LOGPOINT

SaaS

SaaS

*V*1.0.0

CONTENTS

CHAPTER

ONE

LOGPOINT SAAS

1.1 What It Is

A future-forward SIEM + SOAR solution that provides threat detection, investigation, and response from the cloud. One or more on-premise appliances collect, normalize, and enrich your logs and then forward them to the cloud. You access your log data through a dedicated, secure URL connection. From there you can configure what you need to start monitoring and responding to what your log data tells you.

Full cloud-capabilities combined with a minimal on-premise infrastructure lets you focus on security intelligence rather than system monitoring and maintenance. We take care of mundane tasks so you can use your time on what's most important: ensuring the security of your IT infrastructure.

1.2 How It Works

Logpoint SaaS consists of two parts:

1. A cloud-based Threat Detection, Investigation, and Response service. You and your entire organization use a dedicated Logpoint URL to access the SaaS Web UI. Log in and configure your Alert Rules, Dashboards, Search Templates, Report Templates, Investigation and Response Playbooks in the same way as you would through a standard Logpoint SIEM + SOAR. After that you can perform threat detection, investigation and response with vendor and custom alert rules, dashboards, and playbooks. You can also generate compliance reports.
2. Sending Logs to Logpoint SaaS through one or more Cloud Connector appliances that manage local or cloud-based security event log collection, normalization, enrichment and forwarding to SaaS. Your appliances get log data either through listening to dedicated ports or fetching data from log sources. After that they normalize and enrich the data before forwarding it to the cloud.

To enable communication between your Cloud Connector appliances and the cloud service, the Logpoint Cloud Connector is installed on your on-premise appliance. It

forwards log data through a dedicated API Endpoint. Logpoint monitors your local device's critical parameters like CPU, RAM, disk space, connection health, storage resources, and consistent log generation. If any service disruption is detected, Logpoint will contact you.

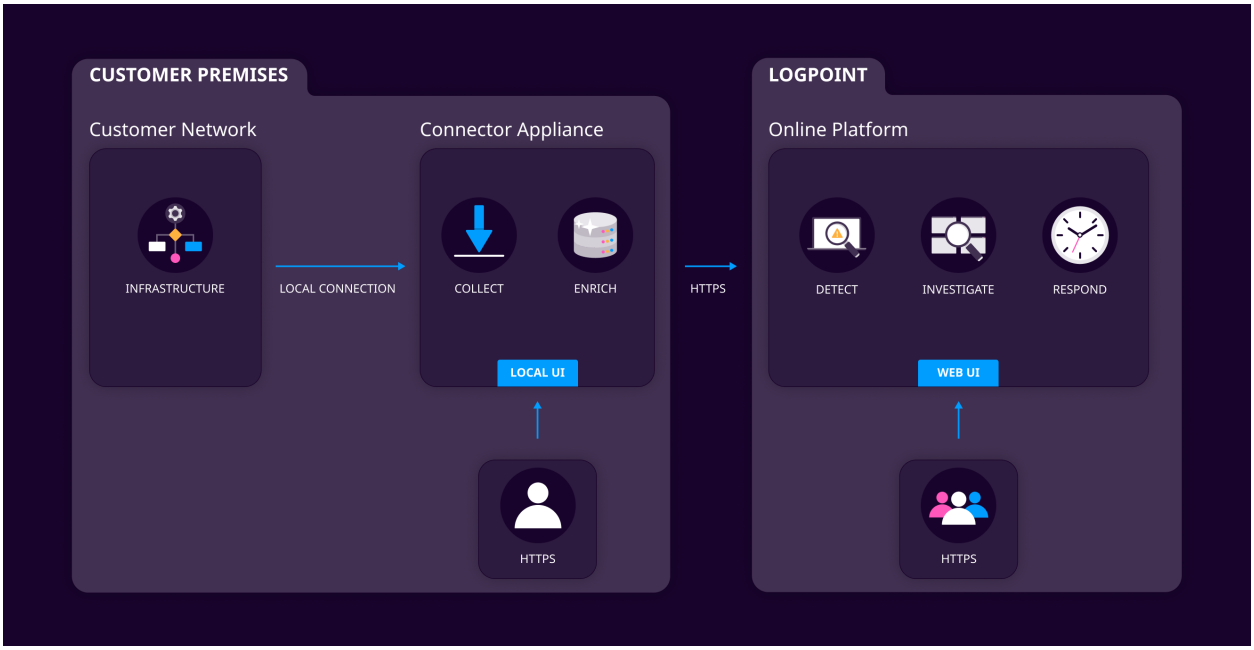


Fig. 1: SaaS

1.3 What It Contains

Logpoint SaaS is a subscription-based service. With your subscription, you receive:

- Dedicated endpoint and secure URL login to access the SaaS Web UI.
- SaaS license and Cloud Connector license for your Connector Appliances.
  - Cloud Connector license includes the necessary addresses and credentials for SaaS.

1.4 Differences between SaaS & Logpoint SIEM+SOAR

Logpoint SaaS functions very similarly to Logpoint SIEM+SOAR. However, some features in on-prem SIEM are not part of SaaS. In addition, there are a few noteworthy differences you should know.

- Enrichment sources need to be configured separately on the Connector Appliance and the SaaS Web UI. Configure ingest-time Enrichment sources on Connector Appliances and search-time enrichment on SaaS Web UI.
- SaaS Web UI can't access enrichment sources located on any of your private networks.
- Search-time DNS Process command only resolves publicly accessible DNS names and IP addresses.
- Logpoint SOAR integrations can only access cloud-based globally accessible services.
- SaaS Web UI can't access device registration entries in Cloud Connector Appliances so you can't restrict access to logs on a per-device basis. To apply per-device access restrictions, Logpoint recommends applying access restrictions on a per-repository basis and to use the User Group Universal Query to limit access to device logs.
- Logpoint Director is not yet supported via SaaS. If your solution includes Logpoint Director, it is still managed on-premises.

CHAPTER

TWO

SAAS PREREQUISITES

There are some important considerations that you - together with Logpoint - need to determine before you start.

2.1 Region

Where your Logpoint SaaS is hosted. Select one of the following supported geographical areas:

- Europe (Ireland)
- US EAST (N. Virginia)
- EU-west-2 (London)

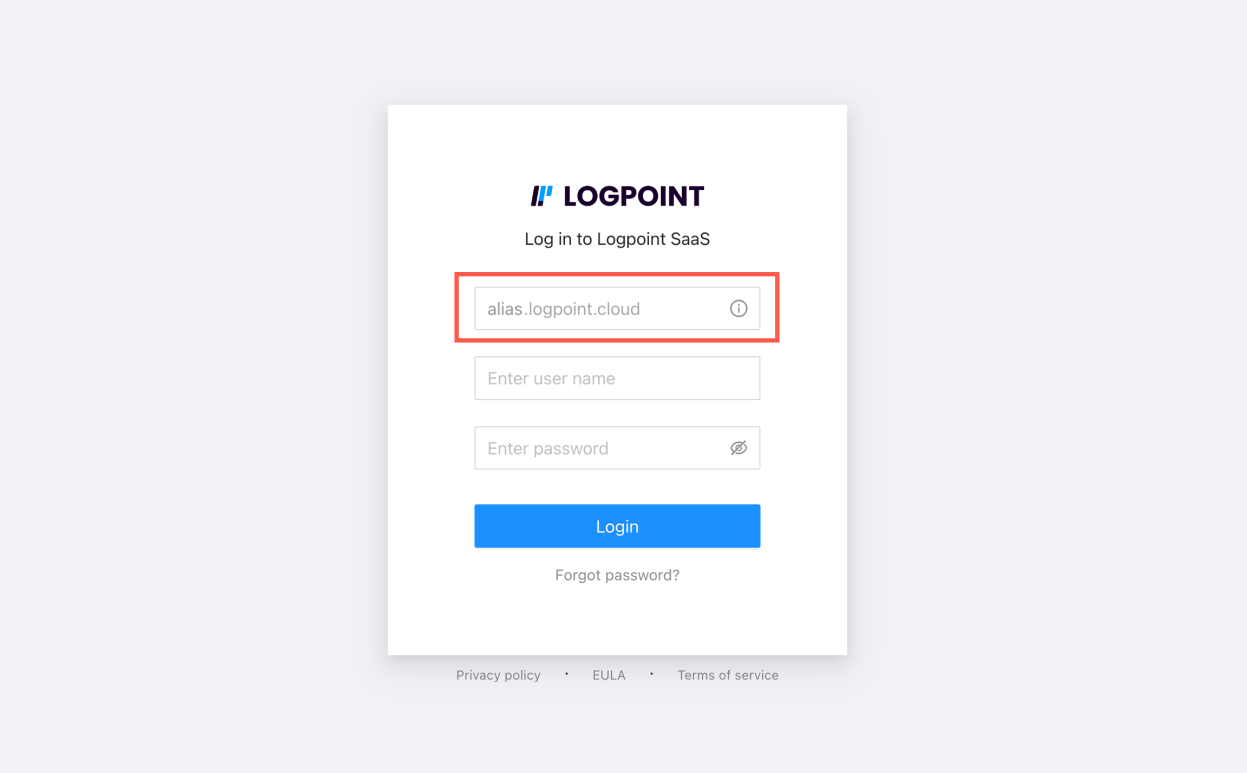
2.2 Target Version

Version number of Logpoint for your SaaS platform. Most will need the latest version of Logpoint, but there are certain scenarios when a different version is preferred. Specify the target version to deploy in SaaS in addition to the following information:

- New customers should provide the version number of their Cloud Connector.
- Current customers moving to SaaS from an on-premise platform should provide their on-prem version.

2.3 Domain Name

Tenant alias or domain name to use during log using the unified sign-in.



2.4 Alert & Email Recipients

To ensure delivery of Logpoint notifications including Alerts or Reports, you need to provide us:

- company-wide domains.
- email addresses of specific individuals whose addresses do not include company domains.

When you change or add domains, send that information to Logpoint Support so they are whitelisted. It's a good idea to remind any and all recipients to check their spam filters.

CHAPTER

THREE

LOGPOINT PORTAL

Logpoint Portal gives you access to Logpoint SaaS related resources including **Logpoint instances**, **Product Hub**, **Knowledge Center** and **Support** from a centralized location. You can also manage SaaS users from the portal. To learn more, go to *User Management from Logpoint Portal*.

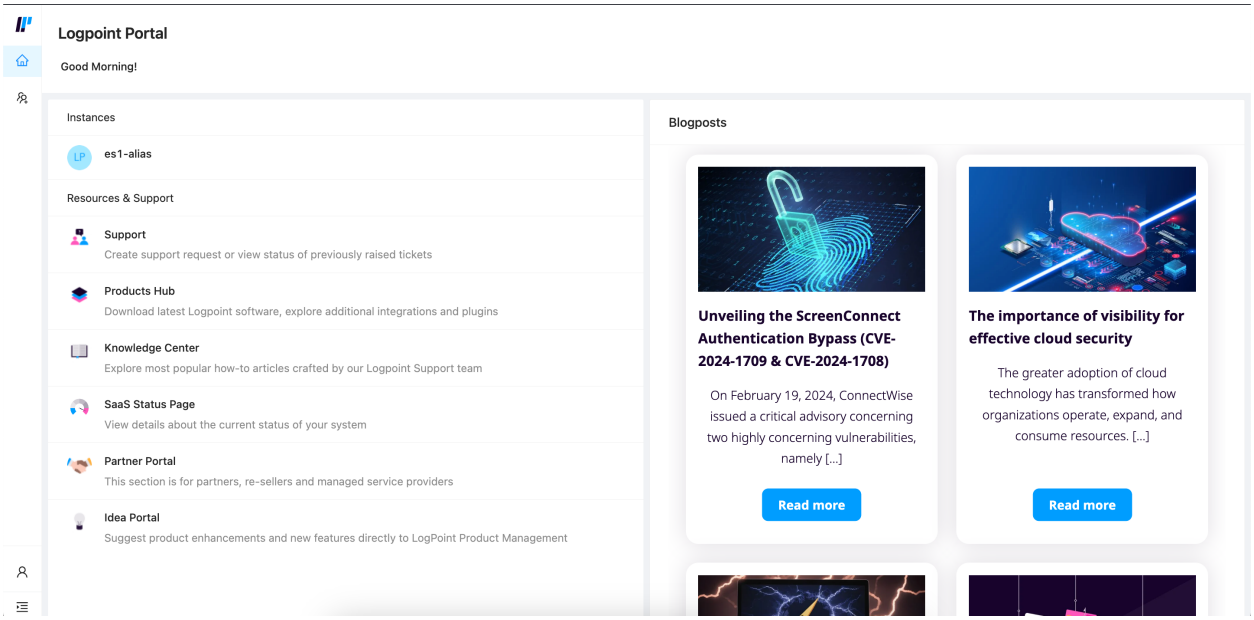


Fig. 1: Logpoint Portal

When you buy a SaaS subscription, Logpoint sends you an email with login details, including the Logpoint Portal URL, and initial access credentials. You are provided with a temporary password, which you need to change on the first login. After you change your password, login with your email and new password.

Note: If you don't see the email, check your spam filter.

After logging in with valid credentials, you access Logpoint. If you are an MSSP administrator you will also have access to all your Logpoint instances.

To login to Logpoint Portal:

1. Go to: https://portal.logpoint.cloud/

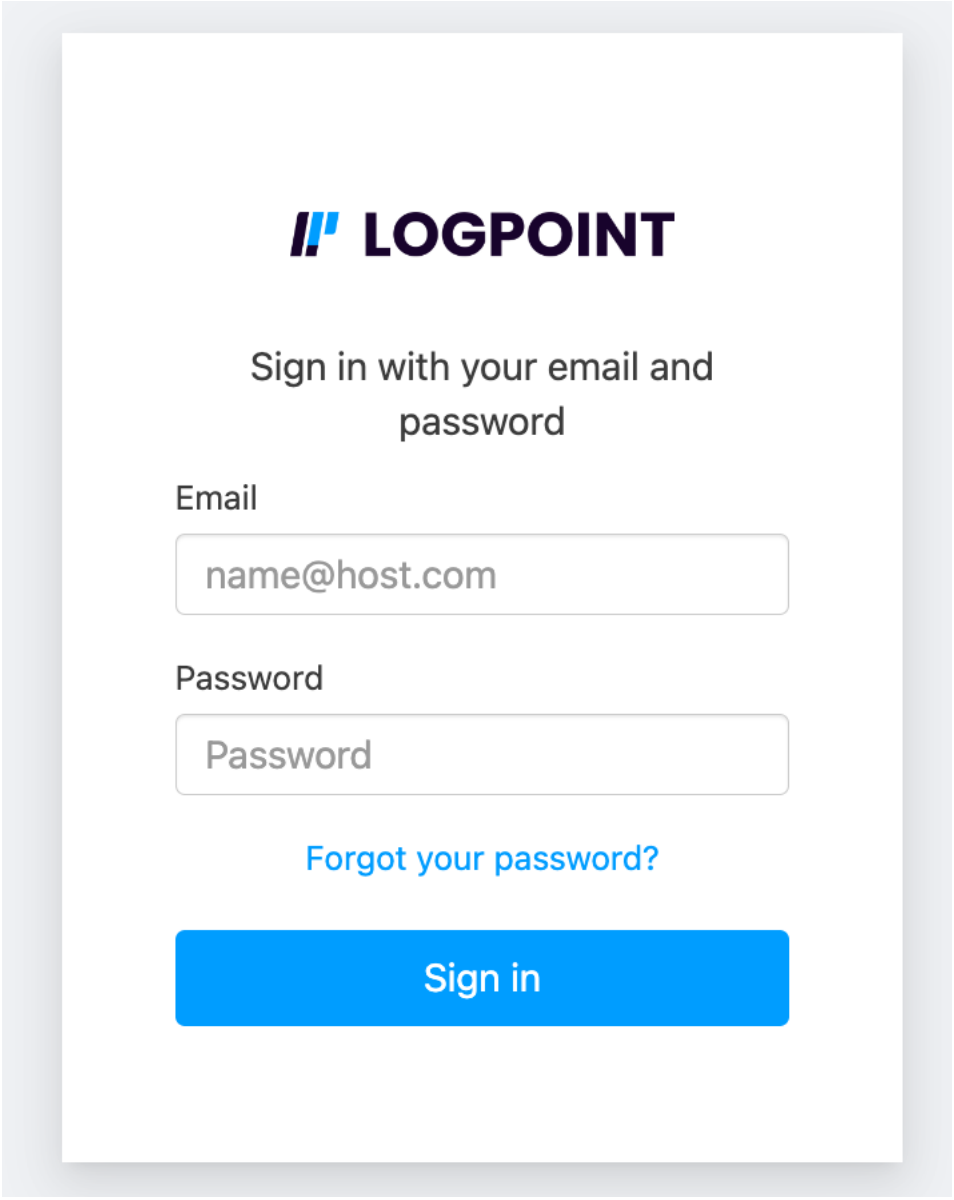


Fig. 2: SaaS Login

2. Enter your access credentials.
3. Access a Logpoint SaaS instance from **Instances**.

3.1. If you are a Logpoint user, click your SaaS instance name.

3.2. If you are an MSSP user, click the SaaS instance you want to access. Go to *Access Multiple SaaS Instances*.

After you access the Logpoint instance:

1. *Configure SaaS Instance*.
2. *Get Started Using SaaS Instance*.

3.1 Configure SaaS Instance

1. Configure the repositories in the cloud connector. The number of cloud-based SaaS repos and their names must match those configured on your on-premise Logpoint's cloud connector.

Warning: If the repositories are not configured this way, logs are discarded and data is lost.

The retention time for the repo in searchable storage is set as per your retention policy in your contract agreement.

2. Configure alert rules, dashboards, search templates, report templates, and playbooks.

3.2 Get Started Using SaaS Instance

All system settings, SMTP, NTP, SNMP, Syslog, Support Connection, Mode of Operation, SSH Key Pair for li-admin, and Lockout Policy, are pre-configured on the SaaS Instances.

After configuration, you can start:

1. Responding to Incidents.
2. Searching and analyzing security events.
3. Perform investigations and threat hunting with Search Templates and Search Packages.
4. Schedule, generate and review generated reports.

3.3 User Management from Logpoint Portal

Logpoint Portal lets you administer **User Management**. **User Management** allows you to add a new user, assign them to a user group, update an existing user and delete a user. Only users who are part of the Logpoint Administrator and User Account Administrator user groups are allowed to add, update and delete the users.

Important: *Permission Groups* and *User Groups* Management:

- You can perform only *User Management* from **Logpoint Portal**. You must manage Permission Groups and User Groups inside the SaaS instances.
- If you are an MSSP user, you must create the *Permission Groups* and *User Groups* within the SaaS instance on which you want to create the new user.

To add a new user:

1. Click ( ) icon on the navbar.
2. Click **Add User** on the top right.
3. Enter **E-mail address**.
4. Enter **First Name**.
5. Enter **Last Name**.
6. Select an instance from the **Instances**.
7. Select user group(s) from the **User Groups**.
8. Click **Save**.

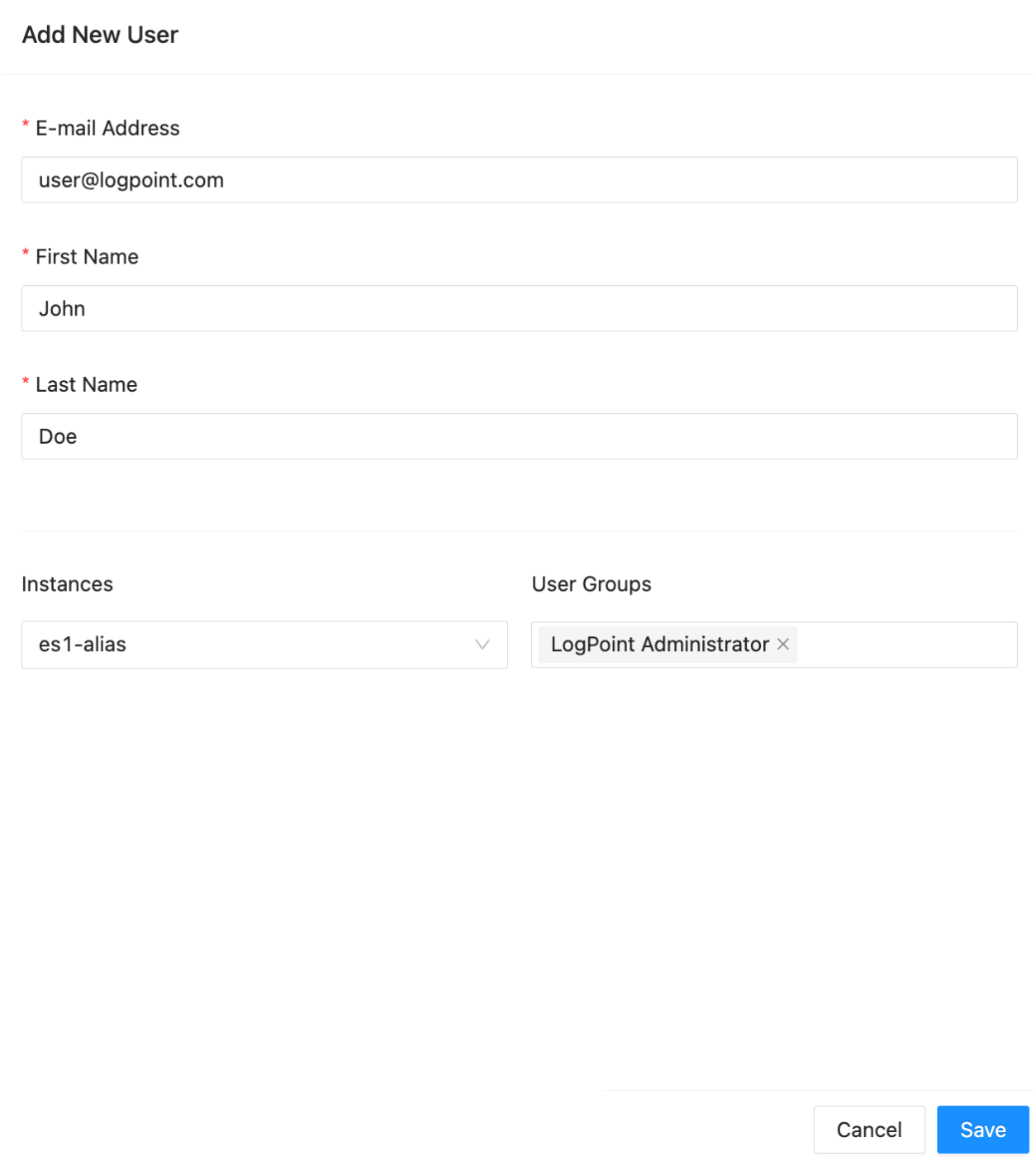


Fig. 3: Adding User

To update a user:

1. Click ( ) icon on the navbar.
2. Click the user you want to edit.

3. Make the changes.
4. Click **Save**.

To delete a user:

1. Click ( ) icon on the navbar.
2. Click the user you want to delete.
3. Click **Delete**.

3.4 Access Multiple SaaS Instances

MSSP users can access multiple Logpoint SaaS instances using a single set of credentials from Logpoint Portal. A list of instances appears under **Instances** for MSSP users.

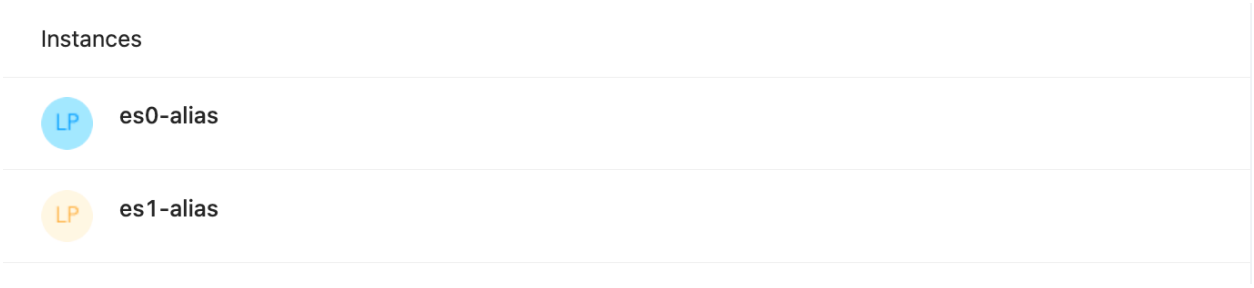


Fig. 4: SaaS Instances

3.5 Supported Browsers

- Safari
- Google Chrome
- Firefox
- Microsoft Edge

CHAPTER

FOUR

SENDING LOGS TO LOGPOINT SAAS

You need to deploy Logpoint Cloud Connector Appliance in your network to send log information to Logpoint SaaS. Logpoint Cloud Connector Appliance allows collection of logs from a large variety of on-premise and cloud-based data sources.

To deploy and configure log collection with Logpoint Cloud Connector Appliances:

1. Provision a virtual machine or device that meets hardware requirements. Use the Cloud Connector Appliance Sizing Helper to estimate your hardware requirements.
2. Install Logpoint SIEM+SOAR from an ISO, VHD, or AMI depending on your infrastructure.
3. Upload your Logpoint license.
4. Install Logpoint Cloud Connector Plugin.
5. Upload the Cloud Connector license.
6. Disable Local Log Storage in the Cloud Connector Plugin.
7. *Configure Repositories*.
8. Configure devices, normalization, and enrichment policies.
9. Configure enrichment subscriber.

4.1 Configure Repositories

You will need to configure repositories with the same names in both Cloud Connector Appliance and SaaS Web UI to successfully send the log information to SaaS service.

Repositories in the Cloud Connector Appliance may use the default storage path, and the Local Log Storage in Cloud Connector Plugin must be disabled. The repository names will be used in the routing policy configurations to route the log data to correct repositories in SaaS Web UI. For more details, go to the Repos section in the Data Integration guide.

Refer to *Configure SaaS Instance* section on how to configure repositories in SaaS Web UI.

CHAPTER

FIVE

ENRICHMENT SUBSCRIBER

Enrichment Subscriber enables your Logpoint SaaS to access your on-premise Logpoint's Enrichment Sources. Currently, CSV, LDAP, and ODBC enrichment source types are supported.

5.1 Forwarding Enrichment Sources to Logpoint SaaS

1. Go to *Settings >> Configuration* from the navigation bar and click **Enrichment Subscriber**.

On the page, you will see the list of all the available enrichment sources. You can use Cloud Connector to forward the enrichment sources to Logpoint SaaS.

2. Click the **Subscribe** ( ) icon under **Actions** of the enrichment source.

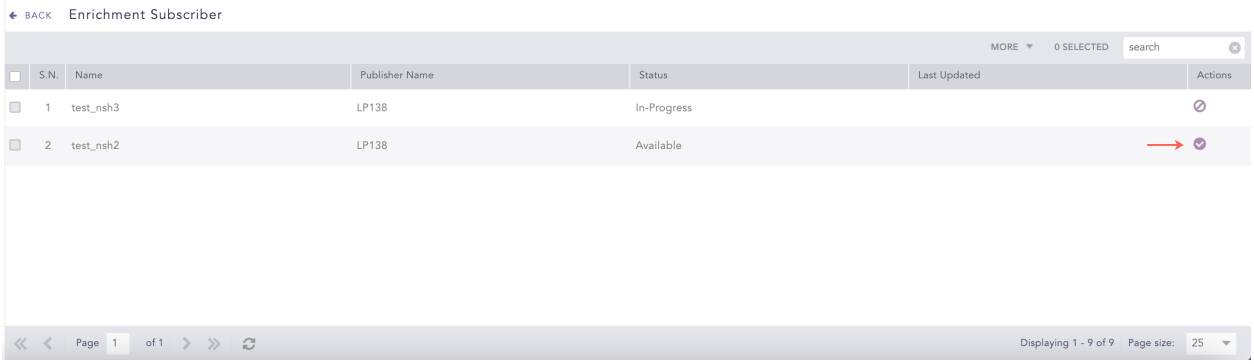


Fig. 1: Subscribe Enrichment Sources

The enrichment source is now forwarded to Logpoint SaaS. You can select and forward all of them at once by clicking the **More** dropdown and selecting **Subscribe All**. To forward only the selected enrichment sources, click the **More** dropdown and select **Subscribe Selected**.

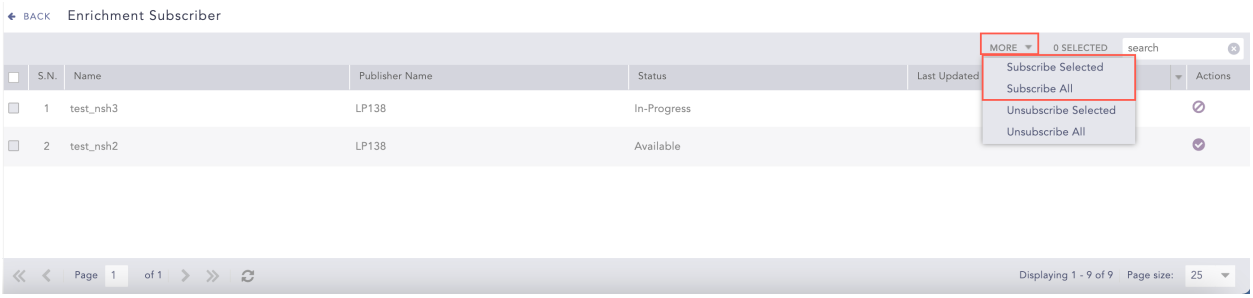


Fig. 2: More Dropdown

You can see the state of the enrichment source from **Status**.

- Available: The enrichment source is ready to be forwarded to Logpoint SaaS.
- In-Progress: Enrichment Subscriber is working on your request to forward or remove the enrichment source.
- Subscribed: The enrichment source is forwarded to Logpoint SaaS.
- Duplicate: The enrichment source with the same name is already forwarded to Logpoint SaaS.
- Failed: The enrichment source forwarding has failed.
- Deleted: The enrichment source is subscribed but not available on the Logpoint SaaS.

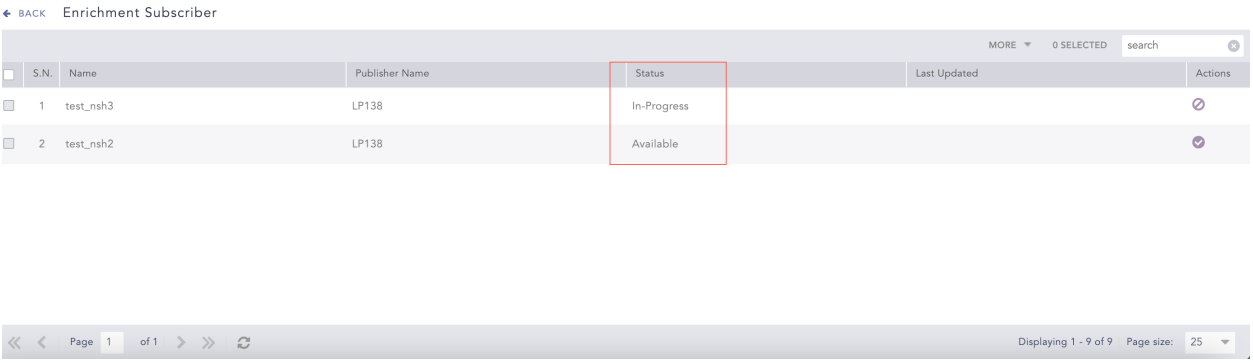


Fig. 3: Status

5.2 Removing Enrichment Sources from Logpoint SaaS

1. Go to *Settings >> Configuration* from the navigation bar and click **Enrichment Subscriber**.

2. Click the **Unsubscribe** (⊘) icon under **Actions** of the enrichment source.

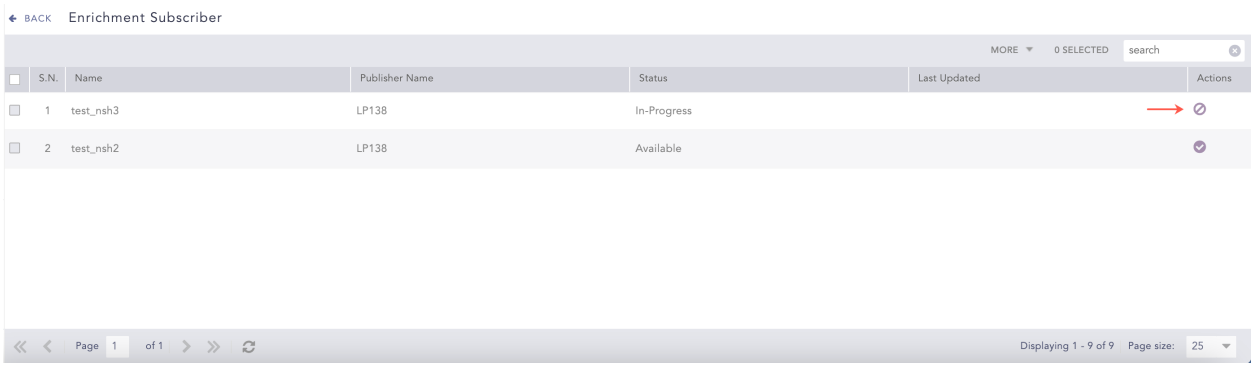


Fig. 4: Subscribe Enrichment Sources

The enrichment source is now removed from Logpoint SaaS. You can also select all the enrichment sources and remove them at once by clicking the **More** dropdown and selecting **Unsubscribe All**. To remove only the selected enrichment sources, click the **More** dropdown and select **Unsubscribe Selected**.

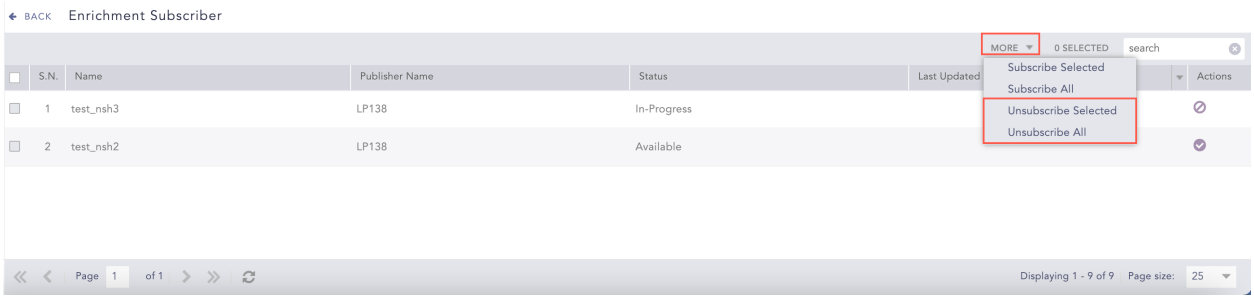


Fig. 5: More Dropdown