One Identity Starling CertAccess

Demo Trial Guide

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 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.**

Starling CertAccess Demo Trial Guide
Updated - 06 October 2021, 09:23

Contents

1

Starling CertAccess demo trials

Starling CertAccess can be subscribed for a limited period to test the product before you make a longer term commitment to using it. Use a Demo Trial to find out how the main functions in Starling CertAccess work. With this, you can try out all the functions using a standard set of sample data, without needing to connect Starling CertAccess to your own One Identity Active Roles installation. A Demo Trial is time-limited to five days, but if you need more time, you can start your trial again before the trial subscription ends.

With a demo trial, you can test different use cases. The following use cases are described here step-by-step:

- Scenario 1: A default user would like to request the **Purchase Analysis** Active Directory group.
- Scenario 2: An attestation supervisor would like to attest a membership in the **Purchase Analysis** Active Directory group. The attestation is granted approval.
- Scenario 3: An attestation supervisor would like to attest a membership in the **Sales Analyst** Active Directory group. The attestation is denied approval.
- Scenario 4: A Starling CertAccess administrator would like to assign managers to identities.
- Scenario 5: A Starling CertAccess administrator would like to assign product owners to system entitlements.
- Scenario 6: A default user would like to claim ownership of the **Cert Publishers** Active Directory group.

> TIP: If you want to go a step further and try Starling CertAccess with data from your own One Identity Active Roles installation, you can request a Proof of Concept trial. This will allow you to trial Starling CertAccess Web Portal functions and also let you see how data is synchronized between your own Active Roles and Starling CertAccess. You will see the product performing exactly how it would with a fully-paid subscription with no restrictions. For more information about the Proof of Concept Trial, see the *One Identity Starling CertAccess Administration Guide for One Identity Active Roles Integration*.

Available documentation

The online version of Starling CertAccess documentation is available in the Support portal under Starling CertAccess online documentation.

Starting a Demo Trial

If you have started a trial subscription and the your trial instance for the Demo Trial is already available, you can start your Demo Trial. For more information about starting a trial subscription, see the *One Identity Starling CertAccess Administration Guide for One Identity Active Roles Integration*.

You can use sample data to test different use cases. There are five identities available to you with which you can log in on the Starling CertAccess Web Portal. For more information, see Identities on page 7.

To start a Demo Trial

1. In the **Your Starling CertAccess subscription is ready** email, click the **Get Started** button.

   This opens the Starling CertAccess website.

   Here you will see the user names of all the identities that you can use for the trial.
2. Next to the identity you want to use to log in on the Starling CertAccess Web Portal, click **Copy**.

   This copies the identity's login name to the clipboard.
3. On the **CertAccess Portal** tile, click **GO**.

   This opens the Starling CertAccess Web Portal's login page.
4. Insert the user name in the **User** field.
5. Switch to the Starling CertAccess website.
6. On the **Demo Trial** tile, click **Copy**.

   This copies the password for logging in on the Starling CertAccess Web Portal to the clipboard.
7. Switch to the Starling CertAccess Web Portal's login page.
8. Insert the password in the **Password** field.
9. Click **Log in**.

   This opens the Starling CertAccess Web Portal's home page.

Related topics

- Ending a Demo Trial on page 5

Ending a Demo Trial

A Demo Trial is time-limited to five days, You can end your Demo Trial at any time within its trial period (30 days) and restart it again.

To end a Demo Trial early

1. In the **Trial Details** section on the Starling CertAccess website, click the **End Trial** button.
2. Click **OK**.

Related topics

- Starting a Demo Trial on page 5

Use cases and identities

The sample data provides you with different identities that you can use to log in on the Starling CertAccess Web Portal and test different use cases (see Identities on page 7). The following use cases are described here.

> NOTE: Some processes that are triggered in the use cases may take a long time (for example, adding attestation cases after starting attestation). Actions that depend on these processes are not available immediately. If an action is not available, wait for a while and reload the page.

Use cases

- Scenario 1: A default user would like to request the **Purchase Analysis** Active Directory group.
- Scenario 2: An attestation supervisor would like to attest a membership in the **Purchase Analysis** Active Directory group. The attestation is granted approval.
- Scenario 3: An attestation supervisor would like to attest a membership in the **Sales Analyst** Active Directory group. The attestation is denied approval.
- Scenario 4: A Starling CertAccess administrator would like to assign managers to identities.
- Scenario 5: A Starling CertAccess administrator would like to assign product owners to system entitlements.
- Scenario 6: A default user would like to claim ownership of the **Cert Publishers** Active Directory group.

Detailed information about this topic

- Identities on page 7
- Scenario 1: Request membership in an Active Directory group on page 8
- Scenario 2: Attesting a group membership with approval granted on page 10
- Scenario 3: Attesting a group membership with approval denied on page 12
- Scenario 4: Assigning a manager to identities on page 14

- Scenario 5: Assigning product owners to system entitlements on page 15
- Scenario 6: Claim ownership of a system entitlement on page 16

Identities

You can use the following identities in the use cases described.

Celestine Eaton

- User name: CELESTINEAT
- Role: Starling CertAccess administrator
- Tasks:
    - Monitor requests and attestation cases
    - Monitor data in the Data Explorer
    - Edit memberships in application roles

Tony Denison

- User name: TONYDEN
- Role: Manager
- Tasks: Approve access requests (request for group memberships) for Tomas Grenier

Tomas Grenier

- User name: TOMASGRE
- Role: Default user
- Tasks: Requests memberships in the following Active Directory groups
    - Accounts payable
    - Enterprise Contract Administrators
    - Expense Manager
    - Marketing Operations
    - Purchase Analysis
    - Sales Analyst
    - Supplier Qualification

Dorreen Palacek

- User name: DORREENPAL
- Role: Product owner of system entitlements

- Tasks: Approves access requests for the following Active Directory groups
  - Accounts payable
  - Enterprise Contract Administrators
  - Expense Manager
  - Marketing Operations
  - Purchase Analysis
  - Sales Analyst
  - Supplier Qualification

Quentin Payton

- User name: QUENTINPAY
- Role: Attestation supervisor
- Tasks: Carries out attestations

Related topics

- Use cases and identities on page 6

Scenario 1: Request membership in an Active Directory group

A default user wants to request membership in the **Purchase Analysis** Active Directory group themselves. The request undergoes an approval procedure. The request is granted approval by the default user's manager and by the owner of the group (product owner). Once the request has been granted approval, the default user's Active Directory user account becomes a member of the requested group. The Starling CertAccess administrator can then verify whether the default user's user account has been assigned to the group.

Identities managed in Starling CertAccess can use requests to apply for access permissions in the connected Active Directory environment. All requests undergo an approval procedure in which approvers grant or deny the requests. In the request history, you can always trace who placed or approved which access requests.

> TIP: If an action is not available yet, it means that a background process is running such as, finding the next approver. Wait for a while and reload the page.

To request the Purchase Analysis Active Directory group

1. Log in on the Starling CertAccess Web Portal as **TOMASGRE**.
2. Request the **Purchase Analysis** Active Directory group.

   a. In the menu bar, click **Requests** > **New Request**.

   b. On the **New Request** page, on the **Purchase Analysis** tile, click **Add to cart**.

   c. On the **Shopping Cart** page, click **Submit**.

   This runs a peer group analysis.

   Tony Denison, Tomas Grenier's manager, is determined to be an approver.

3. Sign out as **TOMASGRE**.
4. Log in as **TONYDEN**.

   A pending requests needs to be approved.

5. Approve the request.

   a. In the menu bar, click **Requests** > **Pending Requests**.

   b. On the **Pending Requests** page, next to the **Purchase Analysis** request, click **Approve**.

   c. In the **Approve Request** pane, click **Save**.

   Dorreen Palacek, the group's owner, is determined to be an approver.

6. Sign out as **TONYDEN**.
7. Log in as **DORREENPAL**.

   A pending requests needs to be approved.

8. Approve the request.

   a. In the menu bar, click **Requests** > **Pending Requests**.

   b. On the **Pending Requests** page, next to the **Purchase Analysis** request, click **Approve**.

   c. In the **Approve Request** pane, click **Save**.

   This finalizes the request approval and adds the membership to the group.

9. Sign out as **DORREENPAL**.
10. Log in as **CELESTINEAT**.
11. In the Data Explorer, check whether the user account has been assigned to the group.

    a. In the menu bar, click **Data** > **Data Explorer**.

    b. In the Data Explorer in the navigation, click **System entitlements**.

    c. In the **Search** field, enter **Purchase Analysis**.

    d. In the list, click **Purchase Analysis**.

    e. In the details pane, click the **Memberships** tab.

    f. On the **Memberships** tab, check whether or not the **Grenier, Tomas (TOMASGRE)** identity's user account is listed as a member.

Related topics

- Identities on page 7
- Scenario 2: Attesting a group membership with approval granted on page 10
- Scenario 3: Attesting a group membership with approval denied on page 12
- Scenario 4: Assigning a manager to identities on page 14
- Scenario 5: Assigning product owners to system entitlements on page 15
- Scenario 6: Claim ownership of a system entitlement on page 16

Scenario 2: Attesting a group membership with approval granted

An attestation supervisor would like to have a membership in the **Purchase Analysis** Active Directory group attested. Membership should be granted. The attestation case is assigned to the member's manager and the owner of the group and confirmed. The Starling CertAccess administrator can then verify whether the user account continues to be a member of the group.

Attestation functionality allows the correctness of various data to be certified. Attestations are run either regularly or they can be triggered explicitly by attestation supervisors. Once attestation starts, attestation cases are created that contain all the necessary information about the attestation objects and the attestor. The attestor checks the attestation objects. They verify the correctness of the data and initiate any changes that need to be made if the data conflicts with internal rules. Attestation cases record the entire attestation sequence. Each attestation step in the attestation case can be audit-proof reconstructed.

> TIP: If an action is not available yet, it means that a background process is running such as, finding the next attestor. Wait for a while and reload the page.

Prerequisite

- Scenario 1 was completed successfully (see Scenario 1: Request membership in an Active Directory group on page 8). Tomas Grenier is a member of the **Purchase Analysis** group.

To attest a membership in an Active Directory group

1. Log in on the Starling CertAccess Web Portal as **QUENTINPAY**.
2. Start the attestation.

    a. In the menu bar, click **Attestation** > **Attestation Policies**.

    b. On the **Attestation Policies** page, next to the **System entitlement membership attestation (peer group analysis)** attestation policy, click ⋮ (**actions**) > **Start attestation**.

   c. In the details pane, next to **TomasGre - Purchase Analysis**, click **Start attestation**.

   Tony Denison, Tomas Grenier's manager, is determined to be an attestor.

3. Sign out as **QUENTINPAY**.
4. Log in as **TONYDEN**.

   A pending attestation needs to be approved.

5. Approve the attestation.

   a. In the menu bar, click **Attestation** > **Pending Attestations**.

   b. On the **Pending Attestations** page, next to the **Should the identity "Grenier, Tomas (TOMASGRE)" have access to the "Purchase Analysis" system entitlement using the "TomasGre" user account?** attestation case, click **Approve**.

   c. In the **Approve** pane, click **Save**.

   Dorreen Palacek, the group's owner, is determined to be an attestor.

6. Sign out as **TONYDEN**.
7. Log in as **DORREENPAL**.

   A pending attestation needs to be approved.

8. Approve the attestation.

   a. In the menu bar, click **Attestation** > **Pending Attestations**.

   b. On the **Pending Attestations** page, next to the **Should the identity "Grenier, Tomas (TOMASGRE)" have access to the "Purchase Analysis" system entitlement using the "TomasGre" user account?** attestation case, click **Approve**.

   c. In the **Approve** pane, click **Save**.

   This finalizes the attestation case and confirms the group membership.

9. Sign out as **DORREENPAL**.
10. Log in as **CELESTINEAT**.
11. In the Data Explorer, check that the user account is still assigned to the group.

    a. In the menu bar, click **Data** > **Data Explorer**.

    b. In the Data Explorer in the navigation, click **System entitlements**.

    c. In the **Search** field, enter **Purchase Analysis**.

    d. In the list, click **Purchase Analysis**.

    e. In the details pane, click the **Memberships** tab.

    f. On the **Memberships** tab, check whether or not the **Grenier, Tomas (TOMASGRE)** identity's user account is listed as a member.

Related topics

- Identities on page 7
- Scenario 1: Request membership in an Active Directory group on page 8
- Scenario 3: Attesting a group membership with approval denied on page 12
- Scenario 4: Assigning a manager to identities on page 14
- Scenario 5: Assigning product owners to system entitlements on page 15
- Scenario 6: Claim ownership of a system entitlement on page 16

Scenario 3: Attesting a group membership with approval denied

An attestation supervisor would like to have a membership in the **Sales Analyst** Active Directory group attested. Membership should be denied. The attestation case is assigned to the member's manager and the owner of the group. An attestor denies the existing group membership and the user account's assignment is automatically removed from the group. The Starling CertAccess administrator can then verify whether the group membership has really been removed.

Attestation functionality allows the correctness of various data to be certified. Attestations are run either regularly or they can be triggered explicitly by attestation supervisors. Once attestation starts, attestation cases are created that contain all the necessary information about the attestation objects and the attestor. The attestor checks the attestation objects. They verify the correctness of the data and initiate any changes that need to be made if the data conflicts with internal rules. Attestation cases record the entire attestation sequence. Each attestation step in the attestation case can be audit-proof reconstructed.

> TIP: If an action is not available yet, it means that a background process is running such as, finding the next attestor. Wait for a while and reload the page.

Prerequisite

- Run scenario 1 for the **Sales Analyst** group (see Scenario 1: Request membership in an Active Directory group on page 8).
- Tomas Grenier is then a member of the **Sales analyst** group.

To attest membership in an Active Directory and to deny that attestation

1. Log in on the Starling CertAccess Web Portal as **QUENTINPAY**.
2. Start the attestation.
   a. In the menu bar, click **Attestation** > **Attestation Policies**.
   b. On the **Attestation Policies** page, next to the **System entitlement membership attestation (peer group analysis)** attestation policy, click ⋮

(**actions**) > **Start attestation**.

c. In the details pane, next to **TomasGre - Sales Analyst**, click **Start attestation**.

Tony Denison, Tomas Grenier's manager, is determined to be an attestor.

3. Sign out as **QUENTINPAY**.
4. Log in as **TONYDEN**.

   A pending attestation needs to be approved.
5. Approve the attestation.
   a. In the menu bar, click **Attestation** > **Pending Attestations**.
   b. On the **Pending Attestations** page, next to the **Should the identity "Grenier, Tomas (TOMASGRE)" have access to the "Sales Analyst" system entitlement using the "TomasGre" user account?** attestation case, click **Approve**.
   c. In the **Approve** pane, click **Save**.

   Dorreen Palacek, the group's owner, is determined to be an attestor.
6. Sign out as **TONYDEN**.
7. Log in as **DORREENPAL**.

   A pending attestation needs to be approved.
8. Deny the attestation.
   a. In the menu bar, click **Attestation** > **Pending Attestations**.
   b. On the **Pending Attestations** page, next to the **Should the identity "Grenier, Tomas (TOMASGRE)" have access to the "Sales Analyst" system entitlement using the "TomasGre" user account?** attestation case, click **Deny**.
   c. In the **Deny** pane, click **Save**.

   This finalizes denial of the attestation case. The group membership is automatically removed.
9. Sign out as **DORREENPAL**.
10. Log in as **CELESTINEAT**.
11. In the Data Explorer, check that the group membership has been removed.
    a. In the menu bar, click **Data** > **Data Explorer**.
    b. In the Data Explorer in the navigation, click **System entitlements**.
    c. In the **Search** field, enter **Sales Analyst**.
    d. In the list, click **Sales analyst**.
    e. In the details pane, click the **Memberships** tab.
    f. On the **Memberships** tab, check whether or not the **Grenier, Tomas (TOMASGRE)** identity's user account is listed as a member.

Related topics

- Identities on page 7
- Scenario 1: Request membership in an Active Directory group on page 8
- Scenario 2: Attesting a group membership with approval granted on page 10
- Scenario 4: Assigning a manager to identities on page 14
- Scenario 5: Assigning product owners to system entitlements on page 15
- Scenario 6: Claim ownership of a system entitlement on page 16

Scenario 4: Assigning a manager to identities

A Starling CertAccess administrator wants to display all the identities that do not have a manager assigned to them. The Starling CertAccess administrator wants to assign a manager to one of these Identities.

To assign a manager to an identity

1. Log in on the Starling CertAccess Web Portal as **CELESTINEAT**.
2. In the Data Explorer, display all the identities that do not have a manger and assign a manager to one of them.
   a. In the menu bar, click **Data** > **Data Explorer**.
   b. In the Data Explorer, click ⚠ **Issues found**.
   c. On the **Data Readiness** page, next to **Identities**, click **View**.
   d. In the list, click the identity that you want to assign a manager to.
   e. In the details pane, in the **Manager** menu, click the manager you want to assign to the identity.
   f. Click **Save**.

Related topics

- Identities on page 7
- Scenario 1: Request membership in an Active Directory group on page 8
- Scenario 2: Attesting a group membership with approval granted on page 10
- Scenario 3: Attesting a group membership with approval denied on page 12
- Scenario 5: Assigning product owners to system entitlements on page 15
- Scenario 6: Claim ownership of a system entitlement on page 16

Scenario 5: Assigning product owners to system entitlements

A Starling CertAccess administrator wants to display all the system entitlements that do not have a product owner assigned to them. The Starling CertAccess administrator wants to assign a product owner to one of these system entitlements. The Starling CertAccess can select an identity or all members of an application role as the product owner.

TIP: For example, product owners might be used as approvers for requests.

To assign a product owner to a system entitlement

1. Log in on the Starling CertAccess Web Portal as **CELESTINEAT**.
2. In the Data Explorer, display all the system entitlements that do not have a product owner and assign a product owner to one of them.

    a. In the menu bar, click **Data** > **Data Explorer**.

    b. In the Data Explorer, click ⚠ **Issues found**.

    c. On the **Data Readiness** page, next to **System entitlements**, click **View**.

    d. In the list, click the system entitlement that you want to assign a product owner to.

    e. In the details pane, click the **Service Item** tab.

    f. On the **Service Item** tab, perform one of the following actions:

    - To specify members of an application role as the product owner, enable the **Select from roles** option, next to the **Product owner** field, click **Assign**/**Change** and select the appropriate application role.
    - To specify an identity as the product owner, enable the **Select from identities** option and then select the corresponding identity in the **Identity** menu.

    g. Click **Save service item**.

Related topics

- Identities on page 7
- Scenario 1: Request membership in an Active Directory group on page 8
- Scenario 2: Attesting a group membership with approval granted on page 10
- Scenario 3: Attesting a group membership with approval denied on page 12
- Scenario 4: Assigning a manager to identities on page 14
- Scenario 6: Claim ownership of a system entitlement on page 16

Scenario 6: Claim ownership of a system entitlement

A default user would like to claim ownership of the **Cert Publishers** Active Directory group. This enters the default user as the product owner of this group who can, for example, make approval decisions about requests in this group or attest memberships in the group. In the context of an attestation, the default user confirms themselves that this assignment is correct.

> TIP: If an action is not available yet, it means that a background process is running such as adding the attestation case. Wait for a while and reload the page.

To claim ownership of the Cert Publishers Active Directory group.

1. Log in on the Starling CertAccess Web Portal as **TOMASGRE**.
2. Assign a product owner.

   a. In the menu bar, click **Responsibilities** > **Assign Ownership**.

   b. On the **Assign an Owner for a System Entitlement** page, in the **System entitlement** menu, click **Cert Publishers**.

   c. Click **Next**.

   d. In the second step, click **I want to take ownership of this system entitlement**.

   e. Click **Next**.

   This creates an attestation case, in which Tomas Grenier confirms the correctness of the assignment.
3. Confirm that Tomas Grenier really wants to claim ownership.

   a. In the menu bar, click **Attestation** > **Pending Attestations**.

   b. On the **Pending Attestations** page, next to the **Who is the correct owner for the "Cert Publishers" system entitlement?** attestation case click **Approve**.

   c. In the **Approve** pane, click **Save**.

   Tomas Grenier is assigned as product owner.

Related topics

- Identities on page 7
- Scenario 1: Request membership in an Active Directory group on page 8
- Scenario 2: Attesting a group membership with approval granted on page 10
- Scenario 3: Attesting a group membership with approval denied on page 12
- Scenario 4: Assigning a manager to identities on page 14
- Scenario 5: Assigning product owners to system entitlements on page 15

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

Index