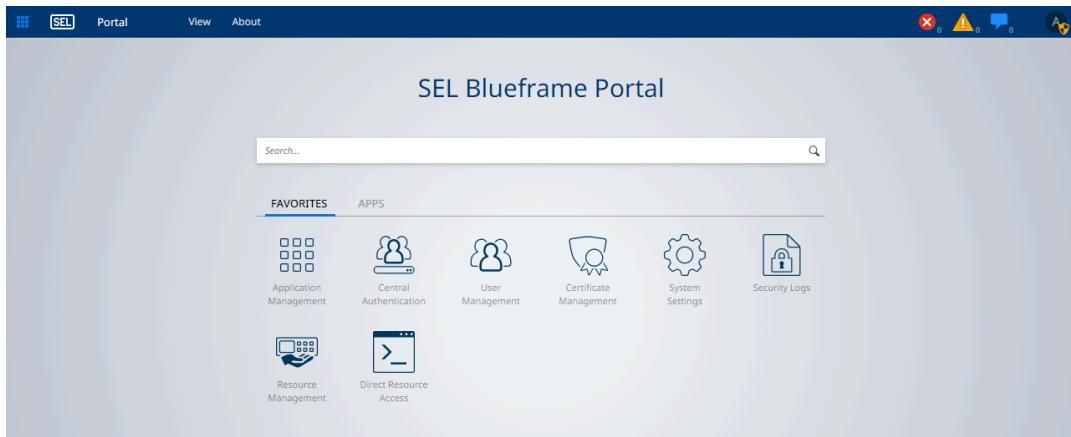


# SEL Blueframe Software

## Application Platform

### Instruction Manual



20250212

© 2021–2025 Schweitzer Engineering Laboratories, Inc. All rights reserved.

Content subject to change without notice. Unless otherwise agreed in writing, all SEL product sales are subject to SEL's terms and conditions located here: <https://selinc.com/termsandconditions/>.

# Table of Contents

## Section 1: Blueframe Overview

What Is Blueframe?.....	11
Supported Hardware.....	11
Initializing and Installing Blueframe.....	12
Blueframe Portal.....	13
Blueframe Operating System.....	19
Troubleshooting.....	20

## Section 2: Blueframe Management Tools

System Settings.....	23
Redundancy.....	37
User Management.....	39
Certificate Management.....	49
Central Authentication.....	62
Notifications.....	71

## Section 3: Resource Management

Overview.....	75
---------------	----

## Section 4: Direct Resource Access

Quick Connect.....	101
--------------------	-----

## Section 5: Protocol Services

Overview.....	103
Adding a Protocol Service.....	103
Configuring a Service.....	104
Protocol Services Toolbar.....	106
Communications Diagnostics.....	107
DNP3.....	107

## Section 6: Data Viewer

## Section 7: Resource Viewer

Overview.....	119
Resource Tree View.....	119
Resource Grid.....	119
Details Pane.....	119
Individual Resource View.....	120

## Section 8: Application Management

Application Packages.....	121
Application Licensing.....	126

## Section 9: Logging

System Logs.....	127
------------------	-----

## Appendix A: Software and Manual Versions

Software.....	133
Instruction Manual.....	145

## Appendix B: Cybersecurity Features

Security Environment.....	151
Version Information.....	151
Installation Characteristics.....	152
Ports and Services.....	152
Access Control.....	152
Backup and Restore.....	154
Decommissioning.....	154
Malware Protection Features.....	154
Revision Management.....	154
Contact SEL.....	154

## Glossary

# List of Figures

Figure 1.1 Blueframe System Architecture.....	11
Figure 1.2 Blueframe Welcome Screen.....	12
Figure 1.3 Blueframe Portal.....	13
Figure 1.4 Blueframe Application Bar.....	13
Figure 1.5 Blueframe Application Launcher.....	14
Figure 1.6 Portal Application Bar Menus.....	14
Figure 1.7 About Blueframe.....	15
Figure 1.8 Blueframe Toast Notification.....	15
Figure 1.9 Error, Warning, and Information Panes.....	16
Figure 1.10 Blueframe User Profile Badge.....	16
Figure 1.11 User Profile Badge Preferences.....	17
Figure 1.12 Blueframe Dark and Light Theme.....	18
Figure 1.13 Portal Applications Tab.....	18
Figure 1.14 Adding an Application to Favorites.....	19
Figure 1.15 Linux Applications Menu.....	19
Figure 1.16 Display Settings.....	20
Figure 2.1 System Settings Icon.....	23
Figure 2.2 System Settings Status Menu.....	24
Figure 2.3 POST Summary, System Alarms, and Time Synchronization Status.....	24
Figure 2.4 System Settings Page.....	25
Figure 2.5 General Device Settings.....	25
Figure 2.6 Device Date & Time Settings.....	26
Figure 2.7 Time Synchronization Options.....	26
Figure 2.8 Network Interfaces.....	27
Figure 2.9 Network Interface Details.....	28
Figure 2.10 New Host Menu.....	30
Figure 2.11 Configuring the Internal Network Address Space.....	31
Figure 2.12 Blueframe Device Settings.....	31
Figure 2.13 Firmware Upgrade Menu.....	32
Figure 2.14 Backup & Restore Menu.....	32
Figure 2.15 New Backup.....	33
Figure 2.16 Delete Backup.....	33
Figure 2.17 Download and Upload Backup Options.....	34
Figure 2.18 TPM Details.....	34
Figure 2.19 PRC Quotes.....	35
Figure 2.20 Application Package Licensing.....	36
Figure 2.21 Export Licenses.....	37
Figure 2.22 User Management Icon.....	39
Figure 2.23 User Management Users Menu.....	40
Figure 2.24 Create New User Menu.....	40
Figure 2.25 User Password Menu.....	41
Figure 2.26 Password Policies Configuration Menu.....	41
Figure 2.27 User Management Roles Menu.....	43
Figure 2.28 Adding a New Role.....	43
Figure 2.29 Creating a New Role Menu.....	44
Figure 2.30 Adding or Removing Role Members.....	45
Figure 2.31 Adding Users to a Role.....	46
Figure 2.32 User Management Application Bar Menus.....	46
Figure 2.33 User Management Import Data Menu.....	47
Figure 2.34 User Management Password Policies Menu.....	48

Figure 2.35 User Management Session Preferences Menu.....	48
Figure 2.36 Certificate Management Icon.....	49
Figure 2.37 Generate Certificate.....	50
Figure 2.38 Identity Information.....	50
Figure 2.39 Activating a Certificate.....	51
Figure 2.40 Privacy Error Message.....	52
Figure 2.41 Your Connection to This Site Isn't Secure Message.....	53
Figure 2.42 Certificate Details.....	54
Figure 2.43 Install Certificate.....	55
Figure 2.44 Certificate Store Selection Window.....	56
Figure 2.45 Exporting a CSR.....	57
Figure 2.46 Certificate Signing Request.....	57
Figure 2.47 Activating a Signed Certificate.....	58
Figure 2.48 Importing a New Certificate.....	59
Figure 2.49 Certificate Management CA Certificates Menu.....	60
Figure 2.50 Adding a Certificate Authority Certificate.....	60
Figure 2.51 Add Certificate Chain Window.....	61
Figure 2.52 CA Certificates Chain.....	61
Figure 2.53 Submitting a CA Certificate.....	62
Figure 2.54 Central Authentication Icon.....	62
Figure 2.55 LDAP Login Process.....	63
Figure 2.56 Central Authentication LDAP Settings.....	63
Figure 2.57 General LDAP Settings.....	64
Figure 2.58 Directory Access Authentication.....	65
Figure 2.59 LDAP Server Settings.....	65
Figure 2.60 User Attribute Maps.....	66
Figure 2.61 Central Authentication Group Maps.....	68
Figure 2.62 Adding an LDAP Group to a Role.....	68
Figure 2.63 Select LDAP Group.....	69
Figure 2.64 Submitting LDAP Group Changes.....	69
Figure 2.65 RADIUS Settings.....	70
Figure 2.66 Notifications Icon.....	71
Figure 2.67 Recipient Group Configuration.....	72
Figure 2.68 Recipient Groups.....	72
Figure 2.69 Define a New Recipient Group.....	73
Figure 3.1 Resource Management Icon.....	75
Figure 3.2 Resource Management Components.....	75
Figure 3.3 Dragging a Resource Into a Folder.....	76
Figure 3.4 Navigation Tree Folder Sorting.....	77
Figure 3.5 Resource Management Filters.....	77
Figure 3.6 Adding a New Resource.....	78
Figure 3.7 Defining a New Resource.....	79
Figure 3.8 Resource Overview.....	80
Figure 3.9 Connection Services.....	81
Figure 3.10 Child Resource Assignment.....	83
Figure 3.11 Ingress and Egress Up/Down Scripts.....	84
Figure 3.12 Resource Sessions.....	84
Figure 3.13 New Sessions Dialog.....	85
Figure 3.14 New Session With Allowlist or Denylist.....	85
Figure 3.15 Role Association.....	86
Figure 3.16 New Access List.....	87
Figure 3.17 Define an Access List Name and Description.....	87
Figure 3.18 Select Role(s) to Access Resources.....	88
Figure 3.19 Define the Resources for the Access List.....	88
Figure 3.20 Sample Access List Restricted View.....	89

Figure 3.21 Resource Management API Documentation.....	90
Figure 3.22 Profiles Creation Workspace.....	90
Figure 3.23 Create a New Profile.....	91
Figure 3.24 Example Profile Name and Description.....	91
Figure 3.25 Statically and Instance-Defined Attributes.....	92
Figure 3.26 Available Profiles.....	92
Figure 3.27 Profile Configuration Spaces.....	93
Figure 3.28 Resource Template.....	93
Figure 3.29 Profile Connection Template.....	94
Figure 3.30 Profile Service Template.....	95
Figure 3.31 Profile Session Template.....	96
Figure 3.32 Deploy Instances.....	97
Figure 3.33 Profile Instances in Resource Management.....	98
Figure 3.34 Instance Credentials.....	98
Figure 4.1 Connected Resources.....	99
Figure 4.2 Available Sessions.....	99
Figure 4.3 Execute a Command.....	100
Figure 4.4 Terminal Tools.....	100
Figure 4.5 Last Session Logs.....	100
Figure 4.6 Web Proxy Session.....	101
Figure 4.7 Quick Connect Option.....	101
Figure 4.8 Quick Connect Dialog.....	102
Figure 5.1 Initial Protocol Service Landing Page.....	104
Figure 5.2 New Client Dialog Field Descriptions.....	104
Figure 5.3 Configuring a New Client in Resource Management.....	105
Figure 5.4 Protocol Services Toolbar With a Draft Protocol Service.....	106
Figure 5.5 Diagnostics Tab for an Online Protocol Session.....	107
Figure 5.6 Adding Points to a Draft DNP3 Client Service.....	108
Figure 5.7 Configuring Data Point Maps in a DNP3 Server Service.....	109
Figure 6.1 Blueframe Data Viewer.....	117
Figure 8.1 Application Management Icon.....	121
Figure 8.2 Application Management Components.....	121
Figure 8.3 Uploading an Application Package.....	122
Figure 8.4 Importing an Application Package.....	122
Figure 8.5 Package State.....	123
Figure 8.6 Application Packages.....	123
Figure 8.7 Package Details—Install and Delete Actions.....	124
Figure 8.8 Uninstalling Warning.....	124
Figure 8.9 Package Details—Upgrade and Downgrade Actions.....	125
Figure 8.10 Delete Warning.....	125
Figure 8.11 Package Service.....	126
Figure 9.1 System Logs Icon.....	127
Figure 9.2 System Logs Overview.....	127
Figure 9.3 System Logs Filter Options.....	128
Figure 9.4 System Logs Application Bar Menus.....	128
Figure 9.5 Export Logs Menu.....	128
Figure 9.6 System Logs Permissions.....	129
Figure 9.7 System Logs Management Settings.....	130
Figure 9.8 System Logs File Menu.....	132
Figure 9.9 Configuration Dialog for Adding Syslog Server Destinations.....	132
Figure A.1 Blueframe Application Versions.....	133
Figure B.1 Blueframe Application Platform System Architecture.....	151

**This page intentionally left blank**

# List of Tables

Table 1.1 Blueframe Hardware Compatibility.....	12
Table 2.1 CIDR Notation.....	28
Table 2.2 LDAP Parameters.....	66
Table 2.3 RADIUS Settings in Blueframe.....	70
Table 3.1 Connection Protocol Options.....	81
Table 5.1 License Level for Data Point Tiers on SEL Embedded Computing Platforms.....	103
Table 5.2 Blueframe Data Point Types.....	106
Table 5.3 Server (Outstation).....	110
Table 5.4 DNP Server (Slave) Object.....	111
Table 5.5 DNP Client (Master) Object.....	113
Table 9.1 Syslog Message Severities Supported in the RTAC.....	131
Table 9.2 Syslog MSG Configuration Message Component Description.....	131
Table A.1 Blueframe Operating System and Hardware Services Package Version History.....	134
Table A.2 Blueframe Core Services Package Version History.....	138
Table A.3 Connection Services Package Version History.....	139
Table A.4 Blueframe Protocol Services Package Version History.....	143
Table A.5 Blueframe Data Viewer Package Version History.....	144
Table A.6 Blueframe Resource Viewer Package Version History.....	144
Table A.7 Instruction Manual Revision History.....	145

**This page intentionally left blank**

---

---

## S E C T I O N   1

---

# Blueframe Overview

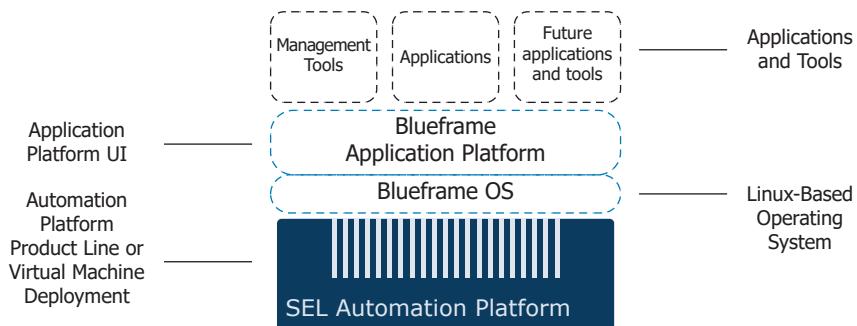
## What Is Blueframe?

---

Blueframe is an embedded, modular, and container-based application platform designed to operate in a secured environment. The modular design of Blueframe enables you to selectively choose the solution applications you want to install to support and solve your system needs. Blueframe Management Tools are included to support common Blueframe system configurations. The solution applications are optional and offered in various ways, from a single application to packages of applications that belong to suites designed to achieve a modular solution to an industrial problem.

The system employs a scheme of smart shared data throughout, so you enter information such as IEDs, connections, and users only once. Each application subscribes seamlessly to the data it needs, saving you configuration time and reducing the chance of introducing manual copy errors into the system.

The Blueframe ecosystem, as shown in *Figure 1.1*, consists of a hardware layer supported by the Automation Platform or a virtual environment with a subscription contract. On top of the hardware layer rests a secured Linux-based operating system that is designed to minimize exposure to attack and which employs security measures, such as allowlisting, to prevent unauthorized access and attacks. Lastly, the Blueframe application platform and its applications rest on top of the Linux operating system and use application containerization. You can access all system applications and tools through a secure web-based environment.



**Figure 1.1** Blueframe System Architecture

## Supported Hardware

---

The Blueframe environment supports devices from the Automation Platforms product line. These devices include the SEL-3350, SEL-3355, SEL-3360E, and SEL-3360S.

Blueframe can also be deployed in a virtual environment for enterprise implementations. The minimum processing, memory, and storage requirements for a Blueframe machine depend entirely on the applications and tasks being performed by the machine. In order to deploy Blueframe virtually, you must enter a subscription contract with SEL. Contact us for any questions related to virtual machine implementations or ordering for a subscription service.

**Table 1.1 Blueframe Hardware Compatibility**

Device Name	Blueframe Support
SEL-3350	•
SEL-3355-2	•
SEL-3360	•
Virtual Deployment	•

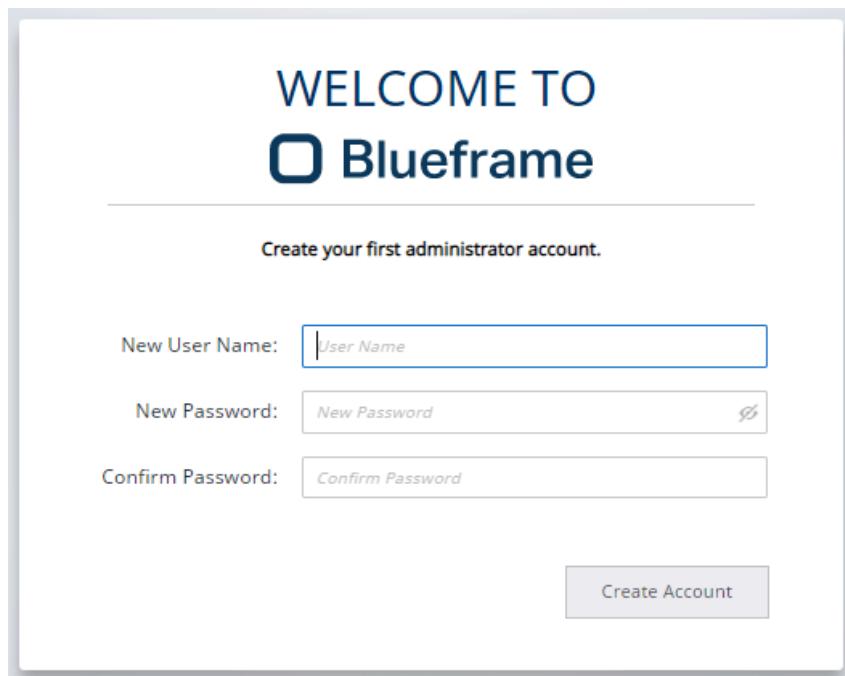
## Initializing and Installing Blueframe

---

Blueframe comes pre-installed with the Blueframe operating system and management tools, and any additionally selected application packages are also installed and licensed (where necessary). Blueframe ships without default user accounts; when you start the platform for the first time, you must create an initial administrator user account on the welcome screen that displays.

### Welcome Screen

After you initiate the startup sequence for the platform, Blueframe displays a welcome screen and prompts you to create a user. Blueframe assigns the initial user automatically to the administrator (admin) role, which provides you all the permissions necessary to create additional users and roles within the system.

**Figure 1.2 Blueframe Welcome Screen**

# Blueframe Portal

After you complete Blueframe initialization, the SEL Blueframe Portal displays, as shown in *Figure 1.3*. In the portal, you will find the Blueframe Management Tools that you can use to facilitate the definition of security parameters, users, data, and other management tools. *Section 2: Blueframe Management Tools* contains details about each tool.



**Figure 1.3** Blueframe Portal

## Application Bar

The Blueframe Application Bar contains the Application Launcher, Application Bar menus, information panes, and the User Profile badge. Certain items of the Application Bar, such as the Application Bar menus, are dynamic and change according to the application in use. Each Blueframe management tool section in the manual contains a description of its relevant menu items. For the Blueframe Portal, for example, the Application Bar menus offer the View and About menus.



**Figure 1.4** Blueframe Application Bar

## Application Launcher

The Application Launcher is an alternative way of navigating to your applications and management tools within Blueframe. It offers home and favorite navigation options as well as category and alphabetical sorting for applications. When you expand the Application Launcher, Blueframe selects the category sorting option by default and arranges contents within this option by management tools and suite applications.

Blueframe Management Tools are included with every installation of the Blueframe application platform. Additionally, when you purchase and install an application package, Blueframe stores the relevant applications under their suite name in the Application Launcher.

Select the blue box icon  to display the Application Launcher.

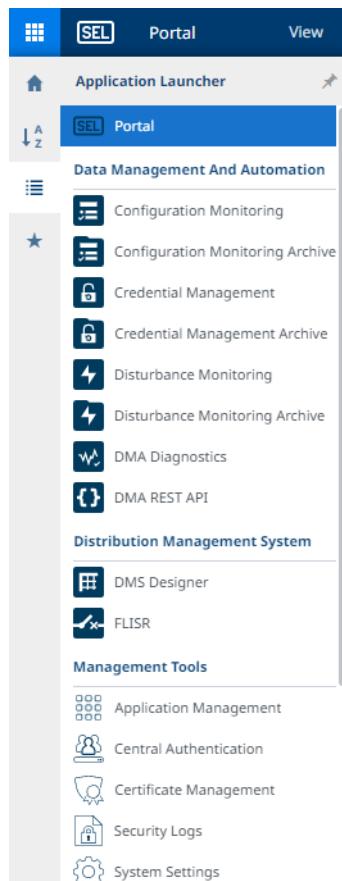


Figure 1.5 Blueframe Application Launcher

## Portal Application Bar Menus



Figure 1.6 Portal Application Bar Menus

**View:** Provides options for viewing either all applications or favorite applications. Also, use this menu for viewing notifications related to the portal.

**About:** Provides information about the Blueframe application platform and offers a link to the SEL Blueframe Getting Started webpage that contains support literature.

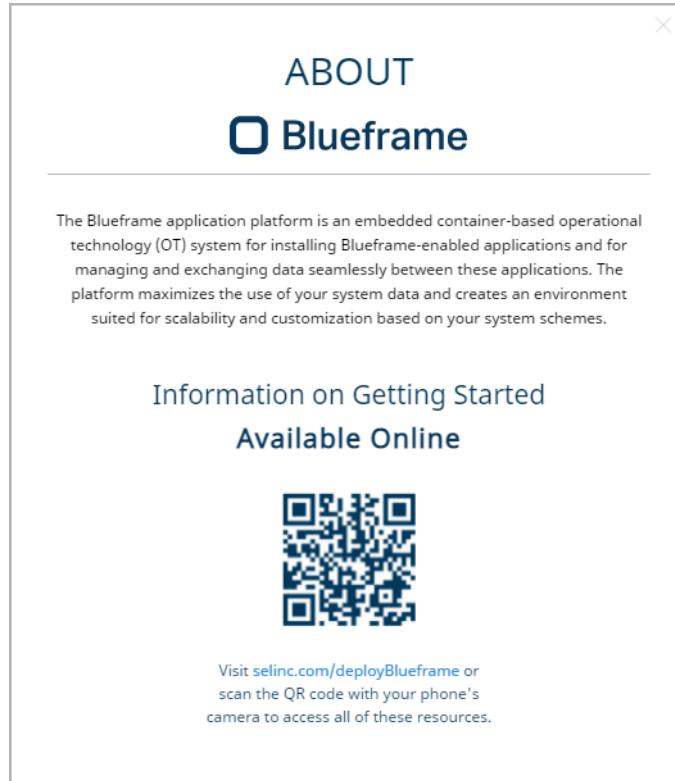


Figure 1.7 About Blueframe

## Error, Warning, and Information Panes

The information menu is a section of the user interface that displays errors, warnings, and information. As new events occur, you can view a momentary toast message on the right side of your browser window. As *Figure 1.8* and *Figure 1.9* show, the event information then displays within an error, warning, or information pane for your review.

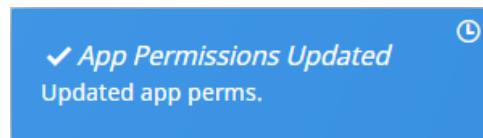


Figure 1.8 Blueframe Toast Notification

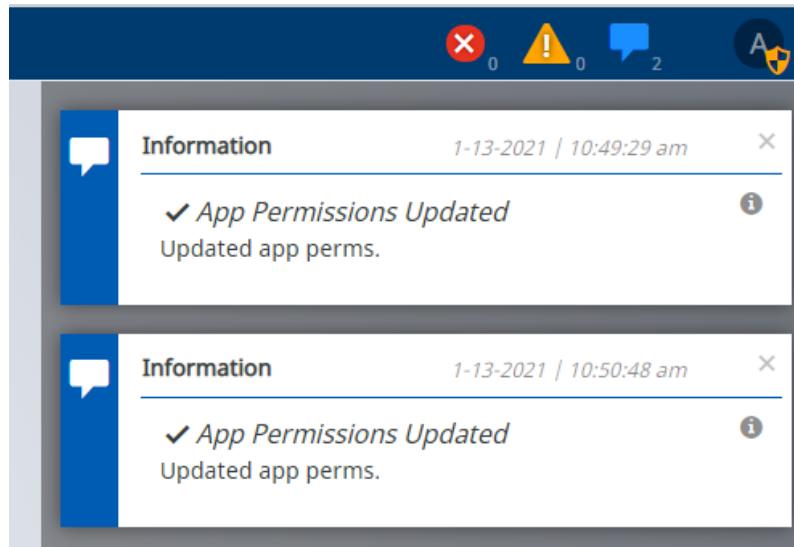


Figure 1.9 Error, Warning, and Information Panes

## User Profile Badge

The Application Bar contains a unique User Profile badge corresponding to the user logged into the Blueframe application platform. Expanding this menu provides you options, such as shown in *Figure 1.10* for customizing your Blueframe user preferences.

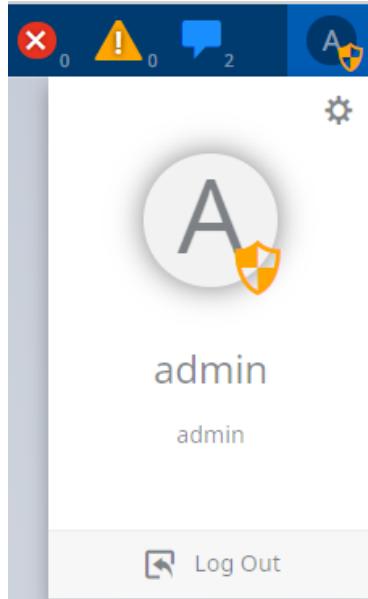
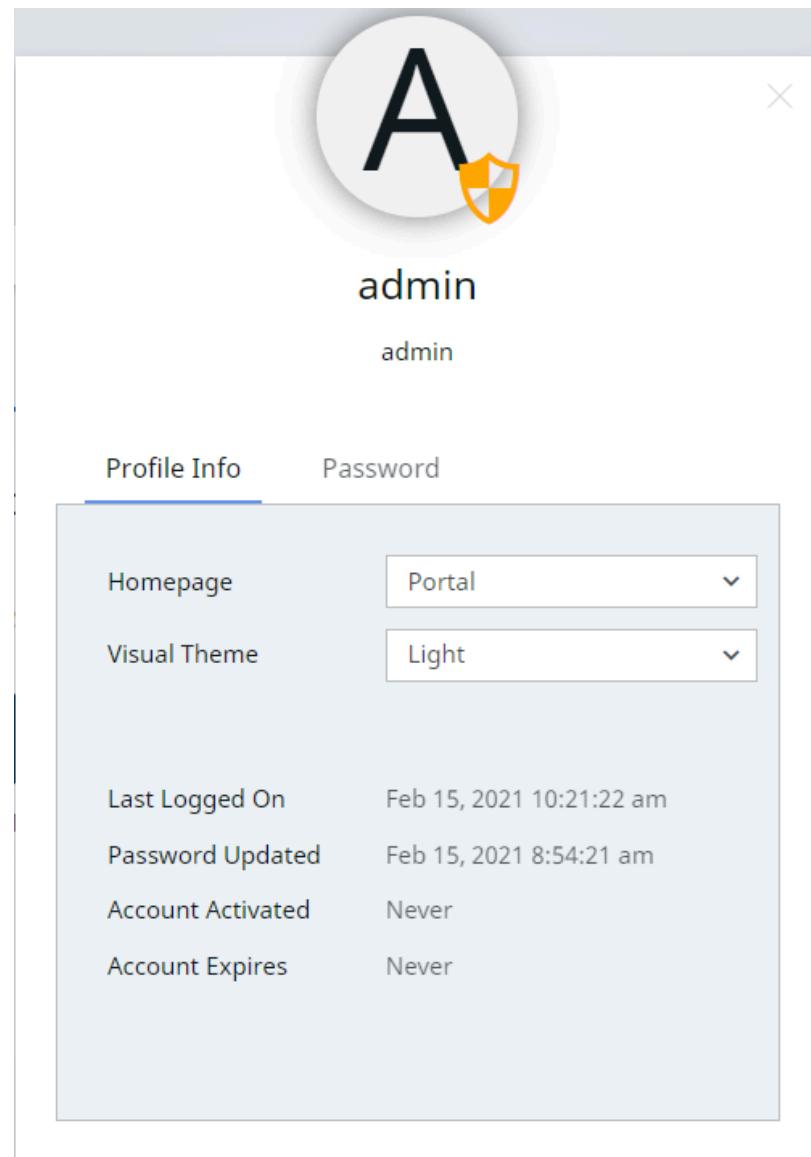


Figure 1.10 Blueframe User Profile Badge

From within the window shown in *Figure 1.10*, select to adjust user preferences such as the Homepage, Visual Theme, and password management. You can also view a brief description of your role memberships and an option to log out of the session (see *Figure 1.11*).



**Figure 1.11 User Profile Badge Preferences**

Your selection of the Homepage determines the landing page that displays when you log in to the system, and it also determines the page to which a user navigates when selecting the home icon from within the Application Launcher.

Your Visual Theme selection (of either Dark or Light) changes the overall look of the interface as shown in *Figure 1.12*.

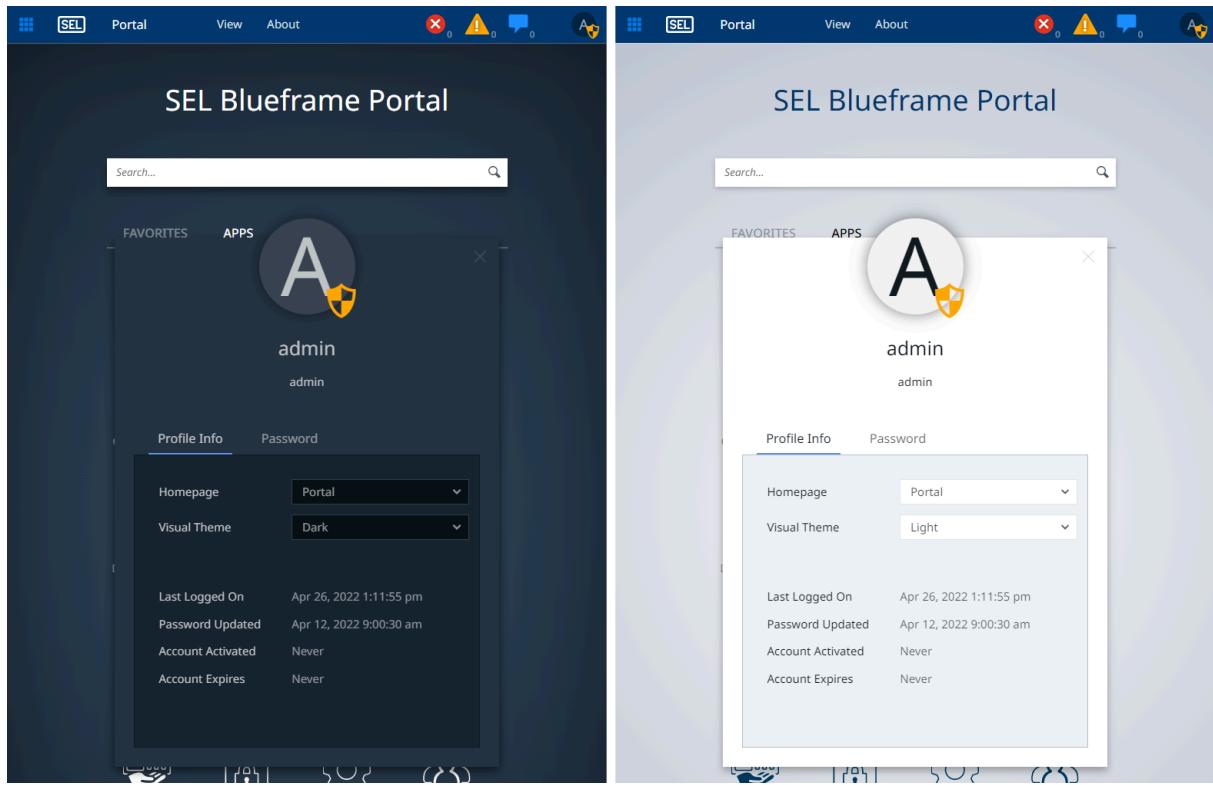


Figure 1.12 Blueframe Dark and Light Theme

The Password tab offers you the option to change your password. For more information on user password requirements, see *User Management on page 39*.

#### NOTE

You must provide your present password to change to a new password.

## Applications Tab

The Applications tab, as shown in *Figure 1.13*, shows an example of installed applications, including Blueframe Management Tools, as well as solution applications. Organize the icons as necessary by selecting and dragging an icon to the desired location.

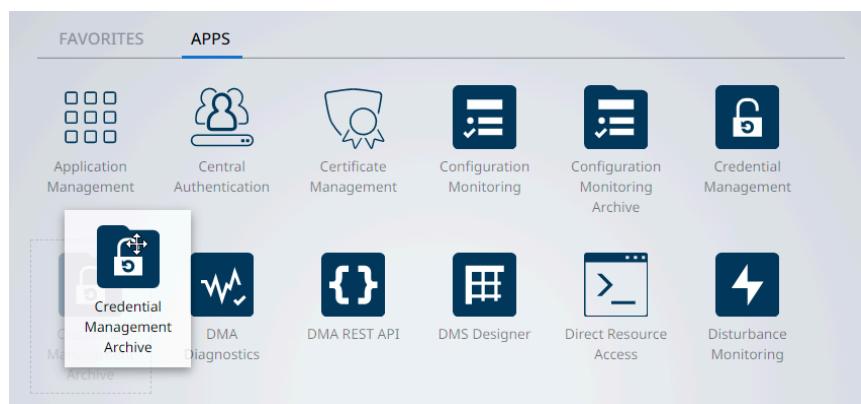


Figure 1.13 Portal Applications Tab

## Favorites Tab

The Favorites tab shown in *Figure 1.14* provides a set of application shortcuts on the Blueframe portal. This list is configurable, so you can add your most used or critical applications as you see fit. To add an application to the favorites list, right-click on the relevant application from the applications list and select **Add To Favorites** (see *Figure 1.14*).

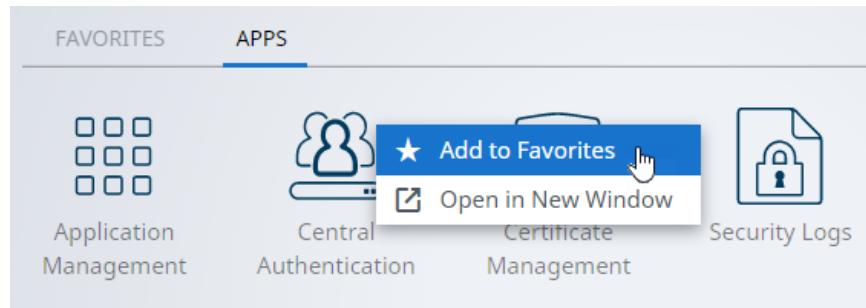


Figure 1.14 Adding an Application to Favorites

## Blueframe Operating System

---

The Blueframe application platform rests on the Blueframe operating system and serves as its main user interface. The Linux-based Blueframe operating system offers basic hardware settings, such as display configuration.

If you are using the local display of a Blueframe node, it is launched by default in Fullscreen mode. Press <F11> to toggle between Fullscreen and windowed mode and to see the underlying Linux operating system.

## Display Settings

The display settings will determine the resolution of the monitor connected to the Automation Platform. By default, connecting a monitor to the Automation Platform will cause the resolution to be automatically updated to the correct dimensions. You can also change the default settings, if desired (see *Figure 1.16*). Access the display settings by selecting **Applications > Settings > Display** (see *Figure 1.15*).

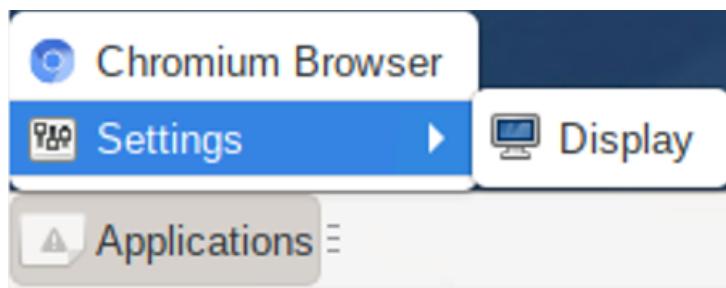


Figure 1.15 Linux Applications Menu

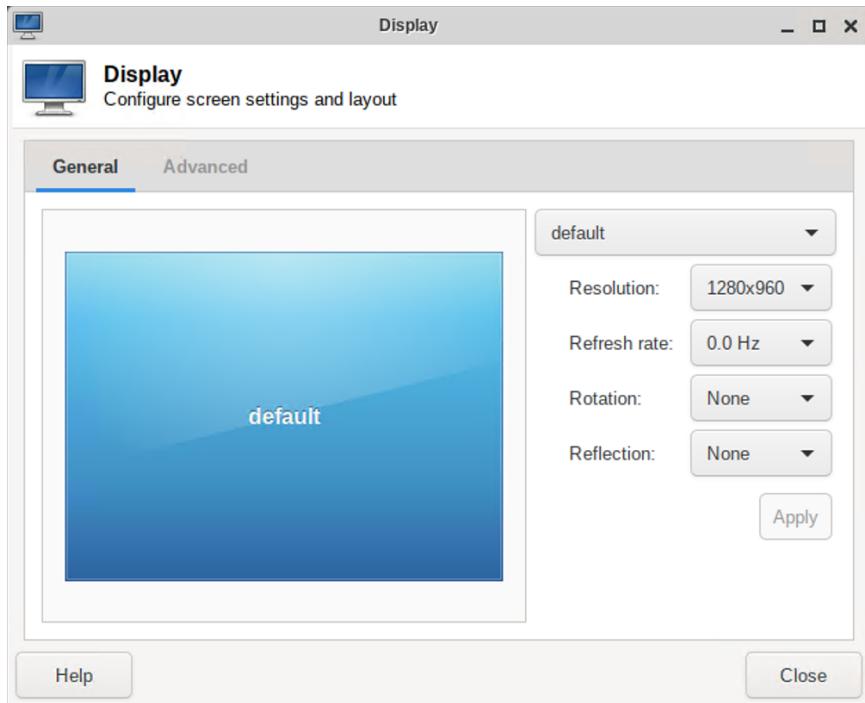


Figure 1.16 Display Settings

## Chromium Browser

The Applications menu also contains a Chromium Browser option to launch the Blueframe Portal (see *Figure 1.15*). Additionally, you can access other devices on your network that support a web interface through the Chromium browser, such as the RTAC.

## Troubleshooting

---

The Blueframe operating system provides a diagnostics console for advanced troubleshooting. The Blueframe Diagnostics user interface can be accessed via the local display by pressing **<Ctrl+Alt+F3>**. Pressing **<Ctrl+Alt+F2>** navigates back to the main Blueframe user interface. The diagnostic page is not available on remote web browser sessions.

The Diagnostics user interface allows a selection of non-modifying commands to be executed for the purpose of gathering information about running processes on a Blueframe device. To execute a command, enter the command in its entirety in the input box labeled "Command", then press **<Enter>** or select **Execute**. A list of supported commands and their descriptions are displayed if the command **help** is executed.

Commands supported in the Diagnostics user interface include:

- **cat**
- **cd**
- **df**
- **du**

- **help**
- **journalctl**
- **kubectl**
- **ls**
- **ps**
- **pwd**
- **top**

Additionally, executing the **kubectl** command is restricted to the use of the following sub-commands:

- **cluster-info**
- **describe**
- **get**
- **logs**
- **top**
- **version**

**This page intentionally left blank**

---

---

## S E C T I O N   2

---

# Blueframe Management Tools

## System Settings

---



**Figure 2.1 System Settings Icon**

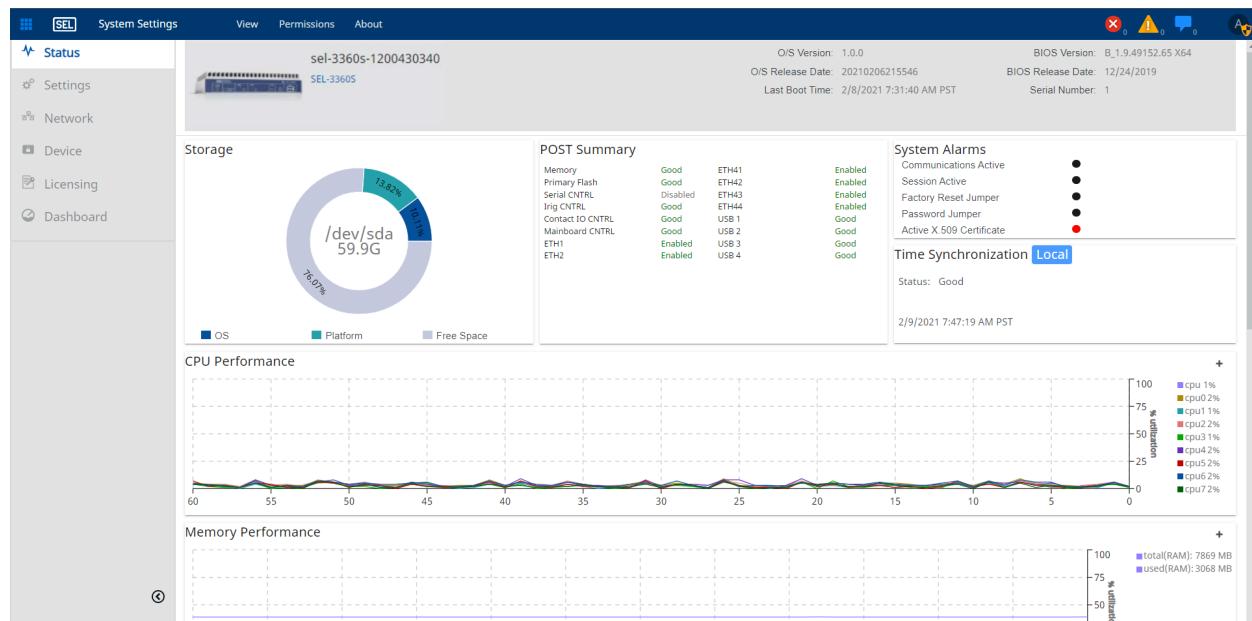
Use the Blueframe System Settings management tool to oversee the operational status and manage time, connections, and system parameters of your Blueframe node. After you launch the tool, the Status page displays high-level statistics related to the performance of the specific Automation Platform or virtual machine in use. Open the Settings page to define naming and time parameters specific to the Blueframe node. Specify network communication and host parameters on the Network page. From the Device page, you can upgrade the operating system, choose system power options, and reset the device. The following sections provide further details about each of these topics.

## Status

The Status page, shown in *Figure 2.2*, displays the current state of your Blueframe system as well as trending graph representations of CPU Performance, Memory Performance, Network Interface I/O, and Storage Disk I/O. The data charted on these graphs can help you gain a better understanding of the processing and storage resources available on the Automation Platform or virtual deployment of Blueframe. You can also use this page to review the burden that multiple applications impose on the overall system resources.

## 24 Blueframe Management Tools

### System Settings



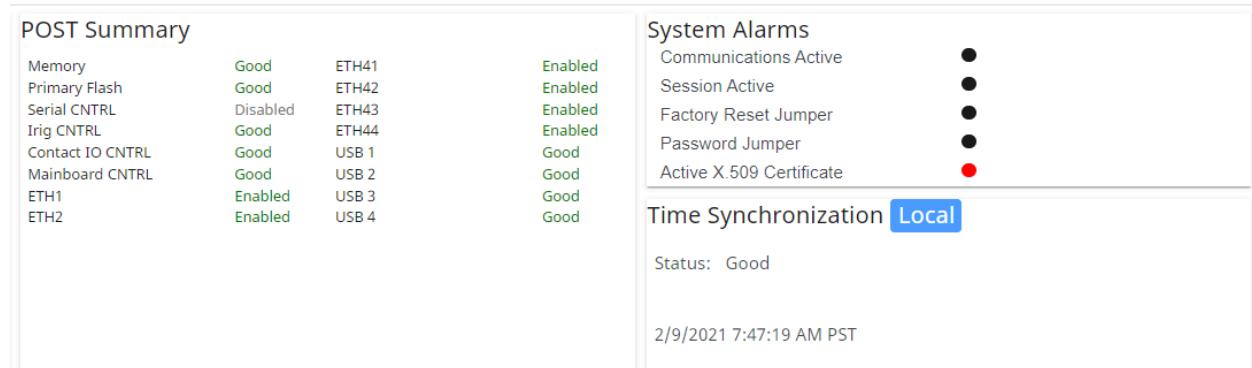
**Figure 2.2 System Settings Status Menu**

The Time Synchronization tile on the Status page displays the health and status of the time-synchronization method being used as a time source. Use the POST Summary and System Alarms tiles to review your communication assets and certain critical system alarm states, as shown in *Figure 2.3*.

#### NOTE

Enabling the Password Jumper allows you to create a temporary user to manage user accounts. While enabled, the Master Reset Jumper causes the Blueframe machine to reset to factory settings every time it is restarted. To learn more about jumper configurations and master reset, consult the manual for the Automation Platform being used.

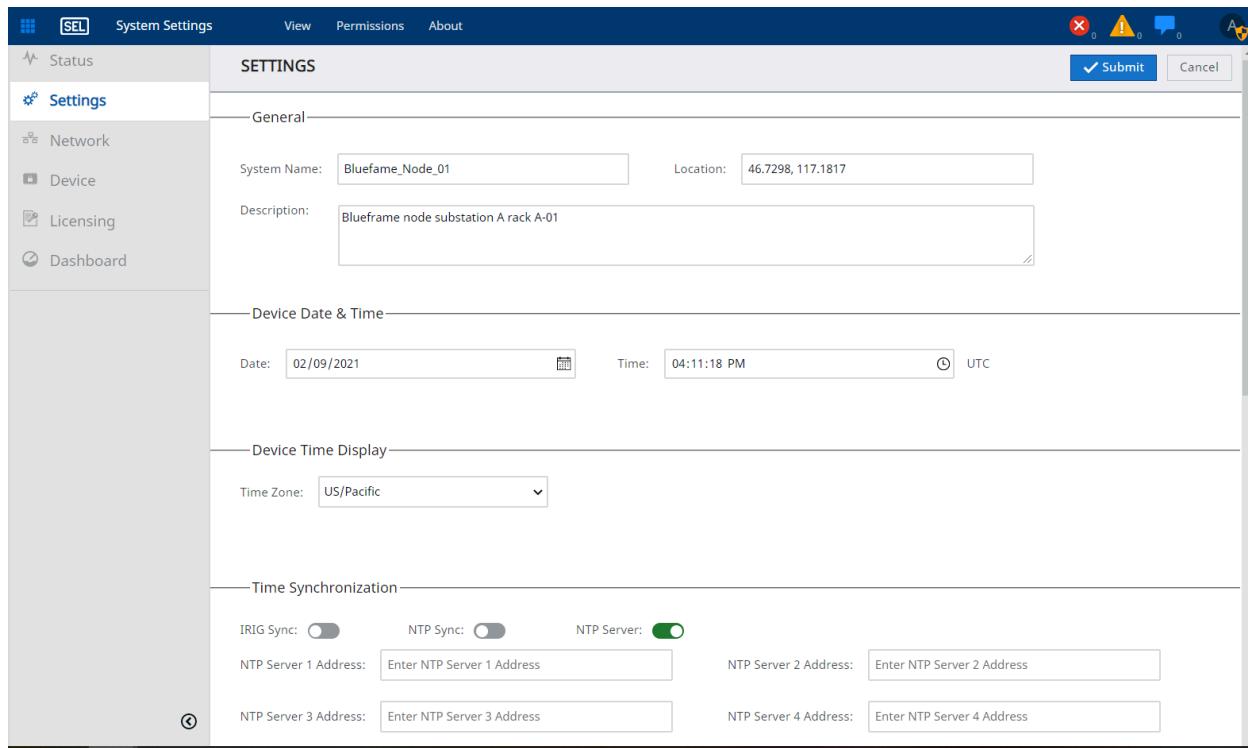
The password jumper is only supported on the Automation Platform hardware. There is no way to bypass the password requirement in virtual environments.



**Figure 2.3 POST Summary, System Alarms, and Time Synchronization Status**

# Settings

Use the Settings menu for configuring system settings relevant to the Automation Platform or virtual deployment used as a Blueframe node. Perform time-synchronization configuration also through this menu. See the following sections for further details.



**Figure 2.4 System Settings Page**

## General

The General device settings window offers the option to configure a device name, location, and its description, as shown in *Figure 2.5*.

The screenshot shows the 'General' device settings window with fields for System Name, Location, and a large Description area.

**Figure 2.5 General Device Settings**

## Device Date & Time

Use these settings to adjust the time for the Blueframe node manually. Ensure that the time is set to UTC +0 to display time stamps correctly throughout the system.

---

Device Date & Time

Date:   Time:   UTC

---

**Figure 2.6 Device Date & Time Settings**

## Device Time Display

This setting is used for specifying the time zone of an Automation Platform's local display.

## Time Synchronization

This section determines the type of time synchronization that you want to use for Blueframe processes. Time synchronization is critical for certain processes that need a precise and reliable time source such as IRIG or NTP. Blueframe provides options for synchronizing to such time sources, as shown in *Figure 2.7*.

---

Time Synchronization

IRIG Sync:       NTP Sync:       NTP Server:

NTP Server 1 Address:       NTP Server 2 Address:

NTP Server 3 Address:       NTP Server 4 Address:

---

**Figure 2.7 Time Synchronization Options**

**IRIG Sync:** When enabled, this setting synchronizes to the time of an incoming IRIG signal.

### NOTE

The SEL-3355 does not have IRIG enabled by default. See the COM 1 Jumpers section in the SEL-3355 instruction manual for instructions on how to enable IRIG via hardware jumpers.

**NTP Sync:** When enabled, this setting synchronizes to NTP reference clock sources. You can configure as many as four NTP servers as sources.

### NOTE

To achieve time synchronization with NTP, the system time should be manually set to within  $\pm 1$  hour of the actual time.

**NTP Server:** When enabled, this setting uses the Blueframe node as an NTP clock source to serve its time to other NTP-enabled devices.

Note that a Blueframe node automatically time synchronizes to the configured reference clock with the best determined quality. If no configured time source is available or the configured time source is determined to be of insufficient quality, no time synchronization occurs, and system time is based entirely on the hardware oscillator of the Blueframe node in use.

## Usage Policy

The Usage Policy field offers a preset text string to inform users about the user policy of the device. You can customize the field contents as necessary to match your usage policy.

# Network

The Network settings offer options for configuring the physical network interfaces of the Automation Platform as well as its host definitions.

## Interfaces

The network interfaces contain the settings for each port available based on the Blueframe hardware in use. To access a Blueframe node remotely, you can enter **https://** and the IP address or hostname of the node. If you use the hostname, as configured in the Global Settings, the Blueframe node must be on a network that can resolve the hostname to the IP address. The Interfaces list also displays all available Web Interfaces, as shown in *Figure 2.8*.

### NOTE

Blueframe's internal container networking system reserves the IP range of 172.17.0.0 through 172.19.255.255. This IP range cannot be set manually or by a DHCP server.

Interface	IPv4 Address	Gateway	DHCP	Enabled
enp3s0	10.202.26.96/22	10.202.24.1		✓

**Figure 2.8 Network Interfaces**

Selecting a Web Interface displays additional configuration options in the Interface Details pane shown in *Figure 2.9*.

Setting	Value
Name	ETH1
MAC Address	00:30:a7:21:11:21
IPv4 Address	10.112.203.254/20
Gateway	10.112.203.1
DNS	10.100.0.20
Domains	
DNS Default	true

**Figure 2.9 Network Interface Details**

**Enable Interface:** Enables/disables the network interface card (NIC).

**Enable DHCP:** Allows a Dynamic Host Configuration Protocol (DHCP) server to assign a dynamic IP address to that NIC.

**Name:** Indicates the non-modifiable identifier of the network interface being edited.

**MAC Address:** Indicates the non-modifiable and unique MAC Address of the Blueframe node device.

**IPv4 Address:** If DHCP is not used, this setting provides configuration of the IPv4 format IP address, including subnet mask. A subnet mask is designated by Classless Inter Domain Routing (CIDR) notation. The Blueframe network interface routes only network packets with IP addresses that conform to the configured mask. *Table 2.1* lists CIDR value and Subnet mask relationships.

**Table 2.1 CIDR Notation**

CIDR Value	Subnet Mask
/32	255.255.255.255
/31	255.255.255.254
/30	255.255.255.252
/29	255.255.255.248
/28	255.255.255.240
/27	255.255.255.224
/26	255.255.255.192
/25	255.255.255.128
/24	255.255.255.000
/23	255.255.254.000
/22	255.255.252.000

CIDR Value	Subnet Mask
/21	255.255.248.000
/20	255.255.240.000
/19	255.255.224.000
/18	255.255.192.000
/17	255.255.128.000
/16	255.255.000.000
/15	255.254.000.000
/14	255.252.000.000
/13	255.248.000.000
/12	255.240.000.000
/11	255.224.000.000
/10	255.192.000.000
/9	255.128.000.000
/8	255.000.000.000
/7	254.000.000.000
/6	252.000.000.000
/5	248.000.000.000
/4	240.000.000.000
/3	224.000.000.000
/2	192.000.000.000
/1	128.000.000.000
/0	000.000.000.000

**Gateway:** Defines the default gateway for this interface. The default gateway is the IP address of a router that provides a path to a network outside the subnet of this interface. You must configure a default gateway if incoming Ethernet traffic to this interface is not on the subnet for this interface. Note that this field cannot be modified when DHCP is enabled.

#### NOTE

Blueframe only supports one default gateway in use at any given time.

**DNS:** This is an optional field where you can define as many as two IPv4 addresses for Domain Name System (DNS) servers reachable through Blueframe to perform DNS resolution.

**Domains:** This is an optional field where you can define a list of domain names to be used as search suffixes for extending single-label hostnames for DNS lookups.

**DNS Default:** When this setting is True, the DNS servers defined on the interface are used to resolve names not matching domain names defined on all other interfaces. When this setting is False, the DNS servers defined on the interface are used to only resolve names for the defined domains on that interface.

## Hosts

Through Blueframe, you can statically map multiple hosts by specifying their hostnames and IP addresses. To map an IP address to a hostname, select the **New Host** button to display a pop-up window from where you can specify the hostname and IP Address. Select **OK** to add the hostname/IP map to the list of hosts.

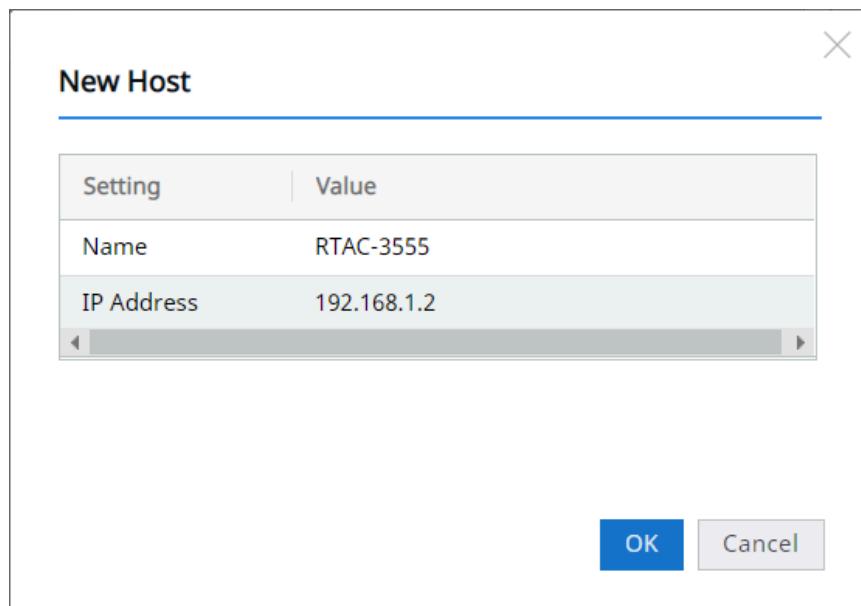


Figure 2.10 New Host Menu

## Internal Network Configuration

Blueframe requires a network IP range for internal communications. By default, the network IP range is composed of three Class B networks with host IP range within the 172.17.0.0–172.19.255.255 address space. This internal private IP range can conflict with external private networks. If a conflict is detected, the error message, "Main error: the IP range 172.17.0.0–172.19.255.255 is reserved for internal use" displays when configuring the network interfaces.

To resolve network interface conflicts, navigate to **System Setting > Network**, select the **Cluster IP** tab, and enter a valid IP address; for example, 172.54.0.1. In this example, the host IP range is 172.54.0.0–172.56.255.255, as shown in *Figure 2.11*.

Setting	Value
Cluster IP	* 172.54.0.1

**Figure 2.11 Configuring the Internal Network Address Space****⚠️ WARNING**

Resetting the internal IP range results in a factory reset. All applications and configurations are lost. Create backups of application configurations before proceeding.

## Device

The Device system settings page provides a menu for managing device-specific settings such as Firmware and Factory Reset and for reviewing information for the Trusted Platform Module (TPM) and Platform Configuration Register (PCR) Quotes. See the following sections for more details.

Property	Value
Manufacturer	IFX
Endorsement Key - RSA	MIIIBIJANBgkqhkiG9w0BAQEFAOCAQ8AMIIIBCgKCAQE1w038Wefdo39Oyi/CqH8+YIqvALoEVyLf8oWewW9qM...

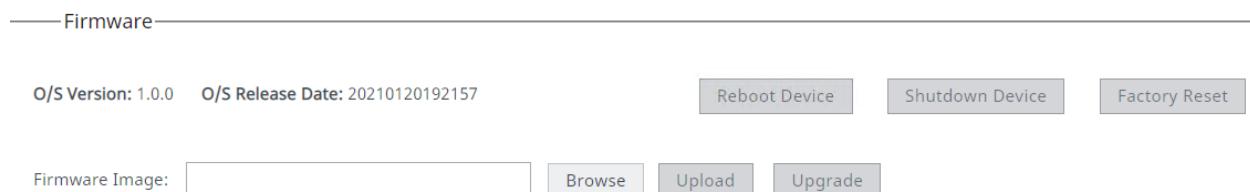
**Figure 2.12 Blueframe Device Settings**

## Firmware

The Firmware section lists the presently installed operating system version and release date as well as an option for upgrading the Blueframe node firmware version. To upgrade firmware, perform the following steps.

- Step 1. Obtain the appropriate firmware file (.strup) from an SEL representative.
- Step 2. Select **Browse** and locate the .strup firmware file you need, then select **Open**.
- Step 3. Select **Upload** to copy the firmware file into the Blueframe node.
- Step 4. After the .strup file has been uploaded, select **Upgrade**.

The Blueframe node will go through the firmware update process which restarts the system to finish applying changes. It will also update the core and hardware services as part of the firmware update.



**Figure 2.13 Firmware Upgrade Menu**

**Reboot Device:** Reboots the Automation Platform device or virtual machine on which the Blueframe node is running.

**Shutdown Device:** Shuts down the Automation Platform or virtual machine on which the Blueframe node is running.

**Factory Reset:** Clears all settings and data completely from the Blueframe machine and obtains a Blueframe instance with factory-default settings and data. Perform a system backup prior to a factory reset in case you may need to restore the system and its configuration to a last known state.

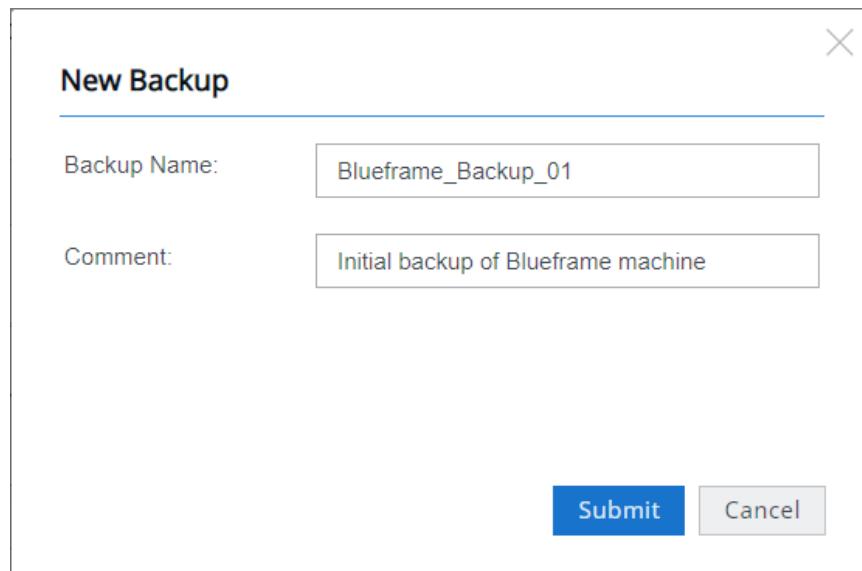
## Backup & Restore

The Backup & Restore section offers multiple options for managing backups of your Blueframe node. Creating a backup makes a copy of all your system settings and configuration data. You can use a backup to restore the system to a previous state.

Backup & Restore				
Creation Time	Name	Size	Backed Up By	Status
1/26/2021 12:25:03 AM	Backup1	1.5 GB	admin	Completed

**Figure 2.14 Backup & Restore Menu**

**New Backup:** Select this option to create a new backup. Select **New Backup** to obtain two fields, one for entering a backup name and another for entering comments about the backup you create.

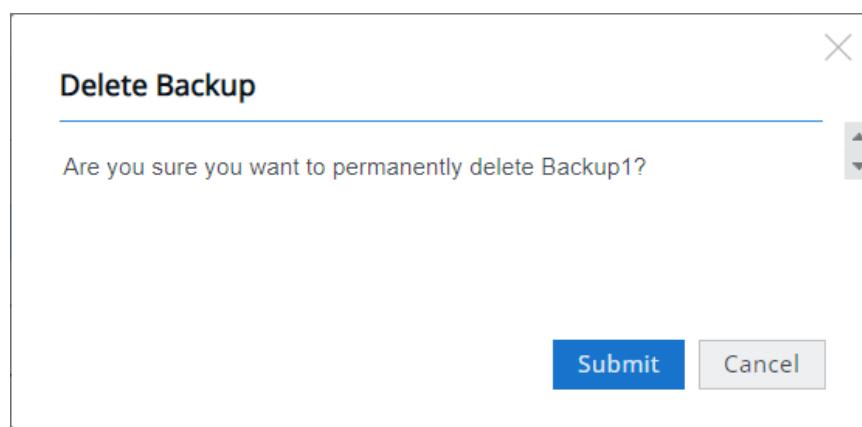


The dialog box is titled "New Backup". It contains two input fields: "Backup Name" with the value "Blueframe\_Backup\_01" and "Comment" with the value "Initial backup of Blueframe machine". At the bottom are "Submit" and "Cancel" buttons.

**Figure 2.15 New Backup**

**Restore:** If you have available backups, select the desired backup entry in the list and select **Restore**. This operation restores the Blueframe system to the state of the selected backup.

**Delete:** To delete a backup, select the record from the list of backups and then select **Delete** to display a message requesting that you verify whether you want to delete the selected backup. Select **Submit** to proceed. Note that a backup no longer exists in the system after you delete it, and any information it contained is lost.



The dialog box is titled "Delete Backup". It contains a message "Are you sure you want to permanently delete Backup1?". At the bottom are "Submit" and "Cancel" buttons.

**Figure 2.16 Delete Backup**

Selecting the menu button  provides you the ability to upload or download a backup. Use **Upload Backup** for uploading a backup file into the Blueframe node. Use **Download Backup** to export the selected backup entry from the list for archival as a .tgz file.

Upload Backup

Download Backup

**Figure 2.17 Download and Upload Backup Options**

## TPM Details

The Trusted Platform Module (TPM) is a chip on the Automation Platform motherboard that can be used for encryption, decryption, and remote verification of the system. The TPM Details interface in this case, as shown in *Figure 2.18*, displays the manufacturer of the chip and its Endorsement Key - RSA.

### NOTE

The TPM is only available on supported hardware and is not supported in virtual environments.

—TPM Details—

Property	Value
Manufacturer	IFX
Endorsement Key - RSA	MIIIBIjANBgkqhkiG9w0BAQEFAOCAQ8AMIIIBCgKCAQEA1w038Wefdo39Oyi/CqH8+YIQvALoEVyLf8oWewW9qM...

**Figure 2.18 TPM Details**

## PRC Quotes

The Platform Configuration Register (PRC) contains critical system information for the Blueframe hardware. Blueframe provides options for generating a quote to obtain such information. To obtain a quote, enter comma-separated PRC indices that you want to include in the quote and then select **Quote**. Note that you can either enter the Nonce manually or generate it automatically.

### NOTE

PRC quotes are not supported in virtual environments.

The screenshot shows the 'PRC Quotes' configuration page. It has two main sections: 'PCRs:' and 'Nonce:'. The 'PCRs:' section contains a text input field with placeholder text 'comma separated list of PCR indices to include in the Quote'. The 'Nonce:' section contains a text input field with the value 'MTgxLDI0MSwyMzksMTU3LDlyNywxMzcsNDksMjU1', a 'Auto GenerateNonce' button, and a 'Quote' button. Below these sections is a 'Results' table with several rows of data. The table has two columns: 'Description' and 'Value'. The 'Nonce' row is highlighted with a blue background. The table also includes rows for Digest, Algorithm, Attestation Data, Signature, RSA Public Key, and PCR 0.

Description	Value
Nonce	MTgxLDI0MSwyMzksMTU3LDlyNywxMzcsNDksMjU1
Digest	H7enV4aIss3OzqcB+VBjD15zqqPMDGk4IzuBG5fHHbU=
Algorithm	SHA-256
Attestation Data	/1RDR4AYACIAC8CQUuxTCvJoyenoL86ihidsax8w1dDwZpMuZoNomOWmAB4xODEsMjQxDIzOSw...
Signature	wQBFFjjqhckKbVLZsPGchh+s2L5rXfEPWA9FqToqIEhySH0cwF2Xjq3/rz4Z1CdepBYED1t1sEyS5+3Ne...
RSA Public Key	MIIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIIBCgKCAQEAE7mdBJLpjFymNe8VroU7ruoMLxE7OwTM...
PCR 0	0JT70IDT08JGJ-M-C6CCCCUQW4-BLDD-DCGUUWMMQ

**Figure 2.19 PRC Quotes**

After the generation of a quote, it displays in the Results section.

## Operation Modes

Blueframe can operate in one of two modes: normal or standby. The operation mode can be managed in **System Settings > Device**.

- ▶ **Normal Mode.** In this mode, all application configurations are accessible and applications execute their configurations immediately.
- ▶ **Standby Mode.** In this mode, all application configurations are accessible but only core-services and hw-services will execute immediately. All other applications will not execute their configurations until the next time Blueframe operates in normal mode. While in standby mode, Blueframe is still accessible from all network interfaces and local displays and logs are still generated and stored. An indicative banner appears in Blueframe while operating in standby mode.

When Blueframe restarts, it will start in the mode in which it was previously operating.

## Dashboard

The Dashboard page displays read-only information related to the containerization technology used by Blueframe. You can review logs of the services that run processes related to Blueframe applications. The Dashboard is meant to be used as a resource for advanced troubleshooting and can only be accessed by users who have been granted permission to view the Dashboard in the System Settings permissions.

## Licensing

When you order a Blueframe machine, it comes from the factory preloaded with licensed applications. However, if you purchase a new application package to add to your Blueframe installation, you must first upload a license file as described in *Upload a License File on page 36*. Then load and install the relevant application package as described in *Section 8: Application Management*.

You can then select each relevant license from the Active Licenses menu to view application package licensing information.

The screenshot shows the 'Active Licenses' tab selected in the top navigation bar. Below it is a table with columns: License, Affected Applications, and Status. The table lists several application packages:

License	Affected Applications	Status
connection-services	1	Installed
core-services	6	Installed
dma-configuration-monitoring	2	Installed
dma-disturbance-monitoring	0	Unknown
dma-simultaneous-connections	0	Unknown

An orange arrow points from the 'Affected Applications' column of the 'core-services' row to a detailed view on the right. This view includes the license name ('core-services:1'), status ('Installed'), and a 'Metadata' section. Another orange arrow points from the 'Affected Applications' section to a list of affected applications, each with a corresponding icon:

- Central Authentication (User icon)
- Certificate Management (Key icon)
- Web Portal (SEL icon)
- Application Management (Grid icon)
- Security Logs (Padlock icon)
- User Management (User icon)

Figure 2.20 Application Package Licensing

## Upload a License File

- Step 1. Select the **Licensing** tab.
- Step 2. Select **Upload License Files** and select the (.lic) file that you obtained from SEL and select **Open**.

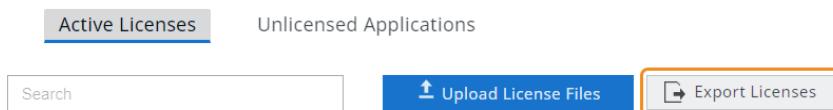
You will now see a license in the list of licenses.

### NOTE

If you are updating an existing application package there is no need to reload a license file. This process is only necessary if you are loading a newly purchased application package. Also note that if you load an application package without its license file, the application bar will highlight that an application has not been licensed until a valid license file is loaded.

## Export a License File

In addition to uploading a license, this menu also offers the ability to export all your existing license information into one .json file that can be used as a backup. If you need to restore your Blueframe machine to factory settings, you can use the exported license file to restore all your application package licenses. To export your licenses, select **Export Licenses**, as shown in *Figure 2.21*. Note that the exported .json file is encrypted and will only be compatible with the Blueframe machine from which it was exported.



**Figure 2.21 Export Licenses**

## Redundancy

---

Blueframe provides the ability to synchronize one installation of Blueframe, including its associated applications and collected data, with another Blueframe installation. In the following discussion, each Blueframe installation will be referred to as a node. As many as six nodes can be included in a redundancy configuration (i.e., one primary node with as many as five backup nodes).

A node being used in a redundancy scheme can be in one of two states:

**Primary:** In this mode, the node operates as normal, executes all configurations in all installed applications, and replicates collected data, configurations, and applications to the backup node.

**Backup:** In this mode, the node synchronizes with the primary node. No data are collected and no execution of installed applications occurs.

The following criteria must be met in order to implement redundancy:

- ▶ All nodes (primary and backup) must have the same OS version.
- ▶ All nodes must have the same disk size.
- ▶ All nodes must be the same asset type. Hardware nodes can only be redundant with other hardware nodes. VM nodes can only be redundant with other VM nodes.
- ▶ All nodes must have the same cluster IP address.

A user role must have the System Settings permission "Can Manage Device" to be able to add, remove, or manage nodes in a redundancy scheme.

When a node is added as a backup node, administrator account credentials for the backup node must be entered on the primary node. (These credentials are used temporarily and are not stored.) Optionally, you can verify the X.509 certificate of the node to be added as a backup to confirm the identity of the node.

Once a node is successfully configured as a backup node, that node restarts and begins operating in backup mode. All previous applications, configurations, and data on that node will be overwritten by the data and applications on the primary node. The only configuration parameters that a backup node maintains independently from the primary node are its IP settings, hostname, and X.509 certificate.

In order for a primary node and backup node to successfully exchange data, they must be able to communicate TCP-based traffic on port 443 and UDP-based traffic on port 3778. All communications between synchronized nodes are encrypted. When more than one backup node is present in a redundancy system, each backup node creates communication sessions with each other backup node. If a backup node loses communication with the primary node but retains communications with other backup nodes, the node that lost synchronization with the primary node will receive updates from the other backup node(s).

After a node is initially configured as a backup in a redundancy scheme, it cannot be promoted to primary until synchronization between the primary and backup nodes are complete. The time it takes to synchronize is partially dependent on the bandwidth of the network connecting the two nodes. The interface of both the primary and backup node will have a visual indication during this initial synchronization. Afterward, the primary node will have a visual indication when the backup node is *not* up-to-date with the primary node.

## Managing Redundancy

Management of a redundancy scheme is performed from the primary node. The only configuration that can be done from the backup node is promoting that node to primary. This should only be used when the backup node and the primary node have lost communications because it could result in two nodes being considered primary at the same time. If this occurs, one node will need to be reset to factory-default settings and then re-added as a backup node to the other. It is the system administrator's responsibility to ensure that two nodes do not become primary simultaneously.

The primary node may initiate a pause in redundancy during which data from the primary node will *not* be sent to the backup node. This can occur, for example, during an upgrade to the OS on the primary node. Once the OS is updated on the primary node, the OS on the backup node will need to be updated to match that on the primary node before redundancy can resume. Updating the OS on the backup node must be done directly on the web interface of that node.

## Removing a Node From Redundancy

If a backup node is removed from a redundancy scheme, the previous backup node will restart in normal mode and execute all configured applications that were synchronized from the previous primary node. All data that were synchronized to the node will also be available. Users may need to factory-reset the unit or disconnect the unit to prevent potential interference with the still-active primary node.

## Backup Node Management

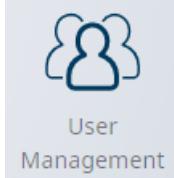
When the IP address of a backup node is entered, the user is redirected to the primary node's web interface. To access the backup node, enter the IP address followed by the url **/admin**. For example, <https://192.168.5.2/admin> directs you to a management interface where you can promote the node to primary, update the operating system version, or enable standby mode. These options are only available when communication to the primary node has been lost or the primary node suspends or disables redundancy.

## Recommended Operation Practices for Redundancy

- If the backup node needs to become the primary node, SEL recommends promoting the backup node to be the primary node through the *primary node* interface. This helps prevent the possibility of two nodes being set as primary at the same time. Promoting a backup node to primary directly through the backup node interface should only be done if the primary node is not powered on or otherwise unavailable.
- If two nodes are both operating as primary nodes, the management interface allows you to either place the node being accessed into backup mode or to set the remote primary node as a backup node so that only one node is primary in the system.
- Backup nodes should not change IP address or hostname while acting as a backup. Doing so will cause loss of communication with the primary node. SEL recommends that backup nodes use static IP address assignment.

## User Management

---



**Figure 2.22 User Management Icon**

Blueframe has a dedicated tool for creating users and assigning them to access roles that propagate throughout the system. You can define application access and management permissions at the role level, simplifying user permissions and access to Blueframe applications. Assign users to one or more roles; the role with the broadest permissions takes precedence when determining user permissions.

## Creating a New User

To create a new user, launch the User Management tool by selecting the User Management icon (see *Figure 2.22*) from the Blueframe Portal, select **Users** in the Navigation Pane, and select **New User**, as shown in *Figure 2.23*, to display the Create New User window shown in *Figure 2.24*.

**40**    Blueframe Management Tools  
**User Management**

Users										
Search										
	Users	Roles	State	Activates	Expires		Password Updated	Last Logged In	Online	
🛡️	admin	admin	Enabled	⌚ Never	⌚ N/A	⌚	Jan 15, 2021 0:59:27 am	Jan 15, 2021 3:14:04 am	✓	
🛡️	Cristian	admin, Automation Engi	Enabled	⌚ Jan 14, 2021	⌚ N/A	⌚	Jan 15, 2021 3:08:45 am	Jan 15, 2021 3:15:24 am	✓	
🛡️	Cailin	admin, Automation Engi	Enabled	⌚ Jan 15, 2021	⌚ N/A	⌚	Jan 15, 2021 3:09:06 am	Never		
👤	Darrin	Automation Engineer	Enabled	⌚ Jan 15, 2021	⌚ Never	⌚	Jan 15, 2021 3:09:24 am	Never		
🛡️	David	admin, Automation Engi	Enabled	⌚ Jan 15, 2021	⌚ N/A	⌚	Jan 15, 2021 3:09:39 am	Never		

**Figure 2.23** User Management Users Menu

The Create New User window defaults to the basic menu for creating a user. You can also expand that menu, by selecting  More , to configure additional attributes such as user role assignment, activation dates, and the user homepage.

Create New User

NewUser

USER NAME

New Password

PASSWORD

Confirm Password

CONFIRM

Force password reset on their next log in

NOTES:

LAST LOG IN: Never OFFLINE

ACTIVATION:

EXPIRATION:

HOME PAGE:

ROLES ASSIGNED TO USER:

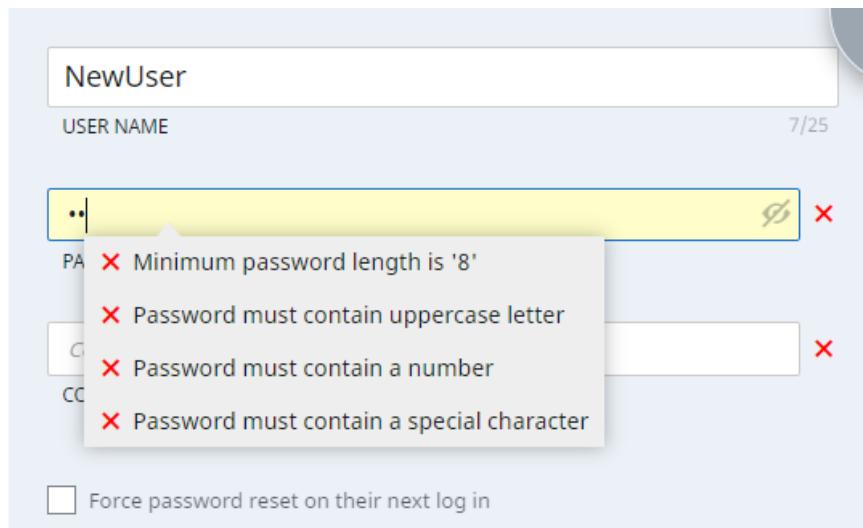
admin  
 Automation Engineer  
 Operator  
 Technician

 Less  Suspend this Account

**Figure 2.24** Create New User Menu

An administrator can manage account usage through the Expiration and Suspend this Account options. Setting the Expiration for an account defines an end date for the user to successfully authenticate to Blueframe; any active sessions will remain operational until they are logged out. Suspend this Account ends any open sessions by the user and ensures that they can no longer authenticate to the system until the account is re-activated.

When creating a password for a user role, it is important to note that an administrator of the system defines the requirements. While you create a password for a user account, a pop-up message displays. This message states which requirements have or have not been met. You cannot complete the user creation process without first satisfying the password policy.



**Figure 2.25 User Password Menu**

If you are a member of the admin group, select **Settings > Password Policies** to view and revise the Password Policies.

The screenshot shows the 'Password Policies Configuration' dialog box. An orange arrow points to the title bar. The dialog contains a table with columns 'Rule', 'Value', and 'Description'. The table rows are:

Rule	Value	Description
Minimum Length	8	Ensures that the password length is not less than the set Minimum Length
Maximum Length	30	Ensures that the password length is not greater than the set Maximum Length
Require Uppercase Character		Ensures that the password contains at least one uppercase character
Require A Number		Ensures that the password contains at least one number
Require Special Character		Ensures that the password contains at least one special character
Password Duration	180	Defines how long a password will be valid before needing to be updated (in days)
Password History	5	Ensures new passwords are not one of the previous passwords within the set history

At the bottom right are 'Update' and 'Cancel' buttons.

**Figure 2.26 Password Policies Configuration Menu**

You can configure a user to be logged in to the local display interface automatically. Only one account can be configured to be logged in automatically. An account that is configured with automatic login can be accessed normally through the web interface. All conditions still apply as they do for an account without automatic login.

## Roles

You must create an initial user during the initial Blueframe bootup sequence. Blueframe assigns that user to the admin role automatically. After the initial setup, you can create custom user roles for more granular system access. You can configure each role with selective access to necessary applications. For each application, you can select the Can Launch or Can Manage option, as shown in *Figure 2.27*.

**Can Launch:** Allows a user to launch an application, modify its configuration, and view its data.

**Can Manage:** Allows a user to select further permissions by launching an application and selecting the Application Permissions option from the Application Bar menus. Each application and management tool has its own set of advanced permissions; if the Application Permissions option is unavailable for an application, that application lacks additional management options.

Once you have created a role, you can add or remove members and these members inherit the permissions of the role you create; there is no need for you to spend time configuring permissions for each user individually. If necessary, you can use the tool to assign multiple roles to a user. That user would inherit the multiple application permission sets of those roles.

### NOTE

You cannot delete the default admin role, and you cannot revise certain permissions within it. This is by default to prevent the loss of critical permissions necessary for system configuration.

The screenshot shows the 'User Management' interface with the 'Roles' tab selected. A search bar at the top right contains the placeholder 'Search...'. Below it is a table of roles:

Role	Members	Created By	Created On	Description
admin	1	admin	Apr 26, 2022 2:43:31 pm	
Automation Engineer	4	admin	Apr 26, 2022 2:43:41 pm	
Operator	2	admin	Apr 26, 2022 2:44:10 pm	
Technician	5	admin	Apr 26, 2022 2:44:28 pm	

A modal window for the 'Automation Engineer' role is open. It shows the role name and a table of users assigned to it:

Name	Roles	State
admin	admin, Automation Engineer, Technician	Enabled
Allie	Automation Engineer, Technician	Enabled
Brooks	Automation Engineer, Technician	Enabled
Cailin	Automation Engineer, Operator, Technician	Enabled

Below this is a section titled 'Application Accessibility' with a table mapping applications to launch and manage permissions:

Application	Can Launch	Can Manage
Application Management	<input type="checkbox"/>	<input type="checkbox"/>
Central Authentication	<input type="checkbox"/>	<input type="checkbox"/>
Certificate Management	<input type="checkbox"/>	<input type="checkbox"/>
Configuration Monitoring	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Configuration Monitoring Archive	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Credential Management	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Credential Management Archive	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Direct Resource Access	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Disturbance Monitoring	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Disturbance Monitoring Archive	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Figure 2.27 User Management Roles Menu

## Creating a New Role

To create a new role, select **New Role** to display the Create a New Role window.

The screenshot shows the 'ROLES' page with a search bar and a 'New Role' button highlighted with an orange box. Below is a table of existing roles:

Role	Members	Created By	Created On	Description
admin	4	admin	Jan 15, 2021 10:27:52 am	
Automation Engineer	4	admin	Jan 15, 2021 10:24:09 am	
Operator	0	admin	Jan 15, 2021 10:24:01 am	
Technician	2	admin	Jan 15, 2021 10:24:27 am	

Figure 2.28 Adding a New Role

From within the Create a New Role window, you can define the Role Name, apply an optional description, define members, and choose the Can Launch and Can Manage permissions for each installed application. Adding a user to the role is optional from this menu; you can assign users to roles in multiple ways.

Create a New Role

ROLE NAME:  7/30

DESCRIPTION:  0/200

ROLE MEMBERS

APPLICATION ACCESSIBILITY

Application	<input type="checkbox"/> Select All	<input type="checkbox"/> Select All
Application Management	<input type="checkbox"/> Can Launch	<input type="checkbox"/> Can Manage
Central Authentication	<input type="checkbox"/> Can Launch	<input type="checkbox"/> Can Manage
Certificate Management	<input type="checkbox"/> Can Launch	<input type="checkbox"/> Can Manage
Configuration Monitoring	<input type="checkbox"/> Can Launch	<input type="checkbox"/> Can Manage
Configuration Monitoring Archive	<input type="checkbox"/> Can Launch	<input type="checkbox"/> Can Manage
Credential Management	<input type="checkbox"/> Can Launch	<input type="checkbox"/> Can Manage
Credential Management Archive	<input type="checkbox"/> Can Launch	<input type="checkbox"/> Can Manage
Direct Resource Access	<input type="checkbox"/> Can Launch	<input type="checkbox"/> Can Manage
Disturbance Monitoring	<input type="checkbox"/> Can Launch	<input type="checkbox"/> Can Manage
Disturbance Monitoring Archive	<input type="checkbox"/> Can Launch	<input type="checkbox"/> Can Manage
DMA Diagnostics	<input type="checkbox"/> Can Launch	<input type="checkbox"/> Can Manage
DMA REST API	<input type="checkbox"/> Can Launch	<input type="checkbox"/> Can Manage
DMS Designer	<input type="checkbox"/> Can Launch	<input type="checkbox"/> Can Manage
FLISR	<input type="checkbox"/> Can Launch	<input type="checkbox"/> Can Manage
Flow Controller	<input type="checkbox"/> Can Launch	<input type="checkbox"/> Can Manage
SEL Portal	<input checked="" type="checkbox"/> Can Launch	<input type="checkbox"/> Can Manage

**Figure 2.29** Creating a New Role Menu

## Modifying Role Members

To assign or remove a user, select the desired role within the ROLES menu and select one of the highlighted options in *Figure 2.30*.

The screenshot shows the 'ROLES' section of the Blueframe Management Tools. At the top, there is a search bar with the placeholder 'Search...' and a magnifying glass icon. Below the search bar is a table with three columns: 'Role', 'Members', and 'Created By'. The table contains four rows:

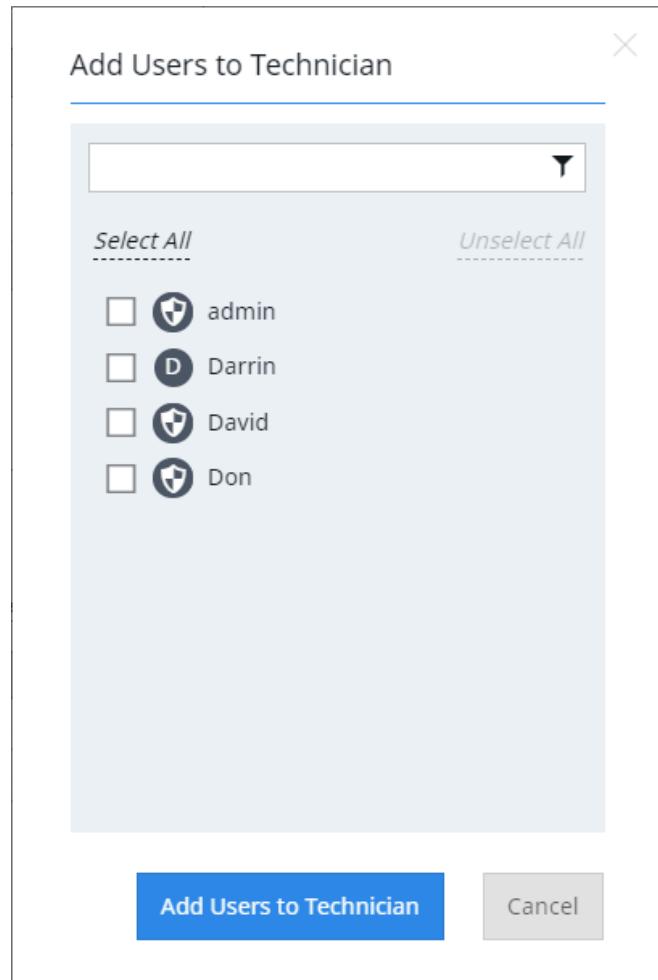
Role	Members	Created By
admin	5	admin
Automation Engineer	4	admin
Operator	0	admin
Technician	2	admin

Below the table, the 'ROLE NAME:' is set to 'admin'. Underneath this, there are two buttons: 'Select All' and a box containing '+ Users' and '- Users'. The '+ Users' button is highlighted with an orange border and an orange arrow points to it from the top. Below these buttons is another table with columns 'Name', 'Roles', and 'State'. It lists three users:

Name	Roles	State
admin	admin	Enabled
Cailin	admin, Automation Engineer, Technician	Enabled
Cristian	admin, Automation Engineer, Technician	Enabled

Figure 2.30 Adding or Removing Role Members

Select **- Users** to remove the highlighted user or set of users. Select **+ Users** to display a pop-up menu for adding users to a Role.



**Figure 2.31 Adding Users to a Role**

Within the pop-up menu, you can select a user or search for the user you want. Note that search characters are not case sensitive and that the tool supports partial character searches.

## User Management Application Bar

The User Management application bar offers the following options.



**Figure 2.32 User Management Application Bar Menus**

**File:** Offers options for creating, importing, and exporting users and roles. Blueframe saves exported files with the .json format, and these files can be used on other Blueframe nodes.

Select the option to Import Data and select the desired .json file to import users and roles. The software guides you through the data import to prevent the possibility of duplicating information.

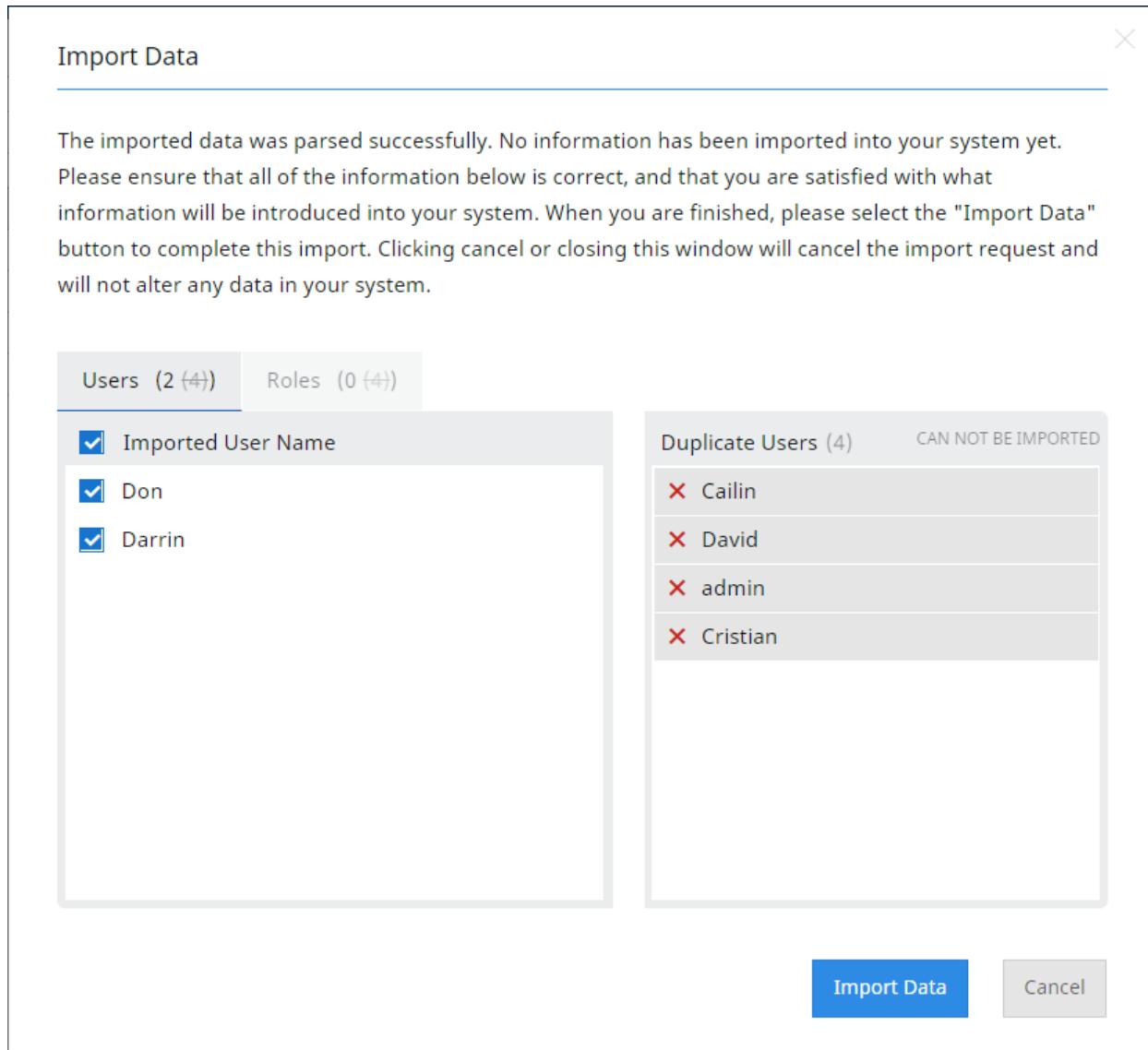


Figure 2.33 User Management Import Data Menu

**View:** Switches the view between the Users and Roles menus and provides options to view notifications.

**Settings:** Provides you access to the Password Policies and Session Preference menus.

**Password Policies:** Provides a more detailed selection of options that Blueframe requires for user password creation. The options are the following:

**48**    Blueframe Management Tools  
**User Management**

Password Policies Configuration

Adjust the settings in the regions below to configure password criteria. Any policy modifications made will be enforced the next time a new user is created or an existing user is prompted to change their password.

Rule	Value	Description
Minimum Length	8	Ensures that the password length is not less than the set Minimum Length
Maximum Length	30	Ensures that the password length is not greater than the set Maximum Length
Require Uppercase Character		Ensures that the password contains at least one uppercase character
Require A Number		Ensures that the password contains at least one number
Require Special Character		Ensures that the password contains at least one special character
Password Duration	180	Defines how long a password will be valid before needing to be updated (in days)
Password History	5	Ensures new passwords are not one of the previous passwords within the set history

**Update**    **Cancel**

**Figure 2.34** User Management Password Policies Menu

**Session Preferences:** Provides the option to select the number of failed login attempts available to a user.

Session Preferences

Adjust the settings for session time outs and login preferences in the regions below. Any preference changes will be enforced immediately upon submitting the data.

Track Login Attempts     attempts

Informs the system of the number of failed login attempts that are allowed. If a user exceeds the number of allowed failures, their account will be locked for the specified amount of time below.

Lock Out Duration     minutes ▾

When a User Account has exceeded the number of specified login attempts, the account will be locked for the specified time.

**Update**    **Cancel**

**Figure 2.35** User Management Session Preferences Menu

**About:** Provides information about the Blueframe application platform and offers a link to the SEL Blueframe Getting Started webpage that contains support literature.

## Certificate Management

---



**Figure 2.36 Certificate Management Icon**

Blueframe supports encrypted connections for HTTPS and Open Database Connectivity (ODBC) using the Transport Layer Security (TLS) protocol. To obtain a trusted connection between a web server and a web client, a valid, signed certificate must be present. The certificate serves the purpose of verifying the identity of the web server so that it can be trusted by a client and a secure encrypted connection can be established.

The X.509 public-key infrastructure (PKI) standard is the format for creating certificates that can be signed by a trusted certificate authority (CA).

Blueframe provides a tool for creating and importing base64 (.cer) X.509 and CA certificates and does not support any of the binary formats. In addition to providing a verified connection, CA certificates are also used for authenticating LDAP and TLS/SSL Ethernet tunneled serial connections. The following sections contain more information about the management tools for X.509 and CA certificates within Blueframe.

## X.509 Certificates

Blueframe offers a tool to create an unsigned certificate with all the needed information to comply with the X.509 standard. The private key remains on the Blueframe node and is not accessible. The public portion of the key is available for export. Because the X.509 certificate is self-generated, it must go through a signing process so that other devices in the network recognize Blueframe as a trusted device.

To generate your own certificate and distribute it to trusted clients, see *Generating and Activating an X.509 Certificate on page 50* and *Distributing an X.509 Certificate to Client Machines on page 51*.

To generate a Certificate Signing Request for a Certificate Authority to verify and sign, see *Signing a Blueframe Generated Certificate on page 56* and *Importing a Verified Certificate Authority Certificate on page 57*.

To import a signed certificate with a private key, see *Importing a New Certificate on page 58*.

## Generating and Activating an X.509 Certificate

Step 1. Launch the Certificate Management tool and go to the X.509 certificates menu on the navigation pane.

Step 2. Select **Generate Certificate**.

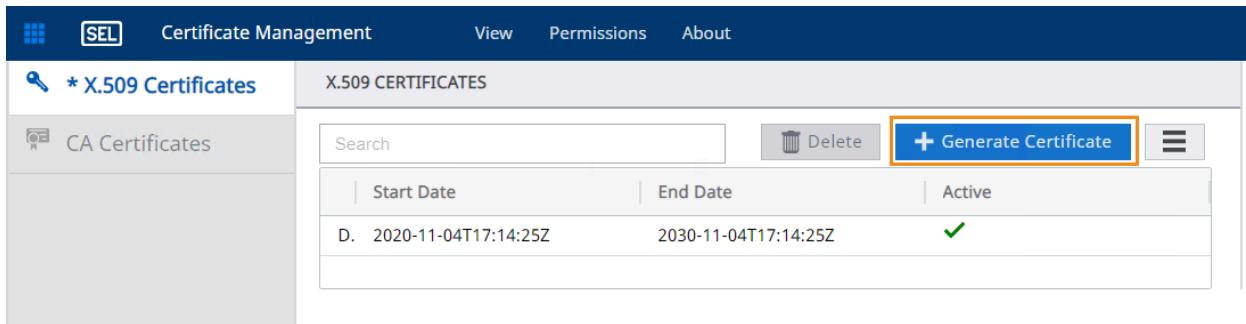


Figure 2.37 Generate Certificate

Step 3. Fill out the Generate X.509 Certificate window that includes all the required fields to generate an X.509 certificate, as shown in *Figure 2.38*.

### NOTE

If **Valid Time Period** is set to 13 months or longer, a "Not Secure" tag appears in the browser address bar.

Step 4. Select **Submit** to generate the certificate.

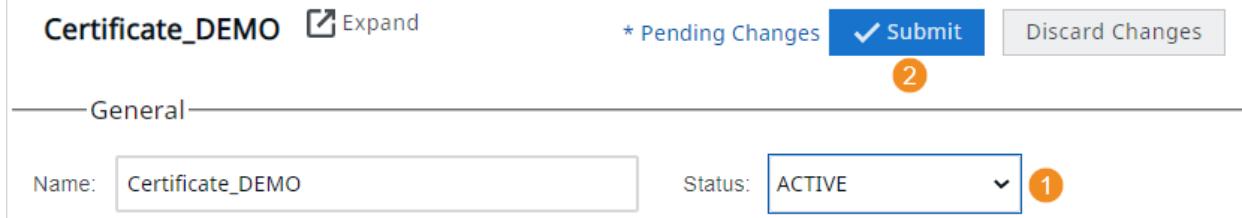
Certificate Name:	BlueframeCert	Organization Name:	SEL
*RSA Key Size:	2048	Organization Unit Name:	Automation
*Country Abbreviation:	US	Email Addresses:	Enter comma separated email addresses
*Common Name:	Input your Blueframe IP address here	Street Address:	Enter street address
Valid Time Period:	1 year	Postal Code:	Enter postal code
State/Province:	WA	Locality:	Enter locality
Subject Alternative Names:	Input your Blueframe IP address here	* indicates required field	
		Submit	Cancel

Figure 2.38 Identity Information

**NOTE**

The Country Abbreviation must be entered as two characters. Also, the Common Name must match the IP address or hostname that you are using in the address bar to access the Blueframe node. Additionally, most web browsers also require the IP address or hostname to be populated in the Subject Alternative Name (SAN) fields. Do not leave this field unspecified.

- Step 5. Select the newly generated X.509 certificate on the left side of the Blueframe user interface and change its status to **ACTIVE** in the certificate attributes window on the right side of the interface.
- Step 6. Select **Submit** to save the changes.



**Figure 2.39 Activating a Certificate**

- Step 7. Refresh your browser so that it begins using the newly activated certificate from that Blueframe node.

## Distributing an X.509 Certificate to Client Machines

Once you have generated and activated a certificate, use the following process to obtain a self-signed certificate that you can distribute to web clients within your network for verified access. To import a certificate, you must launch a browser on each client machine and perform the following steps:

- Step 1. Open the login screen of Blueframe from a client machine. Notice that the browser does not list this as a trusted connection, as shown in *Figure 2.40*.

**NOTE**

This example uses Microsoft Edge, but different browsers may present the following information with different wording and user interface layouts.

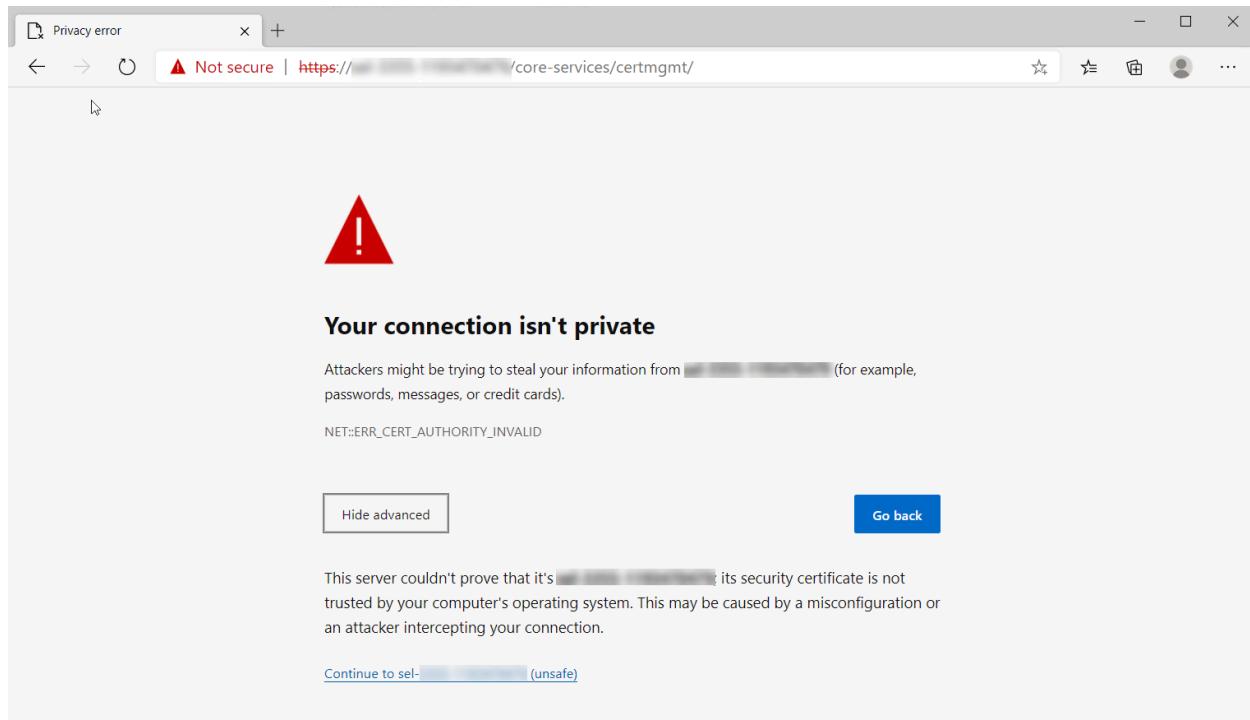
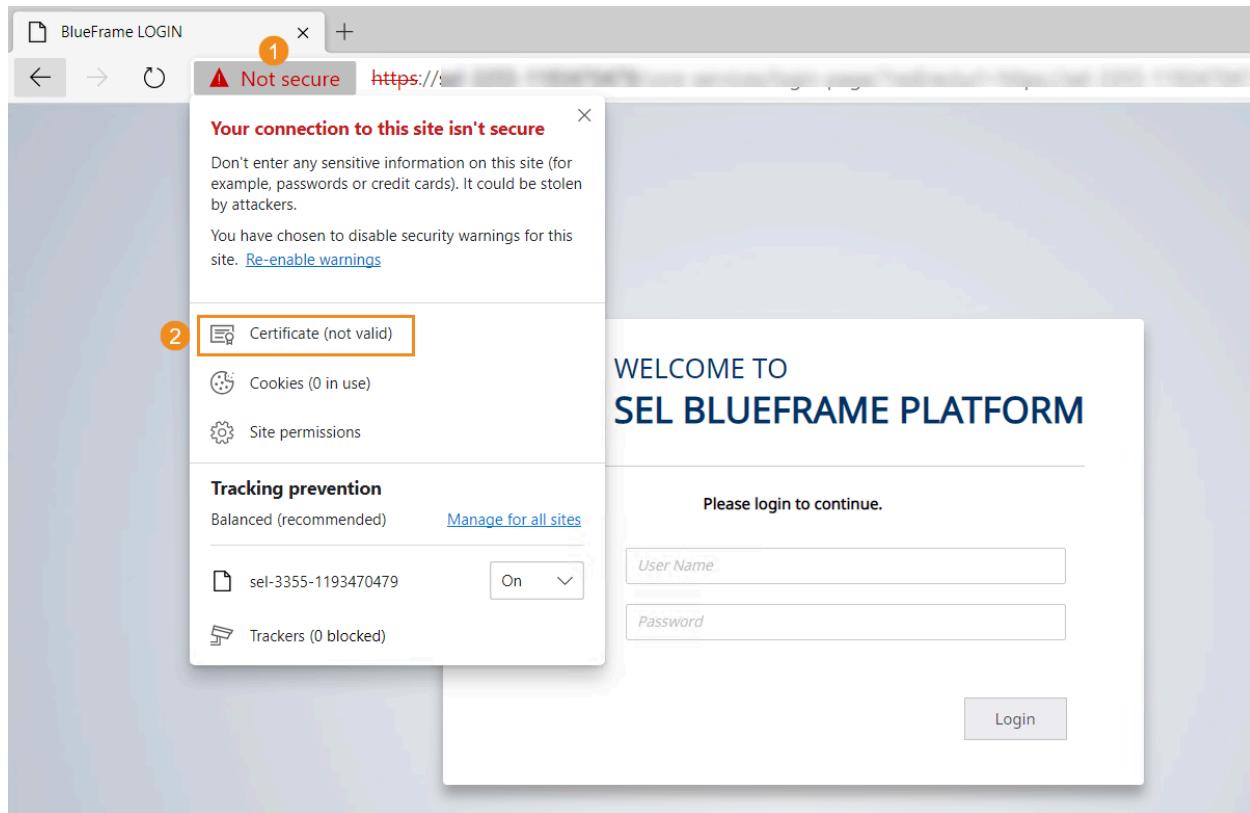


Figure 2.40 Privacy Error Message

- Step 2. Select **Continue to IP address (unsafe)**.
- Step 3. In the login screen for Blueframe, select the **Not secure** warning in the URL bar. This will give you additional options for certificate management. Select **Certificate (not valid)**.



**Figure 2.41 Your Connection to This Site Isn't Secure Message**

Step 4. Once the Certificate window opens, select the **Details** tab.

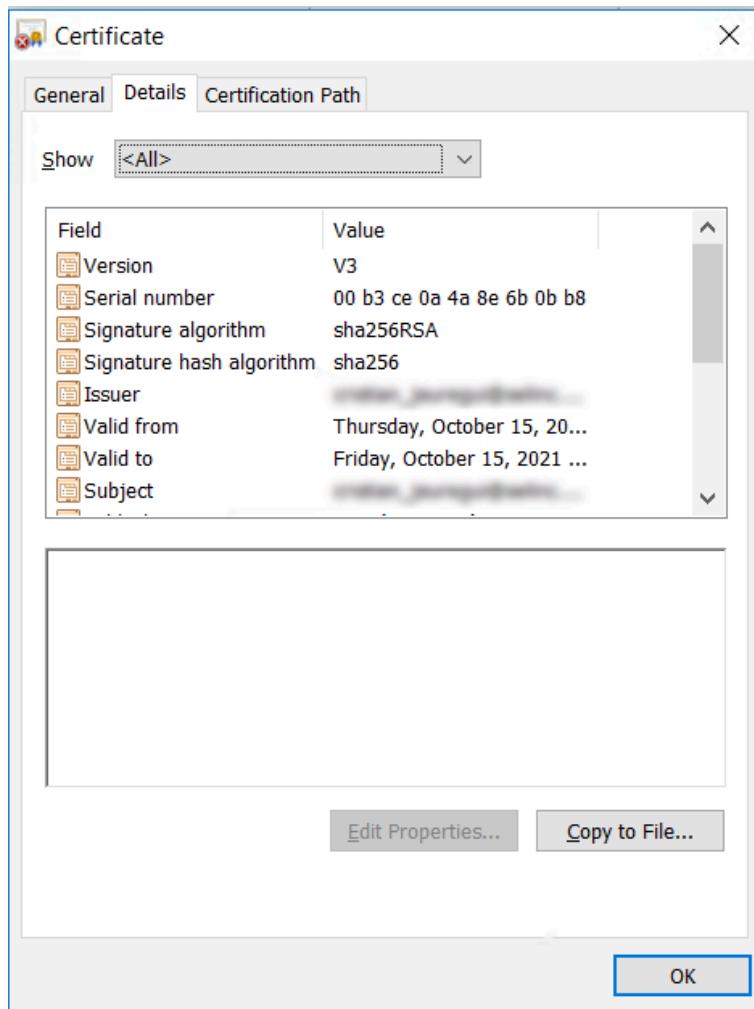
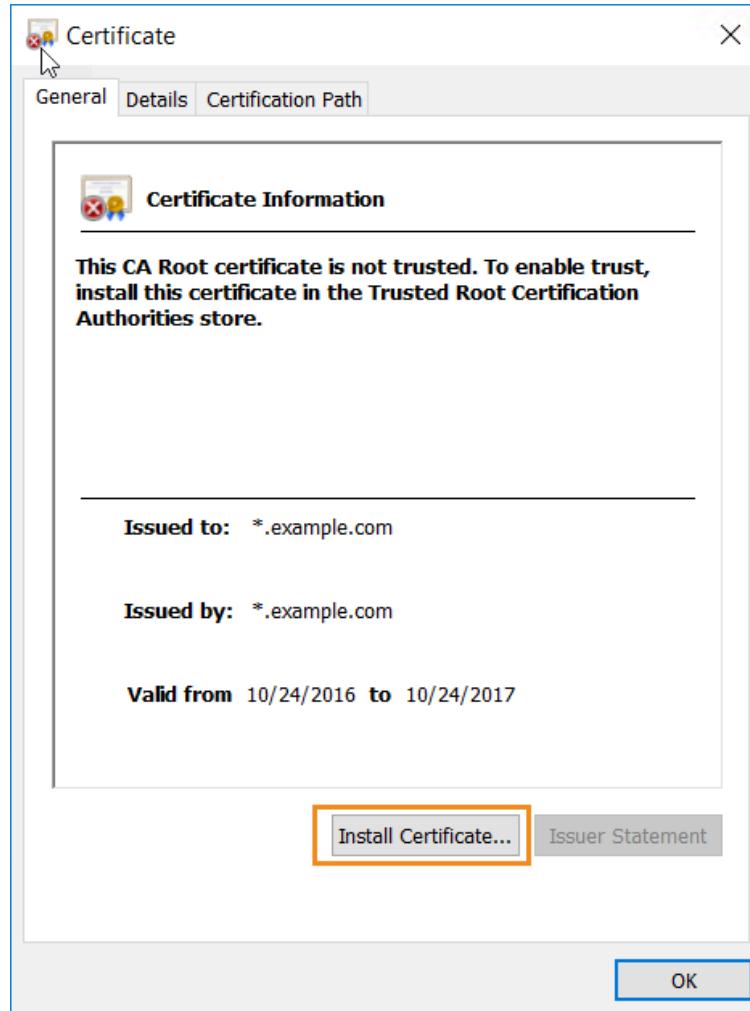


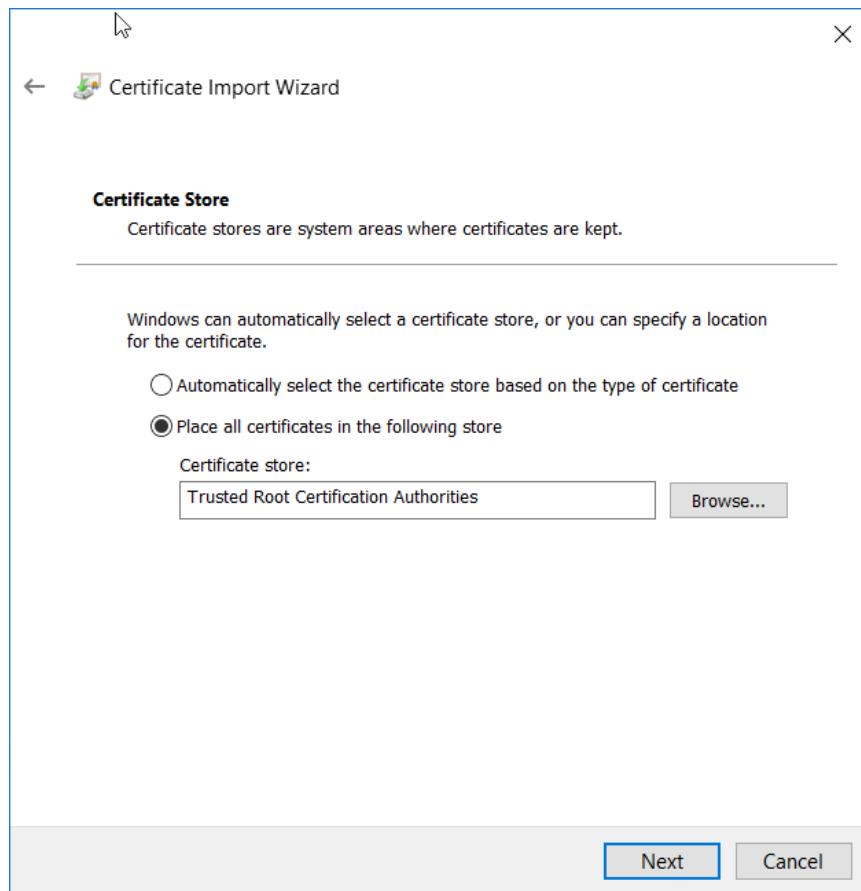
Figure 2.42 Certificate Details

- Step 5. Select **Copy to File** to copy the X.509 certificate .cer file from the Blueframe web server into the local file system. When copying the certificate, use either DER or base64.
- Step 6. After the certificate file is copied to a location within the client machine, open it and select **Install Certificate**, as shown in *Figure 2.43*, to complete the final process of importing the certificate into the local certificate store.



**Figure 2.43 Install Certificate**

Step 7. In the Certificate Import Wizard, select **Place all certificates in the following store**, and select **Browse > Trusted Root Certification Authorities**, as shown in *Figure 2.44*.



**Figure 2.44 Certificate Store Selection Window**

Step 8. Close and re-open your browser and navigate to your Blueframe IP. At this point, you can access the Blueframe node remotely and the web browser will recognize that the connection has been verified. You will no longer see the **Not secure** warning shown in *Figure 2.40*.

**NOTE**

The loaded certificate must be valid, and you must close and re-open the browser for the changes to be recognized by a browser.

## Signing a Blueframe Generated Certificate

A Certificate Signing Request (CSR) contains all the information you entered when generating a certificate. That information is then used by a CA to validate the identity of a Blueframe server. The following process describes how to obtain a CSR to begin the verification process with a Certificate Authority of your choosing:

- Step 1. Locate and select the X.509 certificate for which you need a CSR.
- Step 2. Select  $\equiv$  to view additional options.

Search				
Name	Start Date	End Date	Active	
Default_Web_Cert	2021-01-18T11:00:45Z	2031-01-18T11:00:45Z		

**Figure 2.45 Exporting a CSR**

Step 3. Select **Export CSR** to view a window with the certificate encrypted text. Copy the text into a word processor, such as Notepad, and save it without making any changes.

The screenshot shows a window titled "Certificate Request - Default\_Web\_Cert". The content area contains the following text:

```
-----BEGIN CERTIFICATE REQUEST-----
MIIDHTCCAgUCAQAwgbkxCzAjBgNVBAYTAjVTMRMwEQYDVQQIEwpXYXNoaW5ndG9u
MRawDgYDVQQHEwdQdWxsBFuMQkwBwYDVQQJewAxCTAHBgNVBBETADeMCoGA1UE
ChMjU2Nod2VpdHplciBFbmdpbmVlcmLuZyBMYWJvcmlF0b3JpZXMXGzAZBgNVBAst
EINiY3VyaXR5IFNvbHV0aW9uczEiMCAGA1UEAxMZAHR0cDovL3d3dy5zZWwtc2Vj
dXJlLmNvbTCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBANHJQ7SneMkj
bBLW6pDDnKCrM0u6hAflzilHH5P9c1WzjKu2p0Qda2c3IoUwxpssCUq5kBswUv
nzfYQmda7Pbj67lsSEwX0PC/nvIwYHn+AfN/wWM12Byf8KnQFBm2UYEePUF7Lb
0mCMZu8gQgVsJZUPCVN0IPw7pQv2zNP/2amfmxPKsmv7Mog/MOOdKPyCw2fUNNIA
VsVj0TEKvScTTT7G736/aeErS8pXI40F03QFLb0pKkBKROC5qtOL2/CXOzePIBI
jPCUiOT9CgUWPSZVaRfxSazOSbT1DXTrjpKOOBm7m0H11akITxwVqJUPXyau+c8
OIVgpe418BkCAwEAaAeMBwGCSqGSIb3DQEJDjEPMA0wCwYDVRORBaqAoEAMA0G
CSqGS1b3DQEBCwUAA4IBAQBnRSEyWQUiq+8Ks+PAbwD4s1YsfrCAT66kUZn4kaIo
NcY3Gnm7M4svosdUXjdT6Np75RUVIW+F3tM+/yVwUqyA0gcqY8KIMdTpfpAPZeYT
aqgyhRye2JActgE4l2PsRKaxbH4MGVPdBxwyKWKzj6cq6kiW8ogLaJtkaF3avEC
yBINGXc18hmvEtcqdpXg4Rj6UO7KxqG4w32BQnsom7j4Mskv+aLQxKgHIUZC8q
t5i5LxW+FqaKND9UfjML18zvclLV2+G26KQqncMDPuZoqO93eihHw4qkzLxyaaq
FCOoK9xdrFQR8745A4I7Fzk5pVoEDYhRVj0CaEWUHGS
-----END CERTIFICATE REQUEST-----
```

**Figure 2.46 Certificate Signing Request**

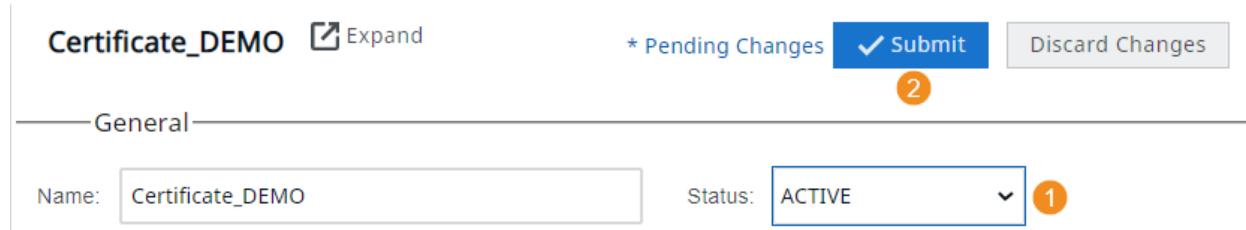
Step 4. Provide the text file to a CA for signing.

## Importing a Verified Certificate Authority Certificate

After a CA gives you a signed certificate, you can import it back into the X.509 certificate that originated the CSR. Once the import process is complete, you can activate the certificate for use on the Blueframe web server. At that point, you no longer see an invalid certificate notification on your browser because the certificate has been verified by a CA.

- Step 1. Obtain a signed certificate from a CA of your choosing.
- Step 2. Open the certificate and copy the encrypted text exactly as it appears on the certificate.
- Step 3. Select the X.509 that was originally used to create the CSR and select  $\equiv$  to obtain additional options.
- Step 4. Select **Import Signed PEM**.
- Step 5. Paste the text you copied in *Step 2* into the Import Certificate window without making any changes.
- Step 6. Select **Submit** to save the changes.

- Step 7. Select the newly generated X.509 certificate on the left side of the Blueframe user interface and change its status to **ACTIVE** in the certificate attributes window on the right side of the interface.
- Step 8. Select **Submit** to save the changes.



**Figure 2.47 Activating a Signed Certificate**

- Step 9. Refresh the browser so that it can recognize the activated certificate.

## Importing a New Certificate

Certain X.509 certificates have a corresponding private key, but they may or may not be signed by a PKI CA or the internal CA of an organization. If signed, you can activate this certificate and it will make the Blueframe node trusted.

Blueframe provides a tool for importing such certificates. Use the following steps to complete that process:

- Step 1. Obtain a PEM certificate, open it in a text editor such as Notepad, and copy its contents without making any changes.
- Step 2. Select  $\equiv$  and select **Import New Certificate**.
- Step 3. In the Import New Certificate window, enter the required information and paste the encrypted text that was copied in *Step 1*.
- Step 4. Select **Submit**.

### NOTE

A password is required only if you are using a private certificate.

**Import New Certificate**

\*Name:  
DEMO

\*Certificate:  

```
subject=/DC=com/DC=page/DC=demo/CN=SEL demo
issuer=/CN=SEL demo
-----BEGIN CERTIFICATE-----
MIIGQDCCBCigAwIBAgITjgAAAAUbWw+7wnTMzgAAAAABTANBgkqhkiG9w0BAQsF
ADAWMRQwEgYDVQQDEwtTRUwgUm9vdCBQTAeFw0xNTEmJjzMDVaFw0zMDEw
MjkyMjMzMDVaMF8xExARBgojkiajk/IsZAEZFgNjb20xFJAUBgojkiajk/IsZAEZ
FgZzZWxpbrMxEjAQBgojkiajk/IsZAEZFgjhZDEcMB0GA1UEAxMTU0VMIEludGVy
bWVkaWF0ZSBQDQTCAIiwDQYJKoZhvcNAQEBBQADggIPADCCAgcCggIBALBF9vmA
QgKAcuY5aSugiDBGjQxoheeimetOuRoNFPe7XNTIA9D9LB7rMAvYDGIAkwAxOFV
QADAgZ7TGrw/HSiUYUx48UKE/ellLT3KoJlVgDZuvN9PbVB+r7DvR61SVYAEZj+
xTMSCILZ12aAwUFnjGdDNTL9XlVoXBikoGRy/Co2w8fjP4aUXY7ntgzW6vojmJ1Q
c08JLfefOcUu/g/LxdX58PHGnbwJxGMOGozVe7iiI6WkgL9cPhRNzXXyLNzktDJ
s2x3d9UFZV4wKajpVChuk9/Ewb4sgU7uPuE2hwoOU4K1ydbc36/d76Dgguy/HBa
ryQzbGpjXC1FUoQs/DuIymikGmYtvWkXOn/9Lus8q8ZwncSiKyrvQgqcW0ZlecM
ukTMwba9yQgVR3mwbtShFYM3NyhUWTGJltxkstjjqMmZXhragRiuUT98VsSbe6QTr
pOlb5ftj6ImdigkVjW+VZikVjSZA+xeFvn94dM+xOTTmbDp4i0ejw1HEDAQcbvFM
eLQkIDbt+qDXpYp1ZCWW+OP3niGDeVOOEhvIK5FFLzYcuJ8P1Ym+F4wDuvse9azdw
X5t+prImZ24grkRdbY9BBnOuB78=
-----END CERTIFICATE-----
```

\*\*Password:  
Enter decryption password

\* indicates required field  
\*\* required only if private certificate

**Submit** **Cancel**

**Figure 2.48 Importing a New Certificate**

Step 5. In the list of X.509 certificates, select the new certificate to view its details. Then, change its status to **ACTIVE** and select **Submit**.

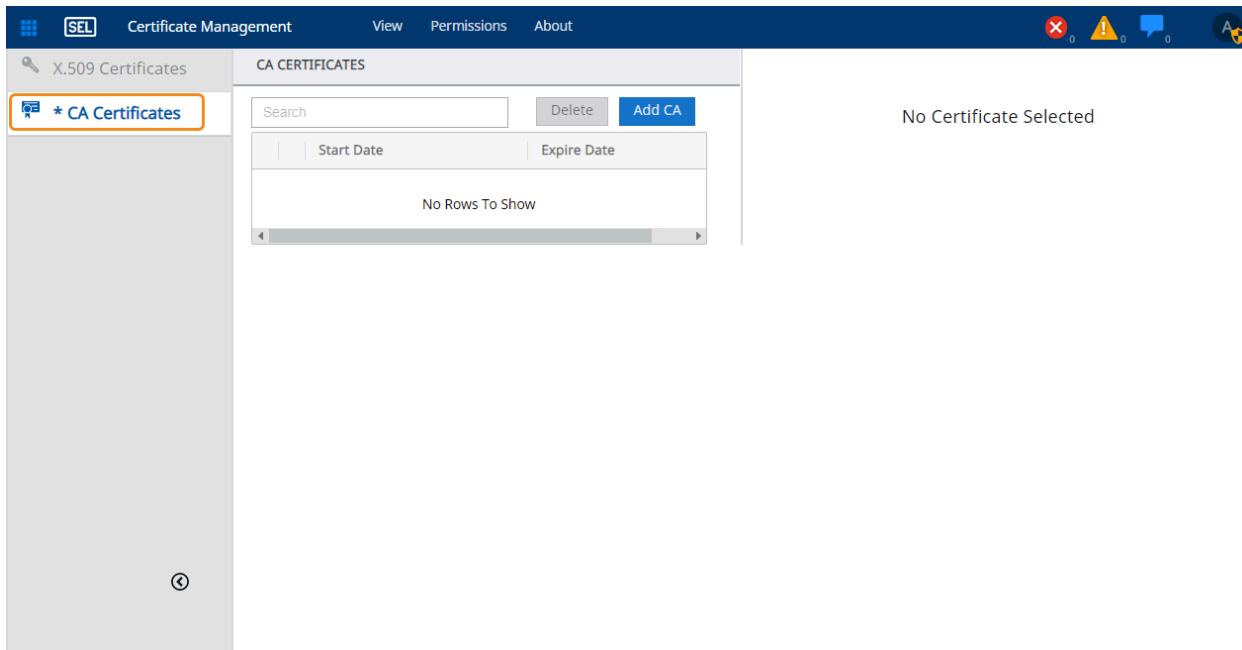
Step 6. Refresh the browser so that it can recognize the activated certificate.

## Certificate Authority Certificates

To establish a trusted connection between a Blueframe web server and a client, a verified CA certificate must be loaded on the Blueframe web server. The following is a brief explanation of certificates and their verification process outside of Blueframe.

During the initial stages of establishing a TLS/SSL encrypted communications session, the web client and server devices exchange public keys. To verify the server's ownership of the public key, CAs digitally sign the certificates used by the server. CA certificates are issued by the CA and contain the public key mathematically related to the private key used to sign an X.509 certificate.

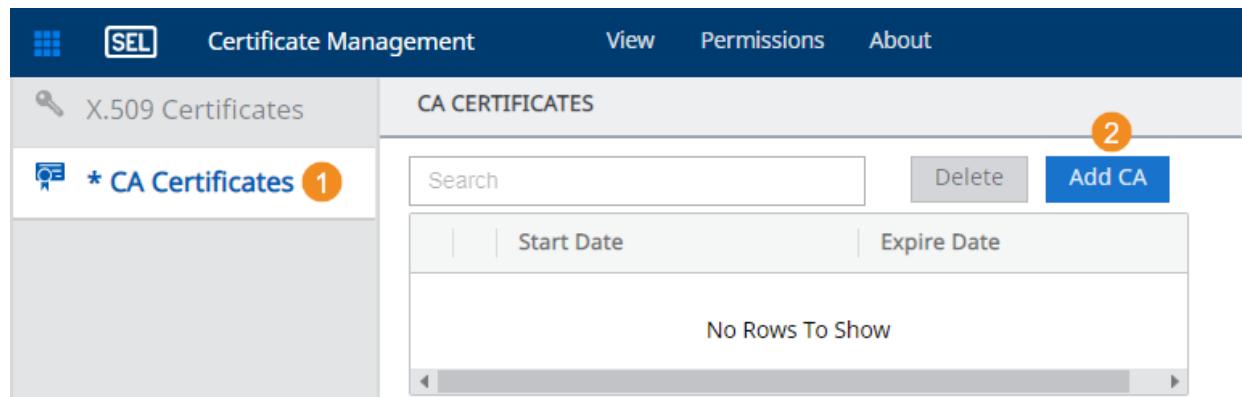
The entity verifying the X.509 certificate cross-references the installed CA certificates to verify that the X.509 certificate is signed by a trusted institution(s). An X.509 certificate may be signed by multiple CAs to create a chain of trust. To successfully validate an X.509 certificate, you must install all CA certificates in the chain of trust in the CA Certificates menu of the Certificate Management tool (*Figure 2.49*).



**Figure 2.49 Certificate Management CA Certificates Menu**

Blueframe provides you with a tool to load CA certificates. Once Blueframe has a trusted certificate, remote connections through a browser will recognize the validity of the CA certificate and you will not see an invalid certificate notification. Use the following steps to load and activate a CA certificate on Blueframe:

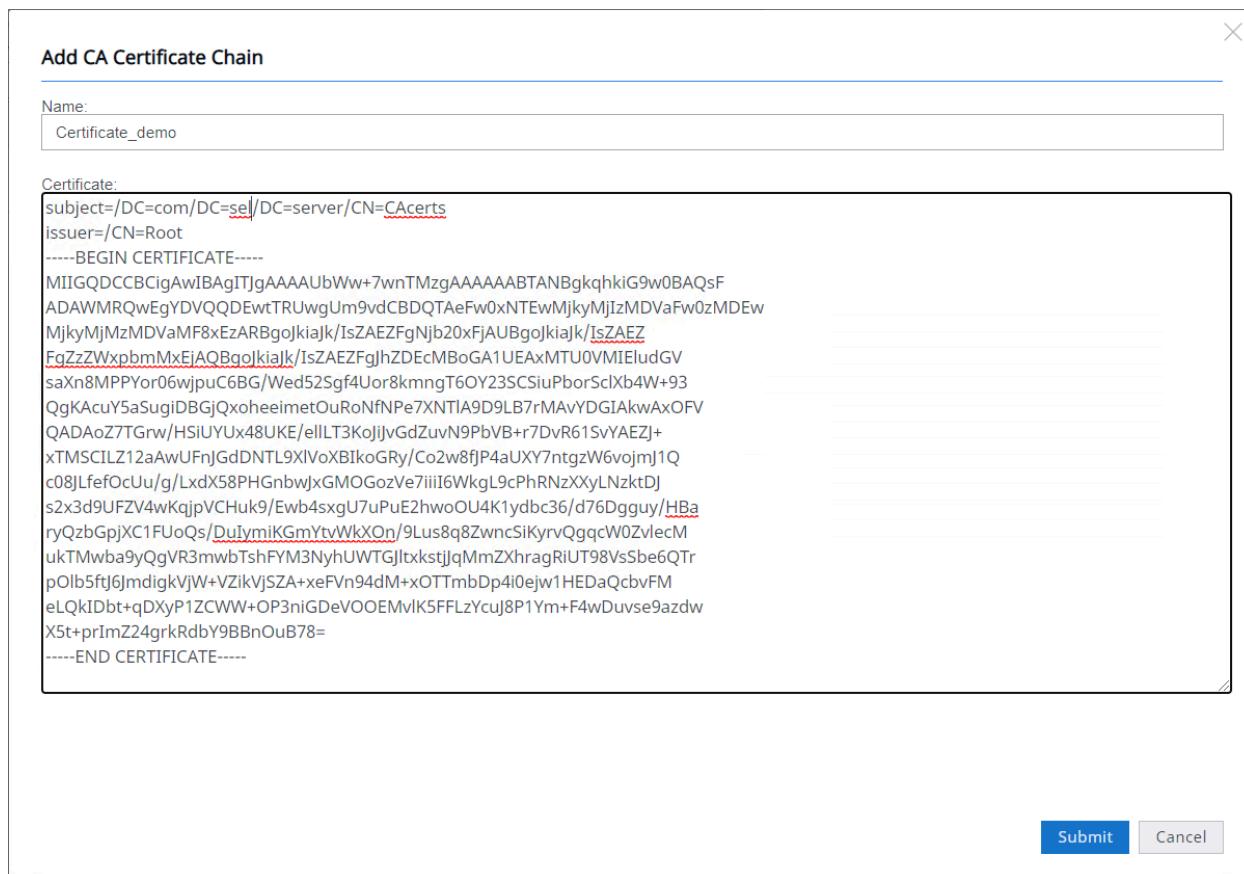
- Step 1. Open the certificate that you obtained from the CA in a text editor such as Notepad and copy its contents without making any changes.
- Step 2. Select **CA Certificates** in the navigation pane and select **Add CA**.



**Figure 2.50 Adding a Certificate Authority Certificate**

Step 3. In the Add CA Certificate Chain window, enter the name of the CA Certificate chain and paste the CA certificate text copied from *Step 1* without making any changes.

Step 4. Select **Submit**.



**Figure 2.51 Add Certificate Chain Window**

Step 5. You will now see an expandable menu next to the certificate you added (Certificate\_demo (2) in this example; however, the name of the menu matches your CA certificate name—see *Figure 2.52*). Expand the menu to view all the certificates in the chain of trust.

CA CERTIFICATES			
Name		Start Date	Expire Date
SEL CA	SE	2015-10-29T22:23:05Z	2030-10-29T22:33:05Z
SEL Root CA	SE	2015-10-29T22:06:01Z	2045-10-29T22:13:33Z

**Figure 2.52 CA Certificates Chain**

- Step 6. Select each of the certificates in the chain to see their encrypted text portions highlighted on the right side of the window.
- Step 7. Select **Submit** to enable the CA certificates on the Blueframe server.

The screenshot shows two windows side-by-side. The left window is titled 'CA CERTIFICATES' and lists two entries: 'SEL Intermediate CA' (selected) and 'SEL Root CA'. The right window is titled 'Certificate\_demo' and shows a certificate submission form. The certificate text is displayed in a large text area, with several lines of text highlighted in blue, indicating selected portions of the certificate chain. A 'Submit' button is visible at the top right of the right window.

**Figure 2.53 Submitting a CA Certificate**

## Central Authentication



**Figure 2.54 Central Authentication Icon**

Within Blueframe, use the Central Authentication management tool to configure Lightweight Directory Access Protocol (LDAP) or RADIUS parameters for connection with a central authentication server. The remote server can be used to manage access to Blueframe with roles defined on Blueframe.

Although you can configure Blueframe to have local user accounts, it also supports central authentication so that users who lack a local Blueframe account can use their central authentication credentials to access a Blueframe node.

### NOTE

LDAP is a powerful and flexible protocol that allows for fast information lookups from servers that are optimized for read access.

### NOTE

The information stored on LDAP servers can be any type of record-based information that is stored in a directory structure. Examples include user and device lists, phone books, and recipes.

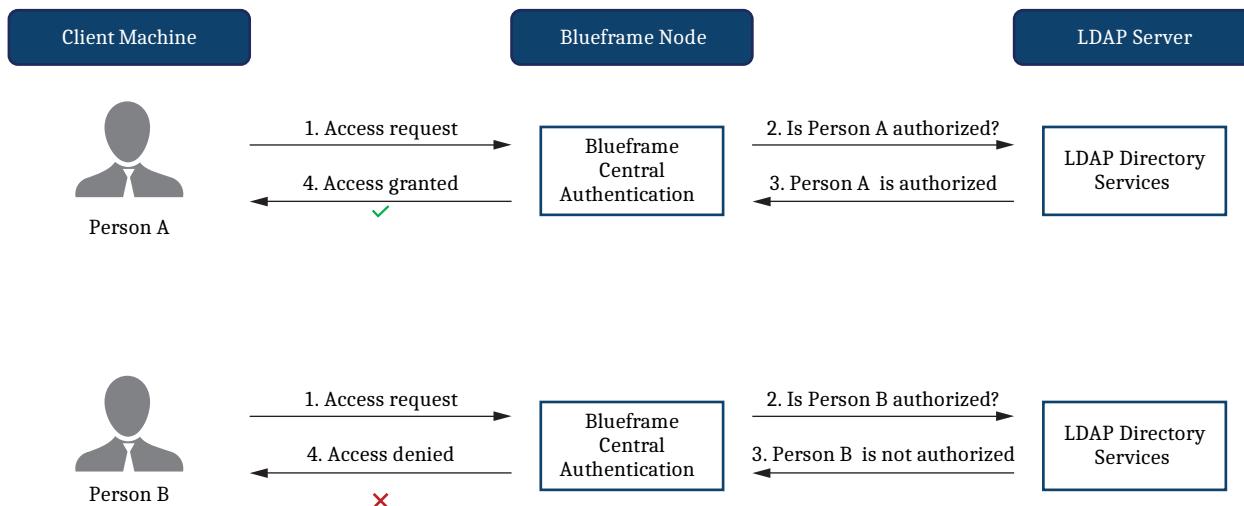


Figure 2.55 LDAP Login Process

## Configuring LDAP Settings

Blueframe provides a list of parameters necessary for use of the central authentication LDAP provides. *Figure 2.56* shows some of the user interface items that must be entered for a successful LDAP configuration. Subsequent sections describe each of the fields in more detail.

### NOTE

Provide Table 2.2 to your LDAP administrator to obtain the necessary information.

The screenshot shows the "LDAP Settings" configuration page under the "Central Authentication" section of the Blueframe Management Tools. The left sidebar includes "SEL", "Central Authentication", "View", "Permissions", and "About". The main area has tabs for "LDAP Settings" (selected) and "Group Maps".

**LDAP SETTINGS**

**General**

- Enable LDAP:
- Search Base:
- Group Filter:
- Paging Size:  (must be less than the LDAP server search size limit)
- User ID Attribute:
- Group Member Attribute:
- Server Synchronization Time:  Hours (0 is every request)

**Directory Access Authentication**

Anonymous Bind    Unauthenticated Bind    Authenticated Bind

Figure 2.56 Central Authentication LDAP Settings

## General LDAP Settings

Use the general settings as shown in *Figure 2.57* and described in the subsequent text for enabling LDAP and modifying certain settings.

The screenshot shows a configuration interface for LDAP settings. At the top, a header reads "General". Below it, several fields are listed with their current values:

- \* Enable LDAP: A toggle switch is turned on.
- \* Search Base: ou=global,dc=rdtest,dc=local
- Group Filter: (|(objectClass=organizationalUnit)(|(objectClass=container)(objectClass=group)))
- Paging Size: 500 (must be less than the LDAP server search size limit)
- User ID Attribute: sAMAccountName
- Group Member Attribute: memberOf
- Server Synchronization Time: 1 Hours (0 is every request)

**Figure 2.57 General LDAP Settings**

**Search Base:** You can consider the LDAP Search Base as the root directory from which you begin your user search. Form this by listing all the components of the search base separated by commas and going from the most specific component to the broadest component. In *Figure 2.57*, the Search base configuration is ou=global,dc=rdtest,dc=local. In this search base, dc refers to the domain component. The domain components combine with “;” to create the search domain. In this case, the search domain is rdtest.local. The “ou” component is the organizational unit, or directory, from which to begin the search. You can interpret this search base as “Start the search from the Global directory residing on an LDAP server in the rdtest.local domain.”

**Group Filter:** A filter used to search for groups and obtain narrower results.

**Paging Size:** Determines the size of a page. This setting must be less than the LDAP server search size limit.

**User ID Attribute:** An LDAP label that identifies the usernames of system users.

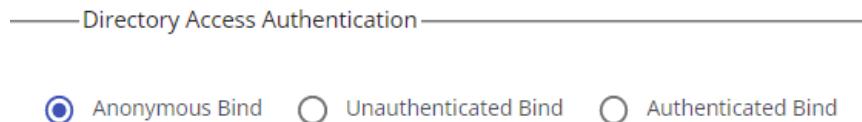
**Group Member Attribute:** An LDAP label that identifies the groups of users.

### NOTE

Ensure that the User ID and Group Member attributes are entered correctly. Blueframe cannot determine which LDAP fields to search for usernames or privileges if the attributes are incorrect.

**Server Synchronization Time:** This option exists to reduce the overhead (such as attributes and role mappings) associated with pulling account information from an LDAP server. You can use hour increments in configuring this so that Blueframe synchronizes with an LDAP server at the set number of hours. Setting this time to 0 causes Blueframe to synchronize every time a user logs on.

## Directory Access Authentication



**Figure 2.58 Directory Access Authentication**

**Anonymous Bind:** Anonymous binds forgo the use of service accounts to access an LDAP server.

**Unauthenticated Bind:** If an LDAP server has this option enabled, a user can access that LDAP server without using a password. This setting only requires a Bind DN.

**Authenticated Bind:** Authenticated binds use a service account to access the LDAP server. If the LDAP service account is revoked, or if the password expires, Blueframe cannot access the LDAP server, and centralized users cannot access the Blueframe node. This setting requires a Bind DN and a Bind Password.

## LDAP Server Settings

The screenshot shows the "LDAP Server Settings" section with two entries: "Server 1" and "Server 2".

**Server 1:**

- \* Enabled:
- Hostname:
- Port:
- CA Certificate:

**Server 2:**

- Enabled:
- Hostname:
- Port:
- CA Certificate:

**Figure 2.59 LDAP Server Settings**

**Hostname:** The hostname for an LDAP server in this field can either be the IP address or hostname string of the server.

**Port:** The port through which you communicate with the LDAP server. LDAP uses Port 389 by default unless your LDAP administrator specifies a different port number.

**CA Certificate:** Use this drop-down menu to select the CA certificate for the LDAP server.

**NOTE**

LDAP requires X.509 authentication to create binds between the server and client. This ensures that attackers do not spoof the authentication server to gain unauthorized access. Blueframe requires that the root certificate of the LDAP servers certificate chain be stored locally. See the instructions in Certificate Authority Certificates on page 59.

**NOTE**

Blueframe allows as many as two LDAP servers for redundancy and increased availability. Blueframe assigns a priority to each LDAP server and queries the servers in their order of priority until it identifies the user attempting to access Blueframe, or until it exhausts the list.

## LDAP User Attribute Maps

Blueframe can pull user attributes from your LDAP server and store those attributes on the local machine. To map your LDAP attributes, enter the appropriate LDAP attributes into the text fields of the User Attribute Maps (see *Figure 2.60*). These settings are optional. Use *Table 2.2* to obtain this information from your LDAP administrator.

User Attribute Maps	
First Name:	givenName
Last Name:	sn
Email:	mail
Telephone:	homePhone

**Figure 2.60** User Attribute Maps

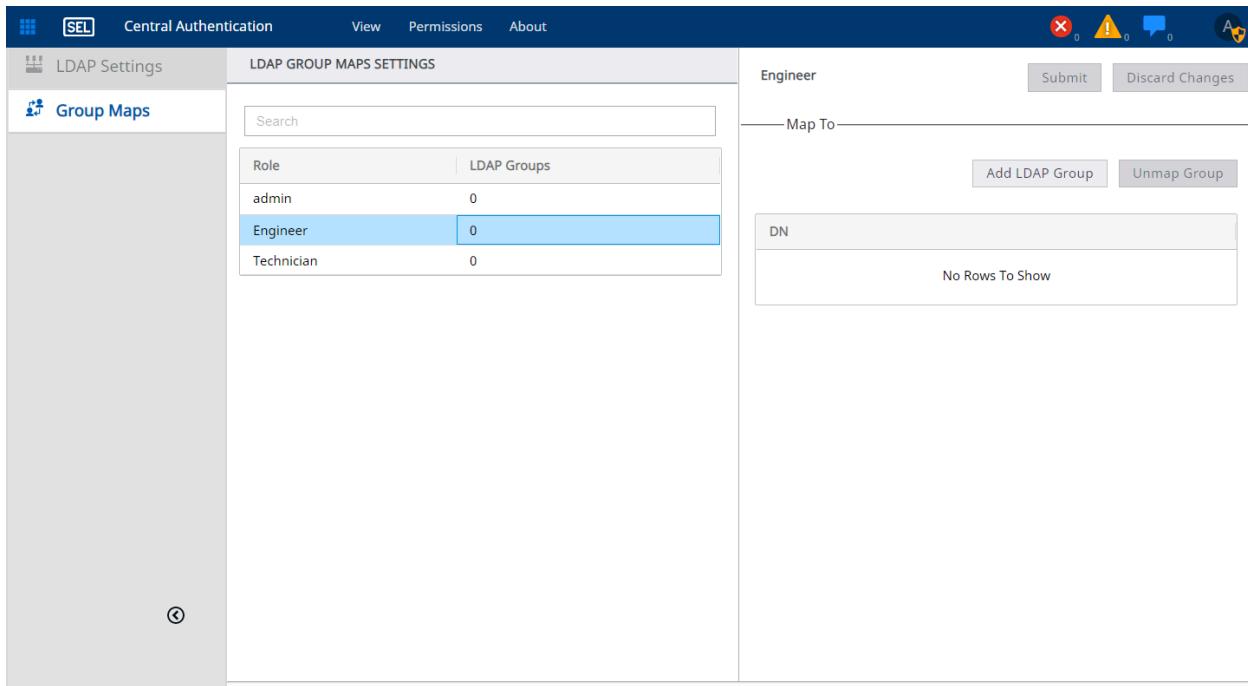
**Table 2.2** LDAP Parameters

General	
Attribute Name	
Search Base	
Group Filter	
Page Size	
User ID Attribute	
Group Member Attribute	
Server Synchronization Time	

Directory Access Authentication		
Attribute Name	Description	
Anonymous Bind		
Unauthenticated Bind	Requires Bind DN	
Authenticated Bind	Requires Bind DN and Password	
Servers		
Attribute Name		
Hostname or IP for server 1		
Port for server 1		
Hostname or IP for server 2		
Port for server 2		
User Attribute Maps (optional)		
Attribute Name		
First Name		
Last Name		
Email		
Telephone		

## Group Maps

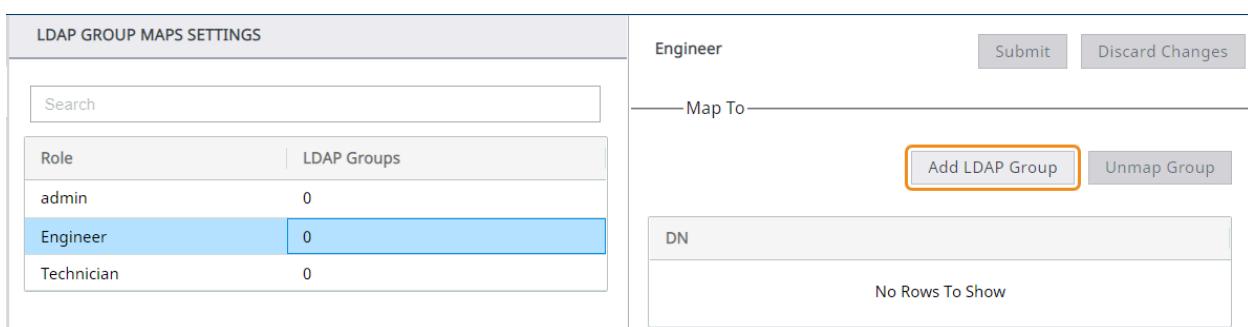
After you enter LDAP parameters into Blueframe, you can use the Group Maps section to manage your LDAP groups on a per-role basis. Use the group maps for specifying which specific user groups of your organization have access to Blueframe. *Figure 2.61* displays the default menu for managing Group Maps.



**Figure 2.61 Central Authentication Group Maps**

Perform the following steps to learn details on how to add a group map.

- Step 1. From the LDAP Group Map Settings menu, select the role to which you want to add LDAP groups.  
  
After this selection, the group map configuration displays on the right side of the window.
- Step 2. Select **Add LDAP Group** to begin the process of associating a group with the role. *Figure 2.62* shows an example for the **Engineer** role.



**Figure 2.62 Adding an LDAP Group to a Role**

- Step 3. The Select LDAP Group window shown in *Figure 2.63* automatically populates a list of available LDAP groups that your Blueframe node can access based upon your search base. Once you have selected a DN, select **Add**.

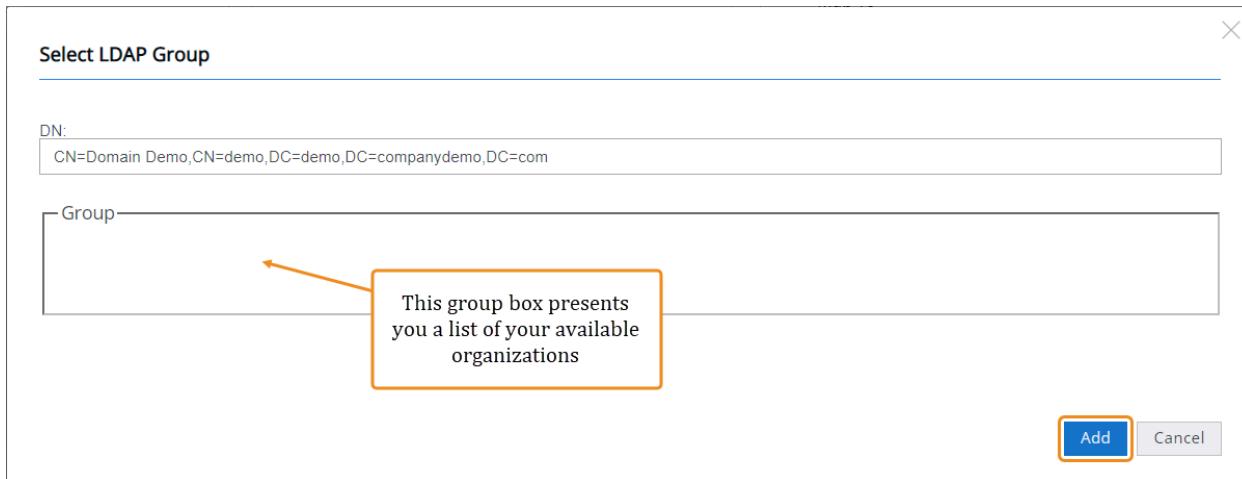


Figure 2.63 Select LDAP Group

Step 4. The DN for the LDAP group you selected displays in the list of LDAP groups (as shown in *Figure 2.64*). Select **Submit** to save all changes. Note that unsaved changes are highlighted with a blue asterisk symbol.

The screenshot shows the 'LDAP GROUP MAPS SETTINGS' page. On the left, there's a table with columns 'Role' and 'LDAP Groups'. It contains four rows: 'admin' (0), 'Engineer' (0, highlighted with a blue background), 'Technician' (0). To the right of the table is a section titled 'Map To' with buttons for 'Add LDAP Group' and 'Unmap Group'. Below this is a 'DN' input field containing the value '\* CN=Domain Demo,CN=demo,DC=demo,DC=companydemo,DC=com'. At the top right of the page are three buttons: 'Engineer', '\* Pending Changes' (highlighted with a blue border), 'Submit' (highlighted with a blue border), and 'Discard Changes'.

Figure 2.64 Submitting LDAP Group Changes

## RADIUS Configuration

Blueframe supports the basic NAS client authentication functionality of the RADIUS protocol. By configuring the RADIUS settings, you can log in using credentials not stored on the RTAC.

SEL cannot guarantee that the device will be compatible with all possible RADIUS server architectures and implementations. Configure communications with a RADIUS server on the RADIUS Settings page in the Central Authentication application.

The screenshot shows the 'RADIUS SETTINGS' configuration page in the Blueframe Central Authentication interface. The left sidebar has tabs for SEL, Central Authentication, View, Permissions, and About. The 'RADIUS Settings' tab is selected. The main area contains the following fields:

- Enable RADIUS:** A toggle switch is turned on.
- \* Primary Server Host/IP:** exampleRadiusServer.com
- Primary Server Port (UDP):** 1812
- \* Backup Server Host/IP:** backupServer.com
- Backup Server Port (UDP):** 1812
- \* RADIUS Shared Secret:** (redacted)
- \* Confirm Shared Secret:** (redacted)
- \* Authentication Types:** EAP-TTLS/PAP
- Connection Timeout (in seconds):** 2
- Prevent Sending Unencrypted Username:** A toggle switch is turned on.
- \* CA Certificate:** radius CA Cert
- NAS Identifier:** edapt-node-35522243614045969443
- NAS IP Address:** 10.202.27.179
- Use LDAP For Group Mappings:** A toggle switch is turned off.
- Enable Logging:** A toggle switch is turned on.

At the bottom left is a back arrow icon, and at the bottom right is a blue 'Dictionary' button with a downward arrow icon.

**Figure 2.65 RADIUS Settings**

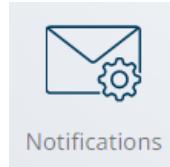
**Table 2.3 RADIUS Settings in Blueframe**

Setting Name	Description
Enable RADIUS	Turn this toggle on to enable RADIUS authentication.
Primary Server Host/IP	Enter the IP address or hostname of the RADIUS server.
Primary Server Port (UDP)	The UDP port on which Blueframe will attempt to contact the Primary RADIUS server. The port range is 1024–65534.
Backup Server Host/IP	(Optional) If populated, when the RADIUS client is unable to exchange information with Primary server, the Backup server will be contacted.
Backup Server Port (UDP)	(Optional) The UDP port on which the RTAC will attempt to contact the Backup RADIUS server. The port range is 1024–65534.

Setting Name	Description
RADIUS Shared Secret	The Shared Secret is a string that is determined by the RADIUS server and must match in order for authentication requests to be successful.
Authentication Types	The method Blueframe uses to communicate with the RADIUS server. The options are PAP, EAP-PEAPv0/MSCHAPv2, and EAP-TTLS/PAP. When selecting an EAP method type, Blueframe will require the full CA certificate chain for the RADIUS server. This certificate will be imported on the CA certificates in the Certificate Management application.
Connection Timeout	This is the time Blueframe will wait for the RADIUS server to respond to an authentication request. Blueframe will attempt to connect to the Primary server three times before waiting for the connection time-out period. If Blueframe does not receive a response, then Blueframe will attempt to authenticate and repeat this process with the Backup server if configured. The range is 1–10 seconds.
Prevent Sending Unencrypted Username	Turn this toggle on to hide usernames by using "anonymous" as the username when sending requests to the RADIUS server. When this is enabled, the actual username is sent in the encrypted portion of the message.
CA Certificate	Select the CA certificate that was added to the Certificate Management application.
NAS Identifier	The hostname that acts as the RADIUS client.
NAS IP Address	The IP address of the Blueframe network interfaces that the RADIUS client uses.
Use LDAP For Group Mappings	Use LDAP configuration to retrieve a user's mapping to Blueframe role type.
Enable Logging	Turn this toggle on to log diagnostic information to System Settings > Dashboard > All namespaces > Pods > Core Services.

The Blueframe SEL RADIUS Dictionary can be downloaded from the RADIUS Settings page. The dictionary lists all current account types configured on Blueframe, including both default roles and custom roles. This file defines the SEL vendor-specific attributes that must be defined on your RADIUS server and are used by your device to appropriately grant or restrict privileges for users.

## Notifications



**Figure 2.66 Notifications Icon**

Blueframe supports emailing data from supported applications through an SMTP server. To identify if an application supports email notifications, check the related application's documentation.

The Notifications application enables the creation of email recipient groups. Define the appropriate email recipients for a group and the email server to be used for outbound messages. Once configured, supported applications can be configured to send emails to the specified recipient groups.

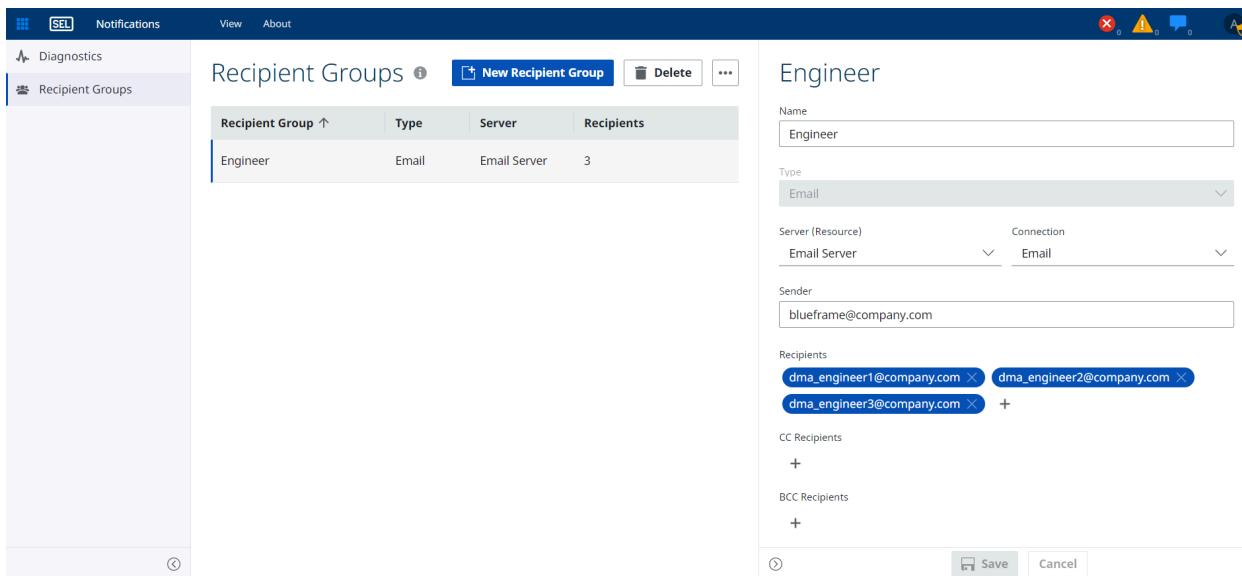


Figure 2.67 Recipient Group Configuration

## Configure a Recipient Group

Note that an SMTP server connection must exist in Resource Management to configure recipient groups.

Step 1. With Notifications launched, select the **Recipient Groups** tab.

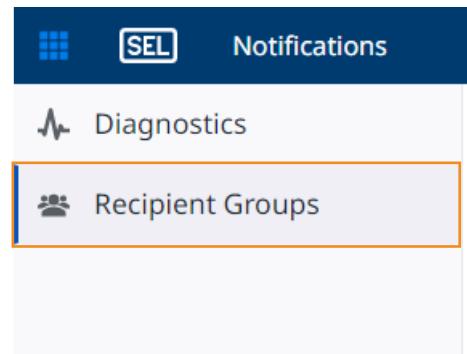


Figure 2.68 Recipient Groups

Step 2. Select **New Recipient Group** to launch the configuration dialog. Enter the appropriate configuration information, as shown in *Figure 2.69*.

New Recipient Group X

Select a valid SMTP server that was defined in Resource Management.

Name \*

Specify a valid email address from which messages are sent.

Type \*

Server (Resource) \*  Connection \*

Sender \*

Add the email addresses of the users that shall receive the email.

Recipients \*   +

CC Recipients +

BCC Recipients +

\*Required Create Cancel

**Figure 2.69 Define a New Recipient Group**

Step 3. Select **Create** and proceed to configure email notifications from the supported application.

**This page intentionally left blank**

## SECTION 3

# Resource Management

## Overview



**Figure 3.1 Resource Management Icon**

Blueframe uses data from multiple network resources throughout its applications. Use the Resource Management tool to define data resources within Blueframe. You can employ data resources such as an RTAC, relay, meter, switch, or other IED devices. Additionally, a resource can also be a remote database or a Blueframe node. Each resource has its own connection methods and attributes that, once defined, can be used throughout Blueframe applications. In Blueframe, you only need to define a resource in the Resource Management tool.

## Resource Management Navigation and Filtering

The screenshot shows the Blueframe Resource Management interface. The top navigation bar includes 'SEL' and 'Resource Management' along with 'View' and 'About' options. The main window is titled 'All Resources' and contains a search bar and a 'New Resource' button. On the left, there's a 'Resources' sidebar with sections for 'All Resources' (including .dma-credential-management-sys, MMS, RTACs, Switches, Z1, Z2, Z2\_WNW\_CV, Z2\_WSW\_MD, Local Node), 'Saved Filters' (Z2\_SEL-451-2 (3)), 'SEL-3XX', and 'Z2 Resources' (Z2\_SEL-451-4 (2), SEL-451-5, SEL-487B, Z2\_SEL-487B-1, Z2\_SEL-487B-1 (2), Z2\_SEL-487E). A 'Resources Filters' section is also present. The central area displays a table of resources with columns for name, company, globalDeviceId, and model. One row is selected, showing detailed information in a right-hand panel: Name (Z2\_SEL-351S-6), Attributes (alias: 37a31632651c4807998..., company: company, globalDeviceId: 37a31632651c4807998..., model: SEL-351S-6, nomFreq: 60, station: station, tz: US/Pacific), Labels (37a31632651c4807998a5a75b554581e), and Connections (Z2\_SEL-351S-6, Protocol: SEL, Method: TunneledSerial, Host: 10.203.123.39, Port: 23). A 'Search Bar' is highlighted in the table header.

**Figure 3.2 Resource Management Components**

## Navigation Tree

The navigation tree provides the means for arranging and grouping resources in a folder structure to meet your needs. Select the new folder  icon to create a new folder within the navigation tree. Once created, select and drag resources to the desired folder to achieve a custom arrangement, as shown in *Figure 3.3*.

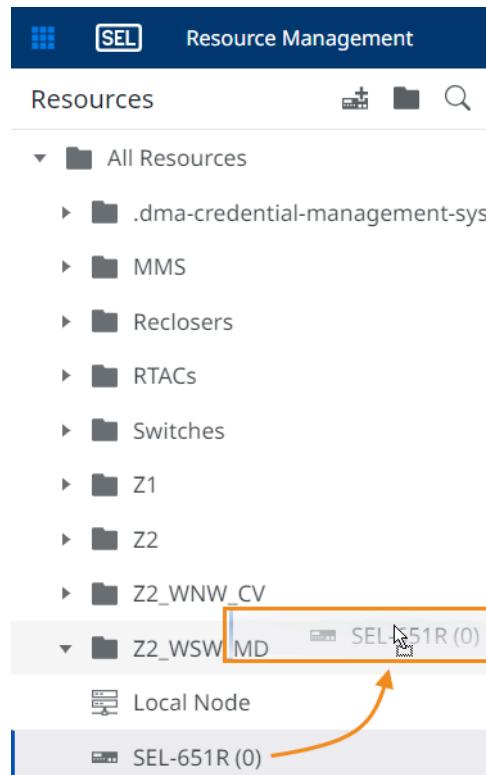


Figure 3.3 Dragging a Resource Into a Folder

## Resource List

The Resource Management tool provides a list of all defined resources within Blueframe. You can sort this list by selecting folders in the navigation tree or by using the search bar.

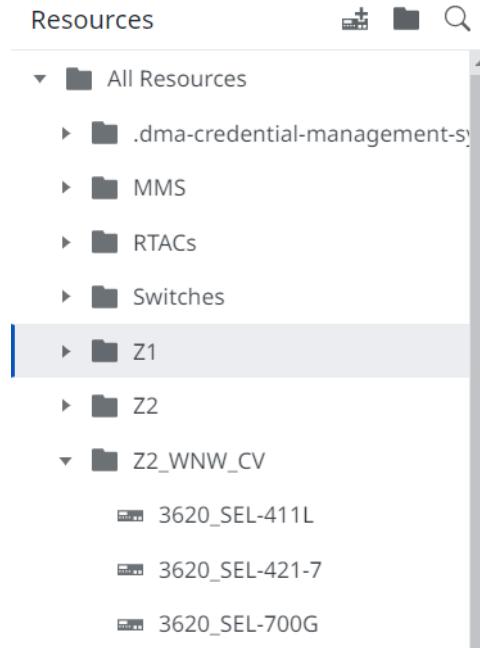


Figure 3.4 Navigation Tree Folder Sorting

## Search Bar

The search bar within Resource Management provides you with flexible options to obtain a selective list of resources. Type full or partial non-case-sensitive terms to obtain filtered results. In addition to the search bar, each column within the resource list offers filtering options to further define a filter by selecting or deselecting items, as well as advanced search capabilities.

The screenshot shows the Resource Management interface with a search bar containing 'SEL-3'. A blue arrow points from the search bar to the search icon in the toolbar above the table. Another blue arrow points from the search term 'SEL-3' to the first row of the table, which contains the name 'Z1\_SEL-3D0G\_2'. The table has columns for 'name', 'company', and 'globalDevId'. The 'name' column is currently sorted, as indicated by the ascending arrow icon above it. The table also includes a header row with column names.

name	company	globalDevId
Z1_SEL-3D0G_2	company	419c393f1b
Z1_SEL-311C-1	company	3a7fe3fa93
Z1_SEL-311C-2	company	3d9395b56
Z1_SEL-311C-3	company	cd4d8de3f3
Z1_SEL-351-2	company	f0b2b836e9
Z1_SEL-351A-1	company	cb3761422f

Figure 3.5 Resource Management Filters

## Adding a New Resource

Select New Resource to add a device or data source to Resource Management.

The screenshot shows a user interface for managing resources. At the top left is a label 'Z1'. To its right is a search bar with the placeholder 'Search...'. Further to the right is a blue button labeled 'New Resource' with a plus sign icon. To the far right is a small three-dot menu icon. Below this header is a table with four columns: 'name', 'company', 'globalDeviceId', and 'model'. The table contains two rows of data:

name	company	globalDeviceId	model
Z1_SEL-2032	company	77d36b15b9884ada9205c...	SEL-2032
Z1_SEL-2411	company	d647110a1ec54a2193a6bc...	SEL-2411

**Figure 3.6 Adding a New Resource**

The New Resource window offers options for a quick definition of a resource. The character string entered in the Name field is the name that will be used for that Resource throughout the Blueframe system. Additionally, you can define custom attributes for the resource, which are visible in the Resource Overview. Add labels to the resource to facilitate searching for it with filters throughout Blueframe. The Group field is used to specify the folder in which you want the resource to exist. However, you can leave the field blank if you do not want the resource to be in any particular folder. The Presets found within the Attributes section provide predefined attributes that simplify configuration of resources for use by applications within Blueframe. *Figure 3.7* shows an example that uses the DMA preset.

The screenshot shows the 'New Resource' dialog box. At the top, there is a 'Name' field containing 'SEL-RTAC\_3555'. Below it is a 'Parent Folder' dropdown set to '/Z1'. Under 'Attributes', a dropdown menu is open with 'DMA' selected. A table below lists resource attributes:

globalDeviceId	RTAC_3555
model	SEL-3555
tz	America/Los_Angeles
nomFreq	60
station	North
company	SEL

Below the attributes is a 'Labels' section with a '+' button and a 'Create Another' checkbox. At the bottom right are 'Create' and 'Cancel' buttons.

**Figure 3.7 Defining a New Resource**

If you desire to create more than one resource at a time, select the **Create another** check box and the window will remain open until all the desired resources have been added. When done, close the window to return to the resources list.

Once you have a resource in your list of resources, you can arrange them by creating a series of folders under the navigation tree.

## Resource Details

Define additional resource properties by double-clicking the resource of interest from the resource list to launch its overview window. The resource provides you with separate tabs for configuring its overview, setting its connection parameters, and Direct Resource Access sessions, as shown in *Figure 3.8*.

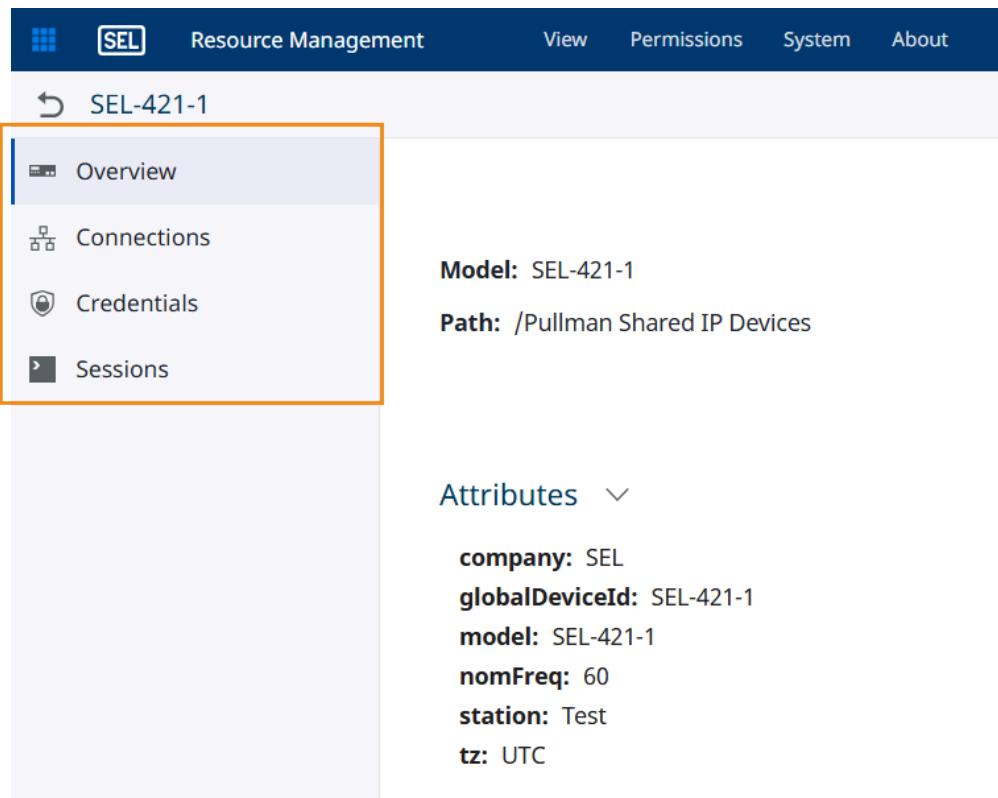


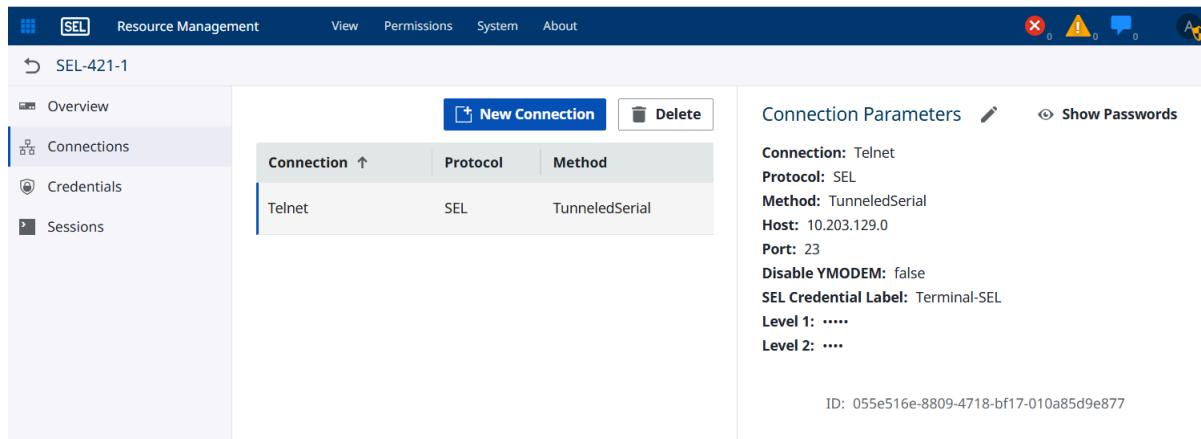
Figure 3.8 Resource Overview

## Overview

The Overview tab provides options to name the resource and add attributes and labels. To make changes in the Value column, select the field you want to modify. The path is defined by the folder hierarchy structure defined in the navigation tree. Additionally, you can add optional custom attributes that provide further details about the resource by selecting the **Add Attributes** button. You can also create custom labels by selecting the **Add Label** button for category grouping to facilitate resource discovery throughout Blueframe applications.

## Connection Settings

The Connection Settings tab provides parameters for configuring the physical connection between the resource and the Blueframe node. The following includes descriptions of each field.

**Figure 3.9 Connection Services**

**Connection Name:** A custom-defined descriptive string for your connection, which is used throughout the Blueframe system.

**Protocol:** *Table 3.1* describes the available protocols and when they should be selected for use.

**Table 3.1 Connection Protocol Options**

Protocol	When to Select
COMPROC	COMPROC is used when communicating to a device located behind a communications processor for direct or direct transparent communications.
DNP/Serial DNP	DNP over Ethernet and serial provides SCADA connectivity for outstation data collection.
FTP/FTPS	FTP is used in making connections to supported non-SEL devices for file transfer. FTPS is used for secure FTP connections, where supported.
HTTP/HTTPS	HTTP/HTTPS is used for connections to web servers.
MMS	MMS is used for file transfer from IEC 61850 MMS supported resources.
POSTGRESQL	PostgreSQL is used for connections to supported databases, such as when connecting to the RTAC database.
SEL-3620 SSH	SEL-3620 SSH should be used when connecting to an SEL security gateway or any managed IED behind an SEL security device.
SEL-3620 TCP	SEL-3620 TCP is used for TCP Ethernet connections to SEL security gateways.
SEL-3620 Telnet	SEL-3620 Telnet is used for Telnet Ethernet connections to SEL security gateways.
SEL over SSH	SEL over SSH is used for SSH connections to supported SEL devices, such as the SEL RTAC.
SEL over Telnet	SEL over Telnet is used to make TELNET connections to SEL devices.
SEL over TCP	SEL over TCP is used when serial to Ethernet converters or other SEL devices are using raw TCP connections.
SEL with FTP	SEL with FTP is used for file transfer from SEL IEDs.

Protocol	When to Select
SFTP	SFTP is used for secure and encrypted file transfers, where supported.
SMTP/SMTPS	SMTP or SMTPS is used for configuring email server settings for use with notifications.
SEL Client Serial	SEL Client Serial is used for serial connections to SEL client devices.
TERMINALGATEWAY	TERMINALGATEWAY is used for custom scripted connections to an SEL resource that are passed through a gateway resource.

## Additional Protocol Settings

- **Type:** Describes the transport method in use for the connection.
- **Gateway Authorization:** Select when the gateway devices are configured to require additional authentication.
- **COMPROC Type:**
  - Select **Legacy** when using an SEL-2020, SEL-2030, or SEL-2032 Communications Processor.
  - Select **RTACSELServer** when communicating through an SEL RTAC Server.
  - Select **RTACAP** when communicating through an SEL RTAC Access Point Router.
- **First/Second Delay Time:** Match with the timeout settings of the communications processor.
- **Termination String:** This is the command sent while communicating through a communications processor to terminate the connection to the device and return to the communications processor prompt. This should be in decimal form, e.g., \004.
- **Port Aux Power:** Enables power output from the connected port.
- **RTS/CTS:** Enables hardware flow control.
- **Xon/Xoff:** Enables software flow control.
- **Disable YMODEM:** Enables interleaved transfer of device data. Note that only some devices support the use of NO YMODEM, and it is recommended that users have an understanding of what data types can and cannot be transferred via NO YMODEM with the configured devices.
- **Host:** The IP address of the resource. For the connection to succeed, the resource must be in a network reachable by the Blueframe node.
- **Port:** The communications port that is used for the connection with the resource.

### NOTE

When you perform a listening operation with an RTAC for event or settings notifications with DMA, the POSTGRESQL port on the RTAC is 5432. You must use this port number to achieve successful listening operations. If your network has port mapping, this port automatically changes to something else.

- **Database:** This setting is unique to the POSTGRESQL protocol. Because it is used for database connections, you must specify the name of the database to which you are connecting.

**NOTE**

To connect to the RTAC database, set the Database communication setting to **3530**.

- **Credentials:** Requires you to enter a valid Username and Password to access the resource and establish a connection.
- **Child Resources:** These are resources that are accessed through the communication connection being configured with the COMPROC, POSTGRESQL, or SEL-3620 SSH protocol. Each child resource must have a globalDeviceId configured to be added on a parent communication connection.

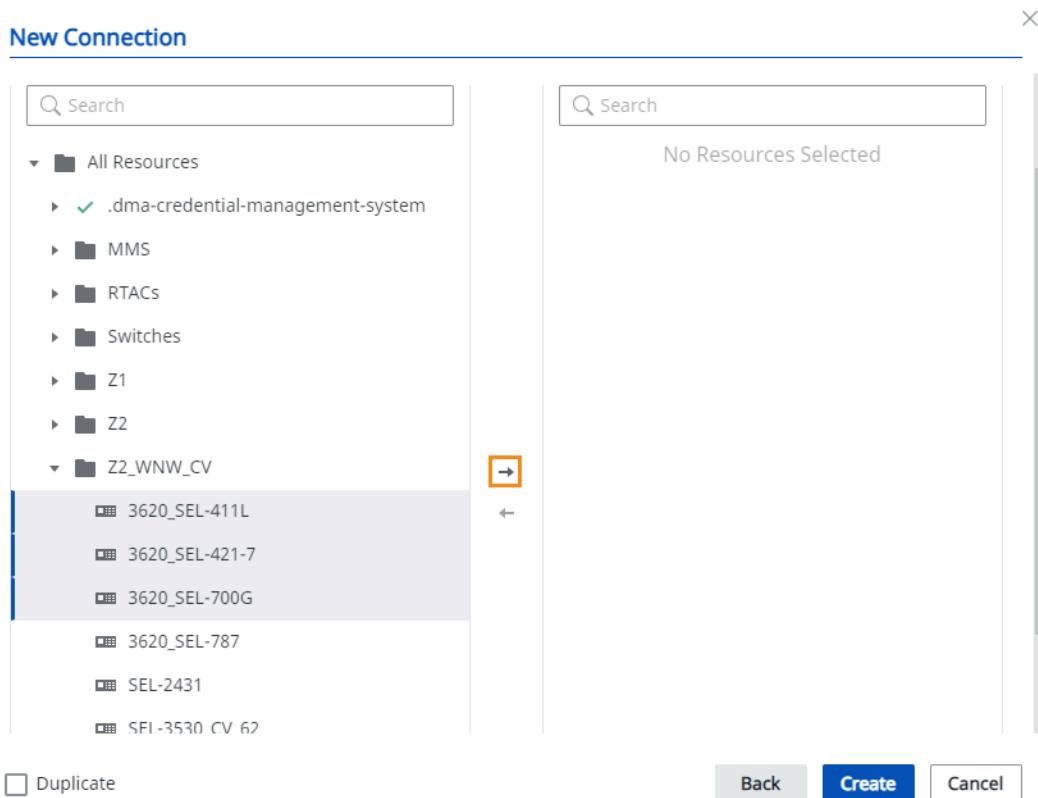
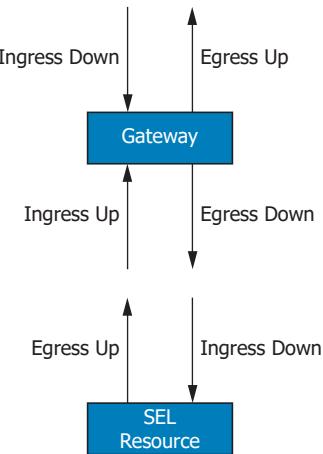


Figure 3.10 Child Resource Assignment

- **Scripted Access:** This checkbox is available on the Terminal Gateway connection type and enables ingress and egress scripts for defining how communications can be navigated to and from the gateway resource. *Figure 3.11* visually represents the ingress and egress scripts. The Log Details checkbox will turn on logging of the back and forth communications. SEL recommends that this box is checked during commissioning to facilitate troubleshooting of the scripts and then unchecked when the system is deployed to a production environment as it is possible that passwords may be sent in plaintext according to how the custom script is written.



**Figure 3.11 Ingress and Egress Up/Down Scripts**

## Resource Sessions

The Sessions tab supports defining terminal and web access sessions to the respective resource. Create a resource session for one of the previously defined resource connections and associate permission-based access through system roles. Each session supports an Allowlist and Denylist which specifies commands that can or cannot be sent to a device. The Access Level permission assigned at the Role Access takes highest priority in command filtering for a session. Connect to sessions created in Resource Management by using Direct Resource Access.

### NOTE

Sessions only appear and become configurable when the Resource Communications Services package is installed.

Session	Session Type	Connection	Roles With Access
Terminal	Terminal	Telnet	2

**Session Parameters**

Name: Terminal  
Session Type: Terminal  
Connection: Telnet  
SSH Access: Available

**Role Access**

Roles: admin, Engineer  
Access Levels: ACC

**Command Filters**

**Allowlist**

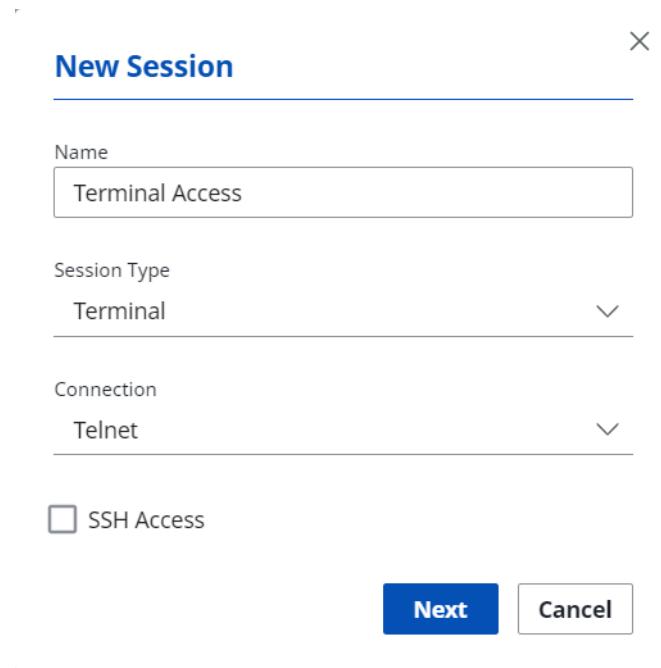
Name	Expression
Status	^STA
ID	^ID

**Denylist**

No Denylist Data Available

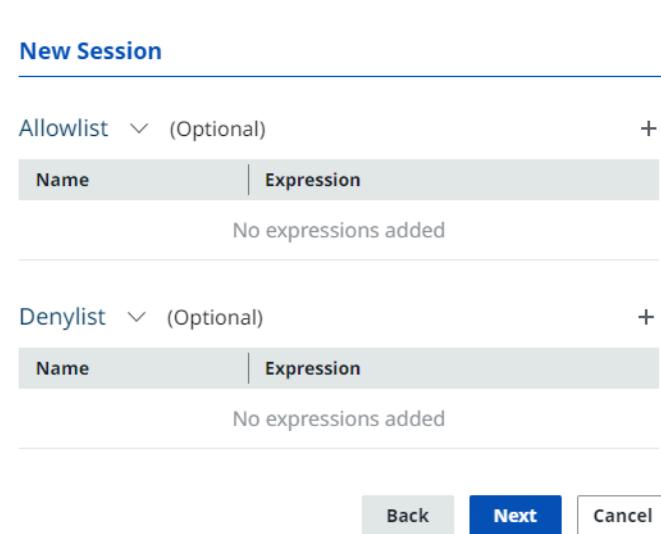
**Figure 3.12 Resource Sessions**

To create a Session, select **New Session**. The New Session dialog will appear, allowing you to enter a Name and select a Session Type and Connection, as shown in *Figure 3.13*. An optional check box for SSH Access can be selected when the Session Type is Terminal. This setting enables a single-use password for proxy access to the device through Blueframe each time the session is connected to Direct Resource Access.



**Figure 3.13** New Sessions Dialog

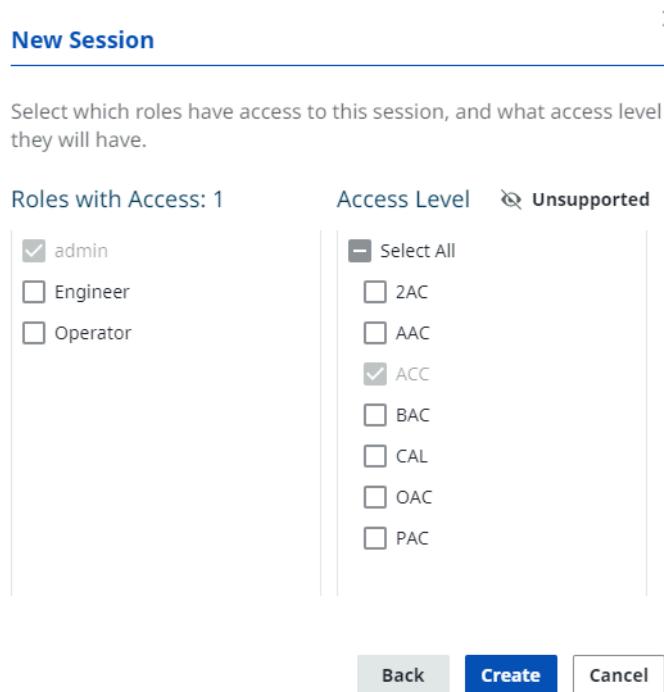
Select **Next**. The command lists will now be available. Optionally add Allowlist or Denylist commands with the + icon, shown in *Figure 3.14*.



**Figure 3.14** New Session With Allowlist or Denylist

Note that Access Level permissions will take precedent over Allowlist or Denylist commands.

Select **Next**. The role selection options will now be available. All Blueframe system roles will appear under **Roles with Access**. Check the box next to each role to specify which roles will have access to connect to the new session and check the box next to each Access Level that the roles shall be able to authenticate to, as shown in *Figure 3.15*.



**Figure 3.15 Role Association**

Select **Create**.

This session is now accessible in Direct Resource Access by any authenticated user in one of the associated roles. See *Section 4: Direct Resource Access* for information on using defined sessions.

## Define Resource Access

To ensure secure, need-to-know access to resources in Blueframe, define resource access lists in Resource Management. Once defined, users will only be able to see information related to the resources to which they have access.

- Step 1. To create a new access list, navigate to Resource Management and select **Permissions > Manage Resource Access**.
- Step 2. Select **New Access List**, as shown in *Figure 3.16*.

The screenshot shows the 'Resource Management Overview' interface. At the top, there's a navigation bar with icons for SEL, View, Permissions, and About, along with status indicators for errors, warnings, messages, and alerts. Below the navigation bar, a left sidebar has a back arrow and the title 'Manage Resource Access'. The main content area is titled 'Create An Access List'. A descriptive text explains that Access Lists grant user roles access to specific resources and provides a 'New Access List' button, which is highlighted with a yellow box.

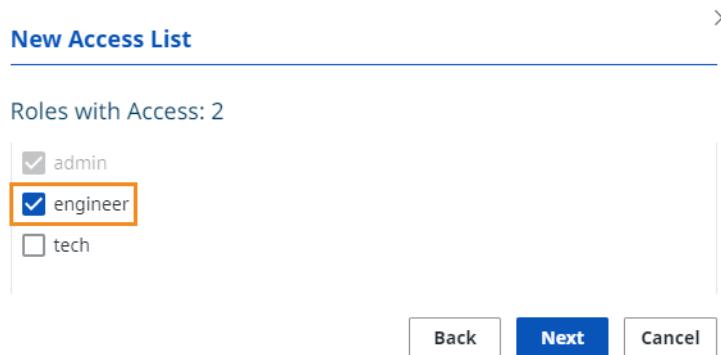
**Figure 3.16** New Access List

Step 3. Enter a name for the access list and, optionally, a description, as shown in *Figure 3.17*, and select **Next**.

The screenshot shows a modal dialog box titled 'New Access List'. It contains two input fields: 'Name \*' with the value 'West Region Engineers' and 'Description' with an empty field. At the bottom are 'Next' and 'Cancel' buttons.

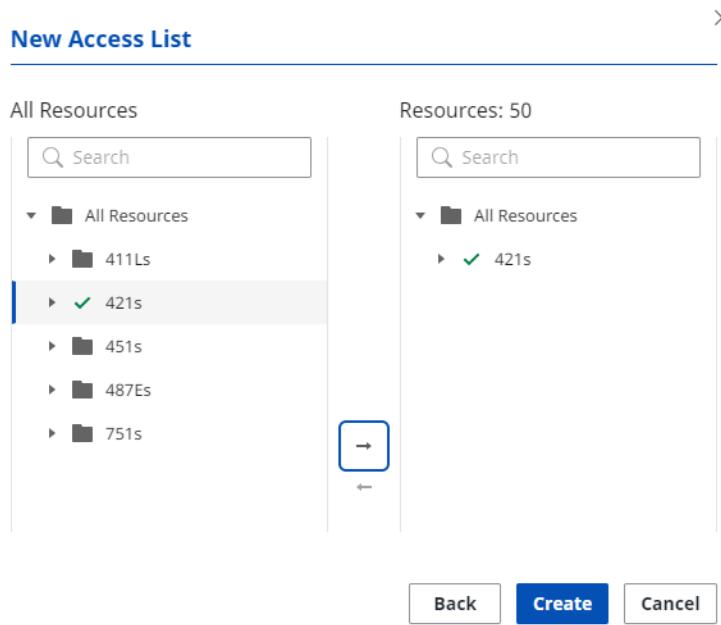
**Figure 3.17** Define an Access List Name and Description

Step 4. Select the role(s) for which you want to provide access to specific resources, as shown in *Figure 3.18*, and select **Next**.



**Figure 3.18 Select Role(s) to Access Resources**

Step 5. Select the resources to which you want the selected role(s) to have access to in the All Resources pane (on the left) and select the arrow button in the middle to move them to the Resources pane (on the right), as shown in *Figure 3.19*, and then select **Create**.



**Figure 3.19 Define the Resources for the Access List**

Resource access lists ensure that only appropriate users have access to the resources specified for them. In an example system configured as shown in *Figure 3.18* and *Figure 3.19*, a user with the "engineer" role, upon logging in to Blueframe and accessing Resource Management, would only be able to see devices in the **421s** folder for which they were provided access, as shown in *Figure 3.20*.

The screenshot shows the Resource Management software interface. On the left, a sidebar titled 'Resources' displays a tree view of resources under 'All Resources'. A folder named '421s' is highlighted with an orange border. The main area shows a table titled 'New Resource' with columns 'Name' and 'com ...'. The table lists 11 rows of resources, all labeled 'SEL' in the 'com ...' column. The first row, 'SEL-421-3 (0)', is selected. To the right of the table, a detailed view for 'SEL-421-3 (1)' is shown, including sections for 'Attributes', 'Labels', 'Connections', and 'Sessions'. The 'Attributes' section lists company: SEL, globalDeviceId: SEL-421-3 (1), model: SEL-421-3, nomFreq: 60, station: Pullman, and tz: UTC. The 'Connections' section shows a single entry for Telnet. The 'Sessions' section also shows a single entry for Telnet.

Figure 3.20 Sample Access List Restricted View

## Resource Management API

Read-only, programmatic access to Resource Management related data is available through an API. To access documentation on available commands, a user with Can Manage permissions to Resource Management (as defined in *User Management* on page 39) can select **View > API Documentation** in the menu bar when Resource Management is launched.

The screenshot shows the Swagger interface for the Device Registry API. At the top, there's a navigation bar with 'SEL' (Resource Management), 'View', 'Permissions', and 'About'. On the right, there are icons for errors (0), warnings (0), and messages (0). Below the navigation is a 'Swagger' logo and a dropdown menu labeled 'Select a definition' with 'device-registry' selected. The main title is 'Device Registry API' with version '0.17.0' and 'OAS3'. A sub-path '/resource-management/device-registry/v1' is shown. Underneath, a 'Servers' dropdown is set to 'lv1'. The main content area is titled 'default' and lists several API endpoints:

- GET /status** API Status
- POST /devices/reset** Reset storage
- GET /devices/{id}** Get device
- GET /devices** Get devices

Figure 3.21 Resource Management API Documentation

## Profiles

Profiles allow you to create common information that will be assigned to new resources created under the profile instance. Within a profile you can specify attributes, labels, connections, and services to accompany a new resource. These properties can be statically defined within the profile or defined per instance. Defining profiles enables simplified resource creation when multiple devices in the system have common properties that should be associated with them.

The following section describes how to define a profile and build resource instances that use that profile.

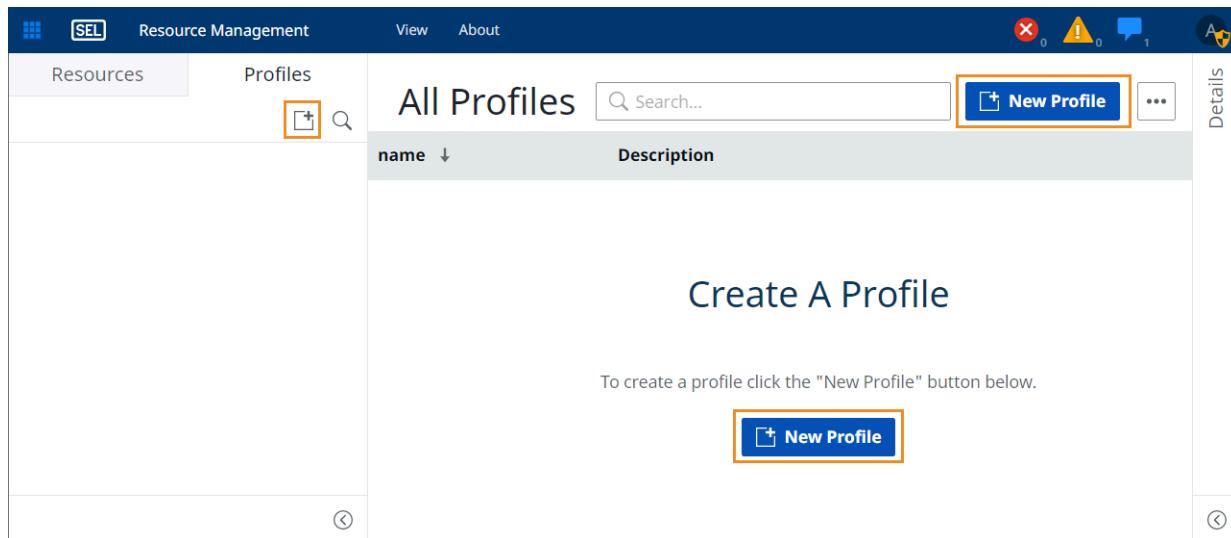
To begin, select the **Profiles** tab in the left-most pane, as shown in *Figure 3.22*.

The screenshot shows the Resource Management interface with the 'Profiles' tab highlighted by an orange box. The left sidebar has 'Resources' and 'Profiles' tabs, with 'Profiles' being the active one. The main area displays a table of resources under 'All Resources':

	All Resources	name ↓
▶	.dma-credential-management-sys	2730M-1
▶	MMS	2730M-2

Figure 3.22 Profiles Creation Workspace

Select **New Profile**, as shown in *Figure 3.23*, to open the New Profile creation dialog.



**Figure 3.23 Create a New Profile**

Enter a name and an optional description for the new profile. This name appears as a reference on each deployed instance in Resource Management.

The 'New Profile' dialog has a title bar 'New Profile' with a close button 'X'. It contains two input fields: 'Name' (containing 'Recloser') and 'Description' (containing 'Profile to be used for all Recloser resources'). Below these is a section titled 'Profile Parameters' with a dropdown arrow and a '+' button. A note says 'Create your first attribute by clicking +' followed by the '+' button. At the bottom are 'Create' and 'Cancel' buttons.

**Figure 3.24 Example Profile Name and Description**

Define any optional Profile Parameters to associate attributes with the profile by selecting the corresponding **+** button.

Attributes can be statically defined for the profile or defined per instance. *Figure 3.25* shows an example of a statically defined attribute and an instance-defined attribute. A statically defined attribute assigns the attribute value automatically, and the attribute cannot be changed by the user creating the resource under the associated profile. An instance-defined attribute adds an attribute to the resource created under the associated profile and requires the user to specify the value of the attribute when the resource instance is created.

**New Profile**

Name: Recloser

Description: Profile to be used for all Recloser resources

Attributes **Static Attribute** +

Check a row to define the attribute per instance of the profile.

Attribute Name	Value
<input type="checkbox"/> company	UtilityXYZ String ...
<input checked="" type="checkbox"/> model	Defined Per Instance String ...

Labels **Instance-Defined Attribute** +

Create your first label by clicking +

**Create** **Cancel**

**Figure 3.25 Statically and Instance-Defined Attributes**

Select **Create** to save the profile.

The screenshot shows the SEL Blueframe Software interface. The top navigation bar includes 'SEL', 'Resource Management', 'View', and 'About'. Below the navigation is a toolbar with icons for 'New Profile', search, and more. The main area has tabs for 'Resources' and 'Profiles'. The 'Profiles' tab is selected, showing a list of profiles. One profile, 'Recloser', is selected and shown in a detailed view on the right. The 'Recloser' profile details are as follows:

- Name:** Recloser
- Description:** Profile to be used for all Recloser resources
- Attributes:**
  - deviceID: Defined per instance
  - deviceName: Defined per instance
  - company: UtilityXYZ
  - model: Defined per instance

**Figure 3.26 Available Profiles**

Once the profile has been created, double-click the row to define the resource template, connection templates, service templates, session templates, and instances.

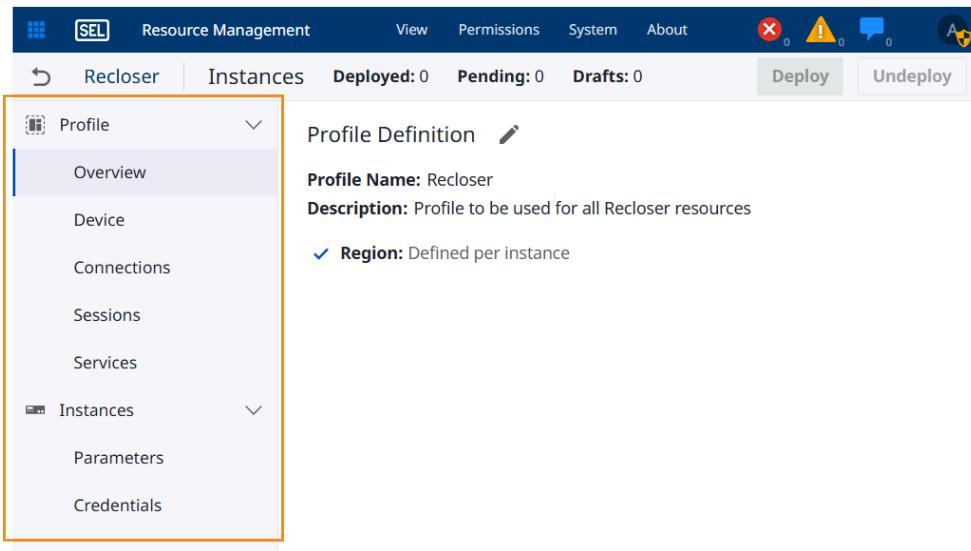


Figure 3.27 Profile Configuration Spaces

## Resource Templates

Define common attributes and labels that are associated with each instance. An Attribute Preset may be selected, which adds all necessary attributes for a specific use case in Blueframe. Additionally, the use of profile parameters may also be used when setting individual attributes.

The screenshot shows the 'Edit Resource Template' dialog box. It has a header with a close button ('X') and a title 'Edit Resource Template'. Below the header is a section titled 'Attributes' with a '+' button. Under 'Attributes', there's a 'Preset' dropdown set to 'Direct Resource Access'. A note says 'Check a row to define the attribute per instance of the profile.' Below this are two rows of attribute definitions:

Attribute Name	Value	Actions
globalDeviceId	GUID	... <span style="color: #ccc;">Delete</span>
model	SEL-651R	String <span style="color: #ccc;">Delete</span>

Below the attributes is a 'Labels' section with a '+' button. It contains a single label entry: 'Recloser' with a 'X' button next to it. At the bottom right are 'Save' and 'Cancel' buttons.

Figure 3.28 Resource Template

## Connection Templates

To define common connection information, select **Connection Templates > New Connection**.

Define the template name and protocol and specify the protocol settings. Protocol settings can have values defined either statically or per instance. *Figure 3.29* shows an example connection template configuration.

The screenshot shows the 'New Connection Template' dialog box. At the top, there is a 'Template Name \*' field containing 'Telnet'. Below it is a 'Protocol \*' dropdown set to 'SEL over Telnet'. The main area is titled 'Protocol Settings' with the sub-instruction 'Check a row to define the attribute per instance of the profile.' It contains two rows: one for 'Host' (value 192.168.1.1) and one for 'Port' (value 23). Below this is a 'Credentials' section with two rows: 'Access Level 1' (value 'Defined Per Instance') and 'Access Level 2' (value 'Defined Per Instance'). At the bottom right are 'Create' and 'Cancel' buttons.

**Figure 3.29** Profile Connection Template

## Service Templates

Service templates define settings for specific applications installed in the Blueframe platform. For details on specific template settings, refer to the respective product instruction manual. Like connection templates, service templates have attributes that can be either statically defined or defined per instance of the profile. *Figure 3.30* shows an example service template configuration.

**Add Service Template**

Name	Template Name
Service Template *	FLISR Scaling

**Template Settings**

Check a row to define the attribute per instance of the profile.

Attribute Name	Value
<input type="checkbox"/> leftPT	
Attribute Name	Value
<input type="checkbox"/> rightPT	
Attribute Name	Value
<input type="checkbox"/> loadCapacity	
Attribute Name	Value
<input type="checkbox"/> normalState	
Attribute Name	Value
<input type="checkbox"/> currentScale	
Attribute Name	Value
<input type="checkbox"/> voltageScale	

**Add Template** **Cancel**

**Figure 3.30 Profile Service Template**

## Session Templates

Session templates define sessions that will be available on the resources created from the profile. These session templates use the defined connection templates made for the profile. For detailed information on configuring sessions, see *Resource Sessions on page 84*. Figure 3.31 shows an example session template configuration.

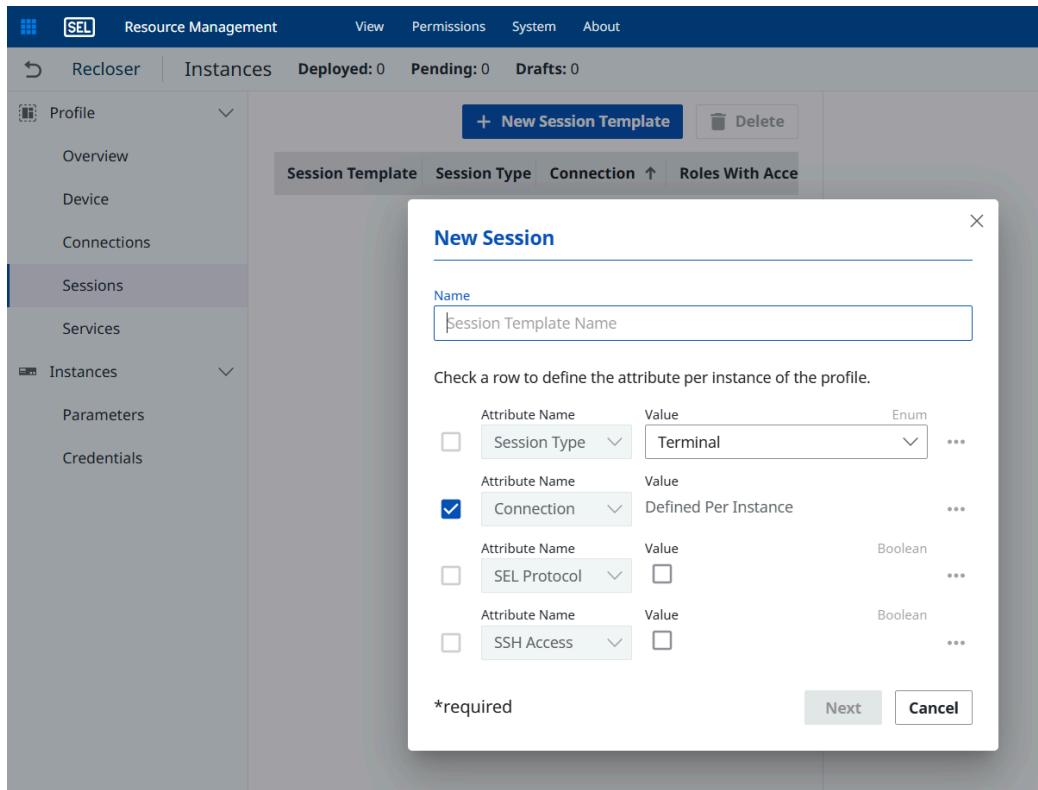


Figure 3.31 Profile Session Template

## Instances

Build resource instances that will appear in Resource Management and use the settings and attributes associated with the profile.

Select **Add Instance** and specify a name and the number of instances to add. An "(n)" will be appended to the name, where n starts at zero and increments by one for each additional instance.

All instance-specific attributes must be completed and saved before they can be deployed to Resource Management. When the Draft column contains a check mark for an instance, that instance is ready to be deployed.

Select **Deploy**, choose which instances to deploy, and then select **Deploy** again, as shown in *Figure 3.32*.

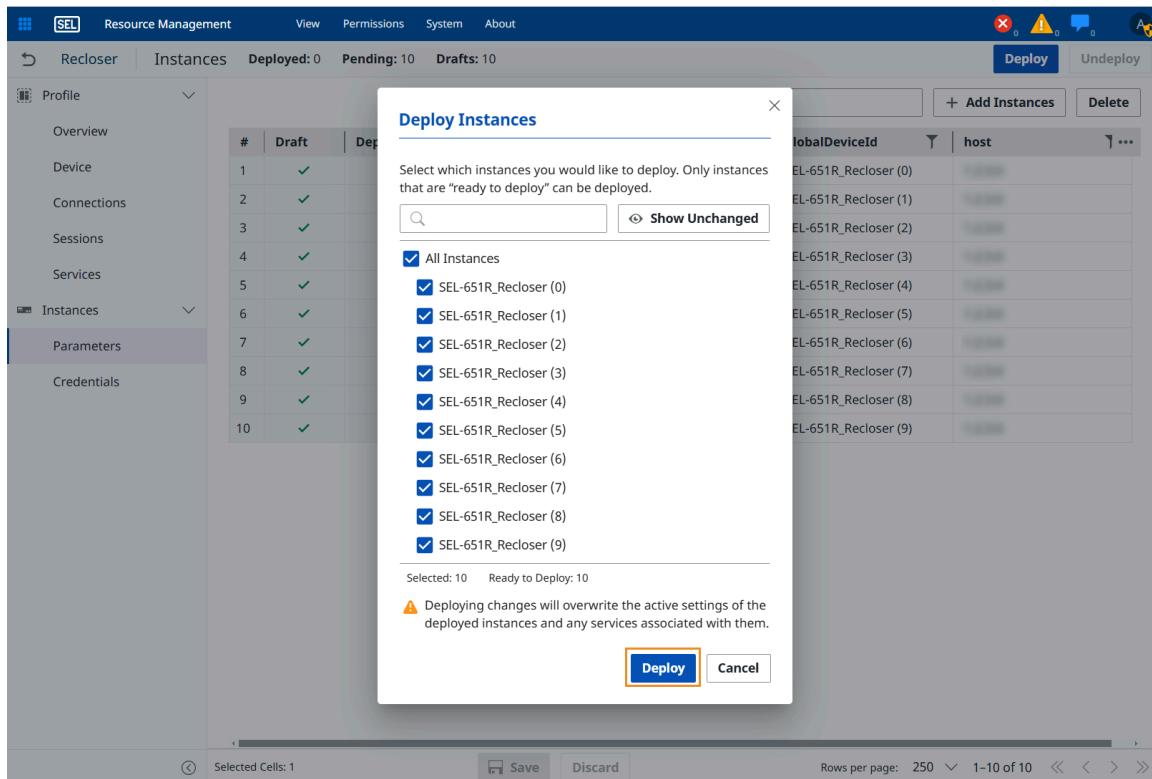
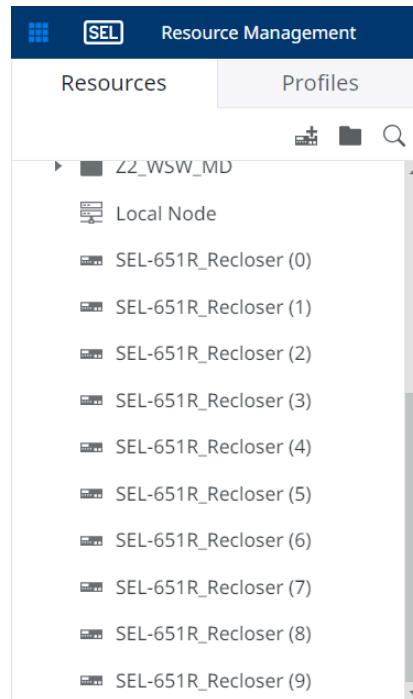


Figure 3.32 Deploy Instances

Once instances are deployed, any changes made to the profile or profile attributes will only be applied to newly deployed instances. To apply changes to already-deployed instances, you must un-deploy and then re-deploy those instances.

Once deployed, instances will appear in the Resources tree in Resource Management, as shown in *Figure 3.33*.

**98** Resource Management  
Overview



**Figure 3.33 Profile Instances in Resource Management**

## Instance Credentials

Specify access level credentials per connection for each created instance. If credentials are being managed by DMA Credential Management, they will be updated here for permitted users to view.

The screenshot shows the SEL Resource Management software interface with the 'Instances' tab selected. The left sidebar has sections for Overview, Device, Connections, Sessions, Services, Instances, Parameters, and Credentials, with 'Credentials' currently selected. The main area features a table titled 'Profile' with columns for #, Resource, Label, Connection, Type, ACC, 2AC, and CAL. There are 10 rows, each corresponding to one of the SEL-651R\_Recloser instances from Figure 3.33. The '2AC' column for row 4 is highlighted with a blue border. A search bar and a 'Create Credentials' button are at the top of the table area.

#	Resource	Label	Connectio...	Type	ACC	2AC	CAL
1	SEL-651R_Recloser (0)	Telnet-SEL	0	SEL	.....	.....	Undefined
2	SEL-651R_Recloser (1)	Telnet-SEL	0	SEL	.....	.....	Undefined
3	SEL-651R_Recloser (2)	Telnet-SEL	0	SEL	.....	.....	Undefined
4	SEL-651R_Recloser (3)	Telnet-SEL	0	SEL	.....	.....	Undefined
5	SEL-651R_Recloser (4)	Telnet-SEL	0	SEL	.....	.....	Undefined
6	SEL-651R_Recloser (5)	Telnet-SEL	0	SEL	.....	.....	Undefined
7	SEL-651R_Recloser (6)	Telnet-SEL	0	SEL	.....	.....	Undefined
8	SEL-651R_Recloser (7)	Telnet-SEL	0	SEL	.....	.....	Undefined
9	SEL-651R_Recloser (8)	Telnet-SEL	0	SEL	.....	.....	Undefined
10	SEL-651R_Recloser (9)	Telnet-SEL	0	SEL	.....	.....	Undefined

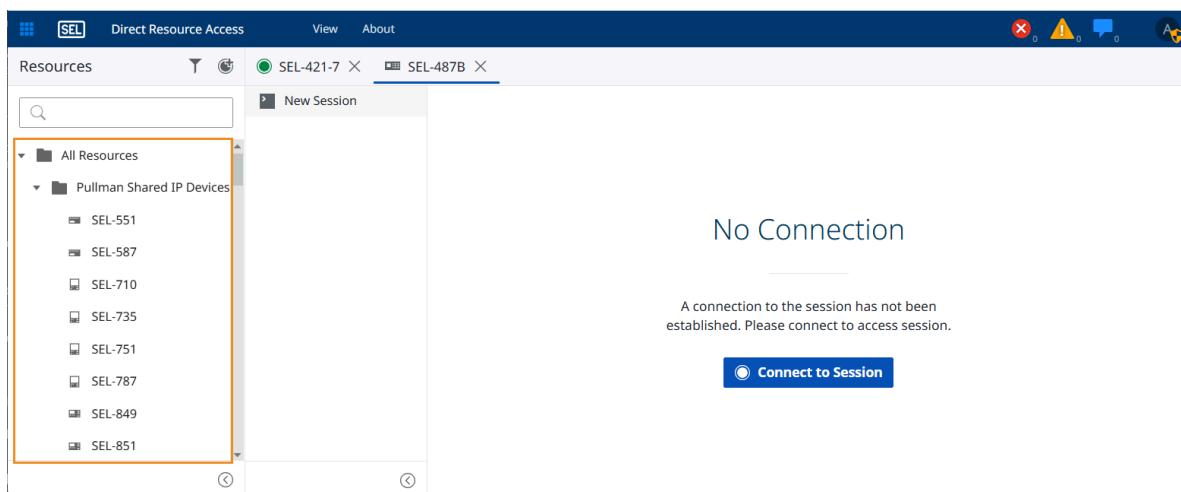
**Figure 3.34 Instance Credentials**

## SECTION 4

# Direct Resource Access

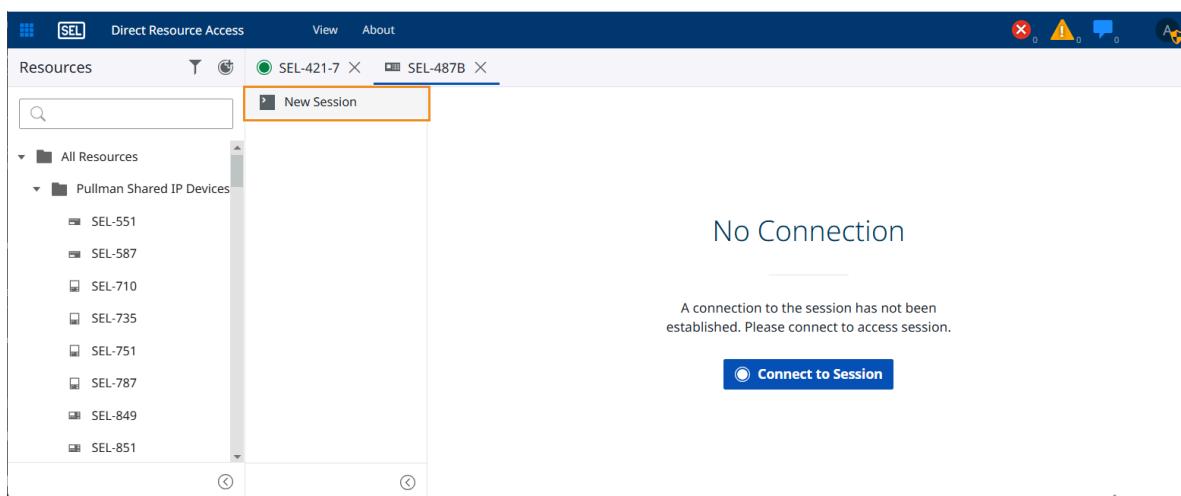
The Direct Resource Access application provides terminal and web proxy access to system resources with a configured connection session. Sessions are defined on a per-resource basis in Blueframe's Resource Management and are tied to specific role access. This ensures that only appropriate users have access to a terminal or web proxy where commands can be issued and device information verified. For information on how to configure a session, refer to *Resource Sessions on page 84*.

Launch Direct Resource Access to view which resources have sessions available based on your user permissions. Available sessions will appear under the resource to which they belong, as shown in *Figure 4.1*.



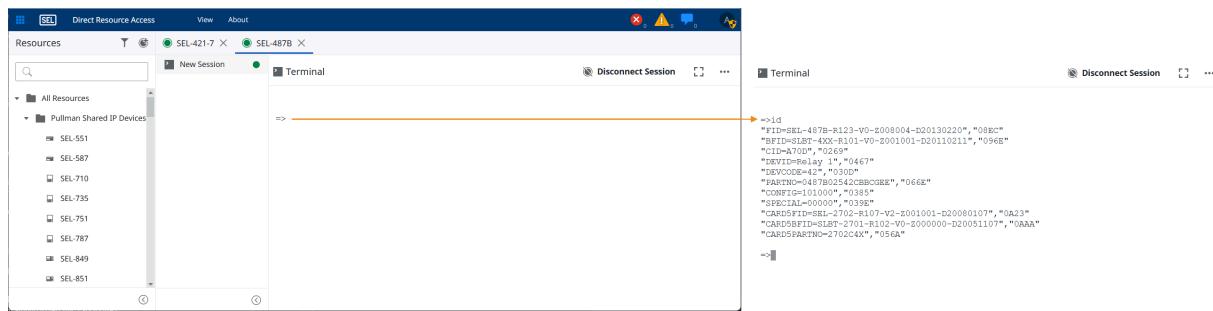
**Figure 4.1 Connected Resources**

Select a resource to view available sessions in the sessions pane, as shown in *Figure 4.2*. A resource can have one or more available sessions.



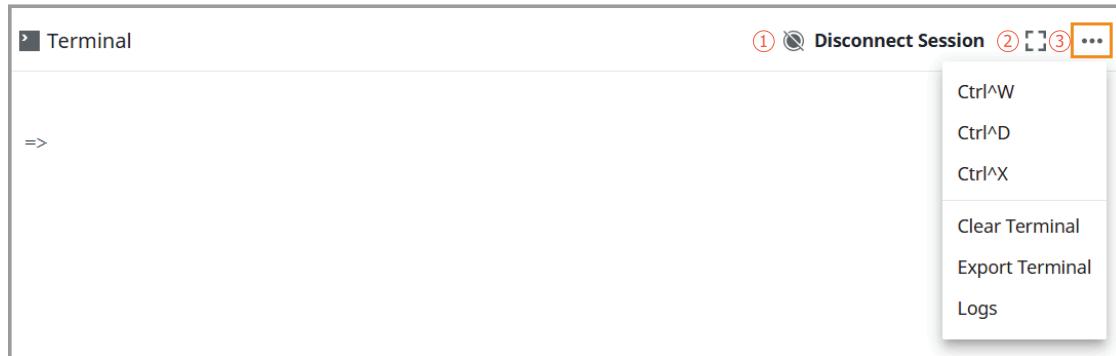
**Figure 4.2 Available Sessions**

With a terminal session selected, select **Connect to Session** to initiate the connection. Once the connection is established, the terminal will appear and commands can be entered in the **Command to Execute** field, as shown in *Figure 4.3*.



**Figure 4.3 Execute a Command**

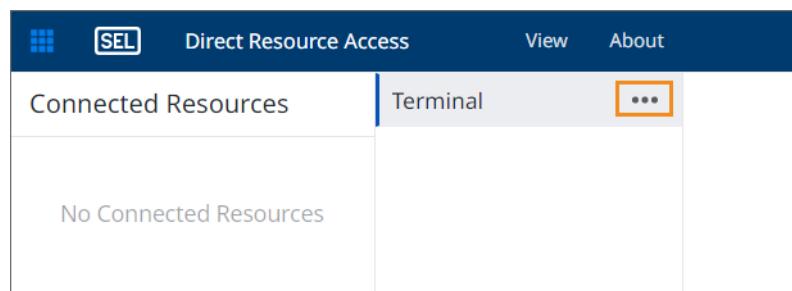
*Figure 4.4* shows and describes the tools available in the terminal.



- ① **Disconnect Session.** Select to terminate the connection to the resource session.
- ② **Fullscreen.** Select to make the terminal full-screen or to return to the initial Direct Resource Access view with available sessions.
- ③ **Terminal Options.** Contains shortcuts to commonly used functions such as control characters and session logs, as well as other terminal options.

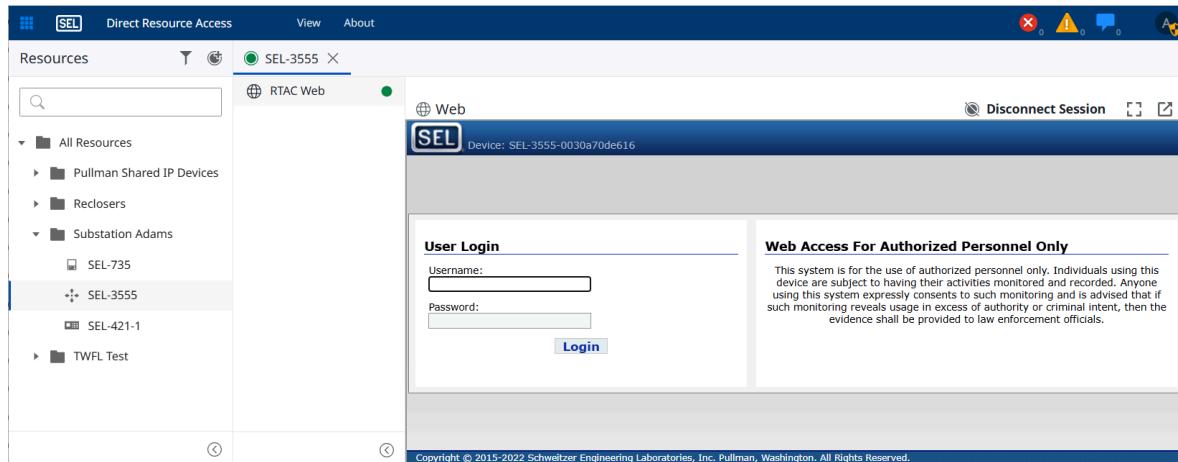
**Figure 4.4 Terminal Tools**

Once a session has been disconnected or terminated, an ellipsis button will appear to the right of the session, as shown in *Figure 4.5*. Selecting this shows the available logs for the previous session, which may be useful for troubleshooting any connection issues that occurred.



**Figure 4.5 Last Session Logs**

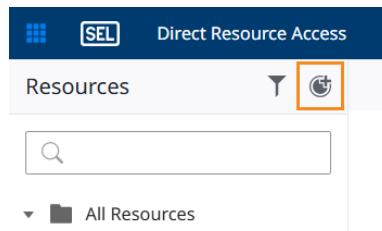
To connect to a web proxy session, select the session to automatically initiate the connection. The webpage will be shown once successfully connected, as shown in *Figure 4.6*.



**Figure 4.6** Web Proxy Session

## Quick Connect

For users with advanced permission, the Quick Connect option is available, as shown in *Figure 4.7*. To manage Quick Connect permissions as an administrator, select **View > Edit Permissions** and check the roles that should have access to this tool.



**Figure 4.7** Quick Connect Option

When the Quick Connect icon is selected, the Quick Connect dialog will appear where you can enter a session name, select the protocol to use, and define the host and port. An example is shown in *Figure 4.8*.

## Quick Connect

Name

Protocol

TELNET



### Protocol Settings

Host

Port

**Connect**

**Cancel**

**Figure 4.8 Quick Connect Dialog**

Select Connect to open a terminal to this connection. This connection will no longer be available after navigating away from Direct Resource Access.

---

---

## S E C T I O N   5

---

# Protocol Services

## Overview

---

Protocol Services provides the functionality for configuring communications protocols data ingress (client) and egress (server) in the Blueframe application platform. This application provides communications data concentration among IEDs (resources) and protocol conversion for upstream SCADA, HMI, or other polling devices. Blueframe does not limit the number of client or server communications services; however, SEL recommends not exceeding the following of number of total connections for the supported device.

Supported Protocols	SEL-3555 and SEL-3360	SEL-3350	Virtual Machine
DNP	256 Clients/servers (combination of both)	100 Clients/servers (combination of both)	Dependent on system resources

## Licensing

There are no licensing requirements for the number of data points that client services can collect when installed on SEL computing platforms. Any additional applications installed on a Blueframe system can use data points in Blueframe. A license is required to serve data points to applications external to a Blueframe system through a server protocol. The license is based on the data point tiers listed in *Table 5.1*. The tiers represent the upper limit of all points transmitted through all server services. You can serve as many as 250 data points through server connections without purchasing a license.

**Table 5.1 License Level for Data Point Tiers on SEL Embedded Computing Platforms**

Server Data Point License Level	Data Point Upper Limit
Level 0 (No license required)	250
Level 1	2500
Level 2	25000
Level 3	100000

## Adding a Protocol Service

---

The Protocol Services landing page provides a navigation tree of configured client and server services. If there are no protocol services configured or selected, a prompt appears that provides icons to configure a client or server protocol service, as shown in *Figure 5.1*. You can also add a service by selecting

the New Service (+) icon in the Services pane. New folders and services appear as a navigation tree. Right-click these items to view context menus specific to the selection(s). You can perform bulk operations in the navigation tree, such as deploy, delete, and rename.

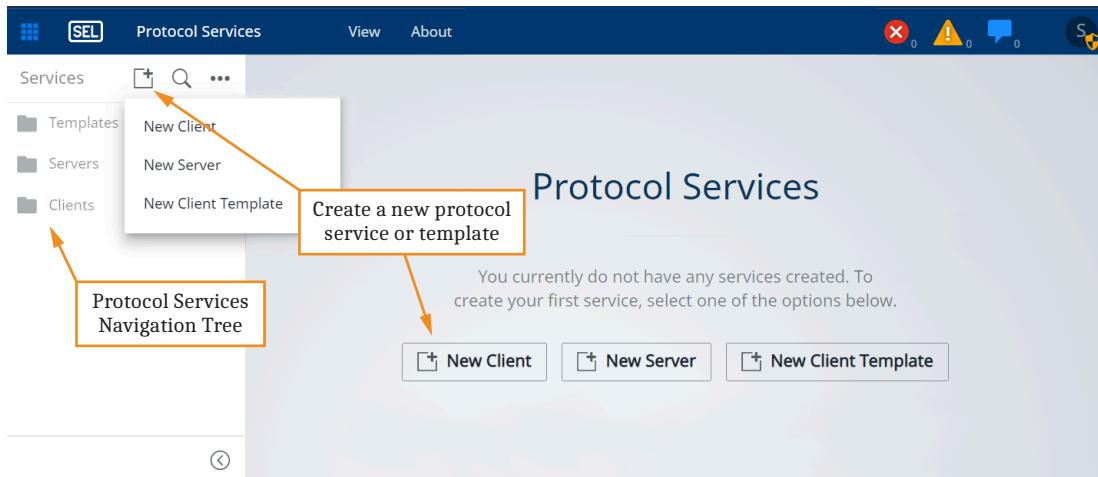


Figure 5.1 Initial Protocol Service Landing Page

## Configuring a Service

---

### Client Services

Once a new client is added, a configuration dialog appears that presents options for the initial connection parameters. The Protocol field presents all available protocol options for the client service. Client connections can be associated with existing resources (i.e., external devices or software systems such as relays, RTUs, meters, databases, or HMIs) in Resource Management. Optionally, you can choose to inherit the resource name from an associated resource by selecting the **Use resource name as client name** check box. If you choose to inherit the resource name, the Name field becomes read-only. For more information on configuring resources and connections, refer to *Section 2: Blueframe Management Tools*.

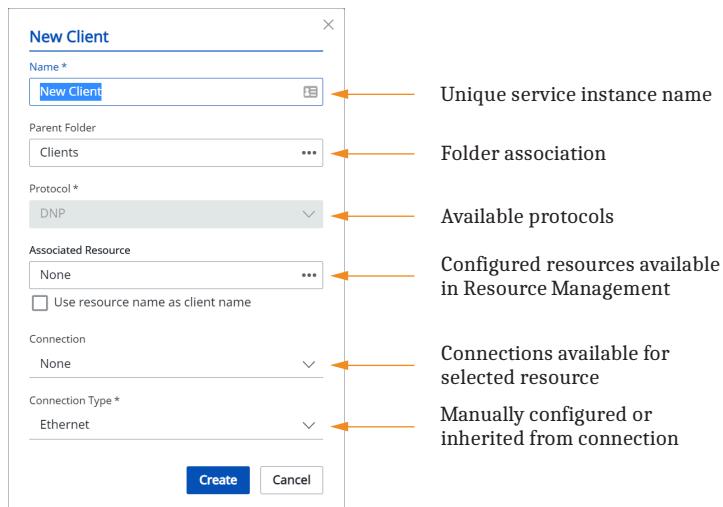


Figure 5.2 New Client Dialog Field Descriptions

A resource may have none, one, or many predefined connections for communications. If the client service is associated with a resource, all available connections that match the communication protocol of the service appear in the Connection dropdown menu. Selecting a matching connection automatically imports the settings configured in the resource connection. When a resource connection is associated with the client, the Connection Type field is auto-filled and set to read-only. If no resource or connection is associated, the manual configuration options are Ethernet, serial, and Ethernet-tunneled serial. Select the **Create** button to make the draft client available in the **Services** directory. You can then add resources and connections to an existing service, as shown in *Figure 5.3*.

* Settings		Associated Resource	Connection
Binary Inputs	SEL-421	SEL-421 DNP	^
	Name	None	☰
	General(1)	SEL-421 DNP	
Double Bit Inputs	Connection Method		
	Communication(7)		
Binary Outputs	Serial Communications Port	* Com_s0p1	
	Serial Communications Port Type	* EIA232	
Counters	Baud Rate	* 19200	
	Data Bits	* 8	
Analog Inputs	Parity (None, Even, Odd)	* None	
	Number of Stop Bits	* 1	
Analog Outputs	Full Duplex	* True	

**Figure 5.3** Configuring a New Client in Resource Management

## Server Services

Once a new server is added, a dialog box appears for configuring the protocol and connection type. The Protocol field presents all available protocol options for the server service and the Connection Type options are Ethernet, serial, and Ethernet-tunneled serial.

## Protocol Data Points

Protocol service data points are classified based on a common set of characteristics and attributes. Each data point has three characteristics: Point Name, Point Type, and Publication Subject. The Point Name is a concatenated name that combines the protocol service and a user-defined name separated by dot notation. The Point Type is the digital representation of the data in Blueframe. All data entered into or generated with Blueframe are normalized into one of the types described in *Table 5.2*. Data are further classified into status and control points. The Publication Subject is a global unique identifier that is used by other services and applications.

**Table 5.2 Blueframe Data Point Types**

Data Point Type	Description
Binary	Data that can represent an on/off state
Double Bit	Data that can represent as many as four states
Integer	Data that represent whole-number increments
Analog	Data that represent floating-point number
String	Data that represent a collection of characters

## Protocol Services Toolbar

The toolbar provides status information and tools for interacting with protocol service instances or templates. From the toolbar, you can add, edit, and change the state for a service or template. The actions available in and the appearance of the toolbar change depending on the service type and the current state of the service.

## Client and Server Services

A client or server service is in a draft state after initial creation. The Service state in the toolbar reflects the Draft state, as shown in *Figure 5.4*, and the setting grid is editable. When a settings change is made to a draft, the changes are indicated by asterisks in front of the setting and a bold highlight. The Action buttons present options to save and cancel the settings changes made to a draft. A warning ( A) appears in both the Service State Selector and the navigation tree, indicating that the draft settings differ from the deployed service. Once the settings changes are saved, the Deploy action button is available.

**Figure 5.4 Protocol Services Toolbar With a Draft Protocol Service**

For client and server services, selecting **Deploy** creates and starts the service, at which point the Service State displays **Comms Offline** or **Comms Online**, depending on whether a successful communication session was established. The Start/Stop Service Action buttons are selectable when the communications session is deployed. When the service is stopped, the Service State displays **Stopped**. You cannot delete a protocol service from the navigation tree until the service is stopped. The state of the service is also displayed in the navigation tree for quick viewing. If the communication session fails to establish, navigate to the **Diagnostics** tab of the service to troubleshoot the error.

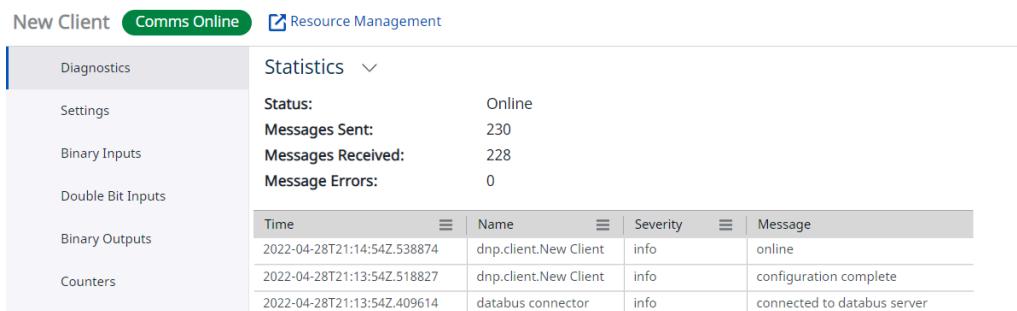
To edit settings after a service is deployed, select the **Edit** action button. This creates a draft of the deployed settings. Any changes made to the draft are temporary until saved, and navigating away from Protocol Services results in the loss of unsaved settings changes. When settings changes are saved, the draft persists until deployed or deleted. The Service State Selector dropdown menu provides navigation between the draft and deployed state.

Selecting the ellipsis in the top right corner of the Protocol Services toolbar provides additional options that vary depending on the state of the services. In general, options for renaming, undeploying a service, deleting a draft, and exporting settings are available. Settings are exported in JSON format. You can edit these files and then import them into an existing service draft.

## Communications Diagnostics

---

Deployed services have an additional Diagnostic tab to aid in troubleshooting communications sessions. The communications status and message statistics appear under **Statistics** and are indicative of the real-time status of the communications session. A log of communications status changes and errors are maintained to provide a history for detailed troubleshooting, as shown in *Figure 5.5*.



The screenshot shows the 'Comms Online' tab selected in the top navigation bar. The main content area has a sidebar on the left with categories: 'Diagnostics' (selected), 'Settings', 'Binary Inputs', 'Double Bit Inputs', 'Binary Outputs', and 'Counters'. The 'Statistics' section displays real-time metrics: Status (Online), Messages Sent (230), Messages Received (228), and Message Errors (0). Below this is a table titled 'Log' with columns: Time, Name, Severity, and Message. The table contains three entries:

Time	Name	Severity	Message
2022-04-28T21:14:54Z.538874	dnp.client.New Client	info	online
2022-04-28T21:13:54Z.518827	dnp.client.New Client	info	configuration complete
2022-04-28T21:13:54Z.409614	databus connector	info	connected to databus server

**Figure 5.5** Diagnostics Tab for an Online Protocol Session

## DNP3

---

### Overview

Configure DNP3 protocol on any of the Blueframe serial or Ethernet ports to communicate with DNP3 IEDs, communications processors, RTUs, and remote client systems. The DNP3 Device Profile Document is included at the end of this section. For more information on DNP3 protocol, go to [www.dnp.org](http://www.dnp.org).

## Settings Tab

The Settings tab contains all configurable items necessary for communications. Check the **Description** column for details on each configuration item. Move the column slider to resize the column to see the entire text of an item description. Select and move the column headers to create an alternate table layout. The menu in the top right corner of every column provides options for manipulating the columns and rows in the table. Select the **Advanced Settings** check box to enable the configuration of advanced settings.

## Configuring Data Points in a DNP3 Client Service

Data in the DNP3 client service are organized into DNP3 object types. Select the tab that represents the data objects in the DNP3 server that is polled or transmitting unsolicited messages. Select the **Add Points** button in the top right corner, as shown in *Figure 5.6*. The service must be in the draft state to add or delete points. Configure the starting point index and quantity, and then select **Add**. All data points have the three attributes described in *Protocol Data Points on page 105* and two additional columns: Point Number, which is the DNP3 index; and Comment, which is a user-defined field. The Binary Outputs have additional columns describing the Control Model and, when applicable, the pulse behavior. To delete points, select the applicable row and select the **Delete** button in the top right corner. To select multiple continuous rows, hold <Shift> and select the first row in the desired range followed by the last row. To select multiple non-continuous rows, hold <Ctrl> while selecting each row you want to include.

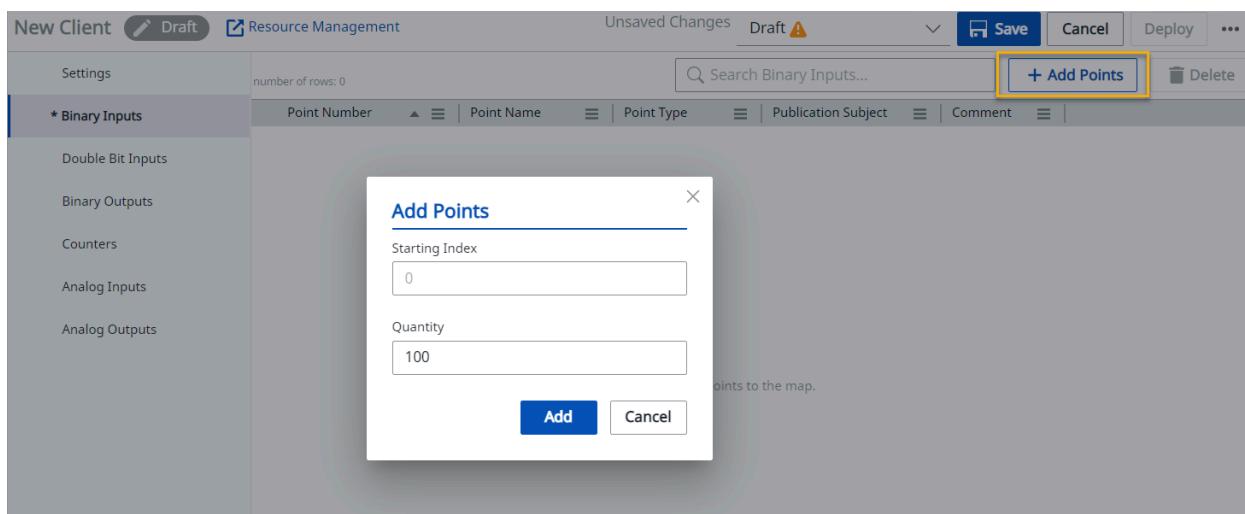


Figure 5.6 Adding Points to a Draft DNP3 Client Service

## Configuring DNP Server Service Communications Client Session Configuration

By default, a new DNP3 server services requires incoming client connections to be defined. The server accepts as many as 20 simultaneous connections and each DNP3 session gets unique buffers to track event and event acknowledgements. Provide the IP addresses and DNP client address for each incoming connection. To allow any DNP3 client to connect to the server service, toggle **Allow Anonymous DNP/IP Clients** to TRUE. When operating in anonymous mode, only one connection is accepted and the event buffer is shared. When a new client connects in anonymous mode, the previous connection is terminated.

## Mapping Data Points to a Server Service

The columns in the data point table are similar to those presented in the client configuration. The notable difference is the substitution of Point Name for Point Reference. The server represents a collection of client, application, or system data points, and the server map only references the mapped data points.

The Point Number is the index of the referenced data point in the server map. Point Type and Publication Subject are inherited from the data point reference and cannot be edited. There are one or more Var Obj columns that allow the configuration of the object variation that is returned to when that object is requested by the client. The Event Class groups data in classes (or groups) for reporting event data. Users can add descriptions for the data in the Comments column. The Binary Inputs tab has an additional column to optionally invert the mapped data point. The Analog Inputs tab has two additional columns for scaling the outgoing data and setting the deadbands that determine when an event is generated. SEL does not recommend setting the deadband to 0 for any analog point.

To map data points to the server, navigate to the tab representing the data object of interest. All data points available for mapping are presented in the Data Points panel. Data points are organized by protocol and point source and are pre-filtered for compatibility based on the point type and classification. The filtering criteria are presented at the top of the panel, as shown *Figure 5.7*.

Point Number	Point Reference	Point Type	Publication Subject	Var Obj 1 Default	Var Obj 2 Default	Event Class	Invert	Comment
0	dnp.New Client.BI_00000	Binary	status.dnp.99233260-46	2	2	1	False	
1	dnp.New Client.BI_00001	Binary	status.dnp.99233260-46	2	2	1	False	
2	dnp.New Client.BI_00002	Binary	status.dnp.99233260-46	2	2	1	False	
3	dnp.New Client.BI_00003	Binary	status.dnp.99233260-46	2	2	1	False	
4	dnp.New Client.BI_00004	Binary	status.dnp.99233260-46	2	2	1	False	
5		Binary		2	2	1	False	
6	dnp.New Client.BI_00006	Binary	status.dnp.99233260-46	2	2	1	False	
7	dnp.New Client.BI_00007	Binary	status.dnp.99233260-46	2	2	1	False	
8	dnp.New Client.BI_00008	Binary	status.dnp.99233260-46	2	2	1	False	
9	dnp.New Client.BI_00009	Binary	status.dnp.99233260-46	2	2	1	False	
10	dnp.New Client.BI_00010	Binary	status.dnp.99233260-46	2	2	1	False	
11	dnp.New Client.BI_00005	Binary	status.dnp.99233260-46	2	2	1	False	
* 12	*	* Binary	* 2	* 2	* 1	* False	*	
* 13	*	* Binary	* 2	* 2	* 1	* False	*	
* 14	* dnp.New Client.BI_00018	* Binary	* status.dnp.99233260-46	* 2	* 1	* False	*	

**Figure 5.7 Configuring Data Point Maps in a DNP3 Server Service**

Select one or more data point(s) and drag the selection onto the map. The points are sequentially appended to the end of the map. To add one or more spare index, select the **Add Points** button in the top right corner. To populate the spare(s), manually type in the data point name or copy an existing data point name from a deployed client or application and paste the name into the Point Reference column. The Point Number represents the index and must be unique per tab or DNP3 object, but you can edit the Point Number to change the indexing of the map. Sort the columns in the map by double-clicking the name of the column by which you want to sort.

## DNP3 Device Profile Document

The following DNP3 Device Profile only shows selections relevant to the Protocol Service DNP3 implementation.

**Table 5.3 Server (Outstation)**

Parameter	Value
Vendor name	Schweitzer Engineering Laboratories
Device name	RTAC
Highest DNP request level	Level 3
Highest DNP response level	Level 3
Device function	Outstation
Notable objects, functions, and/or qualifiers supported	Analog Dead-Band Objects (object 34)
Maximum data link frame size transmitted/received (octets)	292
Maximum data link retries	Configurable, range 0–15
Requires data link layer confirmation	Configurable by setting
Maximum application fragment size transmitted/received (octets)	2048
Maximum application layer retries	None
Requires application layer confirmation	When reporting event data
Data link confirm time-out	Configurable
Complete application fragment time-out	None
Application confirm time-out	Configurable
Complete application response time-out	None
Executes control WRITE binary outputs	Always
Executes control SELECT/OPERATE	Always
Executes control DIRECT OPERATE	Always
Executes control DIRECT OPERATE-NO ACK	Always
Executes control count greater than 1	When pulse count > 1
Executes control Pulse On	Always
Executes control Pulse Off	Never
Executes control Latch Off	Always
Executes control Latch On	Always
Executes control Queue	Never
Executes control Clear Queue	Never
Reports binary input change events when no specific variation requested	Only timetagged
Reports time-tagged binary input change events when no specific variation requested	Binary input change with time
Sends unsolicited responses	Configurable with unsolicited message enable settings. Increases retry time (configurable) when a maximum retry setting is exceeded.
Sends static data in unsolicited responses	Never

Parameter	Value
Default counter object/variation	Object 20, Variation 6
Counter rollover	32 bits
Sends multifragment responses	Yes

**Table 5.4 DNP Server (Slave) Object**

Obj	Var (*default)	Description	REQUEST Func Codes (dec)	REQUEST QualCodes (hex)	RESPONSE Func Codes (dec)	RESPONSE QualCodes (hex)
1	0	Binary Input—All Variations	1,22	0,1,6,7,8,17,28		
1	1	Binary Input	1	0,1,6,7,8,17,28	129	0,1,17,28
1	2*	Binary Input With Status	1	0,1,6,7,8,17,28	129	0,1,17,28
2	0	Binary Input Change—All Variations	1	6,7,8		
2	1	Binary Input Change Without Time	1	6,7,8	129,130	17,28
2	2*	Binary Input Change With Time	1	6,7,8	129,130	17,28
2	3	Binary Input Change With Relative Time	1	6,7,8	129,130	17,28
10	0	Binary Output—All Variations	1	0,1,6,7,8		
10	2*	Binary Output Status	1	0,1,6,7,8	129	0,1
12	0	Control Block—All Variations				
12	1	Control Device Output Block	3,4,5,6	17,28	129	echo of request
12	2	Pattern Control Block	5,6	7		
12	3	Pattern Mask	5,6	0,1		
20	0	Binary Counter—All Variations	1,7,8,9,10,22	0,1,6,7,8,17,28		
20	1	32-Bit Binary Counter	1,7,8,9,10	0,1,6,7,8,17,28	129	0,1,17,28
20	2	16-Bit Binary Counter	1,7,8,9,10	0,1,6,7,8,17,28	129	0,1,17,28
20	5	32-Bit Binary Counter Without Flag	1,7,8,9,10	0,1,6,7,8,17,28	129	0,1,17,28
20	6*	16-Bit Binary Counter Without Flag	1,7,8,9,10	0,1,6,7,8,17,28	129	0,1,17,28
21	0	Frozen Counter—All Variations	1,22	0,1,6,7,8,17,28		
21	1	32-Bit Frozen Counter	1	0,1,6,7,8,17,28	129	0,1,17,28
21	2	16-Bit Frozen Counter	1	0,1,6,7,8,17,28	129	0,1,17,28
21	5	32-Bit Frozen Counter With Time of Freeze	1	0,1,6,7,8,17,28	129	0,1,17,28
21	6*	16-Bit Frozen Counter With Time of Freeze	1	0,1,6,7,8,17,28	129	0,1,17,28
21	9	32-Bit Frozen Counter Without Flag	1	0,1,6,7,8,17,28	129	0,1,17,28
21	10	16-Bit Frozen Counter Without Flag	1	0,1,6,7,8,17,28	129	0,1,17,28

Obj	Var (*default)	Description	REQUEST Func Codes (dec)	REQUEST QualCodes (hex)	RESPONSE Func Codes (dec)	RESPONSE Qual Codes (hex)
22	0	Counter Change Event —All Variations	1	6,7,8		
22	1	32-Bit Counter Change Event Without Time	1	6,7,8	129,130	17,28
22	2*	16-Bit Counter Change Event Without Time	1	6,7,8	129,130	17,28
22	5	32-Bit Counter Change Event With Time	1	6,7,8	129,130	17,28
22	6	16-Bit Counter Change Event With Time	1	6,7,8	129,130	17,28
23	0	Frozen Counter Event —All Variations	1	6,7,8		
23	1	32-Bit Frozen Counter Event Without Time	1	6,7,8	129,130	17,28
23	2	16-Bit Frozen Counter Event Without Time	1	6,7,8	129,130	17,28
23	5	32-Bit Frozen Counter Event With Time	1	6,7,8	129,130	17,28
23	6*	16-Bit Frozen Counter Event With Time	1	6,7,8	129,130	17,28
30	0	Analog Input—All Variations	1,22	0,1,6,7,8,17,18		
30	1	32-Bit Analog Input	1	0,1,6,7,8,17,28	129	0,1,17,28
30	2	16-Bit Analog Input	1	0,1,6,7,8,17,28	129	0,1,17,28
30	3	32-Bit Analog Input Without Flag	1	0,1,6,7,8,17,28	129	0,1,17,28
30	4*	16-Bit Analog Input Without Flag	1	0,1,6,7,8,17,28	129	0,1,17,28
30	5	Short Floating Point Analog Input (32 bit)	1	0,1,6,7,8,17,28	129	0,1,17,28
32	0	Analog Change Event —All Variations	1	6,7,8		
32	1	32-Bit Analog Change Event Without Time	1	6,7,8	129,130	17,28
32	2	16-Bit Analog Change Event Without Time	1	6,7,8	129,130	17,28
32	3	32-Bit Analog Change Event With Time	1	6,7,8	129,130	17,28
32	4*	16-Bit Analog Change Event With Time	1	6,7,8	129,130	17,28
32	5	Short Floating Point Analog Change Event	1	6,7,8	129,130	17,28
32	7	Short Floating Point Analog Change Event With Time	1	6,7,8	129,130	17,28
34	0	Analog Dead Band—All Variations	1	0,1,6,7,8,17,28		

Obj	Var (*default)	Description	REQUEST Func Codes (dec)	REQUEST QualCodes (hex)	RESPONSE Func Codes (dec)	RESPONSE Qual Codes (hex)
34	1*	16-Bit Analog Dead Band	1,2	0,1,6,7,8,17,28	129	0,1,17,28
34	2	32-Bit Analog Dead Band	1,2	0,1,6,7,8,17,28	129	0,1,17,28
34	3	Short Floating Point Dead Band	1,2	0,1,6,7,8,17,28	129	0,1,17,28
40	0	Analog Output Status —All Variations	1	0,1,6,7,8		
40	1	32-Bit Analog Output Status	1	0,1,6,7,8	129	0,1,17,28
40	2*	16-Bit Analog Output Status	1	0,1,6,7,8	129	0,1,17,28
40	3	Short Floating Point Analog Output Status (32 bit)	1	0,1,6,7,8	129	0,1,17,28
41	0	Analog Output Block —All Variations				
41	1	32-Bit Analog Output Block	3,4,5,6	17,28	129	echo of request
41	2	16-Bit Analog Output Block	3,4,5,6	17,28	129	echo of request
41	3	Short Floating Point Analog Output Block (32 bit)	3,4,5,6	17,28	129	echo of request
50	0	Time and Date—All Variations				
50	1*	Time and Date	1,2	7,8 (index=0)	129	07 (quantity=1)
50	3	Time and Date (Last Recorded Time)	2	7 (quantity=1)	129	
51	1	Time and Date CTO			129	07 (quantity=1)
51	2*	Unsynchronized Time and Date CTO			129	07 (quantity=1)
52	1	Time Delay Coarse			129	07 (quantity=1)
52	2	Time Delay Fine			129	07 (quantity=1)
60	1	Class 0 Data	1,22	6,7,8		
60	2	Class 1 Data	1,20,21,22	6,7,8		
60	3	Class 2 Data	1,20,21,22	6,7,8		
60	4	Class 3 Data	1,20,21,22	6,7,8		
80	1	Internal Indications	1 2	0,1 1 (index 4,7)		
NA	NA	No Object	13,14,23,24			

**Table 5.5 DNP Client (Master) Object**

Obj	Var	Description	REQUEST Func Codes (dec)	REQUEST QualCodes (hex)	RESPONSE Func Codes (dec)	RESPONSE Qual Codes (hex)
1	0	Binary Input—Any Variation	1	0,1,6,7,8,17,28		
1	1	Binary Input—Packed Format	1	0,1,6,7,8,17,28	129	0,1,17,28
1	2	Binary Input—With Flags	1	0,1,6,7,8,17,28	129	0,1,17,28

Obj	Var	Description	REQUEST Func Codes (dec)	REQUEST Qual Codes (hex)	RESPONSE Func Codes (dec)	RESPONSE Qual Codes (hex)
2	0	Binary Input Event—Any Variation	1	6,7,8		
2	1	Binary Input Event—Without Time	1	6,7,8	129,130	17,28
2	2	Binary Input Event—With Absolute Time	1	6,7,8	129,130	17,28
2	3	Binary Input Event—With Relative Time	1	6,7,8	129,130	17,28
10	0	Binary Output—Any Variation	1	0,1,6,7,8,17,28		
10	2	Binary Output—Output Status With Flags	1	0,1,6,7,8,17,28	129	0,1,17,28
11	1	Binary Output Event—Status Without Time			129,130	17,28
11	2	Binary Output Event—Status With Time			129,130	17,28
12	1	Binary Command—Control Relay Output Block (CROB)	3,4,5,6	17,28	129	echo of request
20	0	Counter—Any Variation	1,7,8,9,10	0,1,6,7,8,17,28		
20	1	Counter—32-bit With Flag	1	0,1,6,7,8,17,28	129	0,1,17,28
20	2	Counter—16-bit With Flag	1	0,1,6,7,8,17,28	129	0,1,17,28
20	5	Counter—32-bit Without Flag	1	0,1,6,7,8,17,28	129	0,1,17,28
20	6	Counter—16-bit Without Flag	1	0,1,6,7,8,17,28	129	0,1,17,28
21	0	Frozen Counter—Any Variation	1	0,1,6,7,8,17,28		
21	1	Frozen Counter—32-bit With Flag	1	0,1,6,7,8,17,28	129	0,1,17,28
21	2	Frozen Counter—16-bit With Flag	1	0,1,6,7,8,17,28	129	0,1,17,28
21	5	Frozen Counter—32-bit With Flag and Time of Freeze	1	0,1,6,7,8,17,28	129	0,1,17,28
21	6	Frozen Counter—16-bit With Flag and Time of Freeze	1	0,1,6,7,8,17,28	129	0,1,17,28
21	9	Frozen Counter—32-bit Without Flag	1	0,1,6,7,8,17,28	129	0,1,17,28
21	10	Frozen Counter—16-Bit Without Flag	1	0,1,6,7,8,17,28	129	0,1,17,28
22	0	Counter Event—Any Variation	1	6,7,8		
22	1	Counter Event—32-Bit With Flag	1	6,7,8	129,130	17,28
22	2	Counter Event—16-Bit With Flag	1	6,7,8	129,130	17,28
22	5	Counter Event—32-Bit With Flag and Time	1	6,7,8	129,130	17,28
22	6	Counter Event—16-Bit With Flag and Time	1	6,7,8	129,130	17,28
23	0	Frozen Counter Event—Any Variation	1	6,7,8		

<b>Obj</b>	<b>Var</b>	<b>Description</b>	<b>REQUEST Func Codes (dec)</b>	<b>REQUEST Qual Codes (hex)</b>	<b>RESPONSE Func Codes (dec)</b>	<b>RESPONSE Qual Codes (hex)</b>
23	1	Frozen Counter Event—32-Bit With Flag	1	6,7,8	129,130	17,28
23	2	Frozen Counter Event—16-Bit Without Flag	1	6,7,8	129,130	17,28
23	5	Frozen Counter Event—32-Bit With Flag and Time	1	6,7,8	129,130	17,28
23	6	Frozen Counter Event—16-Bit With Flag and Time	1	6,7,8	129,130	17,28
30	0	Analog Input—Any Variation	1	0,1,6,7,8,17,28		
30	1	Analog Input—32-Bit With Flag	1	0,1,6,7,8,17,28	129	0,1,17,28
30	2	Analog Input—16-Bit With Flag	1	0,1,6,7,8,17,28	129	0,1,17,28
30	3	Analog Input—32-Bit Without Flag	1	0,1,6,7,8,17,28	129	0,1,17,28
30	4	Analog Input—16-Bit Without Flag	1	0,1,6,7,8,17,28	129	0,1,17,28
30	5	Analog Input—Single-prec flt-pt With Flag	1	0,1,6,7,8,17,28	129	0,1,17,28
32	0	Analog Input Event—Any Variation	1	6,7,8		
32	1	Analog Input Event—32-Bit Without Time	1	6,7,8	129,130	17,28
32	2	Analog Input Event—16-Bit Without Time	1	6,7,8	129,130	17,28
32	3	Analog Input Event—32-Bit With Time	1	6,7,8	129,130	17,28
32	4	Analog Input Event—16-Bit With Time	1	6,7,8	129,130	17,28
32	5	Analog Input Event—Single-prec flt-pt Without Time	1	6,7,8	129,130	17,28
32	7	Analog Input Event—Single-prec flt-pt With Time	1	6,7,8	129,130	17,28
40	0	Analog Output Status—Any Variation	1	0,1,6,7,8,17,28		
40	1	Analog Output Status—32-Bit With Flag	1	0,1,6,7,8,17,28	129	0,1,17,28
40	2	Analog Output Status—16-Bit With Flag	1	0,1,6,7,8,17,28	129	0,1,17,28
40	3	Analog Output Status—Single-prec flt-pt With Flag	1	0,1,6,7,8,17,28	129	0,1,17,28
41	1	Analog Output—32-Bit	3,4,5,6	17,28	129	echo of request
41	2	Analog Output—16-Bit	3,4,5,6	17,28	129	echo of request

<b>Obj</b>	<b>Var</b>	<b>Description</b>	<b>REQUEST Func Codes (dec)</b>	<b>REQUEST Qual Codes (hex)</b>	<b>RESPONSE Func Codes (dec)</b>	<b>RESPONSE Qual Codes (hex)</b>
41	3	Analog Output—Single-prec flt-pt	3,4,5,6	17,28	129	echo of request
42	1	Analog Output Event—32-bit Without Time			129,130	17,28
42	2	Analog Output Event—16-bit Without Time			129,130	17,28
42	3	Analog Output Event—32-bit With Time			129,130	17,28
42	4	Analog Output Event—16-bit With Time			129,130	17,28
42	5	Analog Output Event—Single-prec flt-pt Without Time			129,130	17,28
42	7	Analog Output Event—Single-prec flt-pt With Time			129,130	17,28
50	1	Time and Date—Absolute Time	1,2	7 (Qty = 1)	129	7 (Qty = 1)
50	3	Time and Date—Absolute Time at Last Recorded Time	2	7 (Qty = 1)	129	7 (Qty = 1)
51	1	Time and Date CTO—Absolute Time, synchronized			129,130	7 (Qty = 1)
51	2	Time and Date CTO—Absolute Time, unsynchronized			129,130	7 (Qty = 1)
52	1	Time Delay—Coarse			129	7 (Qty = 1)
52	2	Time Delay—Fine			129	7 (Qty = 1)
60	1	Class Objects—Class 0 Data	1	6		
60	2	Class Objects—Class 1 Data	1 20,21	6,7,8 6		
60	3	Class Objects—Class 2 Data	1 20,21	6,7,8 6		
60	4	Class Objects—Class 3 Data	1 20,21	6,7,8 6		
80	1	Internal Indications—Packed Format	1 2	0,1 1 (index 4,7)	129	0,1
NA	NA	No Object (function code only)	13,23 14,24			

## SECTION 6

# Data Viewer

The Data Viewer application displays the near real-time status of any data shared across the Blueframe platform. This rich environment gives end users, who are working in any number of applications within the Blueframe ecosystem, an easy way to see what values are being updated across the system. For example, any client or server added to Blueframe by the Protocol Services applications would be visible to the user, allowing for validation and additional troubleshooting to take place in this powerful tool.

This feature includes the following:

- Live updates of data values
- Ability to save reports
- Custom filters and watchlists

The screenshot shows the SEL Data Viewer interface. On the left, a sidebar navigation tree under 'Publishers' shows 'All Publishers' expanded, with 'dnp' selected, revealing 'DNP Client 1' and 'DNP Client 2'. The main area displays a grid titled 'dnp - DNP Client 1' with columns: Publisher, Point Name, Current Value, Last Changed, and Quality. The grid contains numerous rows for various points like AI\_00000 through AI\_00009 and BI\_00000 through BI\_00009, with values ranging from 0 to false and qualities from GOOD to INVALID. A search bar at the top right says 'Search...'. To the right of the grid is a 'Details' panel with a message 'Select a row to view the item's details'. Below the grid is a 'Watchlist' section with a table showing point names and their current values. At the bottom, there are buttons for 'Connected' (green), 'Live Update' (blue switch), and a refresh icon. Navigation controls at the bottom include 'Rows per page: 20', 'Showing: 1 - 20 / 30 records', and arrows.

**Figure 6.1** Blueframe Data Viewer

**This page intentionally left blank**

---

---

## S E C T I O N   7

---

# Resource Viewer

## Overview

---

The Resource Viewer application displays near real-time status information for assets that are defined within Blueframe Resource Management after communications are defined. The dashboard-like application provides an easy way to better understand the status of your resources in a single location. Select an individual resource in the system for additional status information or for help with troubleshooting potential issues within the system.

This feature currently includes support for the following asset types:

- SEL Real-Time Automation Controllers (RTACs)

### NOTE

Resource Viewer requires that labels be associated with an asset to determine if the asset should be included. For example, SEL RTACs require a label of "rtac".

The remainder of this section explains the four main parts of the Resource Viewer application.

## Resource Tree View

---

The Resource Tree View is a hierarchical display of folders on the left side of the application. This pane mirrors the structure of the Resource Management application. Only resources that include a valid label and which are tied to a supported model type are available for viewing. Folders that do not contain valid entries for display in Resource Viewer appear as unavailable. Select an item in the tree view to populate the Resource Grid with entries contained in that item.

## Resource Grid

---

The Resource Grid, located in the center of the application, is a table that displays resource entries. This table is populated by selecting an item in the Resource Tree View and includes searching and filtering capabilities. You can search for resource names, model types, and other attributes via the search box and filter each column by using the filter icon. Columns can be resized, reordered, and sorted (ascending or descending). Table and column settings can also be managed via the table header menu.

## Details Pane

---

The Details Pane is located on the right side of the application and displays resource information. These data update if the selected entry receives any new information or system data.

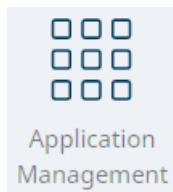
## Individual Resource View

---

Double-clicking a row replaces the Resource Grid with a resource canvas pre-populated with a set number of components, based on the resource type, to provide a deeper look into the status information available in Blueframe.

## SECTION 8

# Application Management



**Figure 8.1 Application Management Icon**

Blueframe offers a rich set of applications that achieve specific tasks. Certain applications are offered in application suites, while others are offered individually. An application suite is designed to have a set of modular applications that solve a set of problems. While applications may belong to a suite, their data and functionality can be shared seamlessly throughout the whole Blueframe system. Use the Application Management tool to learn more about Blueframe applications and manage their installation, versions, components, and health.

## Application Packages

Installations in the Blueframe environment are achieved through the distribution and management of application packages. Blueframe uses application containerization. This means that application installations consist of copying a prepackaged application into Blueframe and then deploying that application package for use within the Blueframe application platform. This section has details on how to add an application package to Blueframe and provides an overview of each package feature.

The screenshot shows the "Application Management" interface. On the left, there's a sidebar with a "SEL" logo and a search bar. The main area is titled "APPLICATION PACKAGES". It lists two packages: "core-services" (SEL, 1.0.4, Installed) and "hw-services" (SEL, 1.0.5, Installed). On the right, a "Package Details" panel is open for "core-services". It shows the package is installed at version 1.0.4 on 2021-02-16T21:43:4... . The "Included Applications" section lists "Application Management" and "Central Authentication". The "Available Versions" section shows "1.0.4" as the installed version. Buttons for "Upgrade", "Downgrade", "Install", "Uninstall", and "Delete" are available.

**Figure 8.2 Application Management Components**

## Adding an Application Package

To begin managing applications, first import an application package file into Blueframe. It is important to understand that importing an application is not the same as installing it. Import an application package file into the Blueframe environment so that you can then manage it. Managing means you can have multiple versions of a package and choose which version to deploy, as shown in *Managing an Application Package on page 123*.

Perform the following steps to import an application package.

- Step 1. To add an application package, launch the Application Management tool and select **Upload Packages**, as shown in *Figure 8.3*.

The screenshot shows the 'Application Management' interface with a dark blue header containing 'SEL' and 'Application Management' along with 'View' and 'About' links. Below the header is a search bar with a magnifying glass icon and a button labeled 'Upload Packages' with an upward arrow icon, both highlighted with orange boxes. The main area is titled 'APPLICATION PACKAGES' and contains a table with two rows of data:

Application Package ▲	Vendor	Installed Version	Package State
core-services	SEL	1.0.1	Installed
hw-services	SEL	1.0.0	Installed

**Figure 8.3 Uploading an Application Package**

- Step 2. Select **Browse**, as shown in *Figure 8.4*, and locate the application package that you want to import into Blueframe. Then, select **Upload** to complete the package import process.

The screenshot shows a modal dialog box titled 'Upload Packages'. At the top right is a close button (X) and a circled '1' over the 'Browse' button, which is highlighted with an orange box. The dialog has two tabs: 'File Name' and 'Size'. Under 'File Name', there is a list item with a delete 'X' icon and the file name 'dma-configuration-monitoring-0.5.3.tgz'. At the bottom right of the dialog is a circled '2' over the 'Upload' button, which is highlighted with an orange box, and a 'Cancel' button.

**Figure 8.4 Importing an Application Package**

- Step 3. Once the import process is complete, Blueframe displays the new package in the list of application packages and the Package State column displays **Available**, as shown in *Figure 8.5*.

APPLICATION PACKAGES				
Application Package ▲		Vendor	Installed Version	Package State
core-services	SEL		0.7.0-beta.f3a6e02	Installed
dma-configuration-monitori...	SEL	--	--	Available
dma-disturbance-monitoring	SEL	--	--	Available
hw-services	SEL		0.0.0-beta.ca5da06	Installed

Figure 8.5 Package State

## Managing an Application Package

Once you have uploaded an application package into Blueframe, you can review its version and description. You can also select the version of the package you want to install into Blueframe. The version you install then becomes available to users of the system. *Installing, Uninstalling, Downgrading, and Deleting an Application Package* on page 123 describes the workflows for installing and uninstalling, downgrading, and deleting a package.

## Installing, Uninstalling, Downgrading, and Deleting an Application Package

Step 1. Select the package you want from the Application Packages list, as shown in *Figure 8.6*.

APPLICATION PACKAGES				
Application Package ▲		Vendor	Installed Version	Package State
core-services	SEL		1.0.1	Installed
hw-services	SEL		1.0.0	Installed

Figure 8.6 Application Packages

Step 2. Select the **Package** tab in the Package Details menu to display one or more package versions under the Available Versions area. Depending on the package version you select, certain action buttons become available or unavailable. The actions include Install, Uninstall, Upgrade, Downgrade, and Delete. Descriptions of these actions follow.

The screenshot shows the 'Package Details' page for the 'core-services' package, version 1.0.1, installed on 2021-02-10T09:23:12Z. The 'Package' tab is selected. Under 'Included Applications', there are six items: Application Management (grid icon), Central Authentication (person icon), Certificate Management (key icon), Security Logs (file with lock icon), User Management (person icon), and Web Portal (SEL logo). Below this is a section for 'Available Versions'. It shows a table with one row for version 1.0.1, which is marked as 'Installed' with a checkmark. The table has columns for Version, Installed, and Description. At the bottom right of the table are buttons for 'Install', 'Uninstall', and 'Delete'. Navigation buttons for 'Upgrade' and 'Downgrade' are also present.

Figure 8.7 Package Details—Install and Delete Actions

**Install:** This action is available when the selected version is not yet installed. Selecting **Install** begins the process of installing the application package into the Blueframe environment.

**Uninstall:** Use the Uninstall action to uninstall an application package. As shown in the *Figure 8.8* warning, if you uninstall a package, you also permanently delete its configuration and any related stored data from the system.

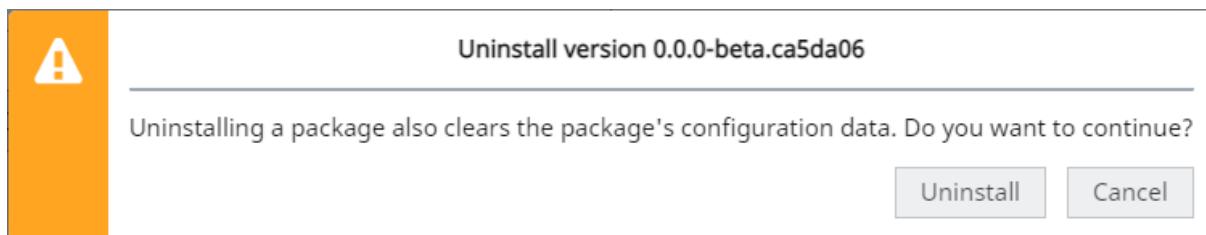


Figure 8.8 Uninstalling Warning

**Upgrade:** The Upgrade action becomes available when you select a newer version of an application package that is presently installed.

**Downgrade:** The Downgrade action becomes available when you select a previous version of an application package that is presently installed.

The screenshot shows the Application Manager interface with the 'Available Versions' tab selected. At the top, there are four buttons: 'Upgrade' (with an upward arrow icon), 'Downgrade' (with a downward arrow icon), 'Install' (with a plus sign icon), and 'Uninstall' (with a minus sign icon). Below these buttons is a 'Delete' button with a trash can icon. A horizontal line separates this from a table. The table has three columns: 'Version', 'Installed', and 'Description'. The first row shows '0.5.0' with a downward arrow icon, 'Connection Services package', and a blue background. The second row shows '0.7.0-alpha.3c3feb6' with a minus sign icon, a green checkmark icon, and 'Connection Services package'. A vertical line also separates the table from the bottom section.

**Figure 8.9 Package Details—Upgrade and Downgrade Actions**

**Delete:** The Delete action is available for application packages that are not presently installed. If you want to delete an installed application package, you must first uninstall it and then delete it.

The screenshot shows the Application Manager interface with the 'Available Versions' tab selected. On the left, there is a sidebar with 'Package Status' and two items: 'Installed' and 'Installed'. In the main area, there is a table with three rows. The first row shows '0.3.0' with an upward arrow icon, 'Security monitoring service'. The second row shows '0.2.0' with a minus sign icon, a green checkmark icon, and 'Security monitoring service'. The third row is partially visible. A modal dialog box is overlaid on the interface. It has an orange header bar with a yellow warning icon and the text 'Delete version 0.1.0'. Below this, a message says 'Are you sure? This action cannot be undone.' At the bottom of the dialog are 'Ok' and 'Cancel' buttons. The background behind the dialog shows the same table and sidebar.

**Figure 8.10 Delete Warning**

#### NOTE

Deleting an application package frees up storage space on your Blueframe node but you lose the capability of downgrading or upgrading to the version you delete.

## Package Services

The Services tab of the Package Details window displays a table with each of the services that make up a package. This table displays a set of columns that indicate the service name and enabled or disabled state. This tab also provides action buttons for restarting, enabling, or disabling a service. *Figure 8.11* shows an example for the core-services application package.

#### NOTE

Do not restart, enable, or disable a service in Application Manager unless SEL technical support directs you to do so. Those options must only be used for troubleshooting purposes.

The screenshot shows the 'Package Details' page for the 'core-services' package. At the top, it displays the package name, installed version (1.0.1), and installation date (2021-02-10T09:23:1...). Below this, there are tabs for 'Package' and 'Services', with 'Services' being the active tab. A row of buttons includes 'Restart Service', 'Enable', and 'Disable'. The main area is a table titled 'Service' with a column for 'Enabled' status. The services listed are: certificate-management, core-services, deployment-lifecycle-manager, dynamic-envoy, l1-opa, l1-proxy-admin, persisted-data, and postgres. All services are marked as 'Enabled' with a green checkmark.

Service	Enabled
certificate-management	✓
core-services	✓
deployment-lifecycle-manager	✓
dynamic-envoy	✓
l1-opa	✓
l1-proxy-admin	✓
persisted-data	✓
postgres	✓

Figure 8.11 Package Service

## Application Licensing

There are two methods for licensing application packages within Blueframe:

1. Purchasing a preconfigured Blueframe machine that comes preloaded with all applications and licenses.
2. Loading a license file into a Blueframe machine.

Note the second method is a two-step process. You must first load the application file by following the instructions described in *System Settings on page 23*. Once the license is installed, upload and install an application package as described in *Adding an Application Package on page 122*.

### NOTE

If you are updating an existing application package, you do not need to reload its license file.

## SECTION 9

# Logging

## System Logs



**Figure 9.1 System Logs Icon**

Blueframe's logging tools help you obtain a historical archive of processes and operations. The System Logs management tool keeps track of security logging events, such as user login and logout attempts, user account changes, and session error occurrences. Such records can help you review overall security logs and gain a good understanding of user actions and processes.

## System Logs Overview

The System Logs management tool displays a historical set of records in a simple grid interface. Additional options provide you the necessary access to manage your records and configure System Logs permissions. *Figure 9.2* shows the main user interface sections.

A screenshot of the System Logs management tool's user interface. The top navigation bar includes icons for SEL, System Logs, View, File, and About. A search bar labeled "Search:" is located above the main grid. The main area is a data table with columns: Timestamp, Username, Severity, Source, Duplica..., and Message. The table contains four rows of log entries:

Timestamp	Username	Severity	Source	Duplica...	Message
04/02/2024, 01:28:50 PM	admin	INFORMATION	securityservice	1	admin logged in
04/02/2024, 11:11:48 AM	admin	INFORMATION	securityservice	1	admin logged in
04/02/2024, 11:11:33 AM	admin	INFORMATION	securityservice	1	admin logged out.
04/02/2024, 10:37:54 AM	admin	INFORMATION	securityservice	1	admin logged in

**Figure 9.2 System Logs Overview**

## System Logs Filters

In addition to the search functionality, the System Logs management tool offers you filters that you can apply and remove effortlessly based on your immediate needs. Each column has a filter icon (🔍) that shows you available options for that column. Selecting one or more filter options in each column automatically results in a combined filter. Certain columns offer options for selecting and deselecting relevant list items, as shown in *Figure 9.3*. Others offer you fields in which you can type key terms and apply logical conditions. Once you apply a filter, the tool displays a dot symbol next to the filter icon to indicate that that column is filtered. You can remove filters by opening the filter menu for each column and unchecking or deleting the applied filters.

System Logs			
Search: <input type="text"/> <input type="button"/>			
Timestamp	Username	Severity	
04/02/2024, 01:28:50 PM	admin	INFORMATION	
04/02/2024, 11:11:48 AM	admin	INFORMATION	
04/02/2024, 11:11:33 AM	admin	INFORMATION	
04/02/2024, 10:37:54 AM	admin	INFORMATION	
04/02/2024, 10:09:39 AM	admin	INFORMATION	

Search...  
 (Select All)  
 Alert  
 Critical  
 Information  
 Notice  
 Warning

Figure 9.3 System Logs Filter Options

## System Logs Application Bar

The System Logs management tool application bar, shown in *Figure 9.4*, provides you with a set of options for further defining parameters for the tool and the management of its logs. The following section describes each available option.



Figure 9.4 System Logs Application Bar Menus

**View:** Provides options for viewing System Logs management tool error, warning, and information notifications.

**File:** Provides three options.

**Export logs:** This menu provides you the ability to export records in .csv format. You can select the number of records you want to export plus other options as shown in *Figure 9.5*.

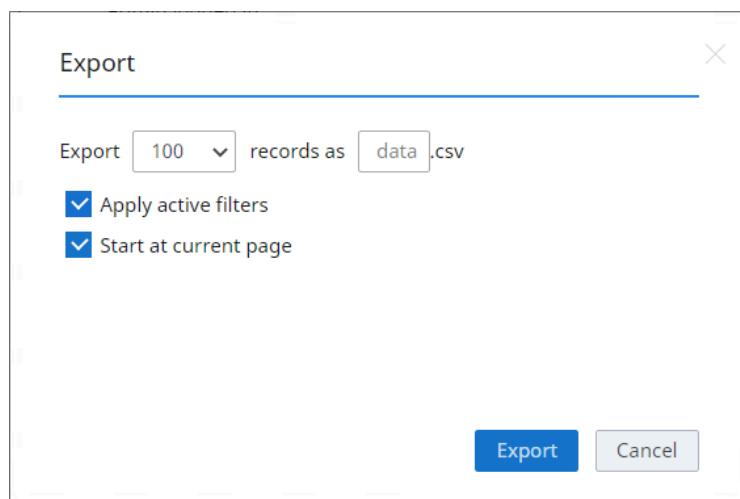


Figure 9.5 Export Logs Menu

**Edit permissions:** Provides options per role to create, delete, manage, and view logs. Note that only users with administrator privileges can adjust these permissions. *Figure 9.6* shows the available options.

**NOTE**

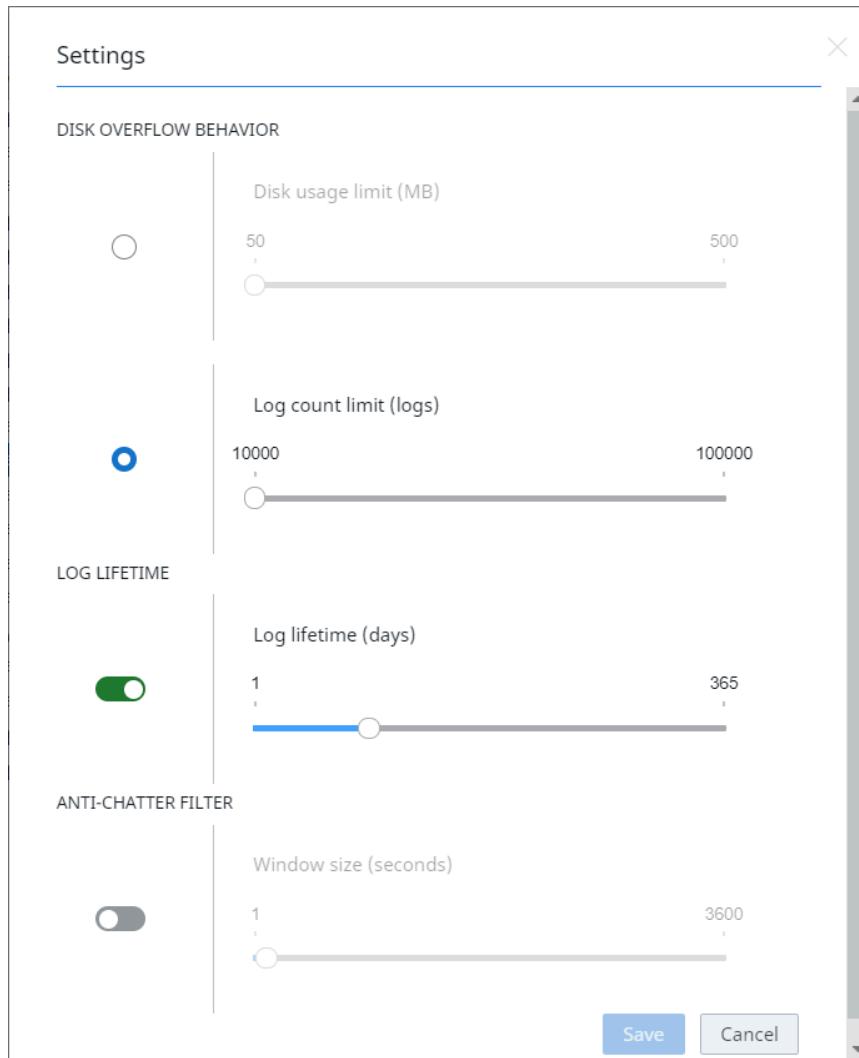
**Create Logs** is enabled by default. You can deselect this option if you do not want to create logs for certain roles within Blueframe.

The screenshot shows a 'Edit Permissions' dialog box. At the top right is a close button (X). Below it is a table titled 'Edit Permissions' with columns for 'Role' and 'Create Logs', 'Delete Logs', 'Manage Logs', and 'View Logs'. The rows represent three user roles: 'admin', 'Engineer', and 'Technician'. The 'Create Logs' column has checked boxes for all three roles. The 'Delete Logs' column has checked boxes for 'admin' and 'Engineer', and an empty box for 'Technician'. The 'Manage Logs' column has checked boxes for 'admin', 'Engineer', and 'Technician'. The 'View Logs' column has checked boxes for 'admin', 'Engineer', and 'Technician'. At the bottom left is a help icon (?), and at the bottom right are 'Save' and 'Cancel' buttons.

Role	Create Logs	Delete Logs	Manage Logs	View Logs
admin	✓	✓	✓	✓
Engineer	✓	□	✓	✓
Technician	✓	□	□	✓

**Figure 9.6 System Logs Permissions**

**Log settings:** The settings menu provides you with multiple options for managing the storage, lifetime, and record-keeping options of the System Logs management tool. For disk storage, you can select disk usage in either MB or a total number of records. Additionally, you can specify the total number of days for the logs to persist. For easier navigation of the system logs list, a final setting is available for displaying redundant records as a single list entry instead of multiple entries.



**Figure 9.7 System Logs Management Settings**

The system log list continues expanding until satisfaction of one of the previously described conditions, at which point newer records replace the oldest records.

**About:** Provides information about the Blueframe application platform and offers a link to the SEL Blueframe Getting Started webpage that contains support literature.

## Syslog

The Syslog protocol, defined in RFC 3164 and RFC 5424, defines how a device can send system event notification messages across IP networks to remote syslog servers. Blueframe sends syslog messages in the RFC 5424 format and can receive syslog messages formatted in either RFC 3164 or RFC 5424. Syslog

is commonly used to send system logs such as security events, system events, and status messages. For example, a printer can send a message that it is running low on ink. The syslog packet size is limited to 1024 bytes and is formatted into three parts: PRI, HEADER, and MSG.

1. **PRI:** A number enclosed in angle brackets that represents both the Facility and Severity of the message. This number is derived as:

$$\text{PRI} = \text{Facility code} \cdot 8 + \text{Severity}$$

The Facility code for a Blueframe node is fixed at 16. The severity is assigned to the message by the system. *Table 9.1* shows the numeric equivalent of various case-sensitive strings. For example, a severity of Informational would have a <134> in the PRI field of the syslog message.

**Table 9.1 Syslog Message Severities Supported in the RTAC**

Numeric Code	Logging Priority String
128	Emergency
129	Alert
130	Critical
131	Error
132	Warning
133	Notice
134	Informational
135	Debug

2. **HEADER:** The message origination time stamp and source. Time stamps are based on the time of the originating host, so it is critical to have time synchronized to accurately correlate events. The source of the message is the Blueframe hostname, which can be configured in **System Setting** on the **Network** page.
3. **MSG:** The human readable body of the message. Messages are constructed from fields as shown in *Table 9.2*.

**Table 9.2 Syslog MSG Configuration Message Component Description**

Logging Device	Blueframe Host ID
Logging Device	Blueframe Host ID
Event Time Stamp	Originating time stamp of the associated log
Log Severity	Specified by the logging application, defaults to <b>Informational</b>
Log Category	Specified by the logging application, defaults to <b>Security</b>
Log Message	Description of the cause of the syslog message

Note the following Syslog message that was generated when user SEL logged in to the Blueframe Portal on March 21, 2022, at 12:09:58.593:

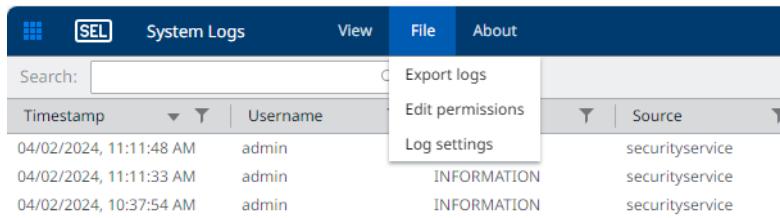
---

```
<134>Mar 21 2022 12:10:08 Blueframe Host ID : 2022-03-21 12:09:58.593, Informational, Security, 'SEL logged in : source'
```

---

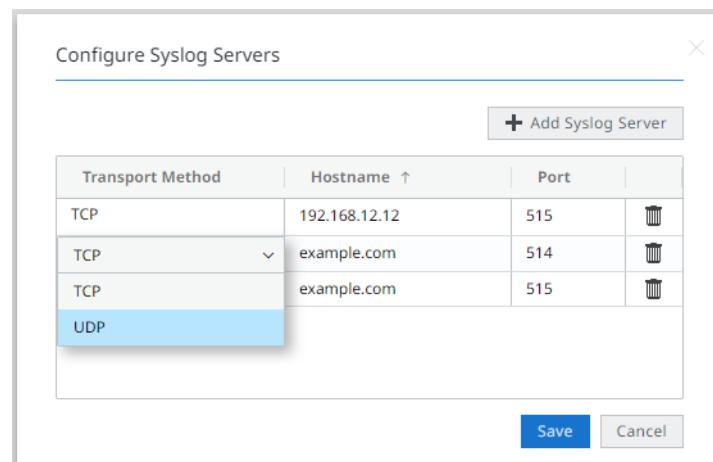
Configure a Blueframe device to send Syslog messages by performing the following steps:

- Step 1. Open the System Logs application and select **File > Log settings**, as shown in *Figure 9.8*.



**Figure 9.8 System Logs File Menu**

- Step 2. Navigate to the Syslog Forwarders configuration section and add a syslog destination. In the resulting dialog, choose a severity level Filter to determine which log messages should be transmitted to that destination.
- Step 3. Select **Add a Syslog Forwarder** and configure the Transport Method, Hostname, and Port. Logs that meet the severity filter criteria for the syslog destination will be sent.



**Figure 9.9 Configuration Dialog for Adding Syslog Server Destinations**

Blueframe can also receive syslog messages from other devices. These messages are stored in system logs and optionally be configured to transmitted to a new end point. Syslog messages can be received via either TCP or UDP on user defined ports.

---

---

## A P P E N D I X    A

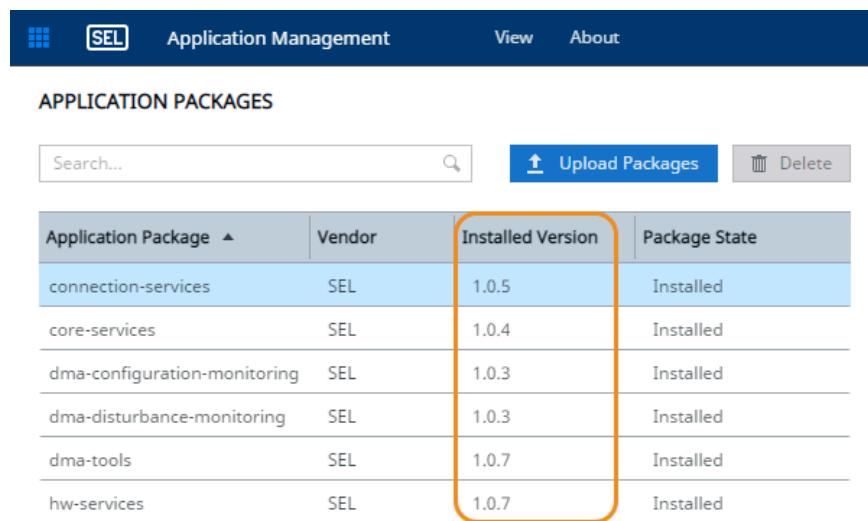
---

# Software and Manual Versions

## Software

---

The following describes the released software versions for the Blueframe application platform and its management tools. For version information related to Blueframe application packages, see their respective manuals. To view the application packages versions currently installed on your Blueframe machine, go to the Application Management tool.



The screenshot shows a web-based application management interface. At the top, there is a header bar with icons for SEL, Application Management, View, and About. Below the header is a search bar labeled "Search..." with a magnifying glass icon, followed by a blue "Upload Packages" button with an upward arrow icon and a grey "Delete" button with a trash can icon. The main content area is titled "APPLICATION PACKAGES". It contains a table with the following data:

Application Package ▲	Vendor	Installed Version	Package State
connection-services	SEL	1.0.5	Installed
core-services	SEL	1.0.4	Installed
dma-configuration-monitoring	SEL	1.0.3	Installed
dma-disturbance-monitoring	SEL	1.0.3	Installed
dma-tools	SEL	1.0.7	Installed
hw-services	SEL	1.0.7	Installed

**Figure A.1 Blueframe Application Versions**

*Table A.1* lists the Blueframe Operating System and Hardware Services package versions, a description of the changes, and the manual date code corresponding to the package version. The table lists the most recent package version first.

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 A.1 Blueframe Operating System and Hardware Services Package Version History**

Package Version Number	Summary of Revisions	Manual Date Code
1.11.0	<ul style="list-style-type: none"> <li>► The local display now supports automatic login for a configured user account.</li> <li>► Added a configurable option to disable the local display.</li> <li>► Network settings changes related to redundancy are disabled when redundancy is enabled.</li> <li>► Added support for a read-only permission in Application Management.</li> <li>► Added a setting for the MTU specification on a network interface.</li> <li>► Modified the severity values of redundancy status messages for syslog.</li> <li>► Added a status message to the portal page for when an account logs into Blueframe with no role assigned.</li> <li>► Resolved an issue where some applications attempted to connect to their source repository.</li> <li>► Resolved an issue where a user who has reached inactivity timeout is shown an access denied screen instead of returning to the login page.</li> <li>► Modified a redundancy node to generate a syslog status message and shut down if the disk state changes to diskless or error.</li> <li>► Added the ability to provide a notification that storage has consumed a user-configurable percentage of available space.</li> <li>► Added an error message screen if Blueframe is unable to load files from the local disk on startup.</li> <li>► Removed the TestLab menu from the web browser on the local display interface.</li> <li>► Added a message to the redundancy state changes to remind users that all nodes must have the same OS version. Otherwise, redundancy will not operate properly.</li> </ul>	20250106
1.10.0	<ul style="list-style-type: none"> <li>► [Cybersecurity] Resolved an issue where an authenticated user attempting to change their password could do so without using the current password.</li> <li>► [Cybersecurity] Resolved a cross-site scripting issue that was only accessible by valid authenticated users.</li> <li>► The System Name setting in the System Settings application now always displays on the header bar.</li> <li>► Added a new account permission to allow access to network diagnostic utilities.</li> <li>► Network diagnostic utility queries are now recorded in Blueframe's system logs.</li> <li>► Resolved an issue where 503 Service Unavailable responses were returned when attempting to access data or open applications.</li> <li>► Resolved an issue where the X.509 certificate could not be deleted.</li> <li>► Resolved an issue where pages would not load or the user was incorrectly redirected to the login page when attempting to navigate the Blueframe UI.</li> <li>► Resolved an issue where some syslog messages did not contain the data from the AppID field in the system logs application.</li> <li>► Resolved an issue where a backup node in a redundancy configuration incorrectly reported an inconsistent disk state.</li> <li>► Resolved an issue where a primary node in a redundancy configuration incorrectly reported a loss of communications to backup nodes with an "incompatible firmware" message.</li> <li>► Resolved an issue where backups could not be restored.</li> <li>► Resolved an issue where IRIG-B synchronization status was shown incorrectly.</li> <li>► Resolved an issue where Blueframe web services could not be accessed through port forwarding or network address translation. Each individual application will need to be updated to support this functionality. Check the release notes for desired applications.</li> </ul>	20241105

Package Version Number	Summary of Revisions	Manual Date Code
1.9.0	<ul style="list-style-type: none"> <li>► [Cybersecurity] Resolved an issue where a specifically crafted query parameter could redirect traffic to an external connection.</li> <li>► [Cybersecurity] Resolved an issue where sensitive data was returned from GET requests in a non-protected format for authenticated users with appropriate permissions.</li> <li>► [Cybersecurity] Users are now logged out after a period of keyboard and mouse inactivity in active Blueframe web connections in addition to when a web browser tab is closed.</li> <li>► [Cybersecurity Enhancement] Updated BIOS versions: <ul style="list-style-type: none"> <li>➢ SEL-3350: 11.3.49152.117</li> <li>➢ SEL-3355-2: 12.6.49152.98</li> </ul> </li> <li>► Added support for receiving and storing syslog messages.</li> <li>► Added support for forwarding received syslog messages.</li> <li>► Added Redundancy support for hardware nodes.</li> <li>► Added Redundancy support for multiple backup nodes.</li> <li>► Improved Redundancy with additional statistics regarding the communications status between nodes.</li> <li>► Added network diagnostics utilities to the System Settings application.</li> <li>► Added Import/Export configuration options to the System Settings, Certificate Management, and Central Authentication applications.</li> <li>► Enhanced RADIUS to detect challenge messages and provide prompts for users to enter additional criteria required by the RADIUS server.</li> <li>► Resolved an issue where backups could not be created if Connection Services version 1.13.1 was installed.</li> <li>► Resolved an issue introduced in version 1.8.0 where the enterprise ID was changed after a factory reset.</li> </ul>	20240425
1.8.0	<ul style="list-style-type: none"> <li>► [Cybersecurity] Resolved an issue introduced in 1.7.2 where the local user interface was not accessible after the cluster IP address was changed from its default value.</li> <li>► [Cybersecurity] Resolved an issue where certificates with a length of 1024 bits could not be activated. Minimum certificate length is now 2048 bits.</li> <li>► [Cybersecurity] Resolved an issue where LDAP users were forced to change their password after the local expiration period for local accounts.</li> <li>► [Cybersecurity] Resolved an issue where applications may not start after a power cycle.</li> <li>► [Cybersecurity] Resolved an issue where LDAP users could not log in after the user was deleted in the User Management application.</li> <li>► Added support for redundancy.</li> <li>► Added support for standby mode.</li> <li>► Resolved an issue introduced in 1.7.2 where the local user interface browser launcher was not available.</li> <li>► Resolved an issue where restoring a system backup file did not delete existing CA certificates.</li> <li>► Resolved an issue in LDAP where authenticated users did not receive the correct role due to a difference in casing between the Blueframe configuration and the text returned from the LDAP server.</li> </ul>	20231127

Package Version Number	Summary of Revisions	Manual Date Code
1.7.2	<ul style="list-style-type: none"> <li>▶ [Cybersecurity] Updated BIOS versions:           <ul style="list-style-type: none"> <li>➢ SEL-3350: 1.3.49152.117</li> <li>➢ SEL-3355-2: 2.6.49152.98</li> </ul> </li> <li>▶ [Cybersecurity Enhancement] Added support for RADIUS.</li> <li>▶ Added support for the ip, ping, traceroute, pdpeek, and help commands in Blueframe Diagnostics GUI.</li> <li>▶ Increased length for Role Names to 64 characters.</li> <li>▶ Renamed the Security Logs application to System Logs.</li> <li>▶ Added verification when importing signed certificates that the private key data matches Blueframe's key.</li> <li>▶ [Cybersecurity] Closed UDP port 8472.</li> <li>▶ [Cybersecurity] Resolved an issue where user accounts associated with LDAP that contained special characters could not login.</li> <li>▶ [Cybersecurity] Resolved an issue when editing Systems Settings Permissions where incorrect settings were displayed to the user.</li> <li>▶ Resolved an issue where packet requests could be issued on other network interfaces than the interface to which the user was currently connected.</li> <li>▶ Resolved an issue introduced in 1.5.1 where the dashboard in System Settings could no longer display some diagnostic information.</li> <li>▶ Resolved an issue where syslog message header components were incorrectly ordered.</li> <li>▶ Resolved an issue where the certificate issuer was incorrectly displayed.</li> <li>▶ Resolved an issue where licenses that did not have an application installed did not show all license data.</li> </ul>	20230912
1.6.3	<ul style="list-style-type: none"> <li>▶ Added the capability for the Virtual Machine Hostname to be edited by the user.</li> <li>▶ Resolved an issue with unclear firmware upgrade stage indications.</li> <li>▶ Resolved an issue where the description and policy on the settings UI would be submitted by the user but not show the change.</li> <li>▶ Resolved an issue that resulted in a state where the Blueframe instance would only return 404 errors.</li> <li>▶ Resolved an issue that would prevent application installation when a static host was configured.</li> <li>▶ Resolved an issue where random Unicode characters would appear in the information screens.</li> <li>▶ Resolved an issue where Host entries would prevent the creation of a backup.</li> <li>▶ Resolved an issue where an LDAP user account would be deactivated in Blueframe when an administrator of Blueframe viewed the account details for the first time after the LDAP user had logged in.</li> </ul>	20230620
1.6.0	<ul style="list-style-type: none"> <li>▶ [Cybersecurity Enhancement] Added Syslog protocol for sending system logs.</li> <li>▶ Added a visual progress indicator for firmware uploads.</li> <li>▶ Added a diagnostic console.</li> <li>▶ Added support for the optional serial expansion board on the SEL-3350 3U.</li> <li>▶ Added support for IRIG on the SEL-3390S8 and SEL-3390T cards.</li> <li>▶ Removed plain text passwords from exported project data.</li> <li>▶ Resolved an issue where the password updated field would not update after a user password change.</li> <li>▶ Resolved an issue where a username with single quotes could not log in to the system.</li> <li>▶ Resolved an issue where a failed application install may prevent future installation.</li> <li>▶ Resolved an issue where logs are not preserved after reboot.</li> <li>▶ Resolved an issue where IRIG was not working on the SEL-3350.</li> <li>▶ Resolved an issue that prevented an upgrade after a failed upgrade attempt.</li> </ul>	20230330
1.5.2	<ul style="list-style-type: none"> <li>▶ Updated BIOS versions:           <ul style="list-style-type: none"> <li>➢ SEL-3350: 1.2.49152.142</li> <li>➢ SEL-3355-2: 2.5.49152.263</li> </ul> </li> <li>▶ [Cybersecurity Enhancement] Added a Security Logs entry when Blueframe is set to factory-default settings that includes the initiating method or user.</li> </ul>	20221103

Package Version Number	Summary of Revisions	Manual Date Code
1.5.1	<ul style="list-style-type: none"> <li>► Added support for the b2069 SEL-3390E4 card.</li> <li>► Prevented attached monitors from entering power-saving mode during periods of inactivity.</li> <li>► Resolved an issue where communications lock up on an SEL-3350 serial port.</li> <li>► Resolved an issue where external network access was unavailable due to Blueframe applications without a configured default gateway.</li> <li>► Fixed duplicate licenses from being shown on the Licensing interface in virtual machine deployments.</li> </ul>	20220930
1.4.1	<ul style="list-style-type: none"> <li>► Resolved an issue where NTP client could not be enabled unless NTP server was enabled.</li> <li>► Resolved an issue where users were permitted to specify static default gateways on multiple interfaces.</li> <li>► Resolved an issue where UTF characters could be entered into some fields but would not display after submission.</li> <li>► Resolved an issue where the Dashboard was not properly displaying the platform metrics.</li> <li>► Resolved an issue where memory usage of the local display would increase until the solution became unresponsive.</li> <li>► Resolved an issue in Virtual Machine deployments where the desktop background was different than on the SEL appliance deployments.</li> <li>► Resolved an issue where the system time could not be set by the user before sync-lock when time synchronization was turned on.</li> </ul>	20220520
1.4.0	<ul style="list-style-type: none"> <li>► Added support for the SEL SDN Flow Controller package.</li> </ul>	20210921
1.3.0	<ul style="list-style-type: none"> <li>► Updated BIOS versions:           <ul style="list-style-type: none"> <li>➢ SEL-3350: 1.1.49152.36</li> <li>➢ SEL-3355-2: 2.4.49152.159</li> </ul> </li> </ul> <p><b>NOTE</b> BIOS updates will be automatically applied on upgrade, if required, and will cause extra restarts as various board-level firmware are updated.</p>	20210914
1.2.3	<ul style="list-style-type: none"> <li>► Added support for virtual environment deployments.</li> </ul>	20210813
1.0.7	<ul style="list-style-type: none"> <li>► Initial version of the Blueframe OS and <b>System Settings</b> management tool.</li> </ul>	20210223

*Table A.2* lists the Blueframe Core Services package versions, a description of the changes, and the manual date code corresponding to the package version. The table lists the most recent package version first.

**Table A.2 Blueframe Core Services Package Version History**

Package Version Number	Summary of Revisions	Manual Date Code
1.4.15	<ul style="list-style-type: none"> <li>► Resolved an issue where group names with unusual characters associated with an LDAP user could prevent successful user authentication into Blueframe.</li> <li>► Resolved an issue where the Application Manager would erroneously report success for failed user-initiated operations.</li> <li>► Clarified the User ID Attribute settings value format and enhanced error messages from incorrect entries.</li> <li>► Resolved an issue where an X.509 certificate imported as a new certificate with a private key could not subsequently be activated.</li> <li>► Resolved an issue where application-specific permissions would not persist after a Blueframe device was restarted.</li> <li>► Fixed duplicate licenses from being shown on the Licensing interface in virtual machine deployments.</li> </ul>	20220930
1.4.6	<ul style="list-style-type: none"> <li>► Resolved an issue where navigating away from the Application Management UI while an application was being installed would cause the installation to be canceled.</li> <li>► Resolved an issue where the self-signed certificate generated by a user for the Blueframe device with the requisite host names could not be directly added as a trusted CA in the user's client browser.</li> <li>► Enhanced the Application Launcher navigation menu to sort group headers for applications alphabetically.</li> <li>► Clarified how the expiration of an account does not suspend active sessions in the Blueframe Instruction Manual.</li> <li>► Resolved an issue where the last login or logout was not being recorded for LDAP users.</li> <li>► Resolved an issue where case-insensitive identity providers such as LDAP could allow multiple user profiles to be created with different casing based on how the user entered their username into the login page.</li> <li>► Resolved an issue with rendering some UTF characters caused by multiple services using inconsistent font families.</li> <li>► Resolved an issue where the initial user creation screen would not allow some passwords that met the default password complexity policy.</li> <li>► Resolved an issue where an external DNS lookup used to access the solution at a subdomain of corporate systems could lead to account permissions failures.</li> <li>► Resolved an issue where large package uploads would fail over slow networks.</li> <li>► Corrected the Common Name for the initially generated self-signed certificate.</li> </ul>	20220520
1.3.2	<ul style="list-style-type: none"> <li>► Added support for the SEL SDN Flow Controller package.</li> </ul>	20210921
1.2.1	<ul style="list-style-type: none"> <li>► Added support for virtual environment deployments.</li> </ul>	20210813
1.0.4	<ul style="list-style-type: none"> <li>► Initial version of Blueframe management tools:           <ul style="list-style-type: none"> <li>► Application Management</li> <li>► Central Authentication</li> <li>► Certificate Management</li> <li>► Security Logs</li> <li>► User Management</li> </ul> </li> </ul>	20210223

*Table A.3* lists the Connection Services package versions, a description of the changes, and the manual date code corresponding to the package version. The table lists the most recent package version first.

**Table A.3 Connection Services Package Version History**

Package Version Number	Summary of Revisions	Manual Date Code
1.16.1	<ul style="list-style-type: none"> <li>► <b>Resource Management</b> functionality: <ul style="list-style-type: none"> <li>➢ Resolved an issue where parameters would fail to update when editing a Profile Session or Connection when users upgraded from Connection Services Package version 1.15.x to 1.16.0.</li> <li>➢ Updated the user interface to indicate where Profile upgrades require user interaction.</li> </ul> </li> </ul>	20250212
1.16.0	<ul style="list-style-type: none"> <li>► <b>Resource Management</b> functionality: <ul style="list-style-type: none"> <li>➢ Resolved an issue that prevented an enumerated parameter list from being edited when the Enter key was pressed.</li> <li>➢ Resolved an issue that caused Sessions to not appear in the Resources detail view.</li> <li>➢ Resolved an issue that caused an exception when a Profile's credential label was changed.</li> <li>➢ Resolved an issue that caused duplicate options in the dropdown menu for per-instance session connection parameter values.</li> <li>➢ Resolved an issue that caused an exception if a built-in template parameter was used in a non-templated access script.</li> <li>➢ Resolved an API issue that prevented Resource Management from retrieving data necessary for display when the resource count was an n-1 value close to the page-size boundary (n).</li> <li>➢ Resolved an issue that caused the header sorting to not work in profile instances.</li> <li>➢ Resolved an issue that caused the session template connection parameters to revert to the to-do value during editing.</li> <li>➢ Resolved an issue that showed a Session's SEL Protocol configuration choice as SSH Access on subsequent edits.</li> <li>➢ Resolved an issue that caused values to be shown by default in the Profile Instance dropdown parameters for new Profile Instances with no defined value.</li> <li>➢ Resolved an issue that caused the Resource Access Lists to report no resources in lists.</li> <li>➢ Added support for Sessions on COMPROC connections.</li> <li>➢ Added a context menu in Resource Management to assign Profile Parameter values to the initially undefined values.</li> <li>➢ Added support for unified importing and exporting of Resource Management Resources, Profiles, and Instances.</li> <li>➢ Added a progress indicator for the export/import process.</li> <li>➢ Added Profile support for the TERMINALGATEWAY protocol connection.</li> <li>➢ Added support for parent-child connection configuration within Profiles.</li> <li>➢ Added an About Resource Management menu item with the ability to collect support data.</li> <li>➢ Added a Select All option for Roles in Session configuration.</li> <li>➢ Updated the Child Resources table to show child resources of COMPROC connections that are unknown devices. These resources can now be removed in the Edit Child Resources dialog window.</li> <li>➢ Updated the required Reset Data confirmation text to be RESET rather than DELETE.</li> <li>➢ Updated the Show/Hide empty folders icon to indicate if there are empty folders.</li> <li>➢ Improved performance of the Resource Access List user interface for large resource counts.</li> </ul> </li> </ul>	20250106
1.15.2	<ul style="list-style-type: none"> <li>► <b>Resource Management</b> functionality: <ul style="list-style-type: none"> <li>➢ Addressed an issue in TERMINALGATEWAY connection children where settings were always shown as changed.</li> <li>➢ Addressed an issue that prevented the assignment of connections to templated session instances.</li> </ul> </li> </ul>	20240905

Package Version Number	Summary of Revisions	Manual Date Code
1.15.1	<ul style="list-style-type: none"> <li>► <b>Resource Management</b> functionality:           <ul style="list-style-type: none"> <li>➢ Resolved an issue that could result in duplicate attribute names being present when changing resource presets.</li> <li>➢ Resolved an issue where resources may remain in the side detail view after being deleted.</li> <li>➢ Resolved an issue that prevented export selection of certain combinations of parent-child devices.</li> <li>➢ Resolved an issue that prevented edits to child device gateway parameters.</li> <li>➢ Resolved an issue that locked the increment/decrement controls of the delay time values on the COMPROC protocol.</li> <li>➢ Resolved an issue that prevented the modification of child device credential used in parent-child connections (this issue did not impact COMPROC parent-child connections).</li> <li>➢ Resolved an issue that prevented the addition of a gateway child to a COMPROC connection.</li> <li>➢ Resolved an issue where a restricted user could be presented with an exception error when a resource access list referenced an unknown device.</li> <li>➢ Resolved an issue that incorrectly marked instance credential labels as duplicates in the Create Credentials features of Profiles.</li> <li>➢ Resolved an issue that caused the show/hide empty folders button in Resource Selection to have no effect.</li> <li>➢ Resolved an issue that prevented BRE and ACC level assignments in Sessions.</li> <li>➢ Resolved an issue that reverted some session template settings to default after editing and saving.</li> <li>➢ Resolved an issue that prevented exporting when a folder and subfolder were both selected.</li> <li>➢ Updated invalid parameter references to now display the reason why they are invalid within their dropdown rows.</li> <li>➢ Updated to allow existing device credentials to be used when a child device is added to a parent connection rather than automatically creating a new credential template every time.</li> <li>➢ Added support for Access Level C on SEL communication processors.</li> <li>➢ Added specific access level support for the SEL-734B and SEL-734W.</li> <li>➢ Added the ability to save changes during profile deployment.</li> <li>➢ Added Parent Folder context to the Create Folder dialog.</li> <li>➢ Added a progress indicator for profile actions.</li> <li>➢ Added support for allow/denylist and access level settings in Profile Sessions templates with per-instance connection configurations.</li> <li>➢ Added the ability to apply a single value to an entire column in a grid in Profile Instance Credentials.</li> </ul> </li> <li>► <b>Notifications</b> functionality:           <ul style="list-style-type: none"> <li>➢ Added the ability to reset all data.</li> </ul> </li> </ul>	20240823
1.15.0	<ul style="list-style-type: none"> <li>► <b>Resource Management</b> functionality:           <ul style="list-style-type: none"> <li>➢ Improved performance for handling higher device counts.</li> <li>➢ Improved application loading times by loading resources either when the resource is selected or when a node in the organizational parent structure is selected.</li> </ul> </li> </ul>	20240628
1.14.2	<ul style="list-style-type: none"> <li>► <b>Resource Management</b> functionality:           <ul style="list-style-type: none"> <li>➢ Resolved a multi-user issue where Profile child device changes from one user would reset another user's unsaved changes.</li> <li>➢ Added the ability to define areas of responsibility for resource access and viewing.</li> <li>➢ Added a resource count and resource name filtering to the profile deployment dialog.</li> <li>➢ Added a "Move To" selection in the right-click menu for organizing resources in Resource Management.</li> <li>➢ Added the ability to add credential settings directly from the Profile Instance Credentials view.</li> <li>➢ Added the ability to add a missing credential setting for a connection in the Connection Settings view.</li> <li>➢ Added the ability to export selected resources.</li> <li>➢ Added a show/hide empty folders option in Resource Tree.</li> </ul> </li> </ul>	20240425

Package Version Number	Summary of Revisions	Manual Date Code
1.13.1	<p>► <b>Resource Management</b> functionality:</p> <ul style="list-style-type: none"> <li>➢ Resolved an issue where the attribute presets would not correctly change the attribute list.</li> <li>➢ Changed Resource Management to resize properly when the application launcher is pinned.</li> <li>➢ Resolved an issue where information messages regarding profile draft or deployment states could be duplicated.</li> <li>➢ Resolved an issue where COMPROC SSH connections did not have an SEL credential.</li> <li>➢ Removed device images from the Resource Overview page.</li> <li>➢ Resolved an issue that prevented connection template edits for certain COMPROC connections.</li> <li>➢ Updated to show users a warning when a folder is being created or renamed to a folder name that already exists at the same position.</li> <li>➢ Enhanced ease-of-use features for the Profile user interface.</li> </ul>	20240112
1.13.0	<p>► <b>Resource Management</b> functionality:</p> <ul style="list-style-type: none"> <li>➢ Resolved an issue where profile group templates were incorrectly displayed in the Services tab.</li> <li>➢ Resolved an issue where all credential levels would inaccurately appear for a profile instance for some SEL relay models.</li> <li>➢ Resolved an issue where exporting a large number of resources could cause a time-out.</li> <li>➢ Resolved an issue where profiles did not correctly handle a POSTGRES connection template.</li> <li>➢ Resolved an issue where older credentials could be referenced in Resource Management when using DMA Credential Management.</li> <li>➢ Added support for exporting selected instances.</li> <li>➢ Added support for customized column sorting.</li> </ul>	20231127
1.12.1	<p>► <b>Resource Management</b> functionality:</p> <ul style="list-style-type: none"> <li>➢ Improved handling of the credential cache.</li> </ul>	20231031
1.12.0	<p>► <b>Resource Management</b> functionality:</p> <ul style="list-style-type: none"> <li>➢ For Profile managed resource instances, credentials may be managed separately from the profile to enable integration with DMA Credential Management.</li> <li>➢ Added column selection to the resource table.</li> </ul>	20231020
1.11.3	<p>► <b>Resource Management</b> functionality:</p> <ul style="list-style-type: none"> <li>➢ Resolved an issue where resource connection would inaccurately reference other resources when the same credential name was used.</li> </ul>	20230922
1.11.2	<p>► Resolved an issue where the Resource Management and Notification applications may not open after low system memory conditions.</p>	20230912
1.11.1	<p>► <b>Resource Management</b> functionality:</p> <ul style="list-style-type: none"> <li>➢ Resolved an issue where changing the profile name made the resource template tab blank.</li> <li>➢ Resolved an issue where a profile would not deploy when there were 500 or more instances.</li> <li>➢ When credential modification actions for a resource are taken, Resource Management now logs entries to the Security Log.</li> </ul>	20230818
1.10.0	<p>► <b>Resource Management</b> functionality:</p> <ul style="list-style-type: none"> <li>➢ Resolved an issue with text rendering when the dark theme is in use.</li> <li>➢ Resource Management import from csv-to-crate tool now handles nested communications processors.</li> <li>➢ Resolved an issue where a device with a missing parent node would cause a failure with the Resource Management import from csv-to-crate tool.</li> <li>➢ Added support for profile parameters in Resource Management.</li> <li>➢ Added support for device attribute presets in Resource Management Profile creation.</li> <li>➢ Added support for enumerated profile template parameters.</li> <li>➢ Added support for RTAC profiles with templated POSTGRES protocol connections.</li> <li>➢ Added support for the SFTP protocol.</li> </ul>	20230620

Package Version Number	Summary of Revisions	Manual Date Code
1.9.5	<ul style="list-style-type: none"> <li>▶ <b>General</b> functionality: <ul style="list-style-type: none"> <li>➢ Resolved an issue where connections using SEL over SSH could lose their credentials during editing.</li> </ul> </li> <li>▶ <b>Resource Management</b> functionality: <ul style="list-style-type: none"> <li>➢ Added support for gateway devices in Resource Management Profiles.</li> <li>➢ Resolved an issue with adding Session Templates to an existing profile with many deployed instances.</li> <li>➢ Added configured session information to the Resource Management details pane.</li> <li>➢ In Resource Management, double clicking on a resource in the navigation tree now opens the details view.</li> <li>➢ Added support for HTTP connections.</li> <li>➢ Added support for SEL Client Serial connections.</li> </ul> </li> <li>▶ <b>Notifications</b> functionality: <ul style="list-style-type: none"> <li>➢ Added the ability to send a test email to a recipient group in Notifications.</li> <li>➢ Added API documentation for Notifications.</li> </ul> </li> </ul>	20230330
1.8.0	<ul style="list-style-type: none"> <li>▶ <b>Resource Management</b> functionality: <ul style="list-style-type: none"> <li>➢ Added support for email notifications with SMTP email servers.</li> <li>➢ Resolved an issue in Resource Management where the connection settings for SELFTP connections showed the TELNET port value as the FTP port.</li> <li>➢ Resolved an issue where custom application permission mappings would be cleared after a power-cycle.</li> <li>➢ [Cybersecurity Enhancement] HTTP responses for Resource Management have the HTTP header X-Frame-Options set to SAMEORIGIN. See <a href="https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options">https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options</a>.</li> <li>➢ Added support for templating HTTPS connections in Profiles.</li> </ul> </li> <li>▶ <b>Notifications</b> functionality: <ul style="list-style-type: none"> <li>➢ Added support for Notifications through SMTP connections.</li> </ul> </li> </ul>	20221216
1.7.7	<ul style="list-style-type: none"> <li>▶ <b>General</b> functionality: <ul style="list-style-type: none"> <li>➢ Added support for SEL over TCP, including Raw TCP.</li> </ul> </li> <li>▶ <b>Resource Management</b> functionality: <ul style="list-style-type: none"> <li>➢ Added Profile and Templates support.</li> <li>➢ Enhanced import and export to include Sessions.</li> <li>➢ Improved feedback when an import fails.</li> </ul> </li> </ul>	20220930
1.6.3	<ul style="list-style-type: none"> <li>▶ <b>Resource Management</b> functionality: <ul style="list-style-type: none"> <li>➢ [Cybersecurity Enhancement] Added enhanced permission definitions to define which users with access to Resource Management may view resource passwords.</li> <li>➢ [Cybersecurity Enhancement] Enhanced support for HTTPS connections to enable publishing to a user-defined HTTPS URL.</li> <li>➢ Exposed the Swagger documentation for the Resource Management read-only API.</li> <li>➢ Added support for COMPROC communications, including SEL-2020, SEL-2030, SEL-2032 Communications Processors; SEL RTAC SEL Server; and SEL RTAC Access Point Routers.</li> <li>➢ Added support for the NO YMODEM setting to interleave transfer of device data.</li> </ul> </li> </ul>	20220811
1.5.0	<ul style="list-style-type: none"> <li>▶ <b>General</b> functionality: <ul style="list-style-type: none"> <li>➢ Moved the DMA communication and logging services (DMA Core) from the Connection Services package to their own package, Resource Communication Services.</li> <li>➢ Expanded SEL device data collection support.</li> </ul> </li> <li>▶ <b>Resource Management</b> functionality: <ul style="list-style-type: none"> <li>➢ Enhanced user interface visual layout.</li> <li>➢ Added Session support for when Direct Resource Access (in the Resource Communication Services package) is installed.</li> <li>➢ Added resource saved filters for quick searching capability.</li> </ul> </li> </ul>	20220520
1.4.0	<ul style="list-style-type: none"> <li>▶ <b>DMA Core</b> functionality: <ul style="list-style-type: none"> <li>➢ Added support for MMS protocol.</li> <li>➢ Expanded SEL device data collection support.</li> </ul> </li> <li>▶ <b>Resource Management</b> functionality: <ul style="list-style-type: none"> <li>➢ Added support for MMS protocol.</li> </ul> </li> </ul>	20211008

Package Version Number	Summary of Revisions	Manual Date Code
1.3.0	<ul style="list-style-type: none"> <li>▶ <b>DMA Core</b> functionality:           <ul style="list-style-type: none"> <li>➢ Added support for Credential Management password rotation automation.</li> </ul> </li> <li>▶ <b>Resource Management</b> functionality:           <ul style="list-style-type: none"> <li>➢ Added details panel viewing for multiple connections.</li> <li>➢ Improved Resource Tree view filtering capability.</li> </ul> </li> </ul>	20210813
1.2.3	<ul style="list-style-type: none"> <li>▶ <b>DMA Core</b> functionality:           <ul style="list-style-type: none"> <li>➢ Added support for SSH and FTP protocols.</li> </ul> </li> <li>▶ <b>Resource Management</b> functionality:           <ul style="list-style-type: none"> <li>➢ Added support for SSH and FTP protocols.</li> <li>➢ Creation of multiple connections for a resource.</li> </ul> </li> </ul>	20210507
1.0.5	<ul style="list-style-type: none"> <li>▶ Initial version that includes support for DMA Core and Resource Management:           <ul style="list-style-type: none"> <li>➢ <b>DMA Core</b> functionality:               <ul style="list-style-type: none"> <li>➢ Automation logic configuration and execution.</li> </ul> </li> <li>➢ <b>Resource Management</b> functionality:               <ul style="list-style-type: none"> <li>➢ Resource definitions for use in the Blueframe system.</li> </ul> </li> </ul> </li> </ul>	20210222

*Table A.4* lists the Blueframe Protocol Services package versions, a description of the changes, and the manual date code corresponding to the package version. The table lists the most recent package version first.

**Table A.4 Blueframe Protocol Services Package Version History**

Package Version Number	Summary of Revisions	Manual Date Code
1.2.1	<ul style="list-style-type: none"> <li>▶ Increased support for as many as 1000 DNP clients and as many as 500K points across all DNP clients.</li> <li>▶ Enhanced the configuration editor to enable/disable related settings fields without saving the configuration first.</li> <li>▶ Resolved an issue where the DNP UDP and TLS transport methods did not accept/create connections.</li> <li>▶ Resolved an issue where some protocol services versions would not upgrade to the next version.</li> <li>▶ Resolved an issue where when an item was copied, additional copies would be generated incorrectly.</li> <li>▶ Resolved an issue where Ethernet multidrop did not accept multiple connections on a single port.</li> <li>▶ Resolved an issue where the Link Status Timeout setting was not applied to the DNP client operation.</li> <li>▶ Resolved an issue in the DNP server where per point object variant settings could not be modified.</li> <li>▶ Resolved an issue in the create copies dialog where text could be entered in a field that was not currently selected.</li> <li>▶ Resolved an issue where a DNP server did not accept a new client connection in a timely manner if the previous client connection did not close the socket connection with a FIN or RST tcp flag.</li> <li>▶ Resolved an issue where a DNP client communication status would incorrectly indicate as offline if the client connection was no longer selected in the tree.</li> <li>▶ Resolved an issue when the quality of the DNP connection status was always invalid when viewed in the Data Viewer application.</li> <li>▶ Resolved an issue where no data would be shown on the screen after closing the SSH Public Key editor and leaving the editor blank.</li> </ul>	20240628
1.1.8	<ul style="list-style-type: none"> <li>▶ [Cybersecurity] Closed TCP port 7890.</li> <li>▶ Resolved an issue where the Protocol Services application may not open after low system memory conditions.</li> </ul>	20230912

Package Version Number	Summary of Revisions	Manual Date Code
1.1.6	<ul style="list-style-type: none"> <li>► Resolved an issue in the DNP server that prevented binary inputs from being inverted and analog inputs from being scaled.</li> <li>► Resolved an issue where a DNP service was not restarted after closing unexpectedly.</li> <li>► Resolved an issue where a DNP client service needed to be manually restarted after sending a clear restart request because the restart IIN bit was set in the server.</li> </ul>	20230406
1.1.5	<ul style="list-style-type: none"> <li>► [Cybersecurity Enhancement] Obfuscated SSH password entry on Ethernet-tunneled serial connections.</li> <li>► Resolved an issue where point counts were not updated correctly.</li> </ul>	20230330
1.1.4	<ul style="list-style-type: none"> <li>► Resolved an issue where sorting or filtering the point grid could cause the wrong points to be deleted on a delete operation.</li> </ul>	20220930
1.0.4	<ul style="list-style-type: none"> <li>► Initial version.</li> </ul>	20220506

*Table A.5* lists the Blueframe Data Viewer package versions, a description of the changes, and the manual date code corresponding to the package version. The table lists the most recent package version first.

**Table A.5 Blueframe Data Viewer Package Version History**

Package Version Number	Summary of Revisions	Manual Date Code
1.0.10	<ul style="list-style-type: none"> <li>► Resolved an issue where Data Viewer would not open when Blueframe was accessed through port forwarding or network address translation.</li> </ul>	20250130
1.0.9	<ul style="list-style-type: none"> <li>► Resolved an issue where data points were not viewable.</li> </ul>	20240830
1.0.8	<ul style="list-style-type: none"> <li>► Updated Data Viewer for compatibility with Blueframe OS 1.8.0.</li> </ul>	20231222
1.0.7	<ul style="list-style-type: none"> <li>► Resolved an issue where data was displayed incorrectly.</li> <li>► Resolved an issue where more than 1,000 data points being added or removed simultaneously could cause the data viewer to stop updating.</li> </ul>	20230912
1.0.6	<ul style="list-style-type: none"> <li>► Updated package to better support manufacturing deliverables.</li> </ul>	20230103
1.0.5	<ul style="list-style-type: none"> <li>► Updated help menu to link to <a href="http://selinc.com/deployBlueframe">selinc.com/deployBlueframe</a>.</li> <li>► Updated package to support services restart in Application Management.</li> </ul>	20221216
1.0.4	<ul style="list-style-type: none"> <li>► Resolved an issue where the installation of the Data Viewer application package failed to install.</li> </ul>	20220930
1.0.3	<ul style="list-style-type: none"> <li>► Initial version.</li> </ul>	20220811

*Table A.6* lists the Blueframe Resource Viewer package versions, a description of the changes, and the manual date code corresponding to the package version. The table lists the most recent package version first.

**Table A.6 Blueframe Resource Viewer Package Version History**

Package Version Number	Summary of Revisions	Manual Date Code
1.6.1	<ul style="list-style-type: none"> <li>► Addressed an issue where DMA plans did not load correctly.</li> </ul>	20250130
1.5.0	<ul style="list-style-type: none"> <li>► Added the Disturbance Monitoring and Configuration Monitoring widgets.</li> </ul>	20240607
1.4.0	<ul style="list-style-type: none"> <li>► Added a diagnostics panel for DMA data collection jobs that include RTAC assets.</li> <li>► Resolved an issue where the Resource Viewer service would continuously restart.</li> </ul>	20240510
1.3.0	<ul style="list-style-type: none"> <li>► Added the ability to select a date display format.</li> </ul>	20231222

Package Version Number	Summary of Revisions	Manual Date Code
1.2.0	<ul style="list-style-type: none"> <li>► Added support to save layouts on a per-user basis.</li> <li>► Added support for Web Session in the Manage Connection options.</li> <li>► Added support to display time data in local time.</li> <li>► Added support to reset column modifications to default.</li> <li>► Resolved an issue where filtering based on a specific day did not show all logs for that day.</li> <li>► Resolved an issue that prevented Resource Viewer from installing on Blueframe OS version 1.7.2.</li> <li>► Resolved an issue where filtering on the Date/Time column did not work.</li> <li>► Resolved an issue where if two resources had the same name, one resource did not receive changes in Resource Viewer.</li> <li>► Resolved an issue where a filter for the label "rtac" would show previous resources even after the "rtac" filter was removed from those resources.</li> <li>► Resolved an issue where changes made to a resource in Resource Management were not displayed prior to the resource being re-deployed.</li> </ul>	20230928
1.1.0	<ul style="list-style-type: none"> <li>► Added the ability to set a time-out value for the device polls.</li> <li>► Added logging for troubleshooting any connection issues.</li> <li>► Added ability to manage which components are visible.</li> <li>► Added new component for viewing URLs within a dashboard.</li> <li>► Added ability to import and export dashboard layouts.</li> <li>► Added ability to adjust components layouts and set defaults.</li> </ul>	20230801
1.0.1	<ul style="list-style-type: none"> <li>► Resolved an issue where package would fail on system backup and restore.</li> </ul>	20230620
1.0.0	<ul style="list-style-type: none"> <li>► Initial version.</li> </ul>	20230505

## Instruction Manual

---

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

*Table A.7* lists the instruction manual release dates and a description of modifications. The most recent instruction manual revisions are listed first.

**Table A.7 Instruction Manual Revision History**

Date Code	Summary of Revisions
20250212	<b>Appendix A</b> <ul style="list-style-type: none"> <li>► Updated Connection Services package to version 1.16.1.</li> </ul>
20250130	<b>Appendix A</b> <ul style="list-style-type: none"> <li>► Updated Data Viewer package to version 1.0.10.</li> <li>► Updated Resource Viewer package to version 1.6.1.</li> </ul>
20250106	<b>Section 2</b> <ul style="list-style-type: none"> <li>► Updated <i>Creating a New User</i> in <i>User Management</i>.</li> </ul> <b>Section 3</b> <ul style="list-style-type: none"> <li>► Updated <i>Figure 3.8: Resource Overview</i>, <i>Figure 3.9: Connection Services</i>, <i>Figure 3.12: Resource Sessions</i>, <i>Figure 3.27: Profile Configuration Spaces</i>, <i>Figure 3.31: Profile Session Template</i>, <i>Figure 3.32: Deploy Instances</i>, and <i>Figure 3.34: Instance Credentials</i>.</li> </ul> <b>Section 4</b> <ul style="list-style-type: none"> <li>► Updated <i>Figure 4.1: Connected Resources</i>, <i>Figure 4.2: Available Sessions</i>, <i>Figure 4.3: Execute a Command</i>, and <i>Figure 4.4: Terminal Tools</i>.</li> <li>► Updated <i>Quick Connect</i>.</li> </ul> <b>Appendix A</b> <ul style="list-style-type: none"> <li>► Updated Connection Services package to version 1.16.0.</li> <li>► Updated Blueframe Operating System and Hardware Services package to version 1.11.0.</li> </ul>

<b>Date Code</b>	<b>Summary of Revisions</b>
20241105	<b>Appendix A</b> ► [Cybersecurity] Updated Blueframe Operating System and Hardware Services package to version 1.10.0.
20240905	<b>Appendix A</b> ► Updated Connection Services package to version 1.15.2.
20240830	<b>Appendix A</b> ► Updated Data Viewer package to version 1.0.9.
20240823	<b>Appendix A</b> ► Updated Connection Services package to version 1.15.1.
20240628	<b>Appendix A</b> ► Updated Connection Services package to version 1.15.0. ► Updated Protocol Services package to version 1.2.1.
20240607	<b>Appendix A</b> ► Updated Resource Viewer package to version 1.5.0.
20240510	<b>Appendix A</b> ► Updated Resource Viewer package to version 1.4.0.
20240425	<b>Section 2</b> ► Updated <i>Redundancy</i> to include support for as many as six nodes. ► Added <i>Backup Node Management</i> to <i>Redundancy</i> . <b>Section 3</b> ► Added <i>Define Resource Access</i> to <i>Overview</i> . <b>Section 9</b> ► Changed name of "Security Logs" to "System Logs". <b>Appendix A</b> ► [Cybersecurity] Updated Blueframe Operating System and Hardware Services package to version 1.9.0. ► Updated Connection Services package to version 1.14.2.
20240112	<b>Section 3</b> ► Updated <i>Overview</i> in <i>Resource Details</i> . ► Updated <i>Figure 3.8: Resource Overview</i> . <b>Appendix A</b> ► Updated Connection Services package to version 1.13.1.
20231222	<b>Appendix A</b> ► Updated Data Viewer package to version 1.0.8. ► Updated Resource Viewer package to version 1.3.0.
20231127	<b>Section 2</b> ► Added <i>Operation Modes</i> to <i>System Settings</i> . ► Added <i>Synchronization</i> . <b>Section 3</b> ► Added <i>Instance Credentials</i> to <i>Profiles</i> . <b>Appendix A</b> ► [Cybersecurity] Updated Blueframe Operating System and Hardware Services package to 1.8.0. ► Updated Connection Services package to version 1.13.0.
20231031	<b>Appendix A</b> ► Updated Connection Services package to version 1.12.1.

Date Code	Summary of Revisions
20231020	<p><b>Section 3</b></p> <ul style="list-style-type: none"><li>▶ Updated <i>Table 3.1: Connection Protocol Options</i>.</li><li>▶ Updated <i>Additional Protocol Settings</i> in <i>Connection Settings</i>.</li><li>▶ Updated <i>Resource Sessions</i> in <i>Resource Details</i>.</li><li>▶ Added <i>Figure 3.12: Ingress and Egress Up/Down Scripts</i> and <i>Figure 3.15: New Session With Allowlist or Denylist</i>.</li><li>▶ Updated <i>Figure 3.13: Resource Sessions</i>, and <i>Figure 3.16: Role Association</i>.</li></ul> <p><b>Appendix A</b></p> <ul style="list-style-type: none"><li>▶ Updated Connection Services package to 1.12.0.</li></ul>
20230928	<p><b>Appendix A</b></p> <ul style="list-style-type: none"><li>▶ Updated Blueframe Resource Viewer package to version 1.2.0.</li></ul>
20230922	<p><b>Appendix A</b></p> <ul style="list-style-type: none"><li>▶ Updated Connection Services package to 1.11.3.</li></ul>
20230912	<p><b>Section 2</b></p> <ul style="list-style-type: none"><li>▶ Added support for RADIUS authentication in <i>Central Authentication</i>.</li><li>▶ Added <i>RADIUS Configuration</i>.</li></ul> <p><b>Appendix A</b></p> <ul style="list-style-type: none"><li>▶ Updated Blueframe Operating System and Hardware Services package to version 1.7.2.</li><li>▶ Updated Connection Services package to version 1.11.2.</li><li>▶ Updated Blueframe Protocol Services package to version 1.1.8.</li><li>▶ Updated Blueframe Data Viewer package to version 1.0.7.</li></ul>
20230801	<p><b>Appendix A</b></p> <ul style="list-style-type: none"><li>▶ Updated Blueframe Resource Viewer package to version 1.1.0.</li></ul>
20230620	<p><b>Section 3</b></p> <ul style="list-style-type: none"><li>▶ Updated <i>Table 3.1: Disturbance Monitoring Supported Devices</i>.</li><li>▶ Updated <i>Figure 3.18: Example Profile Name and Description</i>.</li><li>▶ Updated <i>Profiles</i>.</li><li>▶ Added <i>Resource Template</i>.</li></ul> <p><b>Section 4</b></p> <ul style="list-style-type: none"><li>▶ Added <i>Quick Connect</i>.</li></ul> <p><b>Appendix A</b></p> <ul style="list-style-type: none"><li>▶ Updated Blueframe Operating System and Hardware Services package to version 1.6.3.</li><li>▶ Updated Connection Services package to version 1.10.0.</li><li>▶ Updated Blueframe Resource Viewer package to version 1.0.1.</li></ul>
20230505	<p><b>General</b></p> <ul style="list-style-type: none"><li>▶ Added <i>Section 7: Resource Viewer</i>.</li></ul> <p><b>Appendix A</b></p> <ul style="list-style-type: none"><li>▶ Added <i>Table A.6: Blueframe Resource Viewer Package Version History</i>.</li></ul>
20230406	<p><b>Appendix A</b></p> <ul style="list-style-type: none"><li>▶ Updated Blueframe Protocol Services package to version 1.1.6.</li></ul>
20230330	<p><b>Section 1</b></p> <ul style="list-style-type: none"><li>▶ Added <i>Troubleshooting</i>.</li></ul> <p><b>Section 2</b></p> <ul style="list-style-type: none"><li>▶ Added <i>Internal Network Configuration</i> in <i>Network</i>.</li></ul> <p><b>Section 3</b></p> <ul style="list-style-type: none"><li>▶ Updated <i>Overview</i>.</li><li>▶ Updated <i>Table 3.1: Connection Protocol Options</i>.</li><li>▶ Updated <i>Additional Protocol Settings</i> in <i>Adding a New Resource</i>.</li><li>▶ Updated <i>Figure 3.13: New Sessions Dialog</i>.</li><li>▶ Updated <i>Resource Sessions</i> in <i>Resource Details</i>.</li></ul>

Date Code	Summary of Revisions
	<p><b>Section 4</b></p> <ul style="list-style-type: none"> <li>► Updated <i>Direct Resource Access</i>.</li> <li>► Added <i>Figure 4.6: Web Proxy Session</i>.</li> </ul> <p><b>Section 8</b></p> <ul style="list-style-type: none"> <li>► Added <i>Syslog in Security Logs</i>.</li> </ul> <p><b>Appendix A</b></p> <ul style="list-style-type: none"> <li>► Updated Blueframe Operating System and Hardware Services package to version 1.6.0.</li> <li>► Updated Connection Services package to version 1.9.5.</li> <li>► Updated Blueframe Protocol Services package to version 1.1.5.</li> </ul>
20230103	<p><b>Appendix A</b></p> <ul style="list-style-type: none"> <li>► Updated Blueframe Data Viewer package to version 1.0.6.</li> </ul>
20221216	<p><b>Section 2</b></p> <ul style="list-style-type: none"> <li>► Added <i>Notifications</i>.</li> </ul> <p><b>Section 3</b></p> <ul style="list-style-type: none"> <li>► Added <i>Section 3: Resource Management</i>.</li> </ul> <p><b>Appendix A</b></p> <ul style="list-style-type: none"> <li>► Updated Connection Services package to version 1.8.0.</li> <li>► Changed Blueframe Protocol Services package version 1.1.3 to 1.1.4.</li> <li>► Updated Blueframe Data Viewer package to version 1.0.5.</li> </ul>
20221103	<p><b>Appendix A</b></p> <ul style="list-style-type: none"> <li>► Updated Blueframe Operating System and Hardware Services package to version 1.5.2.</li> </ul>
20220930	<p><b>Section 2</b></p> <ul style="list-style-type: none"> <li>► Added <i>Profiles to Resource Management</i>.</li> </ul> <p><b>Appendix A</b></p> <ul style="list-style-type: none"> <li>► Updated <i>Table A.1: Blueframe Operating System and Hardware Services Package Version History</i>, <i>Table A.2: Blueframe Core Services Package Version History</i>, and <i>Table A.3: Connection Services Package Version History</i>.</li> <li>► Added <i>Table A.4: Blueframe Protocol Services Package Version History</i> and <i>Table A.5: Blueframe Data Viewer Package Version History</i>.</li> </ul>
20220826	<p><b>Section 5</b></p> <ul style="list-style-type: none"> <li>► Added new section.</li> </ul>
20220811	<p><b>Section 2</b></p> <ul style="list-style-type: none"> <li>► Updated <i>Table 2.3 Connection Protocol Options</i>.</li> <li>► Added <i>Additional Protocol Settings</i>.</li> <li>► Added <i>Resource Management API</i>.</li> </ul> <p><b>Appendix A</b></p> <ul style="list-style-type: none"> <li>► Updated <i>Table A.3: Connection Services Package Version History</i>.</li> </ul>
20220520	<p><b>General</b></p> <ul style="list-style-type: none"> <li>► Added <i>Section 5: Direct Resource Access</i>.</li> <li>► Added <i>Section 6: Protocol Services</i>.</li> </ul> <p><b>Section 1</b></p> <ul style="list-style-type: none"> <li>► Updated <i>Table 1.1: Blueframe Hardware Compatibility</i>.</li> <li>► Updated <i>Figure 1.3, Figure 1.5, Figure 1.7, Figure 1.12</i>, and <i>Figure 1.13</i>.</li> </ul>

Date Code	Summary of Revisions
	<p><b>Section 2</b></p> <ul style="list-style-type: none"> <li>► Updated <i>Creating a New User</i> in <i>User Management</i>.</li> <li>► Updated <i>Figure 2.8, Figure 2.26, Figure 2.28, Figure 2.36–Figure 2.46, and Figure 2.49</i>.</li> <li>► Updated <i>Table 2.2: Connection Protocol Options</i>.</li> <li>► Added <i>Resource Sessions</i> to <i>Resource Management &gt; Resource Details</i>.</li> </ul> <p><b>Appendix A</b></p> <ul style="list-style-type: none"> <li>► Updated <i>Table A.1: Blueframe Operating System and Hardware Services Package Version History</i>, <i>Table A.2: Blueframe Core Services Package Version History</i>, and <i>Table A.3: Connection Services Package Version History</i>.</li> </ul>
20211008	<p><b>Section 2</b></p> <ul style="list-style-type: none"> <li>► Updated <i>Table 2.2: Connection Protocol Options</i>.</li> <li>► Updated <i>Figure 2.45: Resource Protocol</i> and <i>Figure 2.46: Child Resource Assignment</i>.</li> </ul> <p><b>Appendix A</b></p> <ul style="list-style-type: none"> <li>► Updated Connection Services package to version 1.4.0.</li> </ul>
20210921	<p><b>Appendix A</b></p> <ul style="list-style-type: none"> <li>► Updated Blueframe Operating System and Hardware Services package to version 1.4.0.</li> <li>► Updated Blueframe Core Services package to version 1.3.2.</li> </ul>
20210914	<p><b>Appendix A</b></p> <ul style="list-style-type: none"> <li>► Updated Blueframe Operating System and Hardware Services package to version 1.3.0.</li> </ul> <p><b>Appendix B</b></p> <ul style="list-style-type: none"> <li>► Added text regarding firmware management for supported hardware in <i>Security Environment</i>.</li> </ul>
20210813	<p><b>Section 2</b></p> <ul style="list-style-type: none"> <li>► Updated <i>Figure 2.36: Resource Management Components</i>.</li> <li>► Updated <i>Figure 2.37: Dragging a Resource Into a Folder</i>.</li> <li>► Changed <i>Filter Bar</i> to <i>Search Bar</i>.</li> <li>► Updated <i>Figure 2.39: Resource Management Filters</i>.</li> <li>► Updated <i>Figure 2.40: Adding a New Resource</i>.</li> <li>► Added Child Resources to <i>Connection Settings</i>.</li> <li>► Added <i>Figure 2.46: Child Resource Assignment</i>.</li> </ul> <p><b>Section 3</b></p> <ul style="list-style-type: none"> <li>► Updated Uninstall paragraph preceding <i>Figure 3.8: Uninstalling Warning</i>.</li> </ul> <p><b>Appendix A</b></p> <ul style="list-style-type: none"> <li>► Updated Blueframe Operating System and Hardware Services package to version 1.2.3.</li> <li>► Updated Blueframe Core Services package to version 1.2.1.</li> <li>► Updated Connection Services package to version 1.3.0.</li> </ul>
20210507	<p><b>Section 2</b></p> <ul style="list-style-type: none"> <li>► Updated <i>Figure 2.44: Connection Services</i> and <i>Figure 2.45: Resource Protocol</i>.</li> <li>► Added <i>Table 2.2: Connection Protocol Options</i>.</li> </ul> <p><b>Appendix A</b></p> <ul style="list-style-type: none"> <li>► Updated <i>Table A.1: Blueframe Operating System and Hardware Services Package Version History</i> and <i>Table A.2: Blueframe Core Services Package Version History</i>.</li> <li>► Added <i>Table A.3: Connection Services Package Version History</i>.</li> <li>► Removed <i>Table A.3: Blueframe Central Authentication</i>, <i>Table A.4: Blueframe Certificate Management</i>, <i>Table A.5: Blueframe Resource Management</i>, <i>Table A.6: Blueframe Security Logs</i>, <i>Table A.7: Blueframe System Settings</i>, and <i>Table A.8: Blueframe User Management</i>.</li> </ul> <p><b>Appendix B</b></p> <ul style="list-style-type: none"> <li>► Updated <i>Passwords</i> with password character limit information.</li> <li>► Updated disclosing security vulnerabilities web link in <i>Revision Management</i>.</li> </ul>
20210223	<ul style="list-style-type: none"> <li>► Initial version.</li> </ul>

**This page intentionally left blank**

---

---

## A P P E N D I X    B

---

# Cybersecurity Features

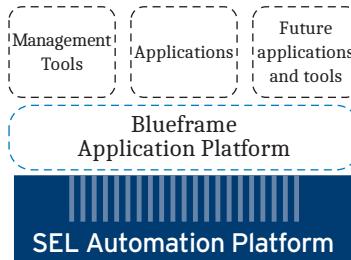
## Security Environment

---

One part of the Blueframe ecosystem is the hardware layer, which can be an SEL-3350 Automation Platform, SEL-3355 Automation Platform, SEL-3360 Automation Platform, or virtual machine deployment. When run on supported hardware, firmware management is performed by Blueframe. On startup, Blueframe will automatically update the BIOS and microcode if they are found to be out-of-date from what the Blueframe version ships with and will load correct firmware into supported expansion boards. As a result, during an upgrade, if these firmware updates must be performed, you may see the device restart several times as each firmware is updated. You can access all system applications and tools through a secure web-based environment named the Blueframe application platform.

The Blueframe system also employs allowlisting and detailed definitions of users and roles for access levels and permissions. In addition to the permissions, Blueframe provides for detailed logging of operations performed by users throughout the system as well as logging of automated operations by the system.

Because Blueframe is accessed through a secure web environment secured by TLS, it also supports X.509 certificates. You can generate certificates to be signed or import certificates into the system after they are signed by a certificate authority (CA).



**Figure B.1 Blueframe Application Platform System Architecture**

Blueframe was designed to be an operational technology solution and as such its recommended deployment is within an operational technology network segment that is isolated from the internet.

## Version Information

---

The Application Management tool in Blueframe gives you options to manage your installed application packages. You can review package versions, release notes, and individual application information. To learn more about Application Management, see *Section 8: Application Management*.

# Installation Characteristics

---

Blueframe uses containerized applications that are distributed in application packages that must be loaded into a Blueframe node and then installed. The process for installing a new package can be found in *Application Packages on page 121*.

## Ports and Services

---

The SEL-3350, SEL-3355, and SEL-3360 support Blueframe. See the respective manuals for more information on their physical ports. The logical port used by Blueframe is Port 80 as a redirect to 443 – HTTPS protocol.

## Access Control

---

### Use of Elevated Privilege

Blueframe employs a system for user privileges and permissions. The system consists of an association between roles and users that can be defined to allow access to applications for operations and application permissions management.

When commissioning Blueframe, a user creates an initial account that is automatically added to a default administrator (admin) role and can be used to create additional users and roles.

For more details on users and roles, see *User Management on page 39*.

## Centrally Managed Accounts

Centrally managed accounts are supported on the Blueframe application platform that uses LDAP authentication. Blueframe provides the means to configure LDAP parameters for connecting with an LDAP server as well as selecting the group maps to be used. If used, centralized LDAP authentication manages the revocation or authorization changes for users of the organization's directory service. The Central Authentication management tool also supports two LDAP servers. For more information, see *Central Authentication on page 62*.

## Local Accounts

Blueframe supports local accounts for users and their roles. Roles are created and configured to have permissions to access and manage permissions on a per-application basis. Users assigned to a role automatically inherit the permissions of the role as it was defined. For more details about users and roles, see *User Management on page 39*.

## Passwords

Passwords within Blueframe are created when a user is defined and can be managed by each user by using the User Profile badge. The software does not ship with default passwords, and a password must be defined for each user that is added to the system. When a member of the admin group creates a user, an option exists to force a user to reset their password on their next login.

Blueframe offers customizable password policies that can be set by an administrator and are implemented for all accounts in the Blueframe instance. If a user attempts to create a password that does not meet the minimum requirements, the operation will fail and the software lists the missing requirements. Blueframe requires that passwords are at least 3 characters and no more than 30 characters.

To view more details on how to create, change, or manage passwords and their policies, see *User Management on page 39*. Also, see *System Logs on page 127* for details on authentication logging.

## X.509 Certificates

Blueframe uses certificates that follow the X.509 standard for establishing trusted connections over HTTPS that uses the TLS protocol. Blueframe uses the included default certificate to obtain an encrypted connection for the initial setup of the system. It is important to note that for a certificate to be trusted, it must go through a CA validation process first and then loaded into the Blueframe machine.

Blueframe offers tools for generating and importing certificates. For more details on those topics, see *Certificate Management on page 49*.

## Logging Features

### Security Events

Blueframe has a dedicated management tool called System Logs, which is used for security logging of operations throughout Blueframe. Certain security events produce entries into the System Logs management tool, which follow NERC CIP-007 requirements. The security events that produce logs are user login, user logout, failed authentication attempt, and failed authentication attempts that reach a threshold, among many others.

For more details on logging features, see *System Logs on page 127*.

## Internal Log Storage

The System Logs management tool provides a set of options for managing the storage of log records into the local disk of a Blueframe node. The options offered are Disk Overflow behavior, Log Lifetime, and an Anti-Chatter filter. You can set multiple thresholds for managing records but once a threshold is reached, the system will discard the oldest set of records and replace them with newer ones. The System Logs management tool also offers options to export log records. See *System Logs on page 127* for more information.

## Alarm Contact

The alarm contact closes once the system has successfully started and passed internal integrity checks. It remains closed unless the system is turned off. There is no other closing behavior.

## Backup and Restore

---

Blueframe supports backups of the system and its settings. To manage backups, you must use the Backup and Restore management tool. See *Backup & Restore on page 32* for more details.

## Decommissioning

---

Blueframe supports the SEL-3350, SEL-3355, and SEL-3360. See the respective manual for more information on how to decommission a device. To fully decommission a Blueframe node, it is recommended to do a Factory Reset through the System Settings management tool. This will ensure all data are fully removed from a Blueframe node.

## Malware Protection Features

---

Blueframe employs malware protection through the exe-GUARD allowlisting technology. It provides protection, implements kernel-level allowlisting, and incorporates secure memory privileges with enforced mandatory access controls.

## Revision Management

---

*Appendix A: Software and Manual Versions* contains a detailed list of release notes for the Blueframe operating system and Management Tools. If you need information about the SEL process for disclosing security vulnerabilities, see <https://selinc.com/support/security-notifications/>.

## Contact SEL

---

For further questions or concerns about product security, contact SEL at [security@selinc.com](mailto:security@selinc.com) or +1.509.332.1890.

# Glossary

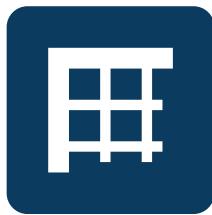
<b>Application Bar</b>	A bar that contains the application launcher, application bar menus, information panes, and the user profile badge.
<b>Application Bar Menus</b>	A set of menu options within the Application Bar that change dynamically based on the application being used.
<b>Application Containerization</b>	An application deployment scheme that employs isolated application containers for security and dependability.
<b>Application Launcher</b>	A list of applications within Blueframe that can be arranged in alphabetical order or by category. Applications can be launched from this menu.
<b>Application Management</b>	Blueframe management tool used to manage application package uploading and installation processes within Blueframe. This tool is also used for reviewing version information.
<b>Application Package</b>	Within Blueframe, an application package is a prepackaged set of application containers that can be loaded into a Blueframe node for installation.
<b>Application Platform</b>	Main user interface of Blueframe where users, resources, and security settings can be configured. It is also where all applications exist within Blueframe.
<b>Automation Platform</b>	Product classification for SEL computing hardware that supports Blueframe.
<b>Blueframe (Enabled) Applications</b>	Any application within Blueframe that is individually distributed or distributed as part of an applications suite.
<b>Blueframe Management Tools</b>	A set of system applications used to configure users, resources, security, and system management.
<b>Blueframe OS</b>	The underlying Linux-based operating system on which the Blueframe UI rests.
<b>Can Launch</b>	Within the User Management tool, "can launch" means a user can launch and make changes to an application configuration.
<b>Can Manage</b>	Within the User Management tool, "can manage" means a user can further define access permissions for applications that support access permissions adjustments.
<b>Central Authentication</b>	Blueframe management tool used to manage LDAP parameters for users of the Blueframe system that make use of central authentication.
<b>Certificate Management</b>	Blueframe management tool used to manage X.509 certificates and CA certificates.
<b>Chromium Browser</b>	The browser used to run the Blueframe application platform on the local display of an Automation Platform.
<b>Error, Warning, and Notification Panes</b>	An information center within Blueframe where you can find errors, warnings, and notifications.
<b>Interfaces</b>	Found within the System Settings Management tool. It provides a list of Ethernet connections available on the Blueframe node for physical connections.

<b>Label</b>	Within the Resource Management tool, a label is a specific string that can be associated with a resource to facilitate its use and discovery throughout Blueframe applications.
<b>Package Services</b>	A set of services that are associated with a specific application package.
<b>Portal</b>	The landing page for the Blueframe application platform. It contains the Application Launcher, applications, favorites, and notifications of the system. All applications and tools can be launched from the portal.
<b>POST Summary</b>	A visual summary within the System Settings management tool that shows you the health of the hardware components of the Automation Platform or virtual machine running the Blueframe node.
<b>Resource</b>	Any source that provides data to Blueframe.
<b>Resource Management</b>	Blueframe management tool used for adding and managing data resources, such as devices, databases, and data concentrators.
<b>Roles</b>	Within the User Management tool, roles are used to define user permissions. A user can be assigned to one or more roles as needed.
<b>Security Logs</b>	Blueframe management tool used for reviewing security-related logging throughout the Blueframe system.
<b>System Settings</b>	Blueframe management tool used for configuring system-specific settings and reviewing system status.
<b>Theme</b>	Within Blueframe, the Visual Theme setting determines a user preference between light or dark user interface themes.
<b>Toast Notification</b>	A momentary notification that appears on the right of the window when certain operations are performed. Once the notification fades from view, it is added to the respective error, warning, or information panes.
<b>User Management</b>	Blueframe management tool used for creating and managing users and roles with relevant system access permissions.
<b>User Profile Badge</b>	A user-specific menu that exists in the Application Bar and is used for managing user preferences and updating a user's password.
<b>Username</b>	A unique text string that defines a user within Blueframe.

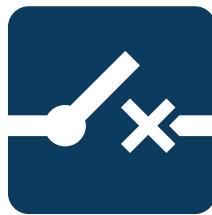
# Distribution Management System

## Suite of Applications Within SEL Blueframe

### Instruction Manual



Power System  
Model



FLISR



Model Data  
Import

20250114

© 2022–2025 Schweitzer Engineering Laboratories, Inc. All rights reserved.

Content subject to change without notice. Unless otherwise agreed in writing, all SEL product sales are subject to SEL's terms and conditions located here: <https://selinc.com/termsandconditions/>.

# Table of Contents

## Section 1: Distribution Management System Overview

Introduction.....	165
What Is Blueframe?.....	166
DMS Application Packages.....	167
Other Packages Commonly Used by DMS Applications.....	168

## Section 2: Model Data Import

Introduction.....	169
GIS Requirements.....	169
GeoJSON File Content Requirements.....	171
CIM File Format Requirements.....	176
CIM File Content Requirements.....	176
Application Usage.....	180
Model Data Importer API.....	191

## Section 3: Power System Model

Overview.....	205
Canvas.....	206
Settings Validation.....	234
PSM Usage Notes.....	234
Model Publishing and Checkout.....	235
Editing a Published System.....	236

## Section 4: FLISR

Overview.....	239
FLISR Fundamentals.....	239
FLISR Operations.....	244

## Section 5: Reports

Introduction.....	261
Response Reports.....	261
Fault Summary.....	262
Voltage Summary.....	265
Retrieve Report Data Programmatically.....	269

## Appendix A: Software and Manual Versions

Software.....	271
Instruction Manual.....	275

## Appendix B: FLISR Data Mapping Tables

Field Data.....	279
SCADA Data.....	289

## Appendix C: Cybersecurity Features

Security Environment.....	299
Version Information.....	299
Installation Characteristics.....	299
Ports.....	299
Access Control.....	299
Backup and Restore.....	300

Revision Management.....	300
Contact SEL.....	301

# List of Figures

Figure 1.1 FLISR Operational Workflow.....	165
Figure 1.2 Scalable DMS FLISR Modular Architecture.....	166
Figure 1.3 Blueframe System Architecture.....	167
Figure 2.1 MDI File Management.....	170
Figure 2.2 Pipeline Manager Interface.....	170
Figure 2.3 Import Inbox Interface.....	180
Figure 2.4 Import Dialog.....	181
Figure 2.5 Assign Pipeline Button.....	181
Figure 2.6 Pipeline Manager Button.....	182
Figure 2.7 Create a Pipeline.....	182
Figure 2.8 Feeder Pipeline Manager.....	183
Figure 2.9 Substation Pipeline Manager.....	183
Figure 2.10 Import Pipeline.....	184
Figure 2.11 Import Inbox.....	184
Figure 2.12 Select All Feeders.....	184
Figure 2.13 Assign Pipeline.....	184
Figure 2.14 Verify Pipeline Assignment.....	185
Figure 2.15 Feeder Pipeline Manager Interface.....	185
Figure 2.16 Substation Pipeline Manager Interface.....	186
Figure 2.17 Asset Panel.....	187
Figure 2.18 GIS Asset Mapping Panel.....	187
Figure 2.19 CIM Asset Mapping Panel.....	188
Figure 2.20 Circuit Breaker Selector Example.....	188
Figure 2.21 Normally Open Load Break Elbow Selector Example.....	189
Figure 2.22 Line Segment Selector Example.....	189
Figure 2.23 Complete Feeder Asset Mapping Example.....	190
Figure 2.24 Asset Right-Click Menu.....	191
Figure 3.1 Power System Model User Interface.....	205
Figure 3.2 Power System Model Drafts.....	208
Figure 3.3 New Manual Feeder.....	208
Figure 3.4 New Node Selection Menu.....	209
Figure 3.5 New Node Expanded Menu.....	209
Figure 3.6 Validation Messages.....	234
Figure 3.7 Draft Panel.....	235
Figure 3.8 Feeder Checkout.....	235
Figure 3.9 PSM Model Editing.....	236
Figure 3.10 Model Management Tools.....	237
Figure 4.1 Fault Event Diagram.....	240
Figure 4.2 Fault Location.....	241
Figure 4.3 Service Restoration.....	242
Figure 4.4 Return to Normal.....	243
Figure 4.5 DMS FLISR User Interface.....	244
Figure 4.6 Feeder Tools.....	245
Figure 4.7 Voltage Operation.....	250
Figure 4.8 FLISR Simulation View.....	252
Figure 4.9 Simulating a Feeder in FLISR.....	253
Figure 4.10 Simulated Feeder User Interface.....	253
Figure 4.11 Simulated Event Entry.....	255
Figure 4.12 Simulated Event Trigger.....	255
Figure 4.13 Simulator Screen.....	256

Figure B.1 Breaker Analog Inputs.....	281
Figure B.2 Breaker Binary Inputs.....	281
Figure B.3 Breaker Binary Outputs.....	282
Figure B.4 Recloser Analog Inputs.....	283
Figure B.5 Recloser Binary Inputs.....	284
Figure B.6 Recloser Binary Outputs.....	284
Figure B.7 Switch Analog Input.....	286
Figure B.8 Switch Binary Inputs.....	287
Figure B.9 Switch Binary Outputs.....	287
Figure B.10 Concentrator Analog Inputs.....	288
Figure B.11 Concentrator Binary Inputs.....	288
Figure B.12 Concentrator Binary Outputs.....	289
Figure B.13 SCADA Breaker Binary Inputs.....	290
Figure B.14 SCADA Breaker Binary Outputs.....	291
Figure B.15 SCADA Recloser Binary Inputs.....	292
Figure B.16 SCADA Recloser Binary Outputs.....	292
Figure B.17 SCADA Switch Binary Inputs.....	294
Figure B.18 SCADA Switch Binary Outputs.....	294
Figure B.19 SCADA Feeder Binary Outputs.....	296
Figure B.20 SCADA Feeder Binary Outputs.....	297

# List of Tables

Table 1.1 Computing Requirements.....	168
Table 2.1 MDI GIS Asset Types (Substation and Distribution).....	172
Table 2.2 Supported Properties.....	173
Table 2.3 Required Properties by Asset.....	174
Table 2.4 MDI CIM Asset Types (Substation and Transmission).....	176
Table 2.5 MDI CIM Node Types (Substation and Transmission).....	178
Table 2.6 Supported Properties.....	178
Table 3.1 Hot Key Reference.....	206
Table 3.2 Transmission Canvas Property Grid Settings.....	210
Table 3.3 Substation Canvas Property Grid Settings.....	210
Table 3.4 Feeder Canvas Property Grid Settings.....	210
Table 3.5 Junction Node Settings.....	211
Table 3.6 Transmission Line Segment Node Settings.....	211
Table 3.7 Transmission Pole Node Settings.....	212
Table 3.8 Transmission Line Node Settings.....	213
Table 3.9 Substation Busbar Node Settings.....	213
Table 3.10 Substation Transformer Node Settings.....	214
Table 3.11 Substation Winding Transformer Node Settings.....	215
Table 3.12 Substation Breaker Node Settings.....	216
Table 3.13 Substation Recloser Node Settings.....	218
Table 3.14 Substation Switch Node Settings.....	219
Table 3.15 Substation Tie Node Settings.....	220
Table 3.16 Substation Fuse Node Settings.....	222
Table 3.17 Substation Capacitor Bank Node Settings.....	222
Table 3.18 Substation Current Transformer Node Settings.....	223
Table 3.19 Substation Potential Transformer Node Settings.....	224
Table 3.20 Substation Series Compensator Node Settings.....	224
Table 3.21 Substation Shunt Compensator Node Settings.....	225
Table 3.22 Substation Line Node Settings.....	226
Table 3.23 Junction Node Settings.....	227
Table 3.24 Placeholder Node Settings.....	227
Table 3.25 Breaker Node Settings.....	228
Table 3.26 Recloser Node Settings.....	230
Table 3.27 Switch Node Settings.....	231
Table 3.28 End-of-Line Node Settings.....	232
Table 3.29 Junction Node Settings.....	233
Table 3.30 Placeholder Node Settings.....	234
Table 4.1 FLISR Feeder Settings.....	246
Table 4.2 FLISR-Specific Settings Established in PSM Settings.....	247
Table 4.3 FLISR-Specific Node Settings.....	248
Table A.1 PSM Package Version History.....	272
Table A.2 FLISR Package Version History.....	273
Table A.3 Manual Revision History.....	275
Table B.1 Breaker Device Data.....	279
Table B.2 Recloser Device Data.....	282
Table B.3 Switch Device Data.....	285
Table B.4 Breaker SCADA Data.....	289
Table B.5 Recloser SCADA Data.....	291
Table B.6 Switch SCADA Data.....	293

Table B.7 Feeder SCADA Data.....	295
Table B.8 Status Supervisor Data.....	295

---

---

## S E C T I O N   1

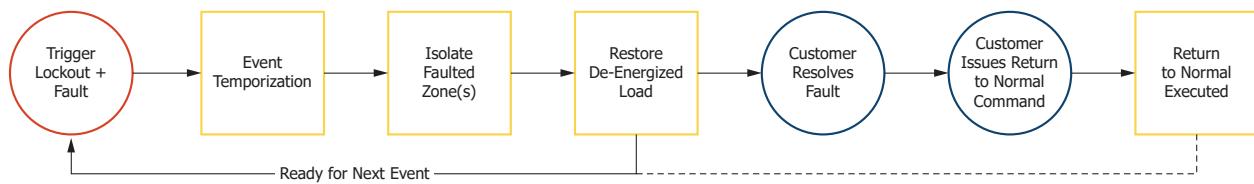
---

# Distribution Management System Overview

## Introduction

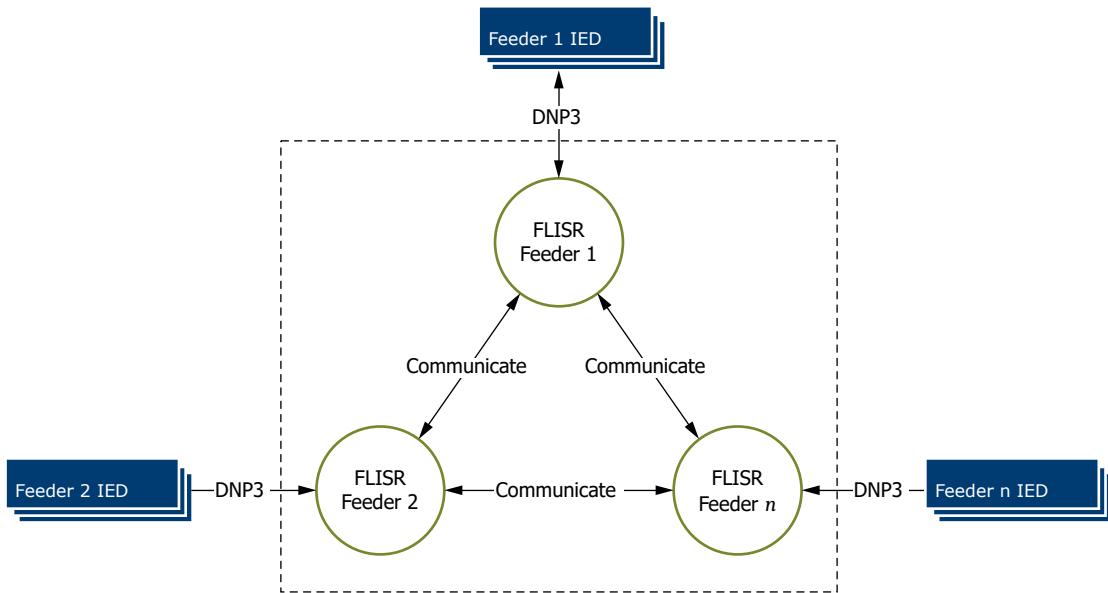
---

The SEL Distribution Management System (DMS) suite is a collection of Blueframe applications that provide wide-area system monitoring, control, and management functionality while emphasizing simplicity, scalability, and security. The DMS suite will expand in capability over time. Its current functionality is Fault Location, Isolation, and Service Restoration (FLISR). DMS FLISR uses field data to identify and automatically isolate faults while restoring load from adjacent sources, which maximizes system margin and minimizes switching. (see *Figure 1.1*).



**Figure 1.1** FLISR Operational Workflow

DMS FLISR overcomes the problems encountered by monolithic control systems where many settings reside in one place in an interconnected or dependent manner. Those systems are complex to scale, and it can be hard to know how much of the system configuration to retest when changes are made. DMS FLISR is modular by design; functionality is configured, tested, and commissioned one feeder at a time, making it possible to maintain consistent simplicity when dealing with the first feeder, the 10th feeder, or the 100th feeder. Each configured feeder communicates with other electrically adjacent feeders to determine fault location and calculate a post-fault restoration solution (see *Figure 1.2*).

**What Is Blueframe?****Figure 1.2 Scalable DMS FLISR Modular Architecture**

**⚠️ IMPORTANT**

Field device and Blueframe time synchronization is necessary because look backs and measurement validity are based on accurate time stamps.

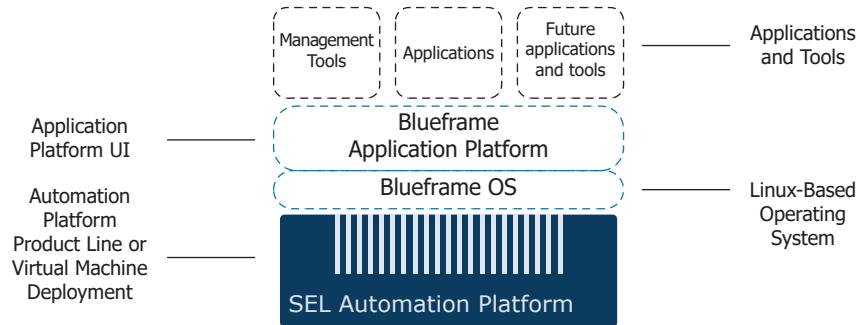
## What Is Blueframe?

---

Blueframe is an embedded, modular, and container-based application platform designed to operate in a secured environment. The modular design of Blueframe enables you to selectively choose the solution applications you want to install to support and solve your system needs. Blueframe Management Tools are included to support common Blueframe system configurations. The solution applications are optional and offered in various ways, from a single application to packages of applications that belong to suites designed to achieve a modular solution to an industrial problem.

The system employs a scheme of smart shared data throughout, so you enter information such as IEDs, connections, and users only once. Each application subscribes seamlessly to the data it needs, saving you configuration time and reducing the chance of introducing manual copy errors into the system.

The Blueframe ecosystem, as shown in *Figure 1.3*, consists of a hardware layer supported by the Automation Platform or a virtual environment with a subscription contract. On top of the hardware layer rests a secured Linux-based operating system that is designed to minimize exposure to attack and which employs security measures, such as allowlisting, to prevent unauthorized access and attacks. Lastly, the Blueframe application platform and its applications rest on top of the Linux operating system and use application containerization. You can access all system applications and tools through a secure web-based environment.



**Figure 1.3 Blueframe System Architecture**

## DMS Application Packages

The DMS suite will expand over time and is currently capable of FLISR functionality and currently supports FLISR functionality and model management through PSM. Each DMS application is considered an independent application within Blueframe and does not require non-Blueframe application integrations, just device data. However, the Blueframe OS can consume non-SEL software information to further support operational needs. Applications like FLISR are supported by multiple core Blueframe applications within the Blueframe OS like protocol services, core services, and connection services. DMS FLISR requires that the DMS model application, PSM, be installed along with FLISR. PSM is broken into two applications PSM (one-line model) and MDI (GIS file consumption). MDI is the pipeline configurator that translates a customer's model to the SEL DMS model. PSM manages the SEL DMS model, whether imported through customer GIS via MDI, manually configured in PSM, or both. FLISR contains all the runtime code necessary for Blueframe to provide FLISR functionality as well as an integrated simulator that makes on-demand, feeder-level testing possible.

## Upgrading and Downgrading FLISR Applications When Feeders Are Commissioned

Upgrading FLISR causes all commissioned feeders to disarm. This is a safety precaution and prevents any potential misoperation while the upgrade is taking place. Once the upgrade is complete, feeders can be re-armed after careful inspection to ensure incoming data are accurate.

Downgrading DMS applications is the same as uninstalling and reinstalling them. Before downgrading PSM or FLISR, decommission any commissioned feeders, perform the downgrade, and re-commission.

## DMS Hardware and Sizing Specifications

You can reference *Table 1.1* to create baseline specifications for hardware components whether you are using SEL hardware or your own customer-supplied virtual machine.

**Table 1.1 Computing Requirements**

Hardware Type	Number of Feeders	Number of CPUs	RAM	Hard Disk Drive
SEL-3350	20	N/A	8 GB	120 GB
SEL-3355	20	N/A	32 GB	200 GB
Virtual Machine	1–74	16	32 GB	200 GB
Virtual Machine	75–150	20–32	32+ GB	250 GB
Virtual Machine	Contact an SEL Representative			

## Other Packages Commonly Used by DMS Applications

The DMS suite uses the following applications to establish communication with IEDs installed in the field, enabling FLISR to receive data and send controls.

- **Resource Management.** This application is used to configure profiles for each unique IED. Profiles make it possible to characterize each IED variation instead of configuring each IED instance. For example, you can create a single profile for an SEL-651R Recloser Control in Resource Management. That profile can contain a DNP map and other settings that do not change from device to device. Once created, you can use that profile to create many instances of the profile quickly and efficiently—one instance for each physical SEL-651R that will be used in DMS FLISR.
- **Protocol Services.** This application is used to configure DNP maps and is responsible for acting as the data broker for all information floating through a protocol connection.

---

---

## S E C T I O N   2

---

# Model Data Import

## Introduction

---

Model Data Import (MDI) is a Blueframe application. It enables users to generate a modular model for the Power System Model (PSM) application based on the GIS information provided in the GeoJSON format and/or the equipment information provided in the CIM format. MDI, like PSM, is feeder-centric by design. It calculates distribution system and substation connectivity using geographic information and divides it into feeders. These feeders can then be organized into substations and regions in PSM. This feeder-centric method makes building models more efficient and simplifies model editing. MDI can use CIM and GeoJSON files that contain only a portion of the model. These files may contain a single feeder, a substation, a region, an area of responsibility, or any other geographic space bounded by an arbitrary area. This flexibility makes integration into existing utility systems simple and fast.

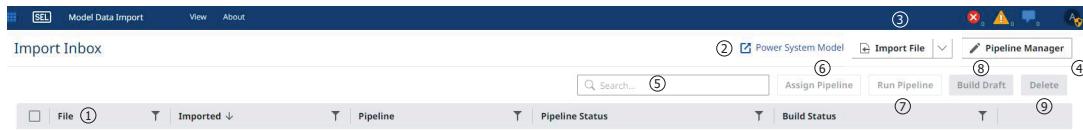
## GIS Requirements

---

Preparing the GIS model for extraction is an important part of MDI consuming your model correctly. The following lists the minimum requirements for extracting the model from GIS.

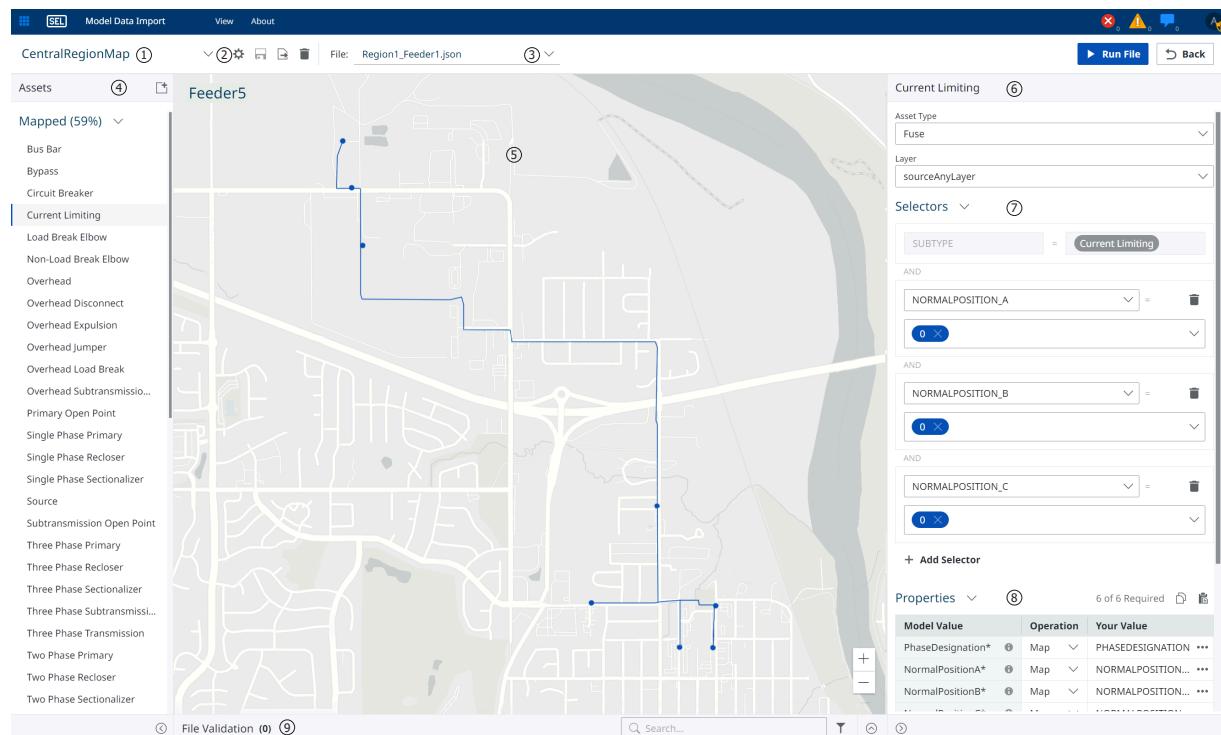
- ▶ Coordinates are formatted as WGS-84.
- ▶ The GIS data are in GeoJSON format (RFC 7946: Section 3.1).
- ▶ Minimum assets
  - Busbar
  - Circuit Breaker
  - Disconnect
  - Elbow
  - Fuse
  - Line
  - Open Point
  - Recloser
  - Sectionalizer
  - Source
  - Switch

## 170 Model Data Import GIS Requirements



**Figure 2.1 MDI File Management**

- ① **Model Data Table.** Where users can import GIS files and load and assign them to a pipeline.
- ② **Power System Model.** A quick hyperlink that takes the user directly to PSM.
- ③ **Import File.** Import GIS GeoJSON files or prebuilt pipelines.
- ④ **Pipeline Manager.** Open the pipeline configuration view.
- ⑤ **Search.** Quickly search through Model Data Table properties.
- ⑥ **Assign Pipeline.** Assign selected files in the Model Data Table to existing pipelines.
- ⑦ **Build Draft.** Populate the feeders to be viewable in PSM once Run Pipeline has been completed.
- ⑧ **Run Pipeline.** Validate that all pipeline properties match and will be imported into PSM once a pipeline is assigned to a GIS file.
- ⑨ **Delete.** Delete any selected GIS import files.



**Figure 2.2 Pipeline Manager Interface**

- ① **Pipeline Selector.** A dropdown section that allows users to switch between pipelines.
- ② **Tools.** The pipeline management tools.
- ③ **GIS Selector.** A dropdown section that allows user to select a GIS feeder.
- ④ **Customer GIS File Assets.** Users can select and define all assets that will be mapped into SEL DMS model.
- ⑤ **Digital Canvas.** The visual mapping aid.

- ⑥ **SEL Model Asset.** Defines what SEL DMS asset will be assigned to what customer model asset.
- ⑦ **Selectors.** Allows for further refinement on asset properties during model migration.
- ⑧ **Properties.** Presented as a table, per asset, that further defines whether an asset gets data from a mapped source or from a user-defined value. The table can be copy and pasted between assets.
- ⑨ **File Validation.** The viewing window for validation errors and warnings.

## GeoJSON File Content Requirements

---

GeoJSON file content varies widely between organizations. MDI has a powerful, yet straightforward, user interface that enables it to be taught how to use files according to the way users organize their GIS data. However, Blueframe uses PSM to drive the operation of distribution automation applications, resulting in some minimum content requirements.

### NOTE

PSM supports feeder and substation models.

## Layers

Geospatial models usually contain layers that allow for easy access to specific elements to allow a user to select what information is visible or hidden at any given time. MDI is able to inspect all layers present in the GeoJSON output file.

## Features

MDI inspects each feature found in the GeoJSON file. Some features get placed into the model as assets, and some features are used only for determining connectivity. How each feature is used in the model is determined by the configuration of the pipeline used to inspect the file. See *Pipeline Configuration on page 181* for more information.

## Supported Asset Types

MDI converts GIS features into model assets. Asset types supported by MDI are listed in the following table. Assets mapped to PSM are used by FLISR and have associated data point and functionality requirements. See *Appendix B: FLISR Data Mapping Tables* for more information about FLISR data point requirements.

**Table 2.1 MDI GIS Asset Types (Substation and Distribution)**

<b>Asset Name</b>	<b>Usage</b>
Source	Used to identify the root of a distribution feeder. This is often the substation circuit breaker.
Circuit Breaker	Used to model a distribution substation feeder breaker. This is a controllable asset that is placed in the model.
<b>NOTE</b>	
	If using both a substation and distribution model with duplicate assets, the user will need to remove the asset from one of their models. If this is not proactively removed, MDI will alarm on the duplication.
	If a user is choosing to update automatically and has not chosen a way to export the model in such a way as to avoid duplication, MDI will alarm on each delta model update.
Recloser	Used to model a three-phase distribution recloser. This is a controllable asset that is placed in the model.
Line	This asset can be used to determine model connectivity and, depending on the SEL DMS application, functionality within an application.
Busbar	This asset can be used to determine model connectivity and, depending on the SEL DMS application, functionality within an application. Used to model and/or expand the busbar in a substation.
Fuse	This asset can be used to determine model connectivity and, depending on the SEL DMS application, functionality within an application.
Elbow	This asset can be used to determine model connectivity and, depending on the SEL DMS application, functionality within an application.
Open Point	This asset can be used to determine model connectivity and, depending on the SEL DMS application, functionality within an application.
Switch	This asset can be used to determine model connectivity and, depending on the SEL DMS application, functionality within an application.
Disconnect	Used to model manually and motor-operated three-phase distribution devices. This asset can be used to determine model connectivity and, depending on the SEL DMS application, functionality within an application.
Sectionalizer	Used to model a three-phase distribution sectionalizer. This asset can be used to determine model connectivity and, depending on the SEL DMS application, functionality within an application.
Capacitor Bank	Used to model a capacitor bank in a substation.
Two-Winding Transformer	Used to model a two-winding transformer in a substation.
Three-Winding Transformer	Used to model a three-winding transformer in a substation.

## Supported Feature Geometry Data

MDI supports feature geometry of both "Point" and "LineString" types. Geometries of the Point type must have a set of coordinates, and geometries of the LineString type must have two or more coordinates.

## Feature Properties

MDI requires that certain properties be present for each feature it uses. This section describes all properties MDI uses for GeoJSON data. Property requirements by asset type are defined in *Table 2.3*.

**Table 2.2 Supported Properties**

Property	Description
PhaseDesignation <sup>a</sup>	Defines which electrical phase the asset is associated with. PSM uses an internal enumeration for different phase designations, so a mapping dialog is provided to transform the GeoJSON content into the correct values on import.
NominalVoltage <sup>a</sup>	Defines the nominal voltage (line to neutral) on the feeder.
NormalPositionA <sup>a</sup>	The 52A type normal position for the A-phase. A 0 is considered Open and a 1 is considered Closed.
NormalPositionB <sup>a</sup>	The 52A type normal position for the B-phase. A 0 is considered Open and a 1 is considered Closed.
NormalPositionC <sup>a</sup>	The 52A type normal position for the C-phase. A 0 is considered Open and a 1 is considered Closed.
AssetType <sup>a</sup>	Defines what type of asset the feature categorizes as in PSM. See <i>Supported Asset Types on page 171</i> for a list of supported types.
UniqueIdentifier <sup>a</sup>	A unique identifier PSM uses to identify each asset instance. This property is usually assigned to the feature's GUID.
AssetName	The human-readable name PSM uses as the asset name.
MeasurementName	A unique identifier that should be mapped for all modeled devices that are enabled with remote communication.
CanLoadBreak	Defines whether the device can be opened under load.
CanLoadMake	Defines whether the device can be closed into a load.
Enabled	Defines whether the device is usable and enabled for use in the model.
Underground	Defines whether the device is constructed for underground (True) or overhead (False) use.

<sup>a</sup> This property is required.

## Required Properties by Asset

This section defines which properties are required for each supported asset type.

**Table 2.3 Required Properties by Asset**

<b>Asset Type</b>	<b>Required Properties</b>
Source	<ul style="list-style-type: none"> <li>► NominalVoltage</li> <li>► MeasurementName</li> <li>► CanLoadBreak</li> <li>► CanLoadMake</li> <li>► Enabled</li> <li>► Underground</li> </ul>
Circuit Breaker	<ul style="list-style-type: none"> <li>► PhaseDesignation</li> <li>► NormalPositionA</li> <li>► NormalPositionB</li> <li>► NormalPositionC</li> <li>► AssetType</li> <li>► UniqueIdentifier</li> <li>► AssetName</li> <li>► MeasurementName</li> <li>► CanLoadBreak</li> <li>► CanLoadMake</li> <li>► Enabled</li> <li>► Underground</li> </ul>
Recloser	<ul style="list-style-type: none"> <li>► PhaseDesignation</li> <li>► NormalPositionA</li> <li>► NormalPositionB</li> <li>► NormalPositionC</li> <li>► AssetType</li> <li>► UniqueIdentifier</li> <li>► AssetName</li> <li>► MeasurementName</li> <li>► CanLoadBreak</li> <li>► CanLoadMake</li> <li>► Enabled</li> <li>► Underground</li> </ul>
Line	<ul style="list-style-type: none"> <li>► PhaseDesignation</li> <li>► AssetType</li> <li>► UniqueIdentifier</li> <li>► AssetName</li> <li>► Enabled</li> <li>► Underground</li> </ul>
Busbar	<ul style="list-style-type: none"> <li>► PhaseDesignation</li> <li>► AssetType</li> <li>► UniqueIdentifier</li> <li>► MeasurementName</li> <li>► CanLoadBreak</li> <li>► CanLoadMake</li> <li>► Enabled</li> <li>► Underground</li> <li>► Name</li> <li>► InService</li> <li>► Nominal Voltage</li> <li>► Phasing</li> <li>► Current Rating</li> </ul>
Fuse	<ul style="list-style-type: none"> <li>► PhaseDesignation</li> <li>► AssetType</li> <li>► UniqueIdentifier</li> <li>► MeasurementName</li> <li>► CanLoadBreak</li> <li>► CanLoadMake</li> <li>► Enabled</li> <li>► Underground</li> </ul>

<b>Asset Type</b>	<b>Required Properties</b>
Elbow	<ul style="list-style-type: none"> <li>▶ PhaseDesignation</li> <li>▶ NormalPositionA</li> <li>▶ NormalPositionB</li> <li>▶ NormalPositionC</li> <li>▶ AssetType</li> <li>▶ UniqueIdentifier</li> <li>▶ AssetName</li> <li>▶ MeasurementName</li> <li>▶ CanLoadBreak</li> <li>▶ CanLoadMake</li> <li>▶ Enabled</li> <li>▶ Underground</li> </ul>
Open Point	<ul style="list-style-type: none"> <li>▶ PhaseDesignation</li> <li>▶ NormalPositionA</li> <li>▶ NormalPositionB</li> <li>▶ NormalPositionC</li> <li>▶ AssetType</li> <li>▶ UniqueIdentifier</li> <li>▶ AssetName</li> <li>▶ MeasurementName</li> <li>▶ CanLoadBreak</li> <li>▶ CanLoadMake</li> <li>▶ Enabled</li> <li>▶ Underground</li> </ul>
Switch	<ul style="list-style-type: none"> <li>▶ PhaseDesignation</li> <li>▶ NormalPositionA</li> <li>▶ NormalPositionB</li> <li>▶ NormalPositionC</li> <li>▶ AssetType</li> <li>▶ UniqueIdentifier</li> <li>▶ AssetName</li> <li>▶ MeasurementName</li> <li>▶ CanLoadBreak</li> <li>▶ CanLoadMake</li> <li>▶ Enabled</li> <li>▶ Underground</li> </ul>
Disconnect	<ul style="list-style-type: none"> <li>▶ MeasurementName</li> <li>▶ CanLoadBreak</li> <li>▶ CanLoadMake</li> <li>▶ Enabled</li> <li>▶ Underground</li> </ul>
Sectionalizer	<ul style="list-style-type: none"> <li>▶ MeasurementName</li> <li>▶ CanLoadBreak</li> <li>▶ CanLoadMake</li> <li>▶ Enabled</li> <li>▶ Underground</li> </ul>
Capacitor Bank	<ul style="list-style-type: none"> <li>▶ Name</li> <li>▶ InService</li> <li>▶ Enabled</li> <li>▶ Underground</li> <li>▶ Nominal Voltage</li> <li>▶ Phasing</li> <li>▶ Current Rating</li> </ul>

Asset Type	Required Properties
Two-Winding Transformer	<ul style="list-style-type: none"> <li>► Name</li> <li>► InService</li> <li>► Enabled</li> <li>► Underground</li> <li>► Phasing <ul style="list-style-type: none"> <li>➢ Primary <ul style="list-style-type: none"> <li>➢ Nominal Voltage</li> <li>➢ Current Rating</li> </ul> </li> <li>➢ Secondary <ul style="list-style-type: none"> <li>➢ Nominal Voltage</li> <li>➢ Current Rating</li> </ul> </li> </ul> </li> </ul>
Three-Winding Transformer	<ul style="list-style-type: none"> <li>► Name</li> <li>► InService</li> <li>► Enabled</li> <li>► Underground</li> <li>► Phasing <ul style="list-style-type: none"> <li>➢ Primary <ul style="list-style-type: none"> <li>➢ Nominal Voltage</li> <li>➢ Current Rating</li> </ul> </li> <li>➢ Secondary</li> <li>➢ Tertiary <ul style="list-style-type: none"> <li>➢ Nominal Voltage</li> <li>➢ Current Rating</li> </ul> </li> </ul> </li> </ul>

## CIM File Format Requirements

---

Most CIM data can be imported without modification. The following are the minimum requirements for extracting the model from CIM:

- CIM data are IEC 61970-301 compliant
- Minimum assets
  - A substation or transmission line
  - A node within the substation or transmission line

## CIM File Content Requirements

---

CIM file data describe equipment as nodes with associated attributes and connections. MDI uses node connections to traverse the CIM tree and construct a representative model in PSM.

## Supported Asset Types

MDI converts CIM elements into model assets. Asset types supported by MDI are listed in *Table 2.4*. Assets mapped to PSM are used by FLISR and have associated data map point and functionality requirements.

**Table 2.4 MDI CIM Asset Types (Substation and Transmission)**

Asset Type	Usage
Region	A collection of substations and transmission lines representing a geographical region.
Substation	A collection of equipment representing a substation.

Asset Type	Usage
Transmission	A collection of equipment representing a transmission line.
Busbar	Used to model and/or expand the busbar in a substation. This asset can be used to determine model connectivity and functionality, depending on the SEL DMS application.
Capacitor Bank	Used to model a capacitor bank in a substation.
Circuit Breaker	Used to model a distribution substation feeder breaker. This is a controllable asset that is placed in the model.
Current Transformer	Used to model a current transformer in a substation.
Disconnect	This asset can be used to determine model connectivity and functionality, depending on the SEL DMS application.
Elbow	This asset can be used to determine model connectivity and functionality, depending on the SEL DMS application.
Egress Point	This asset can be used to determine model connectivity and functionality, depending on the SEL DMS application.
Fuse	This asset can be used to determine model connectivity and functionality, depending on the SEL DMS application.
Ingress Point	This asset can be used to determine model connectivity and functionality, depending on the SEL DMS application.
Line	This asset can be used to determine model connectivity and functionality, depending on the SEL DMS application.
Open Point	This asset can be used to determine model connectivity and functionality, depending on the SEL DMS application.
Potential Transformer	Used to model a potential transformer in a substation.
Recloser	Used to model a three-phase distribution recloser. This is a controllable asset that is placed in the model.
Sectionalizer	This asset can be used to determine model connectivity and functionality, depending on the SEL DMS application.
Series Compensator	Used to model a series compensator in a substation.
Shunt Compensator	Used to model a shunt compensator in a substation.
Source	Used to identify the root of a distribution feeder. This is often the substation circuit breaker.
Switch	This asset can be used to determine model connectivity and functionality, depending on the SEL DMS application.
Three-Winding Transformer	Used to model a three-winding transformer in a substation.
Tie	This asset can be used to determine model connectivity and functionality, depending on the SEL DMS application.
Transformer	Used to model a two-winding transformer in a substation.

## Supported Node Types

MDI categorizes each node from the CIM file as one or more internal types. These are used to describe the relationships between nodes to determine properties.

**Table 2.5 MDI CIM Node Types (Substation and Transmission)**

<b>Node Type</b>	<b>Usage</b>
Container	A logical grouping of equipment into a larger section (Substation, Transmission Line, etc.).
Equipment	A primary equipment asset (e.g., Breaker).
Equipment_Connectivity	A node that connects two or more Equipment nodes.
Container_Connectivity	A node that connects nodes to Container nodes.
Equipment_Property_Supplier	Provides properties to connected Equipment nodes.
Equipment_Property_Bridge	Allows properties to flow across the node onto other Equipment nodes.
Container_Property_Supplier	Provides properties to connected Container nodes.
Container_Property_Bridge	Allows properties to flow across the node onto other Container nodes.
Parent_Object	A node that expects Child_Object nodes to be present.
Child_Object	A node that expects to have a Parent_Object node.

## Supported Properties

MDI supports mapping properties from CIM file data to PSM. There are no required properties that must be mapped in. This section describes all properties MDI uses for CIM data.

**Table 2.6 Supported Properties**

<b>Property</b>	<b>Description</b>
Asset Name	The human-readable name that PSM uses as the asset name.
Asset Type	Defines what type of asset the feature is categorized as in PSM. See <i>Supported Asset Types</i> on page 176 for a list of supported types.
B	Positive-sequence shunt susceptance.
Can Load Break	Defines whether the device can be opened under load.
Can Load Make	Defines whether the device can be closed into a load.
G	Positive-sequence shunt conductance.
High Step	High step of the primary winding.
Increment	Increment of the primary winding.
Is Enabled	Defines whether the device is usable and enabled for use in the model.
Is Gang Operated	Defines whether all phases are operated in unison.
Is Manual	Defines whether an asset is manually operated.
Is Underground	Defines whether the device is constructed for underground (True) or overhead (False) use.
Max Sections	The maximum number of sections for the shunt compensator.
Measurement Name	A unique identifier that should be mapped for all modeled devices that are enabled with remote communication.

<b>Property</b>	<b>Description</b>
Neutral Step	Neutral step of the primary winding.
Neutral Voltage	Neutral voltage of the primary winding.
Nominal Voltage	Defines the nominal voltage (line to neutral) on the asset.
Normal Position A	The 52A type normal position for the A-phase. A 0 is considered Open and a 1 is considered Closed.
Normal Position B	The 52A type normal position for the B-phase. A 0 is considered Open and a 1 is considered Closed.
Normal Position C	The 52A type normal position for the C-phase. A 0 is considered Open and a 1 is considered Closed.
Normal Sections	The nominal number of sections for the shunt compensator.
Normal Step	The step value of the Tap Changer.
Per Section B	Positive-sequence shunt susceptance per section.
Per Section G	Positive-sequence shunt conductance per section.
Phase Designation	Defines which electrical phase with which the asset is associated. PSM uses an internal enumeration for different phase designations, so a mapping dialog is provided to transform the CIM content into the correct values on import.
R	Positive-sequence resistance.
Secondary B	Positive-sequence shunt susceptance for the secondary winding.
Secondary G	Positive-sequence shunt conductance for the secondary winding.
Secondary High Step	High step of the secondary winding.
Secondary Increment	Increment of the secondary winding.
Secondary Low Step	Low step of the secondary winding.
Secondary Neutral Step	Neutral step of the secondary winding.
Secondary Neutral Voltage	Neutral voltage of the secondary winding.
Secondary Nominal Voltage	Nominal voltage of the secondary winding.
Secondary Normal Step	The step value of the secondary winding of the Tap Changer.
Secondary R	Positive-sequence resistance for the secondary winding.
Secondary Type	The type of Tap Changer for the secondary winding, either Ratio or PhaseShift.
Secondary Voltage Rating	Voltage rating of the secondary winding.
Secondary X	Positive-sequence reactance for the secondary winding.
Tertiary B	Positive-sequence shunt susceptance for the tertiary winding.
Tertiary G	Positive-sequence shunt conductance for the tertiary winding.
Tertiary High Step	High step of the tertiary winding.
Tertiary Increment	Increment of the tertiary winding.
Tertiary Low Step	Low step of the tertiary winding.
Tertiary Neutral Step	Neutral step of the tertiary winding.

Property	Description
Tertiary Neutral Voltage	Neutral voltage of the tertiary winding.
Tertiary Nominal Voltage	Nominal voltage of the tertiary winding.
Tertiary Normal Step	The step value of the tertiary winding of the Tap Changer.
Tertiary R	Positive-sequence resistance for the tertiary winding.
Tertiary Type	The type of Tap Changer for the tertiary winding, either Ratio or PhaseShift.
Tertiary Voltage Rating	Voltage rating of the tertiary winding.
Tertiary X	Positive-sequence reactance for the tertiary winding.
Type	The type of Tap Changer, either Ratio or PhaseShift.
X	Positive-sequence reactance.

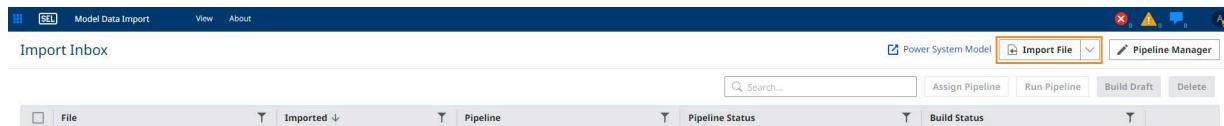
## Application Usage

Generating a model consists of three steps: file import, pipeline execution, and model build. This process can be completed by web-based user interface and REST API. This section describes the user interface first. See *Model Data Importer API* on page 191 for REST API documentation.

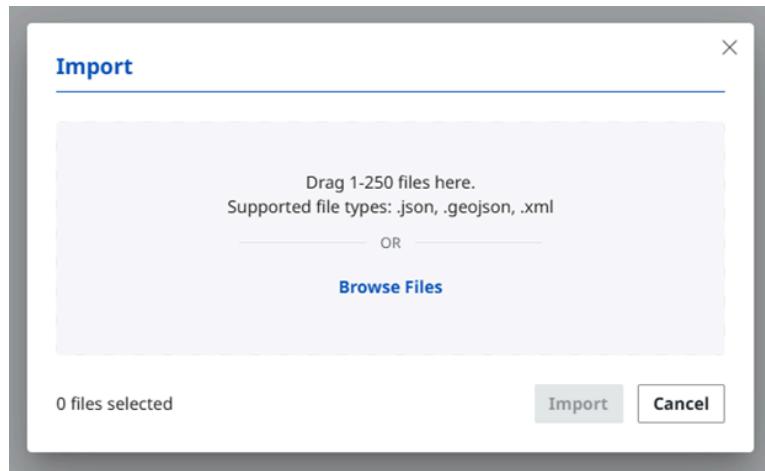
### File Import

Import CIM and GeoJSON files using the Import dialog (see *Figure 2.4*), accessed by selecting the Import button on the MDI Import Inbox page (see *Figure 2.3*). Once the Import dialog is open, one or more files can either be selected or dropped onto the dialog. These files are uploaded and inspected for all feature types, property keys, and property values. These are used to populate pipeline configuration controls, described in *Pipeline Configuration* on page 181. Once file uploads are completed, they appear in a list in the Import Inbox page. Each file in the Import Inbox must be assigned a pipeline in order to be used by MDI. Pipeline assignment is accomplished by selecting the dropdown menu next to each file in the Pipeline column. If no appropriate pipelines exist, a new pipeline may be created.

Use the Import Inbox page (*Figure 2.3*) to upload CIM or GeoJSON files for use by MDI. Also use this page to queue files for pipeline execution and building draft models. Draft models are reviewed and published in the PSM application.



**Figure 2.3 Import Inbox Interface**



**Figure 2.4 Import Dialog**

Select one or more files by selecting their corresponding check boxes, or select all available files by selecting the check box in the header row. Selected files can be assigned to an existing pipeline by selecting **Assign Pipeline**, as shown in *Figure 2.5*. If there are no existing pipelines, see *Pipeline Configuration on page 181*.

A screenshot of the 'Import Inbox' interface. The top navigation bar includes 'SEL Model Data Import', 'View', 'About', 'Power System Model', 'Import File', 'Pipeline Manager', 'Run Pipeline', 'Build Draft', and 'Delete'. The main area shows a table with three rows, each with a checked checkbox in the first column. The columns are 'File', 'Imported', 'Pipeline', 'Pipeline Status', and 'Build Status'. The 'Assign Pipeline' button in the toolbar is highlighted with a yellow box. The table data is as follows:

(6) selected	File	Imported	Pipeline	Pipeline Status	Build Status
<input checked="" type="checkbox"/>	FEEDER_3.json	10/30/2023, 11:43:51 AM	Unassigned	▼ --	✓ Built: 10/30/2023, 12:05:34 PM
<input checked="" type="checkbox"/>	FEEDER_4.json	10/30/2023, 11:43:51 AM	Unassigned	▼ --	✓ Built: 10/30/2023, 12:05:34 PM
<input checked="" type="checkbox"/>	FEEDER_5.json	10/30/2023, 11:43:51 AM	Unassigned	▼ --	✓ Built: 10/30/2023, 12:05:35 PM

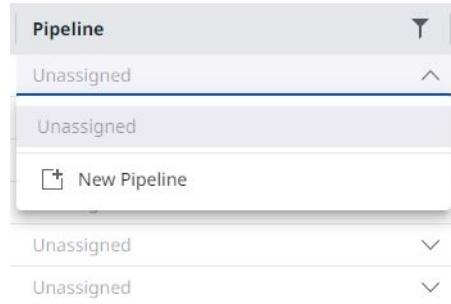
**Figure 2.5 Assign Pipeline Button**

## Pipeline Configuration

The purpose of a pipeline is to enable MDI to inspect a CIM or GeoJSON file, find assets that are passed on to PSM, and determine the electrical topology of the network of power system assets. Pipelines therefore contain rules for how to detect asset types supported by PSM (described in *Table 2.1*) and how to determine connectivity.

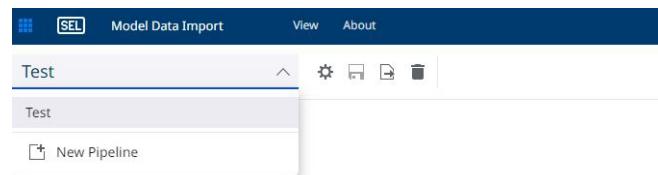
Perform the following steps to create a new pipeline and assign that pipeline (or an existing one) to a single feeder or multiple feeders.

Step 1. Select the dropdown arrow under the Pipeline column, as shown in *Figure 2.6*.



**Figure 2.6 Pipeline Manager Button**

- Step 2. Select the **New Pipeline** option under the dropdown menu, as shown in *Figure 2.7*.



**Figure 2.7 Create a Pipeline**

- Step 3. The New Pipeline window contains the settings necessary for MDI to map the CIM or GIS asset model to the SEL DMS model (in PSM). For GIS, each feature must belong to one or two feeders, as shown in *Figure 2.8*. Features belonging to two feeders are generally open points with connectivity to two different feeders on each side. Provide the correct key value for the **Feeder1 ID** and **Feeder2 ID** fields.

#### NOTE

The **Asset Designation** field is optional. If you choose to select an asset designation, MDI will prepopulate those assets in its left-side panel to increase asset mapping efficiency.

New Pipeline X

Name\*

Type

Assigned files will be organized by feeder. Provide the name of the GeoJSON properties where feeder IDs are stored.

Feeder1 ID\*

Feeder2 ID\*

Asset Designation

\*required

**Figure 2.8 Feeder Pipeline Manager**

New Pipeline X

Name\*

Type

Assigned files will be organized by substation. Provide the name of the GeoJSON properties where substation IDs are stored.

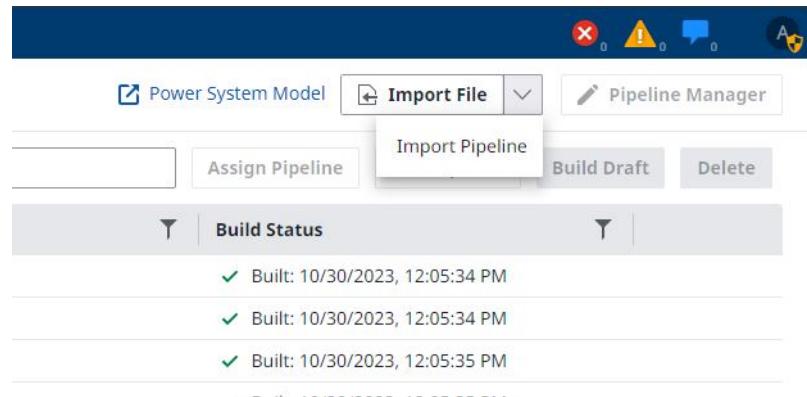
Substation ID

Asset Designation

\*required

**Figure 2.9 Substation Pipeline Manager**

If an existing pipeline has already been created, it can be uploaded by selecting the dropdown arrow next to the Import File option at the top right (*Figure 2.10*). The newly imported pipeline will now be available.



**Figure 2.10 Import Pipeline**

Once a pipeline is created, select **Import Inbox** to select files to import, as shown in *Figure 2.11*.



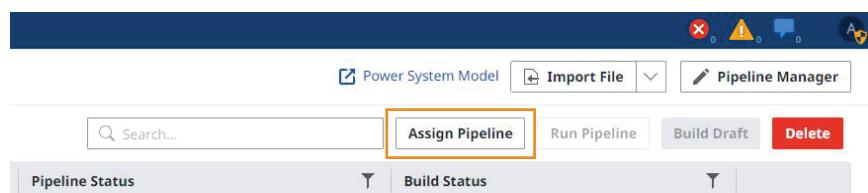
**Figure 2.11 Import Inbox**

Select the individual file(s) you want to assign to a pipeline by selecting the check box next to each individual file. If you want to assign all the files to the same pipeline, select the check box in the header row, as shown in *Figure 2.12*.



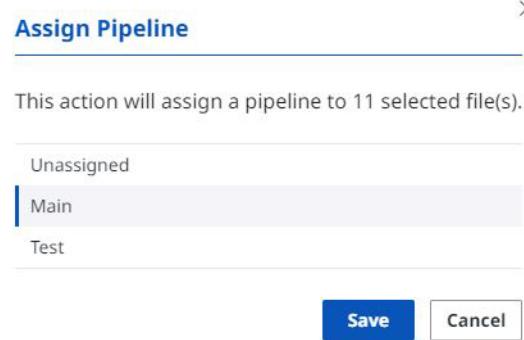
**Figure 2.12 Select All Feeders**

Once you have selected the desired files, select **Assign Pipeline**, as shown in *Figure 2.13*.



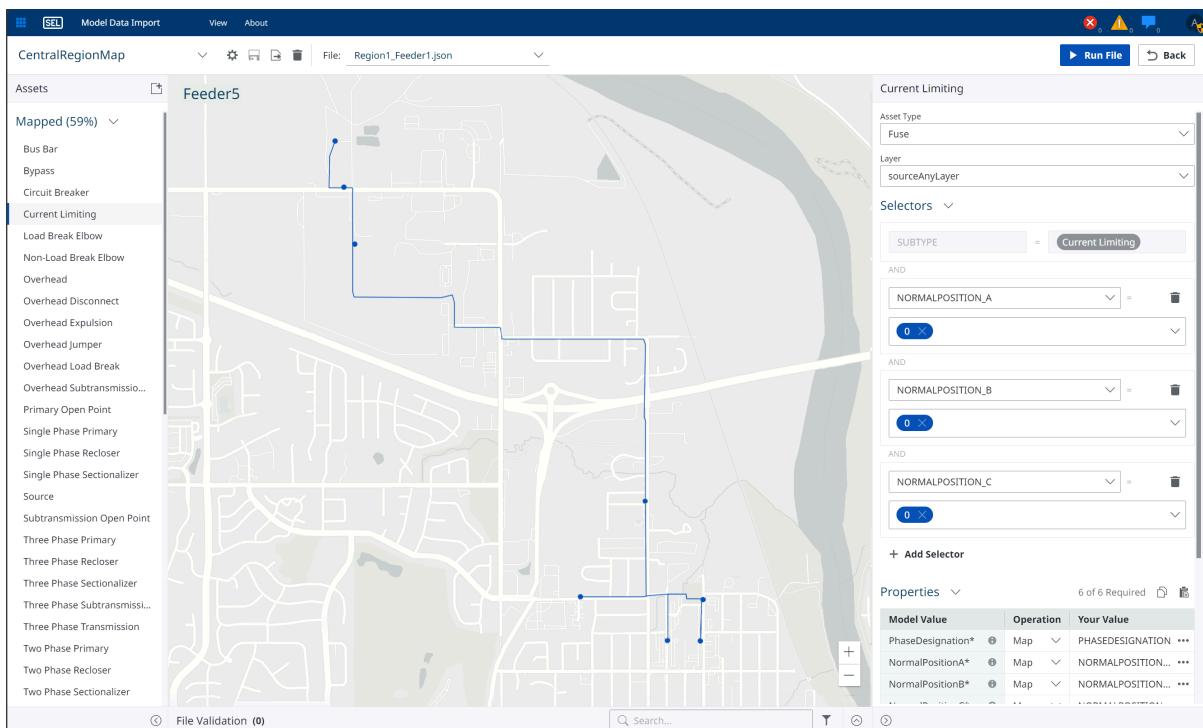
**Figure 2.13 Assign Pipeline**

In the resulting window, verify that the correct pipeline is selected and select **Save**, as shown in *Figure 2.14*.

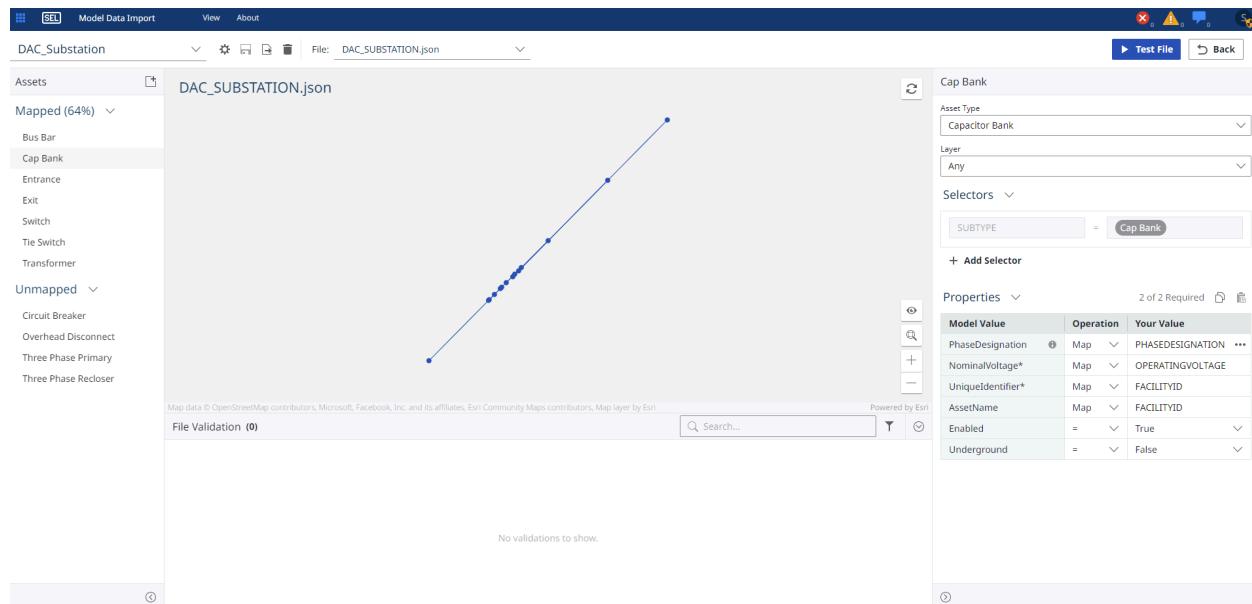


**Figure 2.14 Verify Pipeline Assignment**

Configure pipelines using the Manage Pipelines window (see *Figure 2.15*). The content of files can vary widely. Because of this, pipelines are configured directly by using uploaded files. The data contained within the file itself are used to populate configuration menus within the pipeline configuration process, making it simpler and more efficient to teach MDI how to understand each file. A pipeline cannot be configured or edited without at least one file that is uploaded to MDI and assigned to the pipeline.



**Figure 2.15 Feeder Pipeline Manager Interface**



**Figure 2.16 Substation Pipeline Manager Interface**

## Asset Mapping

Most pipeline configurations are completed on the Asset Mapping page. While multiple feeders or substations can be associated with a single feeder or substation pipeline, respectively, the Asset Mapping page makes it possible to test the pipeline configuration against a single feeder. This reduces configuration and validation time.

The Asset Mapping page provides a GIS map that simplifies viewing the effects of pipeline configuration changes. Select which file to view on a map by using the file selection control located at the top of the map. Use the map to preview the result of pipeline execution on the selected file by selecting **Refresh** at the top right edge of the map.

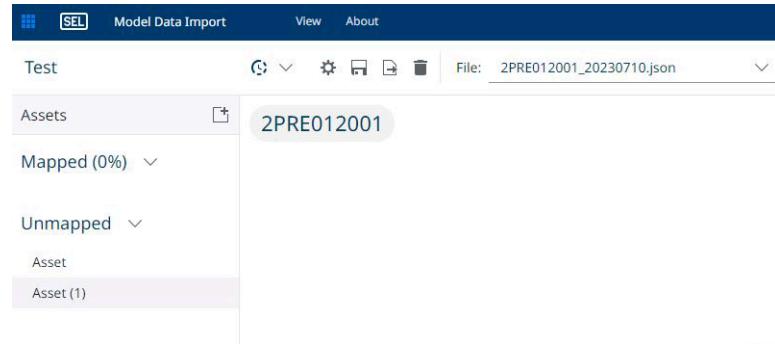
### NOTE

After making any changes to the Property Mapping, SEL recommends saving your progress, then selecting **Test File**, and refreshing the map to visualize the changes. Saving changes intermittently updates the pipeline so that another user can use it to run files. More information on the changes can be found in the File Validation window.

### NOTE

The process shown is specifically for feeders, as noted in Figure 2.16. The Substation MDI is different than the Feeder MDI, even though the process is identical.

To configure an asset, that asset must be present in the Asset panel on the left side of the MDI, as shown in *Figure 2.17*. To add an asset, select the add (**+**) button.

**Figure 2.17 Asset Panel**

Asset mapping configuration consists of two parts (as shown in *Figure 2.18*): Selectors and Properties.

Model Value	Operation	Your Value
PhaseDesignation*	Map	...
NormalPositionA*	Map	...
NormalPositionB*	Map	...
NormalPositionC*	Map	...
UniqueIdentifier*	Map	...
AssetType*	Map	...
AssetName	Map	...
MeasurementName	Map	...
CanLoadBreak	=	True
CanLoadMake	=	False

**Figure 2.18 GIS Asset Mapping Panel**

There are additional options available under the Operation column, as shown in *Figure 2.18*.

**Map:** An operator that maps the customer GIS object to the SEL model object.

**Equals (=):** An operator that allows a customer to manually define the SEL model value.

**Auto:** An operator that allows MDI to automatically map customer GIS objects to an SEL model object. Only available for UniqueIdentifier, AssetName, and NominalVoltage in Substation models.

Model Value	Operation	Your Value	
AssetName	Map		
NominalVoltage	Derive		
SCADA			
MeasurementName	Map		

**Figure 2.19 CIM Asset Mapping Panel**

CIM asset properties are mapped in by using the + button on the top right of the table and selecting the corresponding property in the left column of the table.

There are additional options under the Operation column, as shown in *Figure 2.19*.

**Map:** An operator that maps the customer CIM objects to the SEL model object.

**Equals (=):** An operator that allows a customer to manually define the SEL model value.

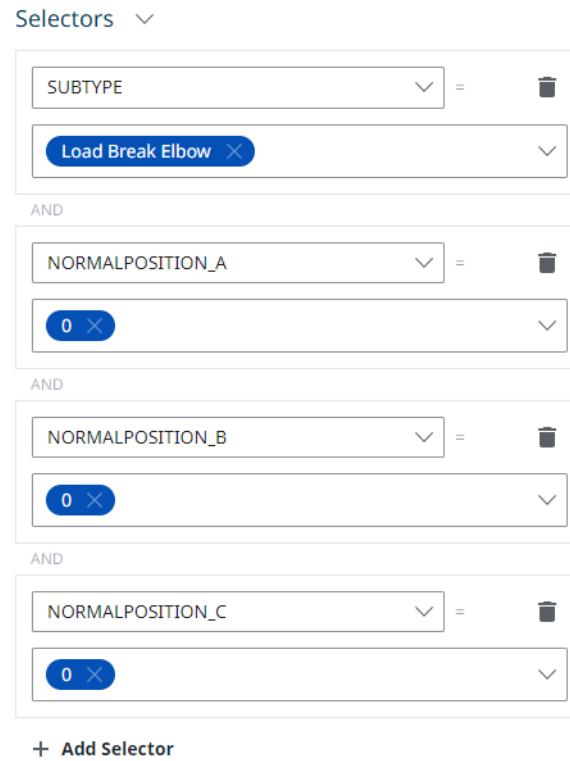
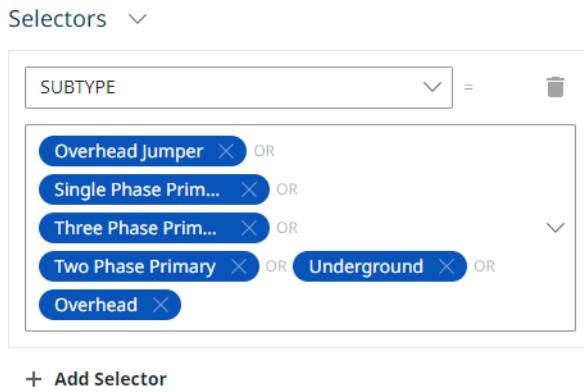
**Derive:** An operator that allows MDI to read the property value from connected nodes in the CIM model.

Selectors provide MDI with the information needed to categorize a CIM element or GIS feature as a specific type of asset. *Figure 2.20* provides an example of a selector configuration to identify a Circuit Breaker. *Figure 2.21* provides an example of a selector configuration to identify a normally open Load Break Elbow. Many different selectors can be defined. Selectors are grouped together using a logical AND. Conditions within each selector are grouped together using a logical OR. *Figure 2.22* provides an example of Line Segment detection by including many different line types within a single selector.

The screenshot shows a dropdown menu with the following options:

- SUBTYPE =
- Circuit Breaker

**Figure 2.20 Circuit Breaker Selector Example**

**Figure 2.21** Normally Open Load Break Elbow Selector Example**Figure 2.22** Line Segment Selector Example

Properties define how an asset within MDI pairs up with the GIS import file. This mapping from MDI to GIS Import is crucial for importing GIS data into PSM.

**NOTE**

In the Properties panel, settings can be copied and pasted between asset type.

Asset mapping is complete when all assets are connected and can be built into PSM. *Figure 2.23* provides an example of complete asset mapping. Note that most of the switch type assets are only used to determine breaks in connectivity. Asset usage is defined in *Supported Asset Types on page 171*.

**NOTE**

When mapping elbows, disconnects, switches, or fuses, it may be useful to add an additional selector for "NormalPosition\_A" and set it to "0", so that it only maps the open points. This helps build the model.

**NOTE**

MDI will only display mapped assets as it walks through the connectivity process. Remember to map Single Phase Primary, Two Phase Primary, and Three Phase Primary as "Lines" to visualize those elements.

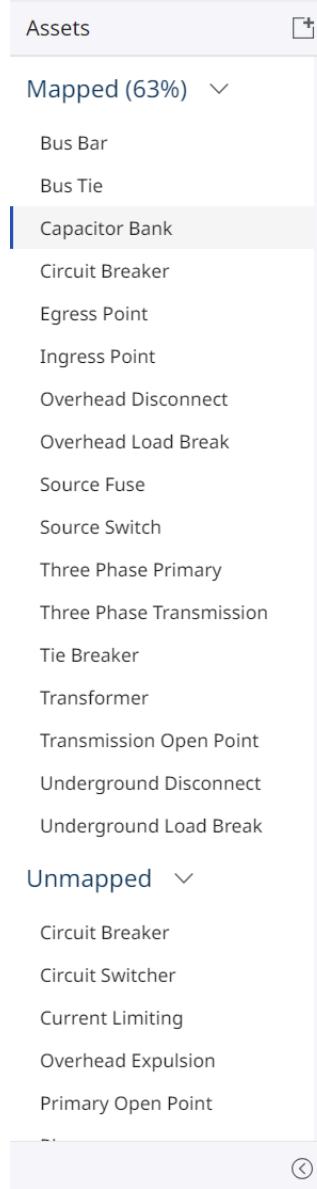
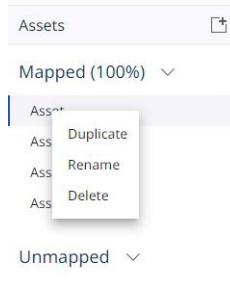


Figure 2.23 Complete Feeder Asset Mapping Example

**NOTE**

The Source asset does not pull assets out of the GeoJSON file. Only one Source can be applied to a feeder, and the asset mapped to the Source must have its Source Selectors correctly assigned. A Source without a correctly configured feeder asset will alarm on "bad source error".

Right-clicking any mapped or unmapped asset in the panel on the left allows the asset to be duplicated, renamed, or deleted, as shown in *Figure 2.24*. In addition, double-clicking an asset lets you rename the asset.



**Figure 2.24 Asset Right-Click Menu**

Each asset has a required properties table. *These properties must be present on each feature within the GIS file assigned to the pipeline according to that feature's asset type.* See *Feature Properties* on page 173 for more information.

## Model Data Importer API

### Overview

This section provides a general overview of the MDI endpoints and their accepted verbs. See *Endpoints* on page 191.

It also provides a general path for uploading files and running them, given an existing pipeline. See *Walkthrough* on page 202.

## Endpoints

.../files

The endpoint responsible for serving and receiving files (see *File* on page 196.)

POST

Body: multipart/form-data with the file in a part

Response: FileUploadResponse

Note: The file in the multipart/form-data request must have a name.

DELETE

Body: An InBodyQuery with the following InBodyQueryValues:

- ids: string, csv of file IDs that should be deleted, default empty string
- format: string, desired response format, default proto, options proto, json

Response: 200 OK

`.../files/run-pipeline`

The endpoint responsible for running a File through a pipeline.

POST

**Body:** An InBodyQuery with the following InBodyQueryValues:

- `ids`: string, csv of file IDs that should be run, default empty string
- `pipelineID`: uint32, ID of pipeline to run file with, default 0
- `user`: uint32, user responsible for running, default empty string
- `format`: string, desired response format, default proto, options `proto`, `json`

**Response:** EnqueueWorkResponse

It is important to note that this endpoint *only* adds the file to the internal work queue.

For updates on the status of the file, either subscribe to the `.../sse/subscribe` endpoint and listen for `FileInfo` updates or query the `.../fileinfos` endpoint every couple seconds to check the status.

`.../files/suggestions`

The endpoint responsible for serving SelectorSuggestions generated on file upload.

GET

- `id`: uint32, ID of file to get suggestions from, default 0
- `format`: string, desired response format, default proto, options `proto`, `json`

**Response:** SelectorSuggestions

`.../files/test-file`

The endpoint responsible for testing files against non-persistent pipelines to see if the container mappings allow for a clean split of the file based on the FEEDER1 ID and FEEDER2 ID properties.

POST

**Body:** TestFileRequest

**Response:** 200 OK or 400 Bad Request

Because of the memory-intensive nature of this type of work, the user must subscribe to the SSE endpoint to get the result of the process. Reaching the endpoint simply adds the test run to the internal work queue of the server. The SSE channel will send a Test File Response over the SSE channel when done.

`.../files/test-feeder`

The endpoint responsible for testing a single feeder against a pipeline to see if any exceptions occur. The GeoJSON returned in the TestFeederResponse is the JSON representation of the container produced by the GIS Import algorithm.

POST

**Body:** TestFeederRequest

**Response:** TestFeederResponse

`../files/test-exceptions`

The endpoint responsible for testing an entire file against a non-persistent pipeline to see if any exceptions occur. This is used on the front end to validate the pipelines before changes have been saved.

POST

**Body:** TestFileRequest

**Response:** 200 OK or 400 Bad Request

It is up to the user to subscribe to the SSE endpoint to get the result of the process. The SSE channel will send a `PipelineResult` over the SSE channel when processing is finished.

`../fileinfos`

The endpoint responsible for serving and updating `FileInfo`s.

PUT

**Body:** FileInfoUpdateRequest

**Response:** FileInfoUpdateResponse

GET

**Query Parameters:**

- `ids`: string, csv of file IDs that should be returned, default empty string.  
If empty, this endpoint uses other query parameters to find `FileInfo`s to return.
- `pipelineID`: uint32, ID of pipeline to run file with, default 0
- `limit`: uint32, maximum `FileInfo` objects in return, default 50, max 1000
- `timestamp`: uint32, only returns objects created after this Unix time, default 0 for no filter
- `format`: string, desired response format, default proto, options `proto`, `json`

**Response:** GetFileInfoResponse

`../pipelines`

The endpoint responsible for updating and deleting pipelines.

DELETE

**Body:** An `InBodyQuery` with the following `InBodyQueryValues`:

- `ids`: string, csv of IDs of pipelines to remove, required

**Response:** 200 OK or 400 Bad Request

POST

**Body:** UpCreatePipelineRequest

**Response:** UpCreatePipelineResponse

`.../pipelines/request`

The endpoint responsible for requesting pipeline objects.

POST

**Body:** An InBodyQuery with the following InBodyQueryValues:

- `ids: string`, csv of pipelines to be returned, default empty string

**Response:** GetPipelineResponse

`.../pipelines/results`

The endpoint responsible for getting PipelineResults generated by the Run Pipeline endpoint.

POST

**Body:** An InBodyQuery with the following InBodyQueryValues:

- `ids: string`, csv of IDs of results to be returned, default empty string
- `format: string`, desired response format, default proto, options proto, json

**Response:** PipelineResult

`.../pipelineinfos`

The endpoint responsible for serving PipelineInfos.

GET

**Query Parameters:**

- `limit: uint32`, max PipelineInfo objects in return, default 50, max 1000
- `timestamp: uint32`, only returns objects created after this unix time, default 0 for no filter
- `format: string`, desired response format, default proto, options proto, json

**Response:** GetPipelineInfosResponse

`.../publish`

The endpoint responsible for taking a PipelineResult and publishing it to the PSM Store as a draft.

If the feeder being uploaded contains links to feeders currently in the PSM Store draft or published stores, they will be checked out and merged if changes need to be made.

POST

Body: An InBodyQuery with the following InBodyQueryValues:

- ids: string, csv of IDs of specific PipelineResults to publish, default empty string
- user: uint32, user responsible for creating draft, default empty string

Response: DraftActionResponse

.../publish/results

The endpoint responsible for serving DraftActionResult generated by the Publish endpoint.

POST

Body: An InBodyQuery with the following InBodyQueryValues:

- ids: string, csv of IDs of specific DraftActionResult, default empty string
- format: string, desired response format, default proto, options proto, json

Response: GetDraftActionResultResponse

.../geojson

The endpoint responsible for serving GeoJSON of specific feeders that have been run through the Run endpoint.

GET

- id: string, ID of file to search through, default 0
- feederID: string, ID of feeder to search for, default empty string
- format: string, desired response format, default proto, options proto, json

Response: GetGeoJSONResponse

.../sse/subscribe

The endpoint responsible for subscribing listeners to SSE channels.

Specifically for the scripted upload use case, the FileInfo update channel sends an SSE message whenever a FileInfo is updated by the work queue.

GET

Query Parameters:

- channel: string, channel to subscribe to, use FileInfo, required

Response: The request will be kept open, user is responsible for refreshes as needed. Data corresponding to the subscribed channel will periodically be sent over the connection. The FileInfo channel should be the only one needed for scripted file pushing.

The data will be in SSE format where the data field has a json blob corresponding to a `FileInfo`.

## Data Definitions

`FileUploadResponse`

```
{  
    "IDs": []uint32,  
    "error": string  
}
```

`InBodyQuery`

```
{  
    "parameters": map[string]stringInBodyQueryValues  
}
```

`File`

```
{  
    "Name": string,  
    "Data": []byte  
}
```

`FileInfo`

```
{  
    "fileID": uint32,  
    "fileName": string,  
    "user": string,  
    "created": uint32,  
    "pipelineID": uint32,  
    "pipelineName": string,  
    "pipelineResultID": uint32,  
    "pipelineStatus": PipelineStatus,  
    "draftResultID": uint32,  
    "draftStatus": DraftStatus  
}
```

`GetFileInfoResponse`

```
{  
    "filter": string,  
    "offset": uint32,  
    "limit": uint32,
```

```
        "IDs": uint32,
        "columnName": string,
        "asc": bool,
        "timestamp": uint32,
        "pipelineID": uint32,
        "fileInfos": []FileInfo
    }
```

---

PipelineResult

```
{
    "ID": uint32,
    "pipelineID": string,
    "fileID": string,
    "created": int64,
    "duration": int64,
    "user": string,
    "status": PipelineStatus,
    "exceptions": []Exception,
    "error": {"value":string}
}
```

---

GetPipelineInfosResponse

```
{
    "offset": uint32,
    "limit": uint32,
    "timestamp": uint32,
    "pipelineInfos": []PipelineInfo,
}
```

---

PipelineInfo

```
{
    "ID": uint32,
    "name": string,
}
```

---

Exception

```
{
    "level": `ExceptionLevel,
    "containerID": string,
    "objectType": SuperType,
    "objectID": string,
    "propertyName": string,
    "reason": string,
    "description": string
}
```

```
}
```

```
GetDraftActionResultResponse
```

```
{
    "draftActionResults": []DraftActionResult
}
```

```
DraftActionResponse
```

```
{
    "result": DraftActionResult,
}
```

```
DraftActionResult
```

```
{
    "ID": uint64,
    "fileID": string,
    "created": int64,
    "status": DraftStatus,
    "user": string,
    "exceptions": []Exception,
    "error": {"value":string}
}
```

```
GetGeoJSONResponse
```

```
{
    "pipelineName": string,
    "data": []byte,
    "containerID": string,
}
```

```
UpCreatePipelineRequest
```

```
{
    "pipeline": Pipeline,
}
```

```
UpCreatePipelineResponse
```

```
{
    "ID": uint32,
    "exceptions": []Exception,
```

```
        "error": {"value":string},
    }
```

#### GetPipelinesResponse

```
{
    "pipelines": []Pipeline,
}
```

#### Pipeline

```
{
    "ID": uint32,
    "name": string,
    "kind": PipelineKind,
    "created": uint32,
    "creator": string,
    "updated": uint32,
    "editor": string,
    "automatic": bool,
    "options": map[string]string,
    "ProhibitList": []string,
    "containerMap": ContainerInputMapping,
    "assetMaps": []Mapping,
    "feederProps": []PropertyMap,
    "cimAssetMaps": []CIMMapping
}
```

#### CIMMapping

```
{
    "class": string,
    "name": string,
    "source": string,
    "nodeType": []string,
    "propertyMaps": []PropertyMap,
    "requiredProperties": []CIMPropertyRef,
    "allowedChildren": []string,
    "containerHierarchyLevel": int32,
}
```

#### CIMPropertyRef

```
{
    "targetProperty": string,
    "referenceName": string,
    "default": string,
}
```

SelectorSuggestions

```
{  
    "Layers": []string,  
    "Suggestions": map[string]SuggestedValues,  
}
```

SuggestedValues

```
{  
    "Values": []string,  
}
```

TestFileRequest

```
{  
    "Pipeline": Pipeline,  
    "FileID": uint32,  
}
```

TestFileResponse

```
{  
    "FileID": uint32,  
    "FeedersFromSplit": map[string]bool,  
    "Exceptions": []Exception,  
    "Error": {"value":string},  
    "FeederID": string,  
    "FeederIDTwo": string,  
    "PipelineID": uint32,  
}
```

TestFeederResponse

```
{  
    "Geojson": string,  
    "Exceptions": []Exception,  
    "Error": {"value":string},  
}
```

TestFeederRequest

```
{  
    "FileID": uint32,  
    "FeederID": string,  
}
```

```
        "Pipeline": Pipeline,  
    }
```

EnqueueWorkResponse

```
{  
    "Results": map[uint32]string,  
}
```

FileInfoUpdateRequest

```
{  
    "FileInfos": []FileInfo,  
}
```

FileInfoUpdateResponse

```
{  
    "Errors": []{"Value":string},  
}
```

## Enum Constants

PipelineKind

```
GeoJSON to Feeder      = 0  
GeoJSON to Substation  = 1  
CIM to Many            = 2
```

PipelineStatus

```
No Status  = 0  
Queued     = 1  
Processing = 2  
Done       = 3  
Failed     = 4
```

DraftStatus

```
No Status  = 0  
Checked Out = 1  
Published   = 2  
Failed      = 3
```

SuperType

```
AUXILIARY = 0
EDGE      = 1
CONTAINER = 2
PORT      = 3
NODE      = 4
```

ExceptionLevel

```
UNSPECIFIED = 0
DEBUG       = 1
INFO        = 2
WARNING     = 3
ERROR       = 4
FATAL       = 5
```

## Walkthrough

### Prerequisites

- A configured pipeline: P
- A file to test on: F

## Steps

### NOTE

These steps assume that the user knows which format they want and are setting it properly in the Query Parameters or sending the correct type of data in the Request Body.

- Step 1. POST a file containing the data for F to the .../files endpoint.
- Step 2. GET the .../pipelineinfos endpoint and find the PipelineInfo that corresponds to P.
- Step 3. GET the .../fileinfos endpoint with the id you got from the FileUploadResponse in Step 1.
- Step 4. Update the FileInfo.PipelineID and FileInfo.PipelineName with the PipelineInfo data from Step 2.
- Step 5. PUT the .../fileinfos endpoint with the updated FileInfo from Step 4.
- Step 6. POST the .../files/run-pipeline endpoint with FileInfo.ID, a user string, and the FileInfo.PipelineID.
- Step 7. By either subscribing to the .../sse/subscribe endpoint or periodically polling the .../fileinfos endpoint, wait until the run has finished. Both options will give a FileInfo object with run result data.
- Step 8. Retrieve (using POST) the PipelineResult from the .../pipelines/results endpoint using the FileInfo.PipelineResultID obtained in Step 7.

- Step 9. Confirm that no Error Level Exceptions were generated during processing. Otherwise, fix errors and restart.
- Step 10. POST the .../publish endpoint with the PipelineResult.ID from *Step 8*.
- Step 11. Retrieve (using POST) the result from the .../publish/results endpoint using the DraftActionResponse.DraftActionResult.ID from *Step 10*.
- Step 12. Confirm that no Error Level Exceptions were generated during the draft process.

**This page intentionally left blank**

## SECTION 3

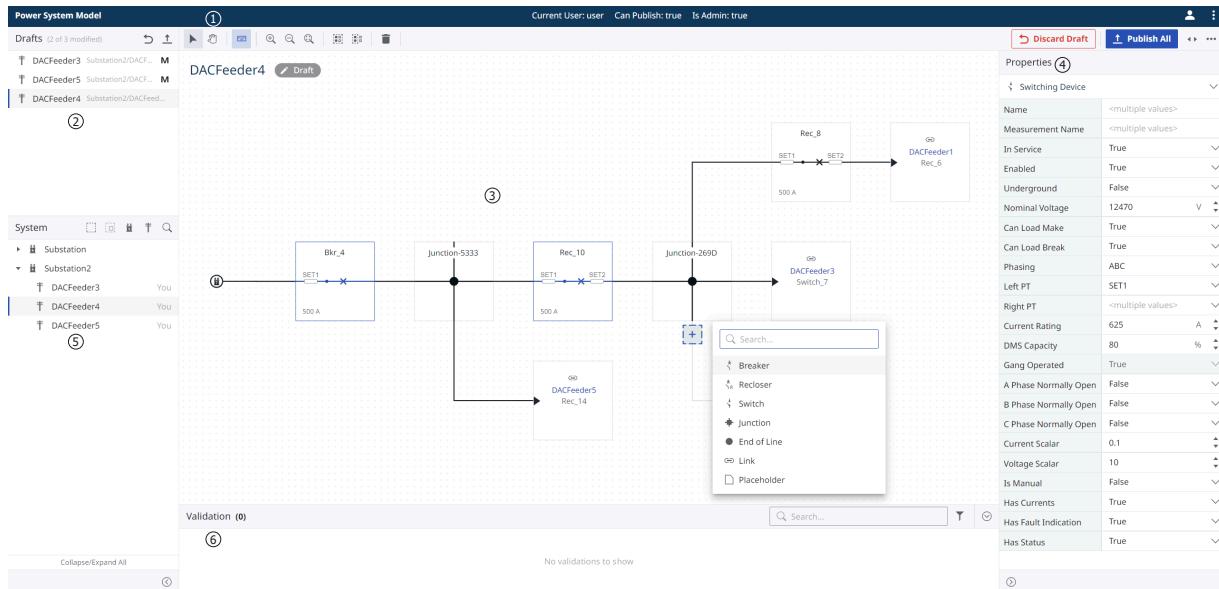
# Power System Model

## Overview

Power System Model (PSM), shown in *Figure 3.1*, provides a graphical configuration environment for DMS applications like FLISR. It is designed to simplify and accelerate the creation of distribution control system settings, as well as provide an intuitive engineering HMI once published.

### NOTE

A user can either hold down **<Ctrl>** and select individual nodes or left-click on the canvas and drag the selection square around nodes to select multiple nodes.



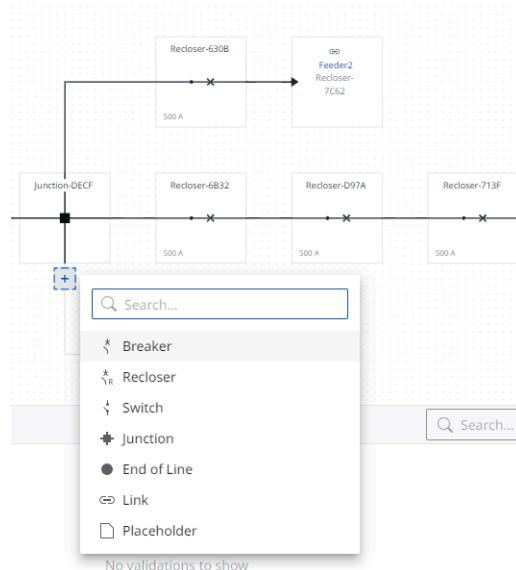
**Figure 3.1** Power System Model User Interface

- ① **Canvas Tools.** Pan, click, and zoom to see areas of interest on the digital canvas in more detail.
- ② **Draft Panel.** Review, publish, and discard new, modified, and removed feeders.
- ③ **Digital Canvas.** Draw your settings quickly using PSM's digital canvas. Once published, the schematic you draw becomes available to your DMS application view, providing at-a-glance insight into your system's status and operations.
- ④ **Property Grid.** Quickly set device-specific settings for your system.
- ⑤ **System Hierarchy Panel.** Quickly create a system hierarchy to separate feeders for quick reference and upstream assignment.
- ⑥ **System Validation.** Active validation and error notifications help you efficiently and successfully configure your system.

The electric power system consists of many distinct elements. While any portion of a power system is complex, you can drastically reduce its complexity when you consider one region at a time. Because it is designed for distribution systems, PSM breaks everything into feeders. A feeder may contain breakers, reclosers, and switches, and the feeder can be electrically connected to one or more adjacent feeders. All these items are graphically configured on the feeder canvas.

## Canvas

PSM is built around the concept of a canvas that uses an auto-directed layout. Each new connection point allows you to select what type of node to add. The canvas also has a Link mode that lets you connect nodes across a canvas. The schematic defines the layout, connectivity, and settings, all of which are used by PSM applications for operations and display purposes.



You can connect feeders together by using either lines or Link mode. When in Link mode, select the target endpoint (regardless of whether it is on the current canvas or a different one). Once a Link node is established between feeders, a clickable node allows for quick navigation between the linked feeders. Each node, whether it be for a breaker, recloser, switch, or feeder connection, has settings associated with it. PSM displays some of these settings on the canvas itself for at-a-glance verification and the Property Grid shows all settings. Select the small box with a "+" in the middle while in the canvas to see assets that can be added.

## Keyboard Hot Keys

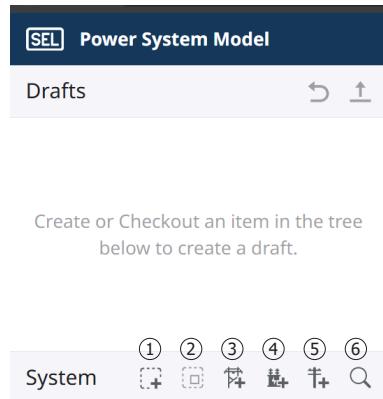
**Table 3.1 Hot Key Reference**

Action	Category	Definition	Hot Key
Exit Link Mode	Canvas	When in Link Mode, exits the mode.	<Esc>
Fit Diagram	Canvas	Center and fit the current diagram to the canvas viewport.	<0>

Action	Category	Definition	Hot Key
Keyboard Mode	Canvas	Enables or disables keyboard mode.	<Ctrl+B>
Pan Mode	Canvas	A mode where no nodes are selectable and the cursor is set to pan the canvas by default.	<P>
Pan Mode (Temporary)	Canvas	When held, temporarily enables Pan Mode	<Space>
Select Mode	Canvas	A mode where the cursor can select nodes and edges by clicking or by dragging a selection box.	<V>
Zoom In	Canvas	Zoom into the center of the canvas by one increment.	<=>
Zoom Out	Canvas	Zoom out of the center of the canvas by one increment.	<->
Add to West Port	Edit	Opens the Add Node Menu for the west (1) port of the selected node.	<Shift+1> (1 in Keyboard Mode)
Add to North Port	Edit	Opens the Add Node Menu for the north (2) port of the selected node.	<Shift+2> (2 in Keyboard Mode)
Add to East Port	Edit	Opens the Add Node Menu for the east (3) port of the selected node.	<Shift+3> (3 in Keyboard Mode)
Add to South Port	Edit	Opens the Add Node Menu for the south (4) port of the selected node.	<Shift+4> (4 in Keyboard Mode)
Delete Selection	Edit	Deletes the selected nodes and edges.	<Del>
Edit Name	Edit	Enables the name field of the selected node.	<Shift+E> (E in Keyboard Mode)
Normal Position	Edit	(Switching Device Only) Toggles the Normal Position property of the selected node.	<Shift+D> (D in Keyboard Mode)
Set Left PT	Edit	(Switching Device Only) Toggles the Left PT property of the selected node.	<Shift+S> (S in Keyboard Mode)
Set Right PT	Edit	(Switching Device Only) Toggles the Right PT property of the selected node.	<Shift+F> (F in Keyboard Mode)
Show/Hide Ports	Edit	(Junction Only) Shows/Hides the unused ports from the selected junction.	<Shift+R> (R in Keyboard Mode)
Select All	Selection	Select all nodes and edges on the canvas.	<Ctrl+A>
Select All of Type	Selection	When a node or edge is selected, selects all of the same type.	<A>
Move Selection West	Selection	Moves the selection over one node in the direction of the selected node's west (1) port.	<Shift+1> (1 in Keyboard Mode)
Move Selection North	Selection	Moves the selection over one node in the direction of the selected node's north (2) port.	<Shift+2> (2 in Keyboard Mode)
Move Selection East	Selection	Moves the selection over one node in the direction of the selected node's east (3) port.	<Shift+3> (3 in Keyboard Mode)
Move Selection South	Selection	Moves the selection over one node in the direction of the selected node's south (4) port.	<Shift+4> (4 in Keyboard Mode)

## Creating a New Model in PSM

PSM is flexible enough to import CIM and GeoJSON data via MDI while maintaining support for building models manually. *Figure 3.2* shows the available functions for manually adding hierarchy to an existing model.



**Figure 3.2 Power System Model Drafts**

- ① **New Region.** Creates a regional hierarchy based on customer zones.
- ② **New Subregion.** Creates a single tier below a region.
- ③ **New Transmission.** Creates a transmission line for substations to attach to.
- ④ **New Substation.** Creates a substation for feeders to attach to.
- ⑤ **New Feeder.** Creates a canvas for a feeder to be drawn on.
- ⑥ **Search Feature.** Allows users to search within model.

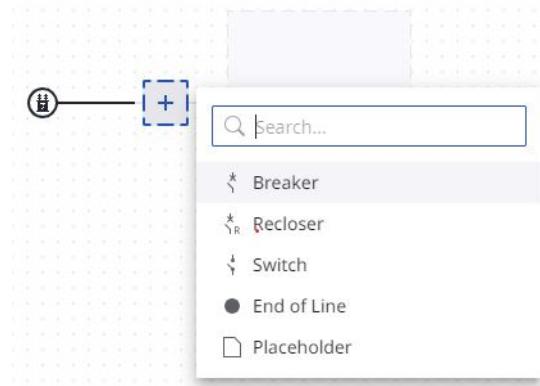
Any element from the above menu has a Checkout, Rename, Discard, and Delete option via a right-click.

A blank canvas appears upon adding a new feeder, as shown in *Figure 3.3*.

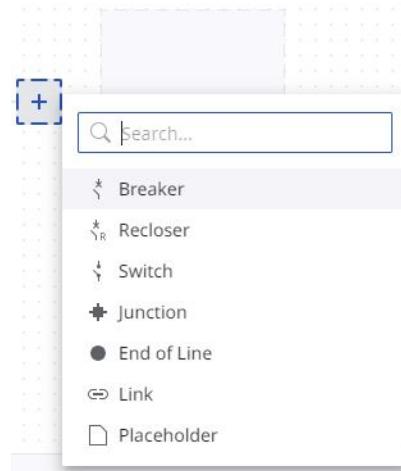


**Figure 3.3 New Manual Feeder**

All feeders must have a device connected to the feeder source (noted by the small transformer in a circle). Select the + (plus) button connected to the feeder source and choose a device type to define the first connected device, as shown in *Figure 3.4*. Once the initial node is defined, a slightly expanded menu will be available by clicking on the + (plus) button, as shown in *Figure 3.5*. The expanded menu allows for additional canvas nodes that help build the one-line diagram and includes Junction and Link Nodes.



**Figure 3.4** New Node Selection Menu



**Figure 3.5** New Node Expanded Menu

All feeders on a canvas need a source, a switching device, and a way to mark either a feeder's end or tie. *Feeder Canvas Nodes and Settings on page 228* provides more detail about each available node type. An End-of-Line, Link, or Placeholder node is required to complete a feeder or branch.

## Canvas Settings

Each canvas has its own model and node settings. Model settings can be configured by selecting any whitespace on the canvas. Node settings can be configured by selecting any node in the Substation and Distribution models.

*Table 3.2* describes the Property Grid Settings for a Transmission Canvas.

**Table 3.2 Transmission Canvas Property Grid Settings**

Setting Name	Description
Name	Substation name. This may only contain printable ASCII characters.
Nominal Voltage	The value (in volts line-to-neutral) that the DMS application uses to determine good or bad voltage.
Measurement Name	Mapped for all devices that have remote communications enabled. The default value is " ". If this setting is empty, it is assumed that Blueframe Protocol Services has not been established with this device.  <b>NOTE</b> This setting must be configured in order for automation applications to run on SCADA data, and the values must match the corresponding name in Protocol Services. If not mapped, that node will not appear in the DMS application.

*Table 3.3 describes the Property Grid Settings for a Substation Canvas.*

**Table 3.3 Substation Canvas Property Grid Settings**

Setting Name	Description
Name	Substation name. This may only contain printable ASCII characters.
Latitude	The north-south coordinate of the substation.
Longitude	The east-west coordinate of the substation.
Measurement Name	Mapped for all devices that have remote communications enabled. The default value is " ". If this setting is empty, it is assumed that Blueframe Protocol Services has not been established with this device.  <b>NOTE</b> This setting must be configured in order for automation applications to run on SCADA data, and the values must match the corresponding name in Protocol Services. If not mapped, that node will not appear in the DMS application.

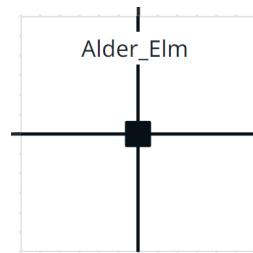
*Table 3.4 describes the Property Grid Settings for a Feeder canvas.*

**Table 3.4 Feeder Canvas Property Grid Settings**

Setting Name	Description
Name	Feeder name. This may only contain printable ASCII characters.
Measurement Name	Mapped for all devices that have remote communications enabled. The default value is " ". If this setting is empty, it is assumed that Blueframe Protocol Services has not been established with this device.  <b>NOTE</b> This setting must be configured in order for automation applications to run on SCADA data, and the values must match the corresponding name in Protocol Services. If not mapped, that node will not appear in the DMS application.
Nominal Voltage	The value (in volts line-to-neutral) that the DMS application uses to determine good or bad voltage. For example, FLISR uses this for display purposes as well as in verifying de-energized devices in fault zones when evaluating an event.
Low Voltage Threshold	This value is used to determine at which percentage of normal measurement a feeder is considered de-energized. (For example, if set to 10 percent, FLISR will confirm that all devices in a known fault zone are under 10 percent of nominal voltage. If true, the zone will be considered de-energized.)

# Transmission Canvas Nodes and Settings

## Junction

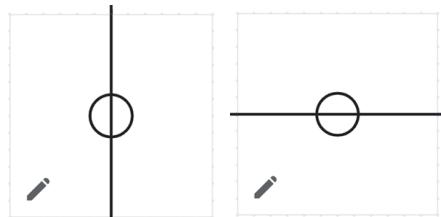


The Junction node indicates when the distribution line splits off in more than one direction. It supports line branching in a total of four directions.

**Table 3.5 Junction Node Settings**

Setting Name	Description
Name	Device name (e.g., Switch 4). This may only contain printable ASCII characters.
In Service	An indication (true or false) of whether the asset is in service. The default value is True.
Enabled	An indication (true or false) of whether the asset is enabled. The default value is True.
Underground	An indication (true or false) of whether an asset is a real underground asset. The default value is False.
Nominal Voltage	System voltage of the feeder. The default value is 12470.
Phasing	The number of phases in the system (single, double, or three-phase) and how they are oriented.
Current Rating	Capacity, in amperes, for the selected node.

## Line Segment



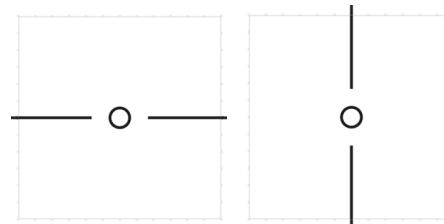
A Line Segment node models a set of Pole nodes. To edit the coordinates of the pole nodes, select the Edit icon and upload a .csv file to the edit dialog.

**Table 3.6 Transmission Line Segment Node Settings**

Setting Name	Description
Name	Device name. This may only contain printable ASCII characters.
Nominal Voltage	System voltage of the transmission line.
X	Positive-sequence line reactance.
R	Positive-sequence line resistance.
B	Positive-sequence shunt susceptance.

Setting Name	Description
G	Positive-sequence shunt conductance.
Measurement Name	<p>Mapped for all devices that have remote communications enabled. The default value is " ". If this setting is empty, it is assumed that Blueframe Protocol Services has not been established with this device.</p> <p><b>NOTE</b> This setting must be configured in order for automation applications to run on SCADA data, and the values must match the corresponding name in Protocol Services. If not mapped, that node will not appear in the DMS application.</p>

## Pole



A Pole node models a physical pole that consists of the following attributes:

- ▶ Latitude
- ▶ Longitude

**Table 3.7 Transmission Pole Node Settings**

Setting Name	Description
Name	Device name. This may only contain printable ASCII characters.
Latitude	The north-south coordinate of the pole.
Longitude	The east-west coordinate of the pole.
Measurement Name	<p>Mapped for all devices that have remote communications enabled. The default value is " ". If this setting is empty, it is assumed that Blueframe Protocol Services has not been established with this device.</p> <p><b>NOTE</b> This setting must be configured in order for automation applications to run on SCADA data, and the values must match the corresponding name in Protocol Services. If not mapped, that node will not appear in the DMS application.</p>

## Link



The Link node connects electrical locations that exist either on the same feeder or on different feeder canvases. You can link a Link node on one canvas to a Link node on another canvas.

## Line



A Line node models a substation line that consists of the following attributes:

- ▶ Three-phase status
- ▶ Phasing

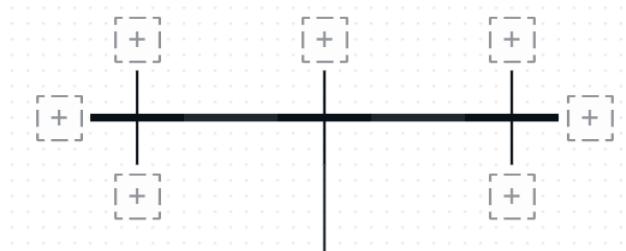
*Table 3.8* describes the Property Grid settings for Line nodes.

**Table 3.8 Transmission Line Node Settings**

Setting Name	Description
Enabled	An indication (true or false) of whether the asset is enabled. The default value is True.
Underground	An indication (true or false) of whether an asset is a real underground asset. The default value is False.
Nominal Voltage	System voltage of the substation. The default value is 12470.
Phasing	The number of phases in the system (single, double, or three-phase) and how they are oriented.
Latitude	The north-south coordinate of the substation.

## Substation Canvas Nodes and Settings

### Busbar



A Busbar node models a substation busbar that consists of the following attributes:

- ▶ Three-phase status
- ▶ Phasing

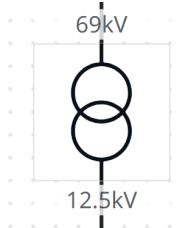
*Table 3.9* describes the Property Grid settings for Busbar nodes.

**Table 3.9 Substation Busbar Node Settings**

Setting Name	Description
Name	Device name (e.g., Switch 4). This may only contain printable ASCII characters.
In Service	An indication (true or false) of whether the asset is in service. The default value is True.
Enabled	An indication (true or false) of whether the asset is enabled. The default value is True.

Setting Name	Description
Underground	An indication (true or false) of whether an asset is a real underground asset. The default value is False.
Nominal Voltage	System voltage of the point of connection. The default value is 12470.
Phasing	The number of phases in the system (single, double, or three-phase) and how they are oriented.
Current Rating	Capacity, in amperes, for the selected node. Default value is 625 A.
Latitude	The north-south coordinate of the equipment.
Longitude	The east-west coordinate of the equipment.

## Transformer



A Transformer node models a substation transformer that consists of the following attributes:

- ▶ Three-phase status
- ▶ Primary winding voltage and current rating
- ▶ Secondary winding voltage and current rating

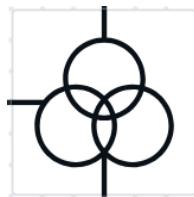
*Table 3.10* describes the Property Grid settings for Transformer nodes.

**Table 3.10 Substation Transformer Node Settings**

Setting Name	Description
Name	Device name (e.g., Switch 4). This may only contain printable ASCII characters.
Measurement Name	A unique setting across all feeders that should be mapped for all devices that have remote communications enabled. The default value is ". If this setting is empty, it is assumed that Blueframe Protocol Services have not been established with this device.
<b>NOTE</b>	
This setting must be configured in order for automation applications to run on SCADA data, and the values must match the corresponding name in Protocol Services. If not mapped, that node will not appear in the DMS application.	
In Service	An indication (true or false) of whether the asset is in service. The default value is True.
Enabled	An indication (true or false) of whether the asset is enabled. The default value is True.
Underground	An indication (true or false) of whether an asset is a real underground asset. The default value is False.
Phasing	The number of phases in the system (single, double, or three-phase) and how they are oriented.
Primary Winding Nominal Voltage	System voltage of the point of connection. The default value is 12470.
Primary Winding Current Rating	Capacity, in amperes, for the selected node. Default value is 625 A.
Secondary Winding Nominal Voltage	System voltage of the point of connection. The default value is 12470.

Setting Name	Description
Secondary Winding Current Rating	Capacity, in amperes, for the selected node. Default value is 625 A.
Latitude	The north-south coordinate of the equipment.
Longitude	The east-west coordinate of the equipment.

## 3-Winding Transformer



A 3-Winding Transformer node models a substation three-winding transformer that consists of the following attributes:

- ▶ Three-phase status
- ▶ Primary winding voltage and current rating
- ▶ Secondary winding voltage and current rating
- ▶ Tertiary winding voltage and current rating

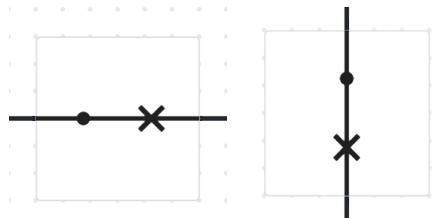
Table 3.11 describes the Property Grid settings for 3 Winding Transformer nodes.

**Table 3.11 Substation Winding Transformer Node Settings**

Setting Name	Description
Name	Device name (e.g., Switch 4). This may only contain printable ASCII characters.
Measurement Name	A unique setting across all feeders that should be mapped for all devices that have remote communications enabled. The default value is " ". If this setting is empty, it is assumed that Blueframe Protocol Services have not been established with this device.
<b>NOTE</b>	
	This setting must be configured in order for automation applications to run on SCADA data, and the values must match the corresponding name in Protocol Services. If not mapped, that node will not appear in the DMS application.
In Service	An indication (true or false) of whether the asset is in service. The default value is True.
Enabled	An indication (true or false) of whether the asset is enabled. The default value is True.
Underground	An indication (true or false) of whether an asset is a real underground asset. The default value is False.
Phasing	The number of phases in the system (single, double, or three-phase) and how they are oriented.
Primary Winding Nominal Voltage	System voltage of the point of connection. The default value is 12470.
Primary Winding Current Rating	Capacity, in amperes, for the selected node. Default value is 625 A.
Secondary Winding Nominal Voltage	System voltage of the point of connection. The default value is 12470.
Secondary Winding Current Rating	Capacity, in amperes, for the selected node. Default value is 625 A.

Setting Name	Description
Tertiary Winding Nominal Voltage	System voltage of the point of connection. The default value is 12470.
Tertiary Winding Current Rating	Capacity, in amperes, for the selected node. Default value is 625 A.
Latitude	The north-south coordinate of the equipment.
Longitude	The east-west coordinate of the equipment.

## Breaker



A Breaker node models a substation breaker that consists of the following attributes:

- ▶ Three-phase breaker status
- ▶ A-phase, B-phase, and C-phase currents
- ▶ Nominal voltage
- ▶ Lockout indication
- ▶ Fault indication
- ▶ Voltage indication
- ▶ DMS capacity (in amperes)

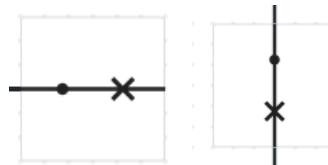
*Table 3.12* describes the Property Grid settings for Breaker nodes.

**Table 3.12 Substation Breaker Node Settings**

Setting Name	Description
Name	Device name (e.g., Breaker 4). This may only contain printable ASCII characters.
Measurement Name	A unique setting across all feeders that should be mapped for all devices that have remote communications enabled. The default value is " ". If this setting is empty, it is assumed that Blueframe Protocol Services has not been established with this device.
<b>NOTE</b>	
This setting must be configured in order for automation applications to run on SCADA data, and the values must match the corresponding name in Protocol Services. If not mapped, that node will not appear in the DMS application.	
In Service	An indication (true or false) of whether the asset is in service. The default value is True.
Enabled	An indication (true or false) of whether the asset is enabled. The default value is True.
Underground	An indication (true or false) of whether an asset is a real underground asset. The default value is False.
Nominal Voltage	System voltage of the point of connection. The default value is 12470.
Phasing	The number of phases in the system (single, double, or three-phase) and how they are oriented.
Left PT	Select which three-phase voltage set is oriented to the left side of the node as drawn on the canvas. The options are Set1, Set2, and None. The default value is None.

Setting Name	Description
Right PT	Select which three-phase voltage set is oriented to the right side of the node as drawn on the canvas. The options are Set1, Set2, and None. The default value is None.
Current Rating	Capacity, in amperes, for the selected node.
DMS Capacity	Rating, in percent, of Current Rating that DMS applications, such as FLISR, can use as a maximum permissible value when evaluating restoration solutions. The default value is 80 percent.
Gang Operated	This property is read-only and is always True. PSM supports only three-phase normal status settings at this time.
A-Phase Normally Open	The normal state of the breaker's A-Phase that is used by DMS applications. The options are False and True. The default value is False.
B-Phase Normally Open	The normal state of the breaker's B-Phase that is used by DMS applications. The options are False and True. The default value is False.
C-Phase Normally Open	The normal state of the breaker's C-Phase that is used by DMS applications. The options are False and True. The default value is False.
Current Scalar	The value by which DMS applications must scale incoming current data points in order to get amperes. (For example, if the incoming current data points are in kiloamperes, the scalar should be set to 1000 to convert to amperes.)
Voltage Scalar	The value by which DMS applications must scale incoming voltage data points in order to get volts. (For example, if the incoming voltage data points are in kilovolts, the scalar should be set to 1000 to convert to volts.)
Is Manual	An indication (true or false) of whether an asset is manually operated.
Has Status	An indication (true or false) of whether an asset has statuses in the data map.
Has Fault Indication	An indication (true or false) of whether an asset has fault indication (not lockout) that will be in the data map.
Has Currents	An indication (true or false) of whether an asset has current measurements that will be in the data map.
Latitude	The north-south coordinate of the equipment.
Longitude	The east-west coordinate of the equipment.

## Recloser



A Recloser node models a substation recloser that consists of the following attributes:

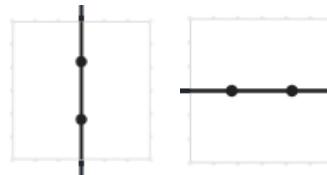
- ▶ Three-phase breaker status
- ▶ A-phase, B-phase, and C-phase currents
- ▶ Nominal voltage
- ▶ Lockout indication
- ▶ Fault indication
- ▶ Voltage indication
- ▶ DMS capacity (in amperes)

Table 3.13 describes the Property Grid settings for Recloser nodes.

**Table 3.13 Substation Recloser Node Settings**

Setting Name	Description
Name	Device name (e.g., Breaker 4). This may only contain printable ASCII characters.
Measurement Name	A unique setting across all feeders that should be mapped for all devices that have remote communications enabled. The default value is " ". If this setting is empty, it is assumed that Blueframe Protocol Services has not been established with this device.
<b>NOTE</b>	
This setting must be configured in order for automation applications to run on SCADA data, and the values must match the corresponding name in Protocol Services. If not mapped, that node will not appear in the DMS application.	
In Service	An indication (true or false) of whether the asset is in service. The default value is True.
Enabled	An indication (true or false) of whether the asset is enabled. The default value is True.
Underground	An indication (true or false) of whether an asset is a real underground asset. The default value is False.
Nominal Voltage	System voltage of the point of connection. The default value is 12470.
Phasing	The number of phases in the system (single, double, or three-phase) and how they are oriented.
Left PT	Select which three-phase voltage set is oriented to the left side of the node as drawn on the canvas. The options are Set1, Set2, and None. The default value is None.
Right PT	Select which three-phase voltage set is oriented to the right side of the node as drawn on the canvas. The options are Set1, Set2, and None. The default value is None.
Current Rating	Capacity, in amperes, for the selected node.
DMS Capacity	Rating, in percent, of Current Rating that DMS applications, such as FLISR, can use as a maximum permissible value when evaluating restoration solutions. The default value is 80 percent.
Gang Operated	This property is read-only and is always True. PSM supports only three-phase normal status settings at this time.
A-Phase Normally Open	The normal state of the breaker's A-Phase that is used by DMS applications. The options are False and True. The default value is False.
B-Phase Normally Open	The normal state of the breaker's B-Phase that is used by DMS applications. The options are False and True. The default value is False.
C-Phase Normally Open	The normal state of the breaker's C-Phase that is used by DMS applications. The options are False and True. The default value is False.
Current Scalar	The value by which DMS applications must scale incoming current data points in order to get amperes. (For example, if the incoming current data points are in kiloamperes, the scalar should be set to 1000 to convert to amperes.)
Voltage Scalar	The value by which DMS applications must scale incoming voltage data points in order to get volts. (For example, if the incoming voltage data points are in kilovolts, the scalar should be set to 1000 to convert to volts.)
Is Manual	An indication (true or false) of whether an asset is manually operated.
Has Status	An indication (true or false) of whether an asset has statuses in the data map.
Has Fault Indication	An indication (true or false) of whether an asset has fault indication (not lockout) that will be in the data map.
Has Currents	An indication (true or false) of whether an asset has current measurements that will be in the data map.
Latitude	The north-south coordinate of the equipment.
Longitude	The east-west coordinate of the equipment.

## Switch



A Switch node models a substation switch that consists of the following attributes:

- ▶ Three-phase breaker status
- ▶ A-phase, B-phase, and C-phase currents
- ▶ Nominal voltage
- ▶ Lockout indication
- ▶ Fault indication
- ▶ Voltage indication
- ▶ DMS capacity (in amperes)

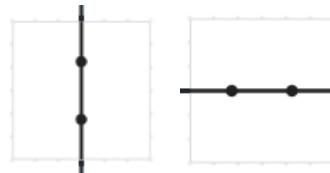
*Table 3.14* describes the Property Grid settings for Switch nodes.

**Table 3.14 Substation Switch Node Settings**

Setting Name	Description
Name	Device name (e.g., Breaker 4). This may only contain printable ASCII characters.
Measurement Name	A unique setting across all feeders that should be mapped for all devices that have remote communications enabled. The default value is " ". If this setting is empty, it is assumed that Blueframe Protocol Services has not been established with this device.  <b>NOTE</b> This setting must be configured in order for automation applications to run on SCADA data, and the values must match the corresponding name in Protocol Services. If not mapped, that node will not appear in the DMS application.
In Service	An indication (true or false) of whether the asset is in service. The default value is True.
Enabled	An indication (true or false) of whether the asset is enabled. The default value is True.
Underground	An indication (true or false) of whether an asset is a real underground asset. The default value is False.
Nominal Voltage	System voltage of the point of connection. The default value is 12470.
Phasing	The number of phases in the system (single, double, or three-phase) and how they are oriented.
Left PT	Select which three-phase voltage set is oriented to the left side of the node as drawn on the canvas. The options are Set1, Set2, and None. The default value is None.
Right PT	Select which three-phase voltage set is oriented to the right side of the node as drawn on the canvas. The options are Set1, Set2, and None. The default value is None.
Current Rating	Capacity, in amperes, for the selected node.
DMS Capacity	Rating, in percent, of Current Rating that DMS applications, such as FLISR, can use as a maximum permissible value when evaluating restoration solutions. The default value is 80 percent.
Gang Operated	This property is read-only and is always True. PSM supports only three-phase normal status settings at this time.
A-Phase Normally Open	The normal state of the breaker's A-Phase that is used by DMS applications. The options are False and True. The default value is False.

Setting Name	Description
B-Phase Normally Open	The normal state of the breaker's B-Phase that is used by DMS applications. The options are False and True. The default value is False.
C-Phase Normally Open	The normal state of the breaker's C-Phase that is used by DMS applications. The options are False and True. The default value is False.
Current Scalar	The value by which DMS applications must scale incoming current data points in order to get amperes. (For example, if the incoming current data points are in kiloamperes, the scalar should be set to 1000 to convert to amperes.)
Voltage Scalar	The value by which DMS applications must scale incoming voltage data points in order to get volts. (For example, if the incoming voltage data points are in kilovolts, the scalar should be set to 1000 to convert to volts.)
Is Manual	An indication (true or false) of whether an asset is manually operated.
Has Status	An indication (true or false) of whether an asset has statuses in the data map.
Has Fault Indication	An indication (true or false) of whether an asset has fault indication (not lockout) that will be in the data map.
Has Currents	An indication (true or false) of whether an asset has current measurements that will be in the data map.
Latitude	The north-south coordinate of the equipment.
Longitude	The east-west coordinate of the equipment.

## Tie



A Tie node models a substation tie that consists of the following attributes:

- Three-phase breaker status
- A-phase, B-phase, and C-phase currents
- Nominal voltage
- Lockout indication
- Fault indication
- DMS capacity (in amperes)

Table 3.15 describes the Property Grid settings for Tie nodes.

Table 3.15 Substation Tie Node Settings

Setting Name	Description
Name	Device name (e.g., Breaker 4). This may only contain printable ASCII characters.
Measurement Name	A unique setting across all feeders that should be mapped for all devices that have remote communications enabled. The default value is " ". If this setting is empty, it is assumed that Blueframe Protocol Services has not been established with this device.
<b>NOTE</b>	This setting must be configured in order for automation applications to run on SCADA data, and the values must match the corresponding name in Protocol Services. If not mapped, that node will not appear in the DMS application.
In Service	An indication (true or false) of whether the asset is in service. The default value is True.

Setting Name	Description
Enabled	An indication (true or false) of whether the asset is enabled. The default value is True.
Underground	An indication (true or false) of whether an asset is a real underground asset. The default value is False.
Nominal Voltage	System voltage of the point of connection. The default value is 12470.
Phasing	The number of phases in the system (single, double, or three-phase) and how they are oriented.
Left PT	Select which three-phase voltage set is oriented to the left side of the node as drawn on the canvas. The options are Set1, Set2, and None. The default value is None.
Right PT	Select which three-phase voltage set is oriented to the right side of the node as drawn on the canvas. The options are Set1, Set2, and None. The default value is None.
Current Rating	Capacity, in amperes, for the selected node.
DMS Capacity	Rating in percent of Current Rating that DMS applications, such as FLISR, can use as a maximum permissible value when evaluating restoration solutions. The default value is 80 percent.
Gang Operated	This property is read-only and is always True. PSM supports only three-phase normal status settings at this time.
A-Phase Normally Open	The normal state of the breaker's A-Phase that is used by DMS applications. The options are False and True. The default value is False.
B-Phase Normally Open	The normal state of the breaker's B-Phase that is used by DMS applications. The options are False and True. The default value is False.
C-Phase Normally Open	The normal state of the breaker's C-Phase that is used by DMS applications. The options are False and True. The default value is False.
Current Scalar	The value by which DMS applications must scale incoming current data points in order to get amperes. (For example, if the incoming current data points are in kiloamperes, the scalar should be set to 1000 to convert to amperes.)
Voltage Scalar	The value by which DMS applications must scale incoming voltage data points in order to get volts. (For example, if the incoming voltage data points are in kilovolts, the scalar should be set to 1000 to convert to volts.)
Is Manual	An indication (true or false) of whether an asset is manually operated.
Has Status	An indication (true or false) of whether an asset has statuses in the data map.
Has Fault Indication	An indication (true or false) of whether an asset has fault indication (not lockout) that will be in the data map.
Has Currents	An indication (true or false) of whether an asset has current measurements that will be in the data map.
Latitude	The north-south coordinate of the equipment.
Longitude	The east-west coordinate of the equipment.

## Fuse



A Fuse node models a substation fuse that consists of the following attributes:

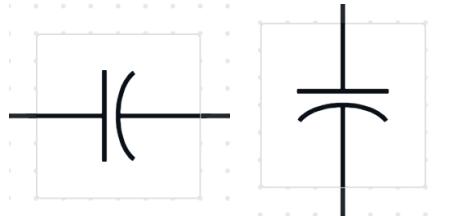
- ▶ Three-phase status
- ▶ Phasing

*Table 3.16* describes the Property Grid settings for fuse nodes.

**Table 3.16 Substation Fuse Node Settings**

Setting Name	Description
Name	Device name (e.g., Switch 4). This may only contain printable ASCII characters.
In Service	An indication (true or false) of whether the asset is in service. The default value is True.
Enabled	An indication (true or false) of whether the asset is enabled. The default value is True.
Underground	An indication (true or false) of whether an asset is a real underground asset. The default value is False.
Nominal Voltage	System voltage of the point of connection. The default value is 12470.
Phasing	The number of phases in the system (single, double, or three-phase) and how they are oriented.
Current Rating	Capacity, in amperes, for the selected node. Default value is 625 A.
Latitude	The north-south coordinate of the equipment.
Longitude	The east-west coordinate of the equipment.

## Capacitor Bank



A Capacitor Bank node models a substation Capacitor Bank that consists of the following attributes:

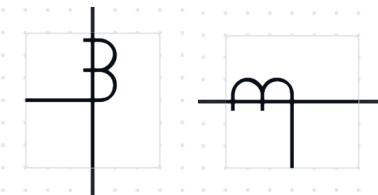
- Three-phase status
- Phasing

*Table 3.17 describes the Property Grid settings for capacitor bank nodes.*

**Table 3.17 Substation Capacitor Bank Node Settings**

Setting Name	Description
Name	Device name (e.g., Switch 4). This may only contain printable ASCII characters.
In Service	An indication (true or false) of whether the asset is in service. The default value is True.
Enabled	An indication (true or false) of whether the asset is enabled. The default value is True.
Underground	An indication (true or false) of whether an asset is a real underground asset. The default value is False.
Nominal Voltage	System voltage of the point of connection. The default value is 12470.
Phasing	The number of phases in the system (single, double, or three-phase) and how they are oriented.
Current Rating	Capacity, in amperes, for the selected node. Default value is 625 A.
Latitude	The north-south coordinate of the equipment.
Longitude	The east-west coordinate of the equipment.

## Current Transformer



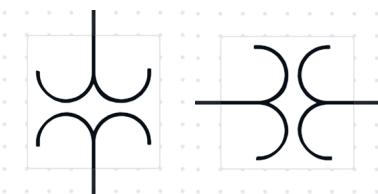
The Current Transformer node models a current transformer that consists of the following attributes:

- ▶ Three-phase status
- ▶ Three-phase current rating

**Table 3.18 Substation Current Transformer Node Settings**

Setting Name	Description
Name	Device name. This may only contain printable ASCII characters.
In Service	An indication (true or false) of whether the asset is in service. The default value is True.
Enabled	An indication (true or false) of whether the asset is enabled. The default value is True.
Underground	An indication (true or false) of whether an asset is a real underground asset. The default value is False.
Nominal Voltage	System voltage of the point of connection.
Phasing	The number of phases in the system (single, double, or three-phase) and how they are oriented.
Current Rating	Capacity, in amperes, for the selected node.
Direction	The reference direction for current with respect to the device with which the CT is associated.
Latitude	The north-south coordinate of the equipment.
Longitude	The east-west coordinate of the equipment.
Measurement Name	A unique setting across all feeders that should be mapped for all devices that have remote communications enabled. The default value is " ". If this setting is empty, it is assumed that Blueframe Protocol Services has not been established with this device.
<b>NOTE</b>	
This setting must be configured in order for automation applications to run on SCADA data, and the values must match the corresponding name in Protocol Services. If not mapped, that node will not appear in the DMS application.	

## Potential Transformer



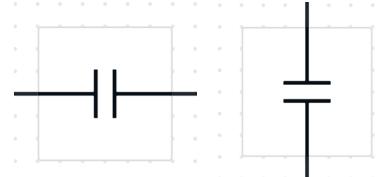
The Potential Transformer node models a potential transformer that consists of the following attributes:

- ▶ Three-phase status
- ▶ Three-phase current rating

**Table 3.19 Substation Potential Transformer Node Settings**

Setting Name	Description
Name	Device name. This may only contain printable ASCII characters.
In Service	An indication (true or false) of whether the asset is in service. The default value is True.
Enabled	An indication (true or false) of whether the asset is enabled. The default value is True.
Underground	An indication (true or false) of whether an asset is a real underground asset. The default value is False.
Nominal Voltage	System voltage of the point of connection.
Phasing	The number of phases in the system (single, double, or three-phase) and how they are oriented.
Current Rating	Capacity, in amperes, for the selected node.
Latitude	The north-south coordinate of the equipment.
Longitude	The east-west coordinate of the equipment.
Measurement Name	A unique setting across all feeders that should be mapped for all devices that have remote communications enabled. The default value is " ". If this setting is empty, it is assumed that Blueframe Protocol Services has not been established with this device.
<b>NOTE</b>	
This setting must be configured in order for automation applications to run on SCADA data, and the values must match the corresponding name in Protocol Services. If not mapped, that node will not appear in the DMS application.	

## Series Compensator



The Series Compensator node models a series compensator that consists of the following attributes:

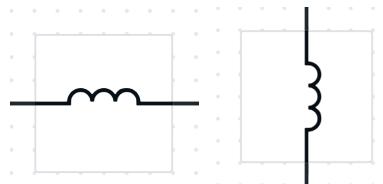
- ▶ Three-phase status
- ▶ Three-phase current rating

**Table 3.20 Substation Series Compensator Node Settings**

Setting Name	Description
Name	Device name. This may only contain printable ASCII characters.
In Service	An indication (true or false) of whether the asset is in service. The default value is True.
Enabled	An indication (true or false) of whether the asset is enabled. The default value is True.
Underground	An indication (true or false) of whether an asset is a real underground asset. The default value is False.
Nominal Voltage	System voltage of the point of connection.
Phasing	The number of phases in the system (single, double, or three-phase) and how they are oriented.
Current Rating	Capacity, in amperes, for the selected node.
X	Positive-sequence reactance.

Setting Name	Description
R	Positive-sequence resistance.
Latitude	The north-south coordinate of the equipment.
Longitude	The east-west coordinate of the equipment.
Measurement Name	A unique setting across all feeders that should be mapped for all devices that have remote communications enabled. The default value is ". If this setting is empty, it is assumed that Blueframe Protocol Services has not been established with this device.
	<p><b>NOTE</b></p> <p>This setting must be configured in order for automation applications to run on SCADA data, and the values must match the corresponding name in Protocol Services. If not mapped, that node will not appear in the DMS application.</p>

## Shunt Compensator



The Shunt Compensator node models a shunt compensator that consists of the following attributes:

- ▶ Three-phase status
- ▶ Three-phase current rating
- ▶ Sections
  - Individual capacitors in a switchable bank
  - Inductors in a switchable bank

**Table 3.21 Substation Shunt Compensator Node Settings**

Setting Name	Description
Name	Device name. This may only contain printable ASCII characters.
In Service	An indication (true or false) of whether the asset is in service. The default value is True.
Enabled	An indication (true or false) of whether the asset is enabled. The default value is True.
Underground	An indication (true or false) of whether an asset is a real underground asset. The default value is False.
Nominal Voltage	System voltage of the point of connection.
Phasing	The number of phases in the system (single, double, or three-phase) and how they are oriented.
Current Rating	Capacity, in amperes, for the selected node.
Max Sections	Maximum number of sections that can be switched in.
Normal Sections	Number of sections switched-in during normal operation.
B per Section	Positive-sequence shunt susceptance per section.
G per Section	Positive-sequence shunt conductance per section.
Latitude	The north-south coordinate of the equipment.

Setting Name	Description
Longitude	The east-west coordinate of the equipment.
Measurement Name	A unique setting across all feeders that should be mapped for all devices that have remote communications enabled. The default value is " ". If this setting is empty, it is assumed that Blueframe Protocol Services has not been established with this device.  <b>NOTE</b> This setting must be configured in order for automation applications to run on SCADA data, and the values must match the corresponding name in Protocol Services. If not mapped, that node will not appear in the DMS application.

## Line



A Line node models a substation line that consists of the following attributes:

- ▶ Three-phase status
- ▶ Phasing

*Table 3.22* describes the Property Grid settings for Line nodes.

**Table 3.22 Substation Line Node Settings**

Setting Name	Description
Enabled	An indication (true or false) of whether the asset is enabled. The default value is True.
Underground	An indication (true or false) of whether an asset is a real underground asset. The default value is False.
Nominal Voltage	System voltage of the points of connection. The default value is 12470.
Phasing	The number of phases in the system (single, double, or three-phase) and how they are oriented.

## Junction



The Junction node indicates when the distribution line splits off in more than one direction. It supports line branching in a total of four directions.

**Table 3.23 Junction Node Settings**

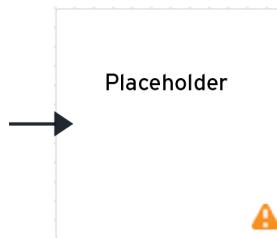
Setting Name	Description
Name	Device name (e.g., Switch 4). This may only contain printable ASCII characters.
In Service	An indication (true or false) of whether the asset is in service. The default value is True.
Enabled	An indication (true or false) of whether the asset is enabled. The default value is True.
Underground	An indication (true or false) of whether an asset is a real underground asset. The default value is False.
Nominal Voltage	System voltage of the points of connection. The default value is 12470.
Phasing	The number of phases in the system (single, double, or three-phase) and how they are oriented.
Current Rating	Capacity, in amperes, for the selected node.
Latitude	The north-south coordinate of the equipment.
Longitude	The east-west coordinate of the equipment.

## Link



The Link node connects electrical locations that exist either on the same substation canvas or on a different canvas. You can link a Link node on one canvas to a Link node on another canvas.

## Placeholder



The Placeholder node is used to define a future Link node, and it allows a user to publish and even run simulations if needed before the link is added. Once the additional canvases are added and links are constructed, the Placeholder node will disappear.

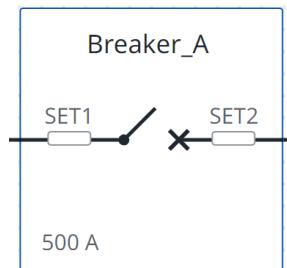
**Table 3.24 Placeholder Node Settings**

Setting Name	Description
Name	Device name (e.g., Switch 4). This may only contain printable ASCII characters.
In Service	An indication (true or false) of whether the asset is in service. The default value is True.
Enabled	An indication (true or false) of whether the asset is enabled. The default value is True.

Setting Name	Description
Underground	An indication (true or false) of whether an asset is a real underground asset. The default value is False.
Nominal Voltage	System voltage of the point of connection. The default value is 12470.
Phasing	The number of phases in the system (single, double, or three-phase) and how they are oriented.
Current Rating	Capacity, in amperes, for the selected node.
Latitude	The north-south coordinate of the equipment.
Longitude	The east-west coordinate of the equipment.

## Feeder Canvas Nodes and Settings

### Breaker



The Breaker node models a three-phase substation breaker that consists of the following attributes:

- ▶ Three-phase breaker status
- ▶ A-phase, B-phase, and C-phase currents
- ▶ Nominal voltage
- ▶ Lockout indication
- ▶ Fault indication
- ▶ Voltage indications (as many as two sets, if configured)
- ▶ DMS capacity, in amperes.

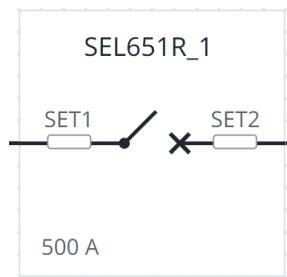
Table 3.25 describes the Property Grid settings for Breaker nodes.

**Table 3.25 Breaker Node Settings**

Setting Name	Description
Name	Device name (e.g., Breaker 4). This may only contain printable ASCII characters.
Measurement Name	A unique setting across all feeders that should be mapped for all devices that have remote communications enabled. The default value is " ". If this setting is empty, it is assumed that Blueframe Protocol Services has not been established with this device.
<b>NOTE</b>	
This setting must be configured in order for automation applications to run on SCADA data, and the values must match the corresponding name in Protocol Services. If not mapped, that node will not appear in the DMS application.	
In Service	An indication (true or false) of whether the asset is in service. The default value is True.
Enabled	An indication (true or false) of whether the asset is enabled. The default value is True.
Underground	An indication (true or false) of whether an asset is a real underground asset. The default value is False.

Setting Name	Description
Nominal Voltage	System voltage of the feeder. The default value is 12470.
Can Load Make	An indication (true or false) of whether the device can be closed into a load. The default value is True.
Can Load Break	An indication (true or false) of whether the device can be opened under load. The default value is False.
Phasing	The number of phases in the system (single, double, or three-phase) and how they are oriented.
Left PT	Select which three-phase voltage set is oriented to the left side of the node as drawn on the canvas. The options are Set1, Set2, and None. The default value is None.
Right PT	Select which three-phase voltage set is oriented to the right side of the node as drawn on the canvas. The options are Set1, Set2, and None. The default value is None.
Current Rating	Capacity, in amperes, for the selected node.
DMS Capacity	Rating in percent of Current Rating that DMS applications, such as FLISR, can use as a maximum permissible value when evaluating restoration solutions. The default value is 80 percent.
Gang Operated	This property is read-only and is always True. PSM supports only three-phase normal status settings at this time.
A-Phase Normally Open	The normal state of the breaker's A-Phase that is used by DMS applications. The options are False and True. The default value is False.
B-Phase Normally Open	The normal state of the breaker's B-Phase that is used by DMS applications. The options are False and True. The default value is False.
C-Phase Normally Open	The normal state of the breaker's C-Phase that is used by DMS applications. The options are False and True. The default value is False.
Current Scalar	The value by which DMS applications must scale incoming current data points in order to get amperes. (For example, if the incoming current data points are in kiloamperes, the scalar should be set to 1000 to convert to amperes.)
Voltage Scalar	The value by which DMS applications must scale incoming voltage data points in order to get volts. (For example, if the incoming voltage data points are in kilovolts, the scalar should be set to 1000 to convert to volts.)
Is Manual	An indication (true or false) of whether an asset is manually operated.
Has Status	An indication (true or false) of whether an asset has statuses in the data map.
Has Fault Indication	An indication (true or false) of whether an asset has fault indication (not lockout) that will be in the data map.
Has Currents	An indication (true or false) of whether an asset has current measurements that will be in the data map.

## Recloser



The Recloser node models a three-phase distribution recloser that consists of the following attributes:

- ▶ Three-phase breaker status
- ▶ A-phase, B-phase, and C-phase currents

- ▶ Nominal voltage
- ▶ Lockout indication
- ▶ Fault indication
- ▶ Voltage indications (as many as two sets, if configured)
- ▶ DMS capacity, in amperes.

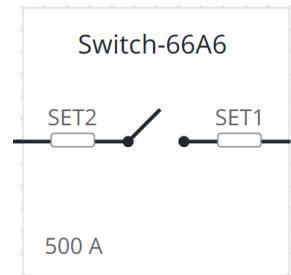
*Table 3.26* describes the Property Grid settings for Recloser nodes.

**Table 3.26 Recloser Node Settings**

Setting Name	Description
Name	Device name (e.g., Recloser 4). This may only contain printable ASCII characters.
Measurement Name	A unique setting across all feeders that should be mapped for all devices that have remote communications enabled. The default value is " ". If this setting is empty, it is assumed that Blueframe Protocol Services has not been established with this device.  <b>NOTE</b> This setting must be configured in order for automation applications to run on SCADA data, and the values must match the corresponding name in Protocol Services. If not mapped, that node will not appear in the DMS application.
In Service	An indication (true or false) of whether the asset is in service. The default value is True.
Enabled	An indication (true or false) of whether the asset is enabled. The default value is True.
Underground	An indication (true or false) of whether an asset is a real underground asset. The default value is False.
Nominal Voltage	System voltage of the feeder. The default value is 12470.
Can Load Make	An indication (true or false) of whether the device can be closed into a load. The default value is True.
Can Load Break	An indication (true or false) of whether the device can be opened under load. The default value is False.
Phasing	The number of phases in the system (single, double, or three-phase) and how they are oriented.
Left PT	Select which three-phase voltage set is oriented to the left side of the node as drawn on the canvas. The options are Set1, Set2, and None. The default value is None.
Right PT	Select which three-phase voltage set is oriented to the right side of the node as drawn on the canvas. The options are Set1, Set2, and None. The default value is None.
DMS Capacity	Rating in percent of Current Rating that DMS applications, such as FLISR, can use as a maximum permissible value when evaluating restoration solutions. The default value is 80 percent.
Gang Operated	This property is read-only and is always True. PSM supports only three-phase normal status settings at this time.
A-Phase Normally Open	The normal state of the breaker's A-Phase that is used by DMS applications. The options are False and True. The default value is False.
B-Phase Normally Open	The normal state of the breaker's B-Phase that is used by DMS applications. The options are False and True. The default value is False.
C-Phase Normally Open	The normal state of the breaker's C-Phase that is used by DMS applications. The options are False and True. The default value is False.
Current Scalar	The value by which DMS applications must scale incoming current data points in order to get amperes. (For example, if the incoming current data points are in kiloamperes, the scalar should be set to 1000 to convert to amperes.)
Voltage Scalar	The value by which DMS applications must scale incoming voltage data points in order to get volts. (For example, if the incoming voltage data points are in kilovolts, the scalar should be set to 1000 to convert to volts.)
Is Manual	An indication (true or false) of whether an asset is manually operated.
Has Status	An indication (true or false) of whether an asset has statuses in the data map.

Setting Name	Description
Has Fault Indication	An indication (true or false) of whether an asset has fault indication (not lockout) that will be in the data map.
Has Currents	An indication (true or false) of whether an asset has current measurements that will be in the data map.

## Switch



The Switch node models a three-phase switch. It differs from the recloser and breaker in that no reclosing attributes are expected. DMS applications base the capability of the switch on how data properties are mapped in *Table 3.27*. This node consists of the following attributes:

- ▶ Three-phase switch status
- ▶ A-phase, B-phase, and C-phase currents
- ▶ Fault indication
- ▶ Voltage indications (as many as two sets, if configured)

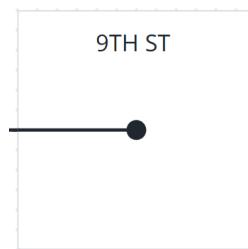
*Table 3.27* describes the Property Grid settings for Switch nodes.

**Table 3.27 Switch Node Settings**

Setting Name	Description
Name	Device name (e.g., Switch 4). This may only contain printable ASCII characters.
Measurement Name	A unique setting across all feeders that should be mapped for all devices that have remote communications enabled. The default value is " ". If this setting is empty, it is assumed that Blueframe Protocol Services has not been established with this device.
<b>NOTE</b>	
This setting must be configured in order for automation applications to run on SCADA data, and the values must match the corresponding name in Protocol Services. If not mapped, that node will not appear in the DMS application.	
In Service	An indication (true or false) of whether the asset is in service. The default value is True.
Enabled	An indication (true or false) of whether the asset is enabled. The default value is True.
Underground	An indication (true or false) of whether an asset is a real underground asset. The default value is False.
Nominal Voltage	System voltage of the feeder. The default value is 12470.
Can Load Make	An indication (true or false) of whether the device can be closed into a load. The default value is True.
Can Load Break	An indication (true or false) of whether the device can be opened under load. The default value is False.
Phasing	The number of phases in the system (single, double, or three-phase) and how they are oriented.
Left PT	Select which three-phase voltage set is oriented to the left side of the node as drawn on the canvas. The options are Set1, Set2, and None. The default value is None.

Setting Name	Description
Right PT	Select which three-phase voltage set is oriented to the right side of the node as drawn on the canvas. The options are Set1, Set2, and None. The default value is None.
DMS Capacity	Rating in percent of Current Rating that DMS applications, such as FLISR, can use as a maximum permissible value when evaluating restoration solutions. The default value is 80 percent.
Gang Operated	This property is read-only and is always True. PSM supports only three-phase normal status settings at this time.
A-Phase Normally Open	The normal state of the breaker's A-Phase that is used by DMS applications. The options are False and True. The default value is False.
B-Phase Normally Open	The normal state of the breaker's B-Phase that is used by DMS applications. The options are False and True. The default value is False.
C-Phase Normally Open	The normal state of the breaker's C-Phase that is used by DMS applications. The options are False and True. The default value is False.
Current Scalar	The value by which DMS applications must scale incoming current data points in order to get amperes. (For example, if the incoming current data points are in kiloamperes, the scalar should be set to 1000 to convert to amperes.)
Voltage Scalar	The value by which DMS applications must scale incoming voltage data points in order to get volts. (For example, if the incoming voltage data points are in kilovolts, the scalar should be set to 1000 to convert to volts.)
Is Manual	An indication (true or false) of whether an asset is manually operated. The default value is False.
Has Status	An indication (true or false) of whether an asset has statuses in the data map. The default value is True.
Has Fault Indication	An indication (true or false) of whether an asset has fault indication (not lockout) that will be in the data map. The default value is True.
Has Currents	An indication (true or false) of whether an asset has current measurements that will be in the data map. The default value is True.

## End of Line



The End-of-Line node indicates an electrical end of the line. This is only necessary in the event that another node, such as a recloser or switch, has nothing electrically significant to PSM on one side of it (all switching device nodes require their left and right connection points to be connected to another node).

**Table 3.28** End-of-Line Node Settings

Setting Name	Description
Name	Device name (e.g., Switch 4). This may only contain printable ASCII characters.
In Service	An indication (true or false) of whether the asset is in service. The default value is True.
Enabled	An indication (true or false) of whether the asset is enabled. The default value is True.
Underground	An indication (true or false) of whether an asset is a real underground asset. The default value is False.

Setting Name	Description
Nominal Voltage	System voltage of the feeder. The default value is 12470.
Phasing	The number of phases in the system (single, double, or three-phase) and how they are oriented.
Current Rating	Capacity, in amperes, for the selected node.

## Junction



The Junction node indicates when the distribution line splits off in more than one direction. It supports line branching in a total of four directions.

**Table 3.29 Junction Node Settings**

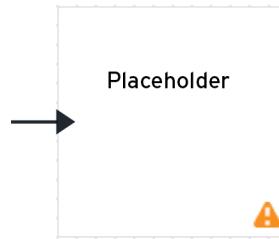
Setting Name	Description
Name	Device name (e.g., Switch 4). This may only contain printable ASCII characters.
In Service	An indication (true or false) of whether the asset is in service. The default value is True.
Enabled	An indication (true or false) of whether the asset is enabled. The default value is True.
Underground	An indication (true or false) of whether an asset is a real underground asset. The default value is False.
Nominal Voltage	System voltage of the feeder. The default value is 12470.
Phasing	The number of phases in the system (single, double, or three-phase) and how they are oriented.
Current Rating	Capacity, in amperes, for the selected node.

## Link



The Link node connects electrical locations that exist either on the same feeder or on different feeder canvases. You can link a Link node on one canvas to a Link node on another canvas.

## Placeholder



The Placeholder node is used to define a future Link node, and it allows a user to publish and even run simulations if needed before the link is added. Once the additional feeders are added and links are constructed, the Placeholder node will disappear.

**Table 3.30 Placeholder Node Settings**

Setting Name	Description
Name	Device name (e.g., Switch 4). This may only contain printable ASCII characters.
In Service	An indication (true or false) of whether the asset is in service. The default value is True.
Enabled	An indication (true or false) of whether the asset is enabled. The default value is True.
Underground	An indication (true or false) of whether an asset is a real underground asset. The default value is False.
Nominal Voltage	System voltage of the feeder. The default value is 12470.
Phasing	The number of phases in the system (single, double, or three-phase) and how they are oriented.
Current Rating	Capacity, in amperes, for the selected node.

## Settings Validation

PSM continuously saves and validates work as you modify settings. The messages provide clear, descriptive validation feedback for the overall project, as well as for each canvas and node in real time (see *Figure 3.6*). You can filter validation messages by canvas and severity.

Validation (5)	
▼ Feeder 1	(5)
● Both sides of a...	Switching devices must have both left and right ports connected.
▲ Island detected...	Device is not connected to source on the given phase.
▲ Island detected...	Device is not connected to source on the given phase.
▲ Island detected...	Device is not connected to source on the given phase.
● Same PT Values	LeftPT and RightPT settings must not be the same set value.

**Figure 3.6 Validation Messages**

## PSM Usage Notes

This section contains a list of usage notes when working with PSM.

## Note 1: FLISR Can Optionally Use PT Measurements to Confirm That All Devices in a Known Fault Zone Are De-Energized

FLISR uses PT measurements to confirm that all devices in a known fault zone are de-energized prior to proceeding with isolation and restoration when the feeder Voltage Integrity Check is enabled. The Voltage Integrity Check uses the Low Voltage Threshold to test for energized feeders. This provides greater operational security against model errors or abnormal switching occurring in the field that FLISR may be inadvertently unaware of.

## Model Publishing and Checkout

---

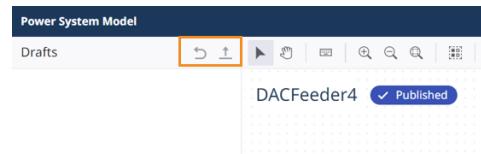
New feeders, substations, transmission lines, and regions are added to PSM as drafts. Drafts appear in the Draft Panel (see *Figure 3.1*). In order to be visible to other Blueframe applications and users, drafts must be published. Draft changes to the model must be published as a batch. Drafts can be discarded either as a batch or individually. Batch publishing or discarding is performed using the controls at the top of the Draft Panel (see *Figure 3.7*). Individual items can be discarded by hovering over the item and selecting the Discard control that appears.

### **IMPORTANT**

Making changes to a canvas that has been commissioned in a Blueframe DMS application will decommission that canvas. A user will need to follow canvas commissioning processes in the DMS application before it will be considered operational.

### **IMPORTANT**

Any model exported in the Unpublished state will lock the model export to the user, i.e., the model must be Published to be exported and shared with other Blueframe users or systems.



**Figure 3.7 Draft Panel**

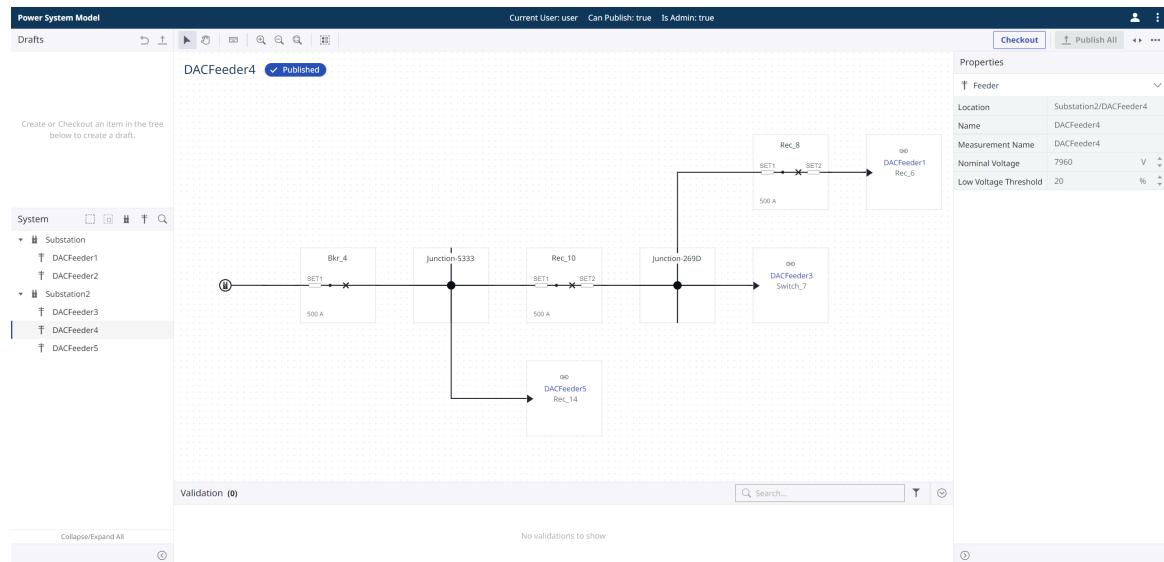
Once a canvas has been published, it is no longer possible to make changes to it without checking it out again (see *Figure 3.8*). Checking out a canvas creates an editable draft.



**Figure 3.8 Feeder Checkout**

# Editing a Published System

Select the **Checkout** button and edit the unpublished canvas to add or remove switching devices, adjust the capacity settings, or change PT configurations on a published canvas (see *Figure 3.9*).

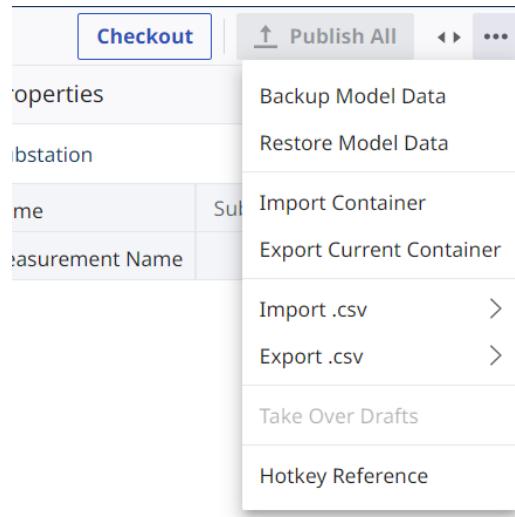


**Figure 3.9** PSM Model Editing

The checkout function removes the canvas from the published branch within the corresponding automation application. A single user can check out multiple canvases, but an individual canvas can only be checked out by one user at a time. Once a canvas is checked out, editing a canvas is similar to drawing a feeder or substation without MDI where nodes can be added or removed and properties changed. See *Creating a New Model in PSM* on page 208 for additional details on adding nodes to a model.

## Model Management Tools

PSM provides multiple ways to manage a model. These are accessed through the ellipsis in the top right, as shown in *Figure 3.10*.



**Figure 3.10 Model Management Tools**

- **Backup Model Data:** Backs up the current model represented in PSM (.json file).
- **Restore Model Data:** Restores any model exported from PSM.
- **Import Container:** Imports all PSM feeders.
- **Export Current Container:** Exports current feeder in PSM (.bin file).
- **Import .csv:** Imports all export containers or devices via .csv.
- **Export .csv:** Exports a PSM model as an editable .csv file. This can either be done by containers (source in canvas) or by all devices (for all containers).
- **Take Over Drafts:** Allows a user with the Administrator role to become owner of a draft that another user has checked out.
- **Hot Key Reference:** Opens a reference to PSM keyboard shortcuts.

## Model Conversion

If you currently have a model created with PSM version 1.0.0 and are upgrading to a later release of PSM, you must make certain changes. The following lists the model differences that need to be accounted for when upgrading from PSM version 1.0.0 to PSM version 1.2.0. SEL recommends upgrading to PSM version 1.2.0 first and then upgrading to newer releases.

- Any mapped value in PSM version 1.0.0 defined as 0 or 1 will not be True or False.
- When opening a PSM version 1.0.0 model in PSM version 1.2.0, any 0 or 1 value will default to a closed position.
- Request JSON by using the API to make any global model changes.

**This page intentionally left blank**

---

---

## S E C T I O N   4

---

# FLISR

## Overview

---

The FLISR application contains the run-time algorithms and simulation capabilities that are compatible with the DMS suite. Feeder canvases commissioned from within PSM are visible when FLISR is launched from the Blueframe Portal. When you view a feeder canvas through the FLISR application, the canvas is populated with DNP3 data incoming from field device connections as well as status information from the FLISR algorithms. The feeder canvas can convey to the user what data FLISR is receiving and what events it is processing in real time, all within a web browser.

## FLISR Fundamentals

---

FLISR improves distribution system reliability by minimizing the impact an outage has on a feeder and on the customers to which it provides power. FLISR analyzes incoming feeder and substation data to determine where a fault, an open phase, or a loss-of-source event has occurred. During these events, FLISR will isolate the event based on the data it is given and restore load to as many customers as it can while considering factors such as human safety and system limitations.

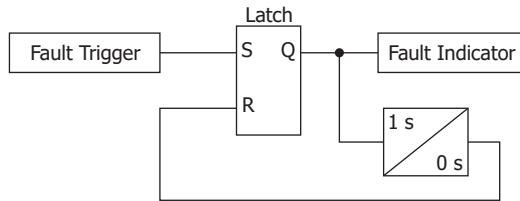
## How Fault Location Works

An automation system can locate a fault by using a wide variety of data and methods. DMS FLISR opts for the simplest, which is trusting the protective relays and switch controls to detect the fault. This eliminates the need for complex fault location analysis, minimizes the data necessary to locate the fault, and eliminates the need for a complex system model. When an overcurrent fault occurs on a radial distribution feeder, the relay asserts a latch that is referred to in this document as a fault latch or fault indication. The fault latch differs from a fault target in that it asserts if any of the phase 51 elements assert—meaning the fault latch asserts even when the protective device does not trip. By using this fault latch, DMS FLISR determines the fault location to the necessary accuracy by using a Boolean indication from each breaker, recloser, and switch, regardless of which protective device ultimately ended up locking out.

The following are some operational notes for DMS FLISR fault location:

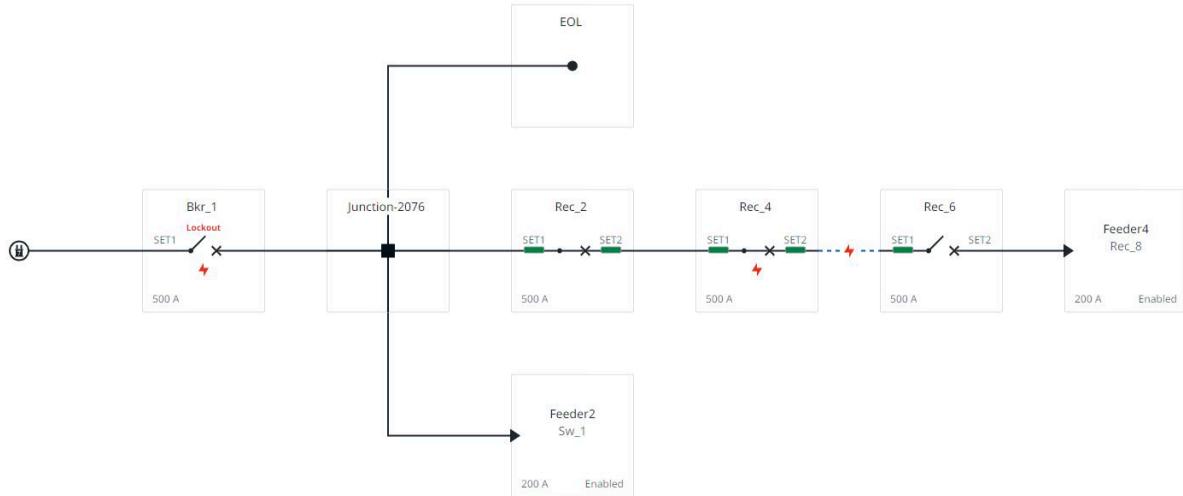
- ▶ **IMPORTANT:** When FLISR detects a fault, the total reclosing time for all field devices must be less than 5 minutes.
- ▶ **IMPORTANT:** To locate faults, FLISR relies on the fault binary point (<device>.fault), mapped in Protocol Services. This fault binary point should assert when an overcurrent pickup occurs. If the relay logic latches the fault binary point when it asserts, the latch should be cleared by the relay logic a short time after, e.g., one second. This time should be small

enough that the fault binary point does not remain asserted and affect later events. By receiving a fault binary point pickup, FLISR latches this information to its internal OvercurrentReported, which is updated based on new fault binary point pickups and cleared after the event completion or two minutes, whichever happens first.



**Figure 4.1 Fault Event Diagram**

- Event detection is driven by field devices reporting a Lockout. Once a Lockout is detected, FLISR looks for a true Fault Latch/Indication. Event detection will wait for Event Detection Delay seconds after a Lockout to confirm enough time has passed for a true Fault Latch/Indication. After a true Fault Latch/Indication, FLISR will validate all other system conditions such as open/close (52A3P), voltage, current, etc.
  - Cold load pickups or inrush can falsely trigger the pickup of phase overcurrent elements. SEL recommends that cold load pickup or inrush detection schemes be implemented to avoid falsely generating fault indications upon re-energization.
  - FLISR will not operate in response to an outage caused by an operation not accompanied by a fault latch.
  - When a permanent fault event is triggered, DMS FLISR traverses the feeder from the source outward. It will locate the fault according to the longest serial path found, regardless of whether the fault latches of intermediate devices are set or not. *Figure 4.2* illustrates this scenario. The fault was located down-line of R4 even though a miscoordination occurred (the breaker locked out) and R2 did not have a fault latch asserted.
  - FLISR does not use voltage or current measurements for fault location; rather, it uses the fault indications received from field devices to locate faults.
- FLISR *does* optionally use voltage measurements to confirm that all devices in a fault zone are de-energized—this behavior is dependent on the Enable Voltage Integrity Check setting of the feeder and the Low Voltage Threshold setting in PSM. FLISR uses current measurements to verify that it does not overload a feeder or its neighbors and to determine how much load is present on each feeder segment.



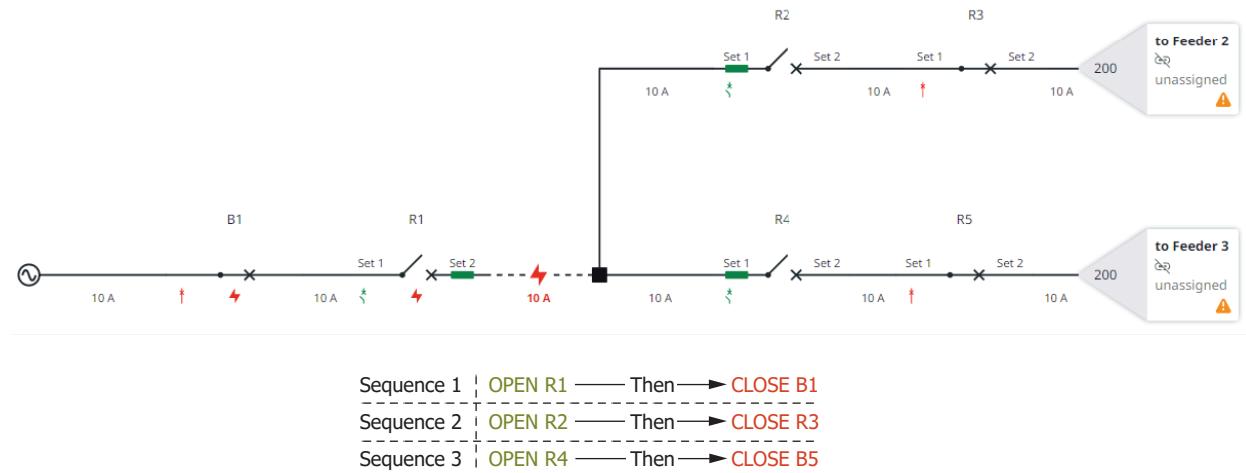
**Figure 4.2 Fault Location**

## How Isolation Works

To isolate a permanent fault, DMS FLISR identifies the breakers, reclosers, or switches that act as boundary devices, which are devices that are electrically nearest to the fault location in both up-line and down-line directions. For example, the boundary devices shown in *Figure 4.2* are Rec\_4 and Rec\_6. Once these devices are identified, DMS FLISR issues an open command simultaneously to each boundary device that is not already open.

## How Service Restoration Works

DMS FLISR minimizes restoration times by placing sequences of restoration switching operations into parallel paths according to their electrical dependencies. For example, an outage that breaks a feeder in two will likely have switching operations that must occur down-line and up-line. This is especially true in the event of a miscoordination. While restoration switching always isolates the fault before re-energizing line segments, DMS FLISR executes up-line and down-line switching in parallel with each other. This is because up-line switching is not dependent on down-line switching; they are electrically separated from each other because of the outage in between the two areas. Operating in this manner also increases the resiliency of DMS FLISR to device failure. Failure to isolate up-line does not impact its ability to continue with restoration switching down-line. *Figure 4.3* illustrates a miscoordination scenario in which the breaker has locked out. FLISR must issue a total of six controls: three to isolate the faulted zone and three to restore load. These controls are broken into three separate switching sequences. FLISR executes the controls within each sequence sequentially, but each sequence is executed in parallel with other sequences.



**Figure 4.3 Service Restoration**

DMS FLISR optimizes restoration operations by ensuring the selected switching plan meets the following criteria in the following order:

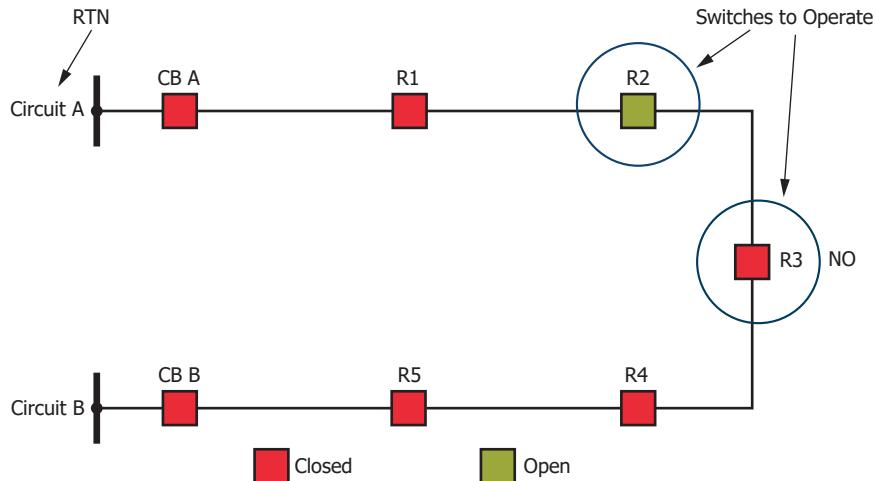
1. Maximize load restored
2. Maximize the number of energized segments
3. Minimize switching operations
4. Maximize post-restoration feeder margin on adjacent feeders

During a fault or voltage reconfiguration event, FLISR will verify that a neighbor feeder either has FLISR mode or Voltage Event mode set to automatic. If either mode is automatic, FLISR uses that neighbor feeder for part of the reconfiguration calculation of the current event.

FLISR optionally uses voltage measurements to confirm that all devices in a fault zone are de-energized prior to proceeding with isolation and restoration. FLISR does not currently use voltage measurements to qualify or prioritize restoration sources.

## Return to Normal

DMS FLISR provides Return to Normal functionality. A single control issued either over DNP3 or via the Return to Normal menu item in the user interface (see ④ in *Figure 4.5*) results in DMS FLISR issuing a control sequence to return the feeder to its normal configuration, as defined by the normal status settings configured in PSM. Return to Normal is performed in a closed transition manner that does not cause any outages and does not connect more than two feeders together at a time. If an unexpected control failure occurs and two feeders remain electrically connected together, FLISR will re-open the open point prior to the start of Return to Normal switching to leave the distribution system in an electrically safe state.



**Figure 4.4 Return to Normal**

Figure 4.4 represents the Return to Normal behavior of two tied feeders. If Return to Normal is enabled on Circuit A and not Circuit B, where Circuit A has Return to Normal being executed, Return to Normal will use Circuit B to switch devices back to normal. However, if a user tries to execute Return to Normal on Circuit B, this request would be dismissed because the Return to Normal is not enabled on Circuit B.

Return to Normal may fail because of the following reasons:

- Unexpected switch change
- Unresponsive device

#### NOTE

Feeders are only connected together during the period of time when the existing open point is closed and until the normal open point is opened.

#### NOTE

During Return to Normal, FLISR does not validate correct phasing between two feeders. Local devices will need to validate phasing.

## Voltage Events

DMS FLISR supports handling voltage events as part of the detection, isolation, and reconfiguration functionality. Voltage events are separated into three categories: Open Phase, Loss-of-Source, and Instrumentation Error.

An Open Phase event is activated when DMS FLISR detects one or more phases open between two measurement devices (typically PTs). FLISR will initiate a reconfiguration if this is enabled.

A Loss-of-Source event is activated when DMS FLISR detects voltage issues on all voltage measurements fed by the local source. FLISR will take action if this is enabled.

An instrumentation error is activated when DMS FLISR senses that one or more voltage measuring devices are in an error state. FLISR does not perform any reconfiguration but does create a report.

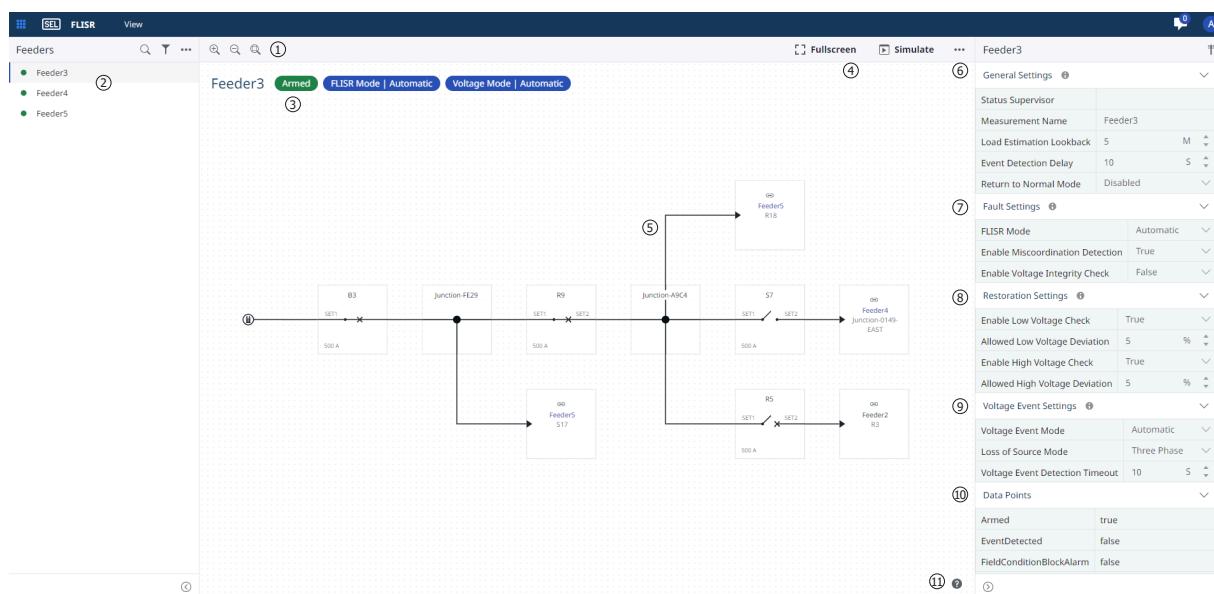
All of these events can occur without a protection device sensing a lockout and fault.

## FLISR Operations

DMS FLISR is designed to be operated either through its built-in web-based graphical interface or through a DNP3 server connection. *Appendix B: FLISR Data Mapping Tables* provides the data points available for placement into a DNP server map. This section covers how to operate the FLISR web-based graphical interface, which is an intuitive zero-software approach to direct control system operation.

### Web-Based User Interface

The DMS FLISR web-based user interface shows the real-time status of FLISR and allows you to browse from feeder to feeder through the intuitive feeder panel and view device details with a single click.



**Figure 4.5 DMS FLISR User Interface**

- ① **Canvas Zoom and Fit Controls.** Simplifies zooming in and out of the feeder canvas.
- ② **Commissioning Panel.** Lists all feeders on the Blueframe instance. Selecting a feeder from this list opens its feeder canvas, enabling you to view real-time field data and FLISR status. An icon beside each feeder indicates the state of the feeder. A green circle indicates the feeder is armed and ready. A red lightning bolt indicates the feeder has detected a permanent fault. A yellow caution symbol indicates the feeder is blocking functionality because of a field device problem, such as hot-line tag, remote control disabled, or communications failure.
- ③ **FLISR Status Display.** Uses chips, which are color-coded labels that use plain text descriptions, to convey its operational status. This area displays arm/disarm state of FLISR, its event status, and its reconfiguration status.  
Available Chips are:

- |            |                          |                               |                                 |
|------------|--------------------------|-------------------------------|---------------------------------|
| ► Armed    | ► Fault                  | ► FLISR Mode   Advisory       | ► Voltage Mode   Isolation Only |
| ► Disarmed | ► Event                  | ► FLISR Mode   Isolation Only | ► Reconfiguring                 |
| ► Blocked  | ► Miscoordination        | ► Voltage Mode   Automatic    | ► Reconfiguration Complete      |
| ► Loop     | ► FLISR Mode   Automatic | ► Voltage Mode   Advisory     | ► Reconfiguration Failed        |

**④ FLISR Controls.** Enables you to arm and disarm the feeder, request a fully automated Return to Normal operation, and more. The following details the available controls:

1. Fullscreen. Maximizes the feeder canvas to the full screen view.
2. Simulate. Launches a simulation that uses a copy of the open feeder in a new browser tab. Doing so from a commissioned feeder does not affect the commissioned feeder; it remains operational and is not affected by the simulation.
3. Arm/Disarm Feeder. Arms or disarms FLISR. When armed, FLISR can detect events. When disarmed, FLISR remains idle and takes no action.
4. Return to Normal. Requests a fully automated Return to Normal switching operation from FLISR.
5. Target Reset. Resets all active operational indications.

**⑤ Feeder Canvas.** Displays the feeder one-line diagram, including device state. To view data for a specific switching device, select the switching device on the feeder canvas to view the data in the Device Details pane.

**⑥ General Settings.** Defines the operations settings required by FLISR.

**⑦ Fault Settings.** Defines what events are captured within FLISR.

**⑧ Restoration Settings.** Defines operation parameters that help FLISR reconfigure after certain events.

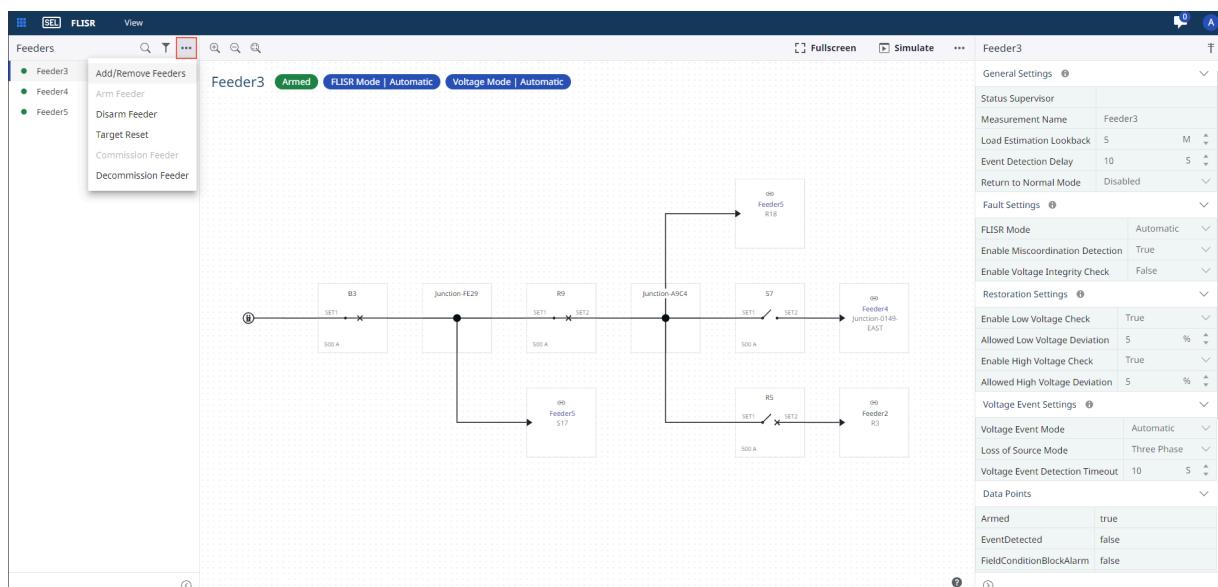
**⑨ Voltage Event Settings.** Defines the operational mode for voltage events when the feeder is commissioned.

**⑩ Data Points.** Provides a quick reference for verifying that data points are mapped to the FLISR system.

**⑪ Help Legend.** Provides descriptions for indicators and symbols used by FLISR and the simulator.

## Adding a Feeder to FLISR

Each canvas allows for feeders in PSM to be displayed in FLISR by selecting the horizontal ellipsis in the commissioning panel, as shown in *Figure 4.6*. FLISR will leverage all imported and manually created customer models in PSM. FLISR scans the PSM for the most-upstream protective device (breaker, recloser, etc.) in the models, which in turn may bring in multiple substation assets.



**Figure 4.6 Feeder Tools**

## FLISR Feeder Settings

Each FLISR feeder has its own settings, as described in *Table 4.1*. These settings can be configured by selecting a feeder canvas and using the FLISR Properties panel. See *Table 3.4* to determine the required FLISR properties set in PSM.

**Table 4.1 FLISR Feeder Settings**

	<b>Setting Name</b>	<b>Description</b>
General Settings	Status Supervisor	When provided, this feeder subscribes to status supervision signals in a DNP Client connection by the same name.
	Event Detection Delay	The time delay for which the feeder will wait following an event trigger before evaluating data and executing a solution. This time is also the amount of time before a loop flag is removed. Acceptable values are integers from 0 seconds to 60 seconds.
	Return to Normal	Defines the operational mode of Return to Normal when the feeder is commissioned. Disabled: Users will not be able to issue a Return to Normal command. Closed Transition: Return to Normal will be enabled using the closed transition algorithm. Closed Transition Advisory: A report will be generated outlining the proposed switching operations, but no actions will be taken.
	Load Estimation Lookback	The maximum amount of time FLISR will review the data for load estimation calculations to validate fault calculations. This time should only be adjusted to account for networks that have large communication delays, such as networks where data are only refreshed every 15 minutes. SEL recommends the new setting being 5 to 6 times the protocol integrity pull. The default value is 5 minutes.
<b>NOTE</b> If FLISR does not read at least five measurements, it uses the most recent measurement(s) from the lookback and enables a warning message. This warning is displayed in the Reports, via the diagnostic section.		
Fault Settings	FLISR Mode	Defines the FLISR operational mode when the feeder is commissioned. Disabled: The system will not detect fault events. Automatic: Detected faults will be isolated and surrounding areas will be restored where possible. Isolation Only: Detected faults will be isolated, but no restoration steps will be taken. Advisory: A report will be generated for each fault event detected, but no actions will be taken.
	Enable Miscoordination Detection	Selects whether this feeder will detect and correct miscoordinations. FLISR Mode must be set to Automatic. The default value is True.
	Enable Voltage Integrity Check	<b>NOTE</b> When Enable Miscoordination Detection is disabled, FLISR will still analyze the feeder for miscoordination, but it will not react to it. In the event engine, if the miscoordinated section of a feeder is considered to be available, FLISR will not close in any corresponding devices and could re-energize the line.
Restoration Settings	Enable Low Voltage Check	Determines if feeder voltages should be used to validate a fault event. If enabled, all voltage measurements in the zone de-energized by the fault must be below the low voltage threshold in order for FLISR to operate. The default value is True.
	Allowed Low Voltage Deviation	When enabled, the system will use low voltage deviation to determine if this feeder can provide power to a neighbor. <sup>a</sup>
	Enable High Voltage Check	Percentage of deviation from nominal voltage at the open point below which the feeder will not be used to restore power to a neighbor. Acceptable values are integers from 1 percent to 15 percent. The default value is 5 percent.

	<b>Setting Name</b>	<b>Description</b>
	Allowed High Voltage Deviation	Percentage of deviation from nominal voltage at the open point above which the feeder will not be used to restore power to a neighbor. Acceptable values are integers from 1 percent to 15 percent. The default value is 5 percent.
Voltage Event Settings	Voltage Event Mode	Defines the operational mode for voltage events when the feeder is commissioned. Disabled: The system will not respond to detected voltage events. Automatic: The system will automatically attempt to isolate voltage events and restore power to the surrounding areas where possible. Advisory: A report will be generated for each voltage event detected, but no actions will be taken. Isolation-Only: Detected voltage events will be isolated, but no restoration steps will be taken.
	Voltage Event Detection Timeout	Time, in seconds, during which a voltage must remain low for the event to be detected and for FLISR to start assessing if reconfiguration conditions exist. Acceptable values are integers from 0 seconds to 60 seconds.
	Loss-of-Source Mode	Defines how FLISR reacts to Loss-of-Source voltage events. Any-Phase: FLISR will look for any single-, two-, or three-phase to report a Loss-of-Source before reacting. Three-Phase: FLISR will react to any three-phase Loss-of-Source event, reconfiguring and creating a report. If a single- or two-phase Loss-of-Source event occurs, FLISR will assert the LossOfSource SCADA point but will not reconfigure or create a report. FLISR uses the Voltage Event Detection Timeout duration to look for all single- and three-phase voltage events. The default value is Any-Phase.

<sup>a</sup> If High- and Low-Voltage Checks are enabled and the PTs are not mapped, the device is out of service, or a communications error occurs, FLISR will treat it as a failed voltage check and skip the device.

*Table 4.2* shows the subset of Breaker, Recloser, and Switch node settings created in PSM and used by FLISR. FLISR does not account for properties in End-of-Line, Junction, or Line Segment nodes.

**Table 4.2 FLISR-Specific Settings Established in PSM Settings**

<b>Setting Name</b>	<b>Description</b>
Name	Device name (e.g., Breaker 4, Recloser 4, Switch 4). This may only contain printable ASCII characters.
Left PT	Select which three-phase voltage set is oriented to the left side of the node as drawn on the canvas. The options are Set1, Set2, and None. The default value is None.
Right PT	Select which three-phase voltage set is oriented to the right side of the node as drawn on the canvas. The options are Set1, Set2, and None. The default value is None.
DMS Capacity	Rating, in percent, of Current Rating that FLISR can use as a maximum permissible value when evaluating restoration solutions. The default value is 80 percent.
A-Phase Normally Open	The normal state of the breaker's A-Phase that is used by FLISR. The options are False and True. The default value is False.
B-Phase Normally Open	The normal state of the breaker's B-Phase that is used by FLISR. The options are False and True. The default value is False.
C-Phase Normally Open	The normal state of the breaker's C-Phase that is used by FLISR. The options are False and True. The default value is False.
Current Scalar	The value by which FLISR must scale incoming current data points in order to get amperes. (For example, if the incoming current data points are in kiloamperes, the scalar should be set to 1000 to convert to amperes.)
Voltage Scalar	The value by which FLISR must scale incoming voltage data points in order to get volts. (For example, if the incoming voltage data points are in kilovolts, the scalar should be set to 1000 to convert to volts.)
Is Manual	An indication (true or false) of whether an asset is manually operated. <sup>a</sup>
Has Status	An indication (true or false) of whether an asset has statuses in the data map. <sup>a</sup>

Setting Name	Description
Has Fault Indication	An indication (true or false) of whether an asset has fault indication (not lockout) that will be in the data map. <sup>a</sup>
Has Currents	An indication (true or false) of whether an asset has current measurements that will be in the data map. <sup>a</sup>

<sup>a</sup>These settings are only required for Switches, see Table 3.14 and Table 3.27. FLISR will override any PSM configurations for Breakers and Reclosers and apply FLISR defaults to the configuration.

Each Node within FLISR that has SCADA values (Measurement Name) also supports the use of data concentrators. Concentrator is available for breakers, reclosers, and switches, as shown in *Table 4.3*.

**Table 4.3 FLISR-Specific Node Settings**

Setting Name	Description
Concentrator	<p>Subscribes to the concentrator signals in a DNP Client connection if provided.</p> <p><b>NOTE</b> Measurement name is set in PSM and FLISR defaults that to the node type. Concentrator is used when a data concentrator is used to support data aggregation between a field device and SEL DMS FLISR.</p>

## Switch Operation

FLISR treats PSM switches dynamically based on how the device is modeled. The PSM properties Is Manual, Has Status, Has Fault Indication, and Has Currents define how FLISR leverages the device in its operation (these are not required for FLISR operation, see *Table 3.27*). These settings are defined in *Feeder Canvas Nodes and Settings on page 228*. When a switch is configured in PSM to have "Have Status" as False, FLISR treats the device as Inhibited because FLISR cannot verify the successful operation of a device without a status update.

FLISR does not support looped conditions where the normally open point is closed and both feeders are tied together. When looped conditions occur, FLISR is automatically disabled. When a device is opened, breaking the loop, FLISR will exit the looped condition. If FLISR is in looped condition (i.e., a loop has been detected, disabling FLISR) and a device opens, FLISR will wait for the Event Detection delay (as many as 60 seconds) before validating if the Fault Latch is true. If the Fault Latch is true, FLISR will *not* exit the looped condition because it assumes the device is actively reclosing. Once a lockout is detected from the actively reclosing device, FLISR initiates standard loop exit processes. If a Fault Latch is not detected during the Event Detection delay, FLISR will use standard loop exiting processes.

## Operational Impacts of Switch Configurations

- When "Has Fault Indication" or "Has Currents" are configured as False, FLISR will not search for the corresponding data within the device data map and will perform its analysis without these data.
- When "Is Manual" is set to True, FLISR will recognize the status of the switch as open or closed, but will not consider the switch in any control decision, because it cannot be remotely operated.

- When "Can Load Make" is set to True, FLISR will allow reconfiguration decisions that close the switch into load.
- When "Can Load Break" is set to True, FLISR will allow reconfiguration decisions that open this switch under load.

## Voltage Operation

When PTs are set on an applicable device in PSM, FLISR expects data points to be mapped (see the example in *Table B.1* for VASet1).

As mentioned in FLISR Fundamentals (see *Voltage Events on page 243*), the Event Types under Voltage Operation are:

- Open Phase
- Loss of Source
- Instrumentation Error

Applicable settings are referenced in *Table 4.2* and *Figure 4.7*. When restoring a feeder, FLISR validates whether the reconfiguration violates the Allowed Low Voltage Deviation or Allowed High Voltage Deviation if the Enable Low Voltage Check or Enable High Voltage Check settings, respectively, are set to True. If no deviation is expected, then FLISR proceeds with reconfiguration. Should a violation exist, FLISR will exclude any connection that is in violation during reconfiguration.

You can choose from four Voltage Event modes:

- **Disabled.** The system will not respond to detected voltage events. In this mode, events will not be captured for future analysis.
- **Automatic.** The system will automatically attempt to isolate voltage events and restore power to the surrounding areas where possible.
- **Advisory.** A report will be generated for each voltage event detected, but no actions will be taken.
- **Isolation-Only.** Detected voltage events will be isolated, but no restoration steps will be taken.

Each voltage capability within FLISR requires working voltage inputs. As an example, Open Phase FLISR isolates with the closest upstream device that is operable and has accurate voltage measurements. This could potentially expand the isolation zone if multiple devices are out of service and/or have poor data or unmapped PTs.

Restoration Settings ⓘ		
Enable Low Voltage Check	True	▼
Allowed Low Voltage Deviation	5	% ▲ ▼
Enable High Voltage Check	True	▼
Allowed High Voltage Deviation	5	% ▲ ▼
Voltage Event Settings ⓘ		
Voltage Event Mode	Automatic	▼
Loss of Source Mode	Three Phase	▼
Voltage Event Detection Timeout	10	S ▲ ▼

Figure 4.7 Voltage Operation

## FLISR and Return to Normal Operational Modes

Each feeder canvas can be commissioned with its own mode settings. Mode settings are available for both FLISR and Voltage Event modes. The following are available FLISR modes:

- ▶ **Automatic.** The feeder attempts to perform both isolation and reconfiguration using available feeders when an event is detected.
- ▶ **Isolation Only.** The feeder performs isolation only when an event is detected and provides a supplemental advisory report that includes a recommended switching sequence and adjacent circuit availability information.
- ▶ **Advisory.** The feeder does not perform any automatic action, but generates an advisory report that includes recommended isolation and reconfiguration control sequences and adjacent circuit availability information.
- ▶ **Disabled.** FLISR does not perform any automatic action. In this mode, events will not be captured for future analysis.

### NOTE

A feeder in Isolation Only or Advisory mode is unable to participate in restoration that may be necessary to minimize an outage on an adjacent feeder. However, if a feeder in Isolation Only or Advisory mode is feeding an adjacent feeder in Automatic mode in such a way that the open point is a member of the adjacent feeder, the open point may be operated as part of a restoration control sequence. This same behavior occurs for Return to Normal.

### NOTE

A device that was closed during a FLISR reconfiguration is reverted during Return To Normal. It will show as an open step in the activity report.

The following are available Return to Normal modes:

- **Closed Transition.** The feeder automatically executes a closed-transition return to normal control sequence when a Return to Normal command is received from a user.

#### NOTE

A closed transition temporarily ties two feeders together in order to avoid a moving outage. Feeders are only tied together for the length of time it takes to close one open point and open another. This time is primarily dependent on the communications polling intervals in use.

- **Closed Transition Advisory.** The feeder does not automatically perform any control sequence execution and generates an advisory report with recommended control sequences.
- **Disabled.** The feeder does not react to any Return to Normal controls received from the user via the web-based user interface or a protocol connection.

The following are scenarios that disable Return to Normal:

- If a feeder in PSM has phasing set to NONE, a loop can be designed and Return to Normal will not operate due to the potential loop.
- If a neighbor feeder is currently de-energized due to it being blocked, disarmed, actively being reconfigured, not enabled, or not found, Return to Normal will not operate.
- If a neighbor feeder has a hot-line tag currently active, FLISR will see that feeder as blocked, and Return to Normal will not operate.

## Arming, Disarming, and Blocking

You can arm and disarm DMS FLISR on a per-feeder basis by using either the web-based user interface or DNP3. The only way to arm a disarmed circuit is to issue an arm command (DMS FLISR will never arm itself automatically).

FLISR automatically blocks itself on a per-feeder basis in reaction to data received from breakers, reclosers, and switches, as well as feeder-level blocking signals. FLISR operations are blocked until the indication is removed on all feeder switching devices. The following are qualifying indications for a FLISR block:

- Hot-line tag
- Remote control disabled
- Loss of communication
- Feeder-level FLISR block indications
- Device-level FLISR block indications

A feeder that is disarmed or blocked does not perform isolation or restoration switching and is not available for use by other feeders requiring restoration support.

## Device-Level Out of Service and Control Inhibit

If a configured device is unable to communicate or, if for any reason, must be worked around and not directly used for FLISR operations, the following options are available:

- ▶ **Control Inhibit.** When applied to a switching device, DMS FLISR uses all data received from the switching device but will not operate the device as part of isolation or restoration.
- ▶ **Out of Service Open.** When applied to a switching device, DMS FLISR ignores all data received by the device, treats it as an electrical open point on the line, and does not operate the device as part of isolation or restoration.
- ▶ **Out of Service Closed.** When applied to a switching device, DMS FLISR ignores all data received by the device, treats it as an electrical closed point on the line, and does not operate the device as part of isolation or restoration.

### NOTE

Return to Normal will operate on feeders with devices in states such as Out of Service Open, Out of Service Closed, and Control Inhibit as long as those devices are in their as-built (Power System Model) state. However, if devices within a feeder are set to Out of Service Open or Out of Service Closed and that does not match the devices as-built Open/Close state, Return to Normal will NOT operate. At the same time, if Return to Normal needs to operate a device with Control Inhibit enabled, Return to Normal will NOT operate.

For example, if the device's as-built state is closed and its as-operated state is Out of Service Open, RTN will NOT operate. Additionally, if a device is reconfigured to now have an as-operated state of open and then set to Out of Service Open, Return to Normal will NOT operate since the device still does not match the closed as-built state.

## On-Demand Simulation

Feeder simulation is tightly integrated into DMS FLISR. Simulation is used to validate FLISR settings, to gain initial and recurring familiarity with FLISR operations, and to answer any "what if" questions that arise with direct, easy-to-obtain results. You can launch the DMS FLISR simulator from any open feeder canvas in FLISR by selecting **Simulate**, as shown in *Figure 4.9*.

### FLISR Simulation

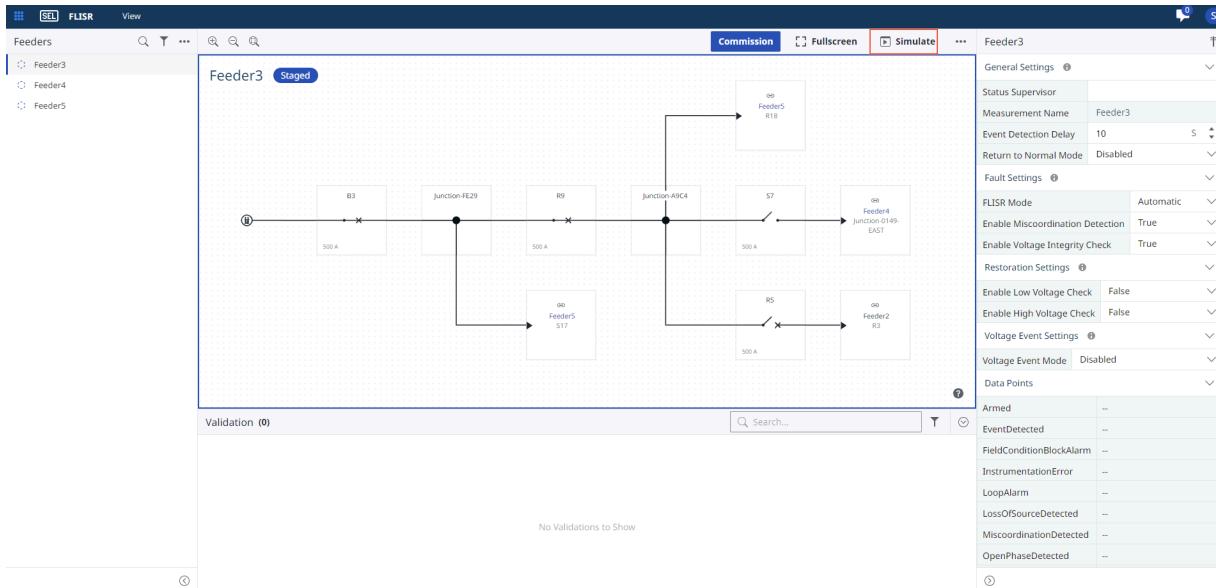
This is a simulation. No action taken here will impact your live system. Remember to ▶ Arm your simulator to have FLISR react to simulated events.

**Dismiss**

**Figure 4.8** FLISR Simulation View

## ⚠️ IMPORTANT

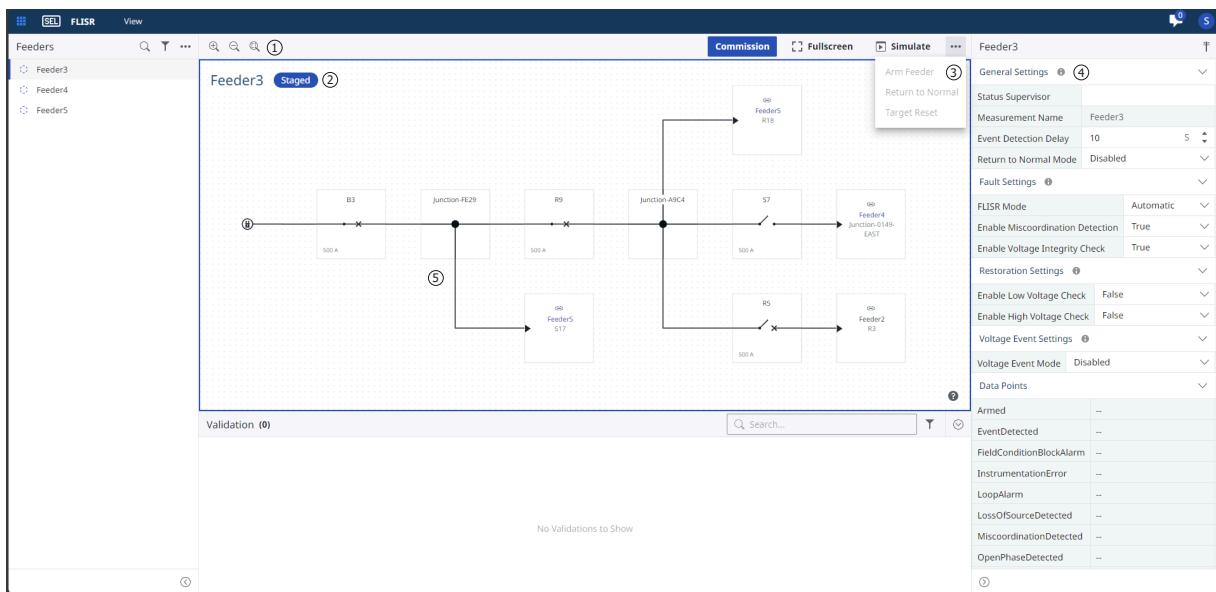
When using the FLISR web-based simulator or another system (like a distribution automation controller (DAC)) to mimic field data in a Quality Assurance/Quality Control (QA/QC) environment, allow the Event chip to deassert and disappear from the canvas display before resetting and running the next event. When FLISR begins processing an event, it enables the Event chip to indicate that it has begun processing the fault. The deassertion of the Event chip indicates that FLISR has completed the analysis.



**Figure 4.9 Simulating a Feeder in FLISR**

The Simulate button opens a new browser tab that contains a dedicated simulation ready for immediate use.

## Simulator Controls and Interaction



**Figure 4.10 Simulated Feeder User Interface**

① **Canvas Zoom and Fit Controls.** Simplifies zooming in and out of the feeder canvas.

② **FLISR Status Display.** Displays chips, which are color-coded labels that use plain text descriptions, to convey its operational status. Use this area to determine the arm/disarm state, event status, and reconfiguration status of FLISR. Available chips are:

- |            |                          |                               |                                 |
|------------|--------------------------|-------------------------------|---------------------------------|
| ► Armed    | ► Fault                  | ► FLISR Mode   Advisory       | ► Voltage Mode   Isolation Only |
| ► Disarmed | ► Event                  | ► FLISR Mode   Isolation Only | ► Reconfiguring                 |
| ► Blocked  | ► Miscoordination        | ► Voltage Mode   Automatic    | ► Reconfiguration Complete      |
| ► Loop     | ► FLISR Mode   Automatic | ► Voltage Mode   Advisory     | ► Reconfiguration Failed        |

③ **Simulation and FLISR Controls.** Controls both the FLISR instance currently running in the simulator, as well as the simulator itself. The following lists the control functionality:

1. Arm/Disarm. Arms or disarms FLISR. When armed, FLISR can detect events. When disarmed, FLISR remains idle and takes no action.
2. Reset. Resets the simulation back to its initial conditions. Loads and device status data return to their initial values and all fault conditions are reset.
3. Fullscreen. Places the simulation view into full screen mode.
4. Clear Fault Latches. Clears any asserted fault indications being simulated on switching devices.
5. Return to Normal. Requests fully automated Return to Normal switching from FLISR.
6. Target Reset. Resets all FLISR status indications.
7. Populate Load History. Establishes the active current readings as the historical values for the simulator during the next simulated event.

④ **FLISR Feeder Properties.** Displays most recent property configurations for FLISR in Simulation mode.

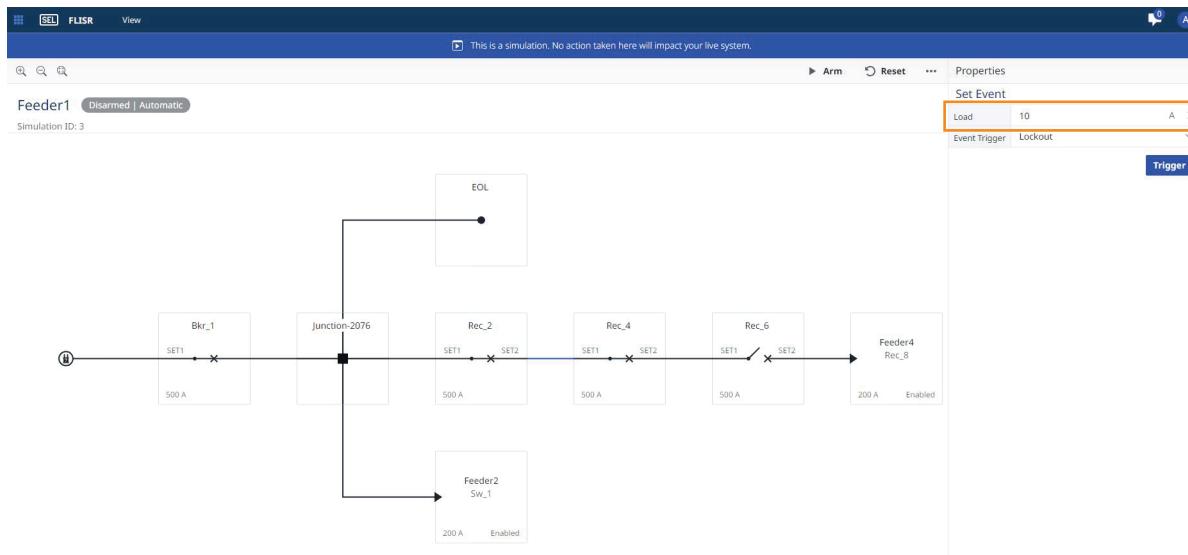
⑤ **Interactive Canvas.** Displays the device data and status of a switching device in the Device Details pane on the right side of the interface. Select a line segment to see line controls in the detail pane.

## How to Simulate a Permanent Fault

### NOTE

If you need FLISR to operate, ensure FLISR is armed prior to proceeding with this step.

Step 1. Configure line loading and the adjacent feeder margin in the Device Details pane. All line segments default to 10 A of load, as shown in *Figure 4.11*. You can adjust these loads by selecting the line segment and changing the loading (in A). All adjacent feeder connections default to 200 A of availability. You can adjust this availability by selecting the adjacent feeder connection and changing the margin (in A).



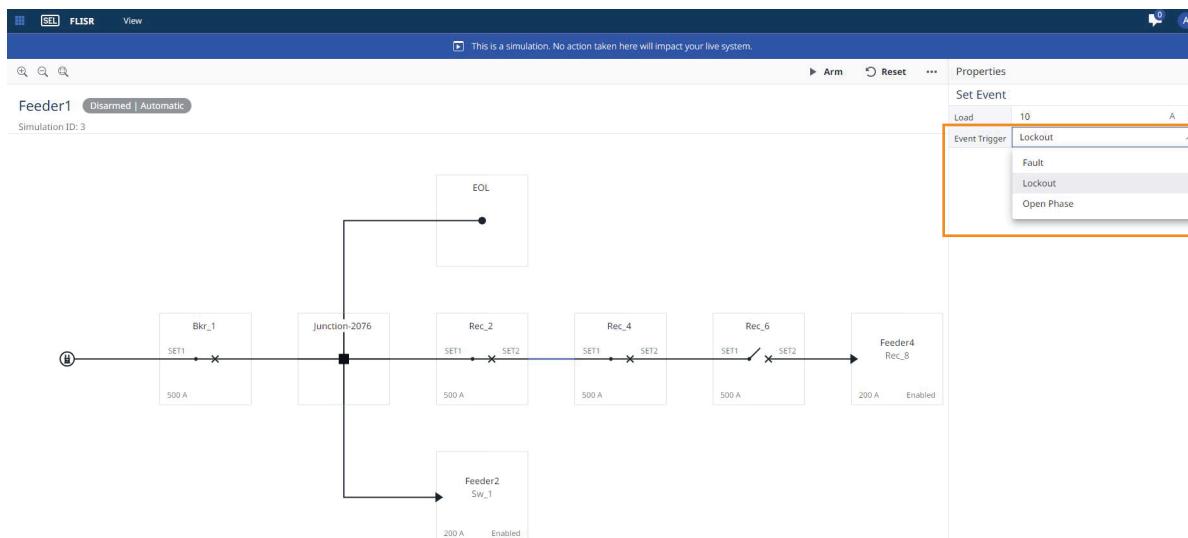
**Figure 4.11 Simulated Event Entry**

Step 2. Apply a Lockout event to the line segment by selecting the line segment where the simulated permanent fault will be located, and change the Event Trigger dropdown menu to **Lockout**, as shown in *Figure 4.12*. This causes the simulator to apply the fault indications to every up-line device and drive the nearest breaker or recloser to lockout.

**Fault.** Simulates a fault without lockout.

**Lockout.** Simulates full lockout (FLISR event).

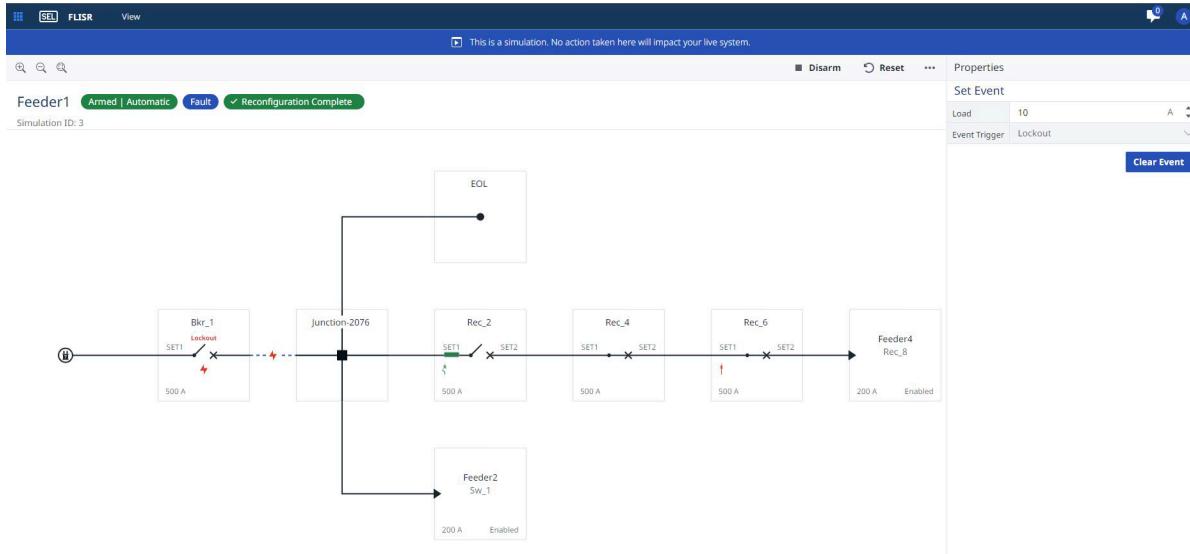
**Open Phase.** Simulates open phase (voltage FLISR event).



**Figure 4.12 Simulated Event Trigger**

Step 3. Review FLISR operational status, event detection status, and controls issued to observe the actions of FLISR post-fault. The status chips along the top of the feeder canvas appear if FLISR indicated that a fault occurred and whether FLISR successfully

(or unsuccessfully) completed its reconfiguration plan. The feeder one-line diagram itself displays the location of the fault, as well as icons with tooltips indicating to which switching devices FLISR issued open and close controls, as shown in *Figure 4.13*.



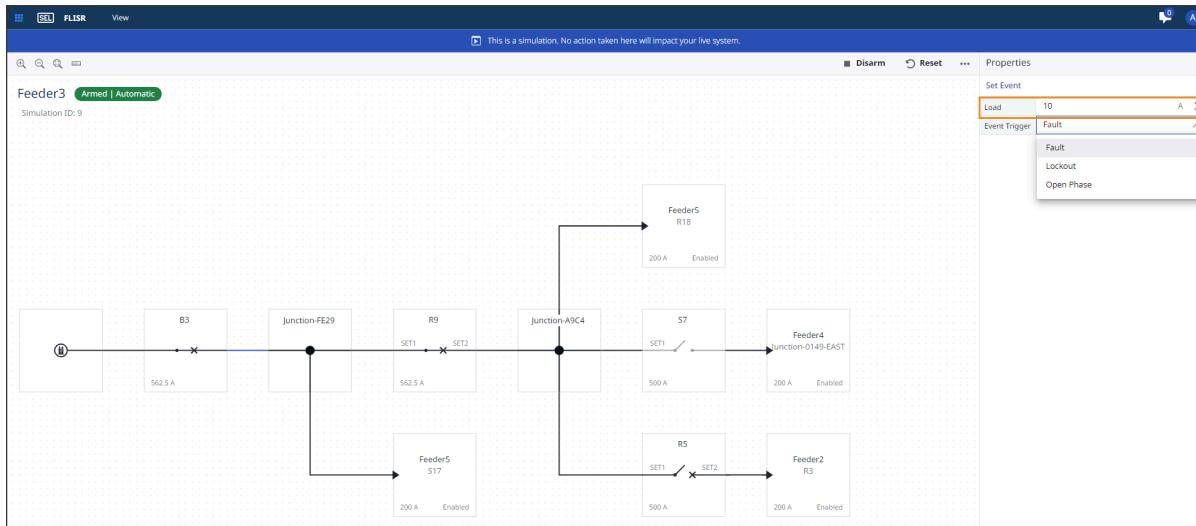
**Figure 4.13 Simulator Screen**

## How to Simulate a Miscoordination

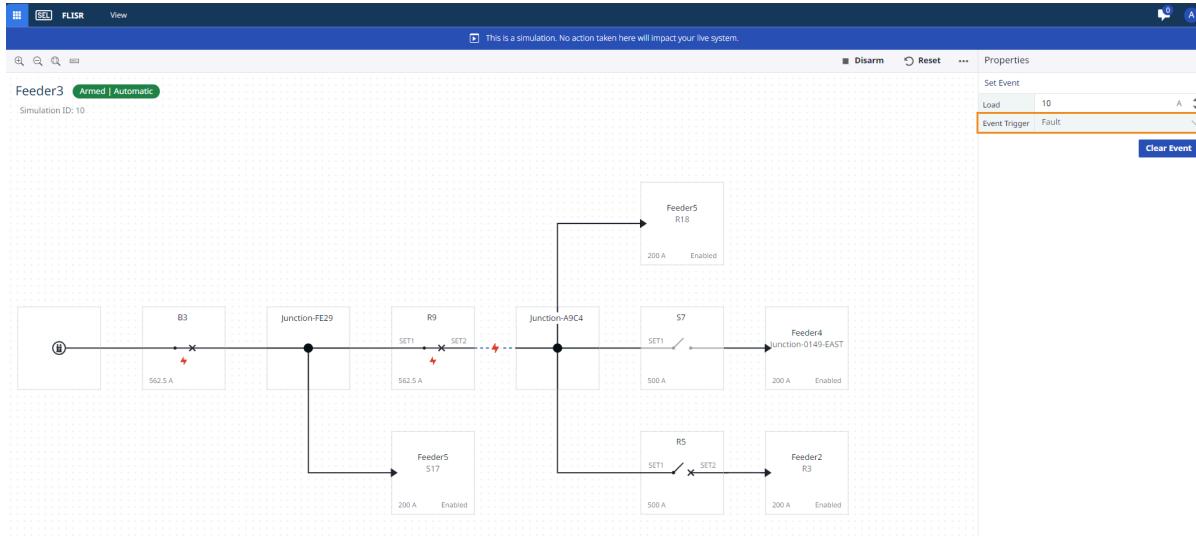
### NOTE

If you need FLISR to operate, ensure FLISR is armed prior to proceeding with this step.

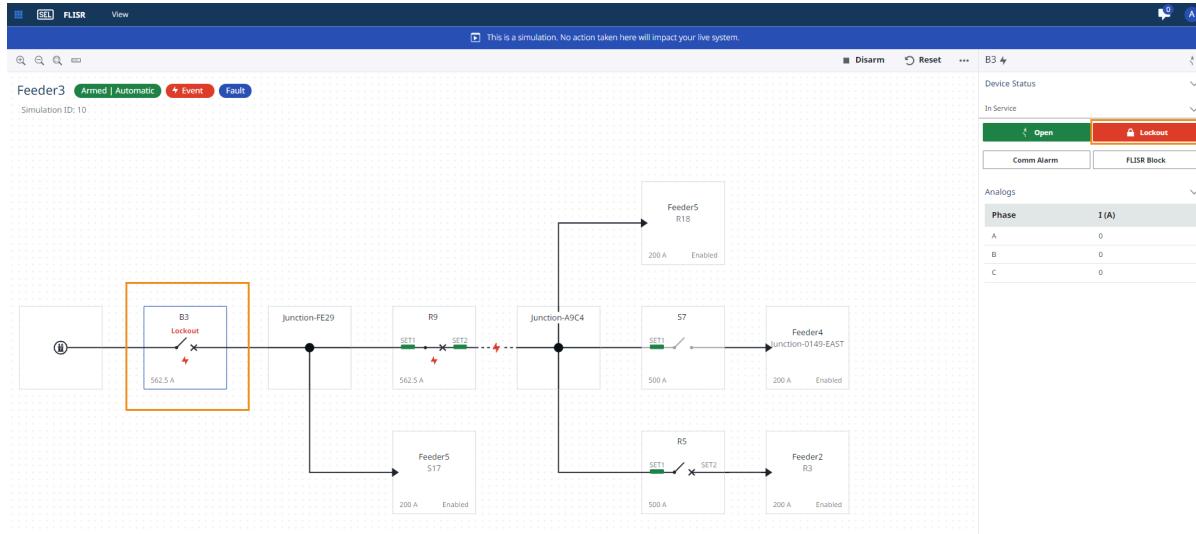
- Step 1. Configure line loading and adjacent feeder margin in the Device Details pane. All line segments default to 10 A of load. You can adjust these loads by selecting the line segment and changing the loading (in A). All adjacent feeder connections default to 200 A of availability. You can adjust this availability by selecting the adjacent feeder connection and changing the margin (in A).



Step 2. Apply a Fault event to the line segment by selecting the line segment where the simulated permanent fault will be located, and change the Event Trigger dropdown menu to **Fault**. This causes the simulator to apply fault indications to every up-line device but no protection action will be simulated.

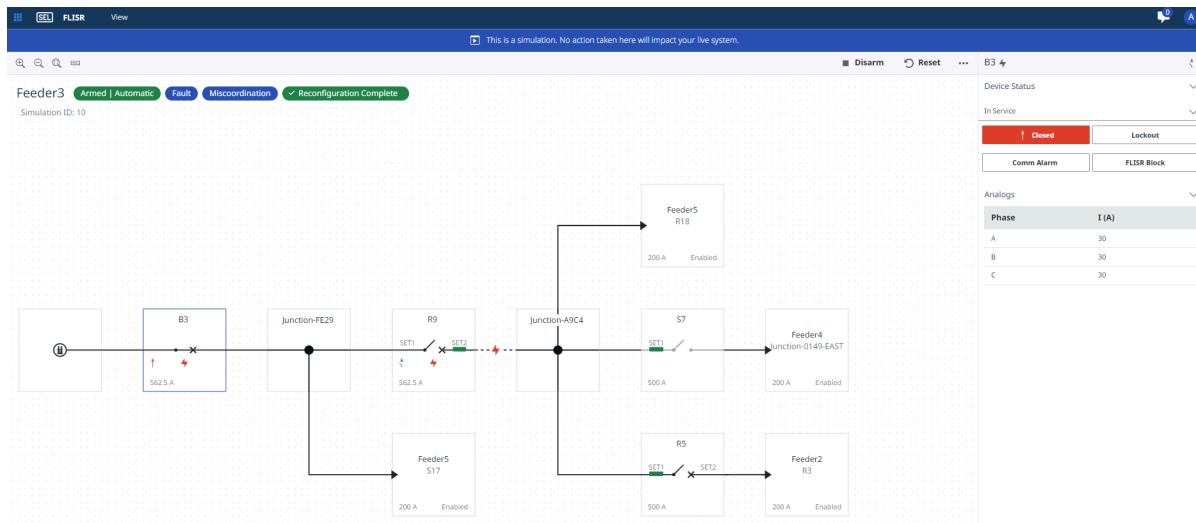


Step 3. Select the miscoordinating device (or devices) and select **Lockout** in the Device Details pane.



Step 4. Review FLISR operational status, event detection status, and controls issued to observe the actions of FLISR post-fault. The status chips along the top of the feeder canvas appear if FLISR indicated that a fault occurred or miscoordination and

whether FLISR successfully (or unsuccessfully) completed its reconfiguration plan. The feeder one-line diagram itself displays the location of the fault, as well as icons with tooltips indicating to which switching devices FLISR issued open and close controls.



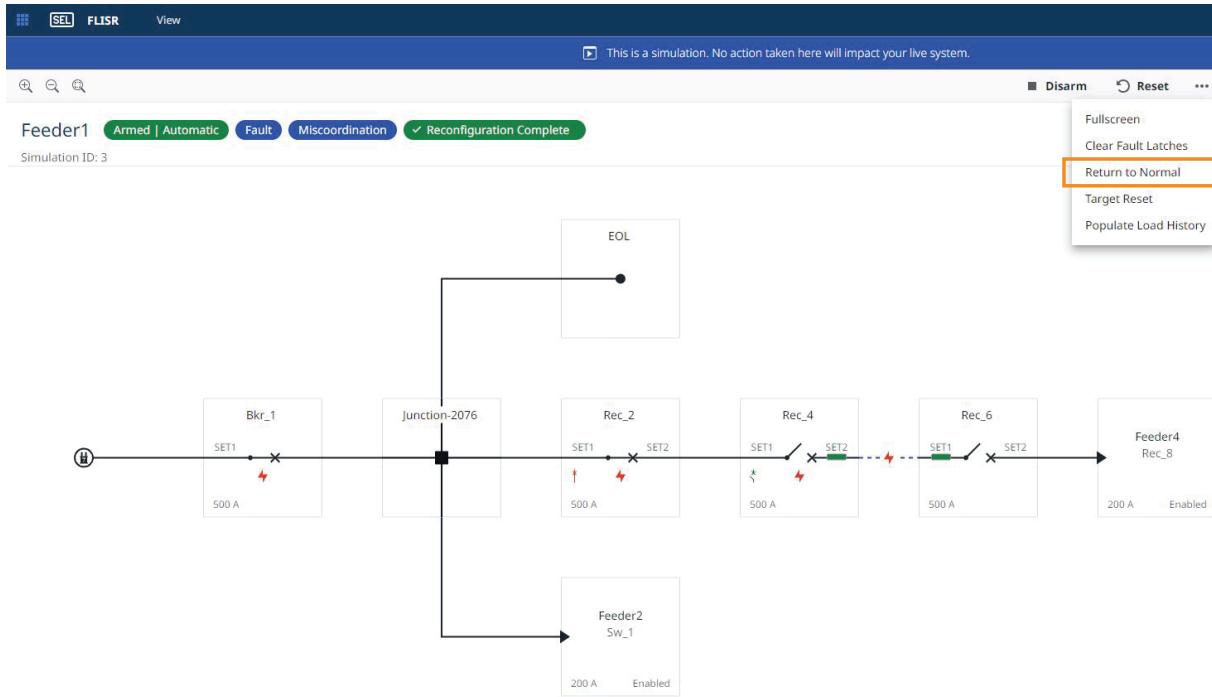
## How to Test Return to Normal

Step 1. Remove the fault event (or events) by selecting the line segments with existing fault conditions and removing them by selecting the **Clear Event** button on the Device Details pane. Alternatively, you can leave the fault conditions and observe that FLISR cancels its Return to Normal switching when it encounters a permanent fault.

**⚠ CAUTION**

Selecting Reset will clear the canvas and all simulator settings will be lost.

Step 2. Select **Return to Normal** in the simulation controls dropdown menu.



## Reports

DMS FLISR generates a report for every event. These reports are accessible via the View menu at the top of the FLISR user interface and provide detailed information about how FLISR responded to an event. Reports are generated for the following events:

- ▶ Permanent faults
- ▶ Return to Normal
- ▶ Commissioning

When a permanent fault occurs, FLISR creates a response report that includes an event summary, a feeder diagram with an indicated fault location, load recovery information, and a switching plan for isolation and service restoration. If the feeder is in Automatic mode, the switching plan includes an indication of success or failure for each step. If the feeder is in Isolation\_Only mode, the plan includes this information for the isolation steps only and also provides a suggested restoration plan for manual execution. If the feeder is in Advisory mode, the report contains recommended isolation and restoration plans for manual execution.

**This page intentionally left blank**

---

---

## S E C T I O N   5

---

# Reports

## Introduction

---

When configuring, maintaining, and operating FLISR, detailed reporting is critical. FLISR automatically generates reports for several different actions and events. Some reports include details about changes made to the FLISR configuration, and other reports include detailed information about an action FLISR took in response to a permanent fault or Return to Normal command. This section describes the types of reports available, their content, and how to access them.



## Response Reports

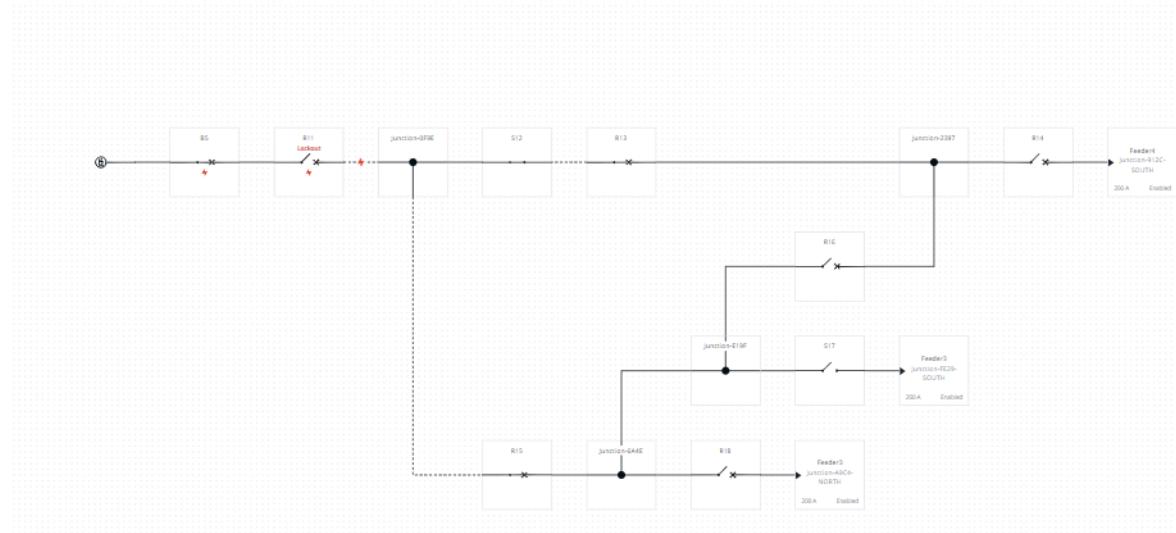
---

FLISR generates a response report every time an event is detected. This report contains detailed information about the event and any mitigation steps taken by FLISR. These reports are designed to be easily read and interpreted and include before and after diagrams that mirror the user interface. The following sections describe operations report content in detail.

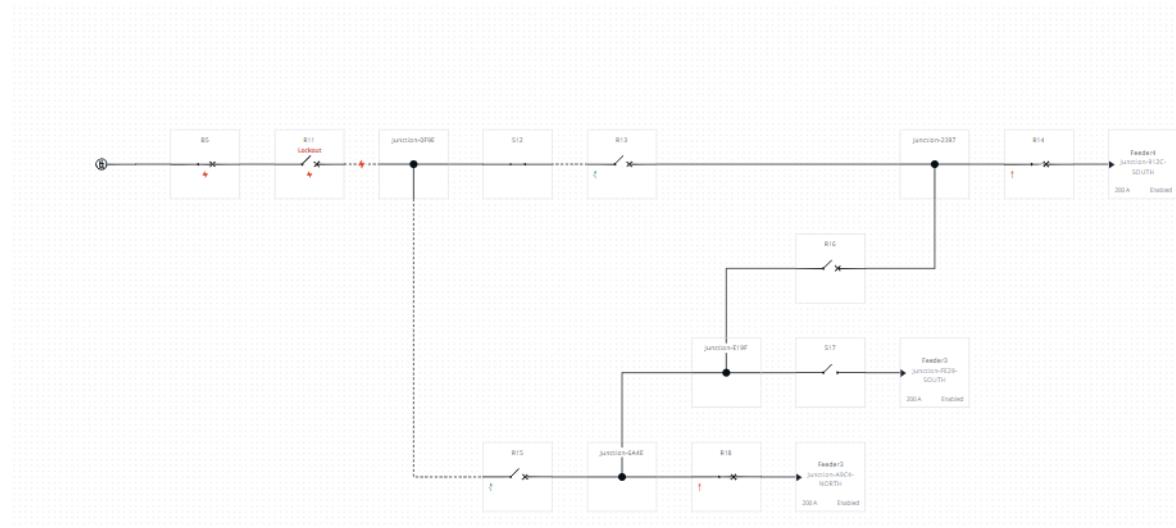
## Feeder State Diagrams

Visualize the feeder state at the moment the event was detected and once the event was complete, including Voltage Event and FLISR control operations.

### Feeder State at Time of Event



### Feeder State After Reconfiguration



## Fault Summary

The fault summary report contains fault-specific information such as customer metadata, event type, and event result. You can select an event to see additional details about that event.

The following Event Types will generate a fault summary report:

- ▶ Fault
- ▶ Voltage Event (Loss-of-Source, Open Phase, or Instrumentation Error)
- ▶ Return to Normal
- ▶ Feeder Commissioned Event Result (Successful, Partial Restoration, or Failure)



## FLISR Automatic Response Report

Permanent Fault detected on Feeder5 at 2024-01-12 | 7:23:36.466 AM

### Summary

**Feeder:** Feeder5 (Sim ID: 2)

**Event Type:** Fault

**Event Start:** 2024-01-12 | 7:23:36.466 AM

**Lockout Time (From Device):** 2024-01-12 | 7:23:36.443 AM

**Event End:** 2024-01-12 | 7:23:51.471 AM

**Duration:** 15.005 seconds

**Event Result:** Partial Restoration

## Device Status Table

View pre-event loading and status, post-event status, and service restoration performance.

### Device Voltages

Device	Voltages at Time of the Event						Voltages After Reconfiguration					
	Left PT			Right PT			Left PT			Right PT		
	A	B	C	A	B	C	A	B	C	A	B	C
B5	7,960	7,960	7,960	N/A	N/A	N/A	7,960	7,960	7,960	N/A	N/A	N/A
R11	7,960	7,960	7,960	0	0	0	7,960	7,960	7,960	0	0	0
R13	0	0	0	0	0	0	7,960	7,960	7,960	7,960	7,960	7,960
R14	0	0	0	7,960	7,960	7,960	7,960	7,960	7,960	7,960	7,960	7,960
R15	0	0	0	0	0	0	0	0	0	7,960	7,960	7,960
R16	0	0	0	0	0	0	7,960	7,960	7,960	7,960	7,960	7,960
R18	0	0	0	7,960	7,960	7,960	7,960	7,960	7,960	7,960	7,960	7,960
S12	0	0	0	0	0	0	0	0	0	7,960	7,960	7,960
S17	0	0	0	7,960	7,960	7,960	7,960	7,960	7,960	7,960	7,960	7,960

### Device Details

Device	Initial Load (A)			Device Status	
	A	B	C	Before	After
B5	127	127	127	Closed	Closed
R11	109	109	109	Open	Open
R13	29	29	29	Closed	Closed
R14	0	0	0	Open	Closed <span style="color:red;">†</span>
R15	40	40	40	Closed	Open <span style="color:green;">*!</span>
R16	0	0	0	Open	Open
R18	0	0	0	Open	Open
S12	58	58	58	Closed	Open <span style="color:green;">*!</span>
S17	0	0	0	Open	Closed <span style="color:red;">†</span>

### Adjacent Circuit Details

Connection	Initial Margin (A)	Feeder State	Connection Status	
			Before	After
Feeder3.Junction-A9C4-NORTH	418	Enabled	Connected	Connected
Feeder3.Junction-FE29-SOUTH	418	Enabled	Connected	Connected
Feeder4.Junction-912C-SOUTH	415	Enabled	Connected	Connected

### Post-Reconfiguration Loading

The following load values are the maximums of the three phases.

**Initial Load Lost (A):** 109

**Restored Load (A):** 98

**Fault Zone Load Lost (A):** 11

**Unrestored Load (A):** 0

# Voltage Summary

---

Voltage reporting supports multiple subtypes. These are noted by the following symbols:

- Loss-of-Source— 
- Open Phase— 
- Instrumentation Error— 

A single report may include multiple subtypes, depending on the simulation that is run or the real world operational elements reported.



## Summary

**Feeder:** Feeder1

**Event Start:** 2023-12-14 | 4:00:45.920 PM

**Duration:** 22.338 seconds

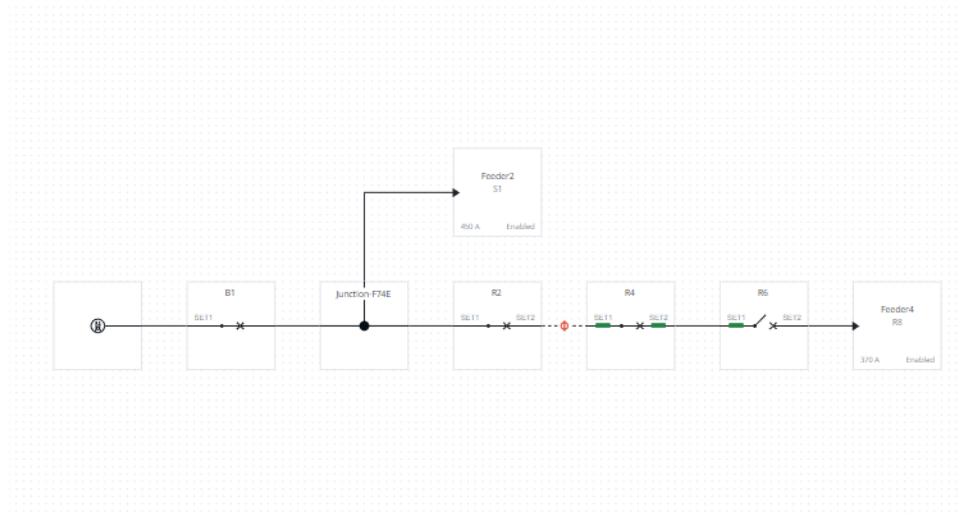
**Voltage Event Subtype:** Open Phase

**Event Type:** Voltage Event

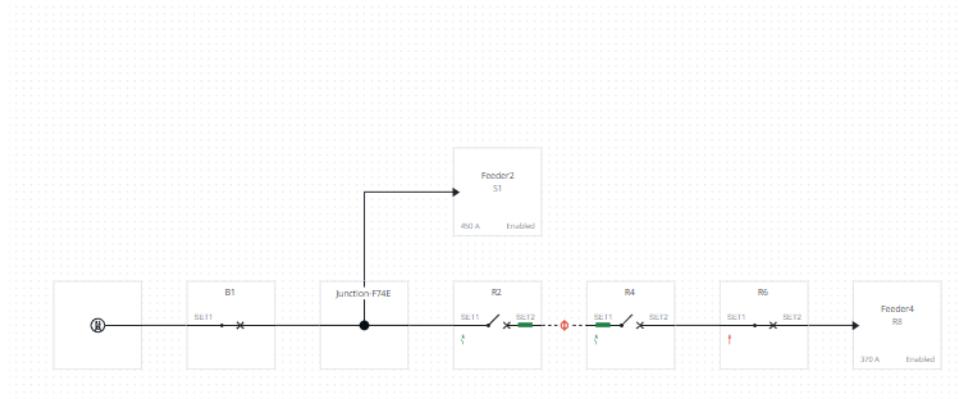
**Event End:** 2023-12-14 | 4:01:08.258 PM

**Event Result:** Success

**Feeder State at Time of Event**



**Feeder State After Reconfiguration**



### Device Voltages

Device	Voltages at Time of the Event						Voltages After Reconfiguration					
	Left PT			Right PT			Left PT			Right PT		
	A	B	C	A	B	C	A	B	C	A	B	C
B1	7,960	7,960	7,960	N/A	N/A	N/A	7,960	7,960	7,960	N/A	N/A	N/A
R2	7,960	7,960	7,960	7,960	7,960	7,960	7,960	7,960	7,960	0	0	0
R4	0	0	0	0	0	0	0	0	0	7,960	7,960	7,960
R6	0	0	0	7,960	7,960	7,960	7,960	7,960	7,960	7,960	7,960	7,960

### Device Details

Device	Initial Load (A)			Device Status		
	A	B	C	Before	After	
B1	68	68	68	Closed	Closed	
R2	40	40	40	Closed	Open 	
R4	20	20	20	Closed	Open 	
R6	0	0	0	Open	Closed 	

### Adjacent Circuit Details

Connection	Initial Margin (A)	Feeder State	Voltage Status			Connection Status	
			A	B	C	Before	After
Feeder2.S1	450	Enabled	Live	Live	Live	Disconnected	Disconnected
Feeder4.R8	370	Enabled	Live	Live	Live	Connected	Connected

### Post-Reconfiguration Loading

The following load values are calculated by taking the sum of the loads for the affected phases.

**Initial Load Lost (A):** 120

**Restored Load (A):** 60

**Voltage Event Zone Load Lost (A):** 60

**Unrestored Load (A):** 0

## Reconfiguration Plan

### Control Sequence 1

- |                 |  |                             |
|-----------------|--|-----------------------------|
| 1. ISOLATE      | Open R15   | Completed at 7:23:48.457 AM |
| 2. SECTIONALIZE | Open R16   | Device was already open     |
| 3. SECTIONALIZE | Open S17   | Device was already open     |
| 4. RESTORE      | Send close request to connection Feeder3.Junction-A9C4-NORTH | Completed at 7:23:48.458 AM |
| 5. RESTORE      | Close R18  | Completed at 7:23:51.471 AM |

### Control Sequence 2

- |                 |  |                             |
|-----------------|--|-----------------------------|
| 1. ISOLATE      | Open R13   | Completed at 7:23:48.456 AM |
| 2. SECTIONALIZE | Open R16   | Device was already open     |
| 3. RESTORE      | Send close request to connection Feeder4.Junction-912C-SOUTH | Completed at 7:23:48.458 AM |
| 4. RESTORE      | Close R14  | Completed at 7:23:51.471 AM |

### Control Sequence 3

- |                 |          |                         |
|-----------------|----------|-------------------------|
| 1. SECTIONALIZE | Open S17 | Device was already open |
|-----------------|----------|-------------------------|

### Control Sequence 4

- |            |          |                           |
|------------|----------|---------------------------|
| 1. ISOLATE | Open R11 | Device was already open   |
| 2. RESTORE | Close R5 | Device was already closed |

### Optimization Order

1. Minimize unrestored load
2. Maximize energized segments
3. Minimize switching operations
4. Maximize margin

## Control Sequence Plan

See what control actions FLISR took to isolate the fault and to restore service.

### Reconfiguration Plan

#### Control Sequence 1

- |            |          |                           |
|------------|----------|---------------------------|
| 1. ISOLATE | Open R11 | Device was already open   |
| 2. RESTORE | Close B5 | Device was already closed |

#### Control Sequence 2

- |                 |  |                             |
|-----------------|--|-----------------------------|
| 1. ISOLATE      | Open R15   | Completed at 9:36:41.112 AM |
| 2. SECTIONALIZE | Open R16   | Device was already open     |
| 3. SECTIONALIZE | Open R18   | Device was already open     |
| 4. RESTORE      | Send close request to connection Feeder3.Junction-FE29-SOUTH | Completed at 9:36:41.115 AM |
| 5. RESTORE      | Close S17  | Completed at 9:36:44.119 AM |

#### Control Sequence 3

- |                 |  |                             |
|-----------------|--|-----------------------------|
| 1. ISOLATE      | Open S12   | Completed at 9:36:41.114 AM |
| 2. SECTIONALIZE | Open R16   | Device was already open     |
| 3. RESTORE      | Send close request to connection Feeder4.Junction-912C-SOUTH | Completed at 9:36:41.115 AM |
| 4. RESTORE      | Close R14  | Completed at 9:36:44.121 AM |
| 5. RESTORE      | Close R13  | Device was already closed   |

#### Control Sequence 4

- |                 |          |                         |
|-----------------|----------|-------------------------|
| 1. SECTIONALIZE | Open R18 | Device was already open |
|-----------------|----------|-------------------------|

### Optimization Order

1. Minimize unrestored load
2. Maximize energized segments
3. Minimize switching operations
4. Maximize margin

# Retrieve Report Data Programmatically

---

Retrieve reports programmatically using the Report API. This API makes it possible to monitor the application for new reports and retrieve those reports as a JSON document for integration into third-party applications, such as operator interfaces and databases for computing performance metrics. Detailed descriptions of each endpoint, including example usage and schemas, are provided in the integrated documentation located in the FLISR application under **View > API Documentation**.

The following endpoints are provided by the Report API:

- ▶ **DELETE https://<Blueframe IP address>/flisr/api/v1/reports:** Deletes all reports matching the provided parameters. Users accessing this endpoint must have the FLISR “Can Launch” and “Can Operate” permission. Deletion of reports cannot be undone.
- ▶ **GET https://<Blueframe IP address>/flisr/api/v1/reports:** Gets a list of reports with full report content matching the provided parameters. Users accessing this endpoint must have the FLISR “Can Launch” permission.
- ▶ **GET https://<Blueframe IP address>/flisr/api/v1/reports/metadata:** Gets a list of report metadata matching the provided parameters. Users accessing this endpoint must have the FLISR “Can Launch” permission.

Report API endpoints require an authentication token with each interaction. The authentication token can be obtained by issuing a POST to /login-page/v1/login.

The following code snippet provides an example in Python of how to use the Report API to retrieve a list of reports. Note that this code snippet must be updated with a correct IP address, username, and password before it will function correctly.

---

```
import requests
import sys
# Note: "verify=False" allows communication without Blueframe having an X.509 certificate signed by a trusted certificate authority.
# This is equivalent to bypassing the security warning in the browser to sign into Blueframe on first login, having not replaced
# the default certificate.
response = \
requests.post('https://<INSERT IP ADDRESS>/login-page/v1/login',
              json={'username': '<INSERT USERNAME>',
                     'password': '<INSERT PASSWORD>'}, verify=False)
if response.status_code != 200:
    sys.exit('Failed to get authentication token')
json = response.json()
token = json['token']['token'] # The authentication token is nested inside a token object

# The authentication token is valid for five minutes, and during that time can be used with the various Blueframe APIs.

# Example: get a list of reports from the FLISR Report API and print the response.

response = \
    requests.get('https://<INSERT IP ADDRESS>/flisr/api/v1/reports',
                 headers={'cookie': 'auth={}'.format(token)},
                 verify=False)
print response.status_code
print response.content
```

---

**This page intentionally left blank**

---

---

## A P P E N D I X    A

---

# Software and Manual Versions

## Software

---

Refer to Application Management in Blueframe to obtain software version information for each DMS application. DMS applications are separated into application packages according to their functionality:

- ▶ The Power System Model (PSM) package includes the PSM and Model Data Import (MDI) applications.
- ▶ The FLISR package includes the FLISR application.

Select the package of interest within Application Management to view the installed version. From Application Management, you can also view the package state, when the package was installed, applications contained within the package, and available versions. See *Section 3: Application Management* in the Blueframe instruction manual for additional information on how to use and navigate within Application Management.

*Table A.1* lists the PSM package versions, a description of the changes, and the manual date code corresponding to the package version. The table lists the most recent package version first.

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 A.1 PSM Package Version History**

Package Version Number	Summary of Revisions	Manual Date Code
1.3.0	<ul style="list-style-type: none"> <li>► <b>PSM:</b> <ul style="list-style-type: none"> <li>➢ All model and single container exports have transitioned to *.json file exports. SEL recommends that all customers update model and single container exports to the new *.json file type because future releases of PSM will not support legacy file types, *.bin and *.bak.</li> <li>➢ Expanded modeling capabilities to support Transmission Lines.</li> <li>➢ Expanded supported assets within the substation model to include Current Transformers, Potential Transformers, Shunt Compensators, and Series Compensators.</li> </ul> </li> <li>► <b>Model Data Import:</b> <ul style="list-style-type: none"> <li>➢ Expanded the modeling function to support CIM (IEC 61970).</li> </ul> </li> </ul>	20241213
1.2.0	<ul style="list-style-type: none"> <li>► <b>PSM Core functionality:</b> <ul style="list-style-type: none"> <li>➢ Added keyboard hot keys.</li> <li>➢ Added the ability to build a substation model in addition to a distribution model.</li> <li>➢ Added the ability for substation and distribution models to be linked.</li> <li>➢ Expanded switch properties to support multiple variants of switches in the field.</li> </ul> </li> <li>► <b>Model Data Import functionality:</b> <ul style="list-style-type: none"> <li>➢ Added functionality to read substation GeoJSON models.</li> <li>➢ Added a new "auto" operator in node properties for Substation models.</li> <li>➢ Updates to API.</li> </ul> </li> </ul>	20240112
1.0.0	<ul style="list-style-type: none"> <li>► <b>PSM Core functionality:</b> <ul style="list-style-type: none"> <li>➢ Initial release. (The PSM package replaces the DMS Designer package.)</li> </ul> </li> <li>► <b>Model Data Import functionality:</b> <ul style="list-style-type: none"> <li>➢ Initial release.</li> </ul> </li> </ul>	20230912

*Table A.2* lists the FLISR package versions, a description of the changes, and the manual date code corresponding to the package version. The table lists the most recent package version first.

**Table A.2 FLISR Package Version History**

Package Version Number	Summary of Revisions	Manual Date Code
2.2.0	<ul style="list-style-type: none"> <li>► Enhanced FLISR to reduce "negative load" calculations and to support low bandwidth communication networks.</li> <li>► Added the Loss-of-Source Mode setting, allowing FLISR configurations to process Loss-of-source events from three-phase as well as from any single-phase Loss-of-Source.</li> <li>► Enhanced FLISR to support non-SEL reclosers with fault indication that only enables when the reclosers are in an overcurrent condition. This is done through FLISR's OvercurrentReported point.</li> <li>► Enhanced boundary device fault management.</li> <li>► Enhanced FLISR's backup/restore capability for larger installations.</li> <li>► Enhanced substation and feeder model connectivity.</li> <li>► Enhanced Loop blocking to prevent processing of events after reclosing.</li> <li>► Enhanced FLISR and Protocol Services integration on application start up.</li> <li>► Enhanced FLISR's visual event chips by standardizing the Event chip across all event types.</li> <li>► Enhanced the accuracy of FLISR when intermediate feeders are used between two sources.</li> <li>► Disabled default parameters of the Open Policy Agent restricting automatic debug reporting.</li> </ul>	20241213
2.1.0	<ul style="list-style-type: none"> <li>► <b>FLISR functionality:</b> <ul style="list-style-type: none"> <li>➢ Added support to consume breakers in Substation or Distribution models.</li> <li>➢ Added support for switch property expansion.</li> <li>➢ Added the ability for FLISR to detect non-overcurrent event outages using field device voltage measurements. These types of outages are typically caused by burned jumpers, broken conductors, or a loss of substation source. This feature will include both open phase detection, loss of source detection, and voltage measurement error detection.</li> <li>➢ Added additional settings to support customer operational needs.</li> <li>➢ Enhanced FLISR to only publish FlisrAlarm for the device in the alarm.</li> <li>➢ Made improvements to the Return to Normal function.</li> <li>➢ Enhanced the FLISR algorithm for disarmed feeders.</li> </ul> </li> <li>► <b>Report API functionality:</b> <ul style="list-style-type: none"> <li>➢ Added voltage events.</li> </ul> </li> </ul>	20240112
2.0.0	<ul style="list-style-type: none"> <li>► Added a staging area to FLISR that will be used for mapping protocol clients and points to FLISR, validating communications, and validating FLISR licenses.</li> <li>► Resolved an issue where FLISR version upgrades could fail when the configuration contained commissioned feeders.</li> <li>► Resolved an issue where an interruption in a Return to Normal operation caused diagnostic messages indicating both "complete" and "interrupted".</li> <li>► Resolved an issue where Reports did not include all line segments in a fault zone on the feeder diagram.</li> <li>► Resolved an issue in Reports where the diagnostic message "could not be restored because it was isolated from all sources" would occur when two faults occurred on the feeder.</li> <li>► Resolved an issue in simulations where a Neighbor Feeder Status Availability change would incorrectly change the availability status for all connected feeders.</li> <li>► Resolved an issue where correcting miscoordination could trigger a separate event if reclosers were programmed to lockout on open.</li> <li>► Resolved an issue where Reports did not include all fault zones in the feeder diagram when multiple faults were reported in the same event.</li> </ul>	20230912
1.4.3	<ul style="list-style-type: none"> <li>► Addressed an issue affecting all previous versions where FLISR does not respond to an event when over 50 feeders are deployed.</li> </ul>	20230823
1.4.2	<ul style="list-style-type: none"> <li>► Enhanced FLISR to restore from the local source by default as much as possible.</li> <li>► Addressed an issue affecting all previous versions where misconfiguration or inaccurate field device data created the appearance of negative load distribution in one or more zones affecting FLISR's restoration calculations.</li> <li>► Addressed an issue affecting all previous versions that caused unnecessary switching operations in an unrestored zone.</li> <li>► Addressed an issue affecting all previous versions where FLISR did not close an adjacent circuit in order to restore a previously energized segment with zero load.</li> <li>► Resolved an issue where closely timed incoming field data might have caused FLISR to fail detecting an event.</li> </ul>	20230602

Package Version Number	Summary of Revisions	Manual Date Code
1.4.1	<ul style="list-style-type: none"> <li>► Changed the behavior of Advisory Mode and Isolation Mode to treat adjacent circuits that are in Advisory Mode or Isolation Mode as if they were in Automatic Mode.</li> <li>► Resolved an issue in FLISR reports where in some cases a switching device opened for isolation was not listed in the control sequence.</li> <li>► Resolved an issue where the FLISR Report API is unable to return a report document when the model contains feeder connections that are left unassigned and not linked to other feeders.</li> <li>► Resolved an issue in the DMS Report API that could cause the JSON response to be missing some device names for reports generated in the simulator.</li> </ul>	20230406
1.4.0	<ul style="list-style-type: none"> <li>► Added an API to FLISR reports that can be used to query and maintain reports.</li> <li>► Addressed an issue affecting all previous versions that caused the "FlisrAlarm" signal to continue to be published if the associated feeder was disarmed or deactivated while an event was in progress.</li> <li>► Enhanced the FLISR feeder list to support multi-select, making it possible to arm, disarm, and reset targets on a selected group of feeders.</li> <li>► Enhanced the FLISR feeder list by adding a right-click context menu, making it possible to arm, disarm, and target reset a selected feeder or all feeders under a selected folder.</li> <li>► Enhanced reports by adding an "Event Result" field that indicates the success of FLISR event processing.</li> <li>► Enhanced FLISR reports by adding fields indicating whether a miscoordination or sub-optimal restoration has occurred.</li> <li>► Enhanced the clarity of FLISR reports by renaming the "Return to Normal Mode" field to "Transition Mode" in Return to Normal reports.</li> <li>► Enhanced FLISR to proceed with restoring line segments with zero measured load even if an additional switching operation is required.</li> <li>► Added an optional model security check that ensures that all devices in a fault zone are de-energized prior to proceeding with isolation and restoration. This behavior is tied to the value of the feeder level "Voltage Integrity Check" setting.</li> </ul>	20230330
1.3.1	<ul style="list-style-type: none"> <li>► Resolved an issue introduced in FLISR 1.3.0 in which the user interface could hang under some circumstances when a feeder is deactivated in DMS Designer.</li> </ul>	20230103
1.3.0	<ul style="list-style-type: none"> <li>► Reduced resources needed to run multiple simulations concurrently.</li> <li>► Resolved an issue that could result in FLISR using as much as 125% capacity as an emergency restoration limit. FLISR now elects to leave necessary load de-energized if more than 100% capacity is required.</li> </ul>	20221216
1.2.1	<ul style="list-style-type: none"> <li>► Resolved an issue where multiple feeders blocking due to a loop would continue to block even after the loop is broken.</li> <li>► Addressed an issue affecting all previous versions that in some cases caused feeder and device level status indications to appear de-asserted in both the user interface and DNP data points. This issue did not affect the secure operation of FLISR but did impact the visibility of these data points in user interfaces.</li> </ul>	20221103

<b>Package Version Number</b>	<b>Summary of Revisions</b>	<b>Manual Date Code</b>
1.2.0	<ul style="list-style-type: none"> <li>► Added Return to Normal Advisory mode and Return to Normal reports.</li> <li>► Enhanced reports for improved consistency across report types.</li> <li>► Added FLISR Advisory and Isolation_Only modes.</li> <li>► Added customizable FLISR block points to devices and feeders.</li> <li>► Added Commissioning Tools feature.</li> <li>► Added support for Blueframe templates and profiles.</li> <li>► Resolved an issue where feeders would incorrectly drop out of Loop Blocked state because neighbor feeders were too busy to answer requests.</li> <li>► Resolved an issue where the FLISR DNP Server point map could become unresponsive after editing or deactivating a feeder.</li> <li>► Resolved an issue that suppressed the FLISR licensing banner on the Blueframe web interface.</li> <li>► Enhanced reports to provide more information in the Neighbor Details table.</li> <li>► Resolved an issue where, in some situations, a line segment would not be restored due to a lack of capacity even though there was adequate capacity.</li> <li>► Resolved an issue where SCADA data were not published for concentrated devices.</li> <li>► Resolved an issue where FLISR would, in certain circumstances, close a device, causing a loop between one or more sources.</li> <li>► Resolved an issue where FLISR would occasionally not restore load when the event feeder had multiple neighbors.</li> <li>► Added selectable neighbor feeder Availability status to FLISR simulation.</li> <li>► Changed loop condition clearing behavior to delay feeder unblocking until the event detection time expires.</li> <li>► [Cybersecurity Enhancement] Restricted FLISR webpages from being embedded in other pages outside the application.</li> <li>► [Cybersecurity Enhancement] Enhanced security of FLISR application webpages to prevent cross-site scripting, injection, and cross-origin attacks.</li> <li>► Enhanced the FLISR user interface to include feeder blocking details.</li> <li>► Resolved an issue that could cause FLISR to no longer know the availability of a device after a long deployment period.</li> </ul>	20220930
1.1.1	<ul style="list-style-type: none"> <li>► Enhanced operations reports to provide more information about adjacent feeder availability.</li> <li>► Enhanced the FLISR upgrade process to support deployed feeders. Deployed feeders will be disarmed as part of the upgrade process.</li> <li>► Resolved an issue that prevented FLISR from re-enabling correctly after a device status change to OOS Closed or Open when a device's DNP connection is removed.</li> <li>► Improved the responsiveness of the integrated simulator.</li> <li>► Added support for exporting communications warnings in XLSX and CSV formats.</li> <li>► Resolved an issue where FLISR was requiring a lockout signal from switches.</li> </ul>	20220601
1.0.0	<ul style="list-style-type: none"> <li>► Initial release.</li> </ul>	20220506

## Instruction Manual

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

*Table A.3* lists the instruction manual date codes and a description of modifications. The most recent instruction manual revisions are listed first.

**Table A.3 Manual Revision History**

<b>Date Code</b>	<b>Summary of Revisions</b>
20250114	<p><b>Section 1</b></p> <ul style="list-style-type: none"> <li>► Added <i>DMS Hardware and Sizing Specifications</i> to <i>DMS Application Packages</i>.</li> </ul> <p><b>Appendix A</b></p> <ul style="list-style-type: none"> <li>► Updated Summary of Revisions for FLISR package version 2.2.0.</li> </ul>
20241213	<p><b>Section 1</b></p> <ul style="list-style-type: none"> <li>► Updated <i>Introductions</i>.</li> </ul>

Date Code	Summary of Revisions
	<p><b>Section 2</b></p> <ul style="list-style-type: none"> <li>► Updated <i>Introduction</i>, <i>GeoJSON File Content Requirements</i>, <i>Application Usage</i>, and <i>Model Data Importer API</i>.</li> <li>► Added <i>CIM Requirements</i> and <i>CIM File Control Requirements</i>.</li> </ul> <p><b>Section 3</b></p> <ul style="list-style-type: none"> <li>► Updated <i>Table 3.7: Substation Breaker Node Settings</i>, <i>Table 3.8: Substation Recloser Node Settings</i>, <i>Table 3.9: Substation Switch Node Settings</i>, <i>Table 3.10: Substation Tie Node Settings</i>, <i>Table 3.16: Breaker Node Settings</i>, <i>Table 3.17: Recloser Node Settings</i>, and <i>Table 3.18: Switch Node Settings</i>.</li> <li>► Updated <i>Canvas</i>, <i>Model Publishing and Checkout</i>, and <i>Model Management Tools</i>.</li> <li>► Added <i>Model Conversion</i>.</li> </ul> <p><b>Section 4</b></p> <ul style="list-style-type: none"> <li>► Updated <i>How Fault Location Works</i>, <i>Return to Normal</i>, and <i>FLISR Operations</i>.</li> <li>► Added <i>Operational Impacts of Switch Configurations</i>.</li> </ul> <p><b>Appendix A</b></p> <ul style="list-style-type: none"> <li>► Updated PSM package version to 1.3.0.</li> <li>► Updated FLISR package version to 2.2.0.</li> </ul> <p><b>Appendix B</b></p> <ul style="list-style-type: none"> <li>► Organized into two sections: <i>Field Data</i> and <i>SCADA Data</i>.</li> </ul>
20240112	<p><b>General</b></p> <ul style="list-style-type: none"> <li>► Revised manual layout to reflect the new position of <i>Model Data Import</i> as Section 2.</li> </ul> <p><b>Section 1</b></p> <ul style="list-style-type: none"> <li>► Updated <i>DMS Application Packages</i>.</li> </ul> <p><b>Section 2</b></p> <ul style="list-style-type: none"> <li>► Added <i>Figure 2.1: MDI File Management</i>, <i>Figure 2.2: Full Pipeline Manager Interface Callout</i>, and <i>Figure 2.9: Substation Pipeline Manager</i>.</li> <li>► Updated <i>Figure 2.8: Feeder Pipeline Manager</i>, <i>Figure 2.15: Pipeline Manager Interface</i>, and <i>Figure 2.21: Complete Asset Mapping Example</i>.</li> <li>► Updated <i>Application Usage</i>.</li> <li>► Updated <i>File Import</i>, <i>Pipeline Configuration</i>, and <i>Asset Mapping</i> in <i>Application Usage</i>.</li> <li>► Updated <i>Endpoints</i> and <i>Data Definitions</i> in <i>Model Data Importer API</i>.</li> </ul> <p><b>Section 3</b></p> <ul style="list-style-type: none"> <li>► Updated <i>Figure 3.1: Power System Model User Interface</i>, <i>Figure 3.7: Draft Panel</i>, <i>Figure 3.8: Feeder Checkout</i>, <i>Figure 3.9: Feeder Checkout</i>, and <i>Figure 3.10: Model Management Tools</i>.</li> <li>► Updated <i>Overview</i>, <i>Canvas</i>, <i>Model Publishing and Checkout</i>, and <i>Editing a Published System</i>.</li> <li>► Added <i>Keyboard Hot Keys</i> in <i>Canvas</i>.</li> <li>► Updated <i>Canvas Settings</i> and <i>Feeder Canvas Nodes and Settings</i> in <i>Canvas</i>.</li> <li>► Added <i>Substation Canvas Nodes and Settings</i> in <i>Canvas</i>.</li> <li>► Added <i>Creating A New Model in PSM</i> and <i>Model Management Tools</i>.</li> <li>► Updated <i>Table 3.3: Feeder Canvas Property Grid Settings</i>, <i>Table 3.16: Breaker Node Settings</i>, <i>Table 3.17: Recloser Node Settings</i>, and <i>Table 3.18: Switch Node Settings</i>.</li> </ul> <p><b>Section 4</b></p> <ul style="list-style-type: none"> <li>► Updated <i>How Fault Location Works</i> and <i>How Service Restoration Works</i> in <i>FLISR Fundamentals</i>.</li> <li>► Added <i>Voltage Events</i> in <i>FLISR Fundamentals</i>.</li> <li>► Updated <i>Adding a Feeder</i>, <i>FLISR Feeder Settings</i>, <i>Return to Normal Operational Modes</i>, <i>How to Simulate a Permanent Fault</i>, and <i>How to Simulate a Miscoordination</i> in <i>FLISR Operations</i>.</li> <li>► Updated <i>Table 4.1: Feeder Canvas Property Grid Settings</i> and <i>Table 4.2: FLISR-Specific Settings Established in PSM</i>.</li> <li>► Added <i>Table 4.3: FLISR-Specific Node Settings</i>.</li> <li>► Updated <i>Figure 4.3: DMS FLISR User Interface</i>.</li> <li>► Added <i>Switch Operation</i> and <i>Voltage Operation</i> in <i>FLISR Operations</i>.</li> <li>► Added <i>Figure 4.6: FLISR Simulation View</i>.</li> <li>► Updated <i>Figure 4.7: Simulating a Feeder in FLISR</i> and <i>Figure 4.8: Simulated Feeder User Interface</i>.</li> </ul> <p><b>Section 5</b></p> <ul style="list-style-type: none"> <li>► Updated figures.</li> <li>► Updated <i>Feeder State Diagrams</i>.</li> <li>► Added <i>Voltage Summary</i>.</li> </ul>

Date Code	Summary of Revisions
	<p><b>Appendix A</b></p> <ul style="list-style-type: none"> <li>► Updated PSM package version to 1.2.0.</li> <li>► Updated FLISR package version to 2.1.0.</li> </ul> <p><b>Appendix B</b></p> <ul style="list-style-type: none"> <li>► Updated <i>Table B.1: Feeder SCADA Data</i>, <i>Table B.4: Breaker SCADA Data</i>, <i>Table B.5: Recloser Device Data</i>, <i>Table B.6: Recloser SCADA Data</i>, <i>Table B.7: Switch Device Data</i>, and <i>Table B.8: Switch SCADA Data</i>.</li> </ul>
20230912	<p><b>General</b></p> <ul style="list-style-type: none"> <li>► Changed name of "DMS Designer" to "Power System Model" (PSM).</li> <li>► Added <i>Section 5: Model Data Import</i>.</li> </ul> <p><b>Section 1</b></p> <ul style="list-style-type: none"> <li>► Updated <i>DMS Application Packages</i>.</li> </ul> <p><b>Section 2</b></p> <ul style="list-style-type: none"> <li>► Updated <i>Figure 2.1: Power System Model User Interface</i>.</li> <li>► Updated <i>Feeder Canvas</i>, <i>Settings Validation</i>, and <i>PSM Usage Notes</i>.</li> <li>► Added <i>Model Publishing and Checkout</i>.</li> <li>► Updated <i>Editing a Published System</i>.</li> </ul> <p><b>Section 3</b></p> <ul style="list-style-type: none"> <li>► Updated <i>FLISR Fundamentals</i>.</li> <li>► Added <i>Adding a Feeder to FLISR</i> and <i>FLISR Feeder Settings to FLISR Operations</i>.</li> </ul> <p><b>Appendix A</b></p> <ul style="list-style-type: none"> <li>► Added <i>Table A.1: PSM Package Version History</i>.</li> <li>► Updated FLISR package to version 2.0.0.</li> <li>► Updated revision summary for FLISR package version 1.4.0 to state that the optional model security check is tied to the value of the feeder "Voltage Integrity Check" setting.</li> </ul> <p><b>Appendix C</b></p> <ul style="list-style-type: none"> <li>► Updated <i>Access Control</i>.</li> </ul>
20230823	<p><b>Appendix A</b></p> <ul style="list-style-type: none"> <li>► Updated FLISR package to version 1.4.3.</li> </ul>
20230602	<p><b>Appendix A</b></p> <ul style="list-style-type: none"> <li>► Updated FLISR package to version 1.4.2.</li> </ul>
20230406	<p><b>Appendix A</b></p> <ul style="list-style-type: none"> <li>► Updated FLISR package to version 1.4.1.</li> </ul>
20230330	<p><b>General</b></p> <ul style="list-style-type: none"> <li>► Added <i>Section 4: Reports</i>.</li> </ul> <p><b>Section 2</b></p> <ul style="list-style-type: none"> <li>► Updated <i>Table 2.1: Feeder Canvas Property Grid Settings</i>.</li> <li>► Updated <i>Feeder Connection in Feeder Canvas</i>.</li> <li>► Updated <i>Note 2: FLISR Can Optionally Use PT Measurements to Confirm That all Devices in a Known Fault Zone are De-Energized in DMS Designer Usage Notes</i>.</li> </ul> <p><b>Section 3</b></p> <ul style="list-style-type: none"> <li>► Updated <i>How Fault Location Works</i> and <i>How Service Restoration Works</i> in <i>FLISR Fundamentals</i>.</li> </ul> <p><b>Appendix A</b></p> <ul style="list-style-type: none"> <li>► Updated FLISR package to version 1.4.0.</li> <li>► Updated Summary of Revisions for FLISR package version 1.2.1.</li> </ul>
20230103	<p><b>Appendix A</b></p> <ul style="list-style-type: none"> <li>► Updated FLISR package to version 1.3.1.</li> </ul>
20221216	<p><b>Appendix A</b></p> <ul style="list-style-type: none"> <li>► Updated DMS Designer package to version 1.2.0.</li> <li>► Updated FLISR package to version 1.3.0.</li> </ul>

Date Code	Summary of Revisions
20221103	<b>Appendix A</b> <ul style="list-style-type: none"><li>► Updated DMS Designer package to version 1.1.1.</li><li>► Updated FLISR package to version 1.2.1.</li></ul>
20220930	<b>Section 2</b> <ul style="list-style-type: none"><li>► Added <i>Feeder Canvas Settings</i> to <i>Feeder Canvas</i>.</li></ul> <b>Section 3</b> <ul style="list-style-type: none"><li>► Updated <i>Return to Normal</i> in <i>FLISR Fundamentals</i>.</li><li>► Updated <i>Figure 3.3: DMS FLISR User Interface</i>.</li><li>► Added <i>FLISR and Return to Normal Operational Modes and Reports</i> to <i>FLISR Operations</i>.</li><li>► Updated <i>Arming, Disarming, and Blocking</i> in <i>FLISR Operations</i>.</li></ul> <b>Appendix A</b> <ul style="list-style-type: none"><li>► Updated DMS Designer package to version 1.1.0.</li><li>► Updated FLISR package to version 1.2.0.</li></ul> <b>Appendix B</b> <ul style="list-style-type: none"><li>► Added a note specifying that all binary outputs must use the operPulse control model.</li><li>► Updated <i>Table B.1: Feeder SCADA Data</i>.</li><li>► Added <i>Table B.2: Status Supervisor Data</i>.</li><li>► Added FlisrBlock1–FlisrBlock5 settings to <i>Table B.3: Breaker Device Data</i>, <i>Table B.5: Recloser Device Data</i>, and <i>Table B.7: Switch Device Data</i>.</li></ul> <b>Appendix C</b> <ul style="list-style-type: none"><li>► Updated <i>Access Control</i>.</li></ul>
20220601	<b>Section 1</b> <ul style="list-style-type: none"><li>► Added <i>Upgrading and Downgrading FLISR Applications When Feeders Are Deployed</i>.</li></ul> <b>Appendix A</b> <ul style="list-style-type: none"><li>► Updated DMS Designer package to version 1.0.2.</li><li>► Updated FLISR package to version 1.1.1.</li></ul>
20220506	► Initial version.

---

---

## A P P E N D I X    B

---

# FLISR Data Mapping Tables

FLISR data mapping is defined by two types of data, Field Data and SCADA Data.

### NOTE

If No is noted under Required for FLISR, the data point does not need to be mapped in Protocol Services. However, if the data point is mapped in Protocol Services, FLISR will require the data to be readable.

### NOTE

When creating a FLISR data point in Protocol Services, a user must use a value from the NAME column of Table B.1–Table B.8. For example, a user could enter **VASet1** as the Point Name input of the Protocol Services and create the dnp.devicename.VASet1 data point.

## Field Data

---

Field data come from assets available over the network. To collect field data, FLISR relies on client connections configured in Protocol Services. The connection can be specific for each asset, such as a breaker, recloser, switch, or data concentrator. Each type of asset has specific data points FLISR requires and does not require, as shown in *Table B.1–Table B.8*.

## Breaker

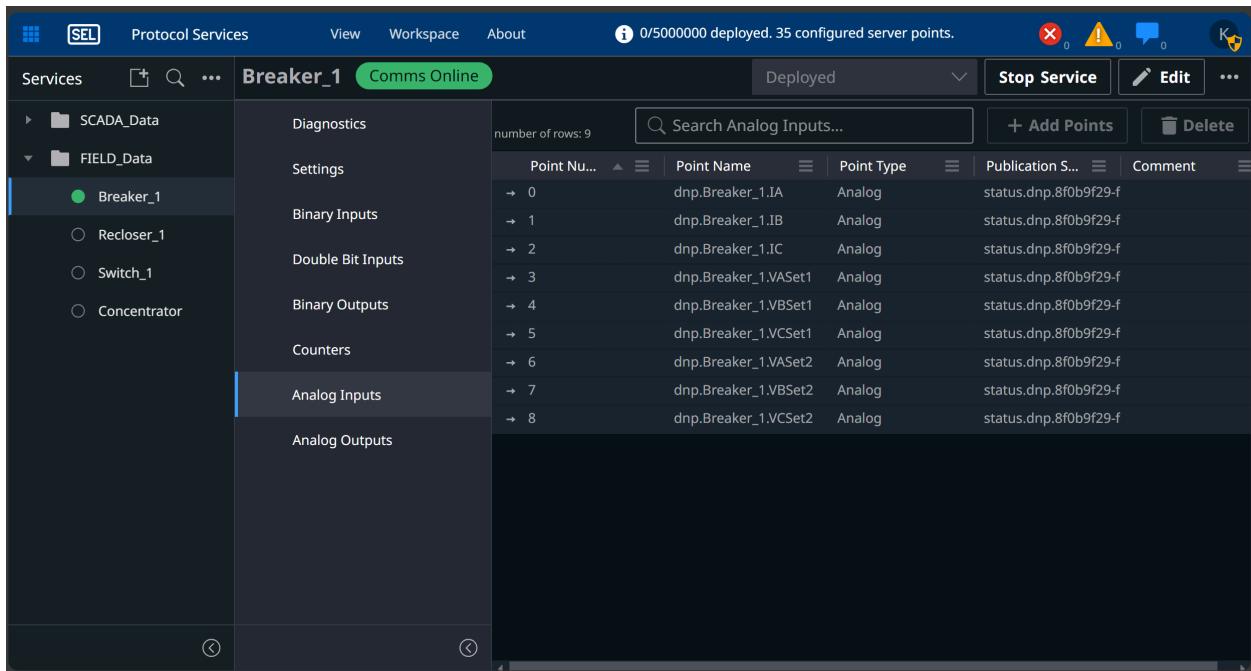
The types of data points FLISR requires and does not require for a breaker are shown in *Table B.1*.

**Table B.1 Breaker Device Data**

Name	Description	Type	Required for FLISR
IA	A-phase current	Analog Input <sup>a</sup>	Yes
IB	B-phase current	Analog Input <sup>a</sup>	Yes
IC	C-phase current	Analog Input <sup>a</sup>	Yes
VASet1	A-phase voltage, PT Set 1	Analog Input <sup>a</sup>	No
VBSet1	B-phase voltage, PT Set 1	Analog Input <sup>a</sup>	No
VCSet1	C-phase voltage, PT Set 1	Analog Input <sup>a</sup>	No
VASet2	A-phase voltage, PT Set 2	Analog Input <sup>a</sup>	No
VBSet2	B-phase voltage, PT Set 2	Analog Input <sup>a</sup>	No
VCSet2	C-phase voltage, PT Set 2	Analog Input <sup>a</sup>	No
52A3P	Three-phase breaker position	Binary Input <sup>b</sup>	Yes
79LO3P	Three-phase lockout	Binary Input <sup>b</sup>	Yes

Name	Description	Type	Required for FLISR
Fault	Fault indication	Binary Input <sup>b</sup>	Yes
RemoteDisabled	Remote control disabled	Binary Input <sup>b</sup>	No
RemoteEnabled	Remote control enabled	Binary Input <sup>b</sup>	No
HotLineTag	Hot-line service tag	Binary Input <sup>b</sup>	No
Online	Device communication is good	Binary Input <sup>b</sup>	Yes, if data concentration is used
OpenCommand	Device open command	Binary Output <sup>c</sup>	Yes
CloseCommand	Device close command	Binary Output <sup>c</sup>	Yes
FlisrBlock1	Customizable FLISR block point 1. The associated feeder automatically blocks FLISR operation when this point is asserted.	Binary Input <sup>b</sup>	No
FlisrBlock2	Customizable FLISR block point 2. The associated feeder automatically blocks FLISR operation when this point is asserted.	Binary Input <sup>b</sup>	No
FlisrBlock3	Customizable FLISR block point 3. The associated feeder automatically blocks FLISR operation when this point is asserted.	Binary Input <sup>b</sup>	No
FlisrBlock4	Customizable FLISR block point 4. The associated feeder automatically blocks FLISR operation when this point is asserted.	Binary Input <sup>b</sup>	No
FlisrBlock5	Customizable FLISR block point 5. The associated feeder automatically blocks FLISR operation when this point is asserted.	Binary Input <sup>b</sup>	No

<sup>a</sup>Shown in Figure B.1.<sup>b</sup>Shown in Figure B.2.<sup>c</sup>Shown in Figure B.3.

**Figure B.1** Breaker Analog Inputs

The screenshot shows the 'Protocol Services' tab selected in the top navigation bar. The main area displays 'Comms Online' for 'Breaker\_1'. A table titled 'Deployed' lists 'Binary Inputs' for the Breaker\_1 device. The table has columns for Point Number, Point Name, and Point Type. There are 11 rows of data, each corresponding to a specific binary input point.

Point Number	Point Name	Point Type
0	dnp.Breaker_1.52A3P	Binary
1	dnp.Breaker_1.79LO3P	Binary
2	dnp.Breaker_1.Fault	Binary
3	dnp.Breaker_1.RemoteDisabled	Binary
4	dnp.Breaker_1.RemoteEnabled	Binary
5	dnp.Breaker_1.HotLineTag	Binary
6	dnp.Breaker_1.FlsrBlock1	Binary
7	dnp.Breaker_1.FlsrBlock2	Binary
8	dnp.Breaker_1.FlsrBlock3	Binary
9	dnp.Breaker_1.FlsrBlock4	Binary
10	dnp.Breaker_1.FlsrBlock5	Binary

**Figure B.2** Breaker Binary Inputs

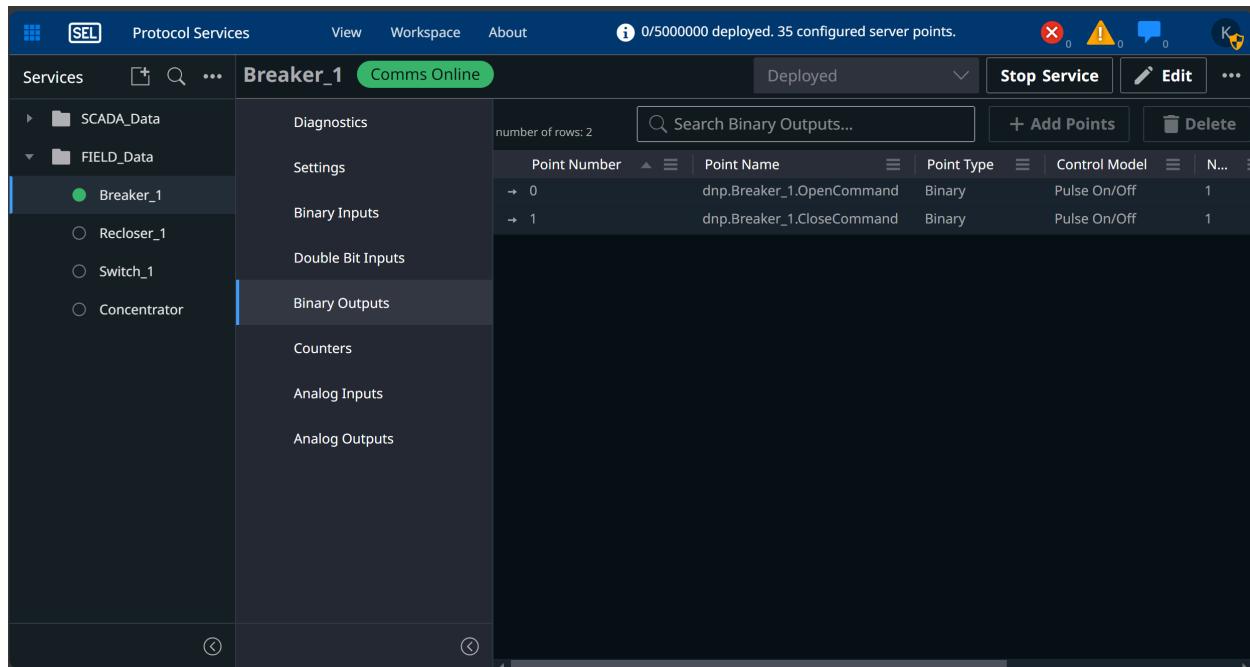


Figure B.3 Breaker Binary Outputs

## Recloser

The types of data points FLISR requires and does not require for a recloser are shown in *Table B.2*.

Table B.2 Recloser Device Data

Name	Description	Type	Required for FLISR
IA	A-phase current	Analog Input <sup>a</sup>	Yes
IB	B-phase current	Analog Input <sup>a</sup>	Yes
IC	C-phase current	Analog Input <sup>a</sup>	Yes
VASet1	A-phase voltage, PT Set 1	Analog Input <sup>a</sup>	No
VBSet1	B-phase voltage, PT Set 1	Analog Input <sup>a</sup>	No
VCSet1	C-phase voltage, PT Set 1	Analog Input <sup>a</sup>	No
VASet2	A-phase voltage, PT Set 2	Analog Input <sup>a</sup>	No
VBSet2	B-phase voltage, PT Set 2	Analog Input <sup>a</sup>	No
VCSet2	C-phase voltage, PT Set 2	Analog Input <sup>a</sup>	No
52A3P	Three-phase breaker position	Binary Input <sup>b</sup>	Yes
79LO3P	Three-phase lockout	Binary Input <sup>b</sup>	Yes
Fault	Fault indication	Binary Input <sup>b</sup>	Yes
RemoteDisabled	Remote control disabled	Binary Input <sup>b</sup>	No
RemoteEnabled	Remote control enabled	Binary Input <sup>b</sup>	No
HotLineTag	Hot-line service tag	Binary Input <sup>b</sup>	No

Name	Description	Type	Required for FLISR
Online	Device communication is good	Binary Input <sup>b</sup>	Yes, if data concentration is used
OpenCommand	Device open command	Binary Output <sup>c</sup>	Yes
CloseCommand	Device close command	Binary Output <sup>c</sup>	Yes
FlisrBlock1	Customizable FLISR block point 1. The associated feeder automatically blocks FLISR operation when this point is asserted.	Binary Input <sup>b</sup>	No
FlisrBlock2	Customizable FLISR blockpoint 2. The associated feeder automatically blocks FLISR operation when this point is asserted.	Binary Input <sup>b</sup>	No
FlisrBlock3	Customizable FLISR block point 3. The associated feeder automatically blocks FLISR operation when this point is asserted.	Binary Input <sup>b</sup>	No
FlisrBlock4	Customizable FLISR block point 4. The associated feeder automatically blocks FLISR operation when this point is asserted.	Binary Input <sup>b</sup>	No
FlisrBlock5	Customizable FLISR block point 5. The associated feeder automatically blocks FLISR operation when this point is asserted.	Binary Input <sup>b</sup>	No

<sup>a</sup>Shown in Figure B.4.<sup>b</sup>Shown in Figure B.5.<sup>c</sup>Shown in Figure B.6.

Point Nu...	Point Name	Point Type	Comment
0	dnp.Recloser_1.IA	Analog	status.dnp.3223bee2
1	dnp.Recloser_1.IB	Analog	status.dnp.3223bee2
2	dnp.Recloser_1.IC	Analog	status.dnp.3223bee2
3	dnp.Recloser_1.VASet1	Analog	status.dnp.3223bee2
4	dnp.Recloser_1.VBSet1	Analog	status.dnp.3223bee2
5	dnp.Recloser_1.VCSet1	Analog	status.dnp.3223bee2
6	dnp.Recloser_1.VASet2	Analog	status.dnp.3223bee2
7	dnp.Recloser_1.VBSet2	Analog	status.dnp.3223bee2
8	dnp.Recloser_1.VCSet2	Analog	status.dnp.3223bee2

Figure B.4 Recloser Analog Inputs

**Field Data**

The screenshot shows the FLISR Data Mapping Tables interface with the title bar "Protocol Services" and "Comms Online". The main area displays "Recloser\_1" with a status of "Deployed". On the left, a sidebar lists "SCADA\_Data" and "FIELD\_Data" sections, with "FIELD\_Data" expanded to show "Breaker\_1", "Switch\_1", and "Concentrator", while "Recloser\_1" is selected and highlighted in green. The right side features a table titled "Binary Inputs" with the following data:

Point Number	Point Name	Point Type	Publication S...	Comment
0	dnp.Recloser_1.52A3P	Binary	status.dnp.3223bee2-	
1	dnp.Recloser_1.79LO3P	Binary	status.dnp.3223bee2-	
2	dnp.Recloser_1.Fault	Binary	status.dnp.3223bee2-	
3	dnp.Recloser_1.RemoteDisabled	Binary	status.dnp.3223bee2-	
4	dnp.Recloser_1.RemoteEnabled	Binary	status.dnp.3223bee2-	
5	dnp.Recloser_1.HotLineTag	Binary	status.dnp.3223bee2-	
6	dnp.Recloser_1.FlirBlock1	Binary	status.dnp.3223bee2-	
7	dnp.Recloser_1.FlirBlock2	Binary	status.dnp.3223bee2-	
8	dnp.Recloser_1.FlirBlock3	Binary	status.dnp.3223bee2-	
9	dnp.Recloser_1.FlirBlock4	Binary	status.dnp.3223bee2-	
10	dnp.Recloser_1.FlirBlock5	Binary	status.dnp.3223bee2-	

**Figure B.5 Recloser Binary Inputs**

The screenshot shows the FLISR Data Mapping Tables interface with the title bar "Protocol Services" and "Comms Online". The main area displays "Recloser\_1" with a status of "Deployed". On the left, a sidebar lists "SCADA\_Data" and "FIELD\_Data" sections, with "FIELD\_Data" expanded to show "Breaker\_1", "Switch\_1", and "Concentrator", while "Recloser\_1" is selected and highlighted in green. The right side features a table titled "Binary Outputs" with the following data:

Point Number	Point Name	Point Type	Control Model
0	dnp.Recloser_1.OpenCommand	Binary	Pulse On/Off
1	dnp.Recloser_1.CloseCommand	Binary	Pulse On/Off

**Figure B.6 Recloser Binary Outputs**

## Switch

The types of data points FLISR requires and does not require for a switch are shown in *Table B.3*.

**Table B.3 Switch Device Data**

Name	Description	Type	Required for FLISR
IA	A-phase current	Analog Input <sup>a</sup>	Yes, if property is set in PSM <i>Table 3.27</i> .
IB	B-phase current	Analog Input <sup>a</sup>	Yes, if property is set in PSM <i>Table 3.27</i> .
IC	C-phase current	Analog Input <sup>a</sup>	Yes, if property is set in PSM <i>Table 3.27</i> .
VASet1	A-phase voltage, PT Set 1	Analog Input <sup>a</sup>	Yes, if property is set in PSM <i>Table 3.27</i> .
VBSel1	B-phase voltage, PT Set 1	Analog Input <sup>a</sup>	Yes, if property is set in PSM <i>Table 3.27</i> .
VCSel1	C-phase voltage, PT Set 1	Analog Input <sup>a</sup>	Yes, if property is set in PSM <i>Table 3.27</i> .
VASet2	A-phase voltage, PT Set 2	Analog Input <sup>a</sup>	Yes, if property is set in PSM <i>Table 3.27</i> .
VBSel2	B-phase voltage, PT Set 2	Analog Input <sup>a</sup>	Yes, if property is set in PSM <i>Table 3.27</i> .
VCSel2	C-phase voltage, PT Set 2	Analog Input <sup>a</sup>	Yes, if property is set in PSM <i>Table 3.27</i> .
52A3P	Three-phase breaker position	Binary Input <sup>b</sup>	Yes, if property is set in PSM <i>Table 3.27</i> .
Fault	Fault indication	Binary Input <sup>b</sup>	Yes, if property is set in PSM <i>Table 3.27</i> .
RemoteDisabled	Remote control disabled	Binary Input <sup>b</sup>	No
RemoteEnabled	Remote control enabled	Binary Input <sup>b</sup>	No
HotLineTag	Hot-line service tag	Binary Input <sup>b</sup>	No
Online	Device communication is good	Binary Input <sup>b</sup>	Yes, if data concentration is used
OpenCommand	Device open command	Binary Output <sup>c</sup>	No
CloseCommand	Device close command	Binary Output <sup>c</sup>	No
FlisrBlock1	Customizable FLISR block point 1. The associated feeder automatically blocks FLISR operation when this point is asserted.	Binary Input <sup>b</sup>	No
FlisrBlock2	Customizable FLISR block point 2. The associated feeder automatically blocks FLISR operation when this point is asserted.	Binary Input <sup>b</sup>	No

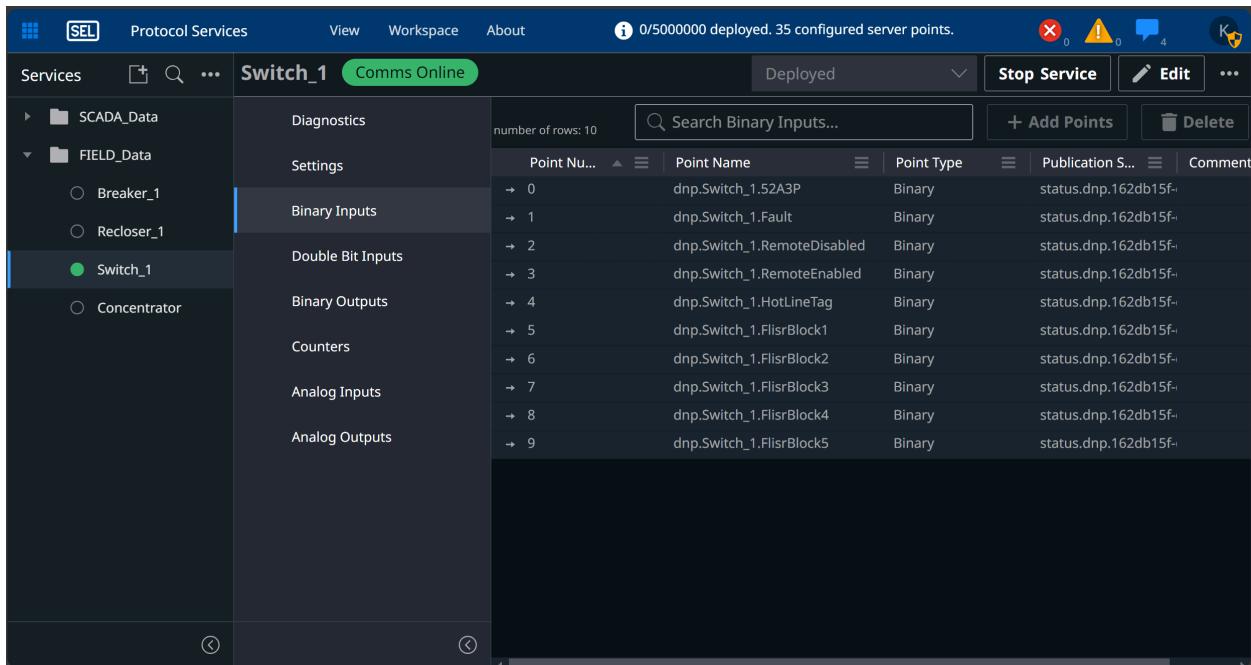
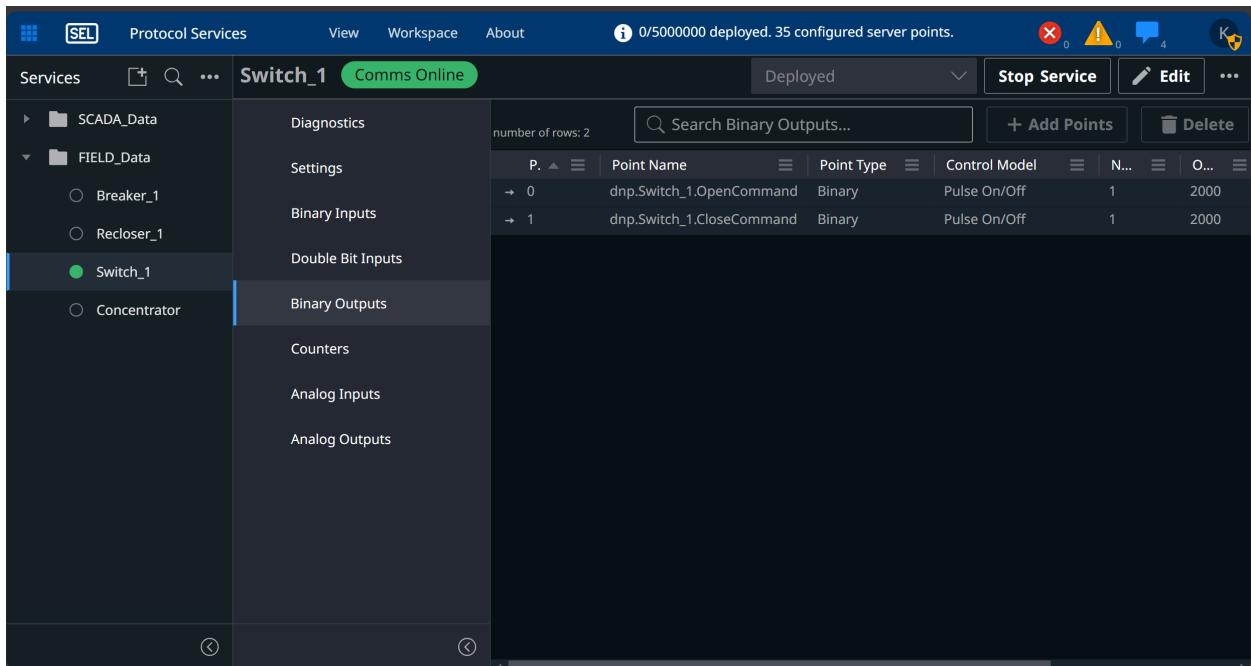
**Field Data**

Name	Description	Type	Required for FLISR
FlisrBlock3	Customizable FLISR block point 3. The associated feeder automatically blocks FLISR operation when this point is asserted.	Binary Input <sup>b</sup>	No
FlisrBlock4	Customizable FLISR block point 4. The associated feeder automatically blocks FLISR operation when this point is asserted.	Binary Input <sup>b</sup>	No
FlisrBlock5	Customizable FLISR block point 5. The associated feeder automatically blocks FLISR operation when this point is asserted.	Binary Input <sup>b</sup>	No

<sup>a</sup>Shown in Figure B.7.<sup>b</sup>Shown in Figure B.8.<sup>c</sup>Shown in Figure B.18.

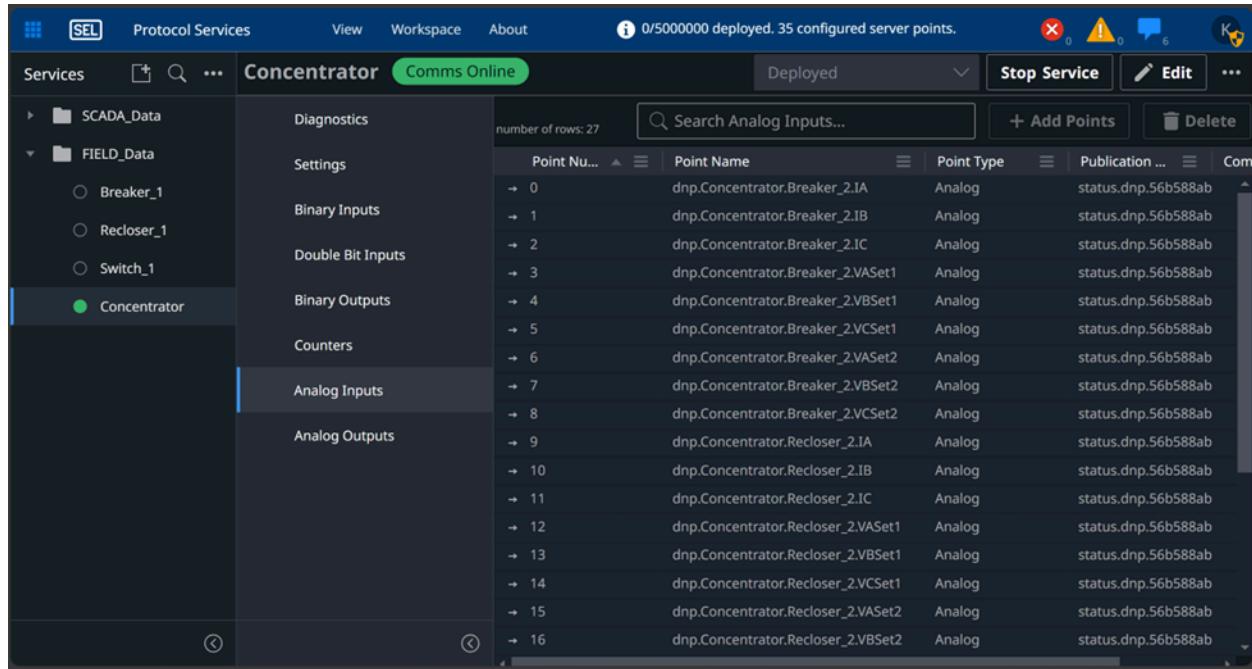
Point Nu...	Point Name	Point Type	Publication S...
0	dnp.Switch_1.IA	Analog	status.dnp.162db15f-
1	dnp.Switch_1.IB	Analog	status.dnp.162db15f-
2	dnp.Switch_1.IC	Analog	status.dnp.162db15f-
3	dnp.Switch_1.VASet1	Analog	status.dnp.162db15f-
4	dnp.Switch_1.VBSet1	Analog	status.dnp.162db15f-
5	dnp.Switch_1.VCSet1	Analog	status.dnp.162db15f-
6	dnp.Switch_1.VASet2	Analog	status.dnp.162db15f-
7	dnp.Switch_1.VBSet2	Analog	status.dnp.162db15f-
8	dnp.Switch_1.VCSet2	Analog	status.dnp.162db15f-

**Figure B.7 Switch Analog Input**

**Figure B.8** Switch Binary Inputs**Figure B.9** Switch Binary Outputs

## Concentrator

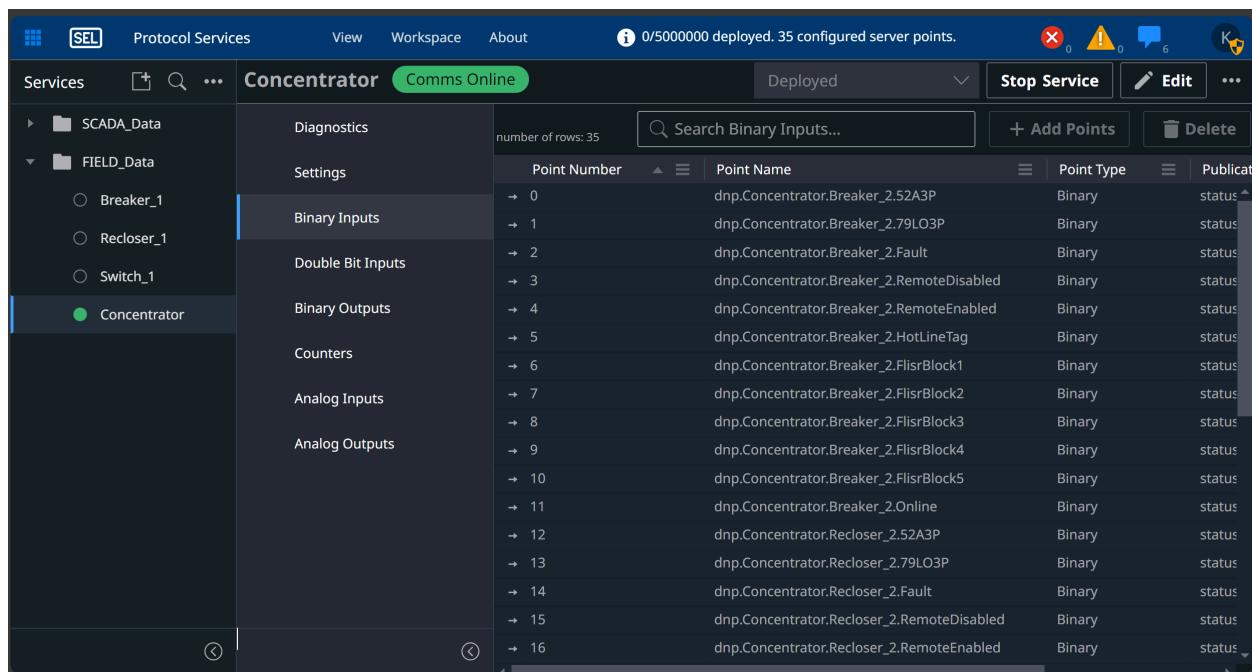
When using concentrators, the data from many assets can be collected by using one client connection. The data maps stack information from each of the assets under that concentrator. FLISR allows the same data points presented in *Table B.1–Table B.3*, and an online point indicating the status of the communication between the concentrator and the asset becomes required. *Figure B.10–Figure B.12* show the various inputs as they appear in the device.



The screenshot shows the 'Concentrator' tab selected in the top navigation bar. On the left, a sidebar lists 'SCADA\_Data' and 'FIELD\_Data' sections, with 'Concentrator' currently selected. The main pane displays a table titled 'Analog Inputs' with the following columns: Point Number, Point Name, Point Type, and Publication. There are 17 rows of data, indexed from 0 to 16.

	Point Nu...	Point Name	Point Type	Publication ...
→ 0	dnp.Concentrator.Breaker_2.IA	Analog	status.dnp.56b588ab	
→ 1	dnp.Concentrator.Breaker_2.IB	Analog	status.dnp.56b588ab	
→ 2	dnp.Concentrator.Breaker_2.IC	Analog	status.dnp.56b588ab	
→ 3	dnp.Concentrator.Breaker_2.VASet1	Analog	status.dnp.56b588ab	
→ 4	dnp.Concentrator.Breaker_2.VBSet1	Analog	status.dnp.56b588ab	
→ 5	dnp.Concentrator.Breaker_2.VCSet1	Analog	status.dnp.56b588ab	
→ 6	dnp.Concentrator.Breaker_2.VASet2	Analog	status.dnp.56b588ab	
→ 7	dnp.Concentrator.Breaker_2.VBSet2	Analog	status.dnp.56b588ab	
→ 8	dnp.Concentrator.Breaker_2.VCSet2	Analog	status.dnp.56b588ab	
→ 9	dnp.Concentrator.Recloser_2.IA	Analog	status.dnp.56b588ab	
→ 10	dnp.Concentrator.Recloser_2.IB	Analog	status.dnp.56b588ab	
→ 11	dnp.Concentrator.Recloser_2.IC	Analog	status.dnp.56b588ab	
→ 12	dnp.Concentrator.Recloser_2.VASet1	Analog	status.dnp.56b588ab	
→ 13	dnp.Concentrator.Recloser_2.VBSet1	Analog	status.dnp.56b588ab	
→ 14	dnp.Concentrator.Recloser_2.VCSet1	Analog	status.dnp.56b588ab	
→ 15	dnp.Concentrator.Recloser_2.VASet2	Analog	status.dnp.56b588ab	
→ 16	dnp.Concentrator.Recloser_2.VBSet2	Analog	status.dnp.56b588ab	

**Figure B.10 Concentrator Analog Inputs**



The screenshot shows the 'Concentrator' tab selected in the top navigation bar. On the left, a sidebar lists 'SCADA\_Data' and 'FIELD\_Data' sections, with 'Concentrator' currently selected. The main pane displays a table titled 'Binary Inputs' with the following columns: Point Number, Point Name, Point Type, and Publication. There are 17 rows of data, indexed from 0 to 16.

	Point Number	Point Name	Point Type	Publication
→ 0	dnp.Concentrator.Breaker_2.52A3P	Binary	status	
→ 1	dnp.Concentrator.Breaker_2.79LO3P	Binary	status	
→ 2	dnp.Concentrator.Breaker_2.Fault	Binary	status	
→ 3	dnp.Concentrator.Breaker_2.RemoteDisabled	Binary	status	
→ 4	dnp.Concentrator.Breaker_2.RemoteEnabled	Binary	status	
→ 5	dnp.Concentrator.Breaker_2.HotLineTag	Binary	status	
→ 6	dnp.Concentrator.Breaker_2.FlsrBlock1	Binary	status	
→ 7	dnp.Concentrator.Breaker_2.FlsrBlock2	Binary	status	
→ 8	dnp.Concentrator.Breaker_2.FlsrBlock3	Binary	status	
→ 9	dnp.Concentrator.Breaker_2.FlsrBlock4	Binary	status	
→ 10	dnp.Concentrator.Breaker_2.FlsrBlock5	Binary	status	
→ 11	dnp.Concentrator.Breaker_2.Online	Binary	status	
→ 12	dnp.Concentrator.Recloser_2.52A3P	Binary	status	
→ 13	dnp.Concentrator.Recloser_2.79LO3P	Binary	status	
→ 14	dnp.Concentrator.Recloser_2.Fault	Binary	status	
→ 15	dnp.Concentrator.Recloser_2.RemoteDisabled	Binary	status	
→ 16	dnp.Concentrator.Recloser_2.RemoteEnabled	Binary	status	

**Figure B.11 Concentrator Binary Inputs**

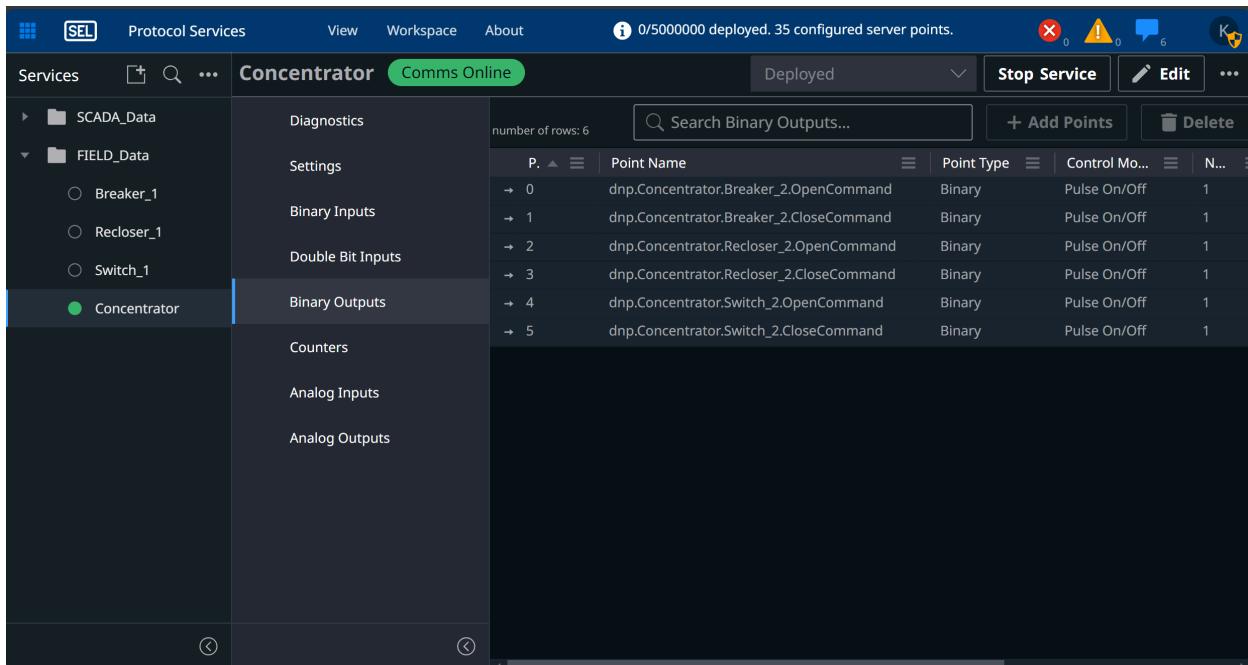


Figure B.12 Concentrator Binary Outputs

## SCADA Data

### NOTE

All binary outputs in Table B.6 and Table B.7 must use the operPulse control model.

FLISR uses protocol service DNP3 to establish a server connection with SCADA. The server makes the collected field data and FLISR statuses available and receives feeder-by-feeder commands.

SCADA data comes from the supervisory system representing the operator controls. To obtain SCADA data, FLISR relies on server connections configured in Protocol Services. The connection is usually individual but can be defined based on system hierarchy. Each type of asset has specific data points that can be integrated with SCADA. In addition, all collected field data can be made available to SCADA through server connections.

## Breaker

The types of data points SCADA requires and does not require for a breaker are shown in *Table B.4*.

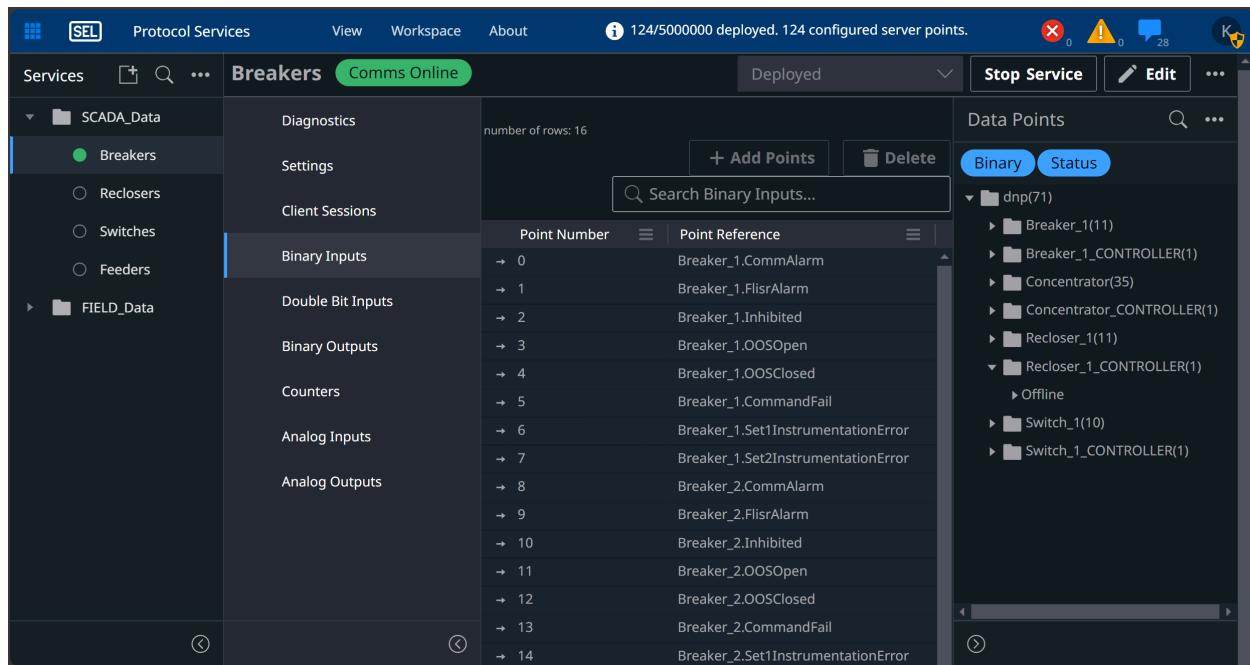
Table B.4 Breaker SCADA Data

Name	Description	Type	Required for FLISR
OvercurrentReported	Fault latch bit that FLISR internally generates.	Binary Input <sup>a</sup>	No
CommAlarm	Device communications status	Binary Input <sup>a</sup>	No

Name	Description	Type	Required for FLISR
FlisrAlarm	FLISR has detected a problem with this device	Binary Input <sup>a</sup>	No
Inhibited	FLISR control of device is inhibited	Binary Input <sup>a</sup>	No
OOSOpen	FLISR is treating this device as Out of Service Open	Binary Input <sup>a</sup>	No
OOSClosed	FLISR is treating this device as Out of Service Closed	Binary Input <sup>a</sup>	No
CommandFail	Open or close commands to the device from FLISR have failed	Binary Input <sup>a</sup>	No
InServiceCommand	Commands FLISR to treat the device as In Service	Binary Output <sup>b</sup>	No
InhibitControlCommand	Commands FLISR to treat the device as Control Inhibited	Binary Output <sup>b</sup>	No
OOSOpenCommand	Commands FLISR to treat the device as Out of Service Open	Binary Output <sup>b</sup>	No
OOSClosedCommand	Commands FLISR to treat the device as Out of Service Closed	Binary Output <sup>b</sup>	No
Set1InstrumentationError	Indicates an instrumentation error was detected on PT(s) on Set 1	Binary Input <sup>a</sup>	No
Set2InstrumentationError	Indicates an instrumentation error was detected on PT(s) on Set 2	Binary Input <sup>a</sup>	No

<sup>a</sup>Shown in Figure B.13.

<sup>b</sup>Shown in Figure B.14.



**Figure B.13 SCADA Breaker Binary Inputs**

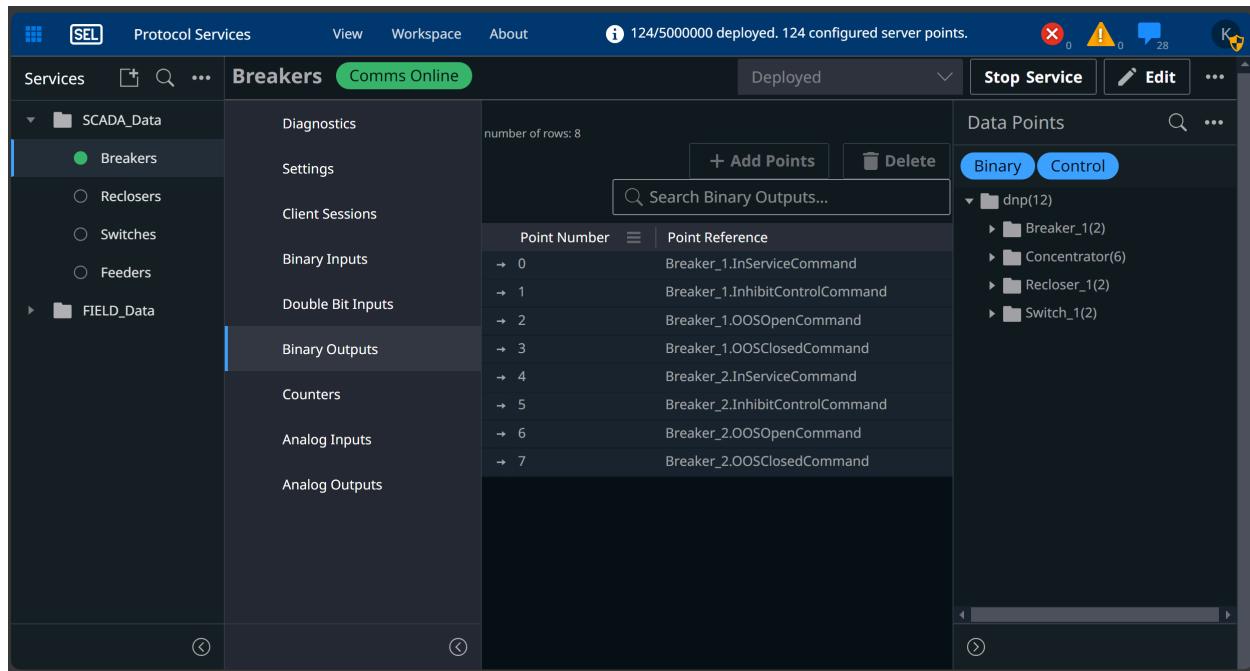


Figure B.14 SCADA Breaker Binary Outputs

## Recloser

The types of data points SCADA requires and does not require for a recloser are shown in *Table B.5*.

Table B.5 Recloser SCADA Data

Name	Description	Type	Required for FLISR
OvercurrentReported	Fault latch bit that FLISR internally generates.	Binary Input <sup>a</sup>	No
CommAlarm	Device communications status	Binary Input <sup>a</sup>	No
FlisrAlarm	FLISR has detected a problem with this device	Binary Input <sup>a</sup>	No
Inhibited	FLISR control of device is inhibited	Binary Input <sup>a</sup>	No
OOSOpen	FLISR is treating this device as Out of Service Open	Binary Input <sup>a</sup>	No
OOSClosed	FLISR is treating this device as Out of Service Closed	Binary Input <sup>a</sup>	No
CommandFail	Open or close commands to the device from FLISR have failed	Binary Input <sup>a</sup>	No
InServiceCommand	Commands FLISR to treat the device as In Service	Binary Output <sup>b</sup>	No
InhibitControlCommand	Commands FLISR to treat the device as Control Inhibited	Binary Output <sup>b</sup>	No
OOSOpenCommand	Commands FLISR to treat the device as Out of Service Open	Binary Output <sup>b</sup>	No
OOSClosedCommand	Commands FLISR to treat the device as Out of Service Closed	Binary Output <sup>b</sup>	No
Set1InstrumentationError	Indicates an instrumentation error was detected on PT(s) on Set 1	Binary Input <sup>a</sup>	No

Name	Description	Type	Required for FLISR
Set2InstrumentationError	Indicates an instrumentation error was detected on PT(s) on Set 2	Binary Input <sup>a</sup>	No

<sup>a</sup>Shown in Figure B.15.

<sup>b</sup>Shown in Figure B.16.

The screenshot shows the SCADA Recloser Binary Inputs configuration screen. The left sidebar lists categories: SCADA\_Data (Breakers, Reclosers, Switches, Feeders), FIELD\_Data. The main area has tabs: Diagnostics, Settings, Client Sessions, and Binary Inputs (selected). A table lists 16 binary inputs:

Point Number	Point Reference
→ 0	Recloser_1.CommAlarm
→ 1	Recloser_1.FlsrAlarm
→ 2	Recloser_1.Inhibited
→ 3	Recloser_1.OOSOpen
→ 4	Recloser_1.OOSClosed
→ 5	Recloser_1.CommandFail
→ 6	Recloser_1.Set1InstrumentationError
→ 7	Recloser_1.Set2InstrumentationError
→ 8	Recloser_2.CommAlarm
→ 9	Recloser_2.FlsrAlarm
→ 10	Recloser_2.Inhibited
→ 11	Recloser_2.OOSOpen
→ 12	Recloser_2.OOSClosed
→ 13	Recloser_2.CommandFail
→ 14	Recloser_2.Set1InstrumentationError

The right panel shows a tree view of data points under 'dnp(71)' and a 'Data Points' section with 'Binary' and 'Status' tabs.

**Figure B.15 SCADA Recloser Binary Inputs**

The screenshot shows the SCADA Recloser Binary Outputs configuration screen. The left sidebar lists categories: SCADA\_Data (Breakers, Reclosers, Switches, Feeders), FIELD\_Data. The main area has tabs: Diagnostics, Settings, Client Sessions, and Binary Outputs (selected). A table lists 8 binary outputs:

Point Number	Point Reference	Point Type
→ 0	Recloser_1.InServiceCommand	Binary
→ 1	Recloser_1.InhibitControlCommand	Binary
→ 2	Recloser_1.OOSOpenCommand	Binary
→ 3	Recloser_1.OOSClosedCommand	Binary
→ 4	Recloser_2.InServiceCommand	Binary
→ 5	Recloser_2.InhibitControlCommand	Binary
→ 6	Recloser_2.OOSOpenCommand	Binary
→ 7	Recloser_2.OOSClosedCommand	Binary

The right panel shows a tree view of data points under 'dnp(12)' and a 'Data Points' section with 'Binary' and 'Control' tabs.

**Figure B.16 SCADA Recloser Binary Outputs**

# Switch

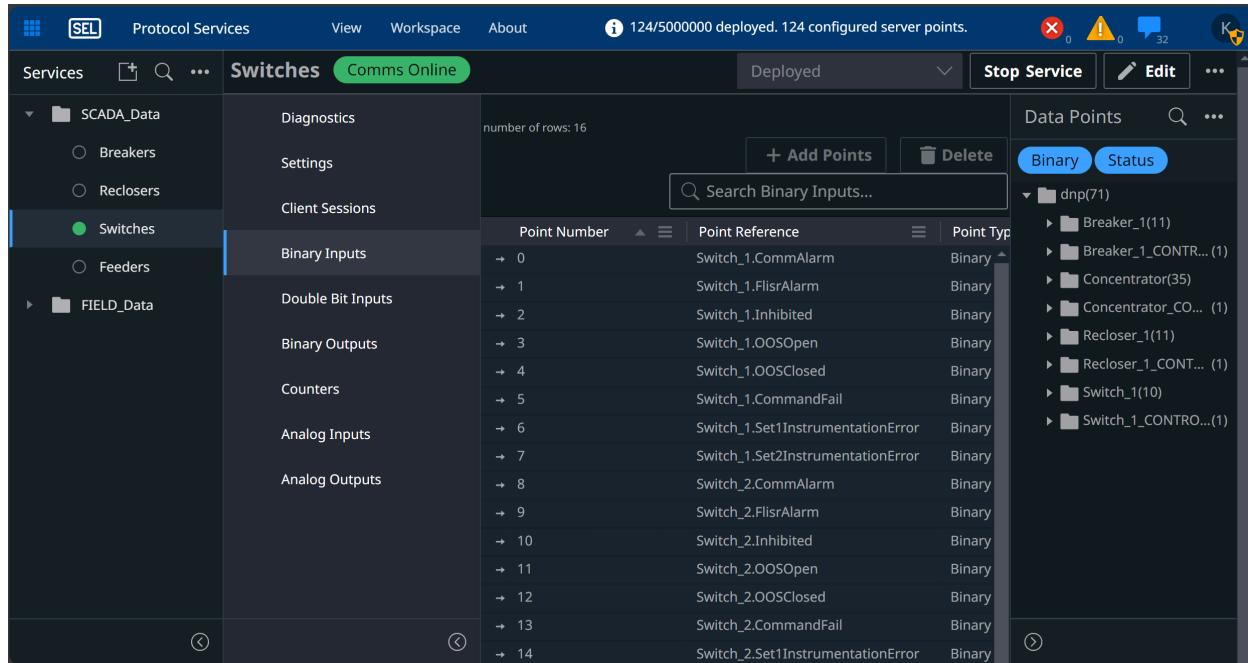
The types of data points SCADA requires and does not require for a switch are shown in *Table B.6*.

**Table B.6 Switch SCADA Data**

Name	Description	Type	Required for FLISR
OvercurrentReported	Fault latch bit that FLISR internally generates.	Binary Input <sup>a</sup>	No
CommAlarm	Device communications status	Binary Input <sup>a</sup>	No
FlisrAlarm	FLISR has detected a problem with this device	Binary Input <sup>a</sup>	No
Inhibited	FLISR control of device is inhibited	Binary Input <sup>a</sup>	No
OOSOpen	FLISR is treating this device as Out of Service Open	Binary Input <sup>a</sup>	No
OOSClosed	FLISR is treating this device as Out of Service Closed	Binary Input <sup>a</sup>	No
CommandFail	Open or close commands to the device from FLISR have failed	Binary Input <sup>a</sup>	No
InServiceCommand	Commands FLISR to treat the device as In Service	Binary Output <sup>b</sup>	No
InhibitControlCommand	Commands FLISR to treat the device as Control Inhibited	Binary Output <sup>b</sup>	No
OOSOpenCommand	Commands FLISR to treat the device as Out of Service Open	Binary Output <sup>b</sup>	No
OOSClosedCommand	Commands FLISR to treat the device as Out of Service Closed	Binary Output <sup>b</sup>	No
Set1InstrumentationError	Indicates an instrumentation error was detected on PT(s) on Set 1	Binary Input <sup>a</sup>	No
Set2InstrumentationError	Indicates an instrumentation error was detected on PT(s) on Set 2	Binary Input <sup>a</sup>	No

<sup>a</sup>Shown in Figure B.17.

<sup>b</sup>Shown in Figure B.18.

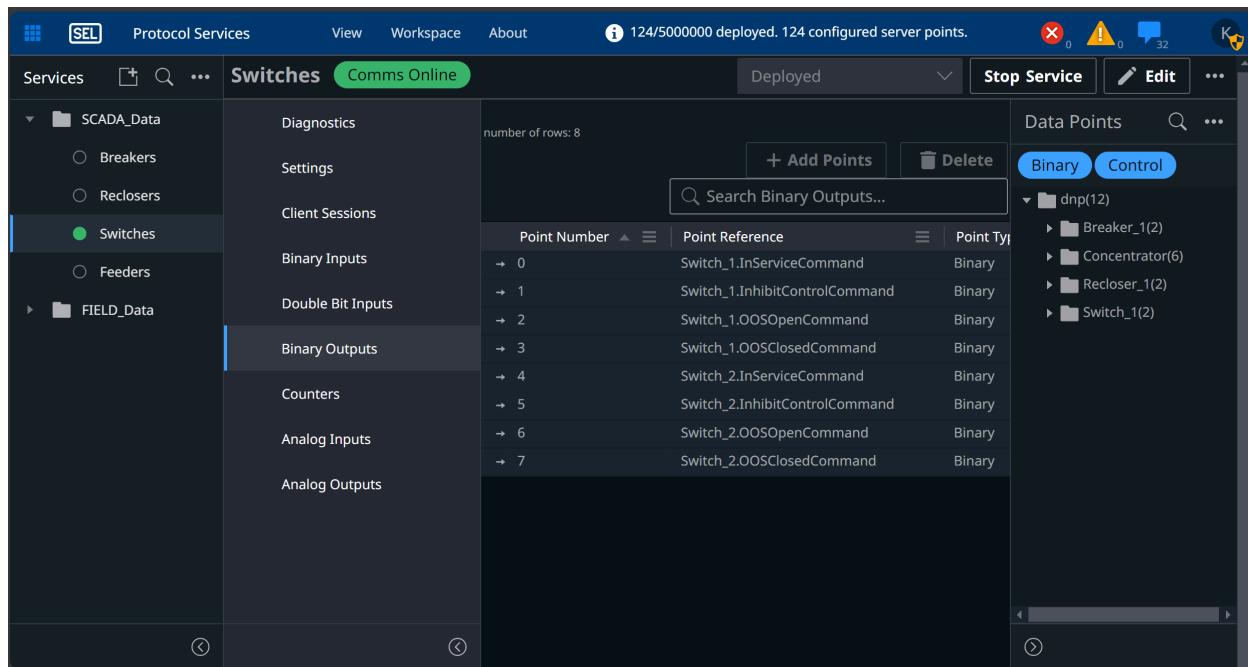


The screenshot shows the FLISR SCADA interface with the 'Switches' tab selected. The left sidebar shows categories: SCADA\_Data (Breakers, Reclosers, Switches, Feeders), FIELD\_Data. The main area has tabs: Diagnostics, Settings, Client Sessions, Binary Inputs, Double Bit Inputs, Binary Outputs, Counters, Analog Inputs, Analog Outputs. The 'Binary Inputs' tab is active, showing 16 rows of data:

Point Number	Point Reference	Point Type
0	Switch_1.CommAlarm	Binary
1	Switch_1.FlIsrAlarm	Binary
2	Switch_1.Inhibited	Binary
3	Switch_1.OOSOpen	Binary
4	Switch_1.OOSClosed	Binary
5	Switch_1.CommandFail	Binary
6	Switch_1.Set1InstrumentationError	Binary
7	Switch_1.Set2InstrumentationError	Binary
8	Switch_2.CommAlarm	Binary
9	Switch_2.FlIsrAlarm	Binary
10	Switch_2.Inhibited	Binary
11	Switch_2.OOSOpen	Binary
12	Switch_2.OOSClosed	Binary
13	Switch_2.CommandFail	Binary
14	Switch_2.Set1InstrumentationError	Binary

The right panel shows 'Data Points' with a 'Binary' tab selected, displaying a tree view of configured server points under 'dnp(71)'.

**Figure B.17 SCADA Switch Binary Inputs**



The screenshot shows the FLISR SCADA interface with the 'Switches' tab selected. The left sidebar shows categories: SCADA\_Data (Breakers, Reclosers, Switches, Feeders), FIELD\_Data. The main area has tabs: Diagnostics, Settings, Client Sessions, Binary Inputs, Double Bit Inputs, Binary Outputs, Counters, Analog Inputs, Analog Outputs. The 'Binary Outputs' tab is active, showing 8 rows of data:

Point Number	Point Reference	Point Type
0	Switch_1.InServiceCommand	Binary
1	Switch_1.InhibitControlCommand	Binary
2	Switch_1.OOSOpenCommand	Binary
3	Switch_1.OOSClosedCommand	Binary
4	Switch_2.InServiceCommand	Binary
5	Switch_2.InhibitControlCommand	Binary
6	Switch_2.OOSOpenCommand	Binary
7	Switch_2.OOSClosedCommand	Binary

The right panel shows 'Data Points' with a 'Control' tab selected, displaying a tree view of configured server points under 'dnp(12)'.

**Figure B.18 SCADA Switch Binary Outputs**

## Feeder

In addition to the asset data, FLISR has internal data points for feeders. These points can be integrated with SCADA to display alarms, receive feeder-level commands to arm or disarm the feeder, return the feeder to normal, and reset the feeder targets.

The types of data points SCADA requires and does not require for a feeder are shown in *Table B.7* and *Table B.6*.

**Table B.7 Feeder SCADA Data**

Name	Description	Type	Required for FLISR
Armed	FLISR feeder is armed	Binary Input <sup>a</sup>	No
FieldConditionBlockAlarm	FLISR is blocking itself from operating because of a field device condition	Binary Input <sup>a</sup>	No
LoopAlarm	FLISR is blocking itself from operating because of an electrical loop on the feeder	Binary Input <sup>a</sup>	No
EventDetected	FLISR has detected an event	Binary Input <sup>a</sup>	No
PermanentFaultDetected	FLISR has detected a permanent fault	Binary Input <sup>a</sup>	No
MiscoordinationDetected	FLISR has detected a miscoordination	Binary Input <sup>a</sup>	No
Reconfiguring	FLISR is reconfiguring the feeder	Binary Input <sup>a</sup>	No
ReconfigComplete	FLISR has successfully reconfigured the feeder	Binary Input <sup>a</sup>	No
ReconfigFail	FLISR has failed to reconfigure the feeder	Binary Input <sup>a</sup>	No
RTN	Commands FLISR to return the feeder to its normal state	Binary Output <sup>b</sup>	No
Arm	Arms FLISR	Binary Output <sup>b</sup>	No
Disarm	Disarms FLISR	Binary Output <sup>b</sup>	No
FlisrTargetReset	Resets FLISR status indicators on the feeder	Binary Output <sup>b</sup>	No
VoltageEventDetected	Indicates that an open phase, loss-of-source or measurement error has been detected.	Binary Input <sup>a</sup>	No
OpenPhaseDetected	Gets published in addition to VoltageEventDetected if the event is determined to be an open phase.	Binary Input <sup>a</sup>	No
InstrumentationError	Gets published in addition to VoltageEventDetected if the event is determined to be a voltage measurement error.	Binary Input <sup>a</sup>	No
LossOfSourceDetected	Gets published in addition to VoltageEventDetected if the event is determined to be a loss-of-source (loss of voltage starting upstream of the breaker).	Binary Input <sup>a</sup>	No

<sup>a</sup>Shown in Figure B.19.

<sup>b</sup>Shown in Figure B.20.

### NOTE

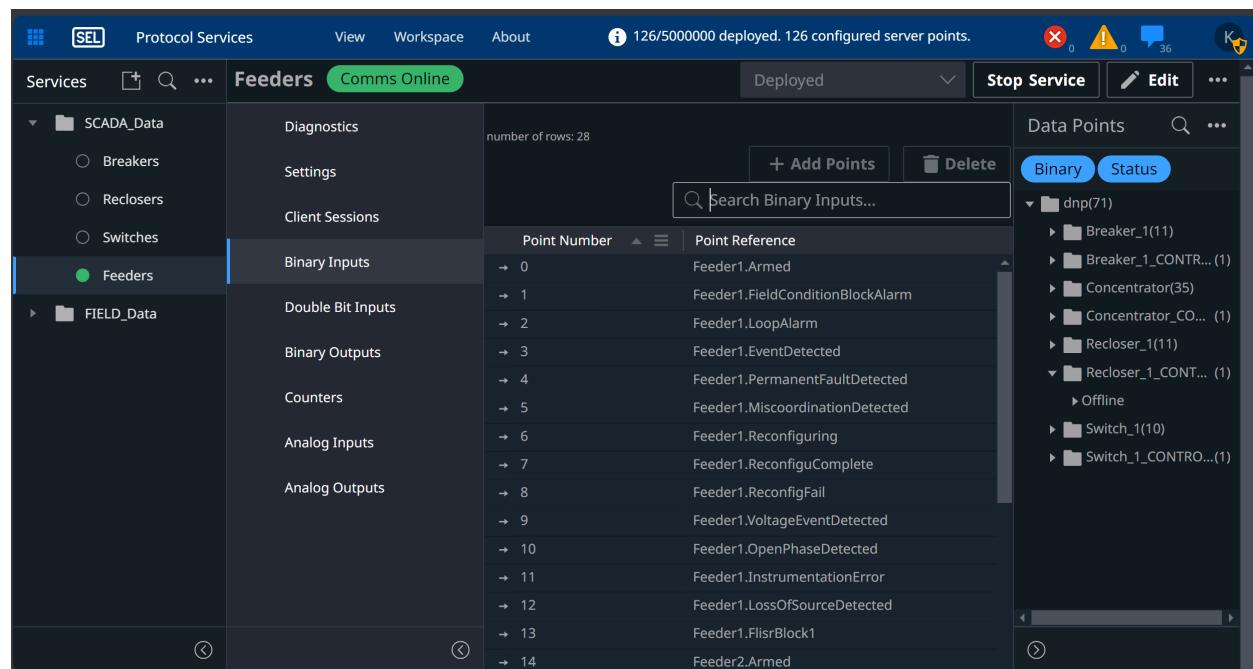
Currently asserted values of ReconfigComplete and ReconfigFail will keep their asserted value until a Target Reset command is sent or a new FLISR event occurs.

**Table B.8 Status Supervisor Data**

Setting Name	Description	Type	Required for FLISR
<Feedername>.FlisrBlock1	Customizable FLISR block point 1. The associated feeder automatically blocks FLISR operation when this point is asserted.	Binary Input <sup>a</sup>	No
<Feedername>.FlisrBlock2	Customizable FLISR block point 2. The associated feeder automatically blocks FLISR operation when this point is asserted.	Binary Input <sup>a</sup>	No

Setting Name	Description	Type	Required for FLISR
<Feedername>.FlisrBlock3	Customizable FLISR block point 3. The associated feeder automatically blocks FLISR operation when this point is asserted.	Binary Input <sup>a</sup>	No
<Feedername>.FlisrBlock4	Customizable FLISR block point 4. The associated feeder automatically blocks FLISR operation when this point is asserted.	Binary Input <sup>a</sup>	No
<Feedername>.FlisrBlock5	Customizable FLISR block point 5. The associated feeder automatically blocks FLISR operation when this point is asserted.	Binary Input <sup>a</sup>	No

<sup>a</sup>Shown in Figure B.19.



**Figure B.19 SCADA Feeder Binary Outputs**

The screenshot shows the 'Feeder' tab of the 'Data Points' section in the FLISR Data Mapping Tables software. The left sidebar shows categories like 'SCADA\_Data' (Breakers, Reclosers, Switches, Feeders), 'FIELD\_Data', and 'Data Sources'. The main area displays a table of binary outputs:

Point Number	Point Reference	Point Type
→ 0	Feeder1.RTN	Binary
→ 1	Feeder1.Arm	Binary
→ 2	Feeder1.Disarm	Binary
→ 3	Feeder1.FlisrTargetReset	Binary
→ 4	Feeder2.RTN	Binary
→ 5	Feeder2.Arm	Binary
→ 6	Feeder2.Disarm	Binary
→ 7	Feeder2.FlisrTargetReset	Binary

On the right, there's a tree view under 'dnp(12)' showing 'Breaker\_1(2)', 'Concentrator(6)', 'Recloser\_1(2)', and 'Switch\_1(2)'. The top status bar indicates '126/5000000 deployed. 126 configured server points.'

Figure B.20 SCADA Feeder Binary Outputs

**This page intentionally left blank**

---

---

## A P P E N D I X   C

---

# Cybersecurity Features

## Security Environment

---

Distribution Management System is designed to control and optimize electrical distribution systems in a secure substation or distribution SCADA environment. See *Appendix B: Cybersecurity Features* in the Blueframe instruction manual for further details on Blueframe cybersecurity features.

## Version Information

---

DMS application packages provide version information through the Blueframe Application Management tool. See *Appendix A: Software and Manual Versions* for details on obtaining version information.

## Installation Characteristics

---

### Container Technology

Blueframe uses container-based technology and orchestration to increase system performance, resilience, scalability, and efficiency by deploying applications and services as they are required. Deployment of DMS within Blueframe involves several containers securely operating together. Should a DMS service unexpectedly stop, the Blueframe orchestration system attempts to automatically restart the service and return the application suite to full functionality.

## Ports

---

### Logical Ports

DMS uses instance-specific internal ports for normal operation. These ports are not externally available. DMS communicates with external devices via DNP3, a protocol provided by the Protocol Services application. The ports used when establishing a DNP3 connection to external devices are dependent on user configuration.

## Access Control

---

Users access DMS applications according to their role privileges assigned in User Management (a Blueframe core service). Roles are defined with specific application access on a "Can Launch" and "Can Manage" basis. A user account can be tied to a corporate Lightweight Directory Access Protocol (LDAP) or create it as a local Blueframe account.

In addition to "Can Launch," and "Can Manage," DMS provides the following permissions:

- **Can Operate.** This permission allows the user to perform the following actions:
  - Issue Return to Normal controls
  - Arm and disarm feeders
  - Set the availability of a device
  - Issue a target reset to FLISR
- **Can Return to Normal.** This permission allows the user to issue a Return to Normal command from the FLISR user interface. It requires the Can Operate permission.
- **Can Commission.** This permission allows the user to send Open and Close controls to field devices for commissioning and testing purposes. It requires the Can Operate permission.
  - Commission a feeder
  - Deactivate a feeder
  - Inherits "Can Operate" permissions

All account credentials are user-defined and are securely stored in the Blueframe application platform. A Blueframe system administrator can specify credential requirements in User Management. See *User Management* in the Blueframe instruction manual for details on configuring credential requirements. MDI is a utility application for PSM. Access to MDI requires "Can Launch" and "Can Manage" permissions for both the PSM and MDI applications.

## Backup and Restore

---

DMS configuration backup and restore occurs through the Blueframe System Settings Backup and Restore tool. For more information on this process, see *System Settings* in the Blueframe instruction manual.

Additionally, you can save feeder canvas configurations from PSM for backup, archival, or for moving to another Blueframe instance. This is achieved by selecting File > Export Project. This prepares all configured feeder configurations in a single file that is downloaded via the web browser. You can import this configuration on another instance of PSM.

### NOTE

Ensure both instances of Blueframe are using the same PSM version before attempting to transfer settings.

## Revision Management

---

*Appendix A: Software and Manual Versions* contains a description of each software update.

See *The SEL Process of Disclosing Security Vulnerabilities* at [selinc.com/security\\_vulnerabilities/](http://selinc.com/security_vulnerabilities/) for details on vulnerability disclosure.

## Software Updates

The application package versions available in DMS are updated through Blueframe Application Management. See *Appendix A: Software and Manual Versions* for details on locating specific version information.

## Software Update Verification

DMS application packages are signed by SEL. Blueframe only allows SEL signed packages to be installed. For instructions on how to verify the signature, see [selinc.com/company/verifying-software-downloads/](http://selinc.com/company/verifying-software-downloads/).

## Contact SEL

---

For further questions or concerns about product security, contact SEL at [security@selinc.com](mailto:security@selinc.com) or +1.509.332.1890.

**This page intentionally left blank**





SCHWEITZER ENGINEERING LABORATORIES, INC.

2350 NE Hopkins Court • Pullman, WA 99163-5603 U.S.A.

Phone: +1.509.332.1890 • Fax: +1.509.332.7990

[selinc.com](http://selinc.com) • [info@selinc.com](mailto:info@selinc.com)