OneTrust Data Discovery offers the following credential store options when configuring and deploying worker nodes for data sources. Data source credentials are stored in a local vault and only referenced to perform scans. They are never sent to the OneTrust Cloud.

For more information on this module's security and encryption practices, please reference Data Discovery Security Guide.

### CyberArk - Conjur

| Field | Description |
|---|---|
| Appliance URL **(Required)** | Enter the URL of the Conjur appliance to which you are connecting. |
| Account **(Required)** | Enter the organization account assigned during the Conjur appliance installation. |
| Login **(Required)** | Enter the fully-qualified ID of a Conjur host for the service broker. |
| API Key **(Required)** | Enter the API Key of the Conjur host whose identity you provided in the Login field. |
| Account Type | Enter the account type. Variable is selected by default. |

As well – **separate** installation guide documentation below

You can opt to follow a guided installation process when creating your on-premises worker node for OneTrust Data Discovery.

For information on how to manually install the worker node, see Manual Installation Overview.

**NOTE**

Some features in this article may only be available as preview feature. Please reach out to your dedicated OneTrust contact or OneTrust Support to learn how you can get early access to this feature.

## Prerequisites

You will need at least the following to support worker node creation with OneTrust Data Discovery. The platform-specific installation articles in Data Discovery Knowledge Base will provide additional detail around what support is needed for the given deployment.

- Environment with nodes to support at least 8 vCPU(s), 32 GB RAM
- A subscription which can run the required cluster
- An owner/contributor user of the given subscription which will be used to access, create, and manage the cluster

- A local (laptop) or remote (Jump box/bastion) machine which will be used to access the cluster master. Minimum: 4 CPU, 8GB RAM, 250 GB HDD, Ubuntu 16+
- Virtual Network and subnet in which the given cluster is getting deployed should have access to data sources
- Virtual Network and subnet in which the given cluster is getting deployed should have access to Internet to reach Docker Hub
- Docker >=19.x ce + pre-installed (OneTrust can also install this)
- Latest version of kubectl to ensure full compatibility of services

## To create worker node

1. On the Data Discovery menu, select Worker Nodes. The **Worker Nodes** screen appears.
2. Click the Add Worker Node button. The **Create Worker Node** modal appears.
3. Enter a name and description for the new worker node.

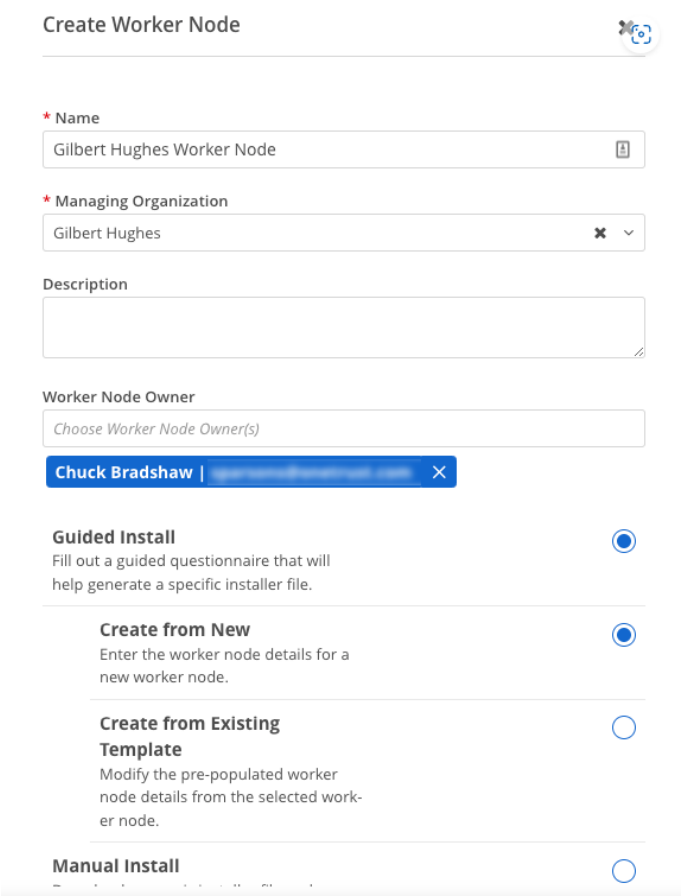
   **NOTE**

   The name you enter here will be populated as the namespace in the follow screen. It will default to lowercase with no spacing in order to meet the namespace formatting requirements.
4. Complete the fields, then select the **Guided Install** option.

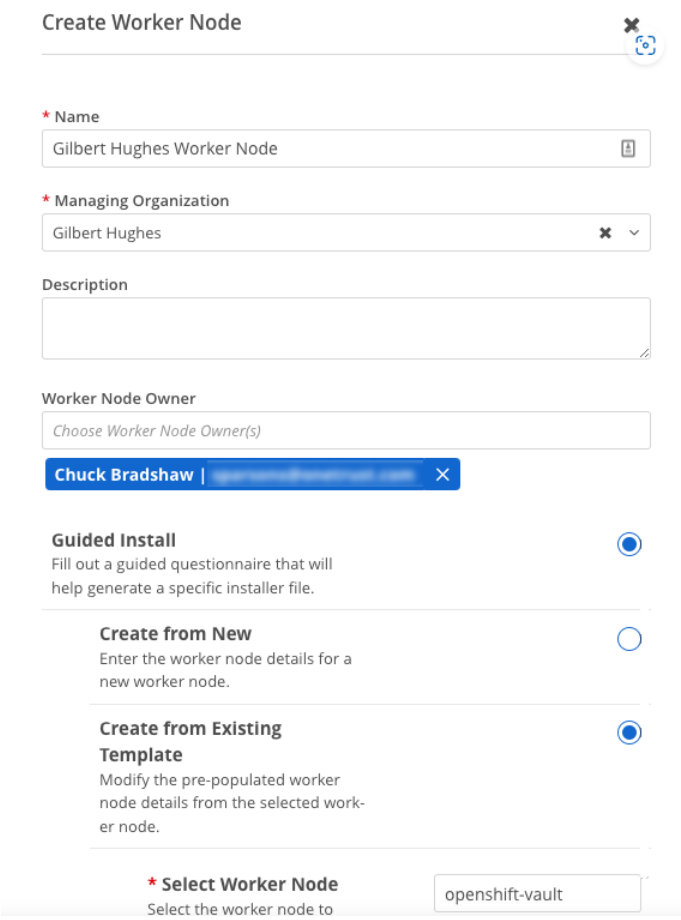
   **NOTE**

   Assigning a managing organization during worker node creating is currently behind preview.

   For more information on worker node owners and email alerts, see Managing Email Notifications for Worker Nodes.



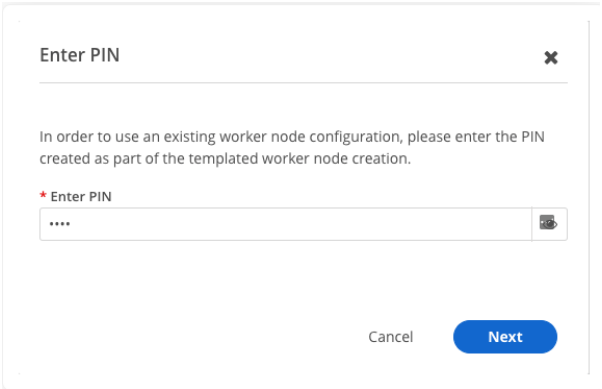

5. **Optional:** With the guided installation option, you can also choose to create the new node by copying an existing guided worker node template configuration.




6. Click the Next button. The **Platform Provider and Credential Store** screen appears. Proceed to To configure worker node.

   If using the worker node template option, the **Enter PIN** modal appears. See step #7 for more.

7. In order to use an existing worker node configuration, please enter the PIN created as part of the templated worker node creation. For more information on how to create and obtain a PIN, see To set up a PIN.



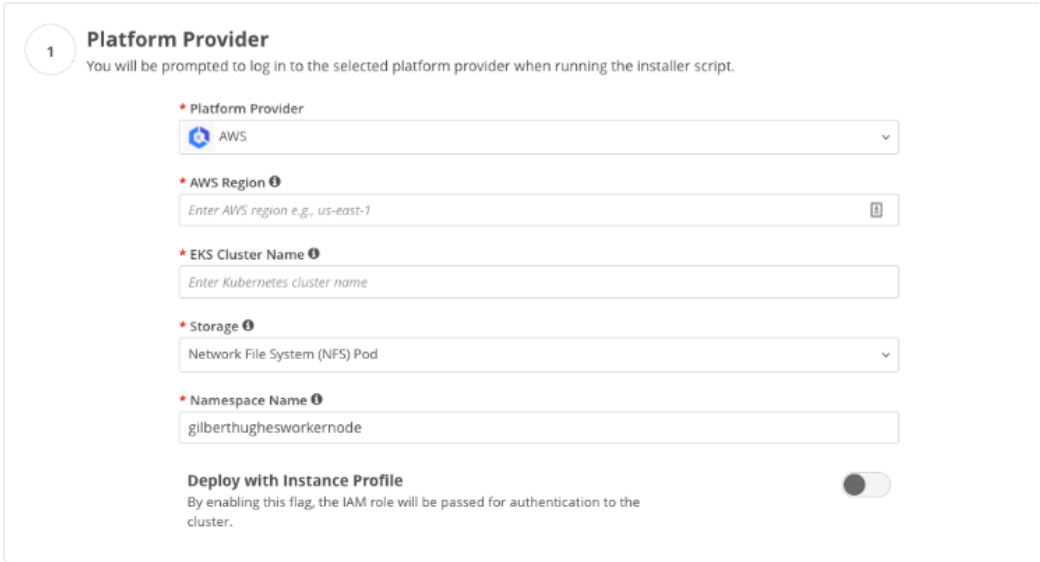

8. Click the Next button. The **Platform Provider and Credential Store** screen appears.

## To configure worker node

By selecting the **Guided Install** option, you can then proceed with configuring the worker node by following the wizard steps. In this example, we're creating a worker node to use with the Azure platform. The majority of these fields will be generally available to any platform provider.

See Data Discovery Deployment Options for more information on available systems.

1. In the **Platform Provider and Credential Store** screen, select your platform provider. The interface will auto-populate fields applicable to the chosen system. Here, we have selected **Azure**.
2. In the **Platform Provider** block, select your desired provider from the field and then complete the fields for given configuration. See the provider information tables below for more information.




3. In the **Credential Store** block, select your desired credential store from the field and then complete the fields with your applicable vault details.

> **NOTE**
>
> For more information on support and configuration of credential vaults, see Credential Vault Configuration for Data Sources.

| Field | Description |
| --- | --- |
| Credential Store | Select from the available **Credential Store** choices. The selection will populate unique fields for each store option. |
| Store Options | AWS Secrets Manager |
| | Azure Key Vault |
| | CyberArk - Conjur |
| | Google Secrets Manager |
| | HashiCorp Vault - Open Source (Internal) |
| | HashiCorp Vault - Open Source (External) |
| | HashiCorp Vault - Enterprise |