and other device information created by other SEL software products. *Table 3* lists the default user accounts by which the SEL Configuration API gains access to the database.

Table 3   PostgreSQL User Accounts

User Account	Password
dm_engineer	Generated randomly at install time
sel_pgsql	Generated randomly at install time

Privilege Level

Administrative privilege is required to install the SEL Configuration API.

Decommissioning

If you are removing a computer from service or no longer require the SEL Configuration API, you can uninstall the application. After you uninstall it, your system will retain some application metadata and settings at C:\ProgramData \SEL\SCA. Delete this folder if you want to completely remove all traces of the application.

Access Controls

The SEL Configuration API uses TLS with X.509 certificates to protect communications with the ACSELERATOR Database.

The SEL Configuration API uses SHA-256 for signature generation and RSA with a key size of at least 2048 bits.

The SEL Configuration API supports using TLS with an X.509 certificate to communicate with its clients if configured as such.

Logging Features

The SEL Configuration API installer generates logs at C:\ProgramData\SEL\SCA\Install. The SEL Configuration API service generates logs at C:\ProgramData\SEL\SCA\Service.

These logs contain operation information for the SEL Configuration API. You can view these log files with any text editor program. The availability of free space on your hard drive limits the size of these logs.

Backup and Restore

The SEL Configuration API supports creating backups of the ACSELERATOR Database that are interoperable with QuickSet.

The SEL Configuration API can restore the ACSELERATOR Database backups generated by the SEL Configuration API or by QuickSet.

The ACSELERATOR Database backups generated by the SEL Configuration API are encrypted by using AES-256 encryption.

Consult the API Programmer's Reference for further details on usage of this feature.

Product Updates

Appendix A: Software and Manual Versions on page 18 contains a list of the SEL Configuration API releases and descriptions of each software update. Software updates that affect cybersecurity are marked with "[Cybersecurity]" if they address a security vulnerability or with "[Cybersecurity Enhancement]" for other security improvements.

Update Verification

The SEL Configuration API installer is signed by SEL. For instructions on how to verify the signature, see *selinc.com/company/verifying-software-downloads/*.

Contact SEL

For further questions or concerns about product security, contact SEL at security@selinc.com or +1.509.332.1890.

Technical Support

We appreciate your interest in SEL products and services. If you have questions or comments, please contact us at:

Schweitzer Engineering Laboratories, Inc.
2350 NE Hopkins Court
Pullman, WA 99163-5603 U.S.A.
Tel: +1.509.338.3838
Fax: +1.509.332.7990
Internet: selinc.com/support
Email: info@selinc.com