Getting Started with Skylar AI

Version 1.1.0

Table of Contents

Chapter 1

Introduction to Skylar AI

Overview

Skylar AI is a software services suite powered by artificial intelligence (AI) that is designed to automatically manage and anticipate IT incidents. Skylar AI reasons over telemetry and the stored knowledge of an organization to deliver accurate insights, recommendations, and predictions.

This chapter provides an overview of Skylar AI and the various components that use Skylar AI.

This chapter covers the following topics:

What is Skylar AI?

Autonomic IT leverages artificial intelligence (AI), automation, and data to intelligently self-manage an entire IT stack. Autonomic IT drives autonomous businesses with rapid decision-making, cost-optimized scalability, and innovative experiences that empower organizations to focus on core innovation. The Skylar AI platform, which includes Skylar Analytics and Skylar Advisor (coming soon), helps customers with their journey towards Autonomic IT.

Skylar AI is a software services suite powered by artificial intelligence (AI) that is designed to automatically manage and anticipate IT incidents. Skylar AI reasons over telemetry and the stored knowledge of an organization to deliver accurate insights, recommendations, and predictions.

SL1 collects data and leverages Skylar AI to learn the patterns for a particular device metric over a period of time. Skylar uses the resulting data to build a device metric-specific model that is used to define a scope of expected behavior as well as anomalous data points.

Features of Skylar AI

Skylar AI is the engine that powers several different software components. The components in the Skylar family of services share the following characteristics:

- **Reactive**. When something fails, Skylar AI tells you in plain language what happened and how to fix it with relevant context.
- **Predictive**. Skylar AI alerts you in advance to an expected out-of-capacity condition.
- **Proactive**. Skylar AI accurately answers any question asked of it with context drawn from company knowledge sources, such as bugs, support tickets, Knowledge Base articles, and Product Documentation, and recommends next steps.

Skylar AI integrates seamlessly with the SL1 platform and other IT management tools. You can interact with Skylar AI through these familiar environments, where it enhances existing workflows with AI-driven insights and automation capabilities. Skylar AI can send you alerts and notifications, which can be customized to suit individual preferences or organizational needs. These alerts help you stay informed about potential issues, ongoing incidents, or opportunities for optimization.

Components of Skylar AI

The Skylar AI family of services includes the following components:

- ***Skylar Analytics***, an advanced reporting and custom analytics service that combines AI-powered analytics with deep data exploration and visualization.
- ***Skylar Advisor***, a proactive IT problem-solving advisory service powered by human-centered AI.

NOTE: This manual covers Skylar AI. At the Product Documentation site, you can find documentation for *Skylar Analytics*.

Data Analyzed by Skylar AI

The following image shows the flow of data into and out of SL1 and the Skylar AI Engine:

The following list contains some of the types of data that SL1 can send to the Skylar AI engine, where the data is analyzed and used by Skylar Analytics and Skylar Advisor:

- Alert and event logs
- Availability data collected by SL1
- Business Service health, availability, and risk metrics from SL1
- Class-Based Quality-of-Service (CBQoS) metadata and CBQoS time series data
- DCM(+R) relationships
- Dynamic Application mapping and performance data
- Metadata for web content, SOAP/XML transaction, and domain name monitors
- Process and service data
- SL1 Agent data, including Gen 1 (SL1 Distributed Environment) and Gen 3 (SL1 Extended Architecture) agents
- Topology data for L2, L3, CDP, LLDP, and ad-hoc relationships between devices

Configuring Skylar AI

NOTE: These instructions are only for on-premises configurations of Skylar AI. The ScienceLogic SRE team performs these steps for SaaS configurations of Skylar AI.

Before you can start using Skylar AI components, you will need to perform the following configurations in SL1 to enable the export of data from SL1 to Skylar:

- *Create a Service Connection*
- *Enable Skylar Analytics for one or more organizations*

After you perform these configurations, you can access Skylar Analytics, Skylar Advisor, and other key Skylar AI components from the **Skylar AI** page ( ) in SL1.

For information about setting up users, user groups, and user roles, see *Configuring Access Control in Skylar AI*.

IMPORTANT: ScienceLogic strongly recommends that you always use the most recent SL1 and AP2 releases in conjunction with the most recent Skylar AI release. Using the most recent releases will ensure that your Skylar AI system has access to the latest datasets and features. For more information, see the *SL1 Platform and AP2 Release Notes*.

Creating a Service Connection

If you are using AP2 Mochi or later with your SL1 system, you can create a service connection for the Skylar AI engine on the **Service Connections** page (Manage > Service Connections) in SL1. ScienceLogic strongly recommends that you upgrade to Mochi or later. For more information, see the *AP2 Mochi release notes*.

The service connection enables communication between your SL1 system and Skylar AI. This process replaces the *Running the Skylar SL1 Management Tool* process in previous releases of Skylar Analytics and SL1.

To create a Skylar AI Engine service connection:

1. In SL1, go to the **Service Connections** page (Manage > Service Connections).
2. Click **Add Service Connection** and select *Skylar AI Engine*. The **Create Skylar AI Engine Credential** window appears.
3. Complete the following fields:
   - ***Name***. Type a name for the new service connection.
   - ***API Key***. Add the access token for Skylar AI, which you can generate on the **Access Tokens** page in Skylar Settings (Instances > Access Tokens). For more information, see *Creating Access Tokens for Users*.
   - ***Skylar AI Engine URL***. Add the URL for your Skylar AI system.
4. Click **[Save]**. The service connection is added to the **Service Connections** page, and a modal displays a link to the **Organizations** page, where you can enable Skylar Analytics for one or more organizations. See the following procedure for more information.

5. Refresh or reload the browser to add all updates to SL1.

> **NOTE:** Newer releases of SL1 include a **Status** and **Status Updated** column, along with a **Service Check** column that displays a **[Run Test]** button for "Skylar AI Engine" service connection types. Click **[Run Test]** to run a script to check the status of the Skylar AI connection and display the results in a modal.

Enabling Skylar AI for One or More Organizations

You will need to select one or more organizations in SL1 that will share data with Skylar AI. This data will come from all of the devices in a selected organization. By default, the Skylar AI features are disabled.

You can see which organizations are currently sending data to Skylar AI by going to the **Organizations** page (Registry > Accounts > Organizations) and looking at the ***Skylar AI Status*** column for the organizations.

To enable Skylar AI with SL1 organizations:

1. In SL1, go to the **Organizations** page (Registry > Accounts > Organizations) and click the check box for one or more organizations.
2. In the ***Select Action*** drop-down, select *Send Data from Selected Orgs to Skylar AI* and click **[Go]** to start sending data about the selected organizations to Skylar AI. The ***Skylar AI Status*** column for the selected organizations changes to *Enabled*.

For Older Versions: Running the Skylar SL1 Management Tool

If you are using a version of AP2 before Mochi, you will need to set up Skylar AI with the steps below for the Skylar SL1 Management Tool instead of the **Service Connections** page in SL1. ScienceLogic strongly recommends that you upgrade to Mochi. For more information, see the *AP2 Mochi release notes*.

The Skylar SL1 Management Tool configures SL1 data and SL1 processes, and it starts monitoring the Skylar connection and configuration. The script is named `sl-otelcol-mgmt.py`, and it is included in the `sl-otelcol` RPM package.

To run the Skylar SL1 Management Tool:

6. Use the following command to run the Management script on the Database Server (an SL1 Central Database or an SL1 Data Engine):

```
sudo sl-otelcol-mgmt.py -vv skylar --skylar-all --skylar-endpoint "<URL_for_skylar_system>" --skylar-api-key "<skylar-access-token>" --ap2-feature-flags
```

where:

- *<URL_for_skylar_system>* is the URL for your Skylar AI system
- *<skylar-access-token>* is the access token for Skylar AI, which you can generate on the **[Access Tokens]** tab of the **Skylar Settings** page. For more information, see *Creating Access Tokens for Users*.

You can also use the following configuration options if needed:

- `--verify-cert false`. Allows users in on-premises environments to connect to Skylar AI using self-signed certificates.
- `--ca-bundle /<path>/bundle.pem`. Allows users to specify a path to a **.pem** file and assign it to the `REQUESTS_CA_BUNDLE` environment variable.
- `--skylar-disable`. Stops all Skylar AI exports and services. This flag performs the same operations as the pause command (see step 3, below) and also removes any Skylar AI pages from the SL1 user interface.

NOTE: If you have already run setup before and are not changing the connection details, you do not need to include `--skylar-endpoint "<URL_for_skylar_system>" --skylar-api-key "<skylar-access-token>"`.

In addition, `--ap2-feature-flags` is only needed the first time you install Skylar AI.

This command configures the OpenTelemetry Collector, restarts services that export data, and checks that connectivity to the supplied endpoints is healthy.

After successfully running the script, on the **System Logs** page (System > Monitor > System Logs), you will see "Info" messages for each configuration change (filter on `sl-otelcol-mgmt`). You will also see "Major" system log messages whenever connectivity fails for the Skylar endpoint or the OpenTelemetry Collector.

After data streams into the Data Visualization dashboards, and other Skylar AI components, they will populate with data. Please note that this process might take several minutes.

7. If you have run the setup script before, run the following command to enable Skylar AI and make sure that everything is working as expected:

```
sudo sl-otelcol-mgmt.py -vv skylar --skylar-all
```

> **TIP:** To check to make sure you have connected Skylar AI to SL1, go to SL1 and look for the **Skylar AI** page ( ). If the page loads, then the connection was successful. You can also go to the **Service Connections** page (Manage > Service Connections) and look for a service connection with a **Type** of "Skylar AI Engine" to verify that the connection was successful. After a few minutes, the Data Visualization charts will populate with data if the connection was successful.

8. If you need to pause Skylar AI, run the following command:

```
sudo sl-otelcol-mgmt.py -vv skylar
```

Pausing sets all Skylar AI toggle fields to disabled; restarts the event engine and data pull services to reflect the changed configuration; stops SL1 managed services such as the Metadata Exporter, Alerts Poller, and sl-otel-mgmt.timer; and stops and disables the sl-otelcol systemd service.

9. To check the status of the installation, run the following command:

```
sudo sl-otelcol-mgmt.py -vv status
```

You should look for the following messages in the output:

```
---------- checking feature toggles

SL_EXPORT_EVENTS = False

SL_EXPORT_METRICS = True

SL_EXPORT_CONFIG = True

---------- checking services

sl-otelcol is enabled and running

---------- checking connectivity

checking: Skylar endpoint is healthy

checking: local OTELCOL endpoint is healthy
```

> **NOTE:** If you need to turn off the Skylar AI connection, run the following command:
>
> `sudo sl-otelcol-mgmt.py -vv skylar --skip-status-service`

10. Continue to the next procedure to specify the organizations you want to use for exporting data to Skylar.

Enabling Skylar AI Event Policies

In addition, the Predictive Alerting and Anomaly Detection components of Skylar Analytics require the "Skylar Analytics Event Policies" PowerPack. This PowerPack collects the SL1 event policies from the "Skylar - Predictive events" and "SL1: Skylar Anomaly Score Event Monitoring" PowerPacks.

Older versions of this PowerPack were named "Skylar Predictive Analysis".

To install the "Skylar Analytics Event Policies" PowerPack:

1. Download the PowerPack from the ScienceLogic Support Site, or use the link provided by ScienceLogic.
2. In SL1, go to the **PowerPacks** page (System > Manage > PowerPacks), click **[Actions]**, and then click **[Import PowerPack]**.
3. Browse and select the downloaded PowerPack and click **[Import]**.
4. On the next screen, click **[Install]** and, when prompted for confirmation, click **[OK]**.

5. To confirm that the PowerPack was installed properly by go to the **Event Policies** page (Events > Event Policies) and type the word "predictive" into the ***Name*** search field. You should see a number of "Predictive Alerting" event policies.

For information about how to use these components, see the following chapters:

- *Skylar Analytics: Anomaly Detection*
- *Skylar Analytics: Predictive Alerting*

Logging In to the Skylar AI User Interface

You can access Skylar AI components from a link in SL1, or if you know the URL of your Skylar AI system, you can go directly to that location instead of using SL1.

1. From SL1, go to the **Skylar AI** page ( ) and click the **[Visit]** button for the Skylar AI component you want to use, such as Skylar Analytics or Skylar Advisor. If you are not currently logged in to Skylar AI, the Skylar AI sign-in page appears.

> **NOTE:** Clicking the **[Visit]** button for Skylar Predictive Alerting and Skylar Anomaly Detection opens new pages for those components in SL1.

2. If you need to log in to Skylar AI, type your email address and password and click **[Continue]**. The Skylar AI landing page appears.
3. Click the name of the Skylar AI component you want to use, such as ***Analytics*** or ***Skylar Settings*** .

> **TIP:** For more information about the **Skylar Settings** page, see *Configuring Skylar AI System Settings*.

Chapter 2

Configuring Skylar AI System Settings

Overview

This chapter covers how to configure the various settings for Skylar AI products by using the **Skylar Settings** page. On this page, you can set up authentication for the Skylar AI site, edit your user preferences, create and edit users and user groups, and configure additional administrative options.

This chapter covers the following topics:

Navigating the Skylar Settings User Interface

Use the following buttons and icons to help you navigate the Skylar Settings user interface:

- To switch between Skylar AI applications, click the menu icon () at top left.
- To return to the Skylar AI login page, click the "Skylar AI" icon at top left.
- To view the email address and role for the current user in the Skylar AI user interface, click the user icon () at top right. On this drop-down menu, you can click the **[Sign Out]** button to sign out of this session.
- To view version numbers for the Skylar Settings user interface, click the **Versions** link in the footer of any page. From the footer, you can also click links to view the Terms of Service and information about licenses and open-source packages.

Overview of Authentication in Skylar AI

Authentication for Skylar AI has the following features:

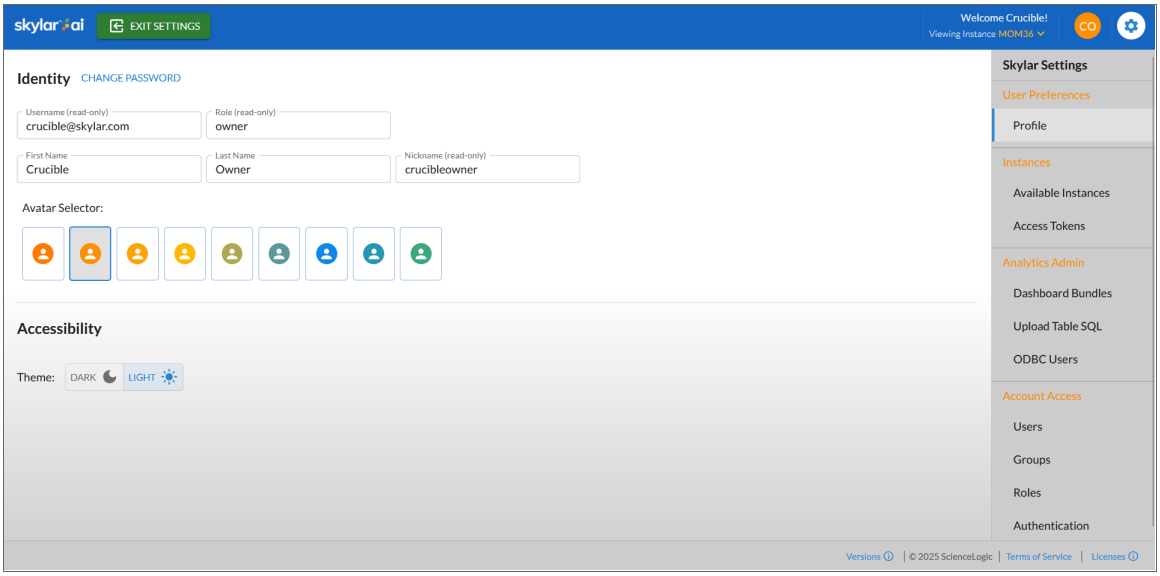
- Multi-tenant support, including a super-user login for host management .
- Multiple instances that represent separate domains of data access within an account (tenant).
- Predefined roles for access control.
- Email and password (local accounts) authorization by default, and Security Assertion Markup Language (SAML) single sign-on (SSO) authorization configured as needed.
- Access tokens for integration with external tools.

When a user is logged in to a Skylar AI component, that session uses the following rules:

- Email domains and SAML are configured per account (tenant).
- The first login for any new user starts with a prompt to create a new password.
- Logging into a user session requires either an email and password combination or a successful SAML2 redirect workflow.
- User passwords must be at least 15 characters long.
- New user passwords must be different from the last five passwords for this user.
- Users will be prompted to reset their passwords every 60 days.
- User sessions that have been idle for 15 minutes are automatically terminated. Administrator user sessions that have been idle for ten minutes are automatically terminated. An Admin user can adjust the timeout value on the **Authentication** page in Skylar Settings (Account Access > Authentication).
- If a user has three failed login attempts within a 15-minute interval, the user's account is locked for 15 minutes. An administrator user can unlock that user account from the **Edit User** dialog on the **Users** page in Skylar Settings (Account Access > Users).
- User accounts that have not been active for 35 days are automatically locked.

Role-Based Access Control in Skylar AI

To access the role-based access control settings, log into the Skylar AI user interface and click **Skylar Settings**. The following image displays a **Profile** page in the **User Preferences** section for a user with the "Owner" role:



Using the different pages available on the right side of the **Skylar Settings** page, you can edit your user profile, add users and groups to your account, assign roles to groups, and create access tokens. Depending on your user role, you can also update dashboards and set up additional forms of authentication.

Elements of Role-based User Accounts in Skylar AI

An ***account*** in a Skylar AI system represents a complete Skylar AI configuration for a company. You can have multiple ***instances*** in a single Skylar AI system. Another way of thinking of an account is that an account is a "tenant", as in "multi-tenant software".

An account contains a combination of the following:

- ***Instances***. An instance is a logical store for account data. In other words, an instance is a complete Skylar AI system with its own set of login credentials and user settings. Examples of instances include a production instance, a QA instance, and a testing instance. An account can contain multiple instances. A ***user*** can view only the instances that are specified on the ***groups*** to which that user is a member. If only one instance is available, you will use the instance labeled "default".

  On the **Available Instances** page in Skylar Settings (Instances > Available Instances), you can view a list of instances for the current user. An "Admin" user can also access the "Analytics Secrets" for an instance, which contains the Microsoft Open Database Connectivity (ODBC) host, password, port, and user information for Data Exploration using ODBC. Also, if your system is using more than one instance, you will be able to select an instance after you log into Skylar Analytics.

- ***Access Tokens***. You can add access tokens to connect Skylar AI with SL1 or a third-party application. The ***scope*** of an access token determines which application or service you can connect to with the access token. You can select more than one scope for an access token. You will need a different access token for each Skylar AI instance you are connecting to with an access token. You can set an expiration date for an access token, and you can also regenerate a token if needed.

  On the **Access Tokens** page in Skylar Settings (Instances > Access Tokens), you can view and add access tokens. For more information, see *Using Access Tokens for Users*.

- ***Users***. Each person that uses Skylar AI should have his or her own user account. A user must belong to at least one ***group***.

  On the **Users** page in Skylar Settings (Account Access > Users), you can view, edit, and add users for an account, and you can also reset the password for a user.

- ***Groups***. A group controls which areas of Skylar AI a user can access. User groups are configured with a ***role*** and either a list of specific instances or *All* instances. If you select *All* instances, any instances that are created later are aligned with this group. Users can belong to more than one group. The active role for a user is based on the highest privilege from the groups aligned with that user.

  On the **Groups** page in Skylar Settings (Account Access > Groups), you can view, edit, and add user groups for an account.

- ***Roles***. A role controls what features a user can access. You assign a role by creating or editing a user, and then aligning a group to that user. The active role for a user is based on the highest privilege from the groups aligned with that user. You can view a list of roles on the **Roles** page in Skylar Settings (Account Access > Roles).

  The types of roles include the following:

  - **Super User**. Assigned to the single **admin** user to manage all user accounts. The default login is **skylar@sciencelogic.com**. The Super User role can create and manage customer accounts, manage multiple instances, and set up SAML authentication for a customer.
  - **Service Provider**. This role lets you provision new accounts and set up SSO for accounts. This role cannot edit the user with the Super User role.
  - **Owner**. This role lets you monitor user management and user access, including the creation and assignment of instances. The **Owner** role also has the privilege to reset a user password.
  - **Admin**. This role lets you perform day-to-day configuration tasks, including integrations and customization. You can also add, edit, and delete users.

    NOTE: For this release of Skylar AI, the **Admin**, **Editor**, and **Viewer** roles are the same. In future releases, these roles will be further defined.

  - **Editor**. For a future release, this role will let a user edit (create, update, and delete) objects, particularly incident type metadata.
  - **Viewer**. For a future release, this role will give a user read-only access to Skylar AI. A **Viewer** user can edit his or her own profile.

- ***Authentication***. Each Skylar AI system is configured by the **Owner** user by default for email authentication, which uses an email address and password combination. An **Owner** user can also set up authentication with a shared Identity Provider through the SAML2 protocol. If you enable single sign-on (SSO) with SAML, users that log in with the specified domain will be redirected to the SAML provider for this account.

  On the **Authentication** page in Skylar Settings (Account Access > Authentication), you can configure SAML for this account. For more information, see *Configuring SSO Authentication with SAML*.

Configuring SSO Authentication with SAML

Users with the **Owner** role can configure single sign-on (SSO) authentication with SAML for their accounts. When SSO authentication with SAML is enabled, all logins for that customer will be authenticated by the SAML identity provider, such as Auth0, Okta, or JumpCloud.

If you have an issue with authenticating, you can contact ScienceLogic to disable SAML for the account and potentially reset the owner's local (non-SAML) password if needed.

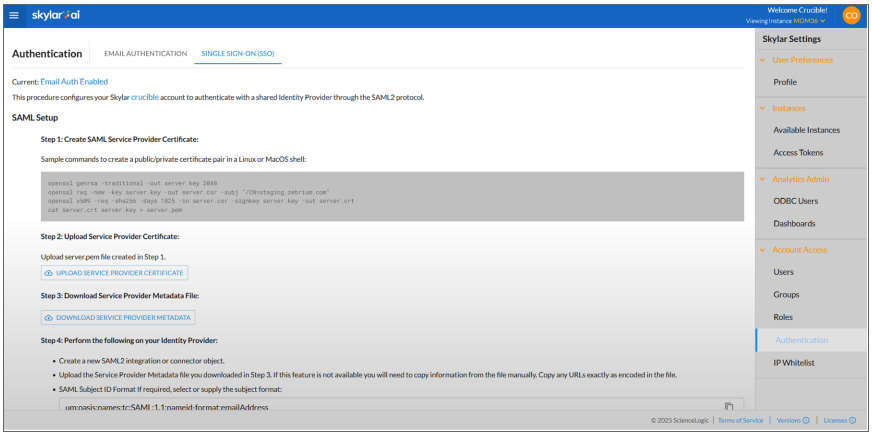
IMPORTANT: Before you can set up SSO authentication with SAML in Skylar AI, you will first need to create your user groups with your SAML identity provider if you do not already have them set up. Be sure to use the same names for your user groups with your SAML provider and with Skylar AI.

IMPORTANT: Do not switch the account to SAML until you have confirmed that the owner of the account has properly configured their SSO provider to recognize the Skylar platform.

To set up SSO Authentication with SAML in the Skylar AI user interface:

1. In Skylar Settings, go to the **Groups** page (Account Access > Groups) and click **[Add Group]**. The **Add Group** dialog appears.
2. Type a name for the group, select a role of *Admin*, and select one or more instances.
3. Click **[Add]**. The group is added to the **Groups** page.

4. Go to the **Authentication** page, click the **[Single Sign-On (SSO)]** tab, and review the instructions for SAML setup:



5. Follow steps 1-7 from the **[Single Sign-On (SSO)]** tab.

> **TIP:** For step 7 on the **[Single Sign-On (SSO)]** tab, after you click the **[Set Authentication Style]** button, you can select *Enable SAML Test Mode for 10 minutes* to test the new authentication configuration. If the authentication works as expected, you can come back to step 7 and select *SAML* to make the configuration permanent.

Creating Access Tokens for Users

You can use the **Access Tokens** page in Skylar Settings (Instances > Access Tokens) to add access tokens to connect Skylar AI with SL1 or a third-party application. A Skylar access token is used for authentication in place of an API key.

You can set an expiration date for an access token, and you can also regenerate a token if needed.

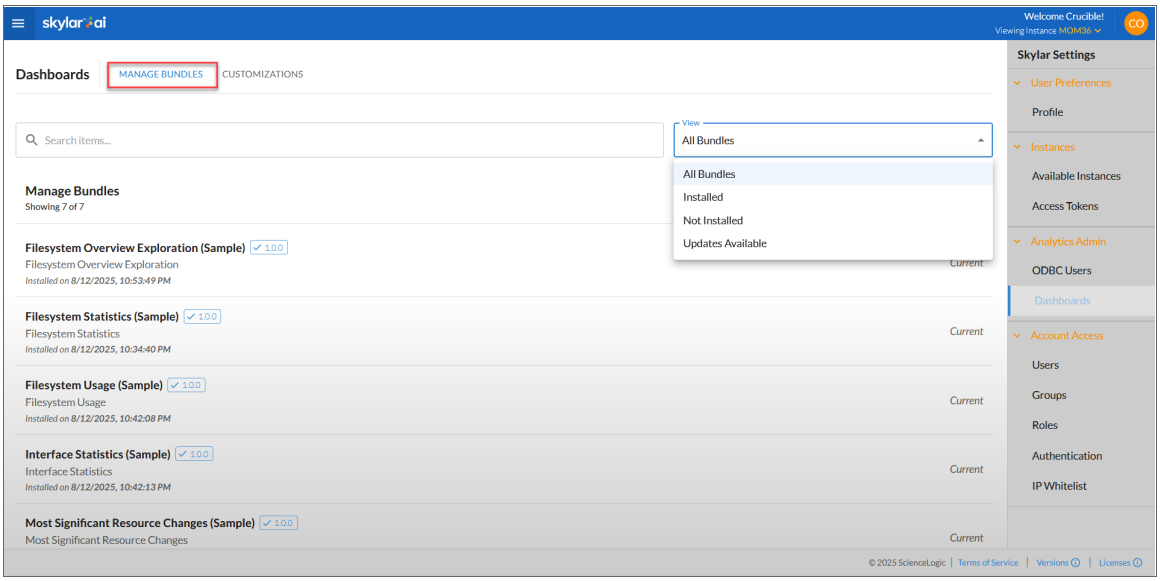
To create an access token:

1. Log in to Skylar AI and select **Skylar Settings**.
2. Go to the **Access Tokens** page (Instances > Access Tokens) .
3. Click the **[Add Access Token]** button. The **Add Access Token** window appears.
4. Complete the following fields:
   - ***Name***. Type a name for the token, such as "SL1 Collector".
   - ***Scopes***. The scope of an access token determines which application or service you can connect to with the access token. You can select more than one scope for an access token. You will need a different access token for each Skylar AI instance you are connecting with access token. If you are creating this access token to *Create a Service Connection* in SL1 , select both *sl1_connector* and *telemetry*.
   - ***Expiration Date***. Select an expiration date.

5. Click the **[Add]** button. The access token is added to the **Access Tokens** page.
6. Click the copy icon ( ) to copy the access token to the clipboard.

Adding and Upgrading Dashboards

A user with an Owner role can add Skylar Analytics dashboards and upgrade existing dashboards on the **[Manage Bundles]** tab of the **Dashboards** page in Skylar Settings:



You can search for dashboard bundles and sort the list of bundles by *All Bundles*, *Installed*, *Not Installed*, and *Updates Available*.

These dashboards include "(Sample)" at the end of each dashboard name.

The options on the **Dashboards** page include:

- ***Current***. Shows that you are running the most recent version of a dashboard.
- **[Add to Skylar]**. Click this button to install a new dashboard for Skylar Analytics
- **[Upgrade Now]**. Click this button to upgrade an existing dashboard.

In addition, you can use the **[Sync Skylar Datasets]** button on the **[Customizations]** tab on the **Dashboards** page to update all of your datasets based on SL1 PowerPacks, including PowerPacks that have been updated in SL1. If all datasets have been updated, the button does not appear, and the text "Datasets are current" appears instead. This button is only available to Owner users in Skylar AI.

Appendix

A

Service Provider Administration for Skylar AI

Overview

This chapter explains the different tasks that a user with the **Service Provider** role can perform in Skylar AI. A **Service Provider** user can provision new accounts.

> **IMPORTANT:** This appendix is intended only for Skylar AI users with a role of **Service Provider**.

This chapter covers the following topics:

First Login as a Service Provider User

When you first log in to your Skylar AI system, you will use the default service provider name of **provider@sciencelogic.com**. The user interface will prompt you to set the ScienceLogic user password before your first login can continue.

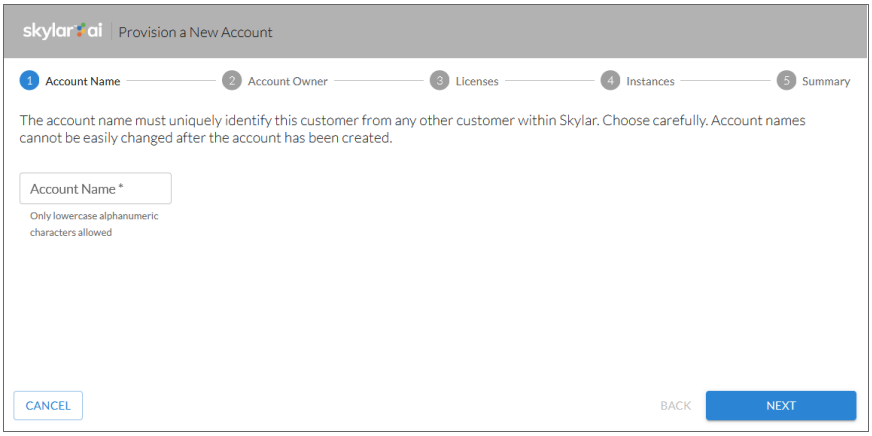
After you log in for the first time, you will see a link for just the ***Skylar Settings*** page on the ***Skylar AI*** home page. Click that link to start setting up new accounts. After you set up a licensed version of Skylar Analytics in the ***Skylar Settings*** page, you will see an ***Analytics*** link on this home page.

Provisioning a New Account

You can have multiple accounts in a single Skylar AI system. To add a new account, you will need to provision that account in the ***Skylar Settings*** page.

To create a new account:

1. On the **Skylar Settings** page, create a new account by clicking the ***All Accounts*** drop-down at the top of the **Skylar Settings** page and clicking **[Provision New Account]** at the bottom of the drop-down. The **Provision a New Account** wizard appears:



2. On the **Account Name** page, type the ***Account Name*** using only lower-case alphanumeric characters, and then click **[Next]**.
3. On the **Account Owner** page, specify the ***First Name***, ***Last Name***, and ***Email*** for the first user of the new account. When you type the email address, Skylar AI adds the domain name from that email into the ***Claim Email Domain*** field. Click **[Next]**.

NOTE: When single sign-on (SSO) through SAML is enabled, users that log in with the domain used by SAML will be redirected to the SAML provider for this account.

4. On the **Licenses** page, select ***Skylar Analytics*** to enable Skylar Analytics for this account.
5. If you select ***Enable ODBC***, you will need to add the IP addresses for your ODBC client in the ***ODBC Client IP Ranges*** field. Be sure to add the public-facing IP address for the ODBC client to the "allow list" for Skylar AI. Click **[Next]**.

> **NOTE:** You will need to add any ODBC users after you complete this procedure. For more information, see *Adding an ODBC User*.

6. On the **Instances** page, type the name of your instance for this account, using only lower-case alphanumeric characters. You can also use *default* as the instance name. Click **[Next]**.
7. On the **Summary** page, review your settings and click **[Begin Provisioning]** to continue setting up the account. The provisioning process begins, and Skylar AI switches to the new account.

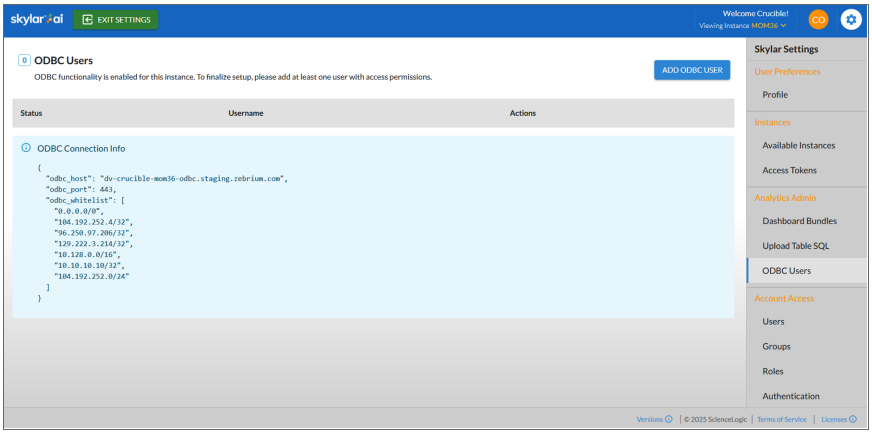
> **NOTE:** When the account is set up, you will need to give the email address you used in step 3 to the first user. On first login, the new user will be prompted to change their password.

8. To set up single sign-on (SSO) authentication with SAML for this new account, see *Configuring SSO Authentication with SAML*.

Adding an ODBC User

When you create a new ODBC connection for the Data Exploration component of Skylar Analytics, you will need to create the ODBC user or users and set their password from the **[ODBC Users]** tab on the **Skylar Settings** page. You can add, edit, disable, and delete ODBC users through the **Skylar Settings** page.

1. In Skylar Settings, got to the **ODBC Users** page (Analytics Admin > ODBC Users). This page displays the ODBC connection information for the Skylar AI system:



2. Click the **[Add ODBC User]** button. The **Add ODBC User** window appears.

3. In the **Username** field, type a name after the "odbc_" prefix, and then type the password in the two **Password** fields.
4. Click the **[Add]** button. The ODBC user is added to the **ODBC Users** page.

800-SCI-LOGIC (1-800-724-5644)

International: +1-703-354-1010