semperis

Directory Services Protector

Version: 4.2

Splunk Integration Guide

May 2025 (6)

Legal Notice

This document is provided strictly on an "AS IS" basis without warranty of any kind, either express or implied, including, but not limited to, the implied warranties of merchantability or fitness for a particular purpose. Semperis and its staff assume no responsibility for any errors that may have been included in this document and reserve the right to make changes to the document without notice. Semperis and its staff disclaim any responsibility for incidental or consequential damages in connection with the furnishing, performance, use of, or reliance on this document or its content.

Contents

Preface

Welcome to the *Splunk Integration Guide for Directory Services Protector*. This guide is intended for administrators responsible for configuring Splunk to receive security indicator and change events from DSP.

Document Revisions

Table 1: Splunk Integration Guide Revisions

Product version	Date	Document revision	Comments
DSP 3.8	March 2023	1	Initial publishing of document
DSP 3.8 or later	March 2024	2	Republished with DSP 4.0 release
DSP 4.1	February 2025	3	Republished to support DSP 4.1
DSP 4.1	March 2025	4	Added Splunk Cloud Configuration
DSP 4.0 SP1/SP2 and DSP 4.1	April 2025	5	Updated version numbers
DSP 4.2	May 2025	6	Updated for compatibility with Splunk Dashboard 4.2.1

Styles and Conventions used in this Document

The following styles are used in this document.

Table 2: Document conventions and styles

Typeface	Description
Bold	Used for names of UI elements, such as buttons, pages, menus, options, fields, dialogs, and columns.
Italics	Used for references to documents that are not hyperlinks to other documents or topics. Also used to introduce new terms.
`Monospace`	Used for command-line input and code examples.
<PLACE HOLDER>	Brackets denote place holder text that is to be replaced with a user-specified value.

The following styles are used for notices:

NOTE:

This notice style is used to provide additional information and background overview.

IMPORTANT!

This notice style is used to present additional important information or warnings.

Contacting Semperis

Thank you for your interest in Semperis and Directory Services Protector. We are here to answer any questions you may have.

- For technical support, contact support@semperis.com
- For licensing issues, contact sales@semperis.com
- For product inquiries or feature requests, contact info@semperis.com

CHAPTER 1

DSP Splunk Solution Overview

Semperis Directory Services Protector (DSP) is known for providing uninterrupted tracking of Active Directory modifications and valuable insight into your Active Directory security posture. In addition to constantly tracking changes and deletions made to Active Directory, it continuously queries Active Directory looking for risky configurations to identify vulnerabilities in your Active Directory deployment.

Splunk Enterprise provides the critical Security Incident and Event Monitoring (SIEM) capabilities that are core to your cyber resilience and security program. The Semperis Directory Services Protector Solution allows you to easily integrate DSP with Splunk Enterprise to present relevant AD Changes, DSP operational events, and DSP Security Indicators mapped to the security frameworks you rely on--such as MITRE.

The Semperis Directory Services Protector Solution Splunk application (DSP Splunk Enterprise application) provides the artifacts required to successfully integrate with Splunk Enterprise. The Semperis Directory Services Protector Solution includes a basic set of components to get you started, for example:

- DSP-specific Splunk indexes created at app installation
- Configuration file for DSP Event log data to be ingested into the Splunk Universal Forwarder
- Dashboards:
  - DSP Quickview
  - DSP Security Indicators
  - DSP Directory Changes
  - DSP Notifications

Using these components as a basis, you can customize the DSP Splunk Enterprise application to best meet your organization's requirements.

Prerequisites

Before you begin setting up Splunk Enterprise to capture DSP security indicator events, ensure you review the following prerequisites and requirements.

Table 3: DSP requirements

Component	Requirement
DSP Edition	One of the following DSP editions is required: • DSP Advanced • DSP Intelligence ***NOTE:*** *The security indicator data is only available with DSP Intelligence. If you are running DSP Advanced, the security initiator views in the Semperis DSP Quickview dashboard, Semperis DSP Security Indicator dashboard, and security indicator related alerts will be blank in Splunk.*
DSP Version	This guide is compatible with DSP 4.2.
Splunk Database Version	Splunk Database version 4.2.1 is compatible with DSP 4.2.
Network ports	The following ports are used to forward DSP data into Splunk Enterprise: • 9997: Used to forward Event logs (DSP security indicator data, operational data, notification rule events) -> semperis_dsp index (Splunk Enterprise). Uses the Universal Forwarder to move data from DSP into the Splunk Enterprise index using the standard port (9997), which can be changed. • 5210: Used to forward Syslog data (AD change data) -> sermperis_dsp_syslog index (Splunk Enterprise) Uses the Syslog output from DSP to move data into the Splunk Enterprise index. This default port can be changed. In addition, you can use either TCP or UDP. • TCP: Use if the DSP Management Server is in a different subnet (default) • UDP: Use if the DSP Management Server is in the same subnet.

CHAPTER 2

Manual Deployment of the DSP Splunk Enterprise Application

If you are new to Splunk Enterprise, please review the Getting Started With Splunk Software documentation from Splunk.

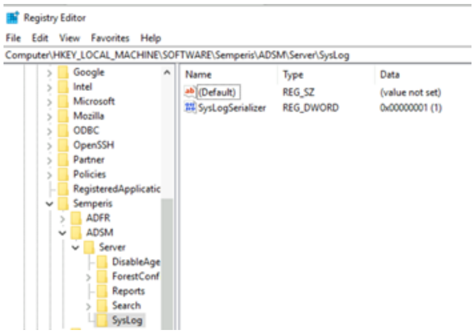
DSP Management Server Configuration

The Semperis Directory Services Protector Solution requires the following on the DSP Management Server.

- Registry key value set for standard Syslog output format.
- Installation of the Splunk Universal Forwarder (UF) with the DSP inputs.conf file deployed.
- DSP SIEM configuration.

To set the DSP registry key for Syslog output format:

1. On the DSP Management Server, open the Registry Editor.
2. Navigate to HKEY_LOCAL_MACHINE\SOFTWARE\Semperis\ADSM\Server.
3. Add new key "SysLog".
4. Add new DWORD value "SysLogSerializer" with a value of "1"



Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Semperis\ADSM\Server\SysLog

Name	Type	Data
(Default)	REG_SZ	(value not set)
SysLogSerializer	REG_DWORD	0x00000001 (1)

To install the Splunk Universal Forwarder:

1. Install the Splunk Universal Forwarder according to the Splunk guidelines. The Splunk Universal Forwarder is installed on the DSP Management Server.
2. On the DSP Management Server open the File Explorer.
3. Navigate to the location where the Universal Forwarder is installed.

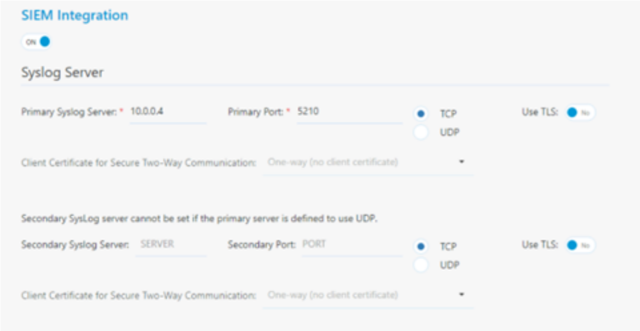
   By default the location is: C:\Program Files\SplunkUniversalForwarder
4. In that directory, navigate to \etc\system\local.
5. If there is not an inputs.conf file, create one.
6. Modify the inputs.conf file to include the following:

```
[WinEventLog://Semperis-DSP-Management/Operational]
disabled = 0
start_from = oldest
current_only = 1
checkpointInterval = 5
index = semperis_dsp
renderXml=false

[WinEventLog://Semperis-DSP-Monitor/Operational]
disabled = 0
start_from = oldest
current_only = 1
checkpointInterval = 5
index = semperis_dsp
renderXml=false

[WinEventLog://Semperis-DSP-Notifications/Operational]
disabled = 0
start_from = oldest
current_only = 1
checkpointInterval = 5
index = semperis_dsp
renderXml=false

[WinEventLog://Semperis-DSP-Reporting/Operational]
disabled = 0
start_from = oldest
```

```
current_only = 1
checkpointInterval = 5
index = semperis_dsp
renderXml=false

[WinEventLog://Semperis-DSP-Security/Operational]
disabled = 0
start_from = oldest
current_only = 1
checkpointInterval = 5
index = semperis_dsp
renderXml=false

[WinEventLog://Semperis-Operation-Log/Operational]
disabled = 0
start_from = oldest
current_only = 1
checkpointInterval = 5
index = semperis_dsp
renderXml=false
```

To set up DSP SIEM configuration:

1. Log in to the DSP Administration portal with a user that has at least the DSP Product Manager Role.
2. Navigate to **Settings** > **Data connections** > **SIEM integration**.
3. Click the SIEM integration toggle at the top of the page to switch it to **On**.
4. In the **Syslog Server** pane, enter the following information to identify the target server where data is to be sent:
   - **Primary Syslog Server**: IP or hostname of the Splunk Syslog target.
   - **Primary Port**: TCP 5210 (Application default. This should be set to the appropriate protocol/port for your deployment.)
   - **Use TLS**: No unless required
   - **Client Certificate**: No change unless required



SIEM Integration

ON ●

Syslog Server

Primary Syslog Server: * 10.0.0.4 Primary Port: * 5210 ● TCP ○ UDP Use TLS: No

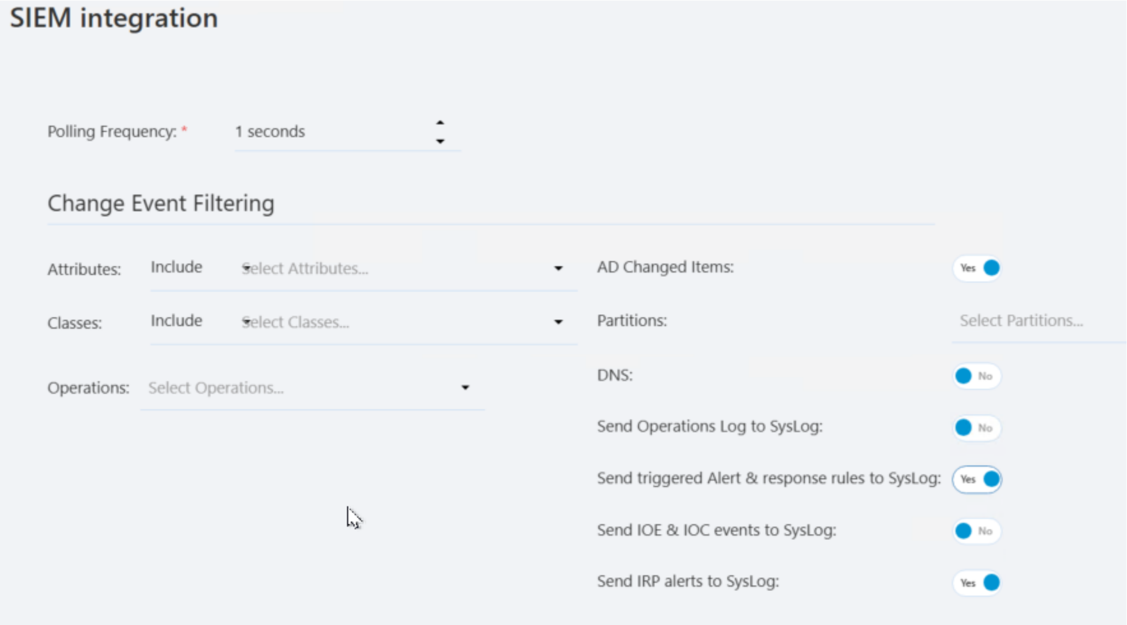
Client Certificate for Secure Two-Way Communication: One-way (no client certificate)

Secondary SysLog server cannot be set if the primary server is defined to use UDP.

Secondary Syslog Server: SERVER Secondary Port: PORT ● TCP ○ UDP Use TLS: No

Client Certificate for Secure Two-Way Communication: One-way (no client certificate)

5. In the **Change Event Filter** section, enter the following to specify what data is being forwarded from DSP:
   - **Attributes**: No change unless required
   - **Classes**: No change unless required
   - **Operations**: No change unless required
   - **AD Changed Items**: Yes
   - **Partitions**: No change unless required
   - **DNS**: No unless required
   - **Send Operations Log to SysLog**: No
   - **Send triggered Alert & response rules to SysLog**: Yes
   - **Send IOE & IOC events to SysLog**: No
   - **Send IRP alerts to SysLog**: Yes



SIEM integration

Polling Frequency: * 1 seconds

Change Event Filtering

Attributes: Include Select Attributes...

Classes: Include Select Classes...

Operations: Select Operations...

AD Changed Items: Yes

Partitions: Select Partitions...

DNS: No

Send Operations Log to SysLog: No

Send triggered Alert & response rules to SysLog: Yes

Send IOE & IOC events to SysLog: No

Send IRP alerts to SysLog: Yes

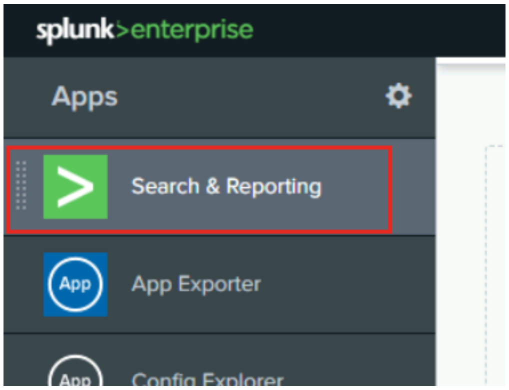
Splunk Enterprise Configuration

The Semperis Directory Services Protector Solution requires the following in Splunk Enterprise:

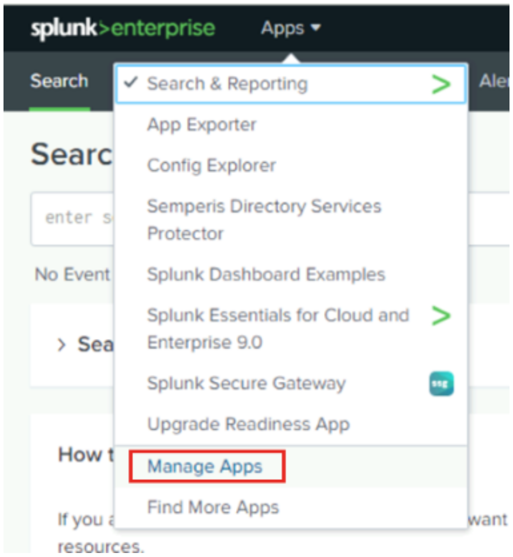
- DSP Splunk Enterprise application installed/imported
- Universal Forwarder location
- Indexes semperis_dsp and semperis_dsp_syslog properly configured to receive DSP data.

To install/import the DSP Splunk Enterprise application:

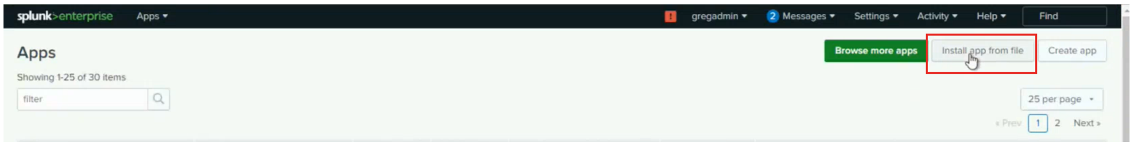
1. Log in to Splunk Enterprise using an account with rights to install an application.
2. In the left navigation pane, click **Search & Reporting**.



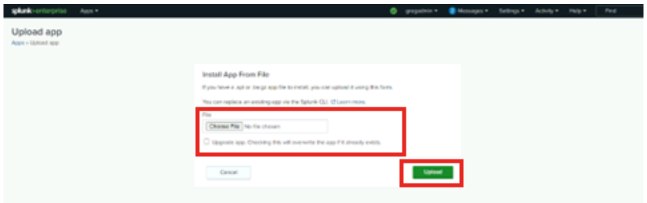
3. At the top of the page, click **Apps** > **Manage Apps**.



4. On the **Apps** page, click the **Install app from file** button.



5. On the **Upload app** page, click the **Choose file** button and select the semperis_ dsp.tar.gz file. If this is an upgrade, select the **Upgrade app** check box. Click the **Upload** button.

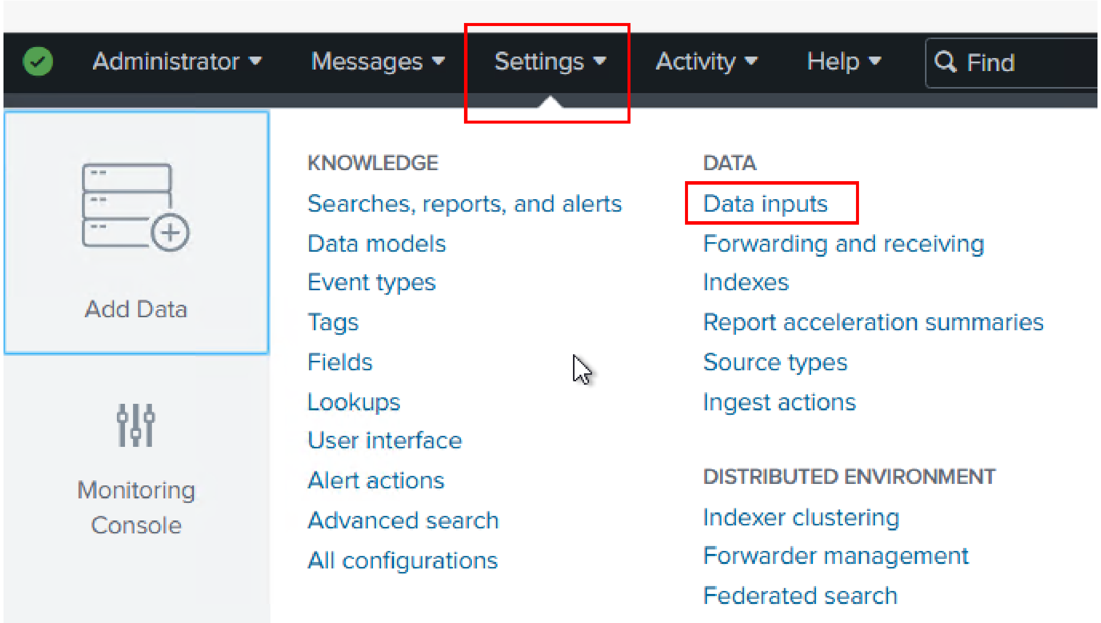

splunk>enterprise
Apps ▾
gregadmin ▾
Messages ▾
Settings ▾
Activity ▾
Help ▾
Find
Upload app
Apps › Upload app
Install App From File
If you have a .spl or .tar.gz app file to install, you can upload it using this form.
You can replace an existing app via the Splunk CLI. Learn more.
File
Choose File
No file chosen
Upgrade app. Checking this will overwrite the app if it already exists.
Cancel
Upload

NOTE:

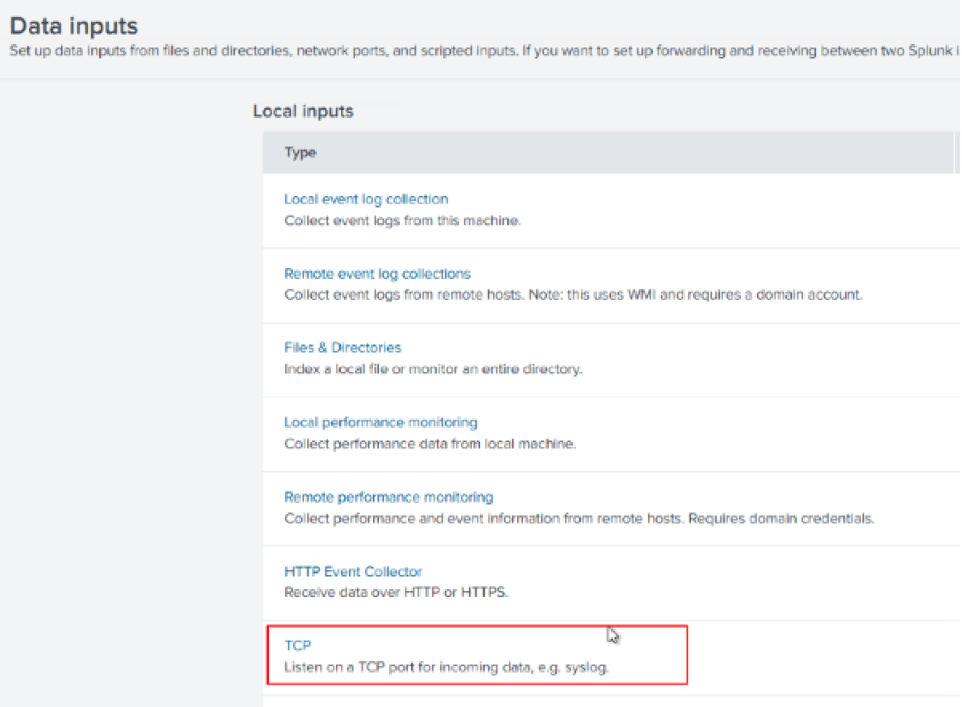
Alternatively, you can download the app from SplunkBase: Semperis Directory Services Protector | SplunkBase.

To configure data input:

1. In Splunk Enterprise, navigate to **Settings** > **Data inputs**.



2. On the **Data inputs** page, select **TCP**.



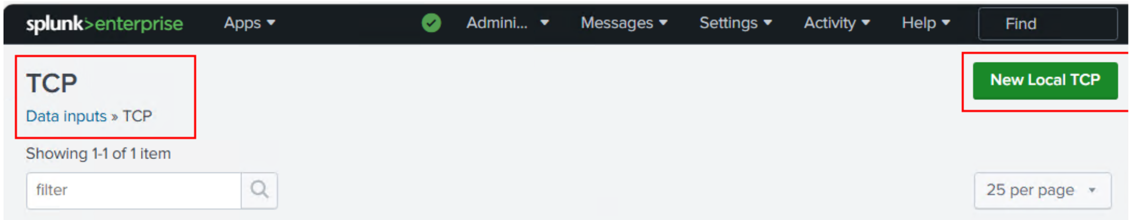
Data inputs

Set up data inputs from files and directories, network ports, and scripted inputs. If you want to set up forwarding and receiving between two Splunk i

Local inputs

Type
Local event log collection Collect event logs from this machine.
Remote event log collections Collect event logs from remote hosts. Note: this uses WMI and requires a domain account.
Files & Directories Index a local file or monitor an entire directory.
Local performance monitoring Collect performance data from local machine.
Remote performance monitoring Collect performance and event information from remote hosts. Requires domain credentials.
HTTP Event Collector Receive data over HTTP or HTTPS.
TCP Listen on a TCP port for incoming data, e.g. syslog.

3. On the **Data inputs** > **TCP page**, click **New Local TCP**.



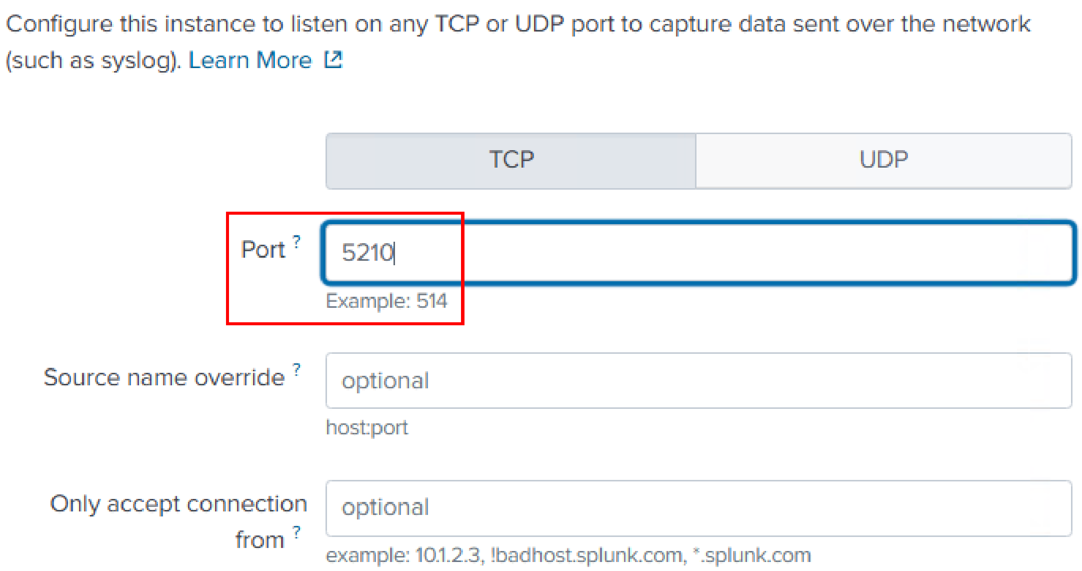
TCP

Data inputs » TCP

Showing 1-1 of 1 item

4. On the **Select Source** page, find the **Port** text field and enter "5210." Click **Next**.

> ***NOTE:***
>
> *Ensure that **TCP** is selected.*



Configure this instance to listen on any TCP or UDP port to capture data sent over the network (such as syslog). Learn More

Port ? 5210
Example: 514

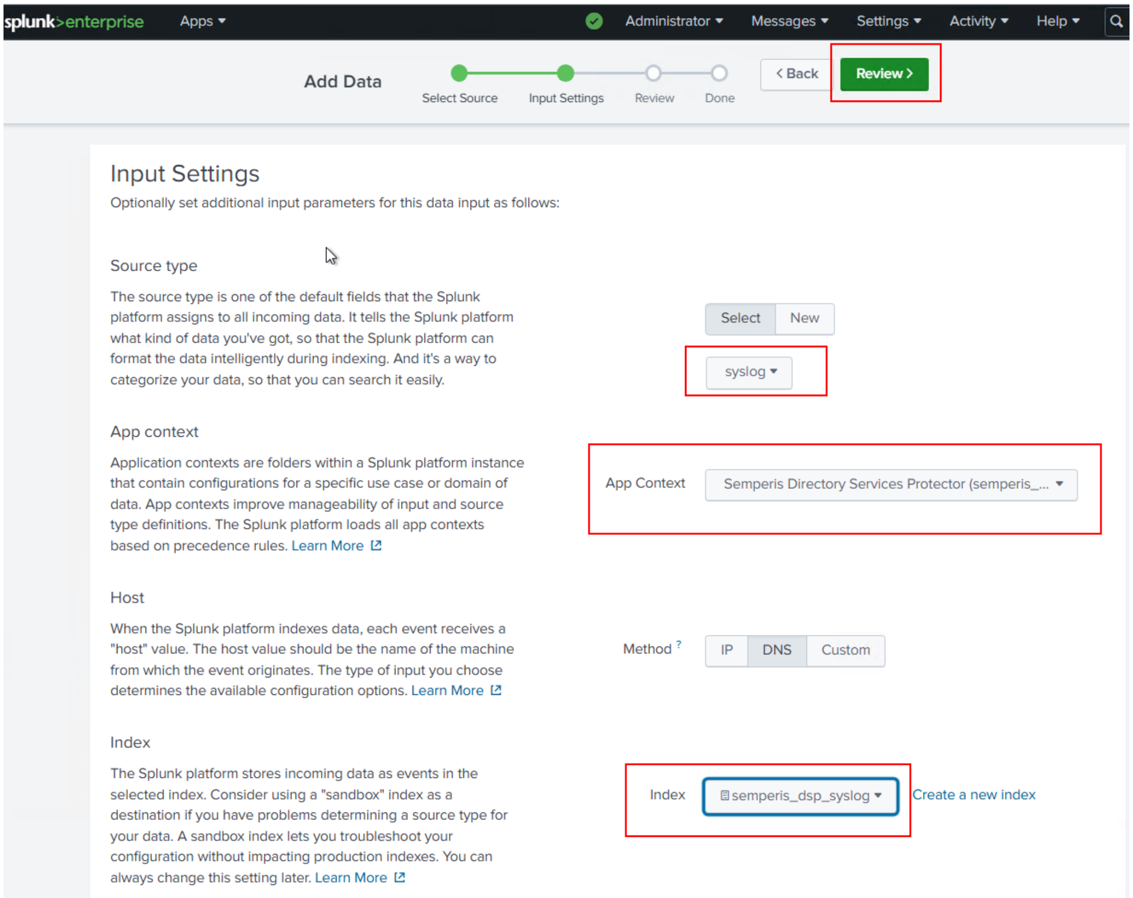
Source name override ? optional
host:port

Only accept connection from ? optional
example: 10.1.2.3, !badhost.splunk.com, *.splunk.com

NOTE:

If you specified a different port for the Syslog data, manually create the receiver at the specified port and point that to the correct index (semperis_dsp_syslog).

5. On the **Add Data** page, select the following options:
   - **Source type**: **syslog**
   - **App context**: **Semperis Directory Services Protector**
   - **Method**: **DNS**
   - **Index**: **semperis_dsp_syslog**



Input Settings

Optionally set additional input parameters for this data input as follows:

Source type

The source type is one of the default fields that the Splunk platform assigns to all incoming data. It tells the Splunk platform what kind of data you've got, so that the Splunk platform can format the data intelligently during indexing. And it's a way to categorize your data, so that you can search it easily.

Select | New

syslog

App context

Application contexts are folders within a Splunk platform instance that contain configurations for a specific use case or domain of data. App contexts improve manageability of input and source type definitions. The Splunk platform loads all app contexts based on precedence rules. Learn More

App Context: Semperis Directory Services Protector (semperis_...

Host

When the Splunk platform indexes data, each event receives a "host" value. The host value should be the name of the machine from which the event originates. The type of input you choose determines the available configuration options. Learn More

Method: IP | DNS | Custom

Index

The Splunk platform stores incoming data as events in the selected index. Consider using a "sandbox" index as a destination if you have problems determining a source type for your data. A sandbox index lets you troubleshoot your configuration without impacting production indexes. You can always change this setting later. Learn More

Index: semperis_dsp_syslog

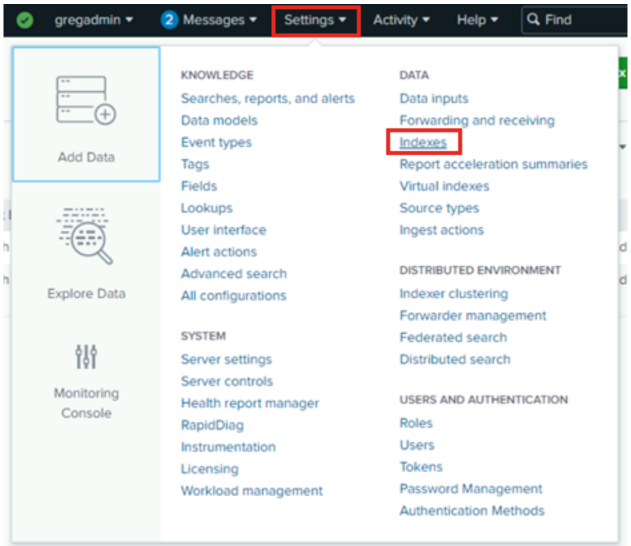
Create a new index

6. Click **Review**.
7. On the **Review** page, click **Submit**.

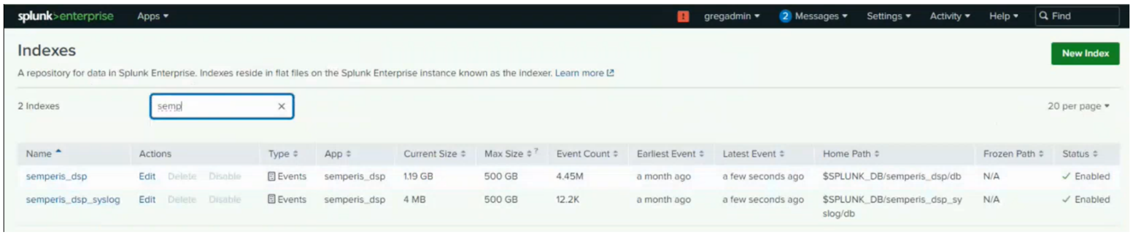
To verify DSP indexes:

The installation of the DSP Splunk Enterprise application will configure the required indexes. Please verify the input and if you need to change the protocol or port, do so now.

1. In Splunk Enterprise, navigate to **Settings** > **Indexes**.



2. On the **Indexes** page, filter for "semperis" and click **Enter**.



Indexes

A repository for data in Splunk Enterprise. Indexes reside in flat files on the Splunk Enterprise instance known as the indexer. Learn more

2 Indexes

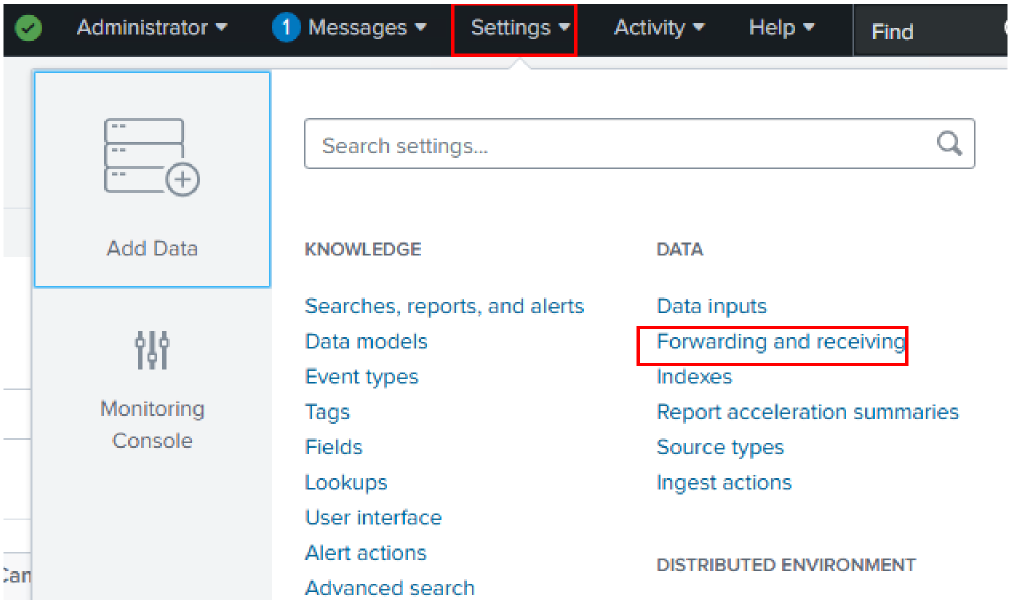
Name	Actions	Type	App	Current Size	Max Size	Event Count	Earliest Event	Latest Event	Home Path	Frozen Path	Status
semperis_dsp	Edit Delete Disable	Events	semperis_dsp	1.19 GB	500 GB	4.45M	a month ago	a few seconds ago	$SPLUNK_DB/semperis_dsp/db	N/A	✓ Enabled
semperis_dsp_syslog	Edit Delete Disable	Events	semperis_dsp	4 MB	500 GB	12.2K	a month ago	a few seconds ago	$SPLUNK_DB/semperis_dsp_syslog/db	N/A	✓ Enabled

The following indexes should be displayed:

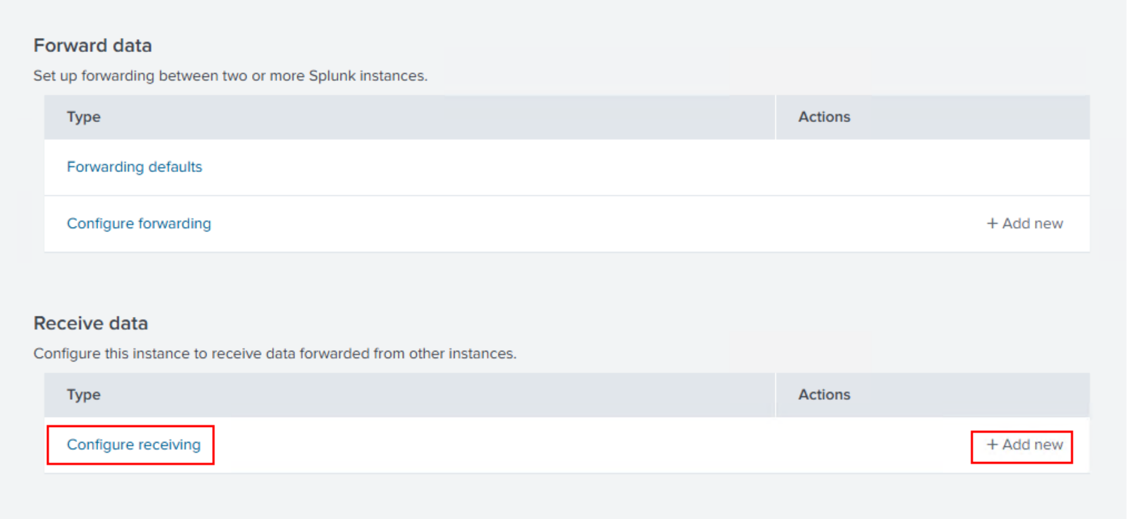
- semperis_dsp
- semperis_dsp_syslog

Configure the Splunk instance to receive data from forwarder(s):

1. In Splunk Enterprise, navigate to **Settings** > **Forwarding and receiving**.



2. In the **Receive data** table, locate **Configure receiving** and click **Add new**.



Forward data

Set up forwarding between two or more Splunk instances.

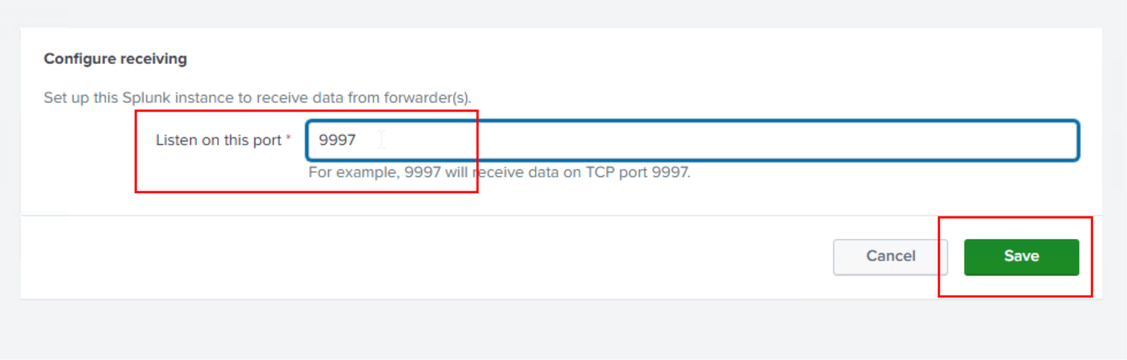
Type	Actions
Forwarding defaults	
Configure forwarding	+ Add new

Receive data

Configure this instance to receive data forwarded from other instances.

Type	Actions
Configure receiving	+ Add new

3. In the **Listen on this port** text field, enter "9997." Click **Save**.



Configure receiving

Set up this Splunk instance to receive data from forwarder(s).

Listen on this port * 9997

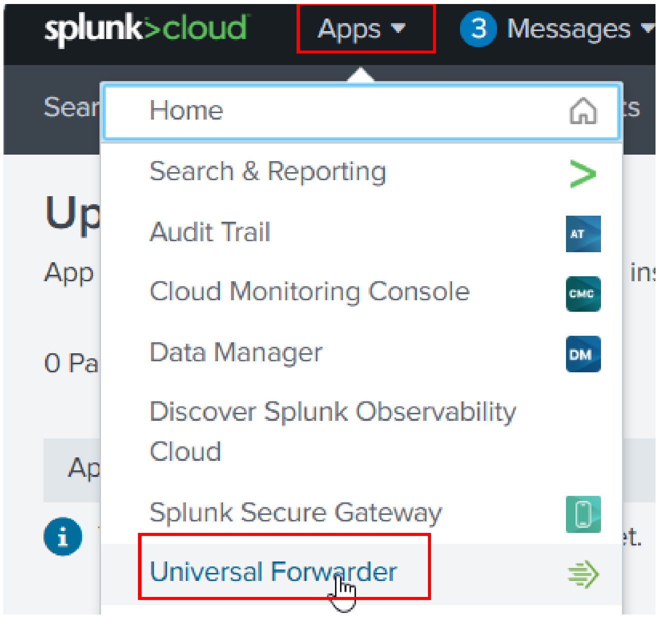
For example, 9997 will receive data on TCP port 9997.

Splunk Cloud Configuration

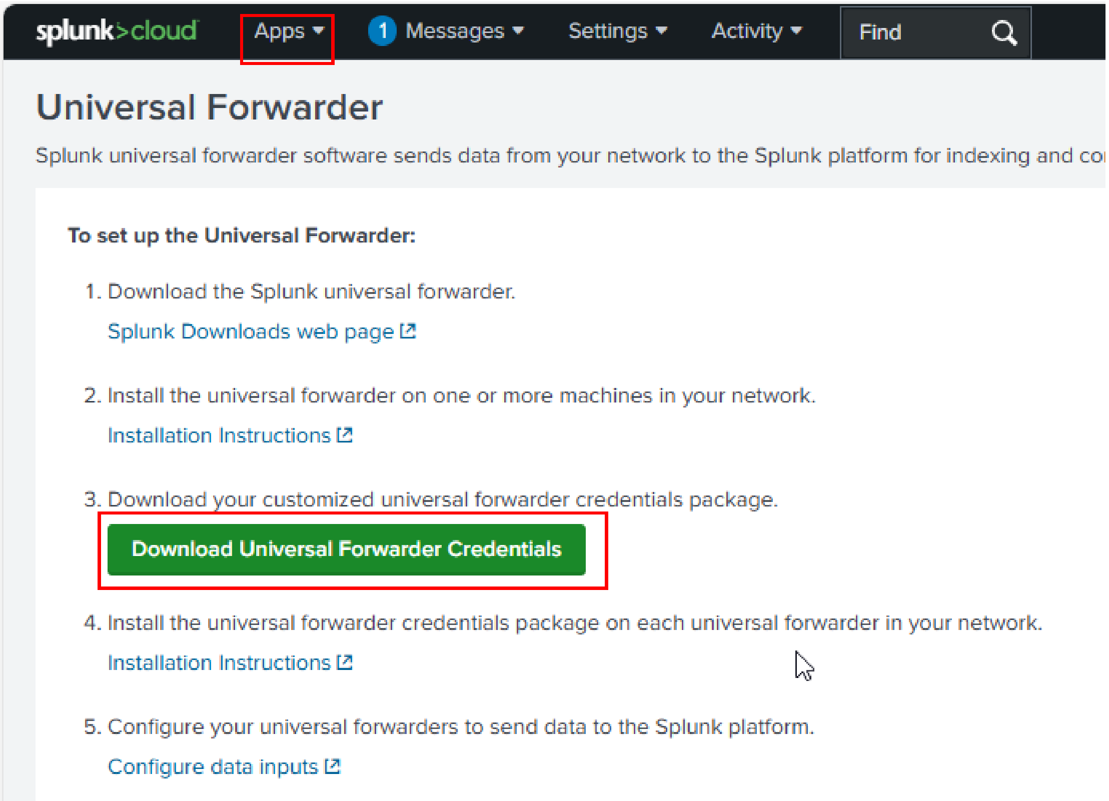
Splunk Cloud instances can only receive Syslog data sent from the Universal Forwarder or the Heavy Forwarder. The following procedure guides you through configuring a Splunk Cloud instance through the Universal Forwarder.

To download the Universal Forwarder credentials from the Splunk Cloud and install it on the Universal Forwarder server:

1. In Splunk Enterprise, navigate to **Apps** > **Universal Forwarder**.



2. On the **Universal Forwarder** page, click **Download Universal Forwarder Credentials**.



Universal Forwarder

Splunk universal forwarder software sends data from your network to the Splunk platform for indexing and co

To set up the Universal Forwarder:

1. Download the Splunk universal forwarder.
   Splunk Downloads web page
2. Install the universal forwarder on one or more machines in your network.
   Installation Instructions
3. Download your customized universal forwarder credentials package.
   Download Universal Forwarder Credentials
4. Install the universal forwarder credentials package on each universal forwarder in your network.
   Installation Instructions
5. Configure your universal forwarders to send data to the Splunk platform.
   Configure data inputs

3. Search for and delete the outputs.conf file in the `C:\Program Files\SplunkUniversalForwarder\etc\system\local` folder. If the outputs.conf file does not exist in that folder, do nothing.
4. Run the following command to install splunkclouduf.spl:

   ```
   C:\Program Files\SplunkUniversalForwarder\bin>splunk.exe
   install C:\Install\Splunk\splunkclouduf.spl
   ```

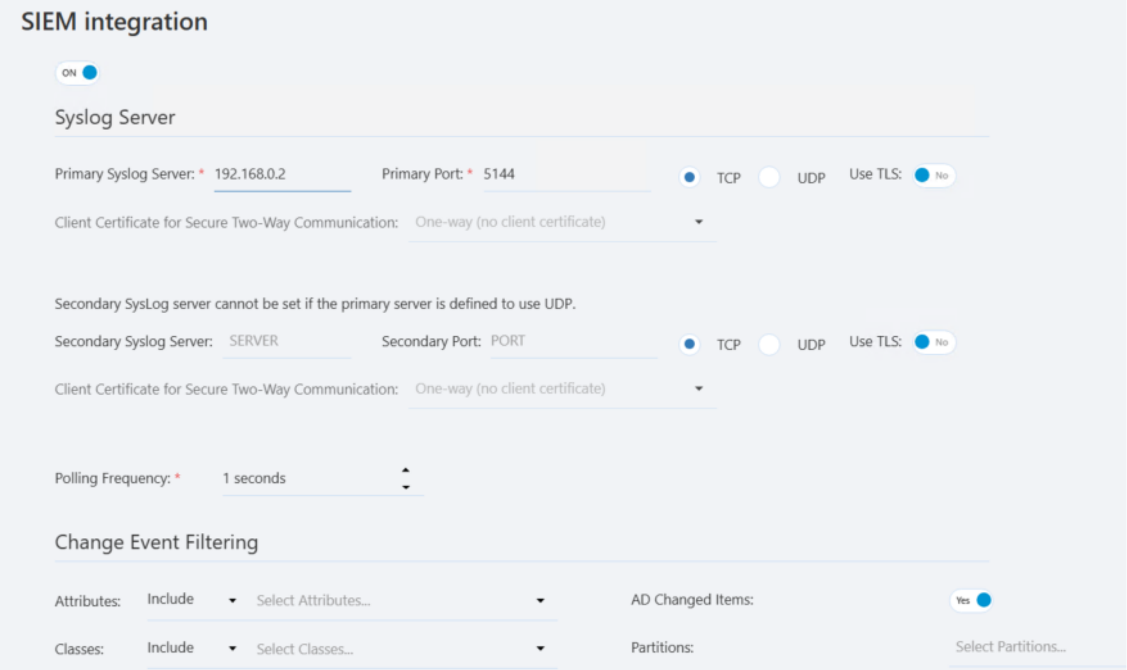
5. Enter the Splunk username and password to connect to the Splunk Cloud instance.
6. Restart the Splunk Forwarder service.
7. Navigate to `C:\Program Files\SplunkUniversalForwarder\etc\system\local`.
8. Add the following code to the top of the inputs.conf file:

   ```
   [tcp://5144]

   index = semperis_dsp_syslog

   disabled=false
   ```

Configure DSP to send Syslog data to the Splunk Cloud instance via the Universal Forwarder:

1. Log in to the DSP Administration portal with a user that has at least the DSP Project Manager Role.
2. Navigate to the **Settings** > **Data Connections** > **SIEM integration** page.
3. In the **Syslog Server** pane, enter the following information:
   - **Primary Syslog Server**: IP of the Universal Forwarder.
   - **Primary Port**: Port configured on the inputs.conf file.
   - **TCP**: Select the circle.

   In the **Change Event Filtering** pane, set the **AD Changed Items** toggle to "Yes."



SIEM integration

ON

Syslog Server

Primary Syslog Server: * 192.168.0.2 Primary Port: * 5144 ● TCP ○ UDP Use TLS: No

Client Certificate for Secure Two-Way Communication: One-way (no client certificate)

Secondary SysLog server cannot be set if the primary server is defined to use UDP.

Secondary Syslog Server: SERVER Secondary Port: PORT ● TCP ○ UDP Use TLS: No

Client Certificate for Secure Two-Way Communication: One-way (no client certificate)

Polling Frequency: * 1 seconds

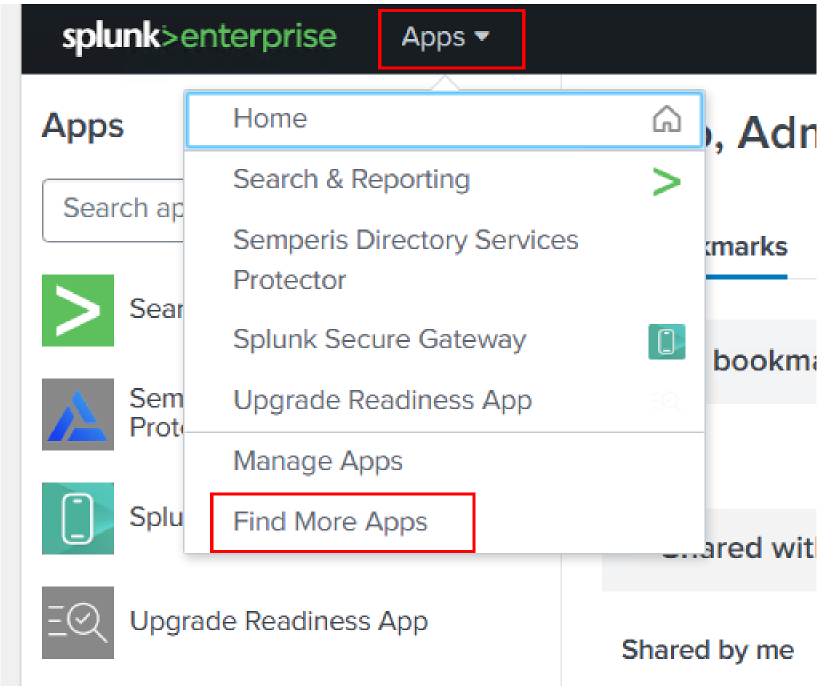
Change Event Filtering

Attributes: Include Select Attributes... AD Changed Items: Yes

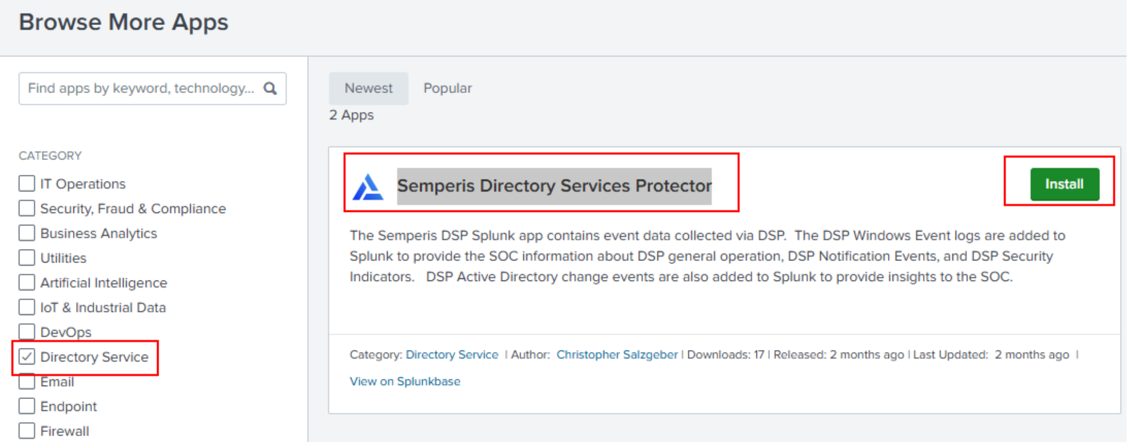
Classes: Include Select Classes... Partitions: Select Partitions...

To install the Semperis Directory Services Protector App on the Splunk Cloud instance:

1. In Splunk Enterprise, navigate to **Apps** > **Find More Apps**.



2. In the **Category** section, select the check box next to **Directory Service**.
3. Ensure that you have the **Semperis Directory Services Protector** selected, then click **Install**.


Browse More Apps

Find apps by keyword, technology...

Newest Popular

2 Apps

CATEGORY

□ IT Operations
□ Security, Fraud & Compliance
□ Business Analytics
□ Utilities
□ Artificial Intelligence
□ IoT & Industrial Data
□ DevOps
☑ Directory Service
□ Email
□ Endpoint
□ Firewall

Semperis Directory Services Protector

Install

The Semperis DSP Splunk app contains event data collected via DSP. The DSP Windows Event logs are added to Splunk to provide the SOC information about DSP general operation, DSP Notification Events, and DSP Security Indicators. DSP Active Directory change events are also added to Splunk to provide insights to the SOC.

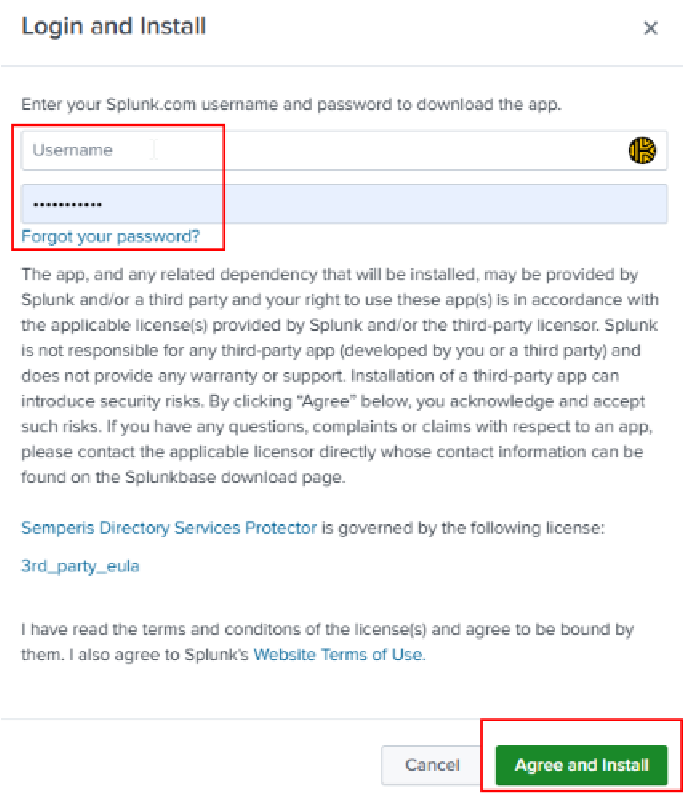
Category: Directory Service | Author: Christopher Salzgeber | Downloads: 17 | Released: 2 months ago | Last Updated: 2 months ago |

View on Splunkbase

4. Enter the credentials for splunk.com in the **Login and Install** dialog, then click **Agree and Install**.

NOTE:

Do not enter the credentials for the Splunk Cloud.



Login and Install

Enter your Splunk.com username and password to download the app.

Username

•••••••••••

Forgot your password?

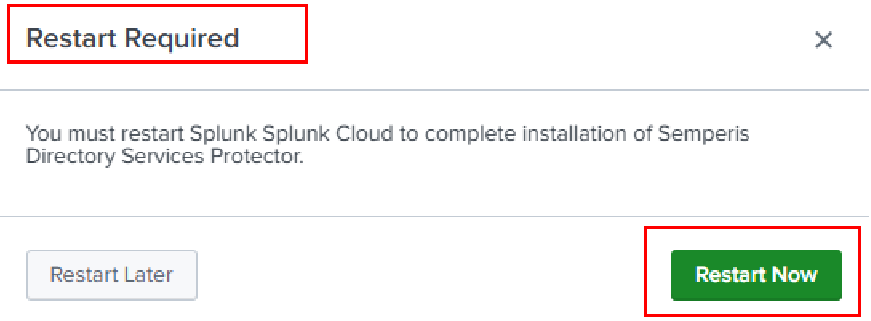
The app, and any related dependency that will be installed, may be provided by Splunk and/or a third party and your right to use these app(s) is in accordance with the applicable license(s) provided by Splunk and/or the third-party licensor. Splunk is not responsible for any third-party app (developed by you or a third party) and does not provide any warranty or support. Installation of a third-party app can introduce security risks. By clicking "Agree" below, you acknowledge and accept such risks. If you have any questions, complaints or claims with respect to an app, please contact the applicable licensor directly whose contact information can be found on the Splunkbase download page.

Semperis Directory Services Protector is governed by the following license:

3rd_party_eula

I have read the terms and conditons of the license(s) and agree to be bound by them. I also agree to Splunk's Website Terms of Use.

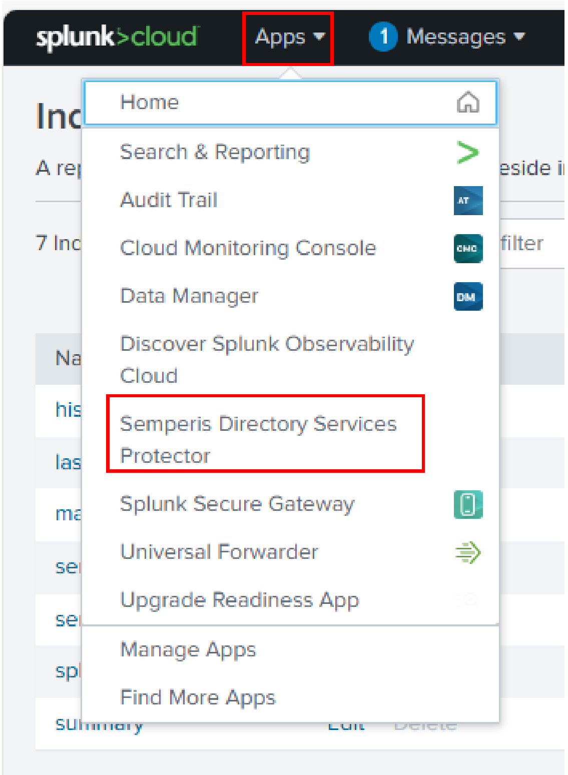
5. In the **Restart Required** dialog, click **Restart Now**.



Restart Required

You must restart Splunk Splunk Cloud to complete installation of Semperis Directory Services Protector.

6. Ensure that the **Semperis Directory Services Protector** app is available in the **Apps** drop-down.


splunk>cloud
Apps
1 Messages
Home
Search & Reporting
Audit Trail
Cloud Monitoring Console
Data Manager
Discover Splunk Observability Cloud
Semperis Directory Services Protector
Splunk Secure Gateway
Universal Forwarder
Upgrade Readiness App
Manage Apps
Find More Apps
filter

CHAPTER 3

DSP Splunk Enterprise Application Usage

The DSP Splunk Enterprise application consists of a baseline of dashboards and alerts. The dashboards provide a view into the data being ingested into Splunk. The alerts are intended as templates to show alerting. They can be modified to alert on alternate conditions in the data or to send alerts to external systems such as ticketing platforms or a SOAR system.

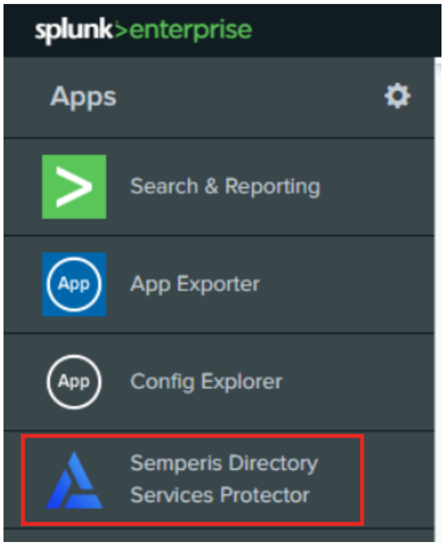
DSP Dashboards

The DSP Splunk Enterprise application consists of four separate dashboards:

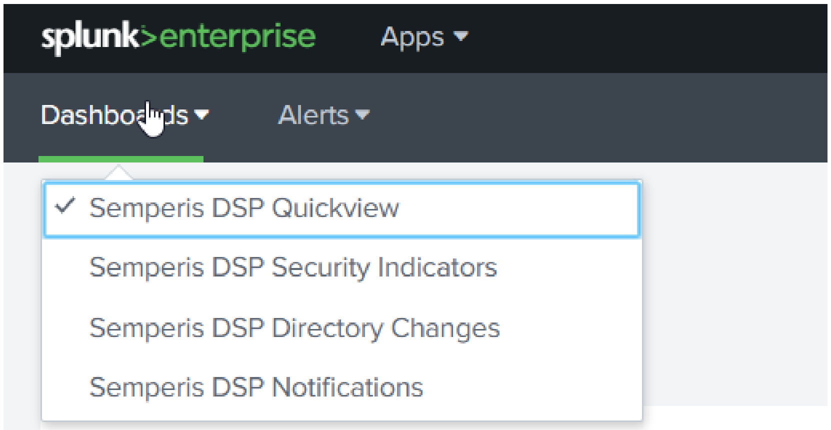
- *Semperis DSP Quickview Dashboard*
  - This dashboard is intended as a general view into DSP data in the SIEM.
  - Data for this dashboard comes from both the semperis_dsp and semperis_dsp_ syslog indexes.
- *Semperis DSP Security Indicators Dashboard*
  - This dashboard is a view into DSP security indicator status.
  - Data for this dashboard comes from the semperis_dsp index.
- *Semperis DSP Directory Changes Dashboard*
  - This dashboard is a view of DSP captured AD changes.
  - Data for this dashboard comes from the semperis_dsp_syslog index.
- *Semperis DSP Notifications Dashboard*
  - This dashboard is a view of DSP notification events.
  - Data for this dashboard comes from the semperis_dsp index.

To view a DSP dashboard:

1. In Splunk Enterprise, select the **Semperis Directory Services Protector** application from the left hand navigation menu.



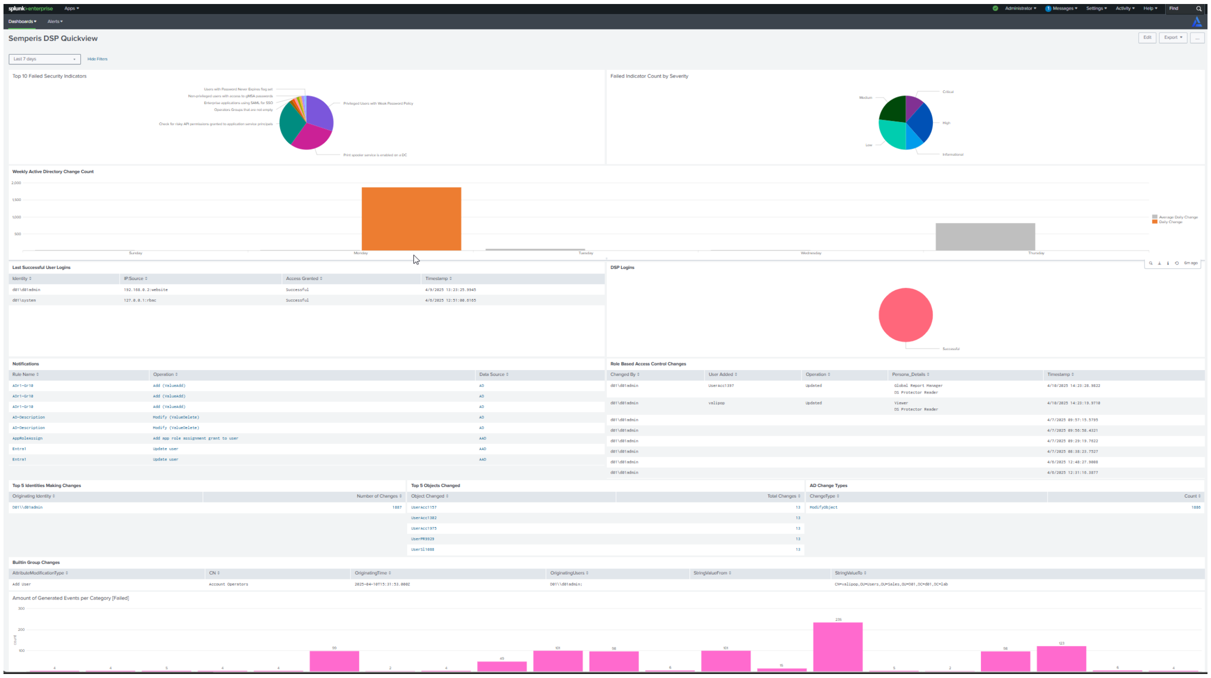
2. Once the DSP application is selected, the **DSP Quickview** dashboard is displayed by default.
3. To select a different DSP dashboard, expand the **Dashboard** control at the top of the page and select the DSP dashboard to be displayed.


splunk>enterprise
Apps
Dashboards
Alerts
✓ Semperis DSP Quickview
Semperis DSP Security Indicators
Semperis DSP Directory Changes
Semperis DSP Notifications

Semperis DSP Quickview Dashboard

The **Semperis DSP Quickview** dashboard contains general views of the DSP data forwarded from the DSP Event logs and Syslog (semperis_dsp and semperis_dsp_syslog indexes). It consists of the following sections:

- *Top 10 Failed Security Indicators* (pie chart)
- *Failed Indicator Count by Severity* (pie chart)
- *Weekly Active Directory Change Count* (column chart)
- *Last Successful User Logins* (table)
- *DSP Logins* (pie chart)
- *Notifications* (table)
- *Role Based Access Control Changes* (table)
- *Top 5 Identities Making Changes* (table)
- *Top 5 Objects Changed* (table)
- *AD Change Types* (table)
- *BuiltIn Group Changes* (table)
- *Amount of Generated Events per Category (Failed)* (column chart)


splunk>enterprise
Apps ▾
Administrator ▾
1 Messages ▾
Settings ▾
Activity ▾
Help ▾
Find
Dashboards ▾
Alerts ▾
Semperis DSP Quickview
Edit
Export ▾
...
Last 7 days
Hide Filters
Top 10 Failed Security Indicators
Users with Password Never Expires flag set
Non-privileged users with access to gMSA passwords
Enterprise applications using SAML for SSO
Operators Groups that are not empty
Check for risky API permissions granted to application service principals
Privileged Users with Weak Password Policy
Print spooler service is enabled on a DC
Failed Indicator Count by Severity
Critical
Medium
High
Low
Informational
Weekly Active Directory Change Count
2,000
1,500
1,000
500
Sunday
Monday
Tuesday
Wednesday
Thursday
Average Daily Change
Daily Change
DSP Logins
Successful
6m ago
Amount of Generated Events per Category [Failed]
300
200
100
count
4
4
5
4
4
99
2
4
40
101
98
6
101
15
236
5
2
98
123
6
4

Last Successful User Logins

Identity	IP:Source	Access Granted	Timestamp
d01\d01admin	192.168.0.2:website	Successful	4/9/2025 13:23:25.9945
d01\system	127.0.0.1:rbac	Successful	4/6/2025 12:51:08.6165

Notifications

Rule Name	Operation	Data Source
ADr1-Gr10	Add (ValueAdd)	AD
ADr1-Gr10	Add (ValueAdd)	AD
ADr1-Gr10	Add (ValueAdd)	AD
AD-Description	Modify (ValueDelete)	AD
AD-Description	Modify (ValueDelete)	AD
AppRoleAssign	Add app role assignment grant to user	AAD
Entra1	Update user	AAD
Entra1	Update user	AAD

Role Based Access Control Changes

Changed By	User Added	Operation	Persona_Details	Timestamp
d01\d01admin	UserAcc1397	Updated	Global Report Manager DS Protector Reader	4/10/2025 14:23:28.9822
d01\d01admin	valipop	Updated	Viewer DS Protector Reader	4/10/2025 14:23:19.9710
d01\d01admin				4/7/2025 09:57:15.5795
d01\d01admin				4/7/2025 09:56:58.4321
d01\d01admin				4/7/2025 09:29:19.7622
d01\d01admin				4/7/2025 08:38:23.7527
d01\d01admin				4/6/2025 12:48:27.9008
d01\d01admin				4/6/2025 12:31:16.3877

Top 5 Identities Making Changes

Originating Identity	Number of Changes
D01\\d01admin	1887

Top 5 Objects Changed

Object Changed	Total Changes
UserAcc1157	13
UserAcc1302	13
UserAcc1975	13
UserPR9929	13
UserSl1088	13

AD Change Types

ChangeType	Count
ModifyObject	1886

Builtin Group Changes

AttributeModificationType	CN	OriginatingTime	OriginatingUsers	StringValueFrom	StringValueTo
Add User	Account Operators	2025-04-10T15:31:53.000Z	D01\\d01admin;		CN=valipop,OU=Users,OU=Sales,OU=D01,DC=d01,DC=lab

Figure 1: Semperis DSP Quickview dashboard

Top 10 Failed Security Indicators

The **Top 10 Failed Security Indicators** pie chart displays the top ten DSP security indicators that are failing (IOE Found).

NOTE:

Security indicator data is only available with DSP Intelligence. Therefore, this view will be blank if you are running DSP Advanced.

Clicking a piece of the pie chart displays the **Semperis DSP Security Indicators** dashboard filtered by the selected security indicator.

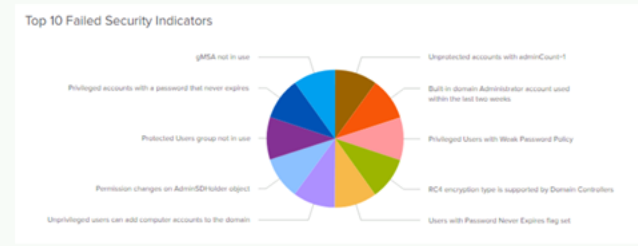

Top 10 Failed Security Indicators
gMSA not in use
Privileged accounts with a password that never expires
Protected Users group not in use
Permission changes on AdminSDHolder object
Unprivileged users can add computer accounts to the domain
Unprotected accounts with adminCount=1
Built-in domain Administrator account used within the last two weeks
Privileged Users with Weak Password Policy
RC4 encryption type is supported by Domain Controllers
Users with Password Never Expires flag set

Figure 2: Top 10 Failed Security Indicators

Failed Indicator Count by Severity

The **Failed Indicator Count by Severity** pie chart shows the failed DSP security indicator count broken down by severity.

NOTE:

Security indicator data is only available with DSP Intelligence. Therefore, this view will be blank if you are running DSP Advanced.

Clicking a piece of the pie chart displays the **Semperis DSP Security Indicators** dashboard filtered by the selected severity.

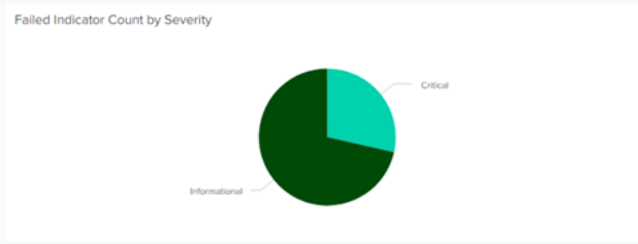


Figure 3: Failed Indicator Count by Severity

Weekly Active Directory Change Count

This column chart compares the average AD change data count per day to the current AD change count this week. The gray columns indicate the average count of AD changes per day. The orange column indicates the amount of AD changes for the day of the week for this week. If you see a huge skew between the average count and daily count you may want to take a closer look.

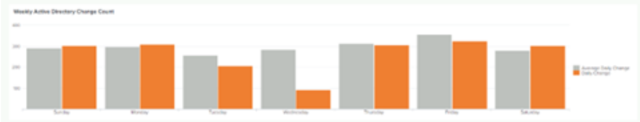
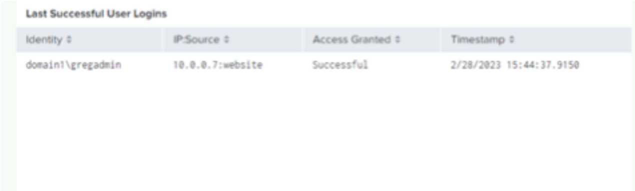


Figure 4: Weekly Active Directory Change Count

Last Successful User Logins

This table displays user login events to DSP along with their source IP and source. It includes both successful and failed login attempts.



Last Successful User Logins

Identity ⇕	IP:Source ⇕	Access Granted ⇕	Timestamp ⇕
domain1\gregadmin	10.0.0.7:website	Successful	2/28/2023 15:44:37.9150

Figure 5: Last Successful User Logins

DSP Logins

The **DSP Logins** pie chart compares successful DSP logins to failed DSP logins.

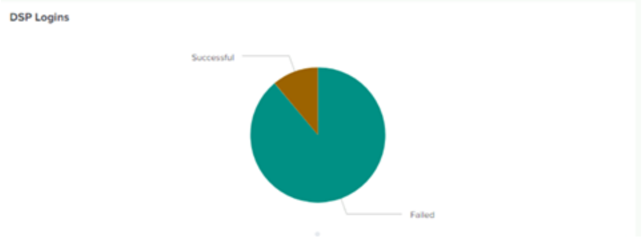
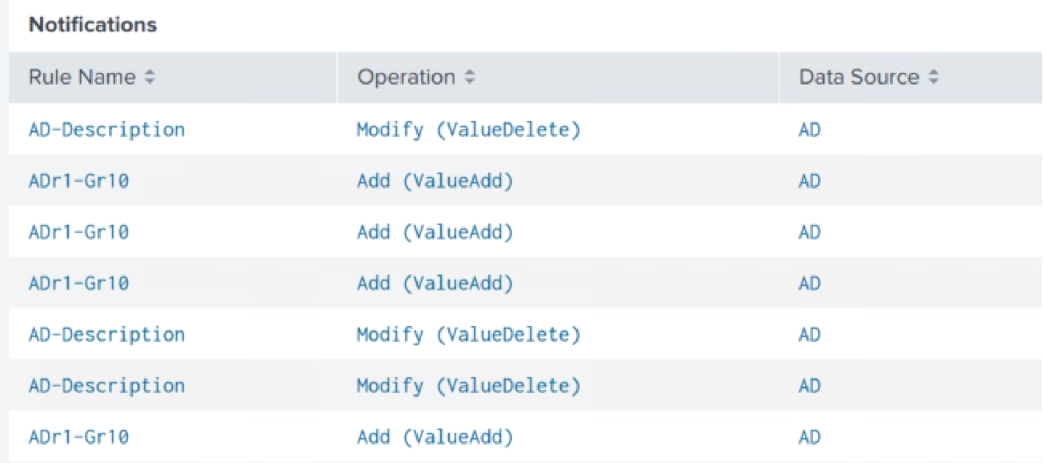


Figure 6: DSP Logins

Notifications

The **Notifications** table displays the most current changes to security notifications in DSP. For example, changes to Privileged Groups. Clicking on a rule in this table displays the **Semperis DSP Notifications** dashboard that provides additional details.



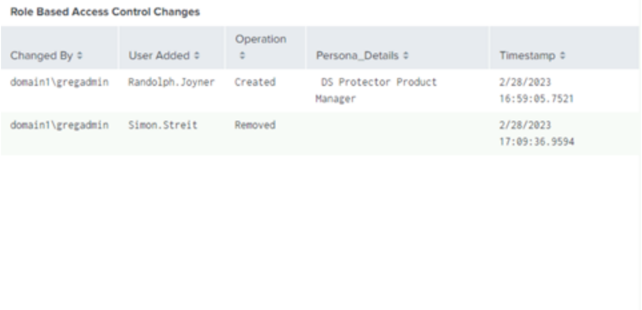
Notifications

Rule Name ⇕	Operation ⇕	Data Source ⇕
AD-Description	Modify (ValueDelete)	AD
ADr1-Gr10	Add (ValueAdd)	AD
ADr1-Gr10	Add (ValueAdd)	AD
ADr1-Gr10	Add (ValueAdd)	AD
AD-Description	Modify (ValueDelete)	AD
AD-Description	Modify (ValueDelete)	AD
ADr1-Gr10	Add (ValueAdd)	AD

Figure 7: Notifications

Role Based Access Control Changes

The **Role Based Access Control Changes** table displays DSP role based access control (RBAC) changes.



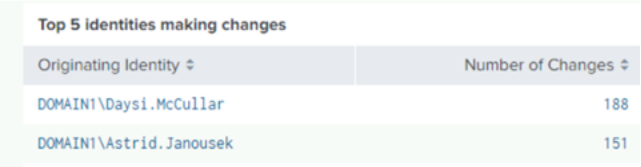
Role Based Access Control Changes

Changed By ⇕	User Added ⇕	Operation ⇕	Persona_Details ⇕	Timestamp ⇕
domain1\gregadmin	Randolph.Joyner	Created	DS Protector Product Manager	2/28/2023 16:59:05.7521
domain1\gregadmin	Simon.Streit	Removed		2/28/2023 17:09:36.9594

Figure 8: Role Based Access Control Changes

Top 5 Identities Making Changes

The **Top 5 identities making changes** table displays the top five identities that are making changes in Active Directory. Clicking an entry in this table displays the **Semperis DSP Directory Changes** dashboard showing the change events initiated by the selected identity.



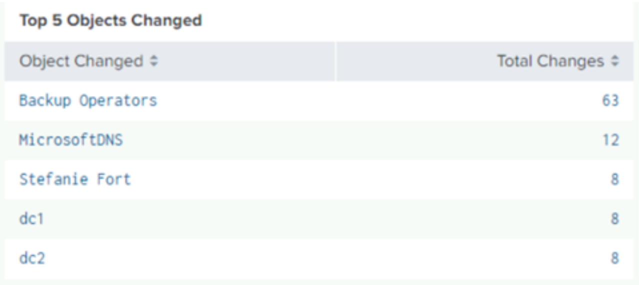
Top 5 identities making changes

Originating Identity ⬍	Number of Changes ⬍
DOMAIN1\Daysi.McCullar	188
DOMAIN1\Astrid.Janousek	151

Figure 9: Top 5 Identities Making Changes

Top 5 Objects Changed

The **Top 5 Objects Changed** table displays the top five Active Directory objects that have had the most changes during the specified time frame. Clicking an entry in this table displays the **Semperis DSP Directory Changes** dashboard showing the change events for the selected object.



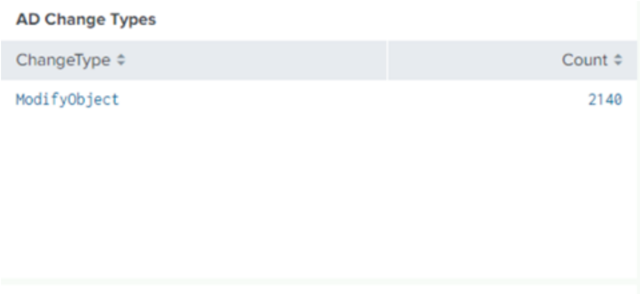
Top 5 Objects Changed

Object Changed ⬍	Total Changes ⬍
Backup Operators	63
MicrosoftDNS	12
Stefanie Fort	8
dc1	8
dc2	8

Figure 10: Top 5 Objects Changed

AD Change Types

The **AD Change Types** table displays the types of changes being made in Active Directory (for example, Add, Modify, Delete). Clicking an entry in this table displays the **Semperis DSP Directory Changes** dashboard showing the change events for the selected type of change.



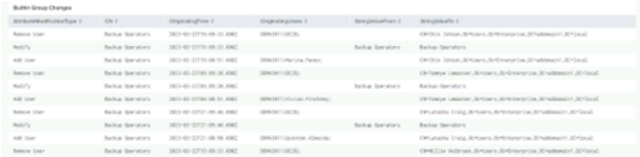
AD Change Types

ChangeType ⬍	Count ⬍
ModifyObject	2140

Figure 11: AD Change Types

BuiltIn Group Changes

The **BuiltIn Group Changes** table displays changes to BuiltIn groups in Active Directory.



BuiltIn Group Changes

AttributeModificationType	CN	OriginatingTime	OriginatingUsers	StringValueFrom	StringValueTo
Remove User	Backup Operators	[illegible]	DOMAIN1\DC2$;		CN=Chie Johnson,OU=Users,OU=Enterprise,DC=addomain1,DC=local
Modify	Backup Operators	[illegible]		Backup Operators	Backup Operators
Add User	Backup Operators	[illegible]	DOMAIN1\Marina.Perez;		CN=Chie Johnson,OU=Users,OU=Enterprise,DC=addomain1,DC=local
Remove User	Backup Operators	[illegible]	DOMAIN1\DC2$;		CN=Tommye Lemaster,OU=Users,OU=Enterprise,DC=addomain1,DC=local
Modify	Backup Operators	[illegible]		Backup Operators	Backup Operators
Add User	Backup Operators	[illegible]	[illegible]		CN=Tommye Lemaster,OU=Users,OU=Enterprise,DC=addomain1,DC=local
Remove User	Backup Operators	[illegible]	DOMAIN1\DC2$;		CN=Latasha Craig,OU=Users,OU=Enterprise,DC=addomain1,DC=local
Modify	Backup Operators	[illegible]		Backup Operators	Backup Operators
Add User	Backup Operators	[illegible]	DOMAIN1\Quinton.Almeida;		CN=Latasha Craig,OU=Users,OU=Enterprise,DC=addomain1,DC=local
Remove User	Backup Operators	[illegible]	DOMAIN1\DC2$;		CN=Millie Holbrook,OU=Users,OU=Enterprise,DC=addomain1,DC=local

Figure 12: BuiltIn Group Changes

Amount of Generated Events per Category (Failed)

The **Amount of Generated Events per Category (Failed)** column chart displays the number of failed DSP security indicator events broken down by MITRE framework category.

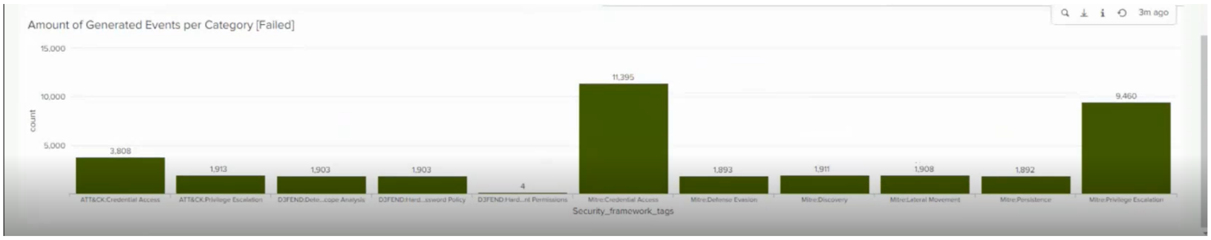


Figure 13: Amount of Generated Events per Category (Failed)

NOTE:

Security indicator data is only available with DSP Intelligence. Therefore, this view will be blank if you are running DSP Advanced.

Semperis DSP Security Indicators Dashboard

The Semperis DSP Security Indicators dashboard displays event data from the DSP Event logs (semperis_dsp index).

NOTE:

Security indicator data is only available with DSP Intelligence. Therefore, this dashboard will be blank if you are running DSP Advanced

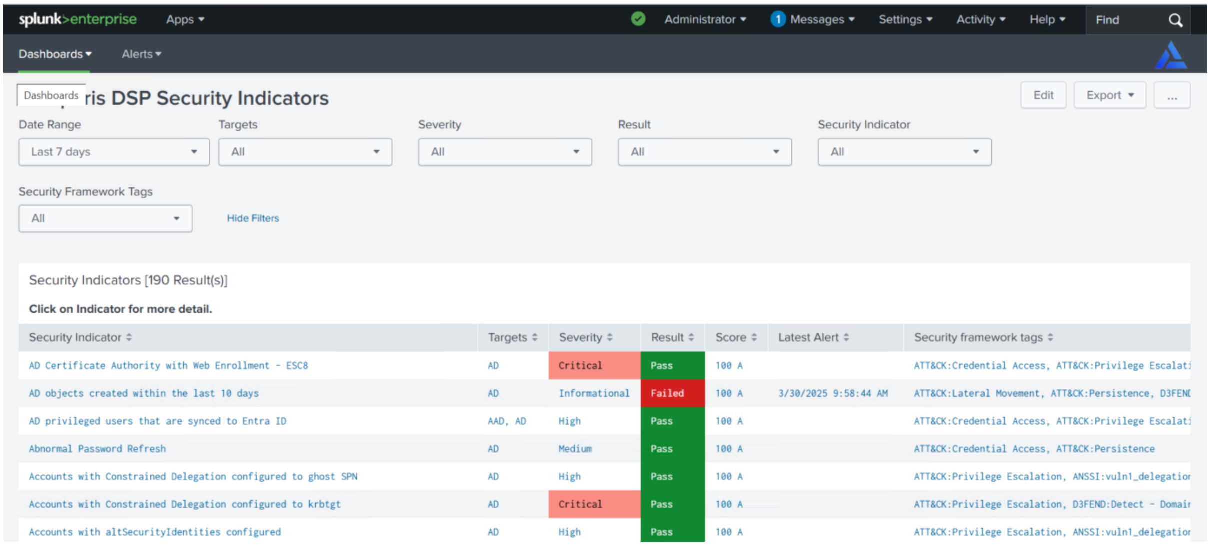
The data can be initially filtered using the controls at the top of the dashboard. Filters available include:

- Date range (Default: Last 7 days)
- Targets
- Severity
- Result

- Security indicator
- Security Framework Tags

NOTE:

It may take a few seconds to load the security indicator data.



Dashboards ris DSP Security Indicators

Date Range: Last 7 days
Targets: All
Severity: All
Result: All
Security Indicator: All
Security Framework Tags: All

Security Indicators [190 Result(s)]

Click on Indicator for more detail.

Security Indicator	Targets	Severity	Result	Score	Latest Alert	Security framework tags
AD Certificate Authority with Web Enrollment - ESC8	AD	Critical	Pass	100 A		ATT&CK:Credential Access, ATT&CK:Privilege Escalati
AD objects created within the last 10 days	AD	Informational	Failed	100 A	3/30/2025 9:58:44 AM	ATT&CK:Lateral Movement, ATT&CK:Persistence, D3FENI
AD privileged users that are synced to Entra ID	AAD, AD	High	Pass	100 A		ATT&CK:Credential Access, ATT&CK:Privilege Escalati
Abnormal Password Refresh	AD	Medium	Pass	100 A		ATT&CK:Credential Access, ATT&CK:Persistence
Accounts with Constrained Delegation configured to ghost SPN	AD	High	Pass	100 A		ATT&CK:Privilege Escalation, ANSSI:vuln1_delegatior
Accounts with Constrained Delegation configured to krbtgt	AD	Critical	Pass	100 A		ATT&CK:Privilege Escalation, D3FEND:Detect - Domair
Accounts with altSecurityIdentities configured	AD	High	Pass	100 A		ATT&CK:Privilege Escalation, ANSSI:vuln1_delegatior

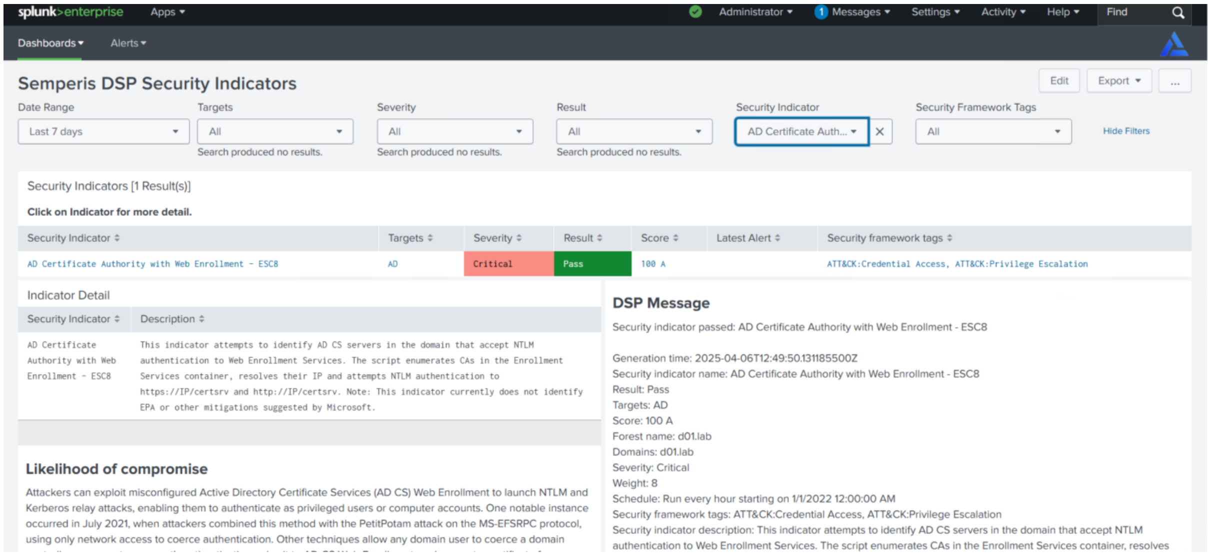
Figure 14: Semperis DSP Security Indicators dashboard: Security indicator events

Once filtered, the security indicator data can be sorted by clicking in a column heading:

- Security indicator
- Targets
- Severity
- Result
- Score
- Latest Alert
- Security framework tags

Clicking a security indicator in the table displays additional details about the selected indicator, including:

- Name and description
- DSP message
- Likelihood of compromise description
- Remediation actions



Semperis DSP Security Indicators

Date Range: Last 7 days
Targets: All — Search produced no results.
Severity: All — Search produced no results.
Result: All — Search produced no results.
Security Indicator: AD Certificate Auth...
Security Framework Tags: All

Security Indicators [1 Result(s)]

Click on Indicator for more detail.

Security Indicator	Targets	Severity	Result	Score	Latest Alert	Security framework tags
AD Certificate Authority with Web Enrollment - ESC8	AD	Critical	Pass	100 A		ATT&CK:Credential Access, ATT&CK:Privilege Escalation

Indicator Detail

Security Indicator	Description
AD Certificate Authority with Web Enrollment - ESC8	This indicator attempts to identify AD CS servers in the domain that accept NTLM authentication to Web Enrollment Services. The script enumerates CAs in the Enrollment Services container, resolves their IP and attempts NTLM authentication to https://IP/certsrv and http://IP/certsrv. Note: This indicator currently does not identify EPA or other mitigations suggested by Microsoft.

Likelihood of compromise

Attackers can exploit misconfigured Active Directory Certificate Services (AD CS) Web Enrollment to launch NTLM and Kerberos relay attacks, enabling them to authenticate as privileged users or computer accounts. One notable instance occurred in July 2021, when attackers combined this method with the PetitPotam attack on the MS-EFSRPC protocol, using only network access to coerce authentication. Other techniques allow any domain user to coerce a domain

DSP Message

Security indicator passed: AD Certificate Authority with Web Enrollment - ESC8

Generation time: 2025-04-06T12:49:50.131185500Z
Security indicator name: AD Certificate Authority with Web Enrollment - ESC8
Result: Pass
Targets: AD
Score: 100 A
Forest name: d01.lab
Domains: d01.lab
Severity: Critical
Weight: 8
Schedule: Run every hour starting on 1/1/2022 12:00:00 AM
Security framework tags: ATT&CK:Credential Access, ATT&CK:Privilege Escalation
Security indicator description: This indicator attempts to identify AD CS servers in the domain that accept NTLM authentication to Web Enrollment Services. The script enumerates CAs in the Enrollment Services container, resolves

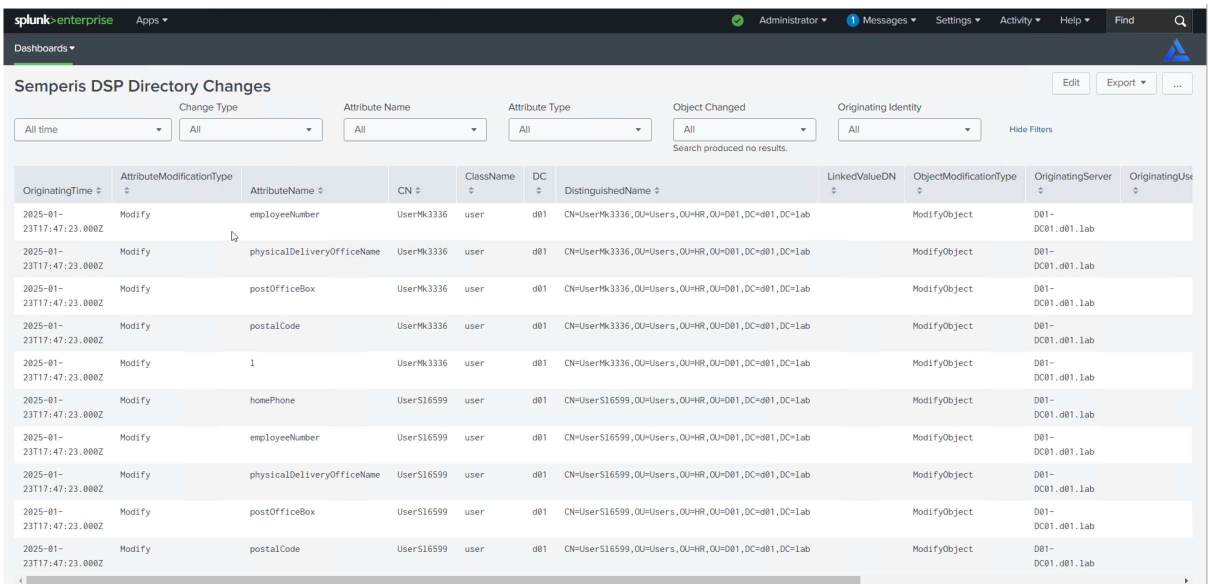
Figure 15: Semperis DSP Security Indicators dashboard: Details pane

Semperis DSP Directory Changes Dashboard

The **Semperis DSP Directory Changes** dashboard contains event data from DSP Syslog output (semperis_dsp_syslog index). It is a running log of AD changes forwarded from DSP (that is, same events as displayed in the **AD Changes** view in DSP). The data can be initially filtered using the controls at the top of the dashboard.

Available filters include:

- Date/time range (Default: All time)
- Change Type
- Attribute Name
- Attribute Type
- Object Changed
- Originating Identity



Semperis DSP Directory Changes

	Change Type	Attribute Name	Attribute Type	Object Changed	Originating Identity
All time	All	All	All	All Search produced no results.	All

OriginatingTime	AttributeModificationType	AttributeName	CN	ClassName	DC	DistinguishedName	LinkedValueDN	ObjectModificationType	OriginatingServer	OriginatingUse
2025-01-23T17:47:23.000Z	Modify	employeeNumber	UserMk3336	user	d01	CN=UserMk3336,OU=Users,OU=HR,OU=D01,DC=d01,DC=lab		ModifyObject	D01-DC01.d01.lab	
2025-01-23T17:47:23.000Z	Modify	physicalDeliveryOfficeName	UserMk3336	user	d01	CN=UserMk3336,OU=Users,OU=HR,OU=D01,DC=d01,DC=lab		ModifyObject	D01-DC01.d01.lab	
2025-01-23T17:47:23.000Z	Modify	postOfficeBox	UserMk3336	user	d01	CN=UserMk3336,OU=Users,OU=HR,OU=D01,DC=d01,DC=lab		ModifyObject	D01-DC01.d01.lab	
2025-01-23T17:47:23.000Z	Modify	postalCode	UserMk3336	user	d01	CN=UserMk3336,OU=Users,OU=HR,OU=D01,DC=d01,DC=lab		ModifyObject	D01-DC01.d01.lab	
2025-01-23T17:47:23.000Z	Modify	l	UserMk3336	user	d01	CN=UserMk3336,OU=Users,OU=HR,OU=D01,DC=d01,DC=lab		ModifyObject	D01-DC01.d01.lab	
2025-01-23T17:47:23.000Z	Modify	homePhone	UserS16599	user	d01	CN=UserS16599,OU=Users,OU=HR,OU=D01,DC=d01,DC=lab		ModifyObject	D01-DC01.d01.lab	
2025-01-23T17:47:23.000Z	Modify	employeeNumber	UserS16599	user	d01	CN=UserS16599,OU=Users,OU=HR,OU=D01,DC=d01,DC=lab		ModifyObject	D01-DC01.d01.lab	
2025-01-23T17:47:23.000Z	Modify	physicalDeliveryOfficeName	UserS16599	user	d01	CN=UserS16599,OU=Users,OU=HR,OU=D01,DC=d01,DC=lab		ModifyObject	D01-DC01.d01.lab	
2025-01-23T17:47:23.000Z	Modify	postOfficeBox	UserS16599	user	d01	CN=UserS16599,OU=Users,OU=HR,OU=D01,DC=d01,DC=lab		ModifyObject	D01-DC01.d01.lab	
2025-01-23T17:47:23.000Z	Modify	postalCode	UserS16599	user	d01	CN=UserS16599,OU=Users,OU=HR,OU=D01,DC=d01,DC=lab		ModifyObject	D01-DC01.d01.lab	

Figure 16: Semperis DSP Directory Changes: Change events

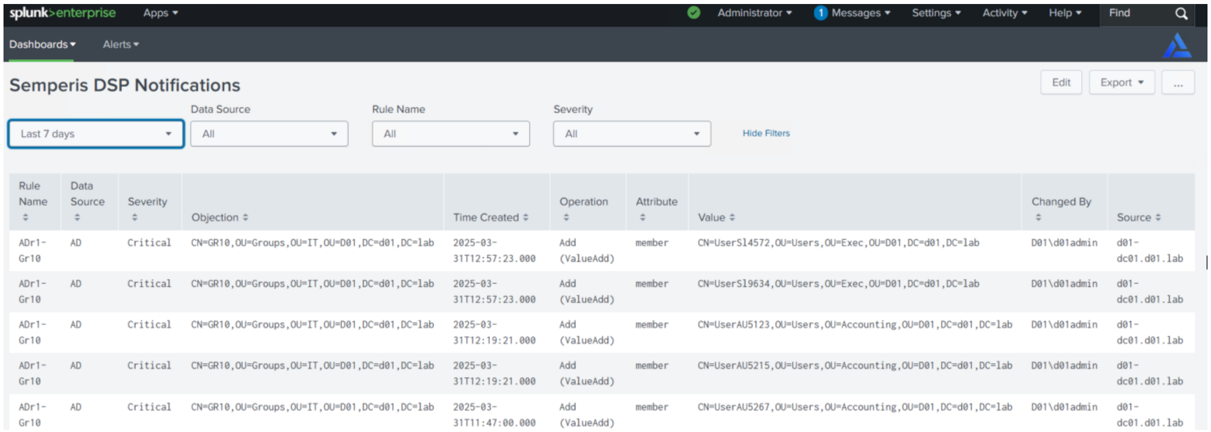
Once filtered, AD change data can be sorted by clicking in a column heading:

- Originating Time
- Attribute Modification Type
- Attribute Name
- CN
- Class Name
- DC
- DistinguishedName
- LinkedValueDN
- ObjectModificaitonType
- Originating Server
- OriginatingUserWorksations
- OriginatingUsers
- PartitionNamingContext
- StringValueFrom
- StringValueTo

Semperis DSP Notifications Dashboard

The **Semperis DSP Notifications** dashboard displays a table of notification rule events forwarded from DSP Event logs (semperis_dsp index). The data can be initially filtered using the controls at the top of the dashboard. Available filters include:

- Date/time range (Default: Last 24 hours)
- Data Source
- Rule name
- Severity



Semperis DSP Notifications

Last 7 days ▾ | Data Source: All ▾ | Rule Name: All ▾ | Severity: All ▾

Rule Name	Data Source	Severity	Objection	Time Created	Operation	Attribute	Value	Changed By	Source
ADr1-Gr10	AD	Critical	CN=GR10,OU=Groups,OU=IT,OU=D01,DC=d01,DC=lab	2025-03-31T12:57:23.000	Add (ValueAdd)	member	CN=UserS14572,OU=Users,OU=Exec,OU=D01,DC=d01,DC=lab	D01\d01admin	d01-dc01.d01.lab
ADr1-Gr10	AD	Critical	CN=GR10,OU=Groups,OU=IT,OU=D01,DC=d01,DC=lab	2025-03-31T12:57:23.000	Add (ValueAdd)	member	CN=UserS19634,OU=Users,OU=Exec,OU=D01,DC=d01,DC=lab	D01\d01admin	d01-dc01.d01.lab
ADr1-Gr10	AD	Critical	CN=GR10,OU=Groups,OU=IT,OU=D01,DC=d01,DC=lab	2025-03-31T12:19:21.000	Add (ValueAdd)	member	CN=UserAU5123,OU=Users,OU=Accounting,OU=D01,DC=d01,DC=lab	D01\d01admin	d01-dc01.d01.lab
ADr1-Gr10	AD	Critical	CN=GR10,OU=Groups,OU=IT,OU=D01,DC=d01,DC=lab	2025-03-31T12:19:21.000	Add (ValueAdd)	member	CN=UserAU5215,OU=Users,OU=Accounting,OU=D01,DC=d01,DC=lab	D01\d01admin	d01-dc01.d01.lab
ADr1-Gr10	AD	Critical	CN=GR10,OU=Groups,OU=IT,OU=D01,DC=d01,DC=lab	2025-03-31T11:47:00.000	Add (ValueAdd)	member	CN=UserAU5267,OU=Users,OU=Accounting,OU=D01,DC=d01,DC=lab	D01\d01admin	d01-dc01.d01.lab

Figure 17: Semperis DSP Notifications dashboard: Notification rule events

Once filtered, notification rule events can be sorted by clicking in a column heading:

- Rule Name
- Data Source
- Severity
- Objection
- Time Created
- Operation
- Attribute
- Value
- Changed By
- Source

APPENDIX A

Manually Add DSP Alerts

You can create alerts in Splunk based on the DSP activity being captured. The following procedure guides you through adding alerts in Splunk, and provides the details required to capture the DSP-related activity used to trigger alerts in Splunk. For more information, see the Splunk guidelines.

This procedure uses the following alerts as examples: Critical DSP Notification Fired, Critical Security Indicator Failed, Failed User logins, Security Indicator Change Pass to Fail, and Trustee RBAC Change. You can replace these alerts to better fit your needs.

1. Stop the Splunkd Service.
2. To add **Alerts** to the navigation bar in the Splunk Enterprise console, add the following information to the `C:\Program Files\Splunk\etc\apps\semperis_dsp\default\data\ui\nav\default.xml` file:

   ```
   <collection label="Alerts">
         <view name="alerts" />
         <a href="/alerts/semperis_dsp" target="_blank">Triggered
         Alerts</a>
   </collection>
   ```

3. To add permissions to the **Alerts** page, add the following information to the `C:\Program Files\Splunk\etc\apps\semperis_dsp\metadata\local.meta` file:

   ```
   [savedsearches/Security%20Indicator%20Failed]
   access = read : [ * ], write : [ <Splunk User> ]
   export = none
   owner = <Splunk User>
   version = <Splunk Version>


   [savedsearches/Security%20Indicator%20Change%20Pass%20to%20Fail]
   access = read : [ * ], write : [ <Splunk User> ]
   export = none
   owner = <Splunk User>
   version = <Splunk Version>
   ```

```
[savedsearches/Critical%20Security%20Indicator%20Failed]
access = read : [ * ], write : [ <Splunk User> ]
export = none
owner = <Splunk User>
version = <Splunk Version>

[savedsearches/Trustee%20RBAC%20Change]
access = read : [ * ], write : [ <Splunk User> ]
export = none
owner = <Splunk User>
version = <Splunk Version>

[savedsearches/Failed%20user%20logins]
access = read : [ * ], write : [ <Splunk User> ]
export = none
owner = <Splunk User>
version = <Splunk Version>

[savedsearches/Critical%20DSP%20Notification%20Fired]
access = read : [ * ], write : [ <Splunk User> ]
export = none
owner = <Splunk User>
version = <Splunk Version>
```

Where:

`<Splunk User>` is the user logged in to the Splunk server

`<Splunk Version>` is the Splunk server version

4. To add alerts to the **Alerts** page, add the following alert settings and search criteria to the `C:\Program Files\Splunk\etc\apps\semperis_dsp\default\savedsearches.conf` file:

> ***NOTE:***
>
> *The alert settings are the same for each type of alert. However, the search criteria is unique to each alert type.*

```
[Critical DSP Notification Fired]
action.webhook.enable_allowlist = 0
alert.severity = 4
alert.suppress = 0
alert.suppress.fields = *
alert.suppress.period = 15m
alert.track = 1
counttype = number of events
cron_schedule = */5 * * * *
dispatch.earliest_time = -5m
dispatch.latest_time = now
display.events.fields =\
["DataValueFrom_StringValue","DataValueTo_StringValue","Result"]
display.general.type = statistics
display.page.search.mode = verbose
display.page.search.patterns.sensitivity = 0.3
display.page.search.tab = statistics
display.visualizations.charting.chart.style = minimal
display.visualizations.custom.type = simple_xml_examples.tagcloud
enableSched = 1
quantity = 0
relation = greater than
request.ui_dispatch_app = semperis_dsp
request.ui_dispatch_view = search
search = index="semperis_dsp"\
source="WinEventLog:Semperis-DSP-Notifications/Operational"\
Severity=Critical | rename Notification_Rule_Triggered as "Rule\
Name" | table "Rule Name" Operation Severity
```

```
[Critical Security Indicator Failed]
action.webhook.enable_allowlist = 0
alert.severity = 4
alert.suppress = 0
alert.suppress.fields = *
alert.suppress.period = 15m
alert.track = 1
counttype = number of events
cron_schedule = */5 * * * *
disabled = 1
dispatch.earliest_time = -5m
dispatch.latest_time = now
display.events.fields =\
["DataValueFrom_StringValue","DataValueTo_StringValue","Result"]
display.general.type = statistics
display.page.search.mode = verbose
display.page.search.patterns.sensitivity = 0.3
display.page.search.tab = statistics
display.visualizations.charting.chart.style = minimal
display.visualizations.custom.type = simple_xml_examples.tagcloud
enableSched = 1
quantity = 0
relation = greater than
request.ui_dispatch_app = semperis_dsp
request.ui_dispatch_view = search
search = index="semperis_dsp" Result=* | sort -_time |\
where Result="Failed" AND Severity="Critical" |\
dedup Security_indicator_name sortby -_time|\
table "Security Indicator", Severity, Result, Message,\
Remediation, "Security framework tags", Likelihood_of_compromise
```

```
[Failed user logins]
action.webhook.enable_allowlist = 0
alert.severity = 4
alert.suppress = 0
alert.suppress.fields = *
alert.suppress.period = 15m
alert.track = 1
alert_condition = search "Failed Logins" > 3
counttype = custom
cron_schedule = */5 * * * *
dispatch.earliest_time = -5m
dispatch.latest_time = now
display.events.fields =\
["DataValueFrom_StringValue","DataValueTo_StringValue","Result"]
display.general.type = statistics
display.page.search.mode = verbose
display.page.search.patterns.sensitivity = 0.3
display.page.search.tab = statistics
display.visualizations.charting.chart.style = minimal
display.visualizations.custom.type = simple_xml_examples.tagcloud
enableSched = 1
quantity = 3
relation = greater than
request.ui_dispatch_app = semperis_dsp
request.ui_dispatch_view = search
search = index="semperis_dsp"\
source="WinEventLog:Semperis-Operation-Log/Operational" \
(EventCode=20000 OR EventCode=20002) Access_Granted=false\
| rex "Occured at \(UTC\)\: (?<Occured>.*)"\
| rex "Source: (?<Source>[.]+)" \
| eval Trustee_Name=lower(Trustee_Name), Source=lower(Source)\
| eval Trustee_Name_Count=Trustee_Name\
| stats count as FailedLogins by Trustee_Name\
| dedup Trustee_Name\
| rename FailedLogins as "Failed Logins"\
| table Trustee_Name, "Failed Logins"
```

```
[Security Indicator Change Pass to Fail]
action.webhook.enable_allowlist = 0
alert.severity = 4
alert.suppress = 0
alert.suppress.fields = *
alert.suppress.period = 15m
alert.track = 1
counttype = number of events
cron_schedule = */5 * * * *
dispatch.earliest_time = -5m
dispatch.latest_time = now
display.events.fields =\
["DataValueFrom_StringValue","DataValueTo_StringValue","Result"]
display.general.type = statistics
display.page.search.mode = verbose
display.page.search.patterns.sensitivity = 0.3
display.page.search.tab = statistics
display.visualizations.charting.chart.style = minimal
display.visualizations.custom.type = simple_xml_examples.tagcloud
enableSched = 1
quantity = 0
relation = greater than
request.ui_dispatch_app = semperis_dsp
request.ui_dispatch_view = search
search = index="semperis_dsp" Result=* | sort _time |\
streamstats current=f window=1 global=f\
last(Result) as last_Result by Security_indicator_name | where\
Result!=last_Result AND Result="Failed" | \
rename Security_indicator_name as "Security Indicator",\
Security_indicator_description as "Description",\
Security_framework_tags as "Security framework tags"|\
table "Security Indicator", Severity, Result, Message,\
Remediation, "Security framework tags", Likelihood_of_compromise
```

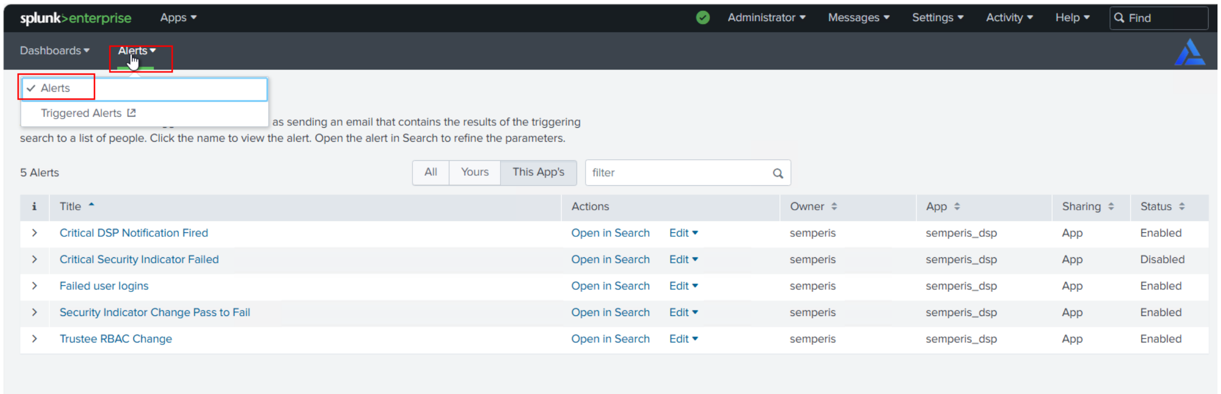
```
[Trustee RBAC Change]
action.webhook.enable_allowlist = 0
alert.expires = 30d
alert.severity = 4
alert.suppress = 0
alert.suppress.fields = *
alert.suppress.period = 15m
alert.track = 1
counttype = number of events
cron_schedule = */5 * * * *
dispatch.earliest_time = -5m
dispatch.latest_time = now
display.events.fields =\
["DataValueFrom_StringValue","DataValueTo_StringValue","Result"]
display.general.type = statistics
display.page.search.mode = verbose
display.page.search.patterns.sensitivity = 0.3
display.page.search.tab = statistics
display.visualizations.charting.chart.style = minimal
display.visualizations.custom.type = simple_xml_examples.tagcloud
enableSched = 1
quantity = 0
relation = greater than
request.ui_dispatch_app = semperis_dsp
request.ui_dispatch_view = search
search = index="semperis_dsp"\
source="wineventlog:semperis-operation-log/operational"\
Component=rbac \
| rex max_match=20 "{ Name =(?<Persona_Details>[\w\s]+) }"\
| rex "Occured at \(UTC\)\: (?<Occured>.*)"\
| rename "Trustee_Name" as "Changed By" "trustee" as "User Added"\
"Access_Granted" as "Access Granted" Occured as Timestamp\
| table "User Added" "Persona_Details" "Access Granted"
```

5. Start the Splunkd Service.

   In the Splunk Enterprise console, click **Alerts** > **Alerts** to view the manually added alerts. Click **Alerts** > **Triggered Alerts** to view triggered alerts.

   NOTE:

   *To edit the alerts after adding them, go to the **Alerts** page, navigate to the alert you want to edit, and click **Edit**.*



as sending an email that contains the results of the triggering search to a list of people. Click the name to view the alert. Open the alert in Search to refine the parameters.

5 Alerts

i	Title	Actions		Owner	App	Sharing	Status
›	Critical DSP Notification Fired	Open in Search	Edit ▾	semperis	semperis_dsp	App	Enabled
›	Critical Security Indicator Failed	Open in Search	Edit ▾	semperis	semperis_dsp	App	Disabled
›	Failed user logins	Open in Search	Edit ▾	semperis	semperis_dsp	App	Enabled
›	Security Indicator Change Pass to Fail	Open in Search	Edit ▾	semperis	semperis_dsp	App	Enabled
›	Trustee RBAC Change	Open in Search	Edit ▾	semperis	semperis_dsp	App	Enabled