SL1 PowerFlow Platform Release Notes

Version 2.3.0

Overview

The *SL1 PowerFlow Platform* version 2.3.0 includes security updates for Department of Defense Information Network (DoDIN) certification, new monitoring options on the **PowerFlow Control Tower** page of the PowerFlow user interface, and updates to the PowerFlow builder. This release also adds a number of additional new features and addresses multiple issues.

This document includes the following topics:

Features

This section covers the features that were included in *PowerFlow Platform* version 2.3.0.

DoDIN Certification

- This release of PowerFlow was updated to include numerous security updates for Department of Defense Information Network (DoDIN) certification.
- Reviewed the following Security Technical Implementation Guides (STIGs) and Security Requirements Guides (SRGs) and updated PowerFlow to ensure that it fully satisfies all applicable STIGs and security requirements to make PowerFlow fully DoDIN-compliant:

  - *Oracle Linux 7 Security Technical Implementation Guide*, Version 1, Release: 1 Benchmark Date: 03 Feb 2020
  - *Web Server Security Requirements Guide*, Version 2, Release: 3 Benchmark Date: 26 Apr 2019
  - *Network Infrastructure Policy Security Technical Implementation Guide*, Version 9, Release: 10 Benchmark Date: 24 Jan 2020
  - *Java Runtime Environment (JRE) version 8 STIG for Unix*, Version 1, Release: 3 Benchmark Date: 27 Oct 2017
  - *Database Security Requirements Guide*, Version 2, Release: 10 Benchmark Date: 24 Apr 2020
  - *Application Security and Development Security Technical Implementation Guide*, Version 4, Release: 10 Benchmark Date: 25 Oct 2019

- Reviewed the Docker Enterprise Edition STIGs and updated all areas of the Docker orchestration to make them DoDIN-compliant.
- Ensured that all PowerFlow containers and packages in containers are FIPS-compliant.
- Ensured that data at rest is encrypted, that the web server utilizes FIPS 140-2 approved encryption modules for storing data, and that passwords are saved on the system with an AES-128 algorithm using Cipher Block Chaining (CBC).
- When installing a MUD-enabled PowerFlow system, the password in **is_pass** is encrypted as part of the installation process.
- Added the "Standard Mandatory DoD Notice and Consent Banner", which must be read and acknowledged by all users before they log into the MUD-enabled PowerFlow system.
- When querying the PowerFlow API or accessing the GUI, the **content-type** header responds with **utf-8** as the content type.
- Audit logging for changes and the user making changes to PowerFlow configuration objects, schedules, and other system data was improved for this release. You can change the default log level of 30 (warning) to 10 (debug) or 20 (Informational) for more verbose logs.
- Updated PowerFlow to generate audit logs when successful or unsuccessful logon attempts occur.
- Updated PowerFlow to generate audit logs for the IP addresses of users connecting to that PowerFlow system.

- Additional log information including user-agent, headers, and true source IP address has been added to the nginx (pf-gui) container logs. If your PowerFlow system is in a cluster with a load balancer, the load balancer must provide the client-source IP address as the value for the **proxy_protocol_addr** header.

- When installing on a DoDIN deployment, a grub2 user "isadmin" is automatically created with a grub2 password defined by the user during the installation process.

- Ensured that the Couchbase service could be run when it had the `read_only` flag enabled in the **docker-compose** file.

- Updated the Couchbase configuration in PowerFlow so that it does not use primary indexes in production.

- Updated the /flower/api to prevent standard "view" users from making changes to a running PowerFlow system.

- Added the following configurations to the **/etc/iservices/isconfig.yml** to improve load balancer compatibility if the load balancer sends requests to the client in proxy protocol format like AWS ELB:

    - **LOAD_BALANCED: true**. Setting this value to *true* specifies that the load balancer will send requests to the client in proxy protocol format. This value is *false* by default.

    - **RATE_LIMITED: true**. Setting this value to true enables rate limiting. This value is *false* by default.

    - **RATE_LIMIT_REQUESTS_PER_SECOND: '50'**. This value specifies the number of rate limit requests per second.

    - **RATE_LIMIT_BURST: '100'**. This value specifies the rate limit burst.

    In addition, the exposed ports in the **docker-compose.yml** file were set to **mode: host** to let PowerFlow capture the proper client IP address of the requests being sent into PowerFlow. This setting lets PowerFlow set the proper rate limits and log transactions. This feature does not using the Swarm ingress; as a result, you will need to scale the gui container and place the container in the nodes that will be expecting ingress traffic.

- Updated Redis to allow more than 511 connections for `net.core.somaxconn`, which specifies the maximum number of connections. Also added a new configuration to the **docker-compose** file to allow users to edit the `net.core.somaxconn` value:

```
redis:
    ... ....
    sysctls:
      net.core.somaxconn: '1024'
```

- Ensured that NGINX uses the latest packages and that the modules in use are signed and verified by the original author.

- Calls to the Dex Server from NGINX were configured to stay internal to the Docker overlay network.

- The default Docker log driver in a PowerFlow system is set to **journald**. For more information, see the *SL1 PowerFlow: System Security Plan for Docker Enterprise* guide.

- A login banner containing information specific to DoDIN appears before you log into a PowerFlow system configured for Military Unique Deployment (MUD), including systems that use Common Access Card (CAC) Authentication.

- If a user does not have access or permissions for a specific feature, that feature is grayed out and can't be used by that user.

- Updated iservices to make it the group owner of the **/etc/iservices** directory and files.

- Updated the steprunner startup to allow for debug logging.

- Created the following documents detailing the configuration of PowerFlow for Department of Defense Information Network (DoDIN) certification and Military Unique Deployment (MUD):

  - *Configuring SL1 PowerFlow for Military Unique Deployment (MUD)*

  - *SL1 PowerFlow: System Security Plan for Docker Enterprise*

> **NOTE:** These documents are not public, but you may contact your ScienceLogic contact to request a copy of the documents.

PowerFlow Control Tower

- The **PowerFlow Control Tower** page in the PowerFlow user interface provides visibility into system health and automation health. You can use it to monitor the health of your PowerFlow system and track the PowerFlow applications that you use the most. You can use this information to quickly determine if various components that make up your PowerFlow instance are performing as expected.

> **NOTE:** The **Dashboard** page that was in the PowerFlow user interface before version 2.3.0 was replaced by the **PowerFlow Control Tower** page. The new page includes new widgets along with the widgets from the previous **Dashboard** page.

- The **PowerFlow Control Tower** houses the **System Health** and **Favorite Applications** widgets alongside high-level statistics about the health of the worker services that are being used by the PowerFlow instance.

  - The **System Health** widget lets you see at a glance the health of the various elements of your PowerFlow system.

  - The **Favorite Applications** widget lets you select the PowerFlow applications that are important to you and track their status. You can also run those applications from this widget.

- The **System Health** widget includes the following features:

  - When you select a component in the **Process Flow View** or the **Tabular View** in this widget, the pop-up that displays data for all items in the component. For example, if you select the *Step Runner* component, the pop-up displays data about all of the containers for that component.

  - The pop-up that displays when you select a component in the **System Health** widget includes current status and related information for all containers in that component. The widget includes links to relevant websites for the selected component, such as a link to the Couchbase user interface for the Couchbase component.

  - When a PowerFlow component is down or needs attention, the **System Health** widget displays the component's icon in red, with a red exclamation point next to the component's icon. The red exclamation point also appears in the corresponding line of the **Tabular View**, along with red ovals for the second and third columns of the table.

  - The **Tabular View** of the **System Health** widget contains a column for how long a component has been running as well as a column for replica information.

- The **Favorite Applications** widget includes the following features:

  - From the list of favorite applications, you can view a history of the last run for each application and a list of successful and failed runs. You can also run the application, view the application detail page, and "unfavorite" the application.

  - You can select more than one favorite application and perform the following bulk actions: "Unfavorite" all selected applications or run all selected applications.

  - If a favorite PowerFlow application is deleted, that application is removed from the **Favorite Applications** widget.

  - The number of favorite applications is limited to 16 applications per user.

- The Control Tower feature uses the following items from the *System Utils* Synchronization PowerPack version 1.1.0:

  - The "PowerFlow Control Tower HealthCheck" application. Queries PowerFlow, gathers health data about the system, and displays the data in the PowerFlow System Health widget on the **PowerFlowControl Tower** page.

  - The "PowerFlow Control Tower HealthCheck Configuration Example" configuration object. Contains the structure needed for the "PowerFlow Control Tower HealthCheck" application.

    > **TIP:** Do *not* use the example configuration object to run PowerFlow applications. Make a copy of the configuration object that you can then customize.

  - "Process PowerFlow System Health Status Data" step. Transforms Docker Swarm data into Health Status for the PowerFlow System Health widget.

- Also, the Control Tower requires the *Flow Control* Synchronization PowerPack version 1.0.1 or later.

CAC Authentication

- Enabled administrators to configure Common Access Card (CAC) Authentication with PowerFlow. The CAC Authentication configuration includes the following features:

  - Added new configuration variables for CAC Authentication. For more information, see the *Managing Users* chapter in the ***SL1 PowerFlow Platform*** manual.

  - When you log out of PowerFlow when using CAC authentication, PowerFlow displays a static page stating that you have been logged out.

- When searching CAC using LDAP authentication, added the ability to toggle between *san* and *cn* in the **data/nginx/conf.d/auth.lua** file on the gui container.

Updates to PowerFlow Builder

- The **PowerFlow builder** page in the PowerFlow user interface was updated with new features and enhancements to improve the user experience when creating and editing PowerFlow applications.

- If you are creating or editing a PowerFlow application on the **PowerFlow builder** page, you can hover over a step to see if any parameters for that step need to be configured before you run the application.

- Steps that are attached below a **Condition** operator now display a label that explains the branching for those steps.

- The **Transform** operator process has been improved with additional pop-up messages and additional text in the user interface.

- To prevent errors, the PowerFlow user interface will not let you create a step with a hyphen in its name.

- For the "MySQL Select" step, the "port" field value was changed to an integer from a string to prevent validation issues.

- Two new mapping Step Parameters were added to this release of PowerFlow:

  - MappingParameterMixOneToMany

  - MappingParameterMixOneToOne

  These parameters let you combine the type of options pulled from a URL (cached values) and a list of options defined by a user (custom values). These parameters let one side consume from the cache and let the other side accept custom values.

- Version 1.3.2 of the *Base Steps* Synchronization PowerPack includes three new parameters for the "QueryRest: OAuth" step:

  - ***scopes***: Add a comma-separated list of OAuth2 Scopes.

  - ***refresh_token***: If the authentication flow requires a refresh_token, specify the string in this field.

  - ***additional_auth_arguments***: Specify a dictionary of key/value pairs to add to the authentication form.

Updates to the PowerFlow User Interface

- On the **SyncPacks** page, the toggle for *Show all SyncPacks* was changed to *Toggle Inactive SyncPacks*. By default, this option is enabled so that all available Synchronization PowerPacks are shown on the SyncPacks page. To disable this option, click the Filter icon ( ) and unselect *Toggle Inactive SyncPacks*.

- On the **SyncPacks** page, you can click the dropdown arrow next to the **[Import SyncPack]** button to import or view dependencies for PowerFlowSynchronization PowerPacks.

- On the **SyncPacks** page, you can delete all versions of a specific Synchronization PowerPack, except for the active version.

- When you run a PowerFlow application that uses the **Trigger Application** operator, the PowerFlow user interface checks the status of the triggered application and refreshes the parent PowerFlow application with that status when the triggered application completes. This update takes into account any retries of a triggered application that might have failed on the first try, but succeeds on the first or second retry.

- Additional pop-up messages were added to the PowerFlow user interface to enhance usability.

Session Management in PowerFlow

- The **Admin Panel** page in the PowerFlow user interface now includes a **Session Management** panel that lets a user with the *Administrator* role view all active PowerFlow sessions for all users. The admin user can also end active sessions as needed. Non-admin users can view user sessions, but they cannot end those sessions.

- When an administrator ends a session for a user, that user is redirected to the PowerFlow login page.

- Added new configuration variables to the PowerFlow configuration file **/etc/iservices/isconfig.yml** that let you enable and configure session management, which is disabled by default. For more information, see the "Managing User Sessions" topic in the *Managing Users* chapter of the **SL1 PowerFlow Platform** manual.

- When the number of user sessions is exceeded, the user trying to log in is redirected to a "Session limit has been reached" page, and then the user is returned to the login page.

- Added a GET **/sessions** endpoint that you can use to retrieve a list of sessions for a PowerFlow system and a DELETE **/sessions** endpoint that deletes all sessions in a PowerFlow system. You can also GET and DELETE **/sessions/status**, **/sessions/username/{username}**, and **/sessions/{session_id}**.

Updates to the powerflowcontrol (pfctl) command-line utility

- The **powerflowcontrol** (pfctl) command-line utility was updated with a number of new improvements and features. The **pfctl** utility is included in this version of the PowerFlow platform.

- The **pfctl** utility can check for "Activate/Install Syncpack" steps that have different versions, and the **autoheal** action can remove all but the most recent version of the step.

Run Book Action (RBA) Queue Retries

- Added two new PowerFlow applications to the *System Utils* Synchronization PowerPack version 1.1.2 to handle Run Book Action retries. Using these applications, PowerFlow will pull and retry PowerFlow applications that were not able to be executed by Run Book Actions because PowerFlow was not available. These new applications are:

- Read SL1 RBA queue and retry PowerFlow Applications

- Run PowerFlow Application and remove it from SL1 RBA queue

> **NOTE:** Version 1.1.2 of the *System Utils*Synchronization PowerPack is included in this release
> of the PowerFlow Platform.

- *System Utils* Synchronization PowerPack version 1.1.2 also includes the "PF RBA retry Configuration Example" configuration object. You can make a copy of this example configuration object to use with the two applications listed above.

- This feature also requires the *Base Steps* Synchronization PowerPack version 1.3.2 and later.

- For more information, see the "Enabling Run Book Automation Queue Retries" topic in the *Managing PowerFlow Applications* chapter of the **SL1 PowerFlow Platform** manual.

PowerFlow Backup Enhancements

- The "Integration Service Backup" application now lets you specify the order of the nodes that you are backing up. If one of the nodes fails or is unavailable, the backup application continues down the list of nodes, in top-down order. An error message appears if the first node fails and single_node backup is not selected. The updated version of the "Integration Service Backup" application is available in version 1.1.2 of the *System Utils* Synchronization PowerPack, which also requires *Base Steps* Synchronization PowerPack version 1.3.2.

- The "Integration Service Backup" application now lets you specify the order of the nodes that you are backing up. If one of the nodes fails or is unavailable, the backup application continues down the list of nodes, in top-down order. An error message appears if the first node fails and single_node backup is not selected. The updated version of the "Integration Service Backup" application is available in version 1.1.2 of the *System Utils* Synchronization PowerPack, which also requires Base Steps Synchronization PowerPack version 1.3.2.

- You have the option of running the "Integration Service Backup" application using an SSH key for authentication instead of using a password. The "IS - System Backup Configuration Example" configuration template in version 1.1.2 of the *System Utils* Synchronization PowerPack was updated to include the **remote_ssh_key** Also, the "Integration Service Backup" and "Integration Service Restore" applications were updated to include the following:

  - *use_ssh_key*. Selecting this option on the **Configuration** pane lets you authenticate using a SSH key to the remote system for the backup or where the backup needs to be restored (depending on the PowerFlow application that you are using).

- *remote_ssh_key*. If you selected *use_ssh_key*, specify a valid SSH key string in this field. You can include the value of this variable in the configuration object aligned with the applications, such as *config.remote_ssh_key*. Use the newline character \n/ as a separator.

> **NOTE**: You will need to edit the SSH Key values in the JSON Editor for this release to ensure the key is properly set. This is a known issue that will be addressed in a future release.

> **NOTE**: To get a one-line string of the SSH key, run the following command:
> ```
> sed -E ':a;N;$!ba;s/\r{0,1}\n/\\n/g' ~/.ssh/id_rsa
> ```

- If the SSH key needs a paraphrase to be decrypted, set the paraphrase by creating a *remote_password* variable in the configuration object aligned with the applications.

Additional Features

- Upgraded the version of Redis used by PowerFlow from version 4.0.11 to 6.0.5.

- You can configure Redis to let the **contentapi** container iterate through multiple potential Redis result stores to find the correct result id for a task. To enable this option in the **docker-compose.yml** file, set the **result_backend** environment variable of the **contentapi** container to a comma-delimited list of URLs for Redis instances, such as **redis://redis:6378/0,redis:///redis2:6380/0**. To deploy multiple Redis instances, make sure that the stack deploys the instances with different aliases, ports, and hostnames. Also, multiple backends are only supported on **contentapi**, not the **steprunners**. Steprunners can only write to a single backend.

- To allow RabbitMQ to better handle network connection errors, the following setting was added to the HA policy: **ha_promote_on_shutdown: always**. With this setting enabled, a problematic node automatically restarts itself, and queues migrate to a new node.

- Added a new configuration object called **casbinpolicy** to the **docker-compose.yml** file that lets you load casbin policies from the **/etc/iservices/casbinpolicy.csv** file.

- The following services are included in this release of PowerFlow:

  - **contentapi**. sciencelogic/pf-api:rhel2.3.0ca2
  - **couchbase**. image: sciencelogic/pf-couchbase:6.0.2-5
  - **dexserver**. image: sciencelogic/pf-dex:2.22.0-3
  - **flower**. image: sciencelogic/pf-worker:rhel2.3.0ca2
  - **gui**. image: sciencelogic/pf-gui:2.3.0ca1-ubi7
  - **pypiserver**. image: sciencelogic/pf-pypi:4.8.1-6
  - **rabbitmq**. image: sciencelogic/pf-rabbit:3.8.11-2
  - **redis**. image: sciencelogic/pf-redis:6.0.4-1
  - **scheduler**. image: sciencelogic/pf-worker:rhel2.3.0ca2
  - **steprunner**. image: sciencelogic/pf-worker:rhel2.3.0ca2
  - **syncpacks_steprunner**. image: sciencelogic/pf-worker:rhel2.3.0ca2

> **TIP:** To view release notes and manuals for previous versions of the SL1 PowerFlow Platform and PowerFlow Synchronization PowerPacks, see [SL1 PowerFlow Documentation](#).

Issues Addressed

The following issues were addressed in *PowerFlow Platform* version 2.3.0:

- Addressed an issue where the "Integration Service Backup" application was not creating backups after an upgrade to PowerFlow version 2.2.0. (Case: 00167157. JIRA ID: EM-43884)
- Addressed an issue where the **/var/lib/docker/containers** directory consumed too much space. (Case: 00159613. JIRA ID: EM-42707)
- Improved the default handling of JSON parameters on the **Configuration** pane in the PowerFlow user interface. If you set 'null' as a value for a JSON parameter, the value reverts to its default value, if a default value exists. You can clear JSON parameters by specifying an empty dictionary {} as the value. Also, upgrading or downgrading a Synchronization PowerPack will not overwrite a user configuration. (Case: 00178898. JIRA ID: EM-44534)
- Addressed an issue where triggered applications failed during the first retry and reported back to the parent application that they had failed. As a result, the parent application (and the **Trigger Application** operator in that application) had a status of *Failure* that would not get updated, even if a user refreshed the page and all of the triggered applications succeed after the first retry. (Case: 00124375. JIRA ID: EM-39912)
- Addressed an issue where the **healthcheck** action in the **powerflowcontrol** (pfctl) command-line utility did not report when PowerFlow steprunners stopped processing jobs. (Case: 00137945. JIRA ID: EM-42158)
- Addressed an issue where the **powerflowcontrol** (pfctl) command-line utility failed while checking the VMware host for nodes in an Amazon Web Services (AWS) environment. (Case: 00176726. JIRA ID: EM-44902)

- Addressed an issue where the **Install Time** for a Synchronization PowerPack listed on the **SyncPacks** page of the PowerFlow user interface updated every time the **syncpack_steprunner** service was restarted. (Case: 00159613. JIRA ID: EM-39934)

- Addressed an issue with network connection errors with RabbitMQ by adding the following setting to the HA policy: **ha_promote_on_shutdown: always**. With this setting enabled, a problematic node automatically restarts itself, and queues migrate to a new node. (Case: 00136045. Jira ID: EM-41157)

- Configured broadcast queues so that they are deleted after their worker is restarted. (Case: 00145227. Jira ID: EM-41909)

- Removed nginx version label from HTTP responses for added security. (Case: 00191368. Jira ID: EM-45630).

- Updated PowerFlow to remove all scheduled runs of any PowerFlow applications that were deleted from the system.

Known Issues

This release contains the following known issues:

- If your PowerFlow system uses self-signed certificates, you will need to manually accept the certificate before you can upload Synchronization PowerPacks. Go to **https://<*IP address of PowerFlow*>:3141/isadmin**, accept the certificate, and then log into PowerFlow. After you log in, you will be able to upload Synchronization PowerPacks.

- The *latest* tag does not exist after the initial ISO installation. This situation only affects users with custom services that point to the *latest* tag. To work around this issue, run the tag latest script manually after running the `./pull_start_iservices.sh` command:

```
python /opt/iservices/scripts/system_updates/tag_latest.py
/opt/iservices/scripts/docker-compose.yml
```

System Requirements

> **NOTE**: PowerFlow Platform version 2.2.1 and later requires version 1.3.1 or later of the *Base Steps* Synchronization PowerPack. This version includes an update to the "Query REST" step that prevents issues with scheduled PowerFlow applications. You can download the latest version of this Synchronization PowerPack from the PowerPacks page of the ScienceLogic Support Site.

The PowerFlow platform does not have a specific minimum required version for SL1. However, certain PowerFlow Synchronization PowerPacks have minimum version dependencies. Please see the documentation for those Synchronization PowerPacks for more information on those dependencies.

The following table lists the port access required by PowerFlow:

Source IP	PowerFlow Destination	PowerFlow Source Port	Destination Port	Requirement
PowerFlow	SL1 API	Any	TCP 443	SL1 API Access
SL1 Run Book Action	PowerFlow	Any	TCP 443	Send SL1 data to PowerFlow
Devpi	PowerFlow	Any	TCP 3141	Internal Python package repository for Synchronization PowerPacks; check for self-certification for PowerFlow
Dex Server	PowerFlow	Any	TCP 5556	Enable authentication for PowerFlow
PowerFlow	SL1 Database	Any	TCP 7706	SL1 Database Access
powerflowcontrol (pfctl, formerly called iservicecontrol) command-line utility	PowerFlow	Any	22 (on all host nodes)	Log in and perform admin tasks on nodes
Encapsulated Security Protocol (ESP)	PowerFlow	IP Protocol 50	n/a	Security; ESP should be open and available between cluster nodes
Couchbase Dashboard	PowerFlow	8091	n/a	Couchbase Dashboard (use your PowerFlow credentials)
RabbitMQ Dashboard	PowerFlow	15672	n/a	RabbitMQ Dashboard (use *guest/guest* for credentials)

ScienceLogic highly recommends that you disable all firewall session-limiting policies. Firewalls will drop HTTPS requests, which results in data loss.

CAUTION: You can configure one or more SL1 systems to use PowerFlow to sync with a *single* instance of a third-party application like ServiceNow, Restorepoint, or Cherwell. You cannot configure one SL1 system to use PowerFlow to sync with *multiple* instances of a third-party application like ServiceNow or Cherwell. The relationship between SL1 and the third-party application can be either one-to-one or many-to-one, but not one-to-many.

NOTE: You can use a single PowerFlow system to manage multiple pairings between one or more SL1 systems and third-party applications like ServiceNow and Cherwell. The pairings must always be one-to-one or many-to-one: one or more SL1 systems connected to only one third-party application.

CAUTION: The site administrator is responsible for configuring the host, hardware, and virtualization configuration for the PowerFlow server or cluster. If you are running a cluster in a VMware environment, be sure to install open-vm-tools and disable vMotion.

NOTE: The default internal network used by PowerFlow services is **172.21.0.1/16**. Please ensure that this range does not conflict with any other IP addresses on your network. If needed, you can change this subnet in the **docker-compose.yml** file.

NOTE: The PowerFlow operating system is an Oracle Linux distribution, and all patches are provided within the standard Oracle Linux repositories. The patches are not provided by ScienceLogic.

TIP: For more information about system requirements for your PowerFlow environment, see the System Requirements page at the ScienceLogic Support site.

Installing PowerFlow

For detailed steps about installing PowerFlow, see the *Installing and Configuring PowerFlow* chapter in the *SL1PowerFlow Platform* manual.

WARNING: Do not deploy this version of PowerFlow to a production environment.