One Identity Starling

User Guide

One Identity LLC.
Attn: LEGAL Dept
4 Polaris Way
Aliso Viejo, CA 92656

Refer to our Web site (http://www.OneIdentity.com) for regional and international office information.

Patents

Trademarks

Legend

WARNING: A WARNING icon highlights a potential risk of bodily injury or property damage, for which industry-standard safety precautions are advised. This icon is often associated with electrical hazards related to hardware.

CAUTION: A CAUTION icon indicates potential damage to hardware or loss of data if instructions are not followed.

StarlingUser Guide
Updated - 24 August 2022, 07:14

For the most recent documents and product information, see Online product documentation.

Contents

One Identity Starling

Introduction to One Identity Starling

Starling helps to combine products from the One Identity line to create a secure and customizable cloud service. Administrators use the Starling site to create a new organization, register new accounts, add services to their organization, and gain secure access to those services. Although the main Starling portal can be used to create a free Starling account and provides access to the services currently available for subscriptions, some of the services must be purchased in order for them to be available for full-time use. For more information on adding a service, use the information associated with each service.

In addition to the main Starling site (https://www.cloud.oneidentity.com/), which contains information and links regarding Starling as well as One Identity overall, are the sites that correspond with the services enabled for use:

> NOTE: The availability of services depends on whether your data is being stored in the United States or European Union data center.

Starling Two-Factor Authentication

- Starling Two-Factor Authentication: Accessible from the Starling site, this service uses advanced two-factor authentication capabilities to further protect your resources. For information regarding this service, see the documentation specific to Starling Two-Factor Authentication.

One Identity Hybrid Subscription

- One Identity Hybrid Subscription: Accessible from the Starling site, this service is only available to users that have a valid license for a One Identity product eligible to join with Starling that have also purchased One Identity Hybrid Subscription. This service allows you to view the One Identity products that have been joined to Starling via the Hybrid subscription and manage the collaborators for the One Identity Hybrid Subscription service.

Starling Connect

- Starling Connect: Accessible from the Starling site, this service allows you to extend cloud based applications to existing SCIM clients. For information regarding this service, see the documentation specific to Starling Connect.

Starling CertAccess

- Starling CertAccess: Accessible from the Starling site, this service allows you to manage access requests and access certifications in an Active Directory environment managed by One Identity Active Roles. For information regarding this service, see the documentation specific to Starling CertAccess.

Safeguard Remote Access

- Safeguard Remote Access: Accessible from the Starling site, this service is designed to act as a client-less, browser-based secure terminal access to servers via integration with the Safeguard for Privileged Sessions (SPS) product. For information regarding this service, see the documentation specific to Safeguard Remote Access.

Starling Cloud Assistant

- Starling Cloud Assistant: Accessible from the Starling site, Starling is a messaging services that allows you to both view and respond to messages from on-premises One Identity products (that have been joined to your Starling organization) in an external channel (for example, Microsoft Teams).

There is also a service information site (http://status.cloud.oneidentity.com/) for viewing the current operational status of each service. This site is useful if you are having difficulties connecting to a service and want to check if there are any reported issues prior to contacting Support for additional assistance.

> NOTE: To view the documentation or contact support within any of the services, click the ? button.

Supported browsers

The following browsers are supported when accessing the Starling service.

Table 1: Supported desktop browsers

Browser	Minimum OS/Platform	Version
Google Chrome	Windows 10 Mac OS X Yosemite	Latest

Browser	Minimum OS/Platform	Version
Mozilla Firefox	Windows 8.1	Latest
Microsoft Edge	Windows 10	Latest
Safari	Mac OS X Yosemite	See OS/Platform

Table 2: Supported mobile browsers

Browser	Minimum OS/Platform	Version
Google Chrome	Android	Latest
Safari	iOS	Latest

Navigating Starling using a mobile device

NOTE: Not all services available through Starling may be compatible with mobile devices. Refer to any additional documentation specific to each service for information.

Starling as well as some of the services to which you can subscribe are compatible with mobile devices. For those services that are compatible, use the button at the top of your screen to display the navigation bar options and account information. Also, be aware that due to space constraints some tables may be condensed when viewed in portrait mode to only display key columns.

Additional hardware and software requirements

In addition to the browser compatibility requirements for Starling (see Supported browsers), some additional requirements may need to be met. See the table below for information on those requirements.

The services available through Starling may also include additional hardware and software requirements. Any requirements that must be met by users of a particular service are available within the documentation specific to the service.

Connectivity requirements for Starling

The following DNS addresses are required when integrating with Starling overall. Depending on the Starling service(s) used, additional DNS addresses may be required. For more information, see the documentation for each service.

Table 3: DNS addresses

DNS Name	Purpose
account.cloud.oneidentity.com account.cloud.oneidentity.eu	Landing page of a Starling organization.
accountsupervisor.cloud.oneidentity.com accountsupervisor.cloud.oneidentity.eu	Join/unjoin a product to a Starling organization.
discovery.cloud.oneidentity.com discovery.cloud.oneidentity.eu	Determine correct URLs for subsequent calls based on geography.
sts.cloud.oneidentity.com sts.cloud.oneidentity.eu	Obtain access tokens for calling various Starling APIs.
www.cloud.oneidentity.com (cloud.oneidentity.com) www.cloud.oneidentity.eu (cloud.oneidentity.eu)	Public landing page of Starling services.
status.cloud.oneidentity.com status.cloud.oneidentity.eu	Public Starling service status page.
directory-proxy.cloud.oneidentity.com directory-proxy.cloud.oneidentity.eu	API endpoint for service to access user and group information.

(Optional) Feature requirements

Table 4: (Optional) Feature requirements

Feature	Requirement
Work accounts	To authenticate using a work account, you need the following: • Fully configured Azure AD tenant capable of authenticating users • In cases where an organization has registered an Azure AD tenant but it is not fully synchronized or an account has not yet been added, the owner of that account will be unable to use Starling at that time unless they register independently from the organization.
Event forwarding	To use the event forwarding feature, you need the following: • A service that supports SYSLOG (for example, Loggly)

Organization creation and management

Introduction to organizations and accounts

One Identity Starling requires you to have a Starling organization and account in order to access the services. These organizations and accounts are created and accessed in one of two ways:

1. General accounts: This type of account setup uses Starling to authenticate users.
    - Creating a new organization
    - Signing in to Starling
2. Work accounts: This type of account setup depends on there being a fully configured Azure AD tenant that is capable of authenticating users. Starling will redirect users with an existing work account to the Azure AD tenant for authentication when they initially create an organization within Starling and for all future access.
    - Creating a new organization using an existing Azure AD tenant
    - Signing in to Starling using an Azure AD tenant

Once you have created and accessed an organization and account, the title bar is used to manage them:

- : If multiple organizations are associated with your account, this button (displaying the name of the organization you are currently viewing) appears and opens a drop-down menu that allows you to move between organizations. See the documentation related to your subscribed services for information on how to create and manage accounts affiliated with multiple organizations.
- : This button (displaying the first name of the user) opens a drop-down menu that allows you to select one of the following options:
    - **Sign out** - Clicking this option signs you out of One Identity Starling.

Creating a new organization

To begin using Starling and its associated services, you must first create an organization.

To create an organization and account

1. Open the Starling site (https://www.cloud.oneidentity.com/).
2. From the Starling home page, click **TRY STARLING**.
3. Select **United States** (for the United States data center) or **European Union** (for the European Union data center).
4. Review the legal notice and accept the use of cookies by clicking **Accept**. This will allow Starling to store your information for future logins.
5. In the email address field, enter the email address that will be associated with the account. The email address must be less than 64 characters for the local-part and for each domain part (the full email must be less than 255 characters). You need access to the specified email account to complete your registration and any future communications regarding your organization and account will be sent to this email address.

   NOTE: If the incorrect data center has been stored, select the displayed name of the currently stored data center (United States or European Union) to reselect your data center region. This will restart the process for storing your login information.
6. Click **Next**.

   NOTE: At this point Starling checks if your email address belongs to a fully configured Azure AD work account. If that is the case, see Creating a new organization using an existing Azure AD tenant.

   If you have an Azure AD tenant registered but not fully configured, you will need to use an account not dependent upon Azure AD when signing up for Starling.
7. In the **Organization Name** field, enter the name of your organization (up to 100 characters long).
8. In the **First Name** field, enter the first name of the account holder (up to 64 characters long).
9. In the **Last Name** field, enter the last name of the account holder (up to 64 characters long).
10. In the **Create Password** field, enter a password for your account. The password must consist of eight to sixteen characters and include three of the following items: uppercase letter, lowercase letter, number, or symbol.
11. Enter a phone number for the account.
12. Read through the Terms of Use, Privacy Policy, Software Transaction Agreement, and SaaS Addendum. If you agree, select the check box associated with the requirement.
13. After entering all your information and accepting the terms and conditions, click **START** to send a verification email. It could take a few minutes for the email to appear in your inbox.

14. Once the verification email has arrived, click the **Complete your registration** link within the email to open the login page of Starling.
15. Enter your credentials to access Starling.

Signing in to Starling

The following procedure applies to users that are accessing a Starling account that is not associated with an existing work account.

To sign in to Starling

> NOTE: If your Starling account is associated with a work account, see Signing in to Starling using an Azure AD tenant for more information.

1. From the Starling home page (https://www.cloud.oneidentity.com/), click **Sign in to Starling**.
2. The next steps will depend on whether or not you have previously stored login information.
    - If signing in to Starling using a browser that has not previously stored login information:
        a. Select **United States** (for the United States data center) or **European Union** (for the European Union data center).
        b. Review the legal notice and accept the use of cookies by clicking **Accept**. This will allow Starling to store your information for future logins.
        c. Enter your email address then select **Next**.

        > NOTE: If the incorrect data center has been stored, select the displayed name of the currently stored data center (United States or European Union) to reselect your data center region. This will restart the process for storing your login information.

        d. Enter your password then click **SIGN IN**.

        You are now signed in to Starling.
    - If signing in to Starling using a browser that has previously stored your login information:
        a. Review your email address and region, then select **Next**.

        > NOTE: If the incorrect data center has been stored, select the displayed name of the currently stored data center (United States or European Union) to reselect your data center region. Follow the steps provided above for a browser that has not previously stored login information.

        b. Once Starling has confirmed there is no work account associated with your email address, a password prompt will appear. Enter your password then click **SIGN IN**.

        You are now signed in to Starling.

Creating a new organization using an existing Azure AD tenant

To begin using Starling and its associated services, you must first create an organization. the following procedure is used when your email address is associated with an existing work account.

To create an organization and account using an existing Azure AD tenant

NOTE: This method requires a fully configured Azure AD tenant that is capable of authenticating users. If you have not yet configured Azure AD to handle authentication, you will need to use an account not dependent upon Azure AD when signing up for Starling.

1. Open the Starling site (https://www.cloud.oneidentity.com/).
2. From the Starling home page, click **TRY STARLING**.
3. Select **United States** (for the United States data center) or **European Union** (for the European Union data center).
4. Review the legal notice and accept the use of cookies by clicking **Accept**. This will allow Starling to store your information for future logins.
5. In the email address field, enter the email address that will be associated with your account. The email address must be less than 64 characters for the local-part and for each domain part (the full email must be less than 255 characters). Any future communications regarding your organization and account will be sent to this email address.

   NOTE: If the incorrect data center has been stored, select the displayed name of the currently stored data center (United States or European Union) to reselect your data center region. This will restart the process for storing your login information.
6. Click **Next**.

   NOTE: At this point Starling checks if your email address belongs to a currently configured work account. If your email address is not associated with an existing work account, see Creating a new organization.
7. You will be redirected to your company's account login page. Follow your company's authentication process until you are redirected back to Starling to complete creating your organization and account. Some of the following fields may already be filled in.
8. In the **Organization Name** field, enter the name of your organization (up to 100 characters long).
9. In the **First Name** field, enter the first name of the account holder (up to 64 characters long).
10. In the **Last Name** field, enter the last name of the account holder (up to 64 characters long).
11. Enter a phone number for the account.
12. Read through the Terms of Use, Privacy Policy, and Software Transaction Agreement. If you agree, select the check box associated with the requirement.

13. After entering all your information and accepting the terms and conditions, click **START**.

    You are now logged in to Starling.

Signing in to Starling using an Azure AD tenant

The following procedure applies to users that are accessing Starling using an existing work account.

To sign in to Starling using an Azure AD tenant

NOTE: If your Starling account is not associated with a work account, see Signing in to Starling for more information.

1. From the Starling home page (https://www.cloud.oneidentity.com/), click **Sign in to Starling**.
2. The next steps will depend on whether or not you have previously stored login information.
    - If signing in to Starling using a browser that has not previously stored login information:
        a. Select **United States** (for the United States data center) or **European Union** (for the European Union data center).
        b. Review the legal notice and accept the use of cookies by clicking **Accept**. This will allow Starling to store your information for future logins.
        c. Enter your email address then select **Next**.

            NOTE: If the incorrect data center has been stored, select the displayed name of the currently stored data center (United States or European Union) to reselect your data center region. This will restart the process for storing your login information.

        d. Once Starling has confirmed there is a work account associated with your email address, you will be redirected to your company's account sign in page. Follow your company's authentication process to finish signing in to Starling.
    - If signing in to Starling using a browser that has previously stored your login information:
        a. Review your email address and region, then select **Next**.

            NOTE: If the incorrect data center has been stored, select the displayed name of the currently stored data center (United States or European Union) to reselect your data center region. Follow the steps provided above for a browser that has not previously stored login information.

b. Once Starling has confirmed there is a work account associated with your email address, you will be redirected to your company's account sign in page. Follow your company's authentication process to finish signing in to Starling.

Resetting password

The following procedure applies to users that have forgotten their password for an existing Starling account and are not using an Azure AD tenant for their authentication.

To reset a Starling account password

1. From the Starling home page (https://www.cloud.oneidentity.com/), click **Sign in to Starling**.
2. The next steps will depend on whether or not you have previously stored login information.
    - If signing in to Starling using a browser that has not previously stored login information:
        a. Select **United States** (for the United States data center) or **European Union** (for the European Union data center).
        b. Review the legal notice and accept the use of cookies by clicking **Accept**. This will allow Starling to store your information for future logins.
        c. Enter your email address then select **Next**.

        NOTE: If the incorrect data center has been stored, select the displayed name of the currently stored data center (United States or European Union) to reselect your data center region. This will restart the process for storing your login information.

        d. On the password prompt page, click **Forgot your password?**.
        e. In the email address field, enter the email address associated with your account.
        f. Click **Next**.
        g. On the password prompt page, click **Forgot your password?**.
        h. Enter the email address associated with your account. A verification code will be sent to that email address.
        i. Click **Next**.
        j. In the **Verification code** field, enter the code you received.
        k. Click **Verify**.
        l. A confirmation of verification page will appear. Click **Continue**.
        m. In the **New Password** field, enter the password to use for your account.
        n. In the **Confirm New Password** field, enter the same password.

o. Click **Continue**.

You have now reset your password and are logged in to Starling.

- If signing in to Starling using a browser that has previously stored your login information:

    a. Review your email address and region, then select **Next**.

    NOTE: If the incorrect data center has been stored, select the displayed name of the currently stored data center (United States or European Union) to reselect your data center region. Follow the steps provided above for a browser that has not previously stored login information.

    b. On the password prompt page, click **Forgot your password?**.

    c. In the email address field, enter the email address associated with your account.

    d. Click **Next**.

    e. On the password prompt page, click **Forgot your password?**.

    f. Enter the email address associated with your account. A verification code will be sent to that email address.

    g. Click **Next**.

    h. In the **Verification code** field, enter the code you received.

    i. Click **Verify**.

    j. A confirmation of verification page will appear. Click **Continue**.

    k. In the **New Password** field, enter the password to use for your account.

    l. In the **Confirm New Password** field, enter the same password.

    m. Click **Continue**.

    You have now reset your password and are logged in to Starling.

Introduction to services

Once you have created a Starling organization, you can begin adding services to that organization. The type of subscription a service is originally designated as may change at a later date. This is due to the continuous improvement and expansion of the main Starling product, as well as any changes and additions made to the available services.

The types of subscriptions available within Starling fall into different categories:

- Paid subscriptions
- Trial subscriptions

Paid subscriptions

The services available for purchase can be accessed by any Starling organization. A subscription to this type of service will provide you with full access to that One Identity product for the length of your contract. For information on purchasing a subscription to a service, on the home page use the **More Information** button associated with the service and consult the documentation specific to that service for additional information.

NOTE: Contact Sales or Support to cancel a paid subscription.

Trial subscriptions

The services available for trials can be subscribed to for a limited period of time before they require a full subscription. This allows you to view and test the product before making a longer term commitment to using the service.

- Starting a service trial
- Ending a service trial

Starting a service trial

Once logged in, you can trial certain services available on the home page of the Starling web site. The available services are listed in the Services section of the page.

To start a service trial

1. Sign in to Starling.
2. From the Starling home page, locate the service you want to trial (the type of service is indicated by the button associated with the service) and click **Trial**.
3. In the dialog, select your country. This field only appears the first time you add a service to your organization.
4. If applicable, a second field will appear in which you must select your state or province from the drop-down list. This field only appears the first time you add a service to your organization.
5. Click **Confirm**.

   The service will be added to the **My Services** section and be available for use until the trial period has ended. The number of days left in your trial is indicated by a countdown on the service access button on the Starling home page. At any point in the trial you can use the **More Information** button associated with the service to find out how to purchase the product.

Ending a service trial

The number of days left in your trial is indicated on the service access button. Once your trial period has ended the service will no longer be accessible. Please see the documentation specific to the service for further information, or use the contact information associated with the service to inquire about purchasing options.

Inviting an administrator to a service

The following procedure applies to organization administrators. It is designed to allow additional administrators to be added and to allow a new administrator to be invited to a service in cases where the last administrator assigned to that service has left the organization.

To invite an administrator to a service

1. Sign in to Starling.
2. From the Starling home page, click the ⋮ button associated with the service to which you want to invite a new administrator.
3. Select **Invite Administrator**.
4. Depending on the type of account, the following methods can be used for inviting a new administrator to the service:
   - To invite an administrator:
     a. Enter the name and email address of the user.
     b. Click **Invite**. An invitation to the service will be sent to the user.
   - To invite an administrator with an Azure AD work account:

     NOTE: This option is only available for organization administrators with an Azure AD work account.

     a. Click the drop-down field.
     b. In the blank search box, begin typing the name of the user. When you have located the user, select them from the list.
     c. Click **Invite**. An invitation to the service will be sent to the user.

Managing multiple organizations

Starling users have the option of adding additional users to their services. In cases where an invited user has already created a Starling organization, they can switch between their organizations.

To switch between organizations

1. Click the  button in the title bar to open a drop-down menu listing the names of the organizations to which you have access.
2. Select the name of the organization to which you want to switch. The services will update to display the information associated with the organization listed in the title bar.

One Identity Starling status

Once you have logged into Starling, in the heading bar there is an icon indicating the status of the Starling service. In the unlikely event that the status page is inaccessible, the status icon will not be displayed. The following icons and options are used to display the status, and clicking the displayed icon provides further information and options:

This icon indicates there are no issues currently being reported for Starling. Upon clicking the icon, a dialog will appear displaying the current status of Starling. Click **View all updates** to open a new tab listing a history of all status updates.

This icon indicates there are issues currently being reported for Starling with the number of issues noted in the upper right corner. Upon clicking the icon, any issues will be listed in the dialog and clicking on an incident will provide a brief explanation of what is happening as well as a **More Details** link should you want more information. Click **View all updates** to open a new tab listing a history of all status updates.

Access Summary page

IMPORTANT: Only organization administrators can access this page.

NOTE: The availability of services depends on whether your data is being stored in the United States or European Union data center.

The **Access Summary** page (see Accessing the Access Summary page for information on accessing this page) allows you to view and manage the users, clients, and joined products associated with your organization.

The following options and information appears on this page:

Show all access

Opening this drop-down menu (which displays **Show all access** by default) filters the listed components and users based on the services they are associated with.

This field is used for filtering the displayed information.

There are four tabs on this page that provide information on the different types of connections.

All Access

The table on this tab contains all of the components and users associated with your Starling service. The following columns appear on this page:

- Name: This is the name of the component or user.
- Identifier: This is the identifier for the component or user. For example, this column might show the email address for a user or the IP address for a configured collector agent.
- Status: This is the current status of the component or user. For example, this column might show the date a product was joined to Starling or the type of access a user has within a service.
- Type: This is the type of component or user.
- Access: This shows the services the component or user is associated with. The following icons are used to denote the services and when clicked will open the service:
  - Starling Two-Factor Authentication
  - One Identity Hybrid Subscription
  - Starling Connect

Users

The table on this tab contains all of the users that have been granted access to a service or are associated with a service in Starling. The following columns appear on this page:

- Name: This is the name associated with the user.
- Email: This is the email address associated with the user.
- Organization Role: This is the type of user.
- Access: This shows the services the user is associated with. The following icons are used to denote the services and when clicked will open the Collaborators page for the service:
  - Starling Two-Factor Authentication
  - One Identity Hybrid Subscription

- Starling Connect

Joined Products

The table on this tab contains all of the products joined with Starling. The following columns appear on this page:

- Instance Name: This is the name of the product instance.
- Product: This is the name of the product.
- Join Date: This shows the date and time the product instance was connected to a Starling service.
- Access: This shows the services the product is associated with.

Accessing the Access Summary page

The **Access Summary** page allows you to view and manage the users associated with your Starling organization.

To access the Access Summary page

NOTE: Only organization administrators can access the **Access Summary** page.

1. Log in to Starling as an organization administrator.
2. Click the **Access Summary** link at the top of the page.

   To return to the Starling home page, click the **Services** link.

Support page

The **Support** page (see Accessing the Support page for information on accessing this page) allows you to access the support resources for your subscribed products as well as provides the licensing information necessary for registering for support.

The following options for support resources appear on this page:

Register for Support

Clicking this button opens the **Create a Support Account** page where you can create a Support Account. This is a One Identity account used to manage your purchased products. In order to register a product for support you will need the licensing key that is located in the **License numbers for Starling subscriptions** section at the bottom of the page.

View Support

Clicking this button opens the One Identity support site.

Contact Support

Clicking this button opens the One Identity **Contact Support** page.

The **License numbers for Starling subscriptions** section of the page is used for accessing product specific support and information sites. Each purchased product will include the license key for your product so that you can register the product for support. If you have not yet purchased a subscription to a product then you can click the **More Information** button for purchasing information.

Accessing the Support page

The **Support** page provides access to support resources for your products as well as provides the licensing information necessary for registering for support.

To access the Support page

1. Log in to Starling.
2. Click the **Support** link at the top of the page.

   To return to the Starling home page, click the **Services** link.

3

Settings

Introduction to the Settings page

The **Settings** page is displayed when the button is clicked in the upper right corner while on the Starling home page. From this page you can access the following settings:

IMPORTANT: The following options vary depending on your user type and data center region. For example, only organization administrators will see the **Delete Organization** option.

- **Event Forwarding**: This page is used to configure event data to be sent to a SYSLOG service. For more information, see Starling event forwarding.
- **Directories**: This page is used for configuring and managing directory services. For more information, see Directories.
- **Applications**: This page is used to create a relying party trust that allows directory users to authenticate and use the target application. For more information, see Applications.
- **Joined Products**: This page is used for unjoining products from Starling in cases where the previously joined product is no longer available. For more information, see Joined Products.
- **Organization Admins**: This page is used for managing the administrators associated with your Starling organization. For more information, see Manage Organization Admins page.
- **Manage GDPR Contacts**: This page is used for managing the General Data Protection Regulation (GDPR) contacts for the organization. For more information, see Managing GDPR contacts.
- **Delete Organization/Leave Organization**: The displayed setting depends on your user type. For more information, see Deleting an organization or Leaving an organization.

Starling event forwarding

The **Event Forwarding** option on the **Settings** page allows you to send Starling event data to a service that supports Syslog. This feature is not enabled by default.

IMPORTANT: For information on the requirements to use this feature, see Additional hardware and software requirements.

To enable event forwarding

IMPORTANT: Only events occurring after the feature has been configured will be sent to your Syslog service and then able to be stored according to your preferences. Events that occur prior to configuration are not forwarded nor are they accessible within Starling.

1. From the Starling home page, click the button in the upper right corner.
2. In the **Event Forwarding** section of the **Settings** page, click **Change**.
3. On the **Configure Event Forwarding** page, click the On/Off toggle to switch it to the **On** position.
4. Fill in the following configuration fields:
    - **Hostname/IP Address**: Enter the hostname or IP address to which the event data will be sent.
    - **Port**: Enter the port number in this field. By default this is 6514.
    - **Structured Data ID**: (Optional) Use this field to specify an ID. For example, this could be passed to the Loggly logging service (https://www.loggly.com/) to identify a specific customer tenant within Loggly.

    Once you have filled in these fields the information will be saved automatically. Clicking the **Send Test Event** button will send a test event to your Syslog service to confirm the connection is working.

Directories

The **Directories** option on the **Settings** page allows organization administrators to register an Azure Active Directory instance with Starling to allow services to read users and groups from the directory.

To register and manage an Azure Active Directory instance for use with Starling services

IMPORTANT: You must have the Global Admin role in Azure Active Directory in order to register it as a directory service within Starling.

1. From the Starling home page, click the button in the upper right corner.
2. In the **Directory Services** section of the **Settings** page, locate **Directories** and click **Manage**.
3. On the **Manage Directories** page, click **Register Directory**.
4. On the **Register Directory** pane, select **Azure Active Directory**.
5. Fill in the following configuration fields:
    - **Display Name**: Enter a name for the directory.
    - **Directory/Tenant ID**: Enter the directory/tenant ID for the Azure Active Directory instance you are registering.
6. Click **Give Consent**.
7. You will be redirected to login to Azure Active Directory using your Global Admin account. Once logged in, read through the permissions and if you agree click **Accept**. You will be returned to Starling with the Azure Active Directory instance listed as registered.

    To make changes, click the tile of the directory to be edited. You will need to renew consent should you make any changes to the configuration. To remove the directory, select **Delete** from the **Options** drop-down.

Applications

The **Applications** option on the **Settings** page allows you to add an application to create a relying party trust that allows directory users to authenticate and use the target application.

There are 2 methods for adding applications:

1. Manually configure the application.
2. Upload SAML2 Metadata for the application.

To add applications manually

To add applications manually

1. From the Starling home page, click the button in the upper right corner.
2. Open the **Applications** page.
3. On the **Manage Applications** page, click the **Add Application** button.
4. Select **Add OpenID Connect Application**.
5. Fill in the following configuration fields:

- **Name**: Enter the name of the application.
- **Client ID**: Enter the client ID for the application.

6. In the **Redirect URIs** section, enter the redirect URI information in the field.
7. Click the **Add Redirect URI** button to save. Add additional redirect URIs as needed.
8. Click **Create** to save the application.

To add SAML2 applications

To add applications using SAML2 metadata

1. From the Starling home page, click the button in the upper right corner.
2. Open the **Applications** page.
3. On the **Manage Applications** page, click the **Add Application** button.
4. Select **Add SAML2 Application**.
5. Click the **Select SAML2 Metadata file** button.
6. From the dialog, locate and select the SAML2 Metadata file associated with the application being added.
7. Click **Open**.
8. Click **Create** to save the application.

Joined Products

The **Joined Products** option on the **Settings** page allows you to view and manage the One Identity products currently joined to your Starling organization.

To delete a joined product

CAUTION: This feature is only intended to be used in rare cases (for example, deleting an uninstalled One Identity product that was not first unjoined from Starling). When using this feature, you are only deleting the Starling side of the connection which means an active One Identity product may still attempt to connect. If at all possible, you should use the unjoin option from within the One Identity Product instead since it will correctly disconnect both products.

1. From the Starling home page, click the button in the upper right corner.
2. In the **Joined Products** section of the **Settings** page, click **Manage**.
3. On the **Manage Joined Products** page, locate the product instance to be removed.
4. Click **Delete**.

5. A confirmation dialog will appear warning you of the potential issues with removing a joined product from within Starling instead of through the product itself. Click **Delete** to remove the joined product.

Manage Organization Admins page

IMPORTANT: Only organization administrators can access this page.

The **Manage Organization Admins** page allows you to view and manage the users associated with your organization.

The following options and information appears on this page:

This field is used for filtering the displayed users.

Name

This is the name associated with the user.

Email

This is the email address associated with the user.

Role

This is the role currently assigned to the user.

Clicking the ⋮ button associated with a user allows you to change a user's role. Depending on the type of user you are looking at, **Promote to Organization Admin** or **Demote to Collaborator** will be available for selection.

NOTE: This option does not appear when you are viewing your own account since you cannot demote your own role. It also does not appear for users that do not have a Starling account (for example, Two-Factor Authentication end users). To view a list of users associated with your services, see Access Summary page.

Editing organization roles

The **Manage Organization Admins** page allows organization administrators to manage the users associated with your Starling organization by promoting or demoting a user's access level within the organization.

To edit a role within an organization

NOTE: Only organization administrators can edit roles within an organization. Also, you cannot demote your own role.

1. From the Starling home page, click the button in the upper right corner.
2. In the **Organization Admins** section of the **Settings** page, click **Manage**.
3. Locate the user you want to edit. You can use the filtering options at the top of the page to filter the listed users.
4. Click the button associated with the user and, depending on their current role, you can select to either demote the user to a collaborator or promote them to an organization administrator.
    - **Demote to Collaborator**: Selecting this option will demote the user to a collaborator within the organization. This role retains access to all services they are currently assigned, but they have limited capabilities when it comes to configuring the organization. This means they will be unable to access the **Access Summary** page and cannot delete the organization.
    - **Promote to Organization Admin**: Selecting this option will promote the user to an organization administrator within the organization. This role retains access to all services they are currently assigned and also allows them to configuring the organization. This means they will be able to access the **Access Summary** page and can delete the organization.

    The new user role will automatically save once an option has been selected.

Managing GDPR contacts

The General Data Protection Regulation (GDPR) is a European Union regulation that requires information to be reported regarding sub-processor changes and data breaches. The **Manage GDPR Contacts** page allows organization administrators to manage the users that will be contacted regarding these GDPR items. This page is used for the following tasks:

NOTE: By default, the organization administrator is automatically added as the GDPR contact.

- Adding GDPR contacts
- Editing GDPR contacts
- Deleting GDPR contacts

Adding GDPR contacts

The **Manage GDPR Contacts** page allows organization administrators to add users that will be contacted regarding General Data Protection Regulation (GDPR) items.

To add a GDPR contact

NOTE: Only organization administrators can add GDPR contacts within an organization.

1. From the Starling home page, click the button in the upper right corner.
2. In the **Manage GDPR Contacts** section of the **Settings** page, click **Manage**.
3. Click **Add Contact**.
4. In the **GDPR Contact** dialog, enter a first and last name for the contact.
5. In the **Email** field, enter an email address for the contact. All related GDPR emails will be sent to this address.
6. Select the check box for each type of email that the contact will be sent.
7. Click **Save**.

   The new contact will now be listed on the **Manage GDPR Contacts** page.

Editing GDPR contacts

The **Manage GDPR Contacts** page allows organization administrators to manage the users that are being contacted regarding General Data Protection Regulation (GDPR) items.

To edit a GDPR contact

NOTE: Only organization administrators can edit GDPR contacts within an organization.

1. From the Starling home page, click the button in the upper right corner.
2. In the **Manage GDPR Contacts** section of the **Settings** page, click **Manage**.
3. Locate the user to edit. You can use the button to filter the listed users.
4. Click the button associated with the user.
5. Click **Edit**.
6. In the **GDPR Contact** dialog, make any necessary changes to the GDPR contact. At least one contact must be configured for each type of email.
7. Click **Save**.

Deleting GDPR contacts

The **Manage GDPR Contacts** page allows organization administrators to delete a user that is being contacted regarding General Data Protection Regulation (GDPR) items.

To delete a GDPR contact

NOTE: At least one contact must be configured to receive each type of email.

1. From the Starling home page, click the button in the upper right corner.
2. In the **Manage GDPR Contacts** section of the **Settings** page, click **Manage**.
3. Locate the user to delete. You can use the button to filter the listed users.
4. Click the ⋮ button associated with the user.
5. Click **Delete**.
6. Click **OK** to confirm. The contact will no longer appear listed on the **Manage GDPR Contacts** page.

Leaving an organization

IMPORTANT: If you are the only administrator associated with the organization, you will only see the **Delete Organization** option. For more information, see Deleting an organization.

This section allows you to disassociate your account from the Starling service while still allowing any other administrators access to the organization.

To leave an organization

1. From the Starling home page, click the button in the upper right corner.
2. In the **Leave Organization** section of the **Settings** page, click **Leave**.
3. In the **Leave Organization** dialog, click **Yes**.

Deleting an organization

This section allows you to permanently delete your organization from Starling in addition to all of its associated services. This will impact all administrator accounts associated with your Starling services.

IMPORTANT: Deleting an organization is permanent and you may continue being billed for any paid subscriptions. Contact Sales or Support if you have any billing issues or concerns.

IMPORTANT: You must unjoin any on-premises products currently connected to One Identity Hybrid Subscription before deleting the organization.

To delete an organization

1. From the Starling home page, click the button in the upper right corner.
2. In the **Delete Organization** section of the **Settings** page, click **Delete**.
3. In the **Delete Organization** dialog, click **Yes**.

One Identity Hybrid Subscription

Introduction to One Identity Hybrid Subscription

The One Identity Hybrid Subscription service is used for viewing the One Identity products you have joined to your Starling organization via a Hybrid subscription. The service is only available in a Starling organization for users that have purchased a Hybrid subscription to one or more Starling services, along with a valid license for a One Identity product eligible to join with Starling. Joining Starling from an eligible One Identity product does not always require a Hybrid subscription.

General information regarding your joined products and links to information regarding the process for joining products is displayed at the top of the page.

> NOTE: In order to join a product with your Starling organization via a Hybrid subscription, you must be an administrator or collaborator for the Hybrid subscription, or an organization admin for the Starling organization. See Inviting an administrator to a service for information on adding an administrator to One Identity Hybrid Subscription and Adding additional collaborators for information on adding a collaborator to One Identity Hybrid Subscription.

Products view

The **Products** view is displayed by default and when the **Products** tab is clicked on the **One Identity Hybrid** page. The **Products** view is used for viewing information on the products currently associated with your One Identity Hybrid Subscription service.

The following information and options appear on this view:

> NOTE: If you have not yet joined a One Identity product with your Starling organization and would like more information regarding this service, click the **Find out more about how to join to Starling** link.

(Product name)

The name of the joined One Identity product.

<nn> instance(s)

The number of product instances that were joined to Starling.

Clicking this button displays additional information about each product instance.

- **Instance Name**: The name of the joined instance.
- **Date Joined**: The date the instance was joined to Starling.
- **Joined By**: The name of the user that joined the instance to Starling.

Collaborators view

The **Collaborators** view is displayed when the **Collaborators** tab is clicked on the **One Identity Hybrid** page. The **Collaborators** view is used for adding and managing the collaborators currently associated with One Identity Hybrid Subscription. These collaborators are able to join products to Starling.

The following field and button appear on this view:

Invite Collaborator

This opens the **Invite Collaborator** dialog so you can add new collaborators to One Identity Hybrid Subscription.

This field is used to locate specific collaborators within the **Collaborator** table. To use the field, start typing the name or email of the collaborator in the field and the table will automatically update to display users that match.

The following information and button appears in the **Collaborator** table on this page:

Name

This displays the name specified in the collaborator invite.

Email

This displays the email address to which the collaborator invite was sent.

Status

This displays the status of the user. When a user is added they will be marked as **Invited** until the invitation has been accepted, at which point the **Status** column will update to display **Registered**.

⋮

This button appears for each collaborator and is used for managing the collaborator and removing collaborators from the service.

NOTE: You are unable to remove yourself as a collaborator, and if you are an administrator for the service then only another administrator can remove your administrator role. Coordinate with other administrators before making edits to their roles to avoid removing each other as administrators.

NOTE: Until an invite has been accepted, the following options are available when clicking the ⋮ button:

- **Re-send Invitation**: Selecting this option will re-send the invitation.
- **Cancel Invitation**: Selecting this option will cancel the invitation. The invited user will not be notified that the invitation was canceled; however, when logged in they will be unable to access the service.

Managing collaborators

The following sections provide information on managing collaborators for the One Identity Hybrid Subscription service.

- Adding additional collaborators
- Adding additional Azure AD work account collaborators
- Removing collaborators

Adding additional collaborators

Collaborators are optional and can be added at any time. For information on adding a collaborator from within your Azure AD account, see Adding additional Azure AD work account collaborators.

To add additional collaborators

1. On the **Collaborators** view, click **Invite Collaborator**.
2. In the **Invite Collaborator** dialog, enter the name and email address of the user you would like to add as a collaborator to your organization.
3. Click **Invite**.

An email will be sent with a link to either register a new account that has access to your organization or, if the recipient has already registered with Starling using this email address, a notification they now have access to your organization's One Identity Hybrid Subscription service. They will be marked as **Invited** until the invitation has been accepted, at which point the **Status** column will update to display **Registered**.

> NOTE: Administrators and collaborators associated with multiple organizations can switch between Starling subscriptions once they have logged in (Managing multiple organizations).

> NOTE: Until an invite has been accepted, the following options are available when clicking the ⋮ button:
>
> - **Re-send Invitation**: Selecting this option will re-send the invitation.
> - **Cancel Invitation**: Selecting this option will cancel the invitation. The invited user will not be notified that the invitation was canceled; however, when logged in they will be unable to access the service.

Adding additional Azure AD work account collaborators

Collaborators are optional and can be added at any time. For information on adding a collaborator from outside your Azure AD account, see Adding additional collaborators.

To add additional Azure AD work account collaborators

1. On the **Collaborators** view, click **Invite Collaborator**.
2. Click in the **Search for collaborator** field and begin typing in the empty field to filter the available collaborators.
3. Click the name of the collaborator you want to add to populate the field.

   > NOTE: If the collaborator cannot be found or is not associated with your Azure AD tenant, click **Unable to find collaborator** and enter the name and email address of the user you would like to add as a collaborator to your organization.

4. Click **Invite**.

   An email will be sent with a link to either register a new account that has access to your organization or, if the recipient has already registered with Starling using this email address, a notification they now have access to your organization's One Identity Hybrid Subscription service.

   > NOTE: Administrators and collaborators associated with multiple organizations can switch between Starling subscriptions once they have logged in (Managing multiple organizations).

Removing collaborators

If a collaborator is no longer needed, you can remove their access to One Identity Hybrid Subscription.

To remove collaborators

1. On the **Collaborators** view, locate the user you want to remove as a collaborator. You can use the **Search for collaborators** field at the top of the page to filter the listed collaborators.
2. Click the ⋮ button associated with the user you want to remove.
3. Select **Remove Collaborator**.

   NOTE: You are unable to remove yourself as a collaborator, and if you are an administrator for the service then only another administrator can remove your administrator role. Coordinate with other administrators before making edits to their roles to avoid removing each other as administrators.
4. In the confirmation dialog, click **OK** to remove their access to One Identity Hybrid Subscription.

About us

One Identity solutions eliminate the complexities and time-consuming processes often required to govern identities, manage privileged accounts and control access. Our solutions enhance business agility while addressing your IAM challenges with on-premises, cloud and hybrid environments.

Contacting us

For sales and other inquiries, such as licensing, support, and renewals, visit https://www.oneidentity.com/company/contact-us.aspx.

Technical support resources

Technical support is available to One Identity customers with a valid maintenance contract and customers who have trial versions. You can access the Support Portal at https://support.oneidentity.com/.

The Support Portal provides self-help tools you can use to solve problems quickly and independently, 24 hours a day, 365 days a year. The Support Portal enables you to:

- Submit and manage a Service Request
- View Knowledge Base articles
- Sign up for product notifications
- Download software and technical documentation
- View how-to videos at www.YouTube.com/OneIdentity
- Engage in community discussions
- Chat with support engineers online
- View services to assist you with your product