One Identity Manager 9.2

# Administration Guide for Behavior Driven Governance

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/trademark-information.aspx. 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.**

One Identity Manager Administration Guide for Behavior Driven Governance
Updated - 02 October 2023, 10:31

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

# Contents

1

# Overview of Behavior Driven Governance

Behavior Driven Governance allows IT administrators and those responsible for compliance to administer entitlements on the basis of usage behavior. This allows entitlements that are no longer needed to be identified and removed. Regular checks and recertification of these entitlements ensure that only entitlements that are really required are always assigned. One Identity Manager provides various default policies and processes for Behavior Driven Governance.

## OneLogin integration

If OneLogin Cloud Directory data is synchronized with One Identity Manager, access to OneLogin applications can be recertified and managed depending on usage behavior. Data from the OneLogin change history is used to do this. There are default policies available for the following tasks:

- Find access to OneLogin application access that has not been used for a specified period of time
- Find OneLogin applications that have not been used by anyone for a specified period of time
- Find OneLogin applications that are assigned to more than OneLogin role.
- Find OneLogin roles that ensure access to more than one OneLogin application

Unused applications can be removed automatically if configured accordingly.

## Integration with other Unified Namespace target systems

If there are target systems mapped in the Unified Namespace, administrators can use a default company policy to determine all the user accounts that have not been used for a specified amount of time. They can use this information to verify and correct target system access permissions. This can reduce the security risks associated with unused but enabled user accounts. The prerequisite being that these target systems provide information about the how long the user accounts were in use and that this data is synchronized.

## Required modules

Behavior Driven Governance can be used if the following modules are installed:

- Company Policies Module
- Attestation Module
- Target System Base Module
- OneLogin Module

## Detailed information about this topic

- Behavior Driven Governance for OneLogin on page 6
- Behavior Driven Governance for target systems in the Unified Namespace on page 19

# Behavior Driven Governance for OneLogin

NOTE: This functionality is only available if the OneLogin Module in installed.

One Identity Manager provides various company policies and attestation policies to test and recertify or remove access to OneLogin applications depending on usage patterns. This means the following scenarios can be handled:

- Access to OneLogin applications that are not used

  OneLogin users should use the applications assigned to them at least once within the given time period. If, according to its application history, an application has not been used, the application assignment to the OneLogin user account should be recertified or deleted.

  A company policy finds all unused access to OneLogin applications. Exception approvers are informed about the applications and user accounts involved. At the same time, a recertification process is launched. During the recertification process, users and their managers or target system managers clarify whether the applications are still required. If not, access to unused applications can be subsequently removed, automatically or manually.

- OneLogin applications that are not used by anyone

  Applications should be used at least once by at least on OneLogin user within the given time period. If, according to its application history, an application has not been used, the application assignments to the OneLogin user account should be recertified or deleted.

  A company policy finds all unused OneLogin applications. Exception approvers are informed about the affected applications. Recertification can be used to clarify whether the applications are still needed. Access to unused applications can be subsequently removed, automatically or manually.

- Non-unique assignment of OneLogin application to OneLogin roles

  Access of OneLogin users to applications is controlled by roles. If access is to be removed, the assignment of OneLogin roles to user accounts must be removed. So that no other permissions are removed that may still be required, precisely one application can be assigned to the roles. If the assignment of applications to roles is unique, unused access to applications can be removed automatically.

Company policies are used to identify all OneLogin roles that have more than one application assigned to them, as well as all applications that are assigned to more than one role. Exception approvers are informed about the affected roles and applications and can take appropriate action.

The time period after which applications are considered unused is defined in the **TargetSystem | OneLogin | UnusedApplicationThresholdInDays** configuration parameter. The default value is 90 days.

For more information about mapping OneLogin applications, OneLogin user accounts, and OneLogin roles, see the *One Identity Manager Administration Guide for Integration with OneLogin Cloud Directory*.

### Detailed information about this topic

- Identifying unused access to OneLogin applications on page 8
- Identifying unused OneLogin applications on page 11
- Assigning OneLogin applications to OneLogin roles on page 14
- Prerequisites for automatic withdrawal of unused OneLogin applications on page 7

### Related topics

- Behavior Driven Governance for target systems in the Unified Namespace on page 19

## Prerequisites for automatic withdrawal of unused OneLogin applications

In order to automatically remove OneLogin user account access to OneLogin applications, One Identity Manager determines which OneLogin roles were used to assign the applications. If a role found in this way is assigned to just one unused application, the user account membership in this role can be removed. This causes the user account to lose its access to the application. If more than one application is assigned to one OneLogin role, the membership is not automatically deleted to ensure that all the other applications in the role still have their access.

> NOTE: Applications assigned directly to user accounts cannot be removed in One Identity Manager. Direct assignments must be removed manually after attestation is denied in the target system.

### Prerequisites

To find and recertify unused applications, the following requirements must be met:

- The OneLogin change history is synchronized. At least the events with types 5, 6, 7, 8, 11, 22, 29 are synchronized (`event_type_id=5,6,7,8,11,22,29`).

- The **TargetSystem | OneLogin | UnusedApplicationThresholdInDays** configuration parameter is set. This value specifies after how many days without access a OneLogin application is considered to be unused.
- The identities linked to the user accounts must have a manager assigned to them.
- A target system manager must be specified for OneLogin.

To remove access from an unused application automatically, the following requirements must be met:

- OneLogin applications are assigned to user account exclusively via OneLogin roles. Only these assignments can be removed automatically or manually in One Identity Manager.
- Only one OneLogin application is assigned to each OneLogin role.

  > TIP: Use the **OneLogin role(s) control only one OneLogin application** company policy to identify roles with more than one application.

### Detailed information about this topic

- Identifying unused access to OneLogin applications on page 8
- Identifying unused OneLogin applications on page 11
- Assigning OneLogin applications to OneLogin roles on page 14

# Identifying unused access to OneLogin applications

OneLogin users are expected to use the applications assigned to them at least once within the given time span. You can use a default company policy to identify all OneLogin application assignments to user accounts that, according to the change history, have not been used during this period. Exception approvers are informed about the applications and user accounts involved. At the same time, a recertification process is launched. During the recertification process, users and their managers or target system managers clarify whether the applications are still required. If not, access to unused applications can be subsequently removed, automatically or manually.

Assignments are identified as unused when the following conditions apply:

- The assignment is in effect (`OLGUserHasApplication.XIsInEffect=1`).
- The OneLogin user has logged in to OneLogin at least once (`OLGUser.LastLogin`).
- The number of days between the date of the last application login (`OLGEvent.CreatedAt`) and the current date is greater than or equal to the value of the **TargetSystem | OneLogin | UnusedApplicationThresholdInDays** configuration parameter.

  - OR -

There is no application login date for the user account in the change history. Therefore, the user has never used the application.

***To find and recertify unused assignments***

1. (Optional) Configure automatic withdrawal of entitlements.

   Depending on the method used to assign OneLogin user accounts to OneLogin roles (directly, via IT Shop request, through hierarchical roles or system roles), different configuration parameters must be set. For more information about this, see the *One Identity Manager Attestation Administration Guide*.

2. (Optional) Check whether policy violation notifications and attestation notifications are set up in the attestation case.

   For more information, see the *One Identity Manager Company Policies Administration Guide* and the *One Identity Manager Attestation Administration Guide*.

3. (Optional) Assign identities to the **Identity & Access Governance | Company policies | Exception approvers** application role if they are to be informed about unused OneLogin applications. These identities are allowed to approve exceptions if necessary.

   1. In the Manager, select the **Company Policies > Basic configuration data > Exception approvers** category.
   2. Select the **Assign identities** task.
   3. In the **Add assignments** pane, add identities.

      > TIP: In the **Remove assignments** pane, you can remove assigned identities.
      >
      > ***To remove an assignment***
      >
      > - Select the identity and double-click ✓.

   4. Save the changes.

4. (Optional) To change the recertification period after an application has been identified as unused, in the Web Portal, edit the **Unused OneLogin application access attestation** attestation policy.

   - Edit the **Unused for x days** condition and change the number of days.

   For more information about this, see the *One Identity Manager Web Portal User Guide*.

5. Enable the working copy of the **Access to OneLogin applications is used regularly** company policy.

   1. In the Manager, select the **Company policies > Policies > Working copies of policies > Predefined** category.
   2. Select the working copy in the result list.
   3. Select **Enable working copy**.
   4. Confirm the security prompt with **Yes**.

    5. Enable the original policy. Confirm the prompt with **Yes**.

   This starts the policy check.

   > TIP: If an enabled company policy already exists, you can start the policy check with the **Recalculate policy** task.

   A predefined schedule starts the policy check once a month.

   > NOTE: If you want to prevent new policy violations from being attested immediately, disable **Start attestation for new policy violations immediately**.

6. (Optional) To periodically recertify approved unused assignments, assign an enabled schedule to the **Unused OneLogin application access attestation** attestation policy.

    1. In the Manager, select the **Attestation > Attestation policies > Predefined** category.
    2. Select the attestation policy in the result list.
    3. Select the **Change main data** task.
    4. Select an enabled schedule from the **Calculation schedule** menu.

       - OR -

       Click + to create a new schedule.
    5. Save the changes.

### Procedure

1. In the Manager, verification of the **Access to OneLogin applications is used regularly** company policy is either scheduled or started by the **Recalculate policy** task.

    - It finds all assignments of OneLogin applications to user accounts where the user account has either never logged in or has not logged in within the specified time period.
    - Exception approvers are notified of policy violations via email.

2. If any assignment violates the policy, it is automatically attested with the **Unused OneLogin application access attestation** attestation policy.

   Approval sequence:

    a. Is the user account linked to an identity?

       - If not, the assignment is submitted to the target system managers for attestation.

    b. The linked identity confirms whether the assigned application is required.

    c. The manager of the linked identity decides whether the assignment stays.

    d. If attestation was denied in an approval level, automatic removal of the assignment is reviewed. This finds all OneLogin roles used to assign applications to the user account.

  - If no other applications are assigned to a role, automatic withdrawal of this role is initiated. This removes the assignment of the role to the user account and provisions the change in the target system, thus removing the entitlement for using the application from the OneLogin user.

    With the subsequent synchronization, assignment of the application to the user account is marked as pending or deleted in the One Identity Manager database, depending on the configuration of the synchronization. Run a full target system synchronization to irrevocably delete pending assignments.

e. If the application is assigned directly to the user account or access to multiple applications is granted through a OneLogin role, the attestation case is submitted to the target system managers for final processing.

  - If the target system managers deny attestation, they must ensure that the assignments are removed manually.

If the manager or target system managers have approved the attestation, the assignment stays. If the assignment is again found to be unused during the subsequent scheduled or manual check, it is resubmitted to the attestors for review.

### Related topics

- Behavior Driven Governance for OneLogin on page 6
- Prerequisites for automatic withdrawal of unused OneLogin applications on page 7
- Identifying unused OneLogin applications on page 11
- Assigning OneLogin applications to OneLogin roles on page 14

# Identifying unused OneLogin applications

Applications should be used at least once by at least one OneLogin user within the given time span. You can use a default company policy to identify all OneLogin applications that, according to the change history, have not been used during this time. Exception approvers are informed about the affected applications. Recertification can be used to clarify whether the applications are still needed. This means that users and their managers or target system managers discuss whether the applications are still required. If not, access to unused applications can be subsequently removed, automatically or manually. Default policies must be enabled and configured to meet company requirements.

Applications are identified as unused when the following conditions apply:

- The application is assigned to at least one OneLogin user account (`OLGUserHasOLGApplication`).

- The number of days between the date of the last application login (`OLGEvent.CreatedAt`) and the current date is greater than or equal to the value of the **TargetSystem | OneLogin | UnusedApplicationThresholdInDays** configuration parameter.

  - OR -

  There is no application login date for a user account in the change history. Therefore, the user has not yet used the application.

***To find and recertify unused applications***

1. (Optional) Configure automatic withdrawal of entitlements.

   Depending on the method used to assign OneLogin user accounts to OneLogin roles (directly, via IT Shop request, through hierarchical roles or system roles), different configuration parameters must be set. For more information about this, see the *One Identity Manager Attestation Administration Guide*.

2. (Optional) Check whether policy violation notifications and attestation notifications are set up in the attestation case.

   For more information, see the *One Identity Manager Company Policies Administration Guide* and the *One Identity Manager Attestation Administration Guide*.

3. (Optional) Assign identities to the **Identity & Access Governance | Company policies | Exception approvers** application role if they are to be informed about unused OneLogin applications. These identities are allowed to approve exceptions if necessary.

   1. In the Manager, select the **Company Policies > Basic configuration data > Exception approvers** category.
   2. Select the **Assign identities** task.
   3. In the **Add assignments** pane, add identities.

      > TIP: In the **Remove assignments** pane, you can remove assigned identities.
      >
      > ***To remove an assignment***
      >
      > - Select the identity and double-click ✓.

   4. Save the changes.

4. Enable the working copy of the **Unused OneLogin applications can be removed** company policy

   For more information about this, see the *One Identity Manager Company Policies Administration Guide*.

   1. In the Manager, select the **Company policies > Policies > Working copies of policies > Predefined** category.
   2. Select the working copy in the result list.
   3. Select **Enable working copy**.

   4. Confirm the security prompt with **Yes**.
   5. Enable the original policy. Confirm the prompt with **Yes**.

   This starts the policy check.

   > TIP: If an enabled company policy already exists, you can start the policy check with the **Recalculate policy** task.

   A predefined schedule starts the policy check once a month.

5. In the Web Portal, edit the **Attestation of OneLogin application access** attestation policy.

   For more information about this, see the *One Identity Manager Web Portal User Guide*.

   a. (Optional) To periodically recertify approved unused applications, select an enabled schedule in the **Calculation schedule** field.

   b. Specify which applications require recertifying. In the **Objects to be Attested by this Attestation Policy** pane, add at least one other condition.

   > Example:
   >
   > 1. Select the **Specific applications** condition type and select one of the applications that has been identified as unused by the company policy.
   > 2. Add another condition with the **Unused for x days** condition type and enter the number of days after which the application is identified as unused.
   > 3. Delete the **All applications** condition.

   If you do not add a condition, attestation cases are created for all the OneLogin application assignments to OneLogin user accounts.

   c. Enable the attestation policy

   - Disable the **Disabled** check box.

   d. Save the changes.

## Procedure

1. In the Manager, verification of the **Unused OneLogin applications can be removed** company policy is either scheduled or started by the **Recalculate policy** task.
   - It finds all OneLogin applications where the user account has either not logged in within the specified time period or never logged in.
   - Exception approvers are notified of policy violations via email.
2. In the Web Portal, attestation with the **Attestation of OneLogin application access** is either scheduled or started manually.

It finds all OneLogin application assignments to user accounts according to the configured condition.

Approval sequence:

a. Is the user account linked to an identity?
   - If not, the assignment is submitted to the target system managers for attestation.
b. The linked identity confirms whether the assigned application is required.
c. The manager of the linked identity decides whether the assignment stays.
d. If attestation was denied in an approval level, automatic removal of the assignment is reviewed. This finds all OneLogin roles used to assign applications to the user account.
   - If no other applications are assigned to a role, automatic withdrawal of this role is initiated. This removes the assignment of the role to the user account and provisions the change in the target system, thus removing the entitlement for using the application from the OneLogin user.

     With the subsequent synchronization, assignment of the application to the user account is marked as pending or deleted in the One Identity Manager database, depending on the configuration of the synchronization. Run a full target system synchronization to irrevocably delete pending assignments.
e. If the application is assigned directly to the user account or access to multiple applications is granted through a OneLogin role, the attestation case is submitted to the target system managers for final processing.
   - If the target system managers deny attestation, they must ensure that the assignments are removed manually.

If the manager or target system managers have approved the attestation, the assignment stays and is submitted for recertification again by the next scheduled check.

### Related topics

- Behavior Driven Governance for OneLogin on page 6
- Prerequisites for automatic withdrawal of unused OneLogin applications on page 7
- Identifying unused access to OneLogin applications on page 8
- Assigning OneLogin applications to OneLogin roles on page 14

# Assigning OneLogin applications to OneLogin roles

OneLogin user access to applications is controlled by roles. To be able to manage access to OneLogin applications automatically, only one OneLogin application can be assigned to a

OneLogin role. When this application is no longer needed, its membership in the role can be removed without withdrawing access to other applications at the same time. Similarly, an application should be assigned to only one OneLogin role. If this application is no longer required, you only need to remove membership from the role.

You can use default company policies to verify that whether the requirements for automatic withdrawal of entitlements are met. Exception approvers are informed about the affected roles and applications and can take appropriate action.

### *To identify OneLogin roles with more than one OneLogin application*

1. (Optional) Assign the identities to be informed about the OneLogin roles affected to the **Identity & Access Governance | Company policies | Exception approvers** application role. These are allowed to approve exceptions if necessary.
    1. In the Manager, select the **Company Policies > Basic configuration data > Exception approvers** category.
    2. Select the **Assign identities** task.
    3. In the **Add assignments** pane, add identities.

        > TIP: In the **Remove assignments** pane, you can remove assigned identities.
        >
        > ***To remove an assignment***
        >
        > - Select the identity and double-click ✓.

    4. Save the changes.
2. (Optional) Check whether notifications of policy violations are setup.

    For more information about this, see the *One Identity Manager Company Policies Administration Guide*.
3. Enable the working copy of the **All OneLogin roles control just one OneLogin application** company policy.
    1. In the Manager, select the **Company policies > Policies > Working copies of policies > Predefined** category.
    2. Select the working copy in the result list.
    3. Select **Enable working copy**.
    4. Confirm the security prompt with **Yes**.
    5. Enable the original policy. Confirm the prompt with **Yes**.

    This starts the policy check.

    > TIP: If an enabled company policy already exists, you can start the policy check with the **Recalculate policy** task.

    A predefined schedule starts the policy check once a month.
4. Check all OneLogin roles that violate the policy and correct the assignments to OneLogin applications.

***To identify OneLogin applications with more than one OneLogin role***

1. (Optional) Assign the identities to be informed about the applications affected to the **Identity & Access Governance | Company policies | Exception approvers** application role. These are allowed to approve exceptions if necessary.
   1. In the Manager, select the **Company Policies > Basic configuration data > Exception approvers** category.
   2. Select the **Assign identities** task.
   3. In the **Add assignments** pane, add identities.

      > TIP: In the **Remove assignments** pane, you can remove assigned identities.
      >
      > ***To remove an assignment***
      >
      > - Select the identity and double-click ✓.

   4. Save the changes.
2. (Optional) Check whether notifications of policy violations are setup.

   For more information about this, see the *One Identity Manager Company Policies Administration Guide*.
3. Enable the working copy of the **All OneLogin applications are controlled by just one OneLogin role** company policy.
   1. In the Manager, select the **Company policies > Policies > Working copies of policies > Predefined** category.
   2. Select the working copy in the result list.
   3. Select **Enable working copy**.
   4. Confirm the security prompt with **Yes**.
   5. Enable the original policy. Confirm the prompt with **Yes**.

   This starts the policy check.

   > TIP: If an enabled company policy already exists, you can start the policy check with the **Recalculate policy** task.

   A predefined schedule starts the policy check once a month.
4. Check all OneLogin applications that violate the policy and correct the assignments to OneLogin roles.

## Related topics

- Behavior Driven Governance for OneLogin on page 6
- Prerequisites for automatic withdrawal of unused OneLogin applications on page 7
- Identifying unused access to OneLogin applications on page 8
- Identifying unused OneLogin applications on page 11

3

# Behavior Driven Governance for Privileged Account Management

NOTE: This functionality is only available if the Privileged Account Governance Module in installed.

One Identity Manager provides various company policies and attestation policies to test and recertify, or remove access to entitlements in One Identity Safeguard depending on the usage behavior of its users. This means the following scenarios can be handled:

- PAM user groups that are not used by your users

  Members of user groups can request access within a defined time period. User accounts with no access requests recorded in the PAM audit log, should have their membership in the user group recertified or deleted.

  A company policy determines all the user accounts without access requests. Exception approvers are informed about the user groups and user accounts involved. At the same time, a recertification process is launched. During the recertification process, attestation policy approvers clarify whether the memberships are still required. Memberships that are not required can then be removed automatically or manually.

- Different PAM entitlements that are not used

  PAM entitlements, such as assets, user groups, or permissions, should be used at least once within a defined period of time. If, according to the PAM audit log, an entitlement has not been used during this period, a recertification procedure can be used to determine whether the entitlement is still required.

  Any unused entitlements are determined by various company policies. Exception approvers are informed about the entitlements involved. Recertification can be used to clarify whether the entitlements are still required. Unused entitlements can then be removed from the target system.

The number of days after which entitlements are considered unused is specified in the **TargetSystem | PAG | UnusedUserAccountThresholdInDays** configuration parameter. The default value is 90 days.

For more information about mapping PAM objects, see the *One Identity Manager Administration Guide for Privileged Account Governance*.

### Related topics

- Behavior Driven Governance for target systems in the Unified Namespace on page 19
- Behavior Driven Governance for OneLogin on page 6

4

# Behavior Driven Governance for target systems in the Unified Namespace

One Identity Manager provides company policies to find user accounts that have not been used for a specified period of time. They can use this information to verify and correct target system access permissions. This can reduce the security risks associated with unused but enabled user accounts.

## Prerequisites

- The user accounts are mapped in the Unified Namespace.
- The target systems provide information about how long the user accounts have been in use. This data is synchronized with the One Identity Manager and mapped in `UNSAccount.LastLogon`.

For more information about mapping target systems and user accounts in the Unified Namespace, see the *One Identity Manager Target System Base Module Administration Guide*.

The number of days after which user accounts are considered unused is specified in the **TargetSystem | UNS | UnusedUserAccountThresholdInDays** configuration parameter. The default value is 90 days.

The following scenarios can be handled:

- User accounts that are not used can be disabled

  If users have not logged in to a target system for a specified period of time, their user accounts can be considered to be unused. These user accounts ought be disabled so that logging in is no longer possible.

- User accounts that are not used can be deleted

  User accounts that have not been used to log in to the target system for a specified period of time can be deleted.

Default company policies can be used to find unused user accounts and to inform exception approvers. How to proceed with these user accounts (disabled or delete) depends on the capabilities of the respective target systems. Define target system-specific processes to do this.

### Detailed information about this topic

- Identifying and disabling unused user accounts on page 20
- Identifying and deleting unused user accounts on page 21

### Related topics

- Behavior Driven Governance for OneLogin on page 6

# Identifying and disabling unused user accounts

Whether unused user accounts can be disabled automatically or manually depends on the capabilities of the respective target systems and your company IT policies. Define processes suitable for notifying administrators, managers, or other responsible parties of unused user accounts and disable the affected user accounts.

***To find and disabled unused user accounts***

1. In the Designer, set the **TargetSystem | UNS | UnusedUserAccountThresholdInDays | DaysUntilDisable** and enter the value as the number of days after which unused user accounts should be disabled. The default value is 180 days.
2. (Optional) Assign identities to the **Identity & Access Governance | Company policies | Exception approvers** application role if they are to be informed about the user accounts involved. These are allowed to approve exceptions if necessary.
    1. In the Manager, select the **Company Policies > Basic configuration data > Exception approvers** category.
    2. Select the **Assign identities** task.
    3. In the **Add assignments** pane, add identities.

        > TIP: In the **Remove assignments** pane, you can remove assigned identities.
        >
        > ***To remove an assignment***
        >
        > - Select the identity and double-click ✓.

    4. Save the changes.
3. (Optional) Check whether policy violation notifications are setup.

    For more information about this, see the *One Identity Manager Company Policies Administration Guide*.

4. Enable the working copy of the **Unused user accounts can be disabled**.
    1. In the Manager, select the **Company policies > Policies > Working copies of policies > Predefined** category.
    2. Select the working copy in the result list.
    3. Select **Enable working copy**.
    4. Confirm the security prompt with **Yes**.
    5. Enable the original policy. Confirm the prompt with **Yes**.

    This starts the policy check.

    > TIP: If an enabled company policy already exists, you can start the policy check with the **Recalculate policy** task.

    A predefined schedule starts the policy check once a month.
5. Check all the user accounts that violate the policy and disable them.
    - To automatically disabled unused user accounts, create target system-specific processes that run when new policy violations occur.

### Related topics

- Behavior Driven Governance for target systems in the Unified Namespace on page 19
- Identifying and deleting unused user accounts on page 21

# Identifying and deleting unused user accounts

Whether unused user accounts can be deleted automatically or manually depends on the capabilities of the respective target systems and your company IT policies. Define processes suitable for notifying administrators, managers, or other responsible parties of unused user accounts and delete the affected user accounts.

***To find and delete unused user accounts***

1. In the Designer, set the **TargetSystem | UNS | UnusedUserAccountThresholdInDays | DaysUntilDelete** and enter the value as the number of days after which unused user accounts should be disabled. The default value is 360 days.
2. (Optional) Assign identities to the **Identity & Access Governance | Company policies | Exception approvers** application role if they are to be informed about the user accounts involved. These are allowed to approve exceptions if necessary.
    1. In the Manager, select the **Company Policies > Basic configuration data > Exception approvers** category.
    2. Select the **Assign identities** task.

    3. In the **Add assignments** pane, add identities.

        > TIP: In the **Remove assignments** pane, you can remove assigned identities.
        >
        > ***To remove an assignment***
        >
        > - Select the identity and double-click ✓.

    4. Save the changes.

3. (Optional) Check whether policy violation notifications are setup.

    For more information about this, see the *One Identity Manager Company Policies Administration Guide*.

4. Enable the working copy of the **Unused user accounts can be deleted**.

    1. In the Manager, select the **Company policies > Policies > Working copies of policies > Predefined** category.
    2. Select the working copy in the result list.
    3. Select **Enable working copy**.
    4. Confirm the security prompt with **Yes**.
    5. Enable the original policy. Confirm the prompt with **Yes**.

    This starts the policy check.

    > TIP: If an enabled company policy already exists, you can start the policy check with the **Recalculate policy** task.

    A predefined schedule starts the policy check once a month.

5. Check all the user accounts that violate the policy and delete them.

    - To automatically delete unused user accounts, create target system-specific processes that run when new policy violations occur.

### Related topics

- Behavior Driven Governance for target systems in the Unified Namespace on page 19
- Identifying and disabling unused user accounts on page 20

# Appendix A

# Configuration parameters for behavior driven governance

The following configuration parameters are relevant for behavior driven governance

**Table 1: Overview of configuration parameters for behavior driven governance**

| Configuration parameter | Description |
|---|---|
| TargetSystem \| OneLogin \| UnusedApplicationThresholdInDays | Number of days after which access to OneLogin applications is considered to be unused (default: 90). |
| TargetSystem \| PAG \| UnusedThresholdInDays | Number of days after which a privileged object, entitlement, or user is considered unused (default: 90). |
| TargetSystem \| UNS \| UnusedUserAccountThresholdInDays | Number of days after which a user account is considered to be unused (default: 90). |
| TargetSystem \| UNS \| UnusedUserAccountThresholdInDays \| DaysUntilDelete | Number of days after which an unused user account should be deleted (default: 365). |
| TargetSystem \| UNS \| UnusedUserAccountThresholdInDays \| DaysUntilDisable | Number of days after which an unused user account should be disabled (default: 180). |
| QER \| Attestation \| AutoRemovalScope and all configuration subparameters | General configuration parameter for defining automatic withdrawal of memberships/assignments if attestation approval is not granted. |

# 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