



One Identity Starling Governance Access Certification

Integration Guide (Technical Preview)

Copyright 2019 One Identity LLC.

ALL RIGHTS RESERVED.

This guide contains proprietary information protected by copyright. The software described in this guide is furnished under a software license or nondisclosure agreement. This software may be used or copied only in accordance with the terms of the applicable agreement. No part of this guide may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying and recording for any purpose other than the purchaser's personal use without the written permission of One Identity LLC .

The information in this document is provided in connection with One Identity products. No license, express or implied, by estoppel or otherwise, to any intellectual property right is granted by this document or in connection with the sale of One Identity LLC products. EXCEPT AS SET FORTH IN THE TERMS AND CONDITIONS AS SPECIFIED IN THE LICENSE AGREEMENT FOR THIS PRODUCT, ONE IDENTITY ASSUMES NO LIABILITY WHATSOEVER AND DISCLAIMS ANY EXPRESS, IMPLIED OR STATUTORY WARRANTY RELATING TO ITS PRODUCTS INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. IN NO EVENT SHALL ONE IDENTITY BE LIABLE FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL, PUNITIVE, SPECIAL OR INCIDENTAL DAMAGES (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, BUSINESS INTERRUPTION OR LOSS OF INFORMATION) ARISING OUT OF THE USE OR INABILITY TO USE THIS DOCUMENT, EVEN IF ONE IDENTITY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. One Identity makes no representations or warranties with respect to the accuracy or completeness of the contents of this document and reserves the right to make changes to specifications and product descriptions at any time without notice. One Identity does not make any commitment to update the information contained in this document.

If you have any questions regarding your potential use of this material, contact:

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

One Identity is proud of our advanced technology. Patents and pending patents may apply to this product. For the most current information about applicable patents for this product, please visit our website at <http://www.OneIdentity.com/legal/patents.aspx>.

Trademarks

One Identity and the One Identity logo are trademarks and registered trademarks of One Identity LLC. in the U.S.A. and other countries. For a complete list of One Identity trademarks, please visit our website at www.OneIdentity.com/legal. All other trademarks are the property of their respective owners.

Legend

-  **WARNING:** A WARNING icon indicates a potential for property damage, personal injury, or death.
-  **CAUTION:** A CAUTION icon indicates potential damage to hardware or loss of data if instructions are not followed.
-  **IMPORTANT, NOTE, TIP, MOBILE, or VIDEO:** An information icon indicates supporting information.

Contents

Access Certification	5
Introduction to Access Certification	5
Supported browsers	5
Navigating Access Certification using a mobile device	6
Additional hardware and software requirements	6
Using the Access Certification service	7
Inviting an administrator to a service	8
Ending a service preview	8
Data Imports	10
Introduction to importing data	10
Data Imports page	11
Identity data	13
Account data	14
Group data	14
Entitlement data	15
Generating CSV files from Safeguard for Privileged Passwords	16
Uploading data	18
Campaigns	20
Introduction to campaigns	20
Campaigns page	20
Managing campaigns	21
Adding a new campaign	21
Running a campaign	22
Duplicating a campaign	23
Editing a campaign	23
Closing a campaign	23
Viewing a campaign as an administrator	24
My Approvals	25
Introduction to approvals	25
My Approvals page	25


Approving campaign results	26
Collaborators	28
Introduction to Collaborators	28
Collaborators page	28
Managing collaborators	30
Adding additional collaborators	30
Adding additional Azure AD work account collaborators	31
Editing roles	32
Removing collaborators	32
About us	34
Contacting us	34
Technical support resources	34

Access Certification

Introduction to Access Certification

Accessible from the Starling site (<https://www.cloud.oneidentity.com/>), this service is used for uploading data from One Identity Safeguard for Privileged Passwords (which is connected to Access Certification using One Identity Hybrid Subscription) in order to run a campaign which allows you to make decisions regarding whether or not the correct permissions are currently in effect.

For example, after uploading the data exported from Safeguard for Privileged Passwords you can run a campaign to find out if the users contained within that data belong within the groups that they are currently assigned. Designated approvers then go through the results from the campaign and either confirm or reject the group membership. Once the campaign has ended and the approvers have gone through the results, the information is then summarized so that appropriate actions can be taken should the data not match the desired group assignments. Additional campaigns can also be run to provide insight into other aspects of the data.

- IMPORTANT:** In order to use Access Certification you need One Identity Safeguard for Privileged Passwords with a valid Hybrid subscription.
- IMPORTANT:** In order to use Access Certification some additional software and hardware requirements must be met. For more information, see [Additional hardware and software requirements](#). You should also review the requirements for Safeguard for Privileged Passwords and One Identity Hybrid Subscription.
- NOTE:** To view the documentation or contact support while using Access Certification or any of the related 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
Internet Explorer	Windows 7	11
Google Chrome	Windows 10 Mac OS X Yosemite	Latest
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 Access Certification using a mobile device

Along with the main Starling portal, Access Certification is compatible with mobile devices. Use the  button at the top of your screen to display the navigation bar options and account information.

Additional hardware and software requirements

Access Certification has additional requirements beyond those necessary for Starling overall (for more information, see the *Starling User Guide*).






Table 3: Access Certification requirements

One IdentitySafeguard for Privileged Passwords with Hybrid subscription (all fully supported versions after 2.5 are eligible to use Access Certification)	See the Safeguard for Privileged Passwords documentation for more information. You will also need to be familiar with the One Identity Safeguard PowerShell scripting resources .
Active Directory domain added to Safeguard for Privileged Passwords	Must include the following: <ul style="list-style-type: none"> User email addresses

ActiveDirectory PowerShell module installed	<ul style="list-style-type: none"> • Users have a manager set • Groups have managedBy set • Users must have been added to Safeguard for Privileged Passwords by adding directory user groups. These directory groups must be used when assigning users to entitlements.
	Remote Server Administration Tools (RSAT) installed and enabled.

Using the Access Certification service

To navigate through the service use the title bar along the top of the site, which contains the following links:

- : 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.
- : This button (displaying the first name of the account owner) opens a drop-down menu that allows you to select one of the following options:
 - **My Services:** Clicking this link takes you to the One Identity Starling home page.
 - **Sign out:** Clicking this link signs you out of One Identity Starling.
- : This button opens a dialog displaying notifications.
- : This button opens the Access Certification [documentation site](#).
- : This button opens the **Settings** page where you can manage your entire Starling account. For information on these settings, see the *Starling User Guide*.

The main pages available within Access Certification are listed in the navigation bar, which is located directly beneath the title bar:



- **Campaigns:** This is the home page of Access Certification and provides access to your campaigns.
- **Data:** The [Data Imports](#) page is where you upload Safeguard for Privileged Passwords data so that it can be used in a campaign. You must upload data before you can run a campaign.
- **Collaborators:** This page is used to manage the administrators and approvers within you Access Certification service.

- **My Approvals:** This page is visible to approvers and provides them access to the campaigns that have been run that need to be reviewed. Users that are only assigned the approver role will only have access to this page within Access Certification. Administrators that are not also assigned the approver role will not have access to this page.

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. From the Starling home page, click the  button associated with the service to which you want to invite a new administrator.
2. Select **Invite Administrator**.
3. 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 menu 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.

Ending a service preview

When you no longer want access to a service available for preview, you can remove the service from your organization and delete all data associated with it. You must be an administrator to remove a service from an organization.

To end a service preview

⚠ CAUTION: The Access Certification technical preview is concluding, so new subscriptions are no longer available. Ending a preview will permanently delete all data associated with that service and Access Certification cannot be resubscribed to.

1. Sign in to Starling.
2. From the home page, locate the service you want to stop previewing and click the  button associated with it.
3. Click **End Preview**.
4. On the warning dialog, click **OK** to end the preview and delete all data associated with the service.

Data Imports

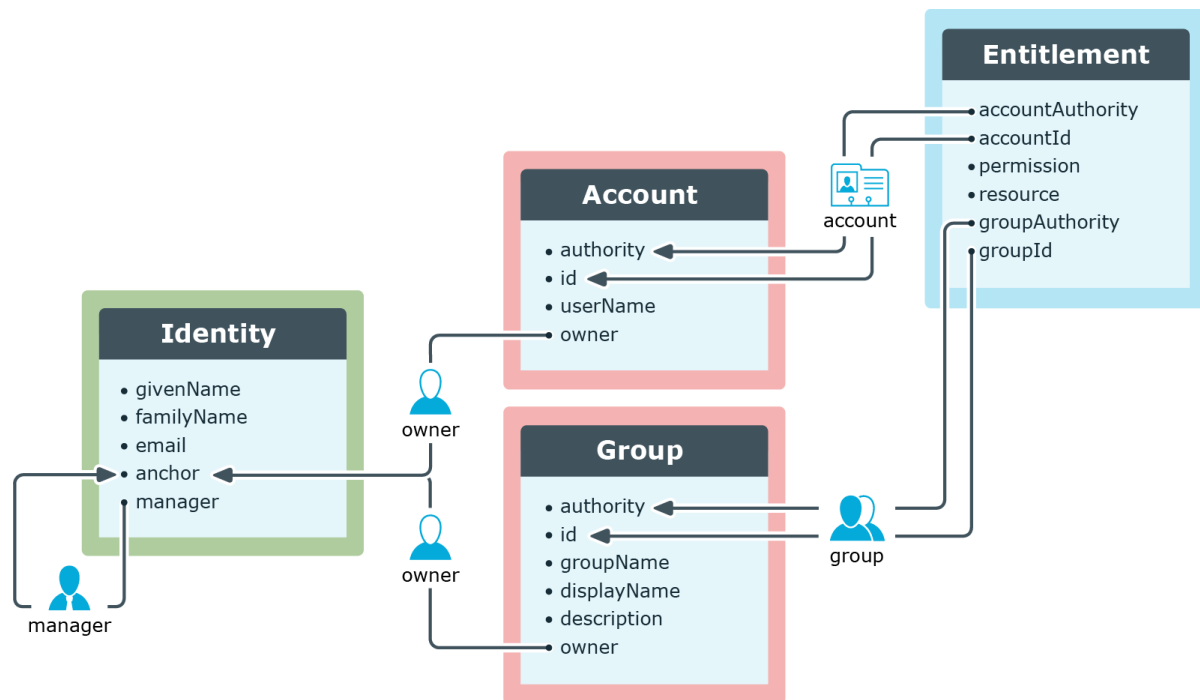
Introduction to importing data

⚠ CAUTION: Make sure you save a copy of the original Safeguard for Privileged Passwords CSV files before making edits to the files or uploading them to Access Certification. This is in case an edit to a CSV file leads to an unintended recommended change within Safeguard for Privileged Passwords. The unedited file can be compared to a newer version in order to identify where the data was changed and if it needs to be corrected.

In order to run a campaign in Access Certification, the data that will be analyzed must first be uploaded. This is done via the [Data Imports page](#) which is accessed by selecting **Data** in the navigation bar.

The Safeguard for Privileged Passwords data that is used by Access Certification fits the following structure:

Figure 1: Structure of CSV data



Data Imports page

CAUTION: Make sure you save a copy of the original Safeguard for Privileged Passwords CSV files before making edits to the files or uploading them to Access Certification. This is in case an edit to a CSV file leads to an unintended recommended change within Safeguard for Privileged Passwords. The unedited file can be compared to a newer version in order to identify where the data was changed and if it needs to be corrected.

The **Data Imports** page is displayed by clicking **Data** in the navigation bar. The **Data Imports** page is used for uploading data to Access Certification in order to run a campaign.

The following appears on this page:

Identity Data

When uploading identity data from Safeguard for Privileged Passwords, the information is coming from the local identity provider (Active Directory) for which Safeguard for Privileged Passwords is the authority and corresponds with the users that have access to Safeguard for Privileged Passwords. It does not include data for disabled Safeguard for Privileged Passwords users, but it does include both Local and Certificate accounts. For information on the specific fields within the CSV file, see [Identity data](#).

Clicking the **Upload Identity Data** button on this tile opens a dialog from which you can select the CSV file associated with the identity data you want uploaded in to Access Certification. Once a new file has been successfully uploaded, the tile will update to display the total number of uploaded identities and the date they were last updated.

Account Data

When uploading account data from Safeguard for Privileged Passwords, the information is coming from the local identity provider (Active Directory) for which Safeguard for Privileged Passwords is the authority. It does not include data for disabled Safeguard for Privileged Passwords users. For information on the specific fields within the CSV file, see [Account data](#).

Clicking the **Upload Account Data** button on this tile opens a dialog from which you can select the CSV file associated with the account data you want uploaded in to Access Certification. Once a new file has been successfully uploaded, the tile will update to display the total number of uploaded accounts and the date they were last updated.

Group Data

The group data being used is that which corresponds with the groupings of Safeguard for Privileged Passwords users for the purpose of assigning entitlements. Because the data is specific to Safeguard for Privileged Passwords and how it manages users, the information might not be mapped to external identity providers. For information on the specific fields within the CSV file, see [Group data](#).

Clicking the **Upload Group Data** button on this tile opens a dialog from which you can select the CSV file associated with the group data you want uploaded in to Access Certification. Once a new file has been successfully uploaded, the tile will update to display the total number of uploaded groups and the date they were last updated.

Entitlement Data

Entitlements are groupings of Safeguard for Privileged Passwords access policies and require that the Accounts and Groups data must first be gathered. This is because both accounts (users within Safeguard for Privileged Passwords) and groups can be added to entitlements. Each entitlement may contain zero or more access policies. However, an individual access policy may only be part of one entitlement. The reason for this is so that changing one access policy does not unintentionally modify a separate entitlement that the administrator may not realize is related. For information on the specific fields within the CSV file, see [Entitlement data](#).

Clicking the **Upload Entitlement Data** button on this tile opens a dialog from which you can select the CSV file associated with the entitlement data you want uploaded in to Access Certification. Once a new file has been successfully uploaded, the tile will update to display the total number of uploaded entitlements and the date they were last updated.

Once you have generated CSV files for each of these data types ([Generating CSV files from Safeguard for Privileged Passwords](#)), you can begin uploading the files using this page ([Uploading data](#)).

Identity data

CAUTION: Make sure you save a copy of the original Safeguard for Privileged Passwords CSV files before making edits to the files or uploading them to Access Certification. This is in case an edit to a CSV file leads to an unintended recommended change within Safeguard for Privileged Passwords. The unedited file can be compared to a newer version in order to identify where the data was changed and if it needs to be corrected.

When uploading identity data from Safeguard for Privileged Passwords, the information is coming from the local identity provider (Active Directory for which Safeguard for Privileged Passwords is the authority and corresponds with the users that have access to Safeguard for Privileged Passwords. It does not include data for disabled Safeguard for Privileged Passwords users, but it does include both Local and Certificate accounts.

The following are descriptions of the fields within the identities CSV file:

NOTE: If any additional columns are included in the identities CSV file, they will be created as identity attributes in the graph.

- `givenName`: A given name (or first name in most western languages)
- `familyName`: A family name (or last name in most western languages)
- `email`: An email address for the identity. The value must be unique for all rows within the identities CSV file.
- `anchor`: This is the anchor attribute that is referenced by the accounts CSV and groups CSV files. It specifies which accounts and groups are owned by this identity (also referenced by the `manager` field). The value must be unique for all rows within the identities CSV file.
- `manager`: This attribute is used to correlate two rows within the identities CSV file. When specifying a manager, set the `manager` value to the `anchor` value of the manager's identity. We recommend that you always include this data, but it is optional for campaigns where the manager is not the approver.

Account data

⚠ CAUTION: Make sure you save a copy of the original Safeguard for Privileged Passwords CSV files before making edits to the files or uploading them to Access Certification. This is in case an edit to a CSV file leads to an unintended recommended change within Safeguard for Privileged Passwords. The unedited file can be compared to a newer version in order to identify where the data was changed and if it needs to be corrected.

When uploading account data from Safeguard for Privileged Passwords, the information is coming from the local identity provider (Active Directory) for which Safeguard for Privileged Passwords is the authority. It does not include data for disabled Safeguard for Privileged Passwords users.

The following are descriptions of the fields within the accounts CSV file:

- **authority:** The authority for the account. This is the system of origin for the account. This column is used to specify whether the account is a local account or external account. The authority value consists of an authority type and the authority realmId separated by a colon.
- **id:** An immutable identifier for the account. Some authorities may use the same value for id and userName, but this might also be an integer value or GUID value.
- **userName:** The user's account name.
- **owner:** Set to the anchor value from a corresponding row in the identities CSV file. This attribute is used to correlate a row of the accounts CSV file to a row in the identities CSV file in order to designate which identity this account belongs to. To correlate an account with an owner, set owner value to the anchor value of the account owner's identity.

Group data

⚠ CAUTION: Make sure you save a copy of the original Safeguard for Privileged Passwords CSV files before making edits to the files or uploading them to Access Certification. This is in case an edit to a CSV file leads to an unintended recommended change within Safeguard for Privileged Passwords. The unedited file can be compared to a newer version in order to identify where the data was changed and if it needs to be corrected.

The group data being used is that which corresponds with the groupings of Safeguard for Privileged Passwords users for the purpose of assigning entitlements. Because the data is specific to Safeguard for Privileged Passwords and how it manages users, the information might not be mapped to external identity providers.

The following are descriptions of the fields within the groups CSV file:

- ❗ **NOTE:** If any additional columns are included in the groups CSV file, they will be created as group attributes in the graph.
- ❗ **NOTE:** Rows having the same `authority` and `id` are considered duplicates. On import, one will overwrite the other.
 - `authority`: The authority for the account. This is the system of origin for the group (that is the system that records the actual group membership). This column is used to specify whether the group is a local group or external group. The `authority` value consists of an authority type and the authority realmId separated by a colon.
 - `id`: An immutable identifier for the group. Some authorities may use the same value for `id` and `groupName`, but this might also be an integer value or GUID value.
 - `groupName`: The system name for the group.
 - `displayName`: (Optional) The display name for the group.
 - `description`: (Optional) Description of the group which should summarize the purpose of the group.
 - `owner`: Set to the `anchor` value from a corresponding row in the identities CSV file. This attribute is used to correlate a row of the groups CSV file to a row in the identities CSV file in order to designate which identity owns this group. To specify a group owner, set `owner` value to the `anchor` value of the group owner's identity.

Entitlement data

⚠ **CAUTION:** Make sure you save a copy of the original Safeguard for Privileged Passwords CSV files before making edits to the files or uploading them to Access Certification. This is in case an edit to a CSV file leads to an unintended recommended change within Safeguard for Privileged Passwords. The unedited file can be compared to a newer version in order to identify where the data was changed and if it needs to be corrected.

Entitlements are groupings of Safeguard for Privileged Passwords access policies and require that the [Account data](#) and [Group data](#) must first be gathered. This is because both accounts (users within Safeguard for Privileged Passwords) and groups can be added to entitlements. Each entitlement may contain zero or more access policies. However, an individual access policy may only be part of one entitlement. The reason for this is so that changing one access policy does not unintentionally modify a separate entitlement that the administrator may not realize is related.

The entitlements CSV file is a representation of the following sentence:

<account> has <permission> on <resource> because of <group>

The following are descriptions of the fields within the entitlements CSV file:

- `accountAuthority`: See `accountId`.
- `accountId`: Together, `accountAuthority` and `accountId` should match a corresponding row in the accounts CSV file.
- `permission`: Human readable description of the permission.
- `resource`: Human readable identifier for the resource.
- `groupAuthority`: See `groupId`.
- `groupId`: Together, `groupAuthority` and `groupId` should match a corresponding row in the groups CSV file.

Generating CSV files from Safeguard for Privileged Passwords

Before you are able to upload data to Access Certification, you must generate a CSV file from Safeguard containing that data. For information on the types of data being uploaded, see [Data Imports page](#).

To generate CSV files from Safeguard for Privileged Passwords

⚠ CAUTION: Make sure you save a copy of the original Safeguard for Privileged Passwords CSV files before making edits to the files or uploading them to Access Certification. This is in case an edit to a CSV file leads to an unintended recommended change within Safeguard for Privileged Passwords. The unedited file can be compared to a newer version in order to identify where the data was changed and if it needs to be corrected.

📘 IMPORTANT: Before generating CSV files, review the [Additional hardware and software requirements](#) information.

📘 NOTE: It is recommended that you review [this diagram](#) before making any edits to the CSV files.

1. Run PowerShell as an administrator.
2. For instructions and information on connecting, see [One Identity Safeguard PowerShell scripting resources](#). You should be using the `PowerShell module` marked *current version* which contains the Access Certification cmdlet.

📘 NOTE: For verification that you are running the correct module version use `Get-InstallModule`.

3. Once you have connected to the Safeguard Appliance (see the Getting Started instructions on the [One Identity Safeguard PowerShell scripting resources](#) page), run the following cmdlet to create all of the required CSV files:

```
Get-SafeguardAccessCertificationAll
```


4. When prompted, enter your Active Directory credentials.
5. Once you have completed generating all CSV files, review the files to ensure the data is both complete and accurate. If you find rows that are incomplete and unnecessary, delete the corresponding row.

NOTE: The cmdlet simplifies the CSV file creation process by allowing you to run a single cmdlet that calls six cmdlets in order to create the required CSV files. You should still ensure the following columns are correct since the information contained in them needs to match the other CSV files:

- Email
- Anchor
- Manager

6. Once you have finished generating and reviewing the CSV files, you'll need to upload them to Access Certification. For more information, see [Uploading data](#).

Generating CSV files individually

As a backup option, Access Certification allows you to run each cmdlet individually rather than all together.

To generate CSV files individually from Safeguard for Privileged Passwords

CAUTION: Make sure you save a copy of the original Safeguard for Privileged Passwords CSV files before making edits to the files or uploading them to Access Certification. This is in case an edit to a CSV file leads to an unintended recommended change within Safeguard for Privileged Passwords. The unedited file can be compared to a newer version in order to identify where the data was changed and if it needs to be corrected.

IMPORTANT: Before generating CSV files, review the [Additional hardware and software requirements](#) information.

NOTE: It is recommended that you review [this diagram](#) before making any edits to the CSV files.

1. Run PowerShell as an administrator.
2. For instructions and information on connecting, see [One Identity Safeguard PowerShell scripting resources](#). You should be using the [PowerShell module](#) marked *current version* which contains the Access Certification cmdlets.

NOTE: For verification that you are running the correct module version use `Get-InstallModule`.

3. Once you have connected to the Safeguard Appliance (see the Getting Started instructions on the [One Identity Safeguard PowerShell scripting resources](#) page), run the following cmdlet to create an identities CSV file for Active Directory identities:

Get-ADAccessCertificationIdentity

4. Run the following cmdlet to create an identities CSV file for Safeguard for Privileged Passwords identities:

Get-SafeguardAccessCertificationIdentity

5. The information from the Active Directory and Safeguard identity CSV files need to be merged so that all information is contained within a single file. This will need to be done manually to ensure the correct information is appearing for every identity.

NOTE: Ensure the following columns are correct since the information contained in them needs to match the other CSV files:

- Email
- Anchor
- Manager

6. Run the following cmdlet to create an accounts CSV file:

Get-SafeguardAccessCertificationAccount

7. Run the following cmdlets to process user groups:

a. Get-SafeguardAccessCertificationGroup

b. Update-SafeguardAccessCertificationGroupFromAD -<csv path from step 7a>

8. Run the following cmdlet to process Safeguard for Privileged Passwords entitlements:

Get-SafeguardAccessCertificationEntitlement

9. Once you have completed generating all CSV files, review the files to ensure the data is both complete and accurate. If you find rows that are incomplete and unnecessary, delete the corresponding row.
10. Once you have finished generating and reviewing the CSV files, you'll need to upload them to Access Certification. For more information, see [Uploading data](#).

Uploading data

In order to run a campaign within Access Certification you must first import the data that will be analyzed as a CSV file. For information on generating the required CSV files, see [Generating CSV files from Safeguard for Privileged Passwords](#).

To upload data

CAUTION: Make sure you save a copy of the original Safeguard for Privileged Passwords CSV files before making edits to the files or uploading them to Access Certification. This is in case an edit to a CSV file leads to an unintended recommended change within Safeguard for Privileged Passwords. The unedited file can be compared to a newer version in order to identify where the data was changed and if it needs to be corrected.

IMPORTANT: Importing data will remove all previous data and replace it with the latest uploaded file.

IMPORTANT: Each CSV file cannot have more than 1000 rows.

1. On the navigation bar, click **Data**.
2. On the **Data Imports** page, click the upload data button associated with the type of data you will be uploading via CSV file. This opens a dialog where you can select the file that is to be uploaded. The following types of data are allowed: [Entitlement data](#), [Account data](#), [Group data](#), and [Identity data](#). For more information on these data types, see [Data Imports page](#).
3. In the dialog, locate and select the CSV file that will be uploaded.
4. Click the **Open** button to begin the upload.

Once the upload has successfully completed, the associated tile will update the item count to include the newly uploaded data as being available.

NOTE: Should the selected CSV file not meet the requirements for upload, information regarding why the upload failed will appear on the tile.

5. Continue uploading CSV files until all four data types have been uploaded. Once finished you can run a campaign on the uploaded data. For more information, see [Introduction to campaigns](#).

Campaigns

Introduction to campaigns

Campaigns in Access Certification are what allow you to understand and use data that has been uploaded. This is done by basing campaigns around answering a straightforward question that approvers are then able to make decisions on without having to locate and analyze the data themselves.

An example question that Access Certification uses for a campaign: Should <identity> be a member of the <group name> group. Access Certification then uses the uploaded [Identity data](#), [Entitlement data](#), [Group data](#), and [Account data](#) to fill in the question so that an approver can go through all possible data that fits the question and therefore needs to be answered. Once a campaign has been completed, the decisions made can be used to ensure the correct groups are being assigned to the correct users.

Campaigns page

The **Campaigns** page is displayed when Access Certification is first opened by administrators and is accessible by clicking **Campaigns** in the navigation bar.

The following options appear on this page:

New Campaign

Clicking this button opens the **New Campaign** dialog so you can add a new campaign to your Access Certification service. For more information, see [Adding a new campaign](#).

Search

The search box is used to locate a specific campaign within the **Campaign** table. To use the field, start typing the name or owner of the campaign in the field and the table will automatically update to display users that match.

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

Name

This displays the name of the campaign.

Owner

This displays the name of the account that created the campaign.

Managing campaigns

The following sections provide information on managing campaigns for Access Certification.

- [Adding a new campaign](#)
- [Running a campaign](#)
- [Duplicating a campaign](#)
- [Editing a campaign](#)
- [Closing a campaign](#)
- [Viewing a campaign as an administrator](#)

Adding a new campaign

The following procedure explains how to add a new campaign.

To add a new campaign

1. On the **Campaigns** page, to add a new campaign use one of the following options:
 - If there are no existing campaigns, click the **Create a new campaign** button.
 - If you have existing campaigns, click the **New Campaign** button.
2. In the **Name** field, enter a name for the campaign.
3. Click **Next** to save the campaign and close the dialog.

After closing the dialog you will be redirected to the **Scope** tab for the campaign.
4. On the **Scope** tab, select one of the following tiles which summarizes the question that will be answered by running the campaign.
 - **Group Membership:** Should <account> be a member of the <group name> group?
 - **Group Granted Entitlements:** Should the <group name> group grant <entitlement>?

The **Scope** tab will update to allow you to configure the specifics of the campaign. If necessary, you can use **Change Campaign Type** to change your selected question.

5. Depending on the question selected, an **Options** tile will be available for selecting whether **Managers** (default) or **Group Owners** will be certifying the campaign.
6. (Optional) Open the **Settings** tab to view and edit the name of the campaign and designate a different campaign support contact. By default, the email address of the person creating the campaign is used as the support contact.
7. (Optional) Open the **What if** tab to view information regarding the impact of running the campaign. This page will also list any errors that may have been found in the data which need to be addressed before you are able to run the campaign.
8. Once you have completed adding a new campaign, see [Running a campaign](#).

Running a campaign

The following procedure explains how to run a campaign once you have completed [Uploading data](#) and [Adding a new campaign](#).

To run a campaign

1. On the **Campaigns** page, click the name of the campaign that you want to run.
2. On the campaign's information pages, click **Run Campaign**.

NOTE: If there are any errors that have been found in the data that need to be addressed before you are able to run the campaign, you will be unable to click this button. If that occurs, check the **What if** tab which provides information on the errors currently preventing the campaign from running.

3. On the **Run Campaign** dialog, click the **Campaign Close** field and select an end date for the campaign. The campaign does not automatically close on this date. Instead, this date is used as a guideline for approvers to know when they should complete their work and allows administrators to determine if the campaign has been fully completed before locking the results. For information on manually closing a campaign, see [Closing a campaign](#).
4. Click **Run, start sending invites** to start the campaign.

The first time a campaign is run, a new **Results** tab will appear on the campaign's information pages listing the start date of the campaign and approvers will see the campaign listed on their **My Approvals** page. Each time the campaign has been run the **Results** tab will update to display information for each campaign run.

Approvers will also receive an email letting them know that a campaign has been run for which they have pending approval work. A Starling invitation will also be sent to new approvers that have been identified as having approval work for the campaign. For information on the approval portion of the campaign, see [Approving campaign results](#).

Duplicating a campaign

The following procedure explains how to duplicate an existing campaign.

To duplicate a campaign

1. On the **Campaigns** page, click the name of the campaign to duplicate.
2. On the campaign's information pages, open the **Actions** drop-down.
3. Select **Duplicate Campaign**.
4. After making any desired changes to the campaign name, click **Create Campaign**.
The duplicated campaign will now appear listed on the Campaigns page.

Editing a campaign

The following procedure explains how to edit an existing campaign.

To edit a campaign

- !** **IMPORTANT:** Edits made will not impact campaigns that have already completed or are currently running.
1. On the **Campaign** page, click the name of the campaign to edit.
 2. On the campaign's information pages, make any required edits to the campaign. All changes will be automatically saved and will apply the next time the campaign is run.

Closing a campaign

The following procedure explains how to close a campaign. Campaigns must always be closed manually.

To close a campaign

1. On the **Campaigns** page, click the name of an active campaign that you want to close.
2. On the campaign's information pages, click **View Active Campaign**.
3. Click **Close Campaign**.
4. Click **OK**.

The campaign will no longer be available for approvals, however the information and work related to the campaign will still be available. Administrators can view this information on the **Results** tab. For more information, see [Viewing a campaign as an administrator](#).

Viewing a campaign as an administrator

The following procedure explains how to view information on a campaign that has been run or is currently in progress.

To view a campaign

NOTE: There may be a delay before certification information is available.

1. On the **Campaigns** page, click the name of the campaign that you want to view.
2. Open the **Results** tab.
3. All runs of the campaign will be listed on the tab. Click the **View** link associated with the run you are interested in viewing.

A dialog will open with a summary of the approvals (**Certifications** tab) and the campaign (**Details** tab). From the **Details** tab, you can also download reports:

- **Remediation Report:** This report lists the certifications that should be remediated since the approver rejected them during the approval process.
- **Full Audit Report:** This report lists all certifications from the campaign.

My Approvals

Introduction to approvals

Once a campaign has begun, the process of deciding whether or not the current Safeguard for Privileged Passwords permissions are correctly configured begins. This is done by approvers that the data identifies as being best suited to answer the question due to their own relationship to the data being reviewed.

For example, say you run a campaign asking this question: Should <account> be a member of the <group name> group. Access Certification then uses the uploaded [Identity data](#) to fill in the question so that you get a list of all possible data that fits the question and therefore needs to be answered. Approvers (in this example either managers or group owners) go through their list of questions and answer each of them based on whether or not the listed account should in fact be a member of the listed group. These answers can then be used to improve Safeguard for Privileged Passwords since permissions marked as rejected mean the account should be removed as a member of that group.

My Approvals page

The **My Approvals** page is located in the navigation bar for approvers. The **My Approvals** page is used for approving or rejecting the results of a campaign that has been run.

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

Campaign Name

This displays the name of the campaign for which you are an approver.

Start

This column displays the date the campaign was run on.

Close

Once a campaign has ended, the close date will be listed in this column and you will be unable to access the campaign. Administrators are responsible for closing campaigns ([Closing a campaign](#)).

Clicking one of the active campaigns opens that campaign's approval page. The following information and options appear on this page:

<Campaign name>

At the top of the page is the name of the campaign and the total number of items to review as a result of the campaign being run.

Complete the following approvals by <date>

This shows the date that all approvals should be completed by for the campaign. After this date the campaign will close and no changes can be made.

<nn> Approvals Remaining

This displays the total number of items left to be reviewed. The percentage of work completed appears below.

View Completed Work/View Work Queue

These links switch the view to display either the items that an approver has already reviewed (Completed Work Queue) or the items that have not yet been reviewed (Work Queue, which is displayed by default).

Each item identified during the campaign as requiring approval is displayed as a tile in the Work Queue. For each tile, click either the **Reject** or **Approve** button to indicate whether or not the permission is appropriate. Once you have made a selection, the tile will be moved to the Completed Work Queue where you can view completed items and edit them if necessary. If you need more information about the data behind the approval request, click on the tile to open an additional information pane. For information on reviewing items, see [Approving campaign results](#).

Approving campaign results

Approvers will receive an email letting them know when they have approvals related to a campaign that was run. The following procedure explains how to approve or reject the results of a campaign.

To approve results for a campaign

1. On the **My Approvals** page, click the name of the active campaign that you want to review.
2. On the campaign's information pages, the approvals to be completed are displayed as tiles. For each tile, click either the **Reject** or **Approve** button to indicate whether or not the permission is appropriate. If you need more information about the data behind this approval request, click on the tile to open an additional information pane.

After you have selected whether or not to approve, the item is moved to the **Completed Work Queue**. So long as the campaign is active, you can change your approval decision by clicking the **View Completed Work** link and selecting **Rejected** or **Approved** for the item. Clicking **Move to Queue** for an item removes any previous decision for an item and returns the item to the work queue (click **View Work Queue** to switch the view back to the list of remaining approvals).

Collaborators

Introduction to Collaborators

Access Certification allows users to add collaborators to their service (as administrators, approvers, or both) based on the type of access required for the user. Adding additional collaborators is optional and can be done at any time using the [Collaborators page](#).

The following roles are available for your collaborators:

- **Administrator:** This role allows you access to the configuration pages within Access Certification service. There must always be at least one administrator associated with the account.
- **Approver:** This role allows you access to the **My Approvals** page of the Access Certification service. Specifically, collaborators that are assigned only the approver role will only have access to the information and pages required to respond to certification requests. All other pages within Access Certification will be hidden from approvers unless they are also assigned the administrator role.

Collaborators page

The **Collaborators** page is displayed when **Collaborators** is clicked in the navigation bar. The **Collaborators** page is used for adding and managing the collaborators currently associated with the Access Certification service.

Collaborators assigned the approver role are also added automatically as a result of running a campaign that requires a specific approver be added.

The following options appear on this page:

Invite Collaborator

This opens the **Invite Collaborator** dialog so you can add new collaborators to your Access Certification service. For more information, see [Adding additional collaborators](#) or [Adding additional Azure AD work account collaborators](#).

Show

Use this drop-down menu to display collaborators based on role. The available options are: **All Roles**, **Administrator**, and **Approver**.



The search box 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.

Roles


This displays the role (or roles) currently assigned to the collaborator.

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 editing the roles for the collaborator and removing collaborators from the account. For more information, see [Editing roles](#) and [Removing collaborators](#).

- NOTE:** You are unable to remove yourself as a collaborator, and if you are an administrator for the account 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 Access Certification service.



- [Adding additional collaborators](#)
- [Adding additional Azure AD work account collaborators](#)
- [Editing roles](#)
- [Removing collaborators](#)


Adding additional collaborators

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

To add additional collaborators

1. On the **Collaborators** page, 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. In the **Collaborator Roles** section, select the check box associated with the roles that will be assigned to the new collaborator (at least one role must be assigned):
 - **Administrator:** This role allows you access to the configuration pages within Access Certification service. There must always be at least one administrator associated with the account.
 - **Approver:** This role allows you access to the **My Approvals** page of the Access Certification service. Specifically, collaborators that are assigned only the approver role will only have access to the information and pages required to respond to certification requests. All other pages within Access Certification will be hidden from approvers unless they are also assigned the administrator role.
4. Click **Invite**.
5. 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 that they now have access to your organization's Access Certification 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 using the  button in the title bar.

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 an Azure AD account, see [Adding additional collaborators](#).

To add additional Azure AD work account collaborators


1. On the **Collaborators** page, 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. In the **Collaborator Roles** section, select the check box associated with the roles that will be assigned to the new collaborator (at least one role must be assigned):
 - **Administrator:** This role allows you access to the configuration pages within Access Certification service. There must always be at least one administrator associated with the account.
 - **Approver:** This role allows you access to the **My Approvals** page of the Access Certification service. Specifically, collaborators that are assigned only the approver role will only have access to the information and pages required to respond to certification requests. All other pages within Access Certification will be hidden from approvers unless they are also assigned the administrator role.
5. Click **Invite**.
6. 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 that they now have access to your organization's Access Certification service.

- NOTE:** Administrators and collaborators associated with multiple organizations can switch between Starling subscriptions once they have logged in using the  button in the title bar.

Editing roles

The following procedure explains how to edit a collaborator's assigned roles.


To edit roles for a collaborator

- NOTE:** It can take up to 15 minutes for changes to take effect for currently logged in users.
1. On the **Collaborators** page, locate the collaborator whose roles you want to edit. You can use the **Search for collaborators** field at the top of the page to filter the listed collaborators.
 2. Once you have located the collaborator to edit, click the  button.
 3. Select the **Edit Roles** option.
 4. In the **Collaborator Roles** dialog, select the check box associated with the roles that will be assigned to the collaborator (at least one role must be assigned):
 - **Administrator:** This role allows you access to the configuration pages within Access Certification service. There must always be at least one administrator associated with the account.
 - **Approver:** This role allows you access to the **My Approvals** page of the Access Certification service. Specifically, collaborators that are assigned only the approver role will only have access to the information and pages required to respond to certification requests. All other pages within Access Certification will be hidden from approvers unless they are also assigned the administrator role.
- NOTE:** If you are an administrator for the account 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.
5. Click **Save** to save your changes and return to the Collaborators page.

Removing collaborators

If a collaborator is no longer needed, you can remove their access to the Access Certification service.

To remove collaborators

1. On the **Collaborators** page, 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 the **Remove Collaborator** option.
 - ① **NOTE:** You are unable to remove yourself as a collaborator, and if you are an administrator for the account 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 your subscription of Access Certification.

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 or other inquiries, visit <https://www.oneidentity.com/company/contact-us.aspx> or call +1-800-306-9329.

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