semperis

Directory Services Protector

Version: 4.0 SP2 to 5.0

Microsoft Sentinel Integration Guide

May 2025 (6)

Legal Notice

Contents

Preface 4
Document Revisions 4
Styles and Conventions used in this Document 4
Contacting Semperis 5
DSP Microsoft Sentinel Solution Overview 6
Prerequisites 7
Getting Started with Microsoft Sentinel 8
Create the Semperis Directory Services Protector Solution app in Azure 9
Deploy the Directory Services Protector Solution 11
Configure DSP to Forward Events 14
Semperis Directory Services Protector Solution Package 22
DSP Data Connectors 22
DSP Parser 23
DSP Workbook 23
Analytic Rules 24
Enable a Sample Analytic Rule 25

Preface

Welcome to the *Microsoft Sentinel Integration Guide* for *Directory Services Protector*. This guide is intended for administrators responsible for configuring Microsoft Sentinel to receive security indicator events from DSP's Security event log.

Document Revisions

Table 1: Microsoft Sentinel Integration Guide Revisions

Product version	Date	Document revision	Comments
DSP 3.5 and later	September 2021	1	Initial publishing of document
DSP 3.8 or later	June 2023	2	Offer updated
DSP 3.8 or later	April 2024	3	Microsoft Sentinel renaming
DSP 3.8 to 4.1	February 2025	4	New configuring process, updated to support DSP 4.1
DSP 4.0 SP2 and DSP 4.1	April 2025	5	Updated version compatibility
DSP 4.0 SP2 to DSP 5.0	May 2025	6	Updated to support DSP 4.2 and DSP 5.0

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.

Typeface	Description
`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 Microsoft Sentinel Solution Overview

Semperis Directory Services Protector (DSP) provides valuable insight into your Active Directory security posture. It queries your Active Directory environment and performs a set of tests against many aspects of Active Directory's security posture, including AD Delegation, Account security, AD Infrastructure security, Group Policy security, and Kerberos security. Each security indicator is mapped to MITRE ATT&CK® framework categories, explains what was evaluated, and indicates how likely an exposure will compromise Active Directory. Each IoE found highlights weak Active Directory configurations and provides actionable guidance on how to close gaps before they are exploited by attackers.

Microsoft Sentinel 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 now available in Microsoft Azure Marketplace allows you to easily integrate DSP with Microsoft Sentinel to present relevant indicators of exposure (IOEs) in familiar Sentinel dashboards mapped to the security frameworks you rely on--such as MITRE.

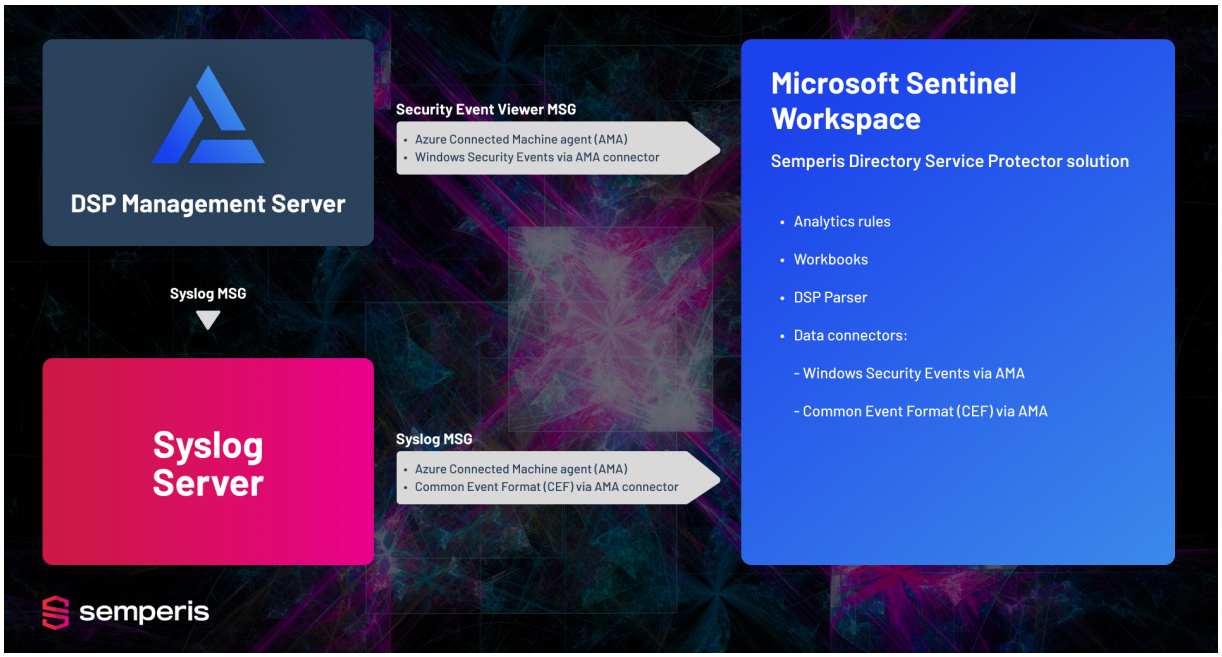


Figure 1: The process of how to forward events to Sentinel

The Semperis Directory Services Protector solution provides the artifacts required to successfully integrate with Microsoft Sentinel. The Semperis Directory Services Protector solution includes a basic set of components to get you started, for example:

- The DSP data connector provides real-time integration with DSP's Security Windows event log to capture events related to the security indicators that continuously run to detect advanced attacks and enable rapid response to Active Directory vulnerabilities.
- A second data connector, Common Event Format (CEF) via AMA, ingests Active Directory change data via Syslog Common Event Format configuration with DSP.
- The parser (dsp_parser) transforms the ingested data into Microsoft Sentinel normalized format. The filtering performed by the parser provides meaningful context that is easy to understand and highly actionable. The dsp_parser is used by the workbooks and analytic rule templates provided.
- The sample analytic rules provided allow you to concentrate on "high value" indicators of exposure and enable you to generate custom alerts based on these incidents.
- The DSP workbook provides a dashboard where you can easily monitor and analyze data within the Azure portal. Using the workbook provided in the Semperis Directory Services Protector solution, you can determine how you are doing from a security perspective, compared to best practice environments.

Using these components as a basis, you can customize the Semperis Directory Services Protector solution to best meet your organization's requirements.

Prerequisites

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

Table 3: DSP requirements

Component	Requirements
DSP Edition	One of the following DSP editions is required: • DSP Advanced • DSP Intelligence
DSP Version	Minimum version supported is v4.0 SP2 up to and including v5.0.

In addition, to get started with Microsoft Sentinel you need a Microsoft Azure subscription and a Linux-based Syslog server with Python installed. Before deploying Microsoft Sentinel, ensure that your Microsoft Entra tenant meets the requirements listed in the Microsoft Sentinel Documentation (https://docs.microsoft.com/en-us/azure/sentinel/prerequisites).

CHAPTER 2

Getting Started with Microsoft Sentinel

If you are new to Microsoft Sentinel, please review this topic to enable Microsoft Sentinel or the Quickstart: Onboard Microsoft Sentinel documentation from Microsoft.

NOTE:

For those already familiar with Microsoft Sentinel, you can skip this getting started topic; however, please note that you need to create a Log Analytics workspace for the DSP log data.

Global prerequisites:

- Active Azure Subscription
- Log Analytics workspace
- To enable Microsoft Sentinel, you need contributor permissions to the subscription where the Microsoft Sentinel workspace resides.
- To use Microsoft Sentinel, you need contributor or reader permissions on the resource group to which the workspace belongs.

To enable Microsoft Sentinel:

1. Sign in to the Azure portal. Ensure you have selected the subscription in which Microsoft Sentinel was created.
2. Search for and select **Microsoft Sentinel**.
3. Select **Add**.
4. On the **Choose a workspace to add to Microsoft Sentinel** screen, search for and select the workspace to be used or click the **Create a new workspace** to create a new one.
5. Select **Add Microsoft Sentinel**.

Next steps:

- *Create the Semperis Directory Services Protector Solution app in Azure*
- *Deploy the Directory Services Protector Solution*

- *Configure DSP to Forward Events*

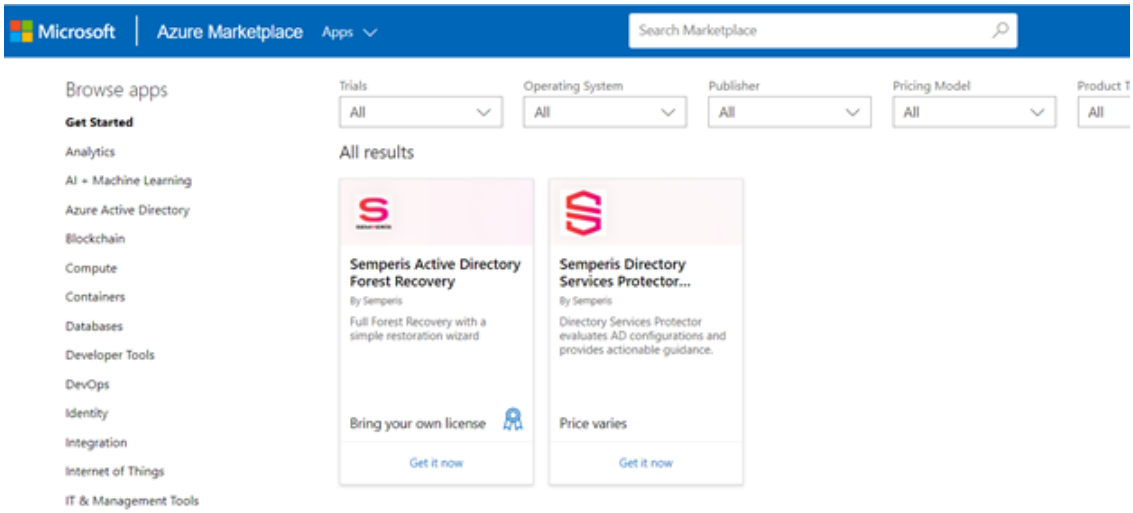
Create the Semperis Directory Services Protector Solution app in Azure

The Semperis Directory Services Protector Solution is available from the Azure Marketplace.

To create the Semperis Directory Services Protector solution app in Azure:

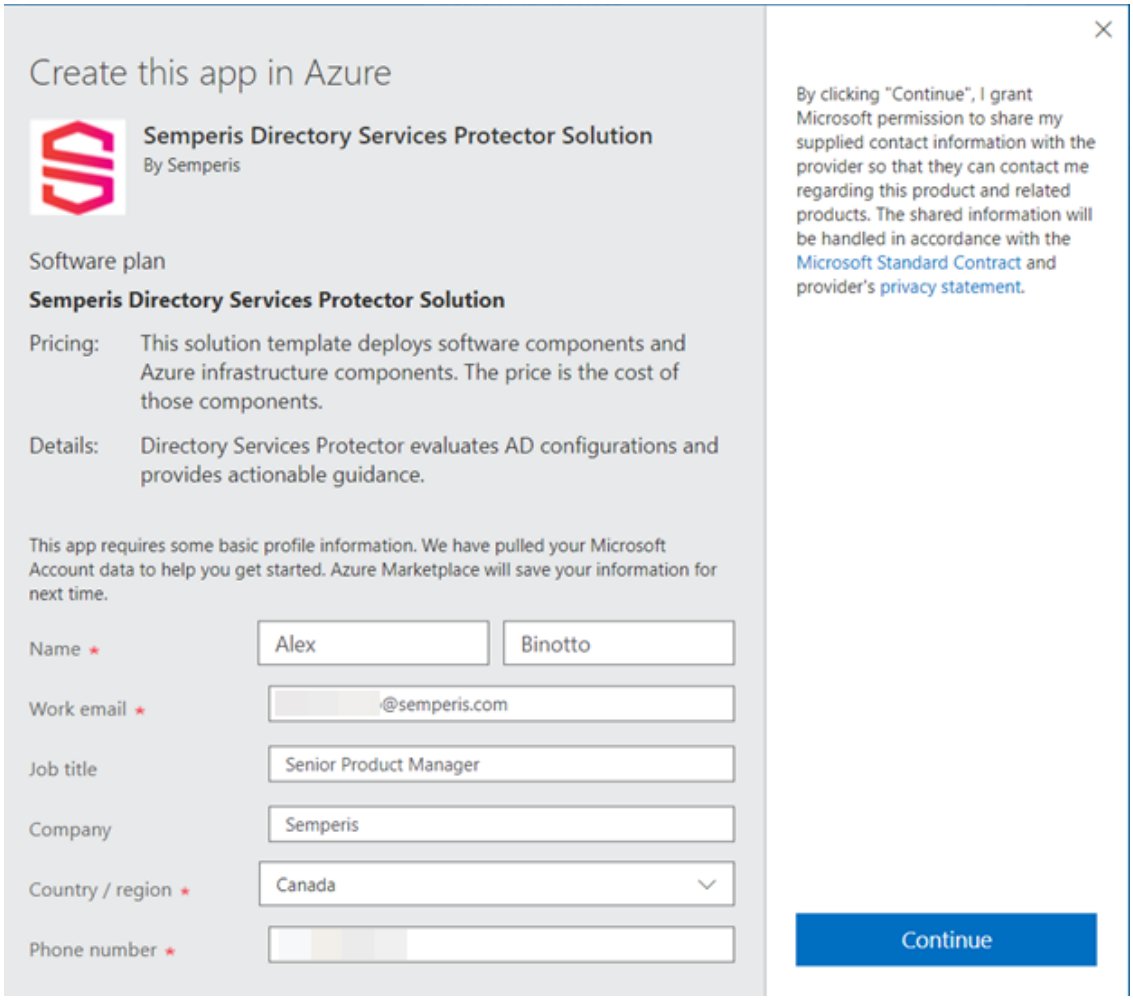
1. Go to Azure Marketplace.
2. In the search bar at the top of the page, enter **semperis**.

   The solutions available from Semperis are listed in the results pane.



3. In the **Semperis Directory Services Protector Solution** tile, click **Get it now**.
4. If you are not signed in, you will be prompted to sign in to Microsoft Azure Marketplace.

   Enter the email address of the account to be used to create and access the Semperis Directory Services Protector app in Azure. Click **Sign in**.
5. On the **Create this app in Azure** screen, enter the requested information.



Microsoft automatically populates fields based on your Microsoft account. Review and update any fields as required (required fields are marked with a red asterisk (*)):

- Name*: First and last name.
- Work email*: Valid work email address.
- Job title: Your job title.
- Company: Name of your company.
- Country / region*: Select the country or region where you reside.
- Phone number *: Valid phone number.

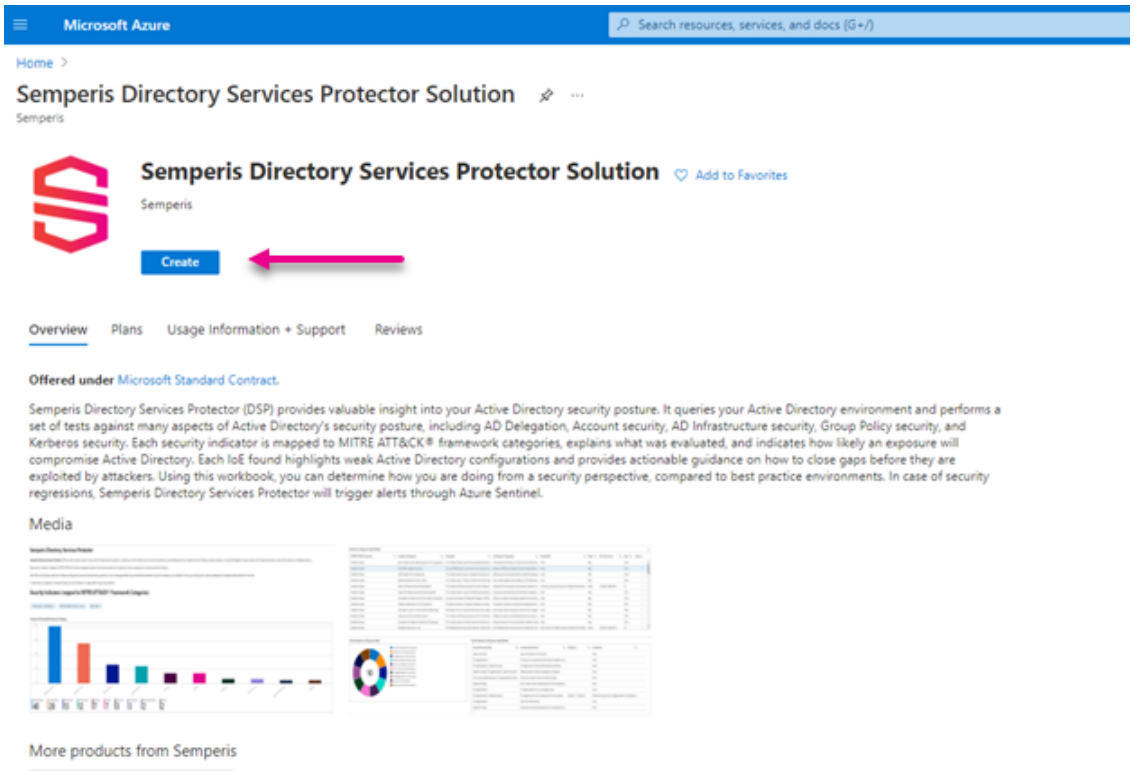
Click **Continue**.

Deploy the Directory Services Protector Solution

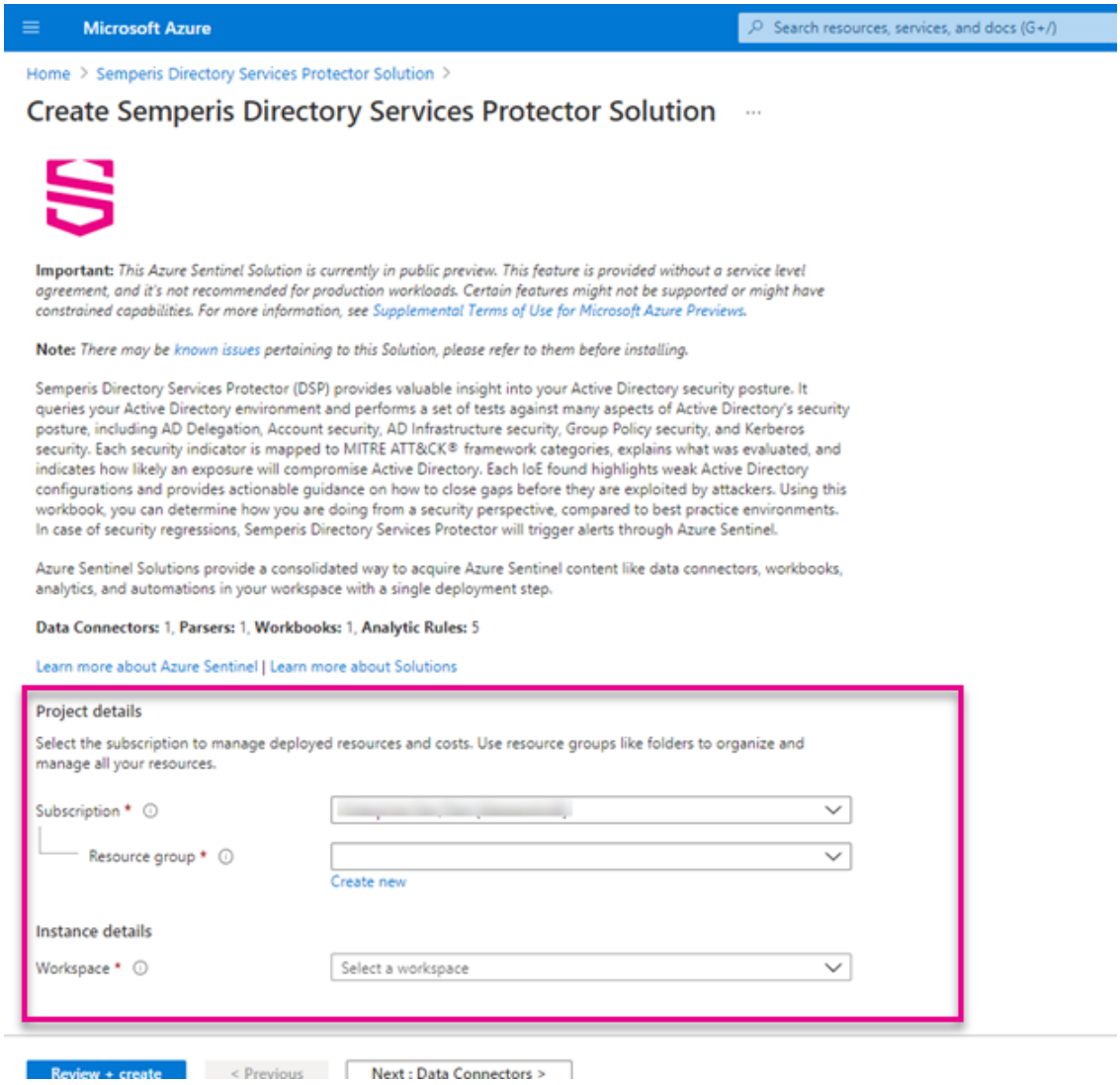
To deploy the Semperis Directory Services Protector solution, you need to log in to your Microsoft Entra tenant.

To deploy the solution:

1. Once you are logged in to the Microsoft Entra tenant, click **Create**.



2. On the **Create Semperis Directory Services Protector Solution** screen, select the Azure subscription, resource group, and Microsoft Sentinel workspace to be used.



In the **Project details** pane, select the following information:

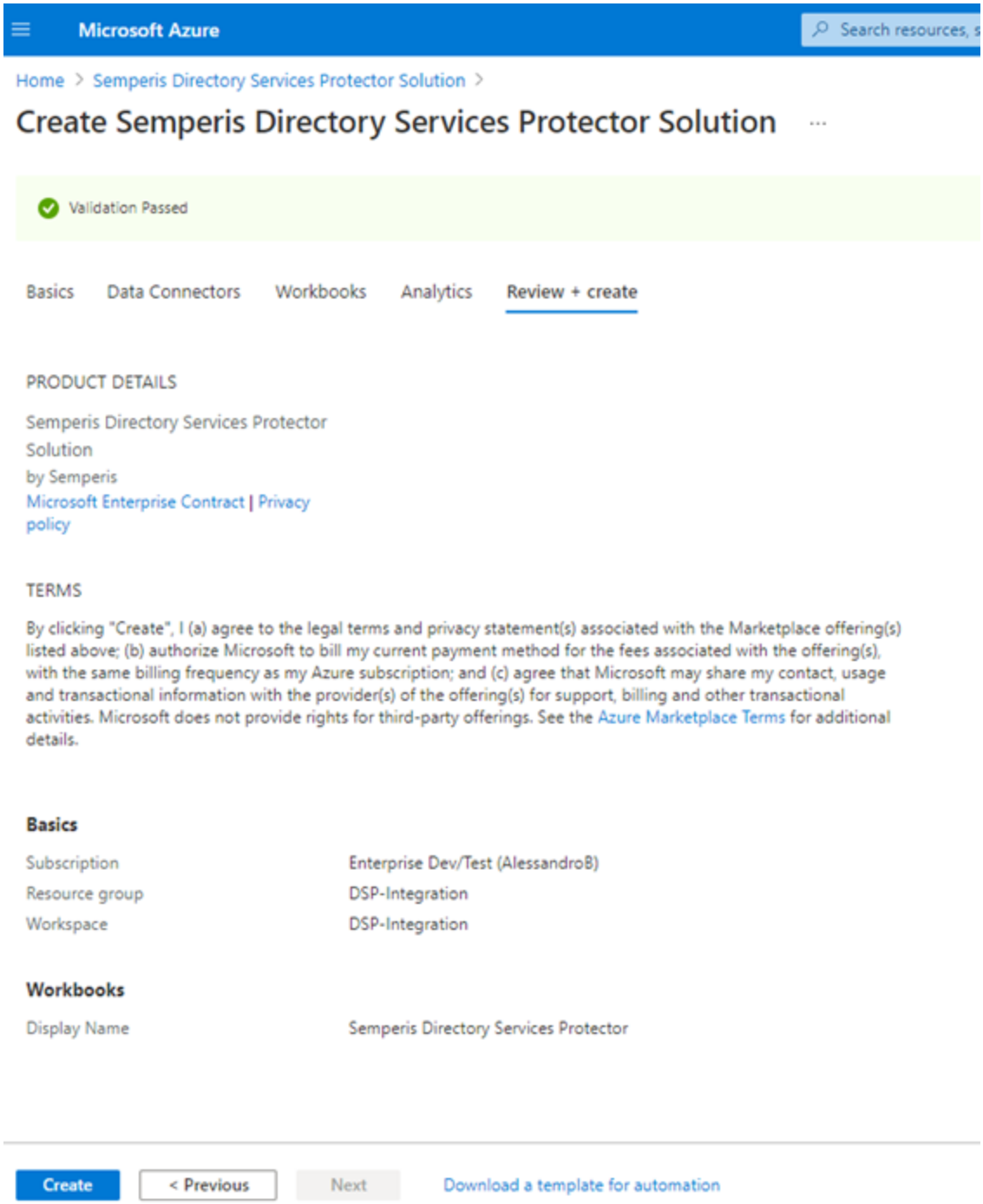
- Subscription*: The subscription in which the Microsoft Sentinel workspace resides.
- Resource group*: The resource group that the workspace belongs to.

In the **Instance details** pane, select the following information:

- Workspace*: The Log Analytics workspace being used for the DSP log data.

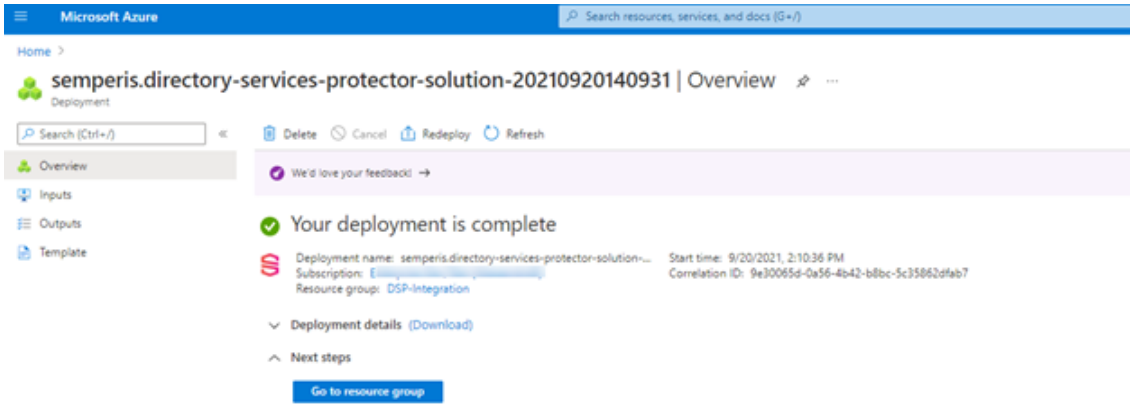
Click **Review + create**.

3. Review and validate the product details displayed, such as subscription, resource group, and workspace. Also review the legal terms under the **Terms** section of this screen.



4. Once validated, click **Create**.

   Once the DSP solution is created, you will see a "Your deployment is complete" message and the product details for the solution.



The newly created Directory Services Protector solution includes the following components:

- Data connector
- Parser (dsp_parser)
- Analytic rules
- Workbook

For more information about these components, see the *Semperis Directory Services Protector Solution Package*.

Configure DSP to Forward Events

To start forwarding the Windows events to the Microsoft Sentinel workspace, you must first configure the Azure Connected Machine Agent on your Semperis Directory Services Protector Management Server and on your Syslog server.

For more information and instructions, see the Microsoft document Connect hybrid machines to Azure using a deployment script.

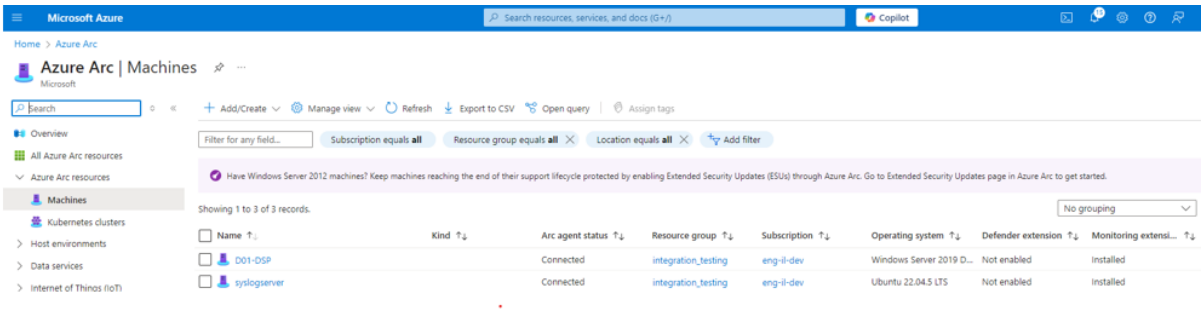
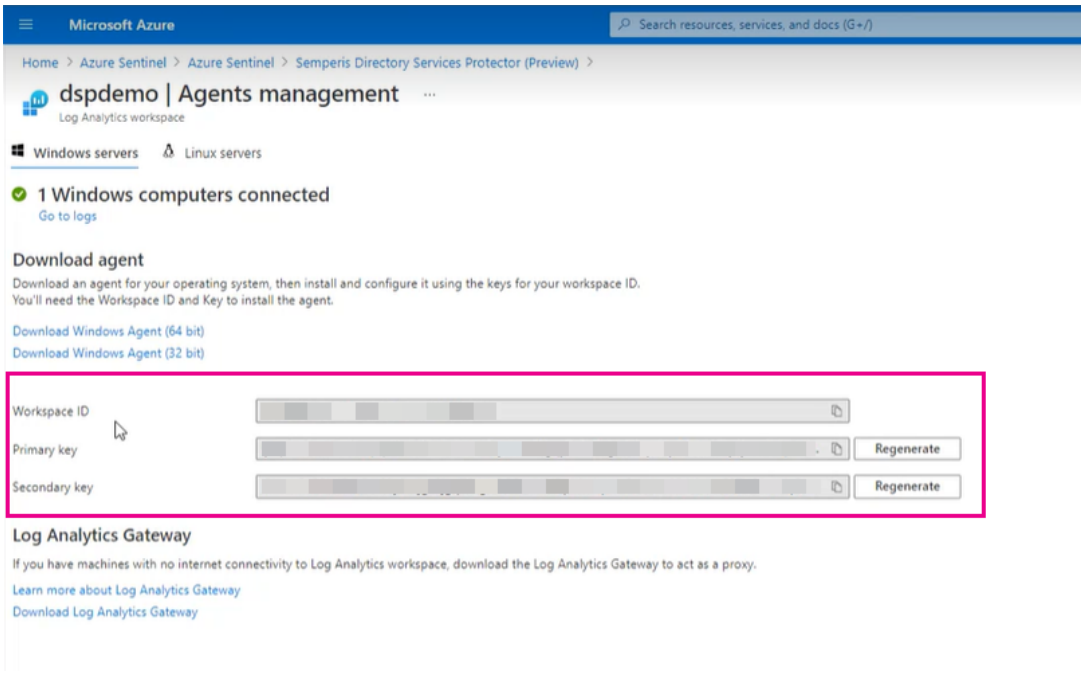


Figure 2: Azure Arc page: View the machines that are connected using Azure Machine Agent (AMA)

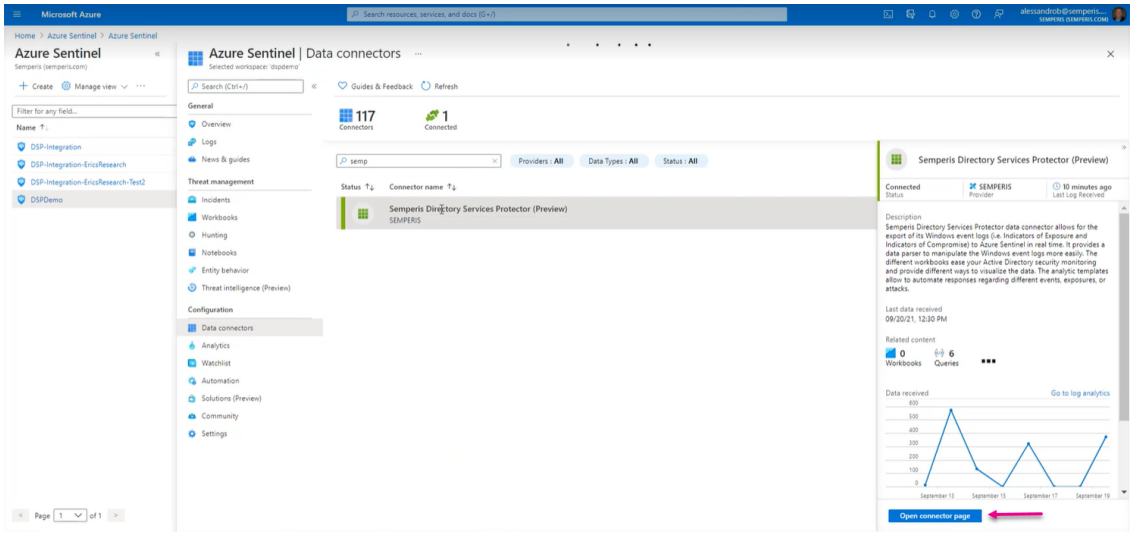
NOTE:

You will need the workspace ID and keys listed on the Log Analytics workspace page to install the agent. You can get back to this page by clicking ***Agents management*** *under the* ***Settings*** *menu in the navigation pane in Microsoft Sentinel.*



To configure DSP to forward events to Microsoft Sentinel:

1. Open Microsoft Sentinel and select the workspace you defined for the DSP solution.
2. Click **Content hub** under the **Content management** menu in the navigation pane.
3. Search for and install **Semperis Directory Services Protector**.
4. Click **Data connectors** under the **Configuration** menu in the navigation pane.
5. From the data connectors gallery, search for and select the **Semperis Directory Services Protector** data connector.
6. At the bottom of the right pane, click the **Open connector page** button.



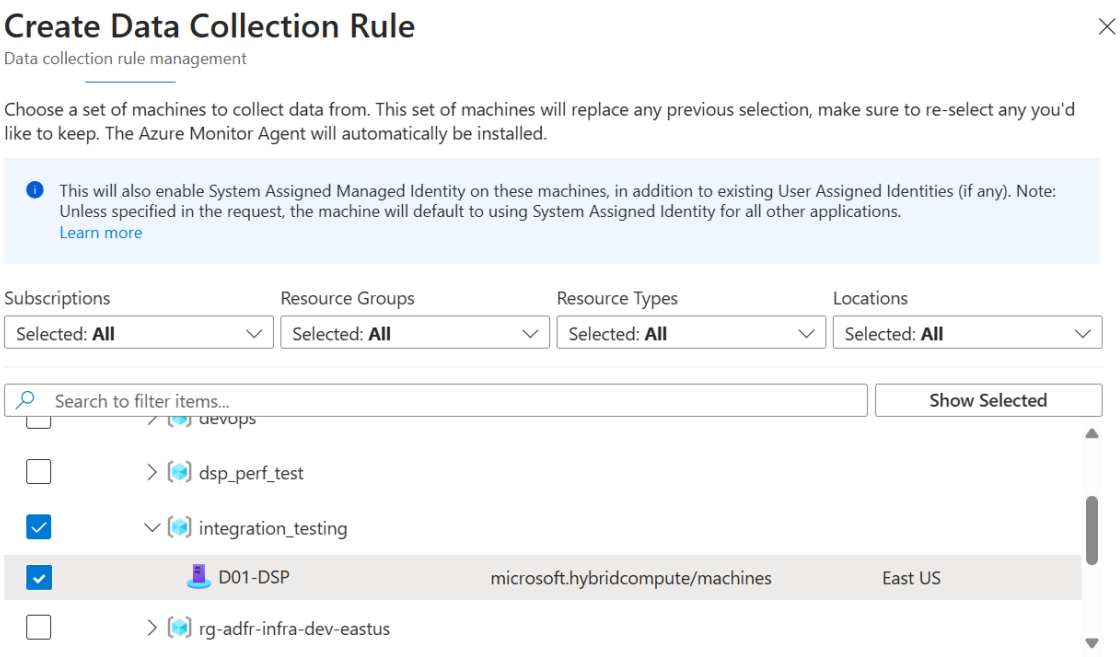
7. From the **Instructions** tab, follow the configuration instructions.

   The instructions provided include the following:

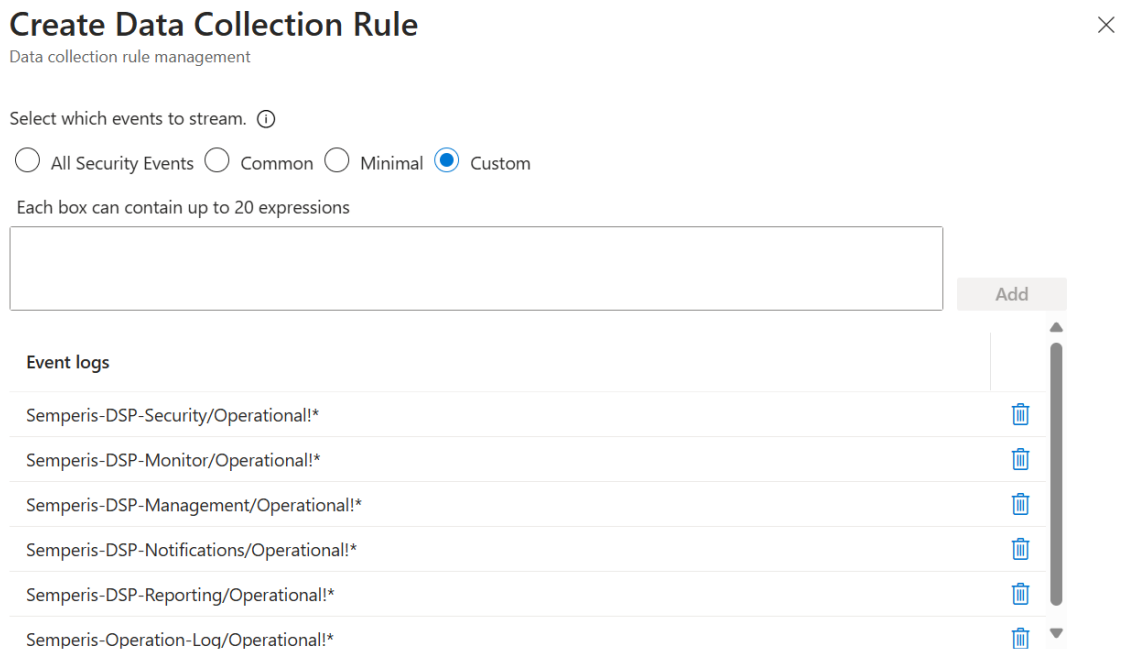
   - Configure Semperis DSP Management Server to send Windows event logs to your Microsoft Sentinel workspace.
   - Configure Semperis DSP Management Server to send Common event format logs to your Microsoft Sentinel workspace.

To configure DSP to forward Windows events to Microsoft Sentinel:

1. Open Microsoft Sentinel and select the workspace you defined for the DSP solution.
2. Click **Content hub** under the **Content management** menu in the navigation pane.
3. Search for and install **Windows Security Events via AMA**.
4. Select **Data connectors** under the **Configuration** menu in the navigation pane.
5. From the data connectors gallery, search for and select the **Windows Security Events via AMA** data connector.
6. At the bottom of the right pane, click the **Open connector page** button.
7. Click **Create Data Collection Rule**.
8. Name the rule and enter the **Subscription** and **Resource group** in the text fields.
9. In the **Resources** tab, verify that the DSP Server machine from which the data is to be collected from is listed.



10. In the **Collect** tab, select **Custom**, then add the following event logs expressions:
    - Semperis-DSP-Security/Operational!*
    - Semperis-DSP-Monitor/Operational!*
    - Semperis-DSP-Management/Operational!*
    - Semperis-DSP-Notifications/Operational!*
    - Semperis-DSP-Reporting/Operational!*
    - Semperis-Operation-Log/Operational!*



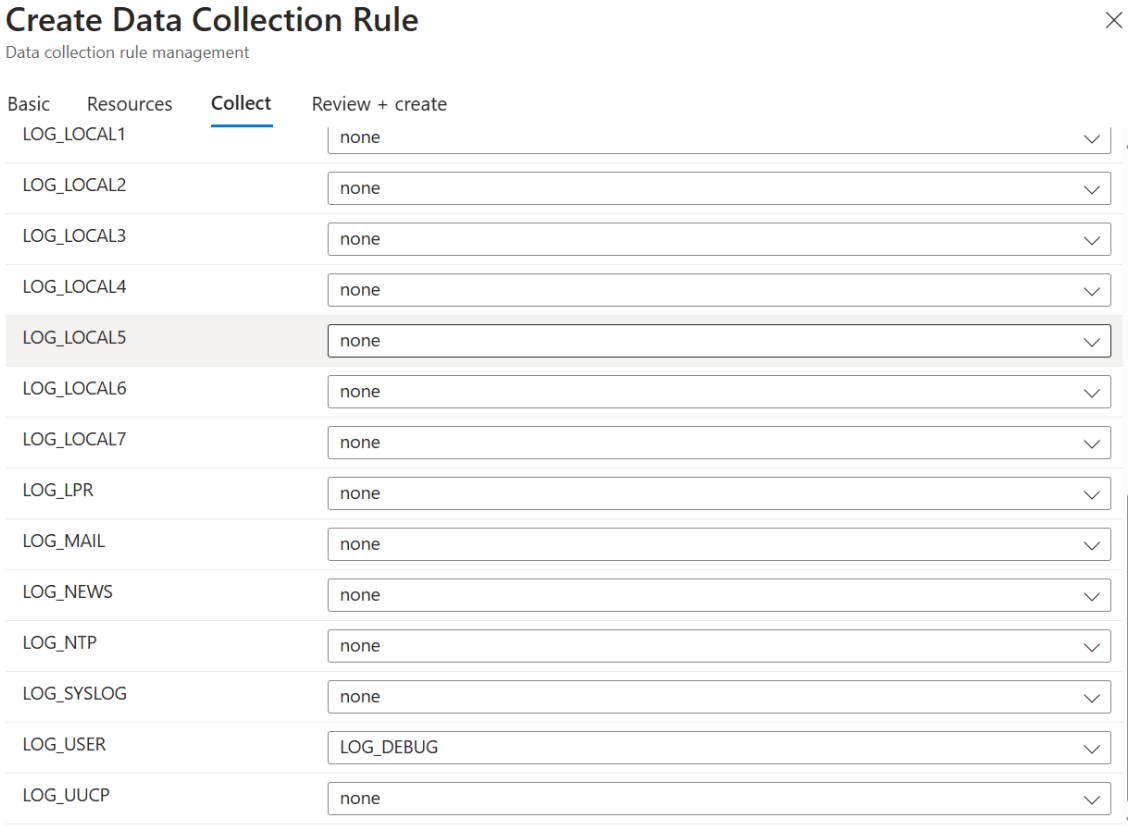
11. Click **Next: Review + Create** and review the information. Click **Create**.

Once the Azure Connected Machine agent is installed and configured to send the DSP Windows event logs, all ingested data will reside in the Security Event table in your Microsoft Sentinel / Log Analytics workspace. However, it may take up to 20 minutes before your logs start to appear in the Log Analytics workspace.

To configure DSP to forward AD change data to Microsoft Sentinel:

1. Open Microsoft Sentinel and select the workspace you defined for the DSP solution.
2. Click **Content hub** under the **Content management** menu in the navigation pane.
3. Search for and install **Common Event Format (CEF) via AMA**.
4. Select **Data connectors** under the **Configuration** menu in the navigation pane.
5. From the data connectors gallery, search for and select the **Common Event Format (CEF) via AMA** data connector.
6. At the bottom of the right pane, click the **Open connector page** button.
7. Run the command to install and apply the CEF collector on the syslog server in your environment.
8. Click **Create Data Collection Rule**.
9. Name the rule and enter the **Subscription** and **Resource group** in the text fields.

10. In the **Resources** tab, verify that the machine from which the data is to be collected from is listed.
11. In the **Collect** tab, select **LOG_USER** with the minimum log level of **LOG_DEBUG**.



12. Click **Next: Review + Create** and review the information. Click **Create**.

Once the Azure Connected Machine agent and the CEF agent are installed and configured to send the DSP AD change data, all ingested data will reside in the CommonSecurityLog table in your Log Analytics workspace / Microsoft Sentinel. However, it may take up to 20 minutes before your logs start to appear in the Azure Log Analytics workspace.

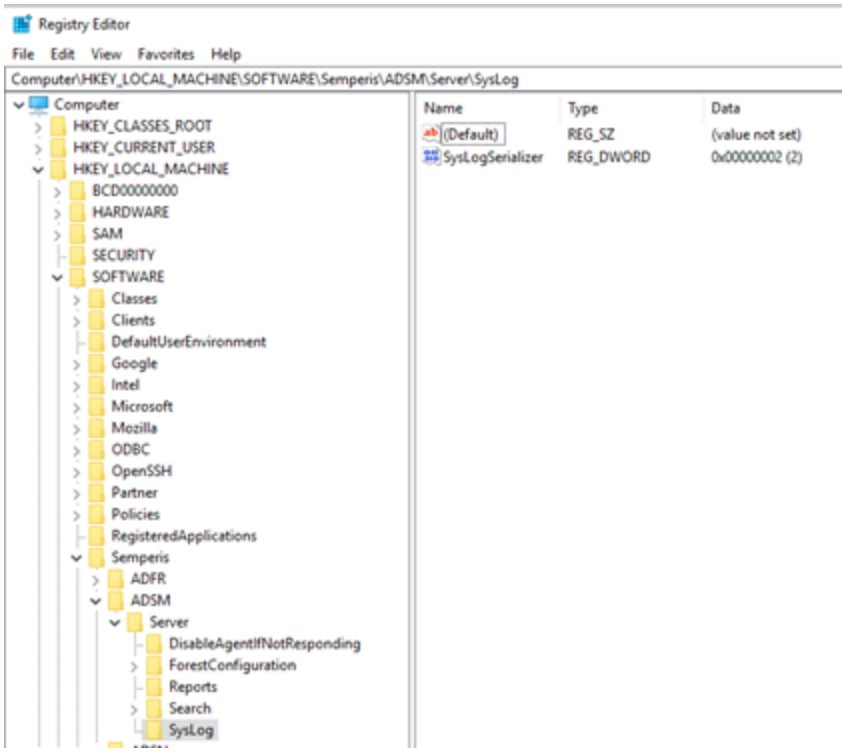
To configure DSP AD change data to send to Syslog (CEF):

1. On the DSP Management Server, open the registry editor.
2. Create or verify that the following registry key is present:

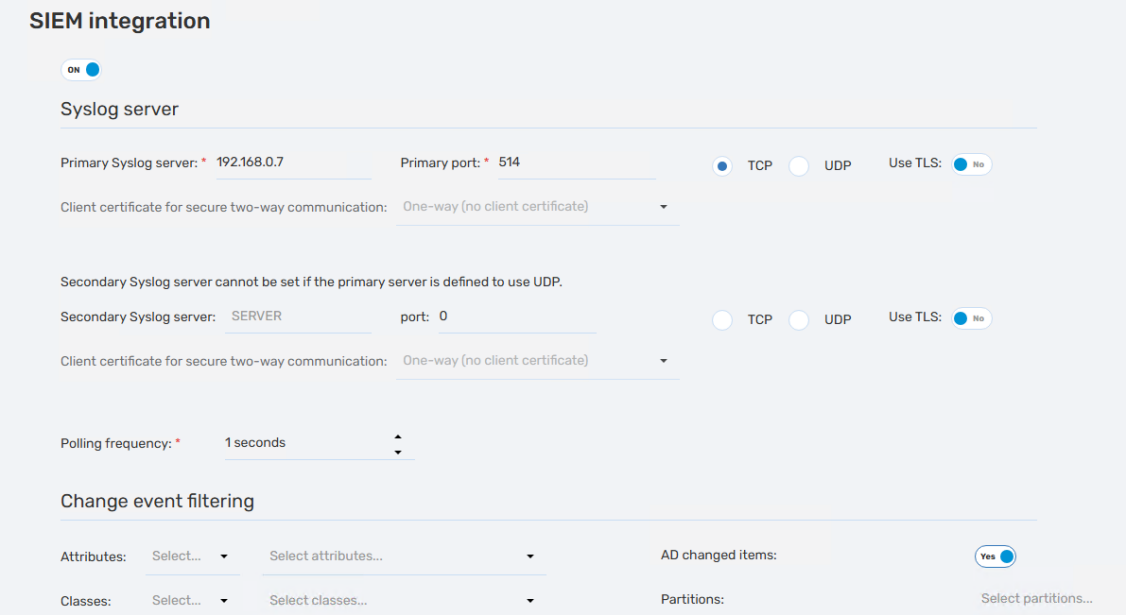
   HKLM_LOCAL_MACHINE\SOFTWARE\Semperis\ADSM\Server\SysLog has a DWORD SysLogSerializer with a value of 2.

> ***NOTE:***
>
> *The Syslog registry key is case sensitive and must use a capital "L".*

This will export Syslog data in Common Event Format (CEF).



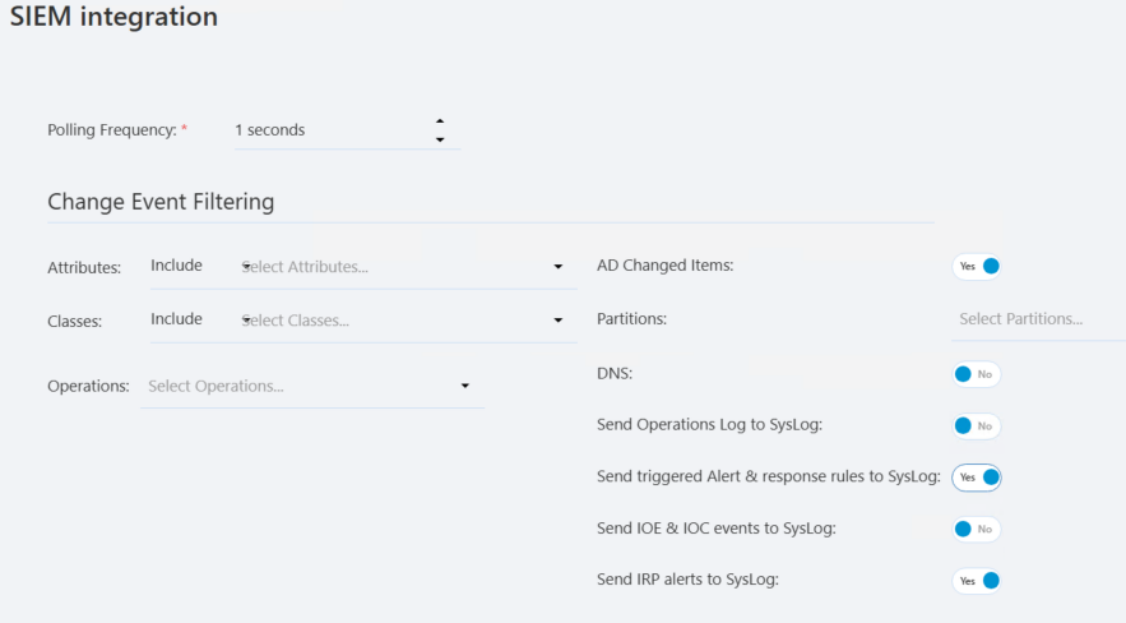
3. Open the DSP Administration portal and navigate to **Settings** > **Data Connections** > **SIEM Integration**.
4. In the **Syslog server** section, configure the Syslog server:
    - **Primary Syslog Server**: Enter the IP address of the Syslog server.
    - **Primary Port**: Enter "514" in the text field.
    - **Polling Frequency**: Specify how often (in minutes) the Syslog is to poll DSP for new events. The value must be between 1 (minute) and 10080 (1 week).



5. In the **Change Event Filtering** section, switch the **AD Changed Items** toggle to "Yes."

   If you have DSP v4.2 or later installed, also switch the following 2 toggles to "Yes":

   - **Send triggered Alert & response rules to Syslog**
   - **Send IRP alerts to Syslog**



6. Click **SAVE**.

CHAPTER 3

Semperis Directory Services Protector Solution Package

The Semperis Directory Services Protector Solution package consists of the following components, which are installed when you create the solution in Microsoft Sentinel:

- *DSP Data Connectors*
- *DSP Parser*
- *DSP Workbook*
- *Analytic Rules*

DSP Data Connectors

The DSP data connectors provide the means to ingest the Semperis Directory Services Protector Windows event logs and AD change data into Microsoft Sentinel. More specifically, the Semperis Directory Services Protector and Common Event Format (CEF) via AMA data connectors allow for the export of the logs from DSP to Microsoft Sentinel in real time.

To view information about the Semperis Directory Services Protector solution:

1. In Microsoft Sentinel, select **Data connectors** under the **Configuration** menu in the navigation pane.
2. In the data collector gallery, search for and select the **Semperis Directory Services Protector Solution**.
3. At the bottom of the right pane, click the **Open connector page** button.

   The left pane of the data collector page provides connection status, when data was last received, the data types being collected, etc.

> **NOTE:**
>
> *At first glance you will not see any activity in the left pane, you must first configure the data connectors (Semperis Directory Services Protector and Common Event Format (CEF) via AMA data collectors). The instructions for configuring the DSP data connectors are displayed in the right pane. For more information, see Configure DSP to Forward Events.*

4. Open the **Next steps** tab on the data connector page to view the sample queries that are available.

DSP Parser

A parser transforms the ingested data into Microsoft Sentinel normalized format. The dsp_ parser installed with the Directory Services Protector solution filters out the following security indicator events from the DSP Security Windows event logs (Semperis-DSP-Security/Operational):

- 9208: Security indicator failed to run
- 9211: Security indicator ran and passed (no IOE was found)
- 9212: Security indicator ran and failed (an IOE was found)

In addition, the filtering performed by the parser provides all relevant data (columns) about these security indicator events to Microsoft Sentinel with meaningful context that is easy to understand and highly actionable.

DSP Workbook

The Semperis Directory Services Protector solution installs one workbook, which can be accessed through the Microsoft Sentinel Workbooks tab once the solution is deployed. The Semperis Directory Services Protector workbook provides different ways to visual the data from the Security log, including:

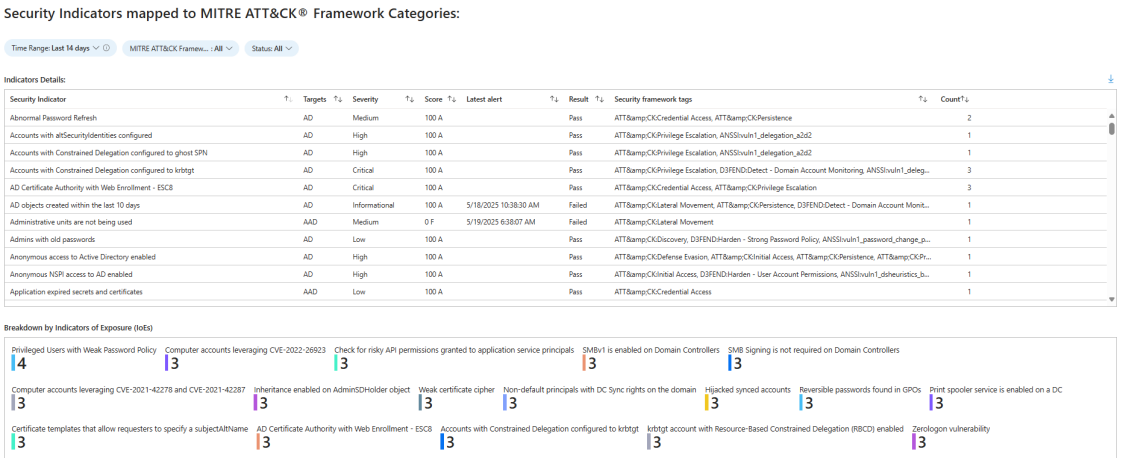
- **Semperis DSP Quickview Dashboard**: Contains general views of the DSP data forwarded from the DSP Event logs and Syslog.
- **Semperis DSP AD Changes**: Contains Active Directory change data from DSP Syslog output.
- **Semperis DSP Notifications**: Displays notification rule events forwarded from DSP event logs.
- **Semperis DSP Security Indicators**: Displays event data from the DSP event logs.

To display the DSP dashboard:

1. In Microsoft Sentinel, select **Workbooks** under the **Threat management** menu in the navigation pane.
2. Select **My workbooks**.
3. Select a DSP workbook, for example **Semperis DSP Security Indicators**, and click the **View saved workbook** button at the bottom of the right pane.

   The Semperis DSP Security Indicators page displays, which provides valuable insight into your Active Directory security posture.
4. Use one or more of the provided filers to further refine the details being displayed:
   - **Time Range**: By default, the results of the last 7 days is displayed. Use this control to filter the results based on a different time range.
   - **MITRE ATT&CK Framework**: By default, all categories are included. Use this control to filter the results based on a specific framework category or categories.
   - **Status**: By default, all statuses are included. Use this control to filter the results based on whether the security indicator failed to run, ran and passed (no IOE found), or ran and failed (IOE found).

   Selecting a different filter automatically adjusts the results displayed on the dashboard. Similar filters are available in the other workbooks as well.



5. Scroll down the dashboard to view additional details about the IOEs as well as top 10 IOE charts.

Analytic Rules

The sample analytic rules installed with the Semperis Directory Services Protector solution can be used to generate custom alerts in Microsoft Sentinel. These rules are deployed in disabled mode in the Analytic rules gallery of your Microsoft Sentinel workspace.

The following sample rules can be configured and enabled from the Analytic rules gallery after the solution is deployed:

- **Semperis DSP Mimikatz's DCShadow Alert**

  Mimikatz's DCShadow switch allows a user who has compromised an AD domain, to inject arbitrary changes into AD using a "fake" domain controller. These changes bypass the security event log and can't be spotted using normal AD tools. This rule looks for evidence that a machine has been used in this capacity.

- **Semperis DSP Kerberos krbtgt account with old password**

  The krbtgt user account is a special (disabled) user account in every Active Directory domain that has a special role in Kerberos function. If this account's password is compromised, Golden Ticket attacks can be performed to get access to any resource in the AD domain. This indicator looks for a krbtgt user account whose password hasn't been changed in the past 180 days. While Microsoft recommends changing the password every year, STIG recommends changing it every 180 days.

- **Semperis DSP Recent sIDHistory changes on AD objects**

  This indicator detects any recent changes to sIDHistory on AD objects, including changes to non-privileged accounts where privileged SIDs are added.

- **Semperis DSP well-known privileged SIDs in sIDHistory**

  This indicator looks for security principals that contain specific SIDs of accounts from built-in privileged groups within their sIDHistory attribute. This would allow those security principals to have the same privileges as those privileged accounts, but in a way that is not obvious to monitor (e.g. through group membership).

- **Semperis DSP Zerologon vulnerability**

  This indicator looks for security vulnerability to CVE-2020-1472, which was patched by Microsoft in August 2020. Without this patch, an unauthenticated attacker can exploit CVE-2020-1472 to elevate their privileges and get administrative access on the domain.

- **Semperis DSP Failed Logons**

  This rule looks for failed logon attempts into the DSP Administration portal.

- **Semperis DSP RBAC Changes**

  This rule looks for changes made to the DSP role-based access control (RBAC) model.

Enable a Sample Analytic Rule

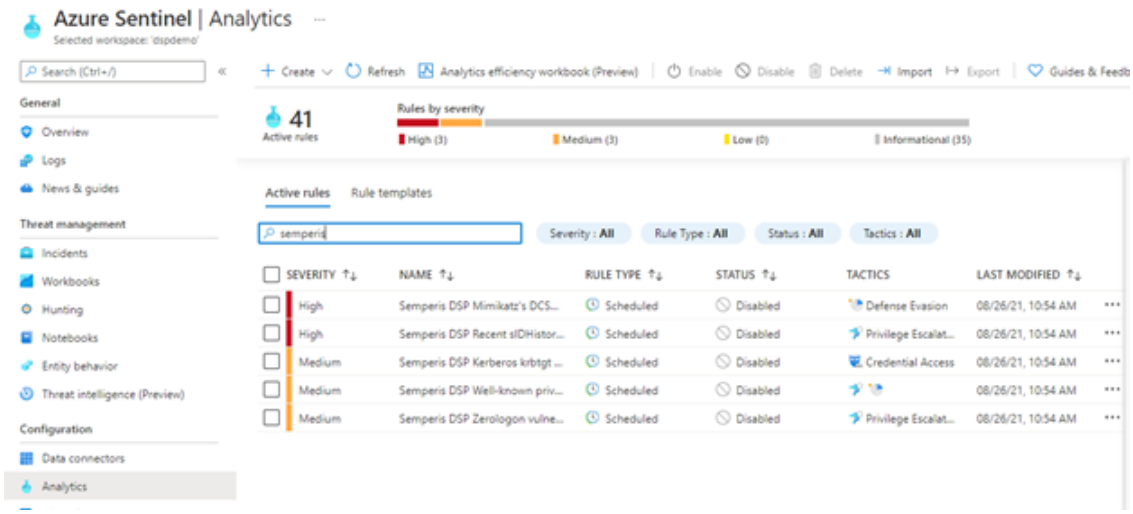
Simple analytic rules are provided by default with the Semperis Directory Services Protector solution, which when enabled can be used to generate a custom alert in Microsoft Sentinel.

NOTE:

Anyone familiar with the Kusto query language can create customized rules to capture additional or different events.

To enable an analytic rule:

1. In Microsoft Sentinel, select **Analytics** under the **Configuration** menu in the navigation pane.
2. Open the **Active rules** tab to view the Analytic rules gallery.
3. Search on **semperis** to list the sample rules included in the Directory Services Protector solution.



4. Select a rule to review the details about the rule, including the dsp_parser rule query associated with the rule. From this details pane (right pane), you can edit the specifics regarding the selected rule.
5. Select one or more rules from the list and click the **Enable** tool bar button at the top of the screen.