SAP NetWeaver® Identity Management Identity Center

Implementation Guide

- Self-service password reset

Version 7.2 Rev 7

Preface

The product

SAP NetWeaver Identity Center is a high-end identity management solution, capable of handling a large amount of repositories containing an unlimited amount of information. The Identity Center offers a robust, flexible and scalable high-availability solution for workflow, provisioning, data synchronization and joining for a large number of data repositories. The Identity Center provides a framework for a number of jobs.

The reader

This manual is written for people who are to configure and use self-service password reset.

Prerequisites

To get the most benefit from this manual, you should have the following knowledge:

- General knowledge about the SAP NetWeaver Identity Center and job definitions for instance as described in *SAP NetWeaver Identity Management Identity Center Initial Configuration* and *SAP NetWeaver Identity Management Identity Center Tutorial – Basic synchronization.*
- General knowledge about provisioning and task definitions as described in the *SAP NetWeaver Identity Management Identity Center Tutorial – Provisioning*.

The following software is required:

- For setting of the productive password in UME one of the following SAP NetWeaver versions is required:
  - SAP NetWeaver 2004 SP 23+ (means SP 23 and following)
  - SAP NetWeaver 7.0 SP 18+
  - SAP NetWeaver 7.0 Enhancement Package (EHP) 1 SP 2+
  - SAP NetWeaver 7.0 EHP 2 SP 0+
  - SAP NetWeaver Composition Environment (CE) 7.1 SP 7+
  - SAP NetWeaver CE 7.1 EHP 1 SP 1+
  - SAP NetWeaver CE 7.2 SP 0+
  - SAP NetWeaver 7.3 SP 0+
  - SAP NetWeaver 7.3 EHP 1 SP 0+
  - SAP NetWeaver 7.4 SP 0+
- SAP NetWeaver Identity Management Identity Center version 7.2 (or higher), correctly installed and licensed.
- An Identity Center where at least one dispatcher has been configured and is running.
- An identity store with at least one user (in addition to admin user).

- An Identity Management User Interface configured for this Identity Center and identity store according to *SAP NetWeaver Identity Management Identity Center Installing and configuring the Identity Management User Interface.*

The manual

This tutorial consists of six sections describing how you create, configure and run the password reset task. The last section describes how you can create a task used to set the new password for the users and reset the number of failed password reset attempts.

This tutorial is not a substitution for training.

Person names used in this tutorial are fictional.

Related documents

You can find useful information in the following documents:

- *SAP NetWeaver Identity Management Identity Center Initial Configuration.*
- *SAP NetWeaver Identity Management Identity Center Tutorial – Basic synchronization.*
- *SAP NetWeaver Identity Management Identity Center Tutorial – Provisioning.*
- *SAP NetWeaver Identity Management Identity Center Installing and configuring the Identity Management User Interface.*
- Logon screen customization for releases SAP NetWeaver 2004, SAP NetWeaver 7.0, SAP NetWeaver 7.0 EHP 1 and SAP NetWeaver 7.0 EHP 2, see Customizing the Logon Screens on http://help.sap.com/saphelp_nw70ehp2/helpdata/en/23/c0e240beb0702ae10000000a155106/frameset.htm.
- Logon screen customization for releases SAP NetWeaver CE 7.1, SAP NetWeaver CE 7.1 EHP 1, SAP NetWeaver CE 7.2, SAP NetWeaver 7.3 SAP NetWeaver 7.3 EHP 1 and SAP NetWeaver 7.4, see Developing a Custom Logon Screen on http://help.sap.com/saphelp_nw73/helpdata/en/23/c0e240beb0702ae10000000a155106/content.htm.
- Logon Help for SAP NetWeaver Identity Management Implementation Guide available on Help Portal: http://help.sap.com/saphelp_nwidmic_72/helpdata/en/0d/71c8bb0f744c308c7b5e91657ddcbf/frameset.htm.

Table of contents

Introduction

This document describes how to configure and implement self-service password reset in SAP NetWeaver Identity Management 7.2 or higher.

In addition to the solution described in this document, as of SAP NetWeaver Identity Management 7.2 SP8 you can also use the Logon Help to change passwords. For information about this additional solution, see *Logon Help for SAP NetWeaver Identity Management Implementation Guide* available on Help Portal: http://help.sap.com/saphelp_nwidmic_72/helpdata/en/0d/71c8bb0f744c308c7b5e91657ddcbf/frameset.htm.

The password reset process consists of the following three (3) steps:

- Identify: In this step, the user will be asked for the unique identifier, the default is *MSKEYVALUE*. Other options are to ask for another unique attribute (e.g. email address) in addition to or instead of the *MSKEYVALUE*. This is configured on the password reset task in the Identity Center (see section *Setting the password reset parameters* on page 18).
- Verify identity (authenticate): The user answers some question(s) only he/she knows the answer to. It will be possible to define any number of questions on a system, using the attributes on the format *MX_AUTHQ_nnn* (e.g. *MX_AUTHQ_001*, *MX_AUTHQ_002* etc). Five (5) attributes are defined by default, but any implementation may add additional attributes following the naming syntax. A task needs to be created where the user is required to answer a minimum number of these questions, i.e. you can define how many of the defined questions the user has to answer (see section *Setting the password reset parameters* on page 18 and *Section 3: Creating a self-service task for editing of authentication information* on page 22). You can also define a maximum number of login attempts in the identity store configuration.

  Note:
  Every failed attempt of password reset is logged, and a task is executed. For security reasons the user is not told why a password reset attempt failed, if too many attempts are made to reset the password or if the provided unique identifier does not exist, as this would provide a potential attacker with additional information. Instead, the password reset will proceed but random authentication questions may be displayed to the user (including the ones that user has not defined the answers for) and the password reset will fail regardless of the input information being correct or not.
- Set password: A new password is provided to the user, either as input by the user as will be shown in this document (stored in the attribute *MX_PASSWORD*) or system generated. In either case, the password is validated towards the UME (User Management Engine) password policy, and a task is started. This task can then perform any desired operations, e.g. sending the new password to the user via e-mail or SMS, provision the password etc.

  Note:
  If the password is not accepted upon the validation towards the UME password policy, then nothing is written to the database (or the UME) and the user may try to set the password again.

The questions used for password reset authentication are system specific, i.e. all users in the same identity store will have the same questions available and in the same language (the authentication questions are available in several languages). By default, the following questions are given:

- What is your favorite color?
- What make of car do you drive?
- What is your pet's name?

- What is your mother's maiden name?
- What street did you grow up on?

The questions may be changed by altering the display name of attributes *MX_AUTHQ_001* to *MX_AUTHQ_005* (see *Section 5: Changing the authentication questions* on page 33).

Note:
This change of questions should be done during the implementation of the self-service password reset, and it is especially important that this is done before the task allowing the users to enter answers to the authentication questions is available for the users. Changing the questions after the users have provided their answers will cause the answers not to fit well any more.

Preparations

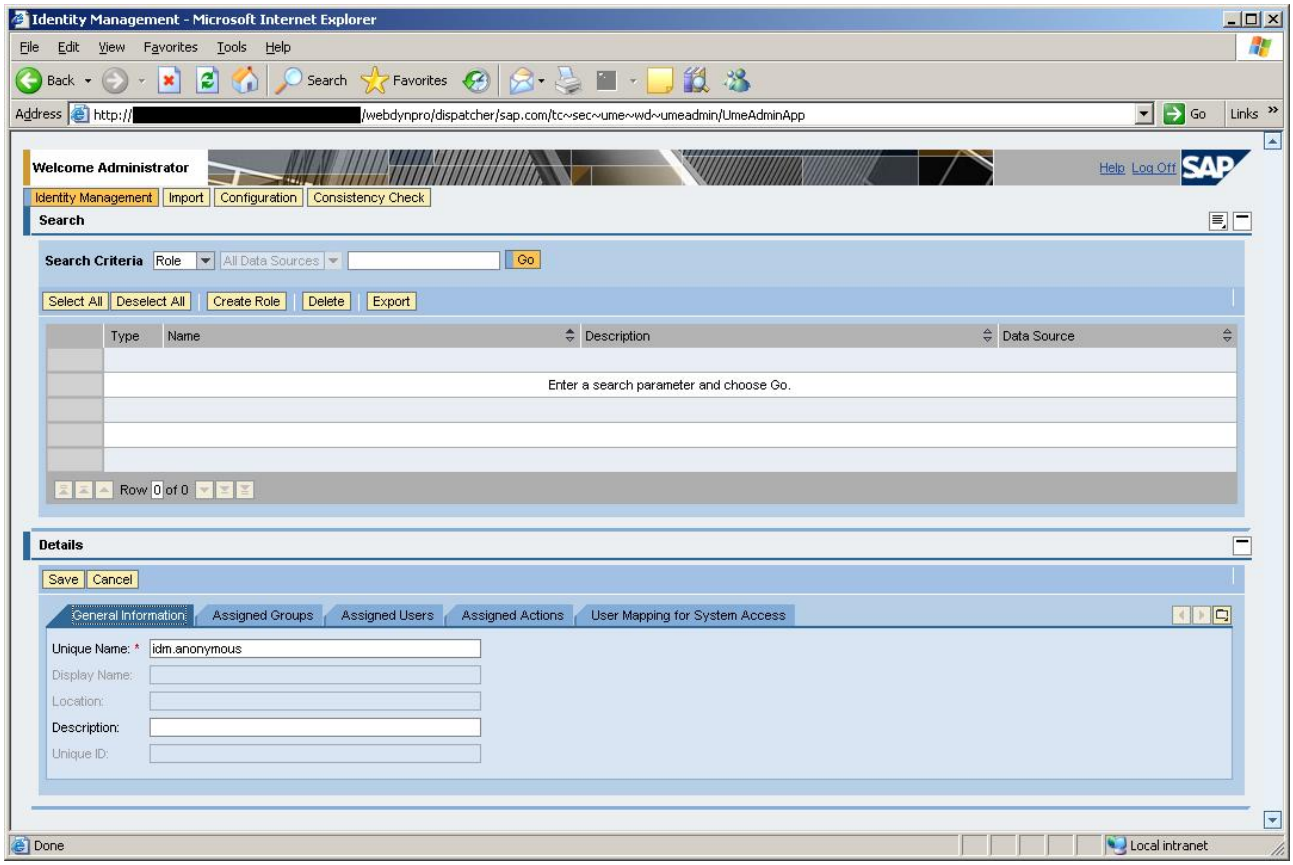
Before configuring the password reset tasks, the following needs to be in place:

- At least one user in the identity store (in addition to the admin user).
- A UME role with action idm_anonymous assigned to group "Anonymous Users" in the User Management Engine (in addition to roles described in the document *SAP NetWeaver Identity Management Identity Center Installing and configuring the Identity Management User Interface*).

To create the UME role "idm.anonymous", do the following:

1. Enter http://<host>:<port>/index.html in your browser. This will open the SAP J2EE Engine Start Page.
2. Select "User Management", which starts the user management administration console for the User Management Engine (UME).
3. Provide your UME credentials and choose "Log on".

4. Change search criteria to "Role", and then choose "Create Role":

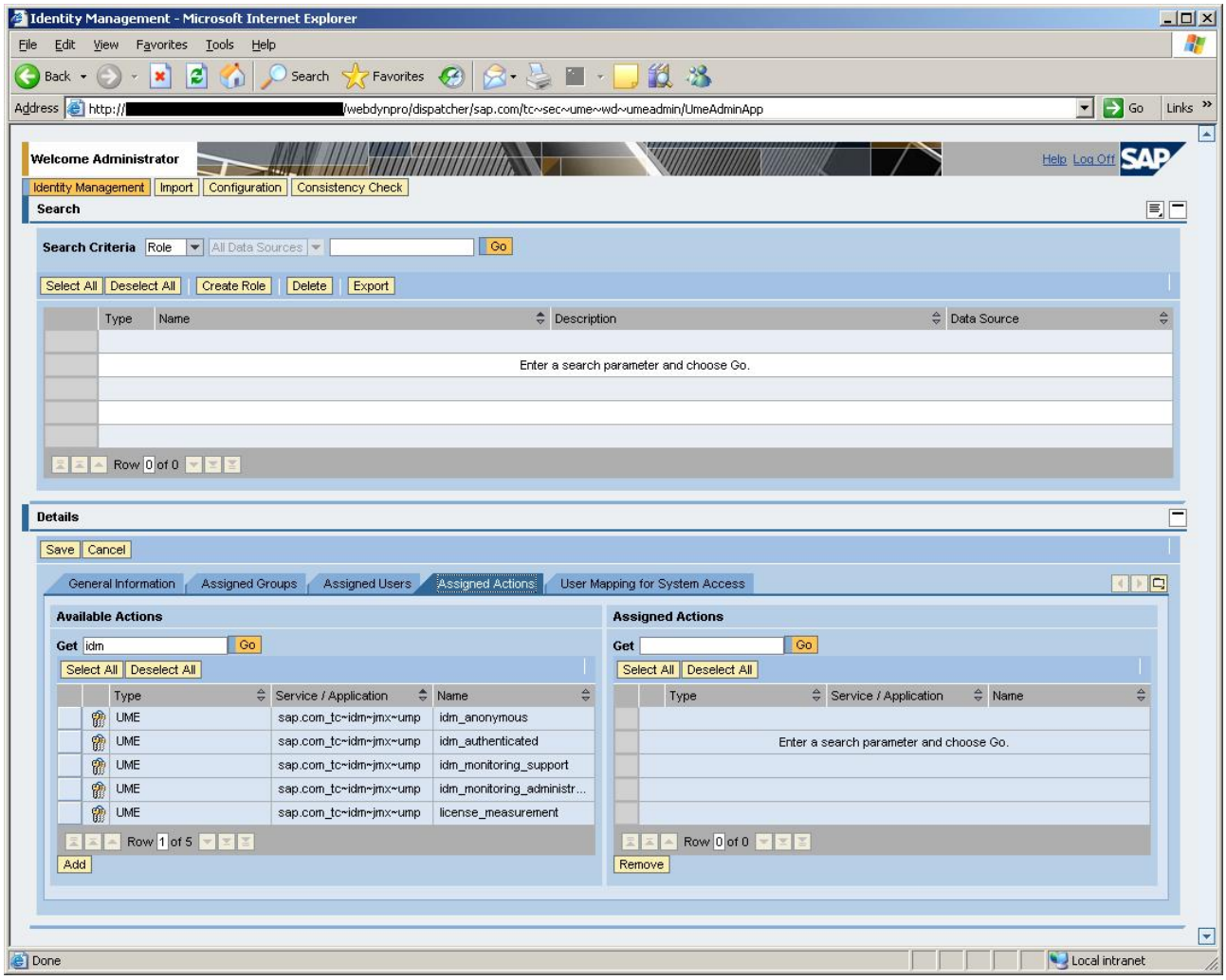


In the "General Information" tab fill in the following:

Unique Name
Give the role a describing name (here "idm.anonymous").

Description
Short description of the role can be added as well. This is not a mandatory field.

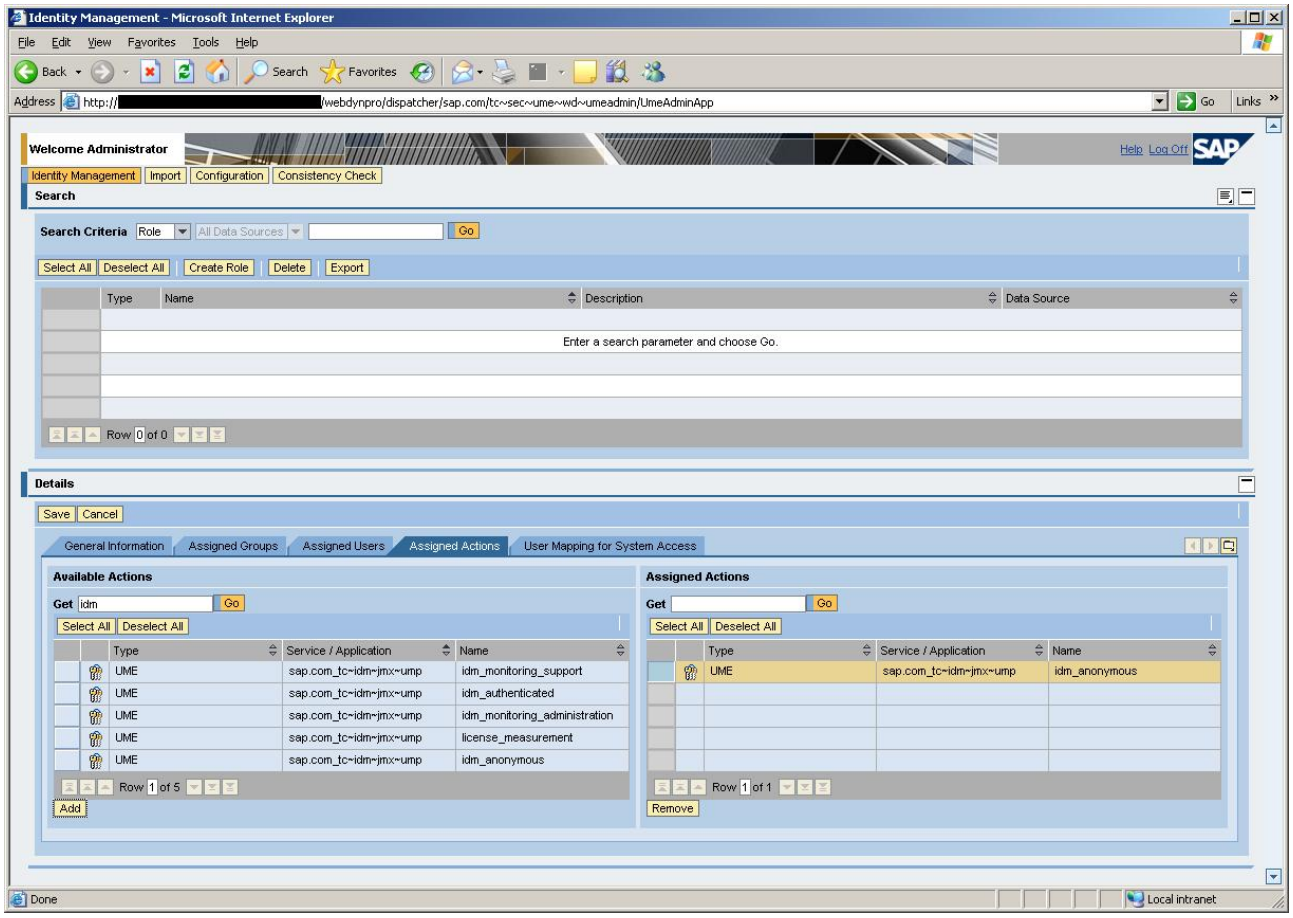
5. Select the "Assigned Actions" tab.



In the left pane (**Available Actions**):

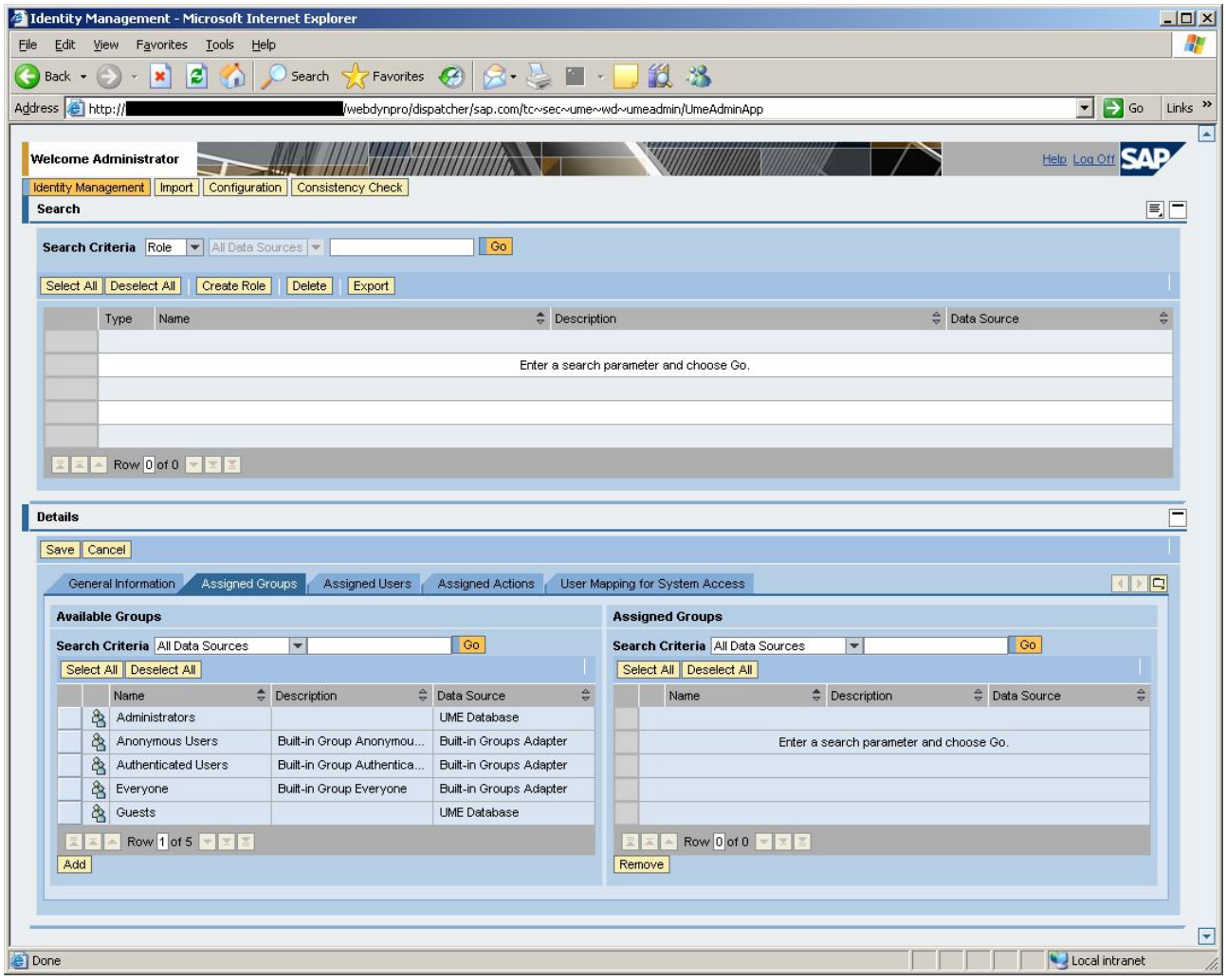
Type " idm*" in the field "Get" and choose "Go". This will list the actions/access rights it is possible to link to the role.

6. Select the "idm_anonymous" action and choose "Add".



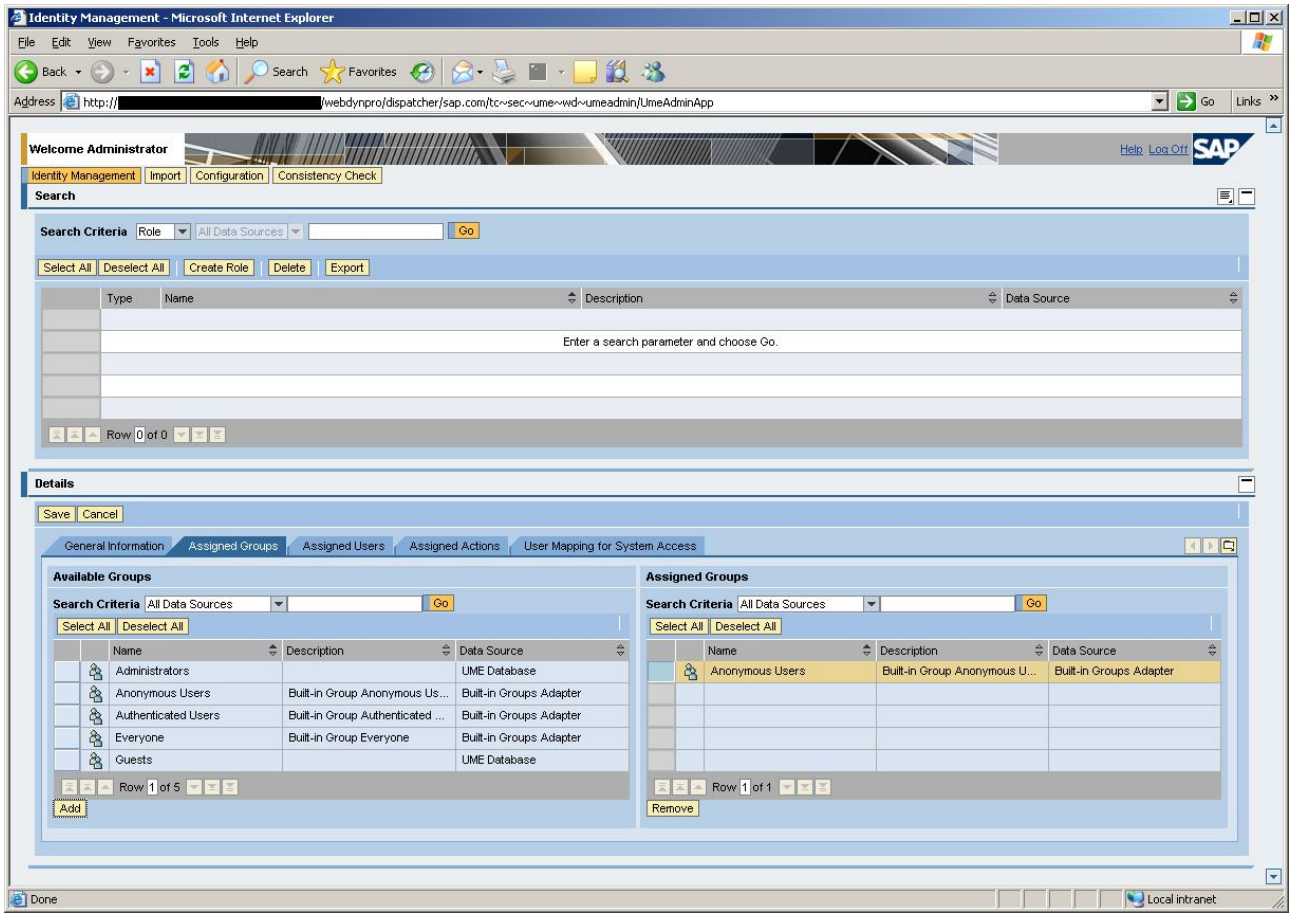
The "idm_anonymous" action is now assigned to the role and this will be shown in the right pane (**Assigned Actions**).

7. Select the "Assigned Groups" tab:



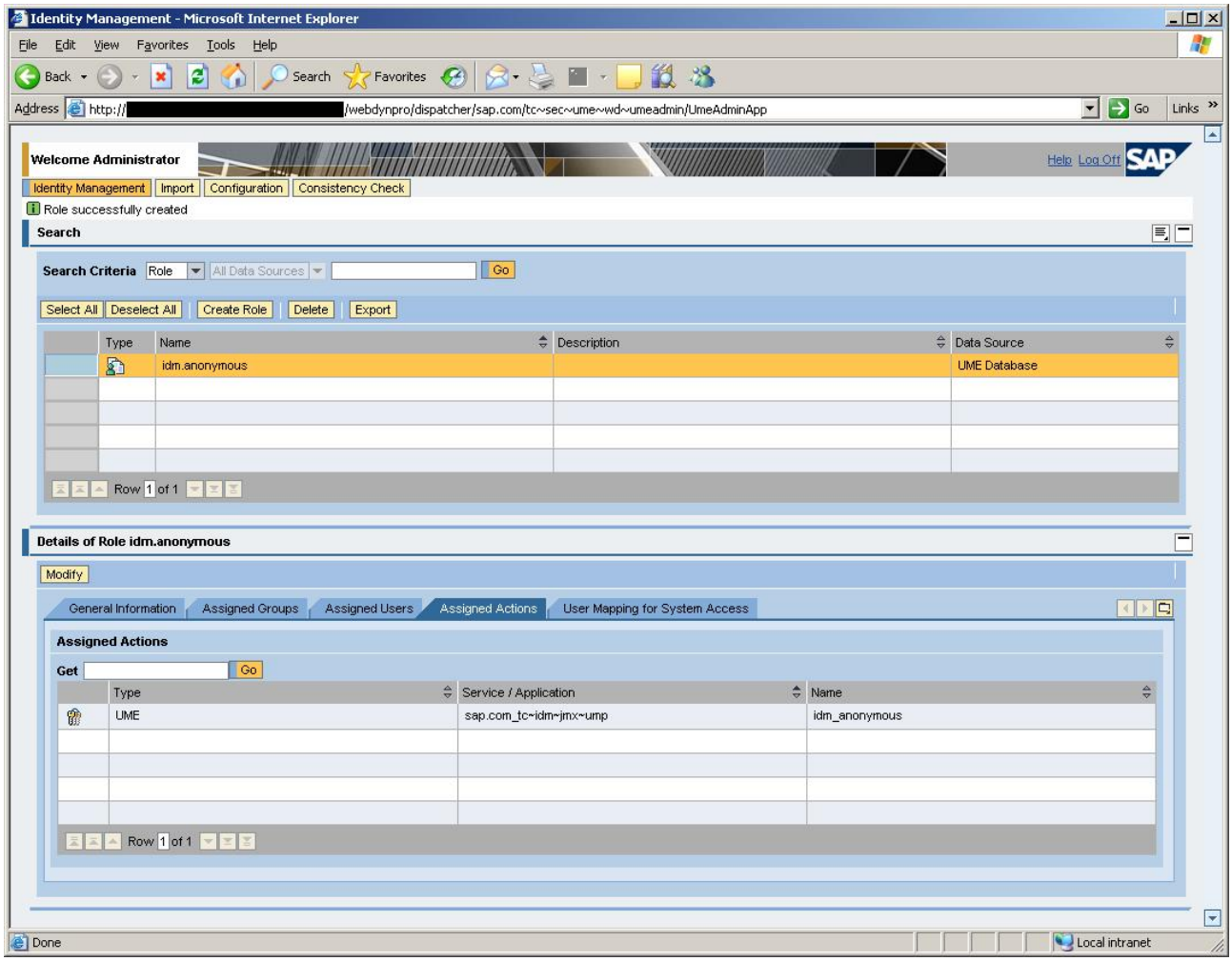
In the "Available Groups" pane, choose "Go" to list all available groups.

8. Select the "Anonymous Users" group and choose "Add".



The "Anonymous Users" group is now given the role and this will be shown in the right pane (**Assigned Groups**).

9. Choose "Save" to confirm and create the new role, which will give access to the password reset to every anonymous user. The just created role will be displayed in the list of the roles available:



Section overview

The tutorial consists of the following sections:

Section 1: Creating the tasks	This section describes how you create and configure the password reset task and the password reset failed task.
Section 2: Configuring the identity store	Configuring of the identity store is described in this section, i.e. adding the reference to the tasks created in the previous section, and defining the password reset parameters.
Section 3: Creating a self-service task for editing of authentication information	Five questions are by default used to authenticate user. Answers to these questions need to be defined by the user, which can be done by user through a self-service task defined in this section.
Section 4: Self-service password reset	This section describes the use of the self-service password reset functionality.
Section 5: Changing the authentication questions	In this section, how to alter the default authentication questions is described.
Section 6: Resetting the number of failed password reset attempts	This section describes a task used for setting of the password for the user, and resetting of the failed password reset attempt counter.

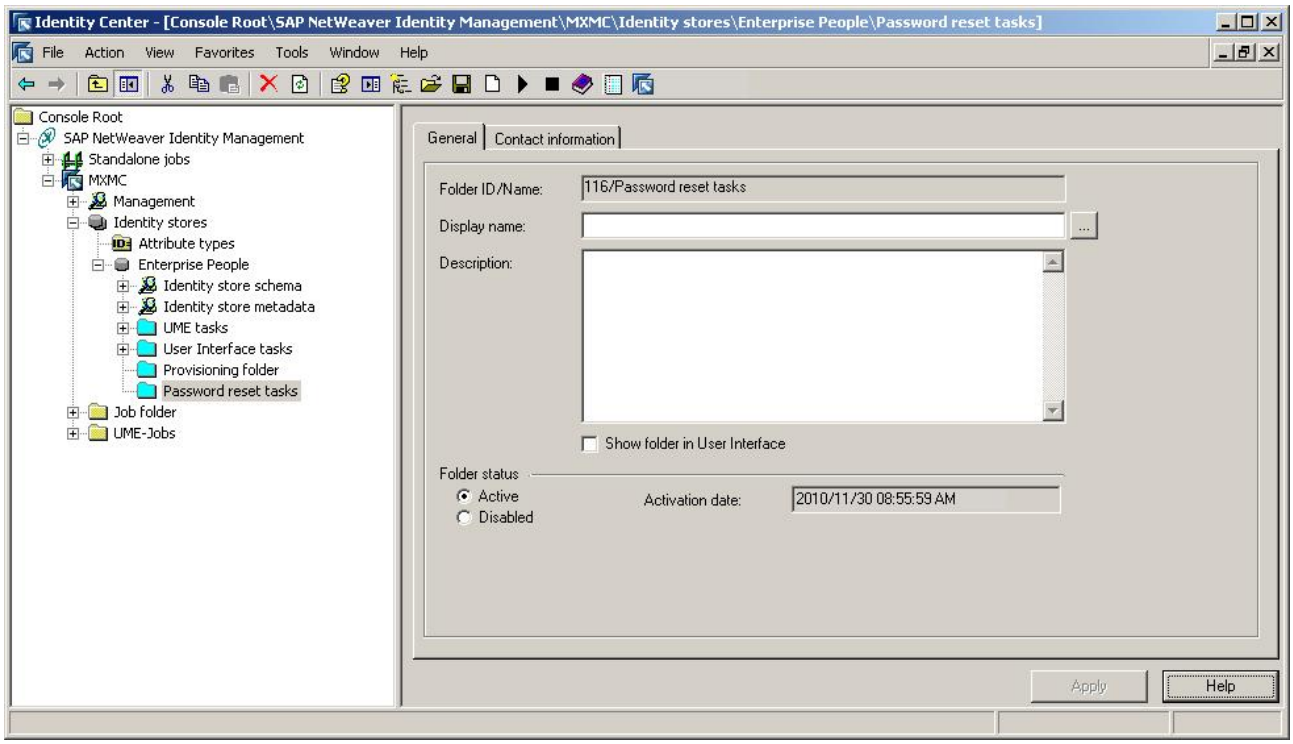
Section 1: Creating the tasks

The password reset task is used to generate a new password for a user who has forgotten his/her password. The task is then added to the identity store configuration so that it will be available for the anonymous users. The password reset failed task, which is run every time the password reset process fails, also needs to be created and added to the identity store configuration.

Creating the folder for the tasks

Before creating the tasks, we are going to create a folder for the tasks in the identity store:

1. Select the identity store node in the console tree and choose **New/Folder…** from the context menu to create the folder (name the folder e.g. "Password reset tasks".



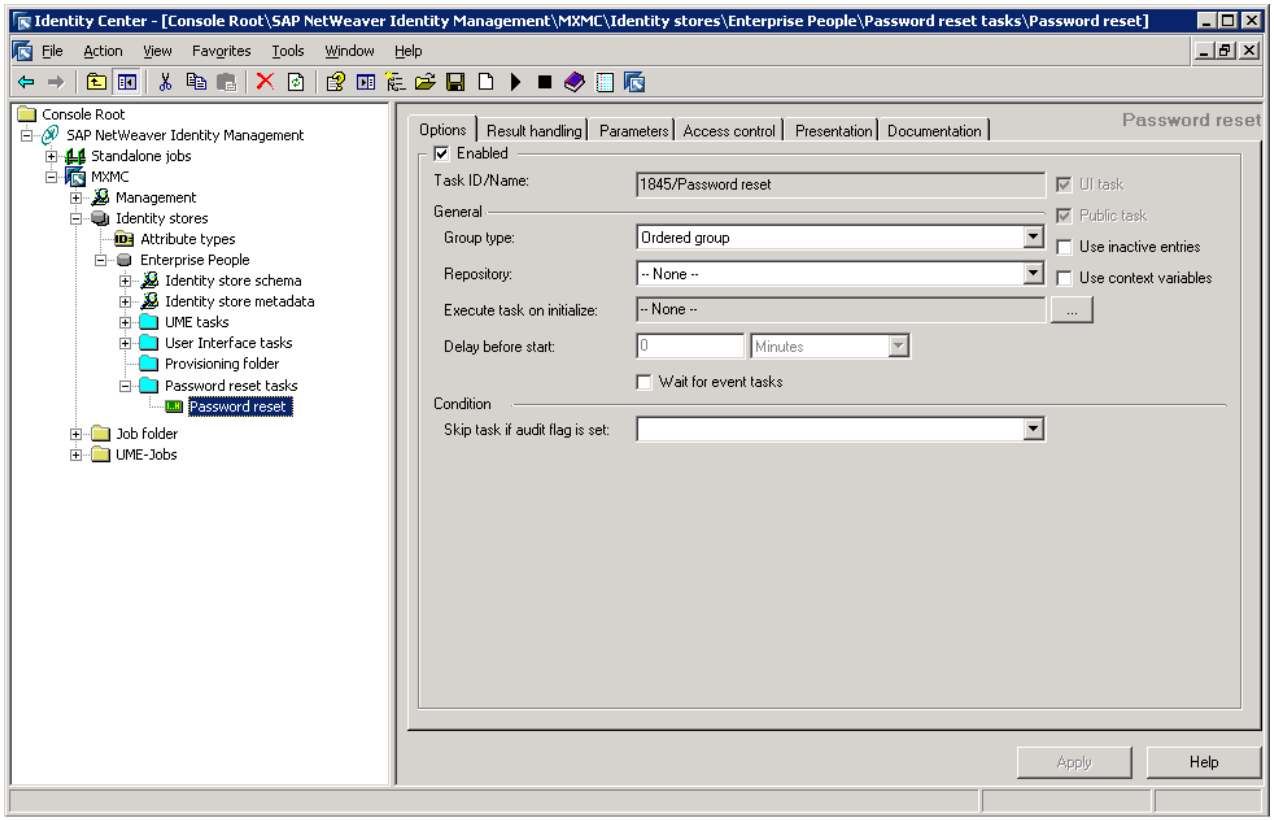
   Deselect "Show folder in User Interface".

2. Choose "Apply".

Creating the password reset task

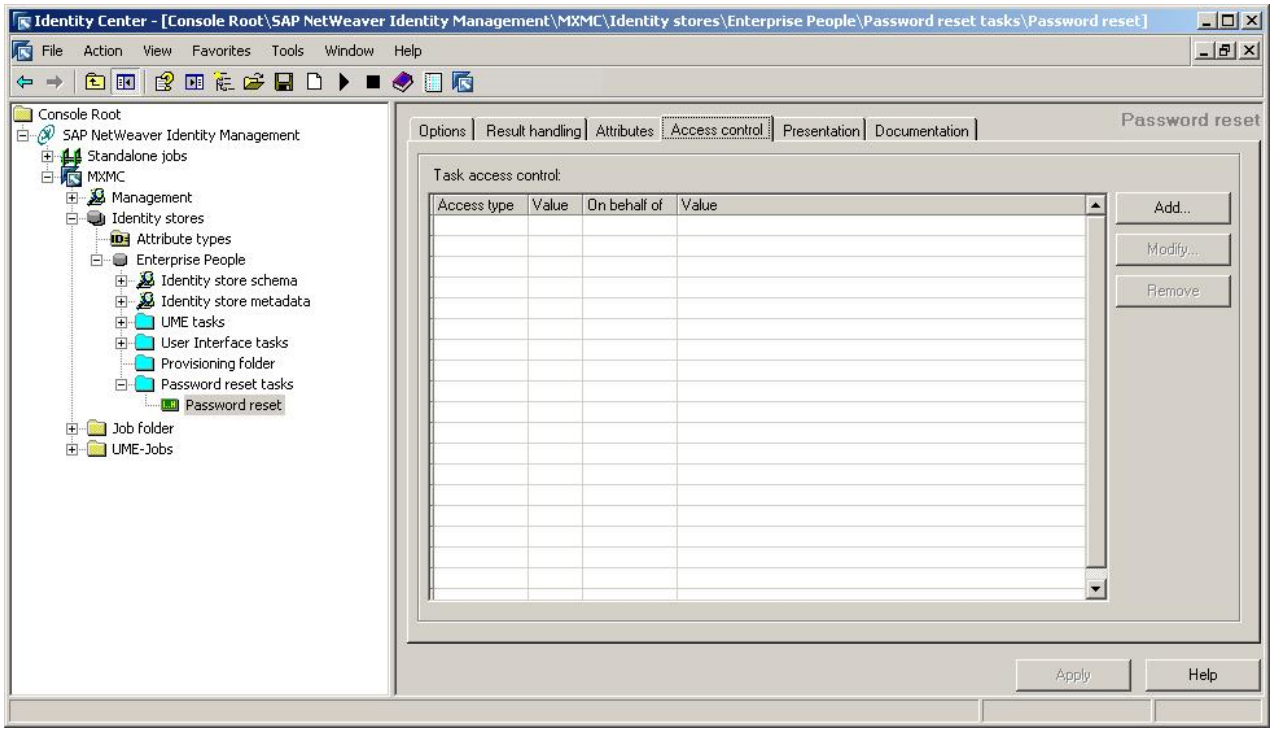
To create the password reset task, do the following:

1. Select the folder you just created and choose **New/Guided task/Password reset** from the context menu.

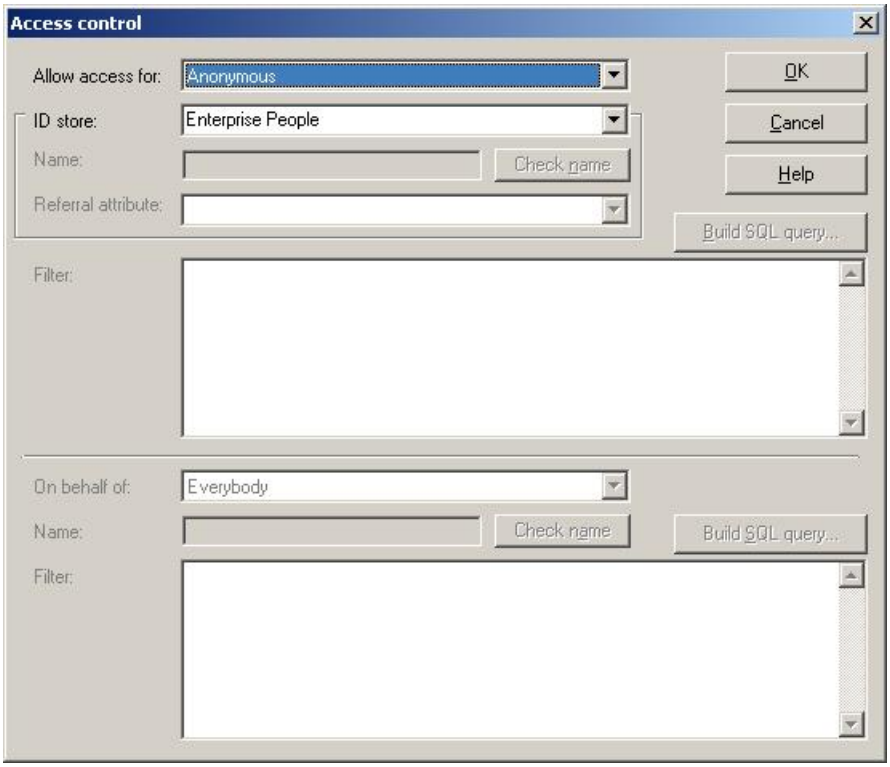


Modify the name of the task in the console tree (e.g. "Password reset").

2. Select the "Access control" tab.

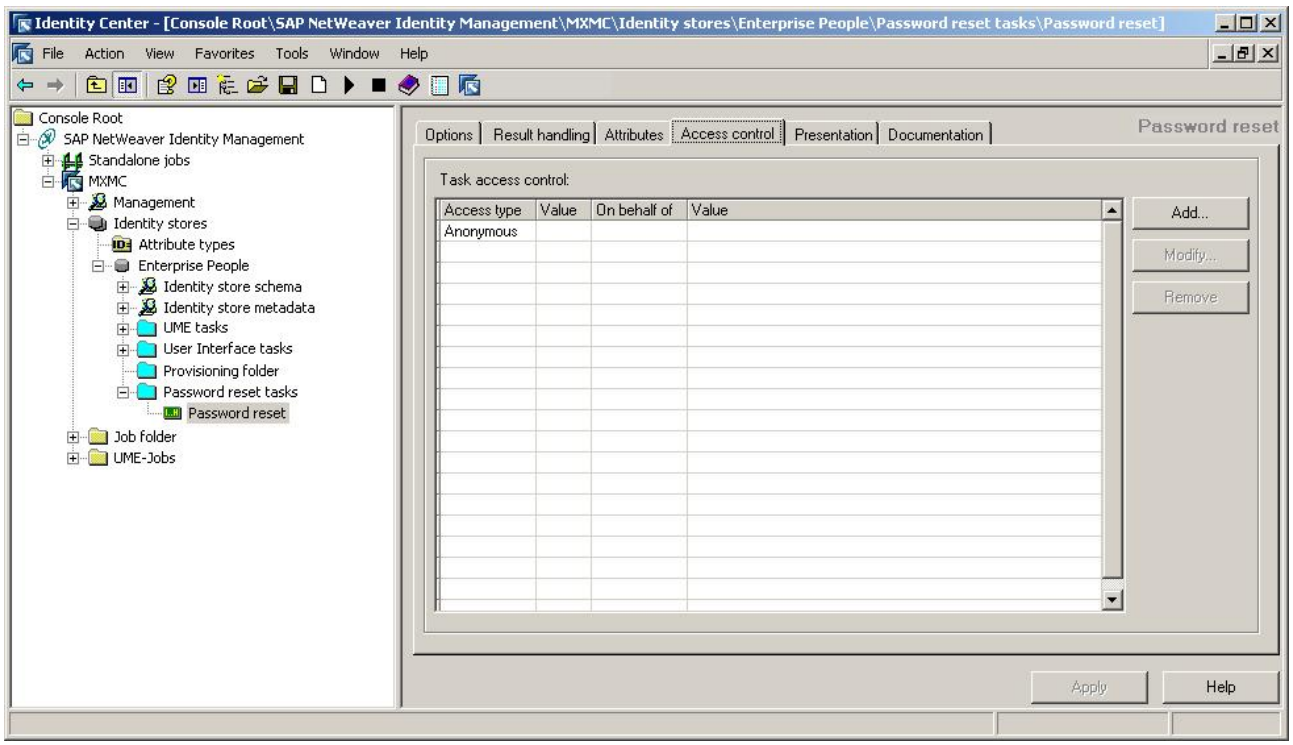


3. Choose "Add…".



Select "Anonymous" in the "Allow access for" field and make sure that the correct identity store is selected in the "ID store" field.

4. Choose "OK".



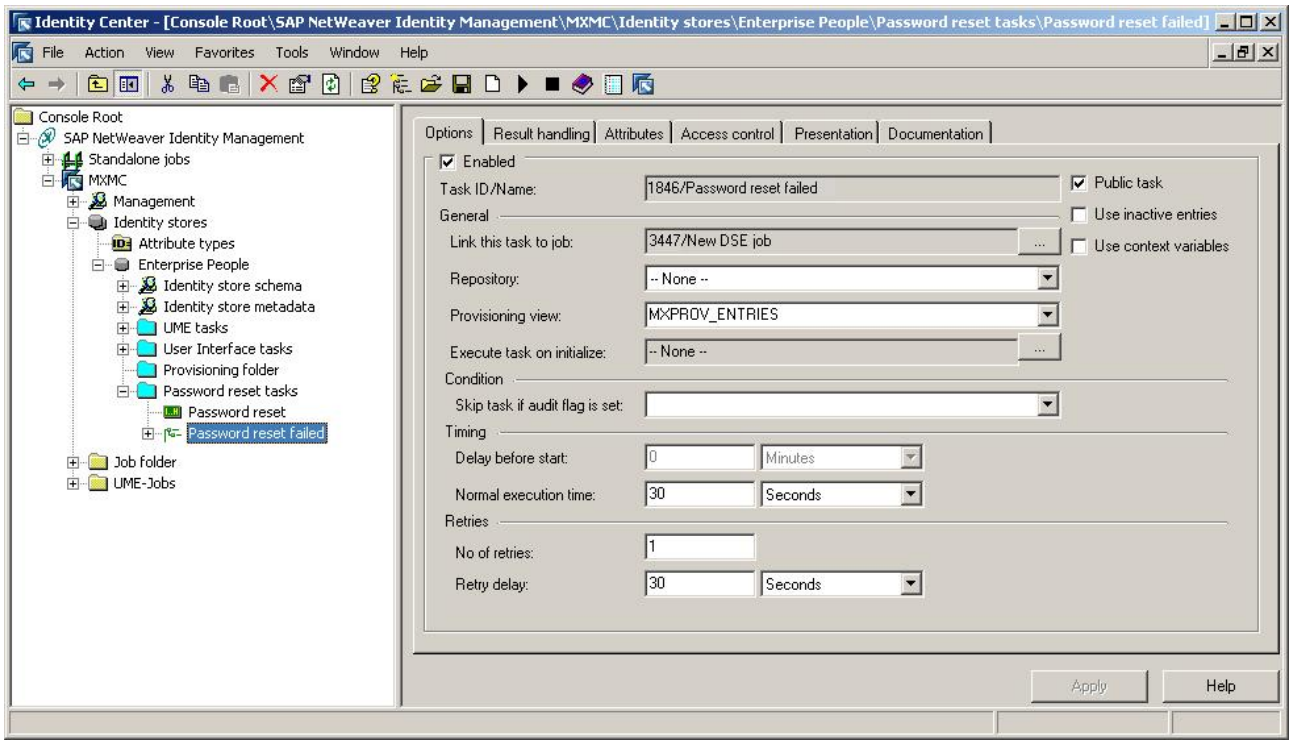
5. Choose "Apply".

The password reset task is now defined.

Creating the password reset failed task

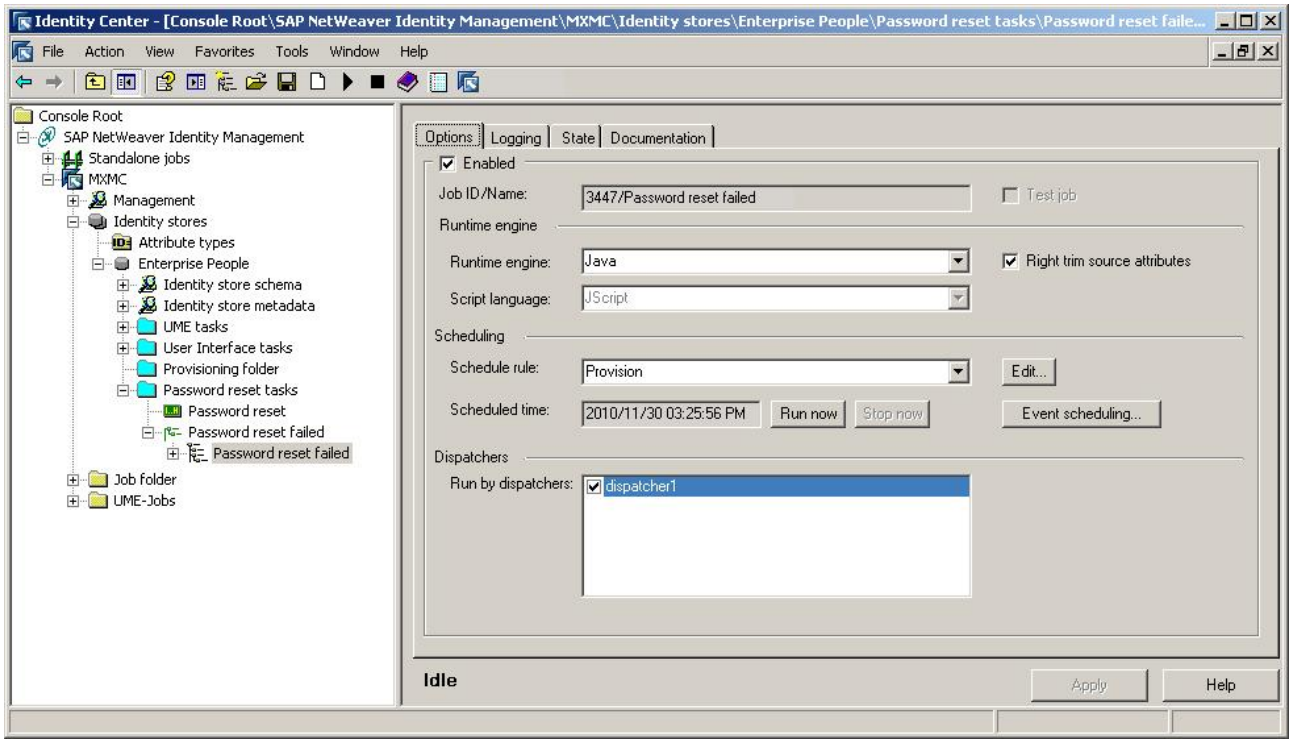
We have created the task that is run when the user requests a password reset. Next, we want to create the password reset failed task – the task that is run every time the password reset process fails. This task can be configured to do several things upon the password reset error – in this document the task creates an ASCII file and logs the error information. To create this task, do the following:

1. Select the "Password reset tasks" folder in the console tree and choose **New/Action task/Empty job** from the context menu or create the task by choosing an ordered or unordered task group from the context menu. (As of SAP NetWeaver Identity Management 7.2 SP9, you can create the task by choosing only ordered task group.)



Modify the name of the task (e.g. "Password reset failed") in the console tree.

2. Select the job:



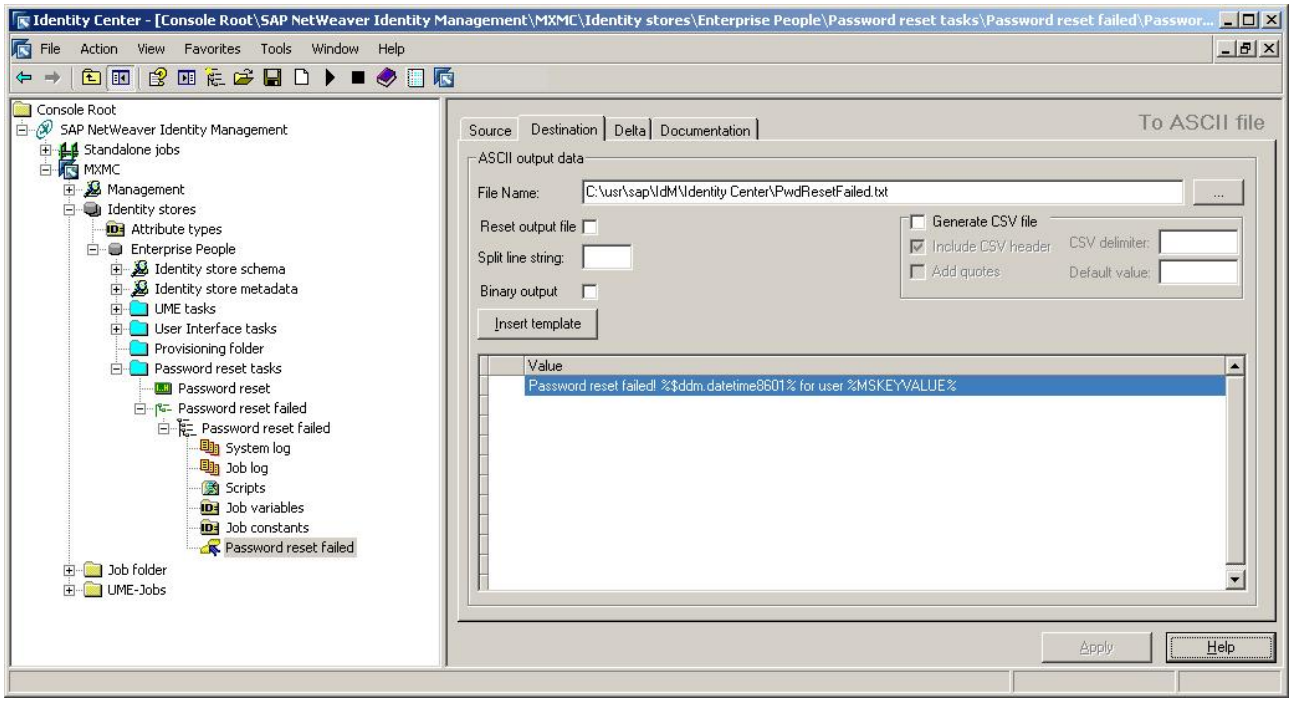
Modify the name of the job in the console tree.

Modify the job properties:

Enabled
Select this check box to enable the job to be run by a dispatcher.

Run by dispatchers
Select a dispatcher that should be responsible for running this job.

3. Choose "Apply".
4. Now select the job in the console tree and choose **New/To ASCII file** to create a pass.



In the "Destination" tab modify the following properties:

File name
Specify the location and the name of the file where the information about the failed password reset process will be available (e.g. *C:\usr\sap\IdM\Identity Center\PwdResetFailed.txt*).

Value in the definitions pane
Type any value to be written to the ASCII file in the "Value" field in the definitions pane, e.g.:

```
Password reset failed! %$ddm.datetime8601% for user %MSKEYVALUE%
```

Use the context menu to insert the system parameter *ddm.datetime8601* and the source attribute *MSKEYVALUE*.

5. Choose "Apply".

Section 2: Configuring the password reset parameters

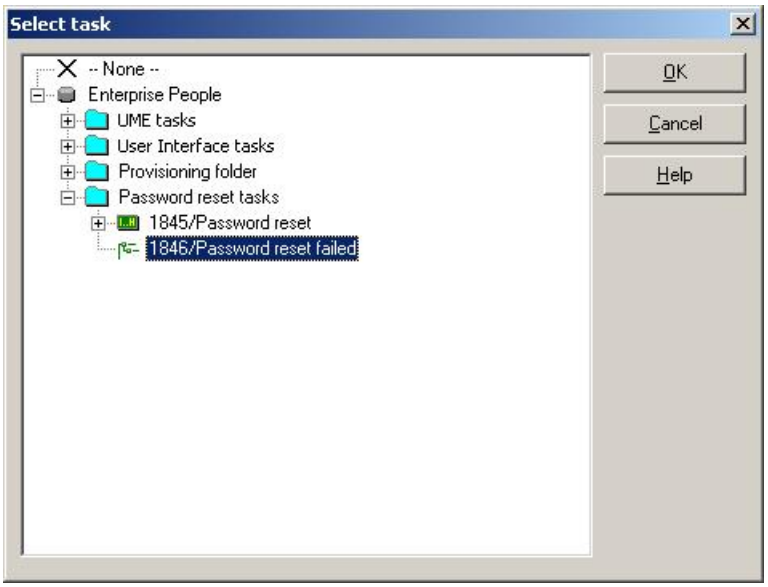
The password reset task must be configured to call the task *Password reset failed*. Parameters, like defining a minimum number of validation answers or a number of authentication questions that should be displayed for the user, need to be defined also. The password reset task must also be referenced from the identity store. This section shows how to configure the parameters on the *Password reset* task and on the identity store.

Adding a reference to password reset failed task

To configure the *Password reset* task to call the task *Password reset failed*, do the following:

1. Select the "Password reset" task in the console tree and choose the "Parameters" tab.

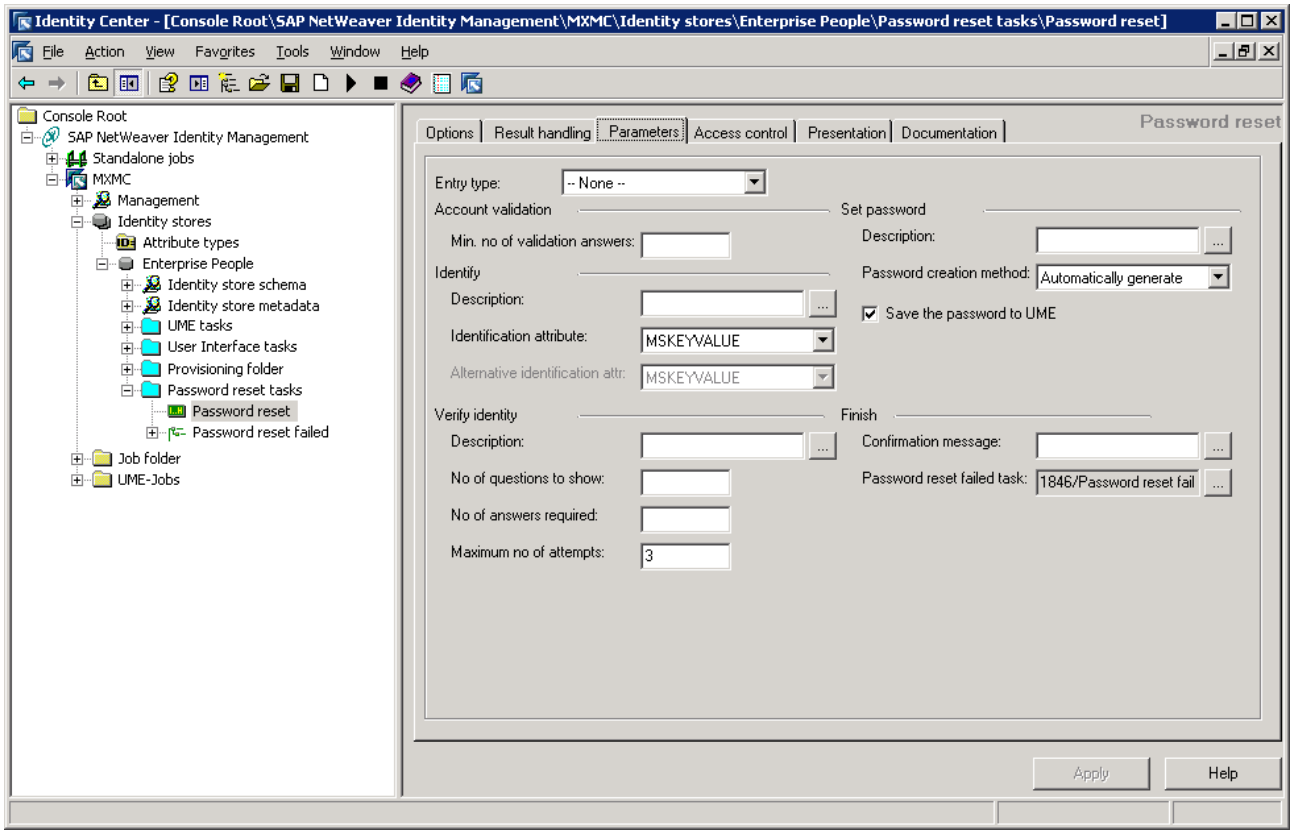
   Choose "…" to the right of the "Password reset failed task" field to open the "Select task" dialog box.



   Navigate to the "Password reset failed" task we just created and choose "OK".

2. Choose "Apply".

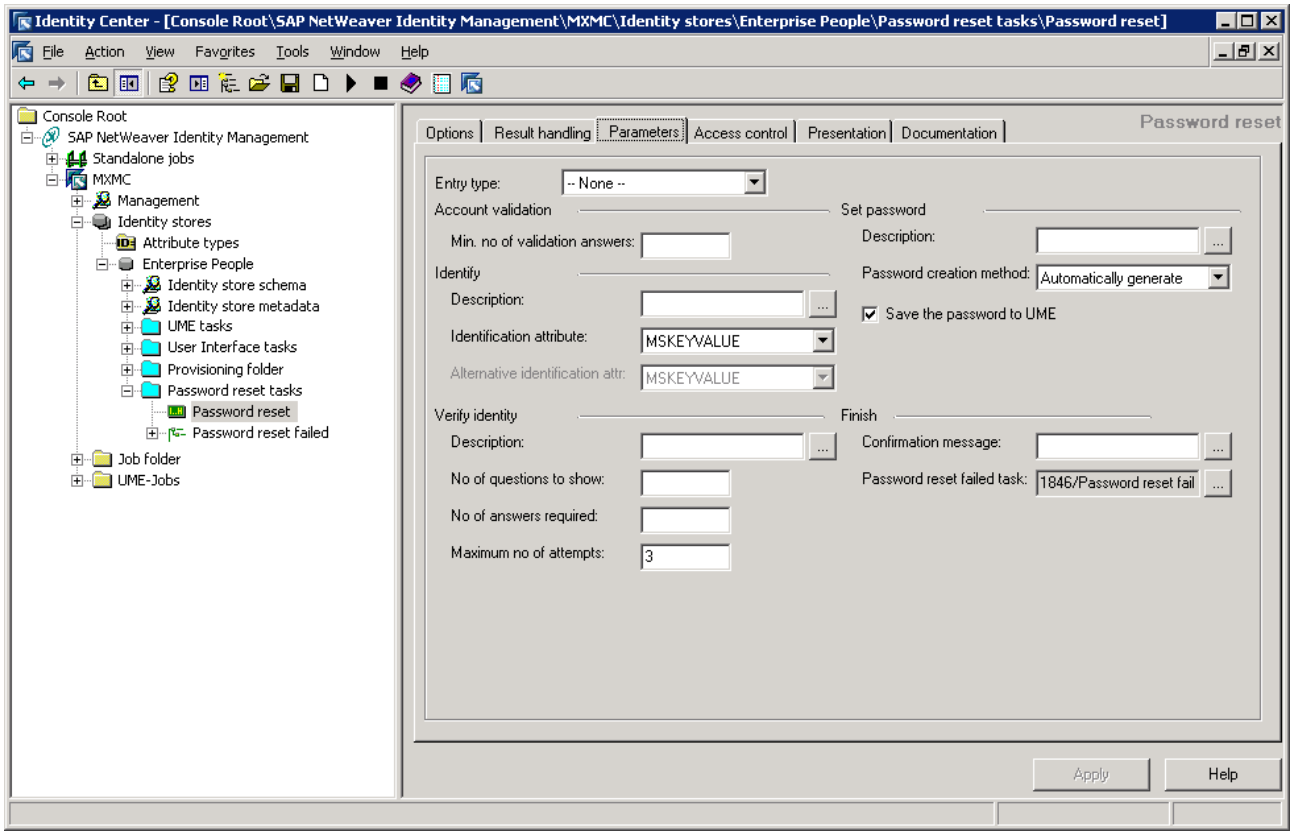
The task is now added:



Setting the password reset parameters

To set other parameters in the password reset task, do the following:

1. Select the "Password reset" task in the console tree and choose the "Parameters" tab:



Configure the following parameters:

Entry type
Select the entry type for this task, usually MX_PERSON. The task will only be available for entries of this entry type.

Min. no of validation answers
In a task showing the authentication questions (see *Section 3: Creating a self-service task for editing of authentication information* on page 22), the user may be required to define an answer for a minimum number of these questions. In the field "Minimum number of validation answers" you define how many of the defined questions the user has to answer. This number should be the same or higher than the number defined in the "Number of answers required" field.

Description (Identity)
This is description for the step one of the password reset guided task: "Enter User Identification".

Identification attribute/alternative identification attribute
In the process of identifying a user he/she will be asked for the unique identifier. This identifier is *MSKEYVALUE* by default. In addition, there are two other options you can choose to configure: 1) the identifier is other unique attribute (e.g. email address) instead of the *MSKEYVALUE*, and 2) the identifier is other unique attribute in addition to the *MSKEYVALUE*.

Description (Verify identity)
This is description for the step two of the password reset guided task: "Answer the Following Question(s)".

No of questions to show
This number will define how many questions there will be displayed for the user during the authentication process. The number should be the same or higher than the number defined in the "Number of answers required" field, usually the same since there is no need of displaying more questions than the number required answering on. The questions are randomly selected from the attributes where the user has provided an answer.

No of answers required
The parameter will define how many of the defined authentication questions the user has to answer in order to identify himself/herself. Number defined in this field should be the same or lower than the number defined in the "Minimum number of validation answers" field.

Maximum no of attempts
Here you can define a maximum number of attempts the user has before the authentication and the password reset process fails. There are three (3) attempts by default.

Description (Set password)
This is description for the third step of the password reset guided task: "Choose 'Finish' to set the password".

Password creation method
The password creation method can be defined here. There are two methods available – a method where the password is automatically generated (by default) and a method where the user is asked to enter the new password.

Note:
Here, in this document, the method "Ask the user" is used. When using the method where the password is generated automatically, the delivery information should be specified – a task which sends the new password to the user by SMS or e-mail needs to be created. In an organization using password provisioning, the users will have the same password both for the Identity Management User Interface and the e-mail system. In this case, it will be no point in sending the password to the user's e-mail address, as the user will not be able to access the e-mail system.

Save the password to UME
Enable this option if you wish to save the password to UME. Setting the productive password in UME is possible with one of the following SAP NetWeaver versions:

- SAP NetWeaver 2004 SP 23+ (means SP 23 and following)
- SAP NetWeaver 7.0 SP 18+
- SAP NetWeaver 7.0 Enhancement Package (EHP) 1 SP 2+
- SAP NetWeaver 7.0 EHP 2 SP 0+
- SAP NetWeaver Composition Environment (CE) 7.1 SP 7+
- SAP NetWeaver CE 7.1 EHP 1 SP 1+
- SAP NetWeaver CE 7.2 SP 0+
- SAP NetWeaver 7.3 SP 0+
- SAP NetWeaver 7.3 EHP 1 SP 0+
- SAP NetWeaver 7.4 SP 0+

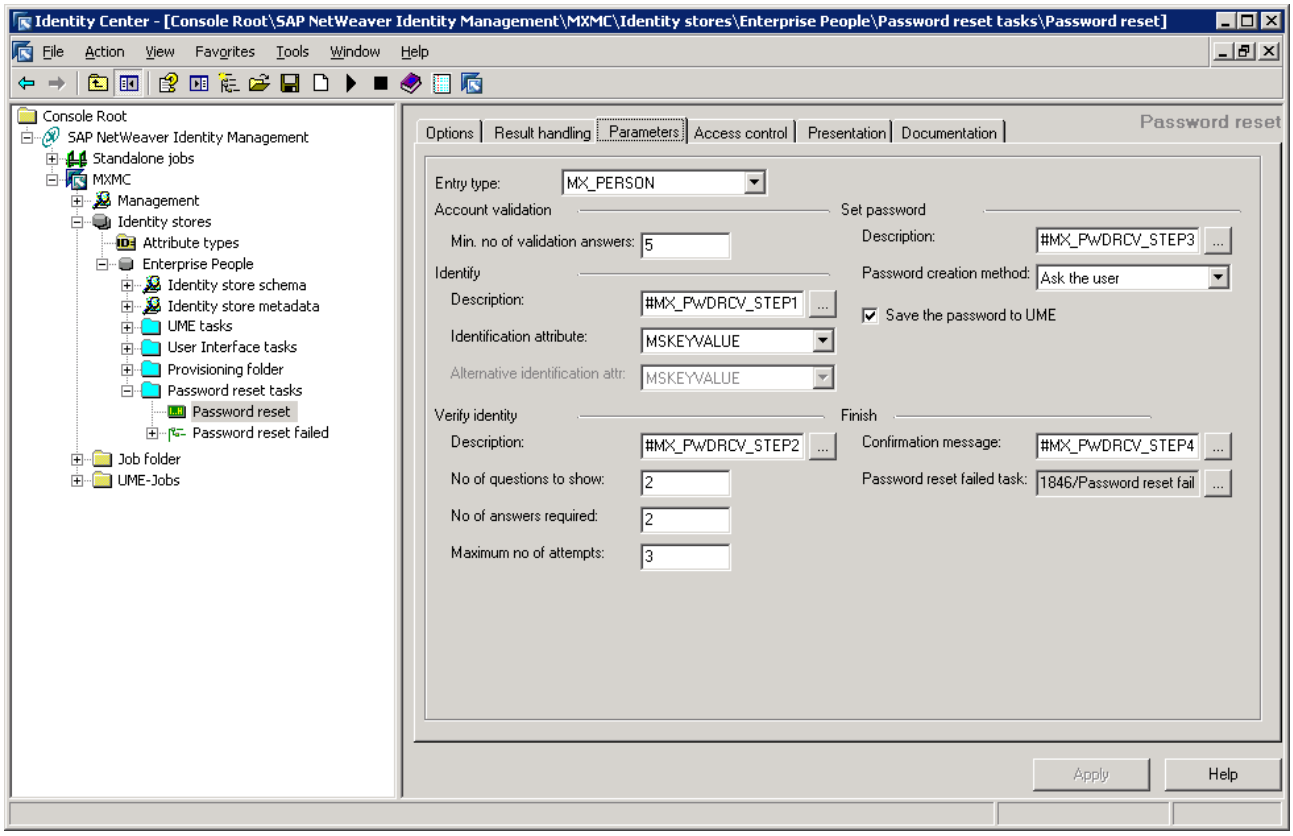
The option is enabled by default. The only use case where this option should be disabled is when the user does not have an account in UME, i.e. does not have access to Identity Management User Interface.

What password policy is selected when creating a password depends on whether this option is set or not. When the option is enabled, then the UME password policy is applied and not the Identity Management policy (even if defined). When the option is disabled, the defined Identity Management policy applies. See page 21 for more about the Identity Management password policy/validation.

Confirmation message
This is the confirmation message that appears when the task is executed: "Password Set".

2. After configuring the parameters choose "Apply" to confirm.

The configuration may look something like this:

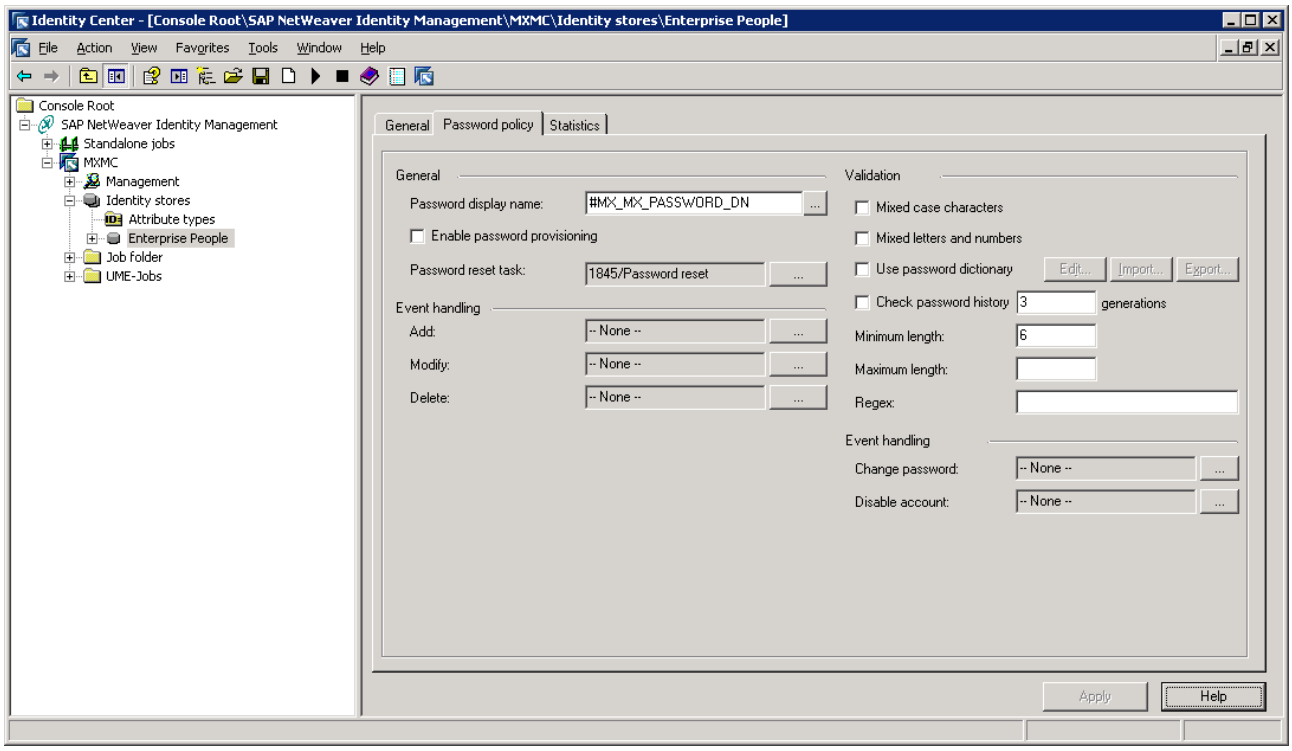


Now the implementing and configuring of the self-service password reset is completed. The next step is to create a self-service user task where the user can define the answers to the authentication questions.

Adding a reference to password reset task on identity store

The identity store must be configured to reference the task *Password reset*. Do the following:

1. Select the identity store in the console tree and select the "Password policy" tab.
2. Define the password reset task in the "Password reset task" field. Choose "…" to navigate to the task.



3. Choose "Apply".

Here you can also define the Identity Management password policy, under section "Validation". The following can be defined:

- Whether the password should contain mixed case characters or not.
- Whether the password should contain letters and numbers.
- Enabling/disabling the use of password dictionary.
- Whether the previous passwords should be considered when creating a new one or not. And if yes, how many of the previous passwords should be remembered by the system.
- The minimum and the maximum length of the password.
- Regular expressions (regex).

Note:
The event handling fields "Change password" and "Disable account" are not in use and will be removed from the Identity Center Management Console.

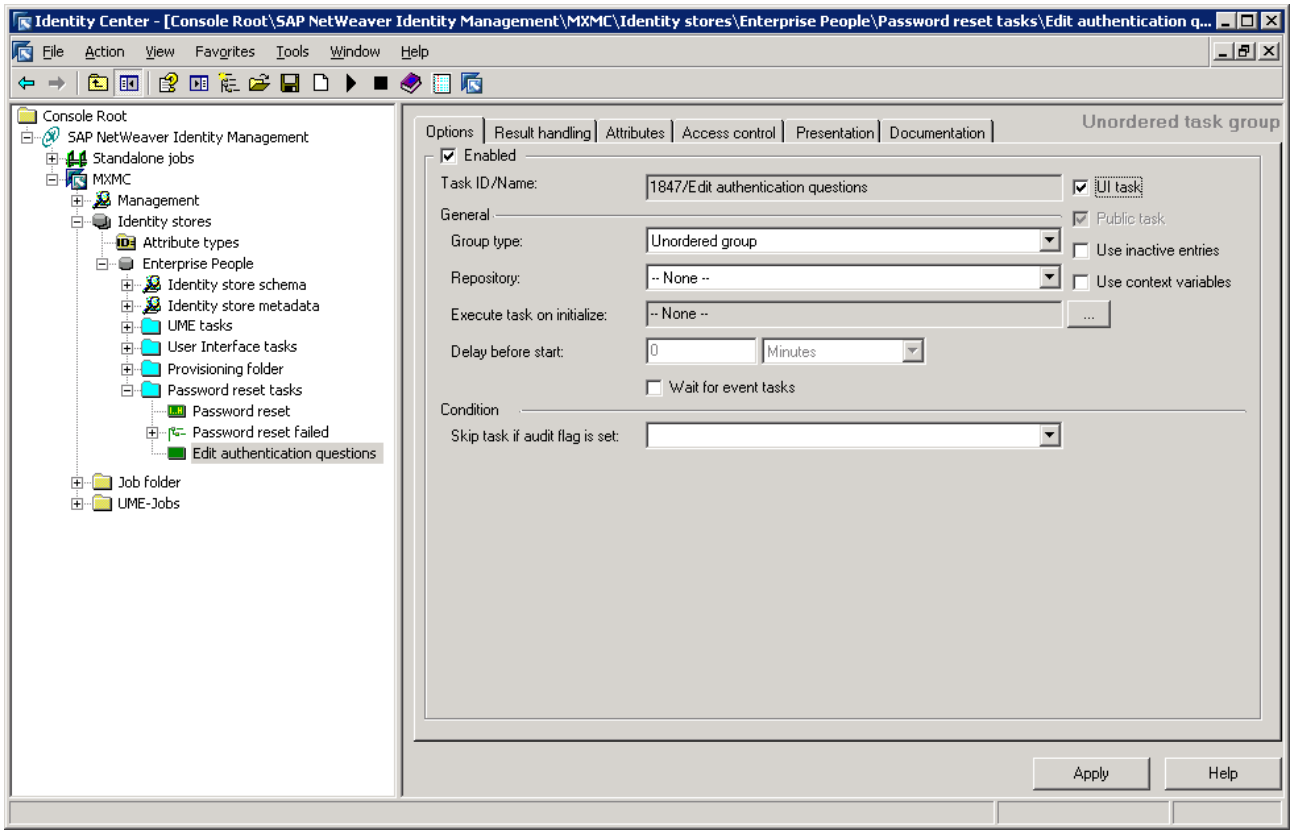
Section 3: Creating a self-service task for editing of authentication information

Now that the self-service password reset is implemented and configured the user needs to define the answers to the authentication questions, and to be able to do that a self-service task for the user is needed. In this document a task *Edit authentication questions* is created for that purpose, but this can typically be done in a user profile task – i.e. if you have defined a self-service task where the users can edit their user profile, add the attributes *MX_AUTHQ_001* to *MX_AUTHQ_005* to this task.

Creating the self-service task

To create the self-service user task, do the following:

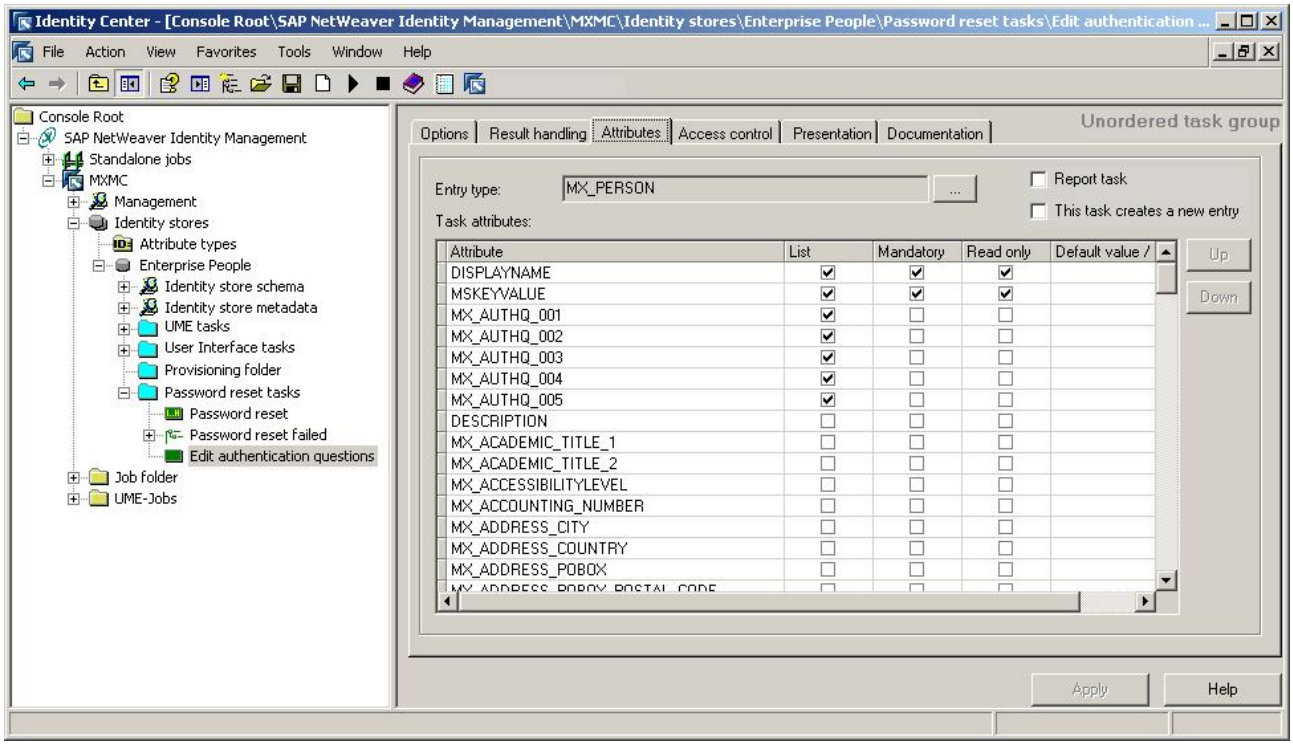
1. Select the "Password reset tasks" folder in the console tree and choose **New/Unordered task group** from the context menu. (As of SAP NetWeaver Identity Management 7.2 SP9, you can choose only ordered task group.)



Modify the name of the task in the console tree (e.g. "Edit authentication questions").

Select the "UI task" option.

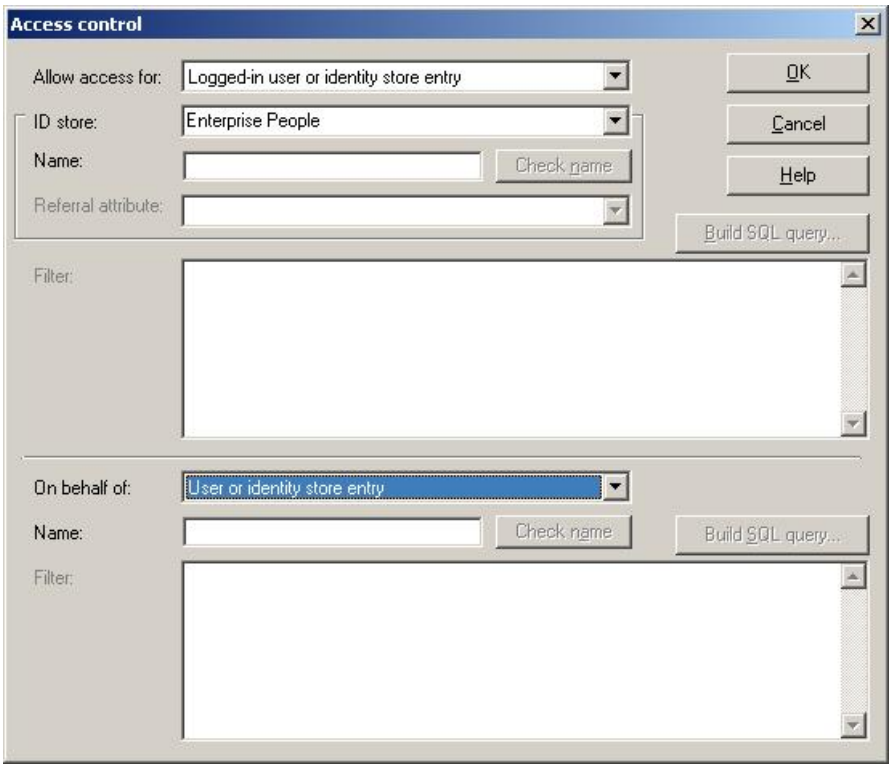
2. Select the "Attributes" tab:



Choose "…" and select "MX_PERSON" in the "Entry type" field, select the attributes *MX_AUTHQ_001* to *MX_AUTHQ_005* and configure the attributes as shown above.

3. Choose "Apply".

4. Select the "Access control" tab and choose "Add…".



Modify the following properties:

Allow access for
Select "Logged-in user or identity store entry".

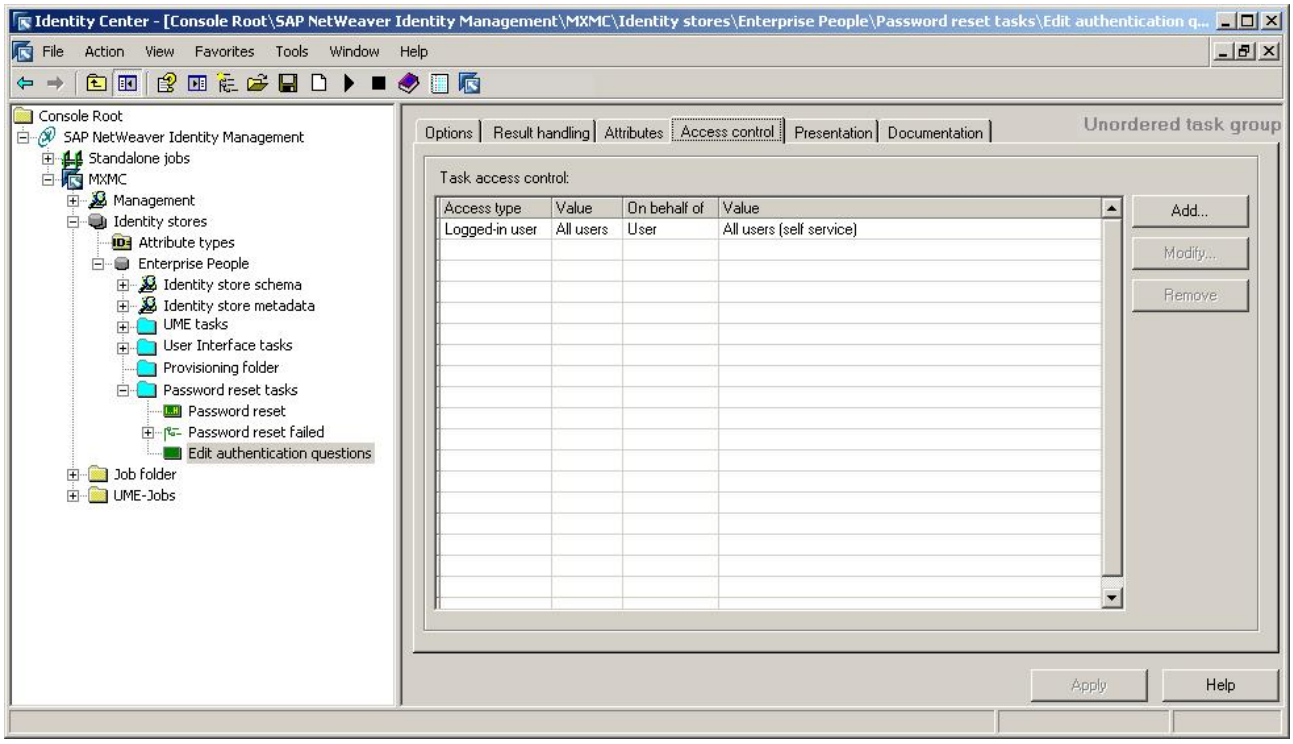
ID store
Select the correct identity store. In this example "Enterprise People" is used.

Name
Leaving this field empty will make the task accessible to everyone. Name is entered when restricting the access to the task (e.g. enter Administrator name to give access to this task only to the "Administrator" user).

On behalf of
There are two ways of creating a self service task. You either select "User or identity store entity" or "Relation - Self". Both ways are legitimate.

5. Choose "OK" and then "Apply".

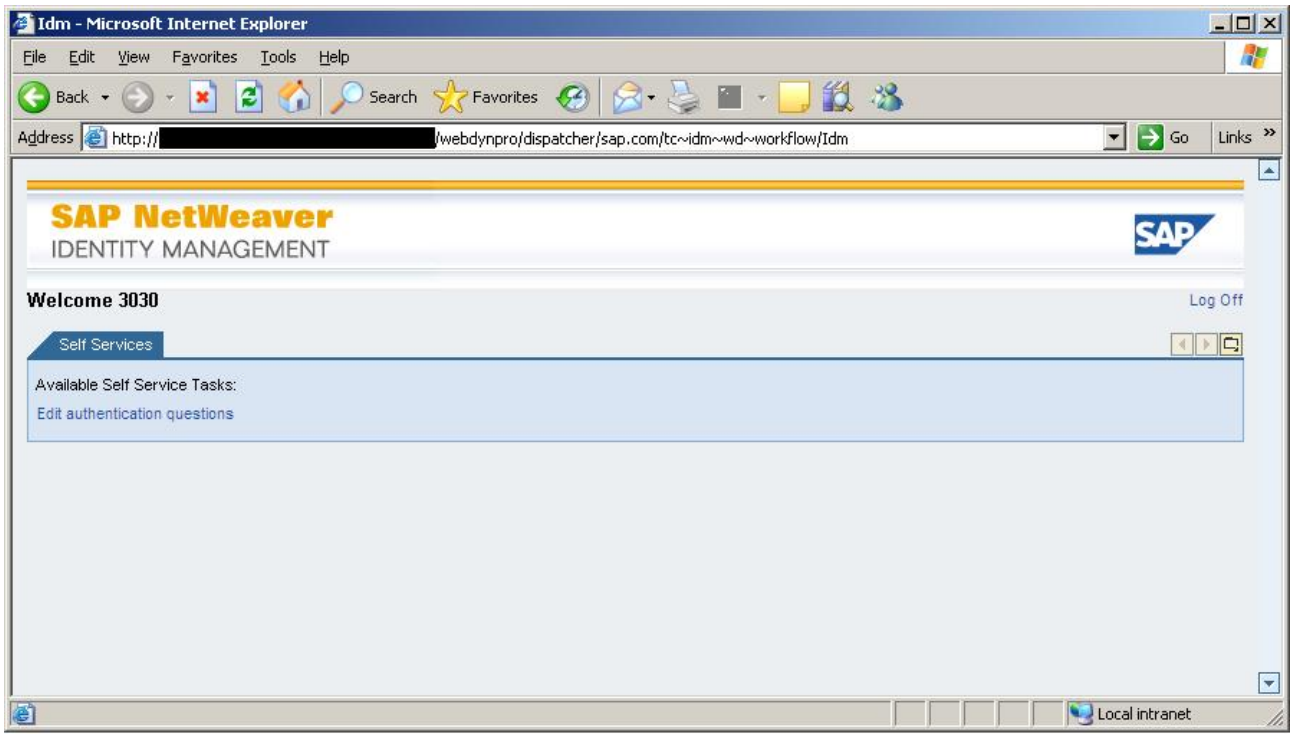
The access definition is added to the task:



Editing the authentication information

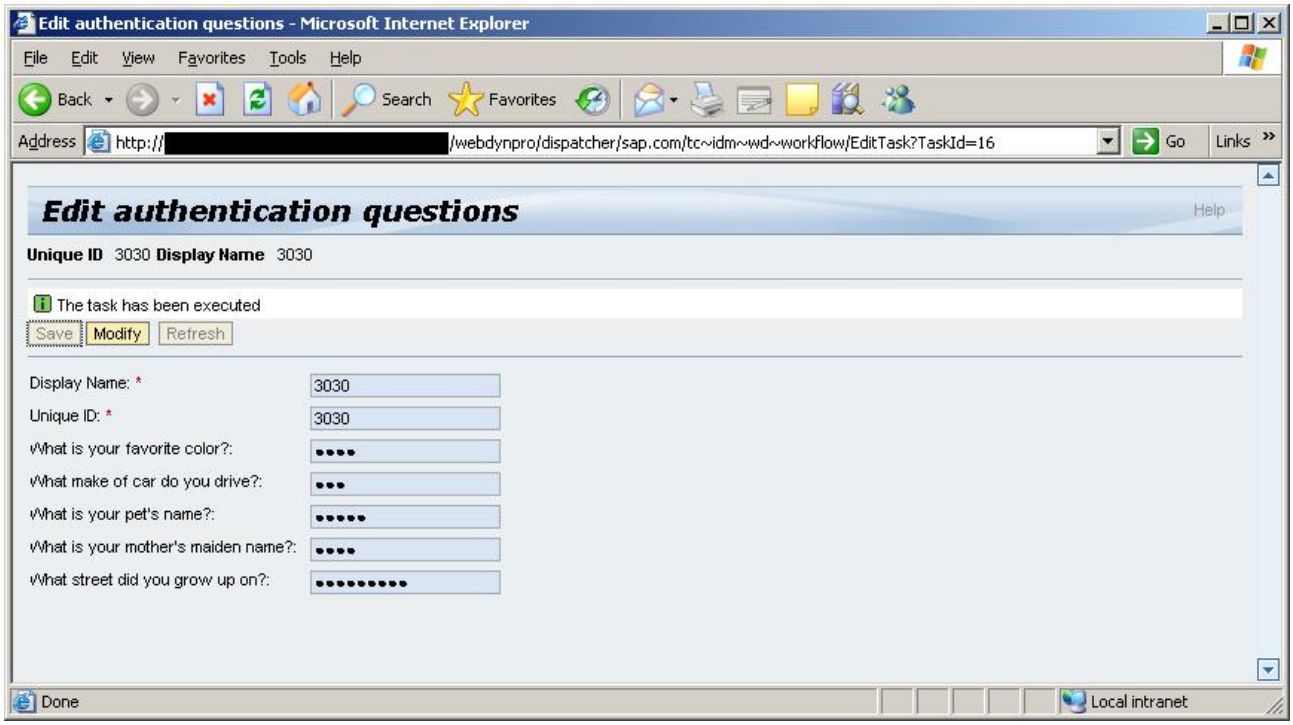
For user to edit the authentication information, i.e. define the answers to the authentication questions, he/she needs to access the self-service user task *Edit authentication questions*. Do the following:

1. Enter http://<host>:<port>/idm in your browser to access the User Interface and provide the credentials in the log-in window.
2. Choose "Log on".



You are now logged on in the User Interface. The image above shows the logged-in user with access to the "Self Services" tab and the self-service task "Edit authentication questions" created in the previous section.

3. Select the "Edit authentication questions" task:

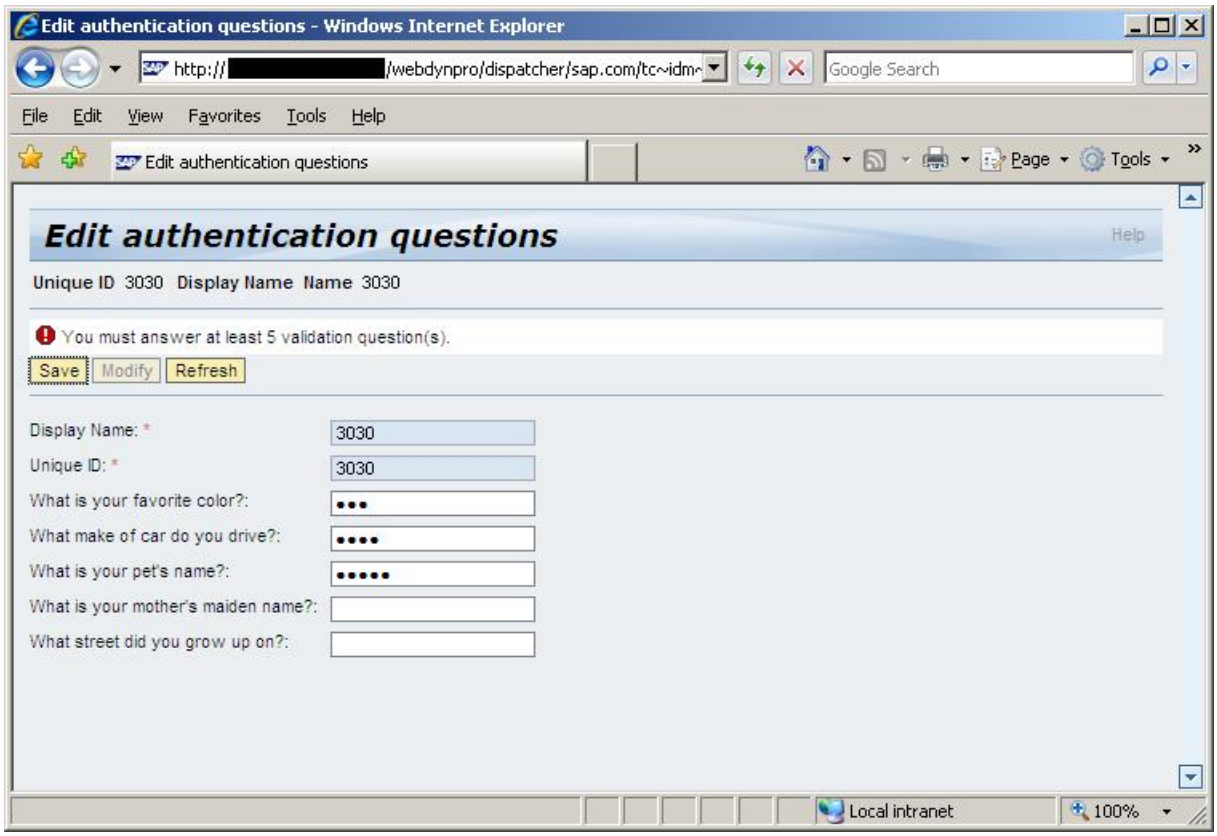


Enter the answers to the displayed authentication questions.

4. Choose "Save" and then close the task.

The answers only known by the user are now defined for the authentication questions.

Note:
If you try to save the information after entering the answers to fewer questions than requested, the task will fail and an error message will appear as displayed in the picture below.



Section 4: Self-service password reset

The password reset process is now defined and the self-service password reset functionality is ready for use. In this section, we will test the self-service password reset functionality and their tasks *Password reset* and *Password reset failed*.

To be able to access the password reset task, make sure to be logged out of the identity store. Make also sure that all browser windows are closed.

Note:
In what language the self-service password reset is available is determined in the following way:

- *The language is determined by the language preferences specified by the browser settings ("accept-language" HTTP header) if existing.*
- *Otherwise, the language is determined by the language preferences specified in the application properties if existing.*
- *Otherwise, the language is determined by the language preferences specified in the Web Dynpro system properties if existing.*
- *Otherwise, the language is determined by the language preferences of the VM.*

Providing a new password

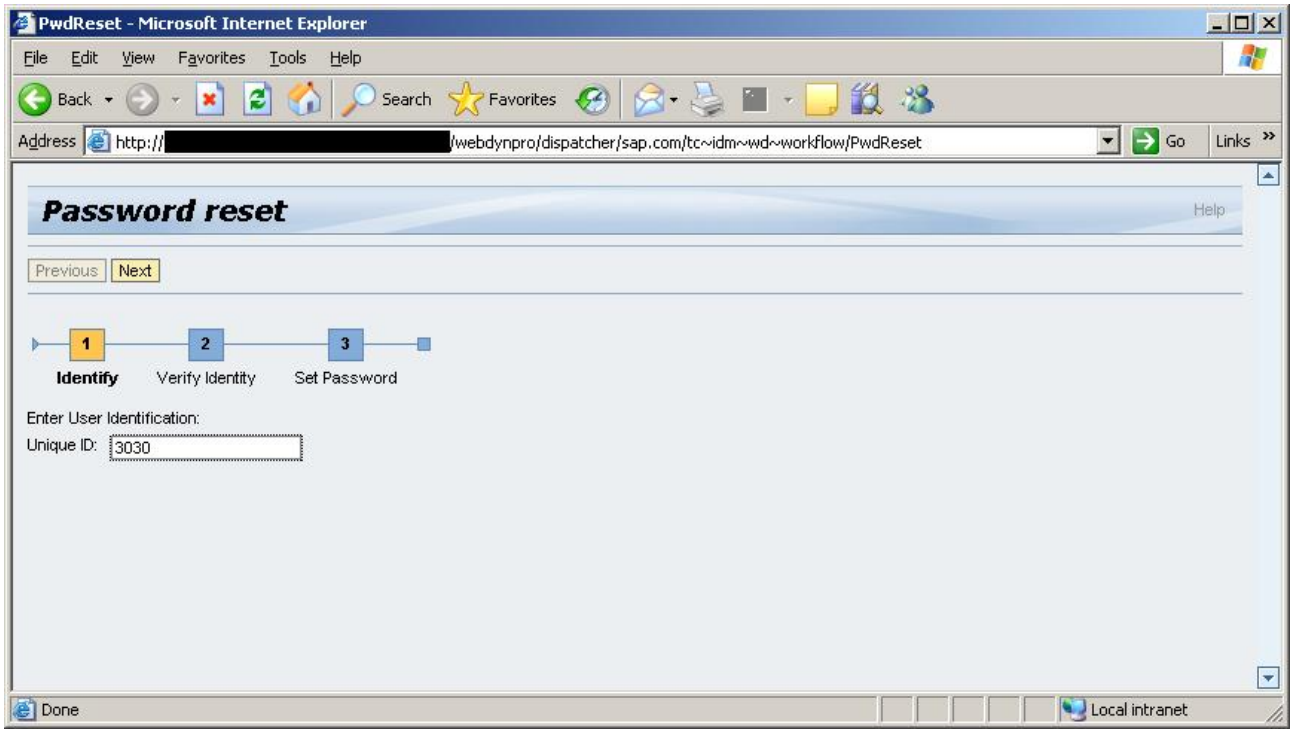
To access the self-service password reset functionality and reset the password, do the following:

1. Open your browser and enter http://<host>:<port>/idm/pwdreset to access the password reset self-service task.

   Note:
   You might wish to incorporate the password reset link to the logon screens (welcome pages) of application servers accessed by users (assuming these are serviced by Identity Management).

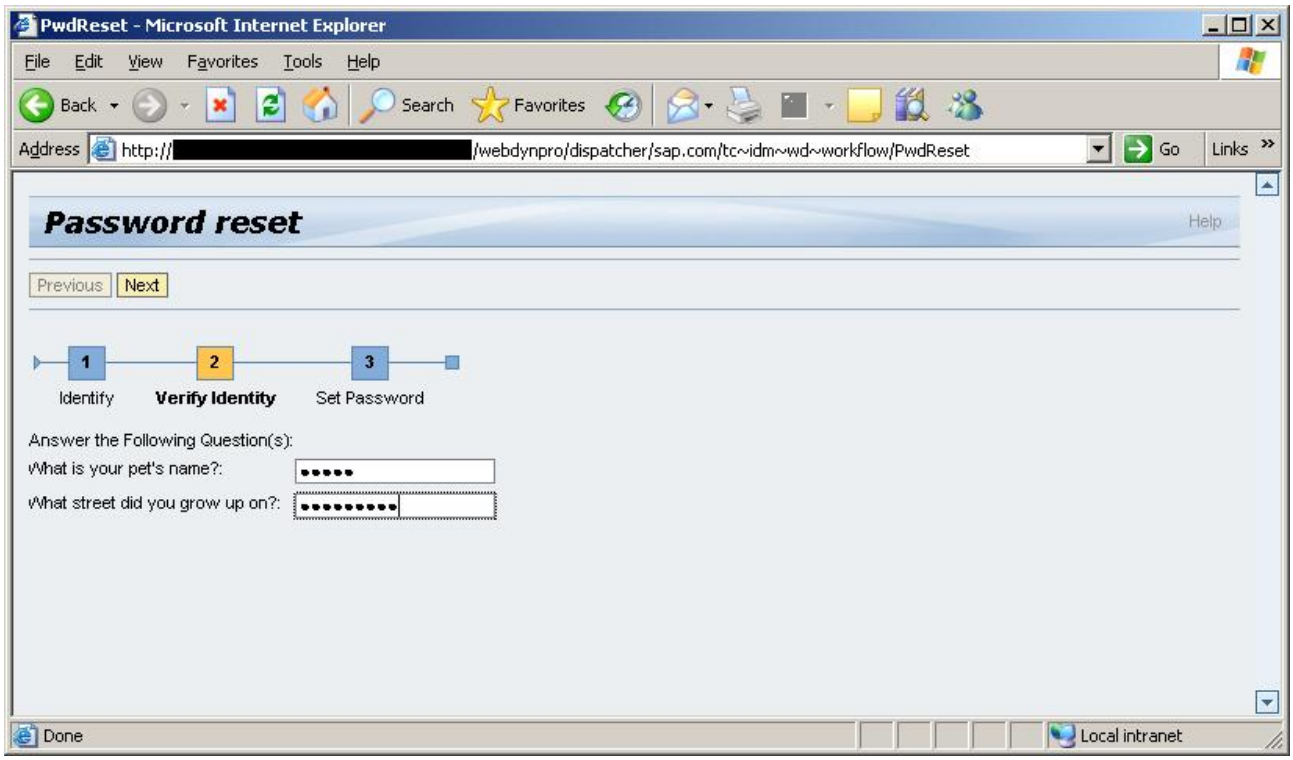
   For example, if your users access an SAP NetWeaver Application Server Java, then you can customize the logon screen for that host to access the password reset URL of SAP NetWeaver Identity Management. For more information, see the SAP Help Portal documentation relevant for your AS Java release:

   - *For releases SAP NetWeaver 2004, SAP NetWeaver 7.0, SAP NetWeaver 7.0 EHP 1 and SAP NetWeaver 7.0 EHP 2, see Customizing the Logon Screens.*
   - *For SAP NetWeaver CE 7.1, SAP NetWeaver CE 7.1 EHP 1, SAP NetWeaver CE 7.2, SAP NetWeaver 7.3, SAP NetWeaver 7.3 EHP 1 and SAP NetWeaver 7.4, see Developing a Custom Logon Screen.*



Enter the unique ID (here *MSKEYVALUE* as previously defined).

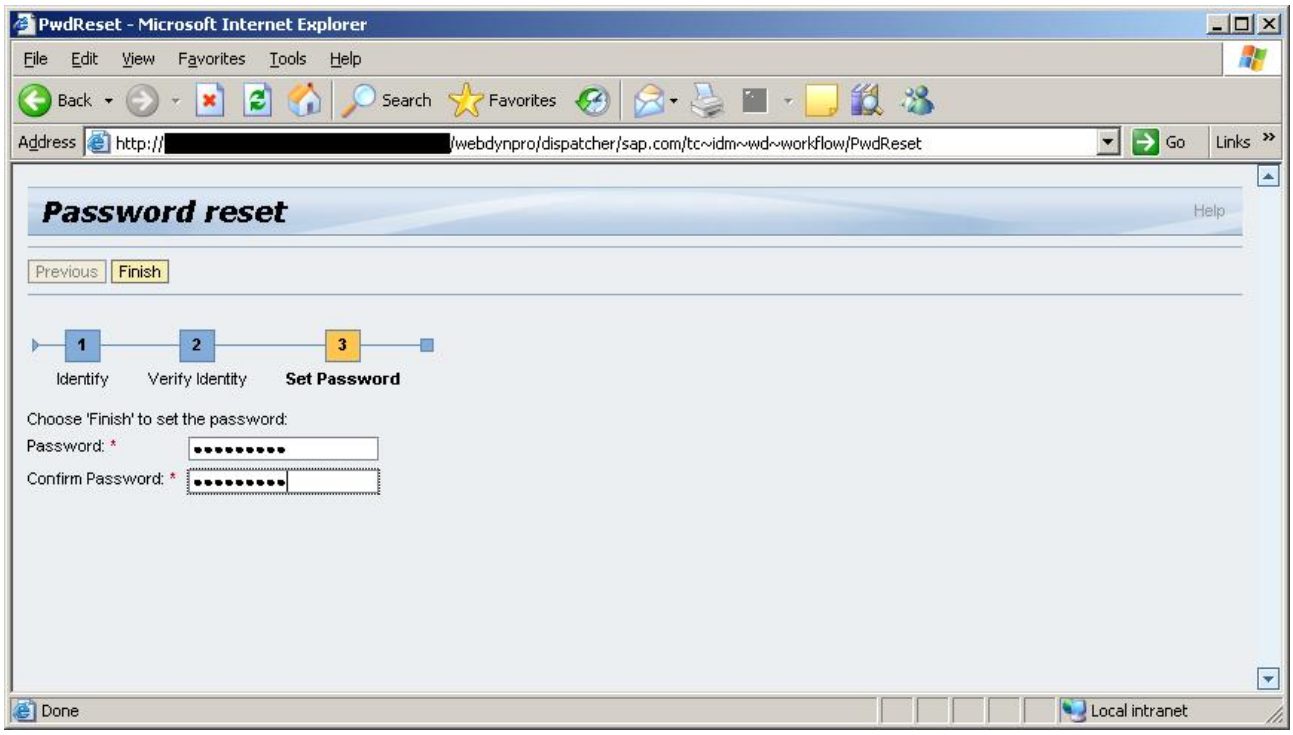
2. Choose "Next".



Enter the answers to the authentication questions.

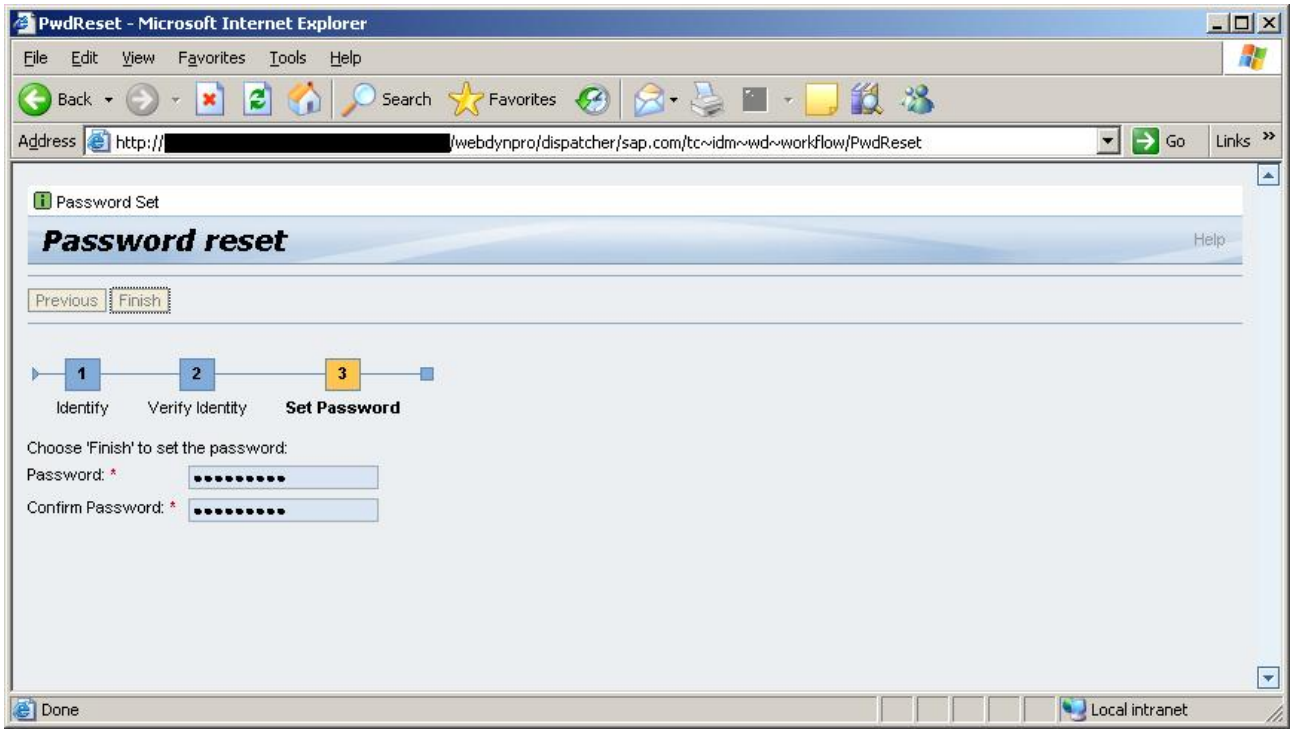
3. Choose "Next".

   If the authentication succeeds, it will be possible to set the new password. In this document the method "Ask the user" is used for password creation, giving the user the possibility of defining its own password:



Enter the new password and confirm it.

4. Choose "Finish" to set the password.

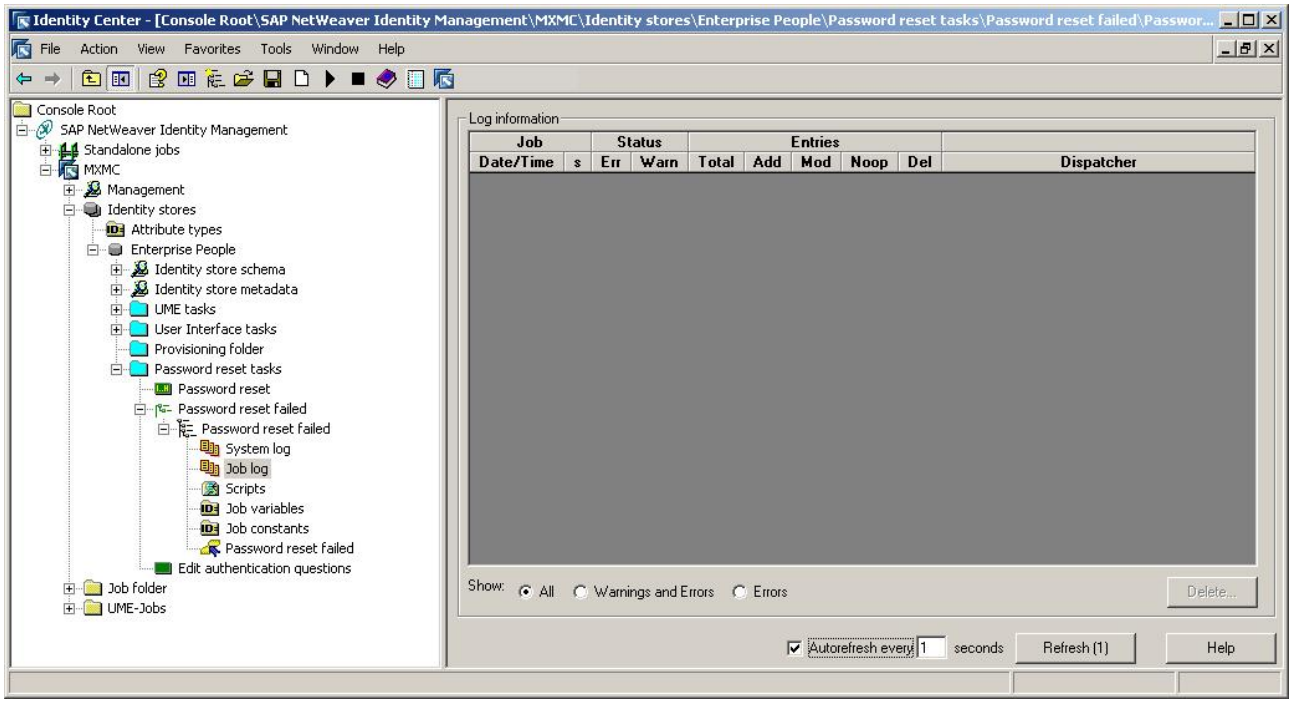


The password is now reset.

Testing the task "Password reset failed"

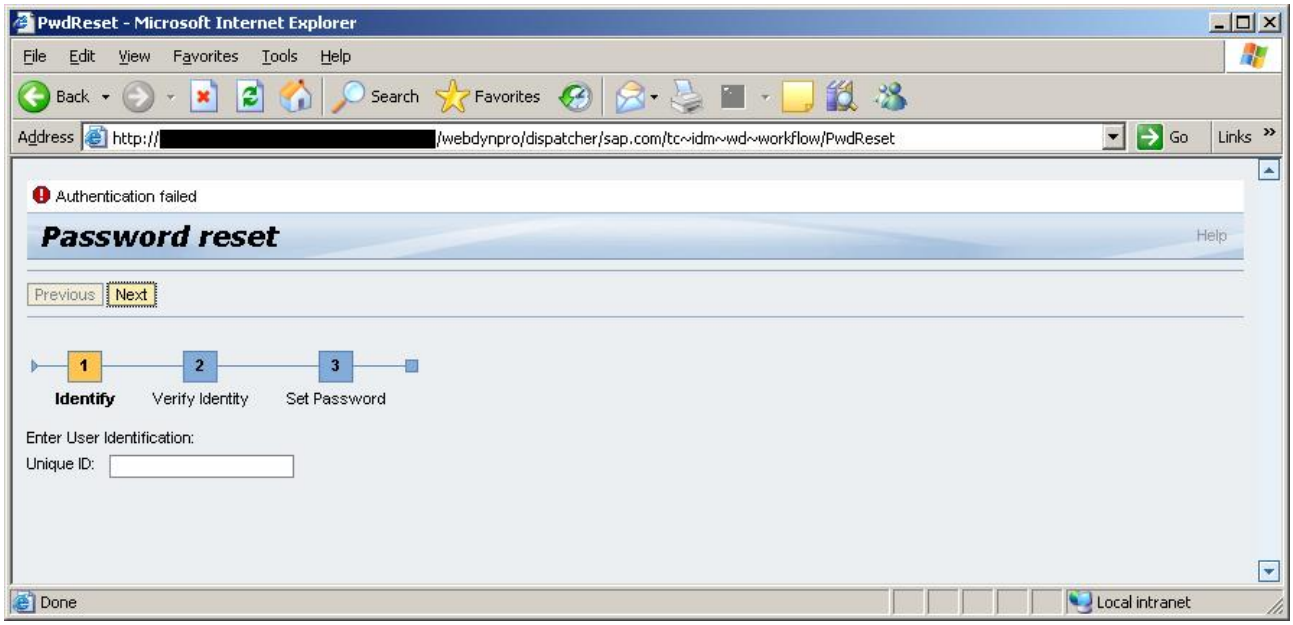
To test and verify that the "Password reset failed" task works, do the following:

1. Navigate to and select the "Password reset failed" job log.

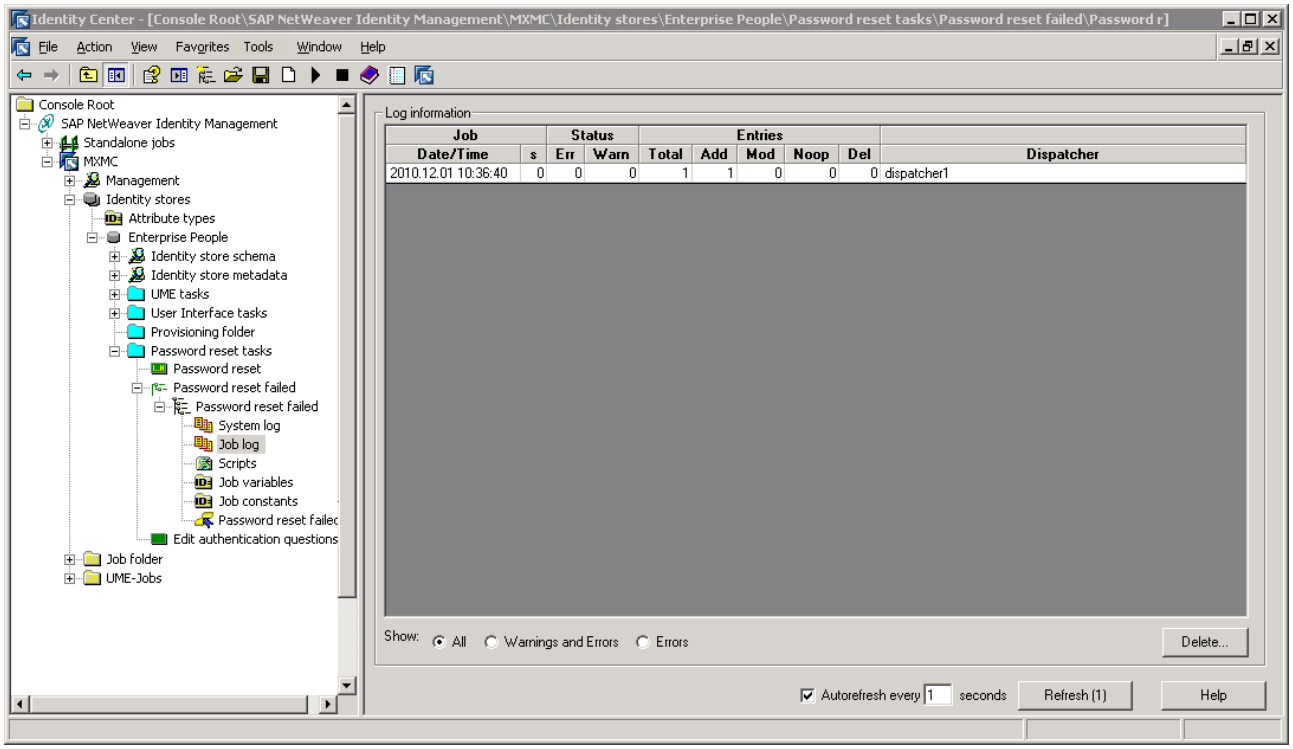


Select the auto-refresh feature in the job log and set it to 1 second.

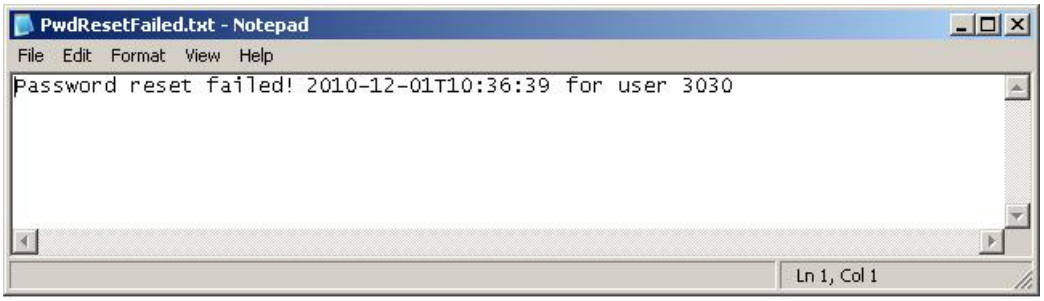
2. Open your browser and enter http://<host>:<port>/idm/pwdreset to access the password reset self-service task, enter the unique ID and then enter wrong credentials (i.e. the wrong answers to the authentication questions) to cause authentication error:



3. Inspect the job log to verify that the job has run without errors:



4. Also check the defined location of the file to verify that the file was created with the expected input. The file may look something like this:



Note:
Every failed attempt of password reset is logged. For security reasons the user is not told why a password reset attempt failed, if too many attempts are made to reset the password or if the provided unique identifier does not exist, as this would provide a potential attacker with additional information. Instead, the password reset will proceed but random authentication questions may be displayed to the user (including the ones that user has not defined the answers for) and the password reset will fail regardless of the input information being correct or not.

Note:
Aborting the self-service password reset (e.g. by closing the browser window) while in Step 2 (Verify Identity) or Step 3 (Set Password) will count as a failed password reset attempt, but this type of failed password reset attempt will not be recognized by the "Password reset failed" task and thus not be logged to the specified file.

Section 5: Changing the authentication questions

As previously mentioned, the authentication questions are by default:

- What is your favorite color? (*MX_AUTHQ_001*)
- What make of car do you drive? (*MX_AUTHQ_002*)
- What is your pet's name? (*MX_AUTHQ_003*)
- What is your mother's maiden name? (*MX_AUTHQ_004*)
- What street did you grow up on? (*MX_AUTHQ_005*)

The questions may be changed by changing the display name of attributes *MX_AUTHQ_001* to *MX_AUTHQ_005*. This change of questions should be done during the implementation of the self-service password reset, before the task allowing the users to enter answers to the authentication questions is available for the users. Changing the questions after the users have provided their answers will cause the answers not to fit well any more.

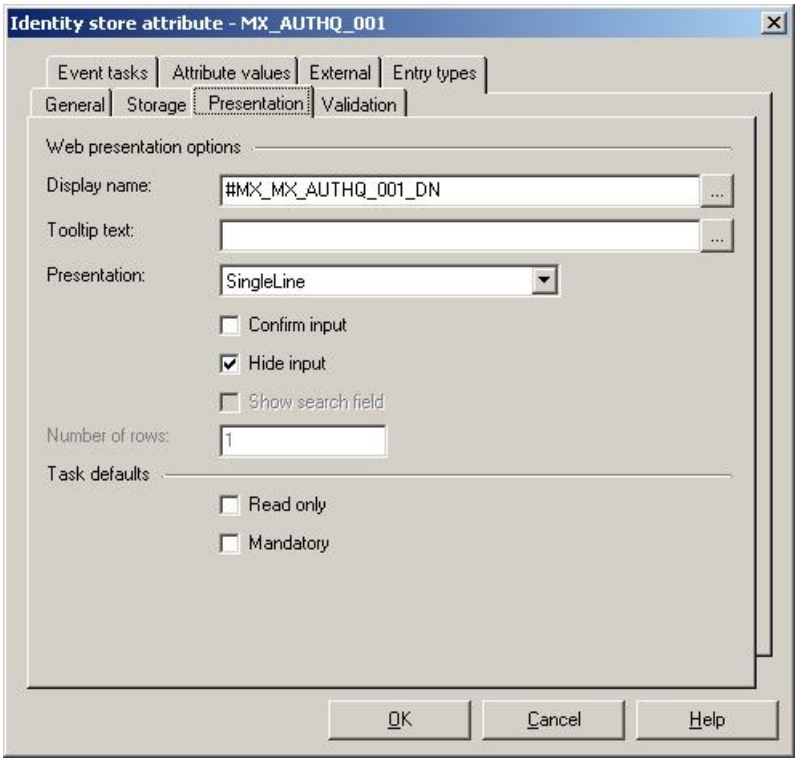
Note:
The display names of the authentication questions are determined by the language dependable text keys #MX_MX_AUTHQ_001_DN to #MX_MX_AUTHQ_005_DN available for a set of languages, and they are presented in language selected for your Identity Center. Changing the display name of the authentication question will replace this language dependable text key with your own text key with a value of your choice in a language of your choice.

To change the authentication questions, do the following:

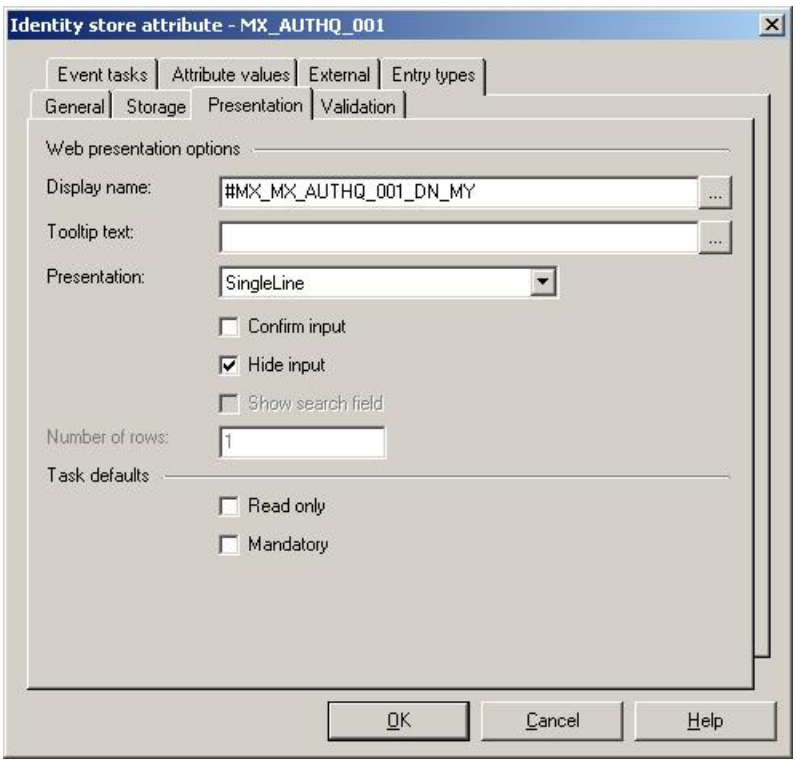
1. Navigate to and select "Attributes" for your identity store in the console tree.

   All attributes in your identity store will be listed.

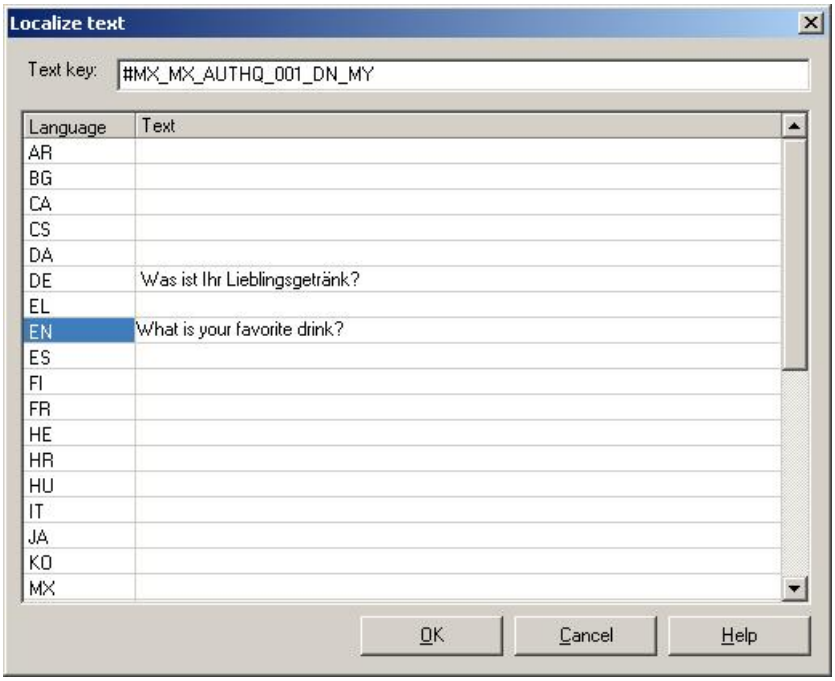
2. Navigate to and view the properties of the attribute you wish to change, e.g. the attribute *MX_AUTHQ_001*, and select the "Presentation" tab:



3. In the "Display name" field, alter the displayed text key to (make your own) e.g. "#MX_MX_AUTHQ_001_DN_MY":



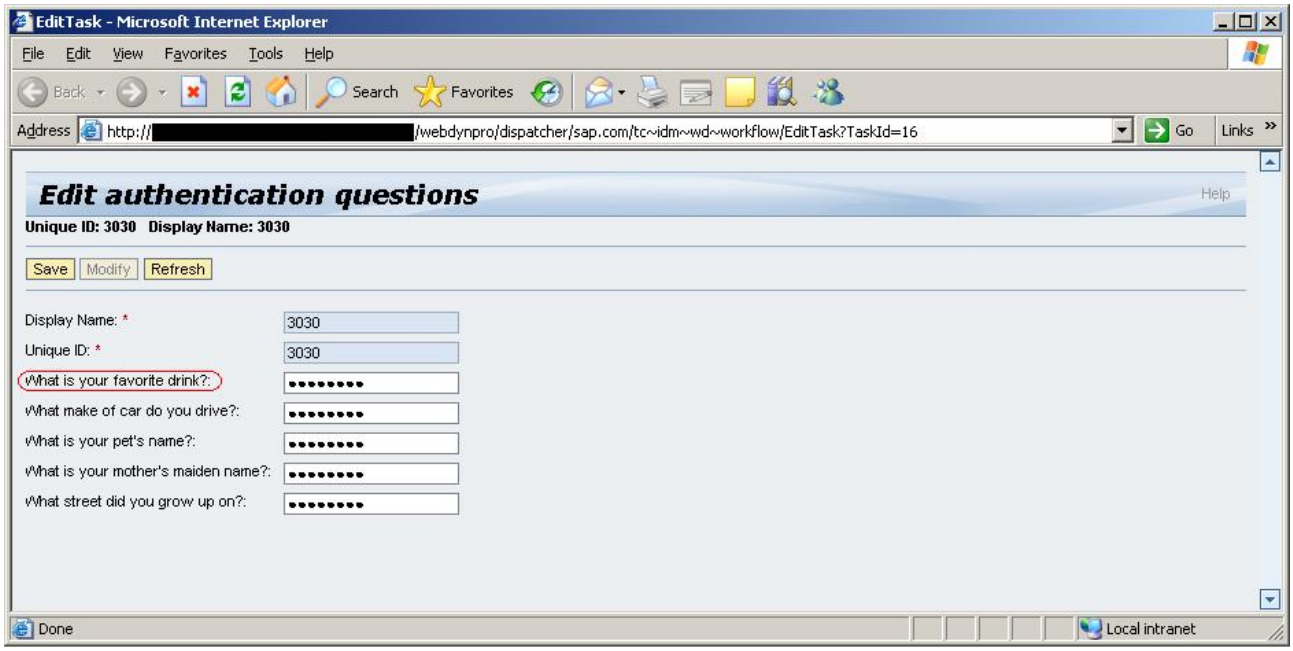
4. Choose "…" to define the values for the new text key.



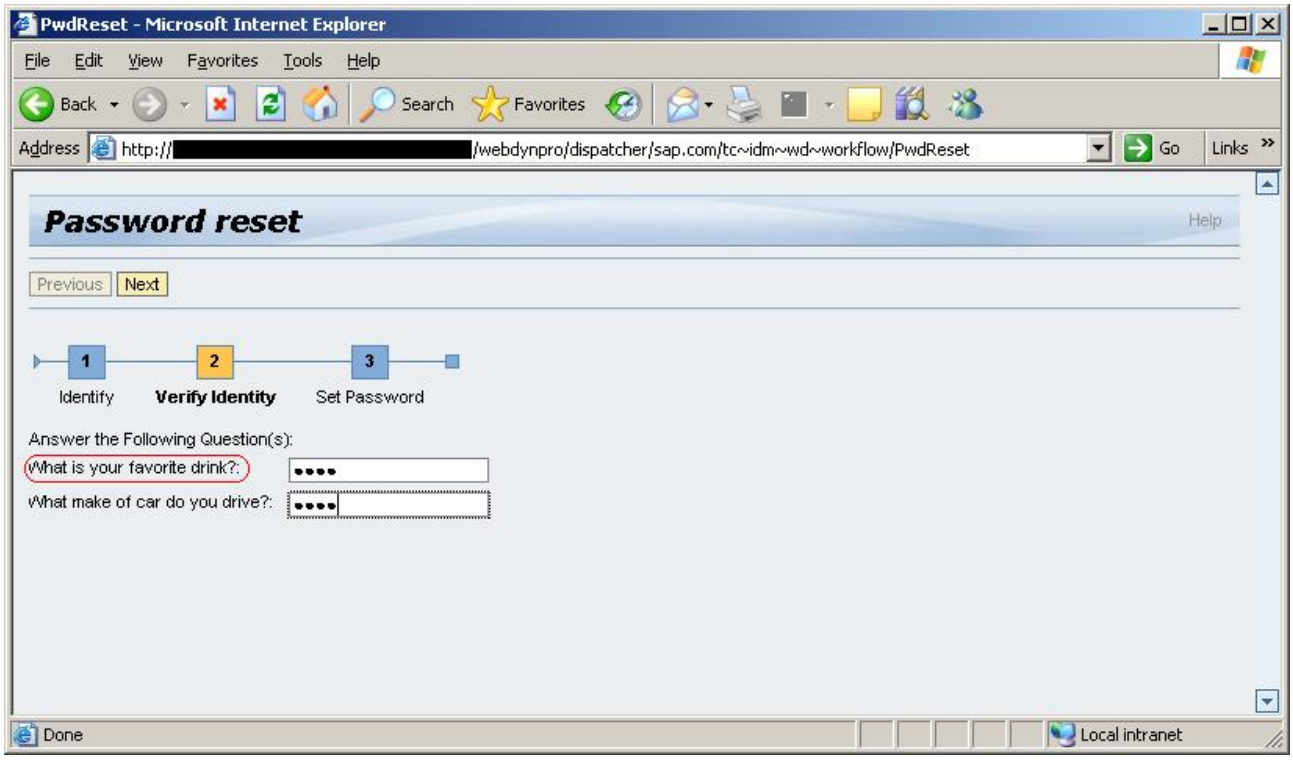
Enter the authentication question changes for the languages of interest (in this example the changes are defined for English and German).

5. Choose "OK" to confirm and close the dialog box.

You have now changed the question from "What is your favorite color?" to "What is your favorite drink?". You can observe the change in the self-service task where the user defines the answers to the authentication questions:



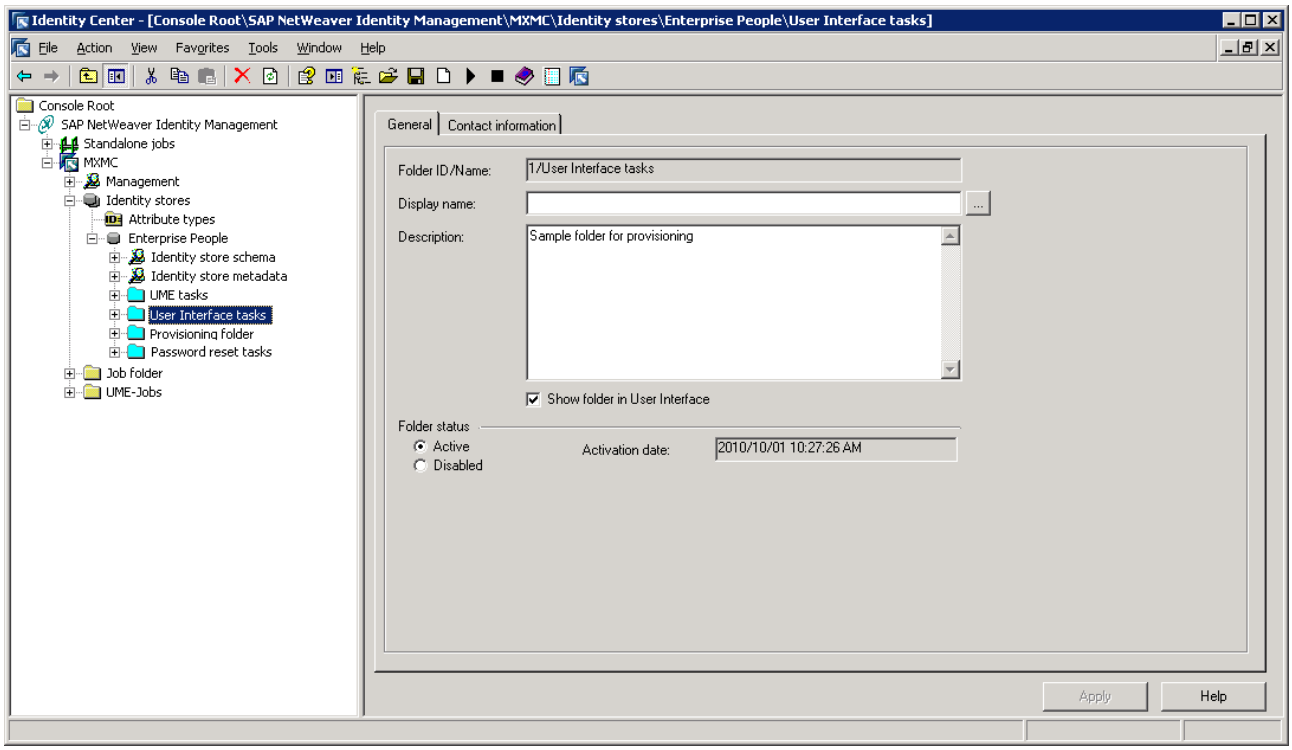
The change is also visible in the password reset task:



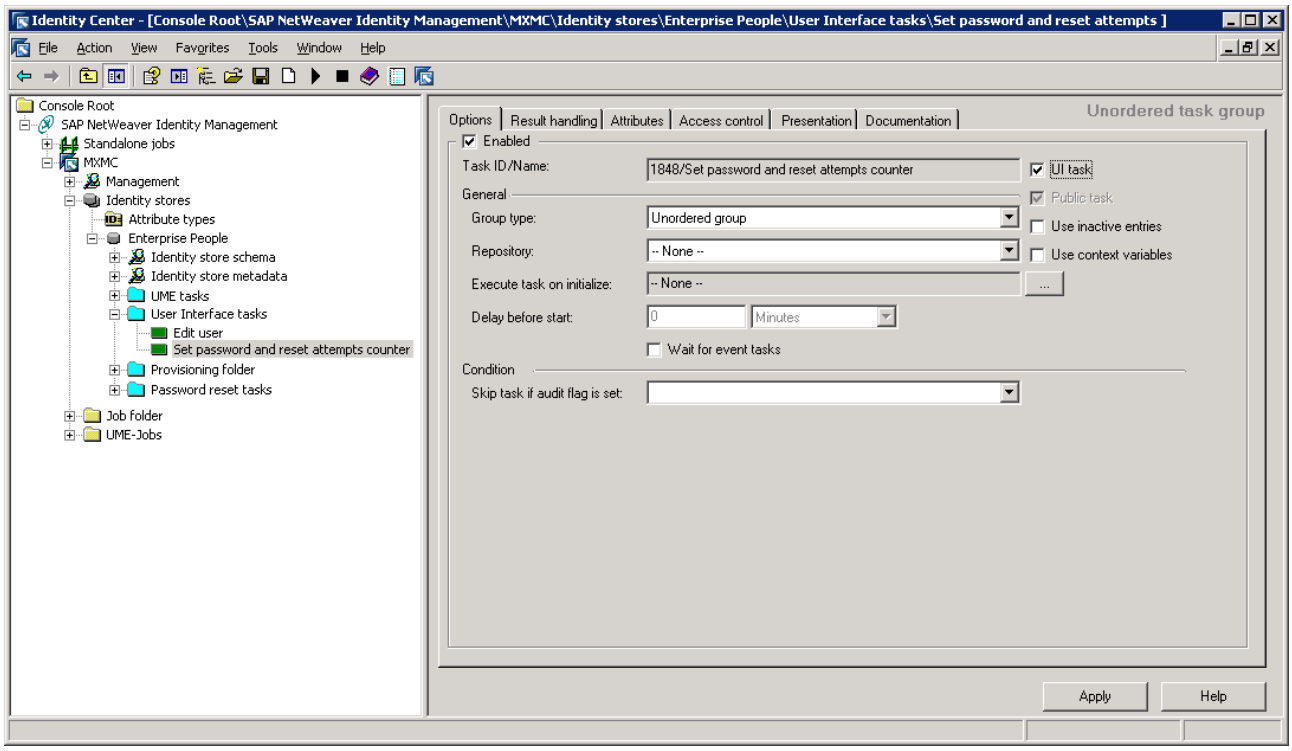
Section 6: Resetting the number of failed password reset attempts

If a user has exceeded the maximum number of failed password reset attempts, the number must be reset (cleared). A task can be created for setting of password for the user and resetting of the number of attempts. Do the following:

1. Select a folder visible from the User Interface (a folder where "Show folder in User Interface" is selected) – here folder "User Interface tasks".



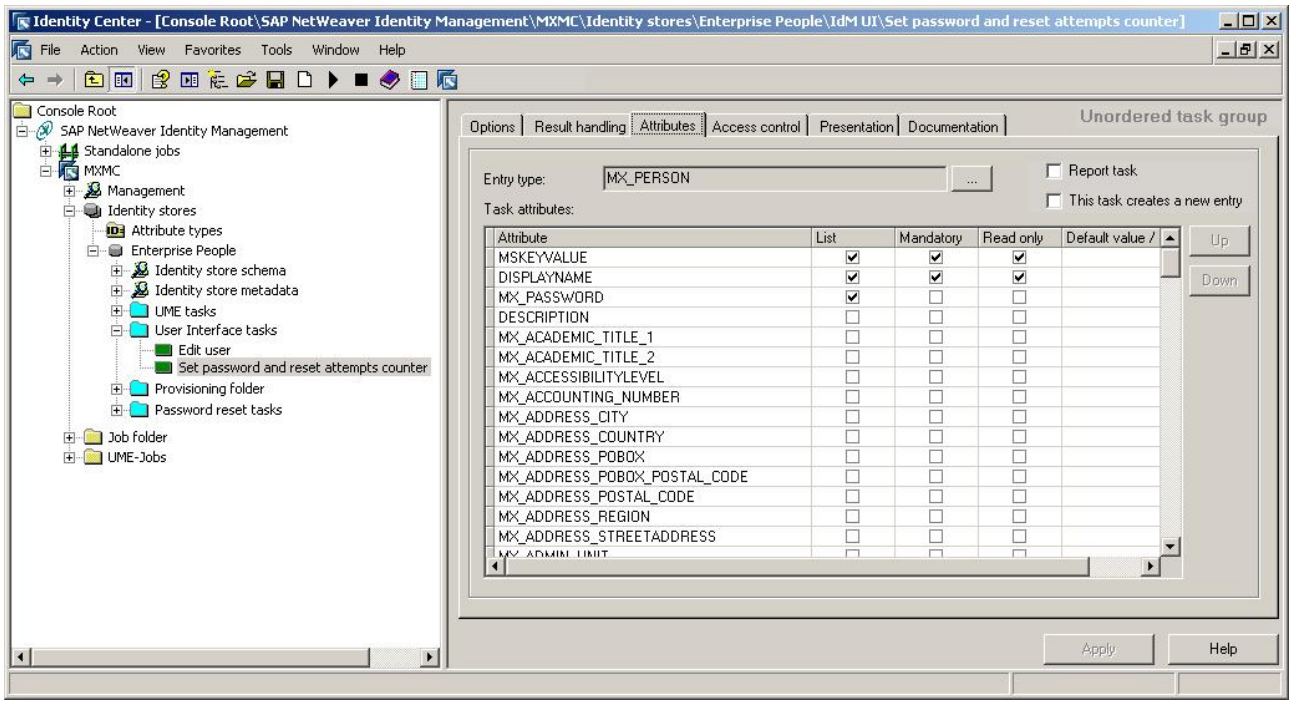
2. Choose **New/Unordered task group**. (As of SAP NetWeaver Identity Management 7.2 SP9, you can choose only ordered task group.)



Modify the name of the task in the console tree.

Select the "UI task" option.

3. Select the "Attributes" tab:

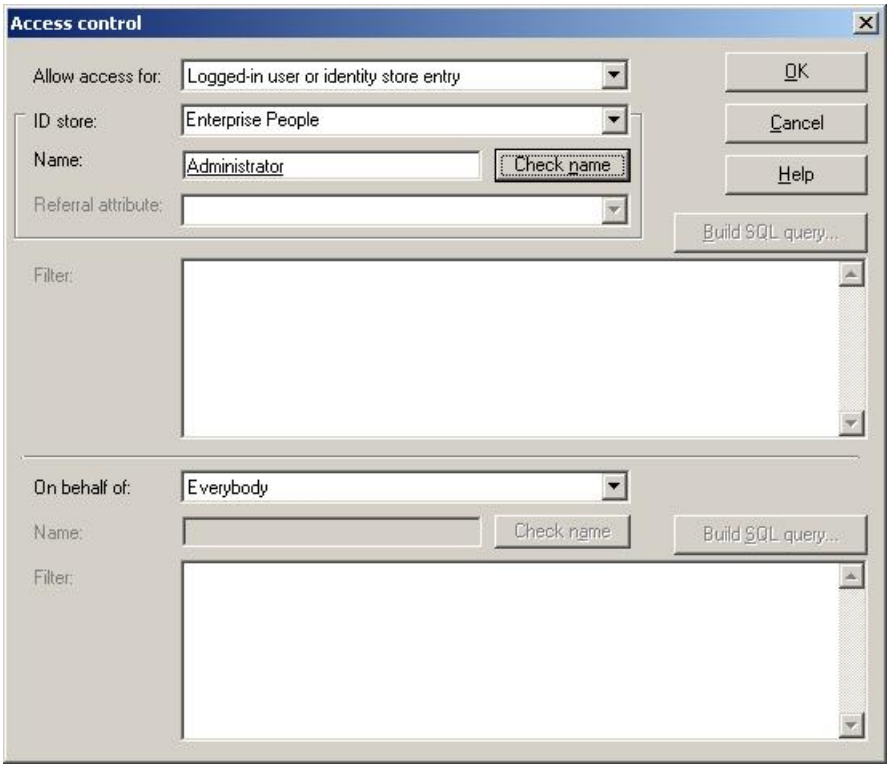


Select "MX_PERSON" as entry type.

Note:
A dialog box will appear asking you to confirm your choice. Choose "Yes" to confirm and to close the dialog box.

Configure the attributes for the task as displayed above. Use "Up" (or "Down") to place the attributes in the exact same order as shown in the picture above.

4. Choose "Apply".
5. Select the "Access control" tab and choose "Add…".



Select "Logged-in user or identity store entry" in the "Allow access for" list.

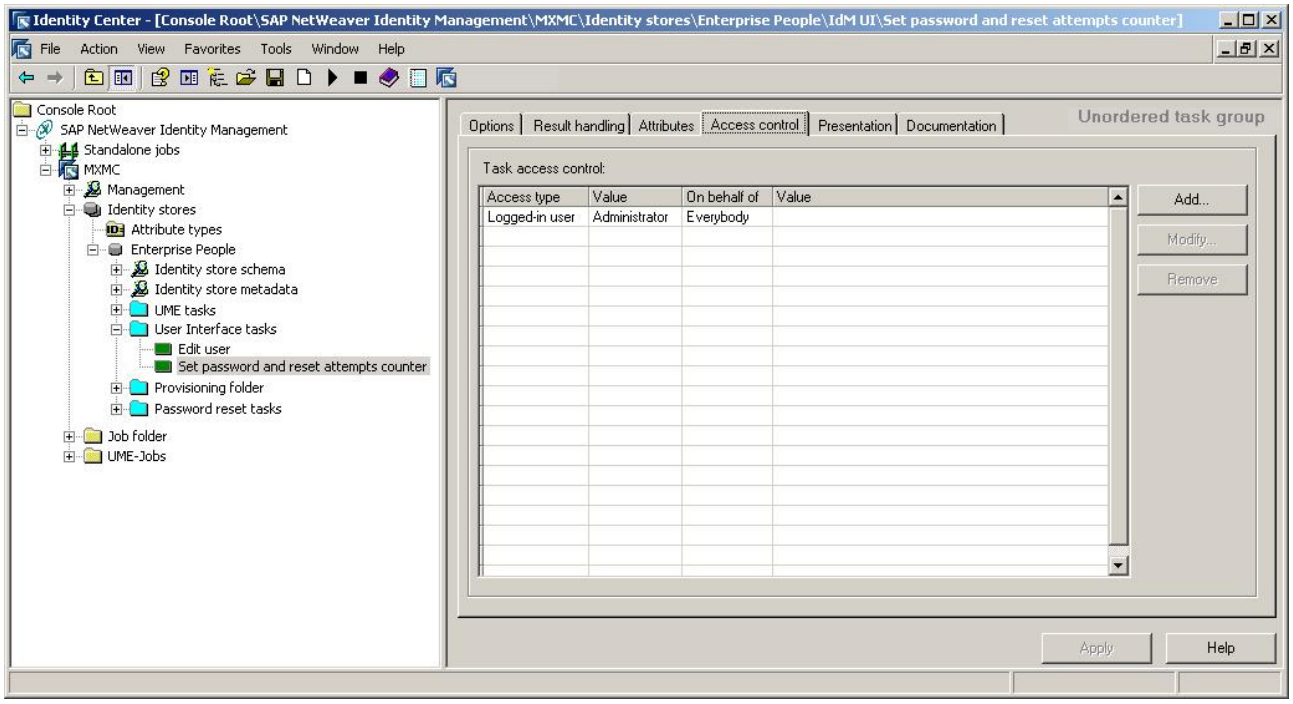
Make sure that the correct identity store is selected.

Enter the name of the identity store user with the access to the "Manage" tab in the User Interface (here *Administrator*). You might use "Check name" to ensure that the name you entered is correct and exists. This allows the administrator user access to the task.

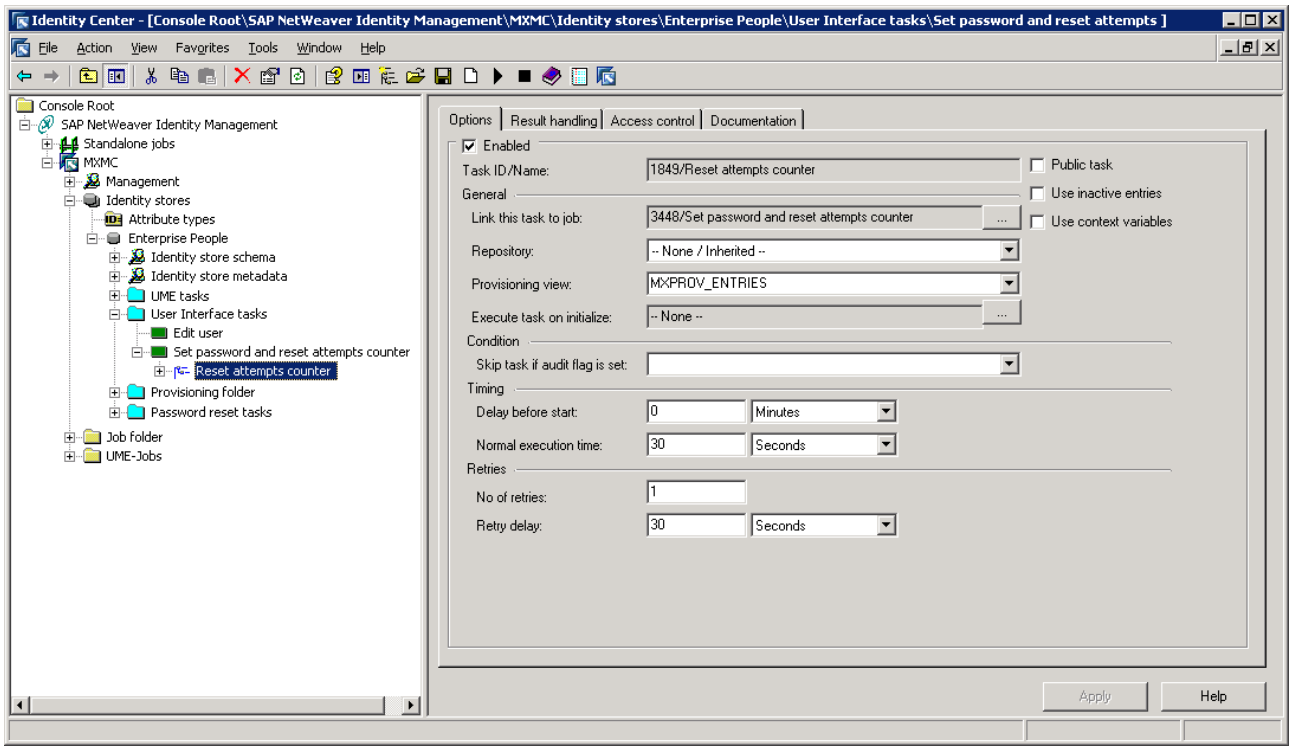
Select "Everybody" in the "On behalf of" list.

6. Choose "OK".

The resulting access control is displayed in the details pane.

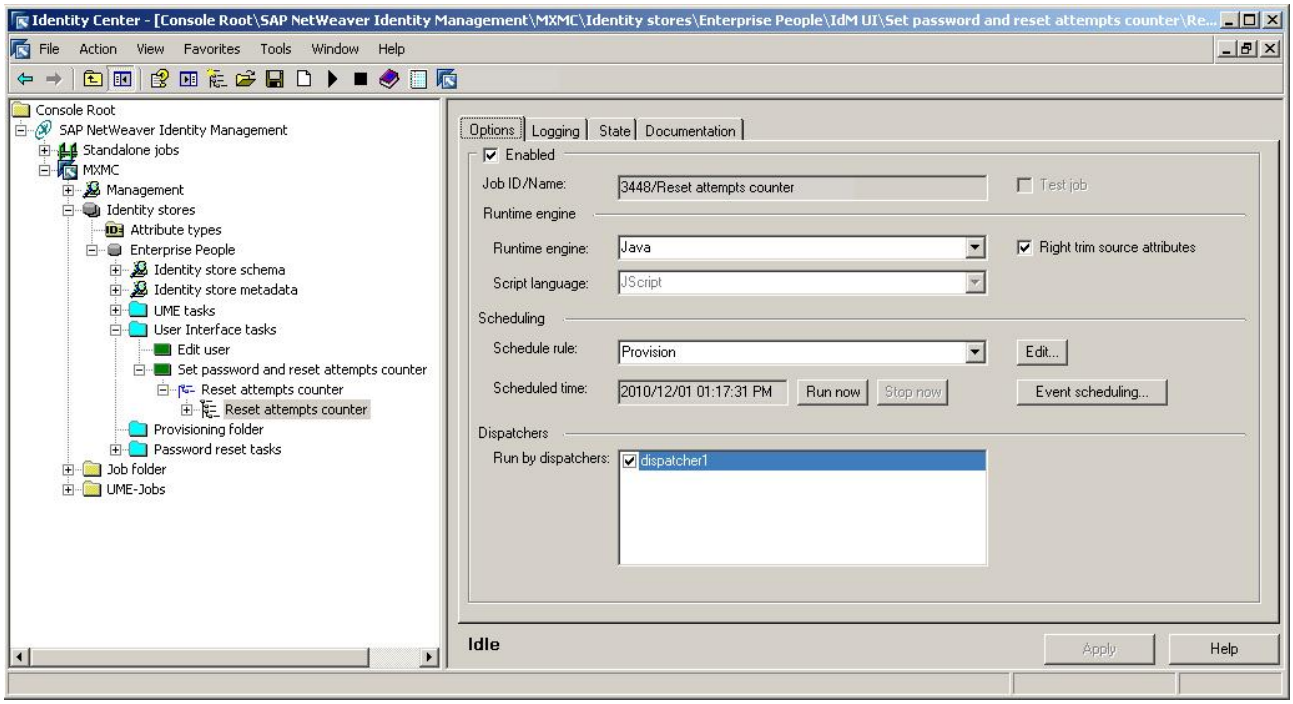


7. Choose "Apply".
8. Select the task in the console tree and choose **New/Action task/Empty job** in the context menu.



Modify the name of the task in the console tree.

9. Select the job in the console tree.



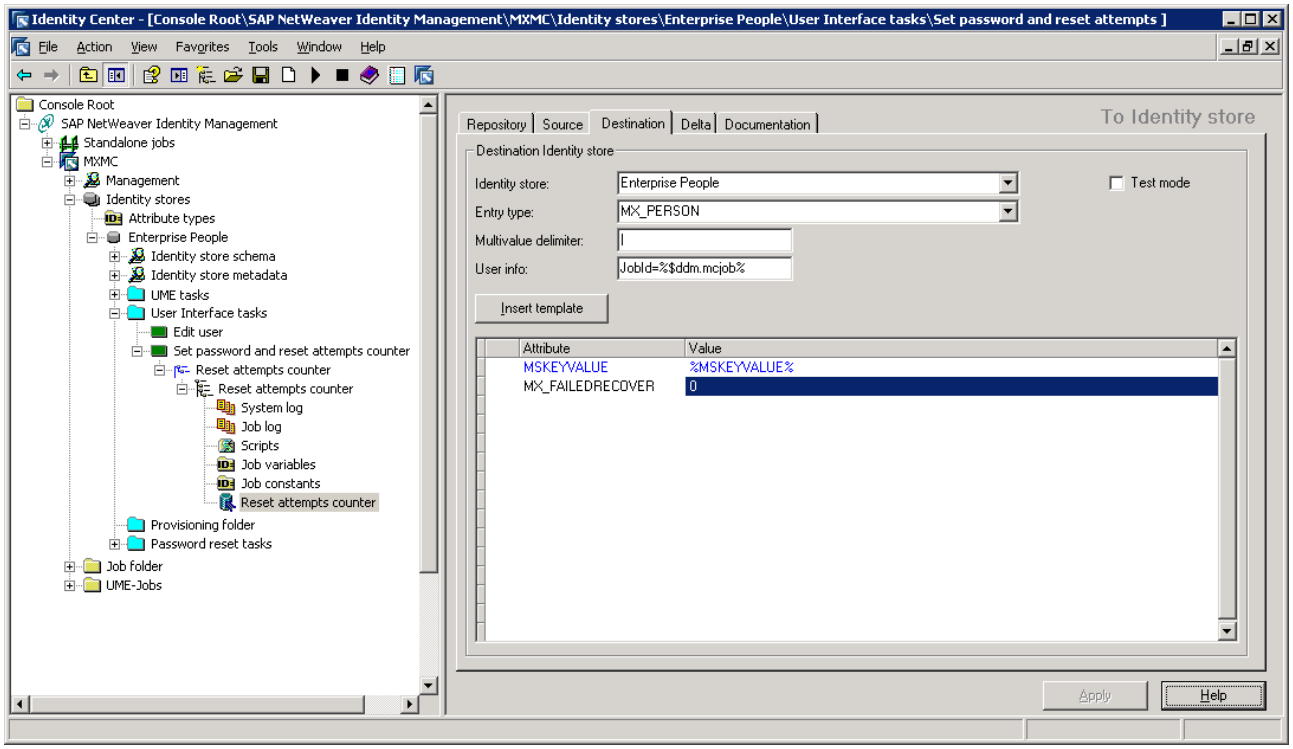
Modify the job name in the console tree and the following job properties:

Enabled
Select this check box to enable the job to be run by a dispatcher.

Run by dispatchers
Select a dispatcher that should be responsible for running this job.

10. Choose "Apply".

11. Select the job in the console tree and choose **New/To Identity store** from the context menu.



In the "Destination" tab modify the following:

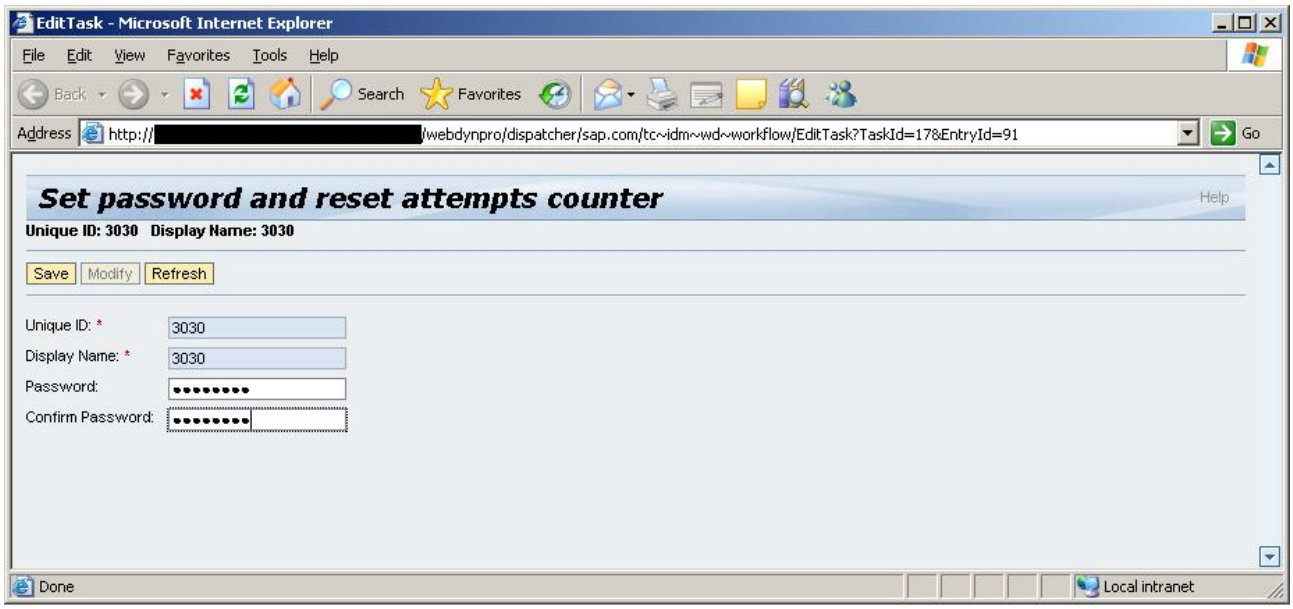
Identity store
Make sure the correct identity store is selected.

Entry type
Select entry type *MX_PERSON*.

Definitions
Add the attributes to the definitions as shown in the picture above (you can use the context menu to insert the attributes).

12. Choose "Apply".

    The task is now created and can be used. When entered in the User Interface the task will look like this:



The password can be set for the user and the number of failed attempts will be automatically cleared for the given user when the task is saved (i.e. the job *Reset attempts counter* will be run).

View the job log to verify that the job executed without errors: