EVIDEN

Identity and Access Management

DirX Identity

Password Management

Version 8.10.12, Edition August 2025

Table of Contents

Preface

DirX Identity **Web Center for Password Management** is a Web application that provides password change and password reset functionality for end users and service desk members. The application runs on Apache Tomcat and can be accessed by supported Web browsers. Web Center for Password Management is only available with the Password Management license. Its configuration and functions overlap with the full Web Center application.

This document describes the configurations and functions that are specific to Web Center for Password Management. It consists of the following chapters:

- Chapter 1 provides an overview of Web Center for Password Management features and functions and gives decision support information about the product.
- Chapter 2 describes the procedures for configuring Web Center for Password Management.

DirX Identity Documentation Set

The DirX Identity document set consists of the following manuals:

- *DirX Identity Introduction*. Use this book to obtain a description of DirX Identity architecture and components.
- *DirX Identity Release Notes*. Use this book to understand the features and limitations of the current release. This document is shipped with the DirX Identity installation as the file **release-notes.pdf**.
- *DirX Identity History of Changes*. Use this book to understand the features of previous releases. This document is shipped with the DirX Identity installation as the file **history-of-changes.pdf**.
- *DirX Identity Tutorial*. Use this book to get familiar quickly with your DirX Identity installation.
- *DirX Identity Provisioning Administration Guide*. Use this book to obtain a description of DirX Identity provisioning architecture and components and to understand the basic tasks of DirX Identity provisioning administration using DirX Identity Manager.
- *DirX Identity Connectivity Administration Guide*. Use this book to obtain a description of DirX Identity connectivity architecture and components and to understand the basic tasks of DirX Identity connectivity administration using DirX Identity Manager.
- *DirX Identity User Interfaces Guide*. Use this book to obtain a description of the user interfaces provided with DirX Identity.
- *DirX Identity Application Development Guide*. Use this book to obtain information how to extend DirX Identity and to use the default applications.
- *DirX Identity Customization Guide*. Use this book to customize your DirX Identity environment.
- *DirX Identity Integration Framework*. Use this book to understand the DirX Identity framework and to obtain a description how to extend DirX Identity.
- *DirX Identity Web Center Reference*. Use this book to obtain reference information about the DirX Identity Web Center.
- *DirX Identity Web Center Customization Guide*. Use this book to obtain information how to customize the DirX Identity Web Center.
- *DirX Identity Meta Controller Reference*. Use this book to obtain reference information about the DirX Identity meta controller and its associated command-line programs and files.
- *DirX Identity Connectivity Reference*. Use this book to obtain reference information about the DirX Identity agent programs, scripts, and files.
- *DirX Identity Troubleshooting Guide*. Use this book to track down and solve problems in your DirX Identity installation.
- *DirX Identity Installation Guide*. Use this book to install DirX Identity.
- *DirX Identity Migration Guide*. Use this book to migrate from previous versions.

Notation Conventions

Boldface type
In command syntax, bold words and characters represent commands or keywords that must be entered exactly as shown.

In examples, bold words and characters represent user input.

Italic type
In command syntax, italic words and characters represent placeholders for information that you must supply.

[ ]
In command syntax, square braces enclose optional items.

{ }
In command syntax, braces enclose a list from which you must choose one item.

In Tcl syntax, you must actually type in the braces, which will appear in boldface type.

|
In command syntax, the vertical bar separates items in a list of choices.

...
In command syntax, ellipses indicate that the previous item can be repeated.

userID_home_directory
The exact name of the home directory. The default home directory is the home directory of the specified UNIX user, who is logged in on UNIX systems. In this manual, the home pathname is represented by the notation *userID_home_directory*.

install_path
The exact name of the root of the directory where DirX Identity programs and files are installed. The default installation directory is *userID_home_directory*/**DirX Identity** on UNIX systems and **C:\Program Files\DirX\Identity** on Windows systems. During installation the installation directory can be specified. In this manual, the installation-specific portion of pathnames is represented by the notation *install_path*.

dirx_install_path
The exact name of the root of the directory where DirX programs and files are installed. The default installation directory is *userID_home_directory*/**DirX** on UNIX systems and **C:\Program Files\DirX** on Windows systems. During installation the installation directory can be specified. In this manual, the installation-specific portion of pathname is represented by the notation *dirx_install_path*.

dxi_java_home
The exact name of the root directory of the Java environment for DirX Identity. This location is specified while installing the product. For details see the sections "Installation" and "The Java for DirX Identity".

tmp_path

The exact name of the tmp directory. The default tmp directory is /tmp on UNIX systems. In this manual, the tmp pathname is represented by the notation *tmp_path*.

tomcat_install_path
The exact name of the root of the directory where Apache Tomcat programs and files are installed. This location is defined during product installation.

mount_point
The mount point for DVD device (for example, **/cdrom/cdrom0**).

1. Overview

The DirX Identity Web Center for Password Management is a licensed package that provides a separate Web application intended for password management only. It offers the following features:

- Users can choose different passwords for different accounts.
- Service desk users can change a user password after having verified the user's challenge responses.

The overall principle is to use one master password that can be synchronized automatically to other target systems. The user can select these accounts. The other accounts can have different passwords. The administrator defines the password master systems. The master systems and the DirX Identity user must have the same password.

The master password can be changed by the user or by the service desk using the challenge/response feature.

Definition of password reset and password change:

- Password reset – the system generates a new password, sends it to the user and the user must change the generated password on the next login.
- Password change – the user defines a new password which is valid for the period specified by the password policy's expiration duration.

1.1. Feature Comparison

The following table illustrates the enhanced features of Web Center for Password Management compared to the standard Web Center functionality:

Feature	Web Center (standard)	Web Center for Password Management
Forgot password - Set new password using authentication questions	Yes	Yes
Change password	Yes	Yes
Set authentication questions	Yes	Yes
Login with Active Directory domain account	No	Yes
Synchronize master password for all accounts	Yes	Yes
Set password for only a subset of accounts	No	Yes
Service desk can reset user (master) password	Yes	Yes

Feature	Web Center (standard)	Web Center for Password Management
Service desk can reset user master and account password by verifying user's responses to authentication challenges	No	Yes

As a pre-requisite, the end users and their accounts need to be known to DirX Identity and the system must be configured appropriately.

The following figure illustrates the activity flow in end user and service desk password management:

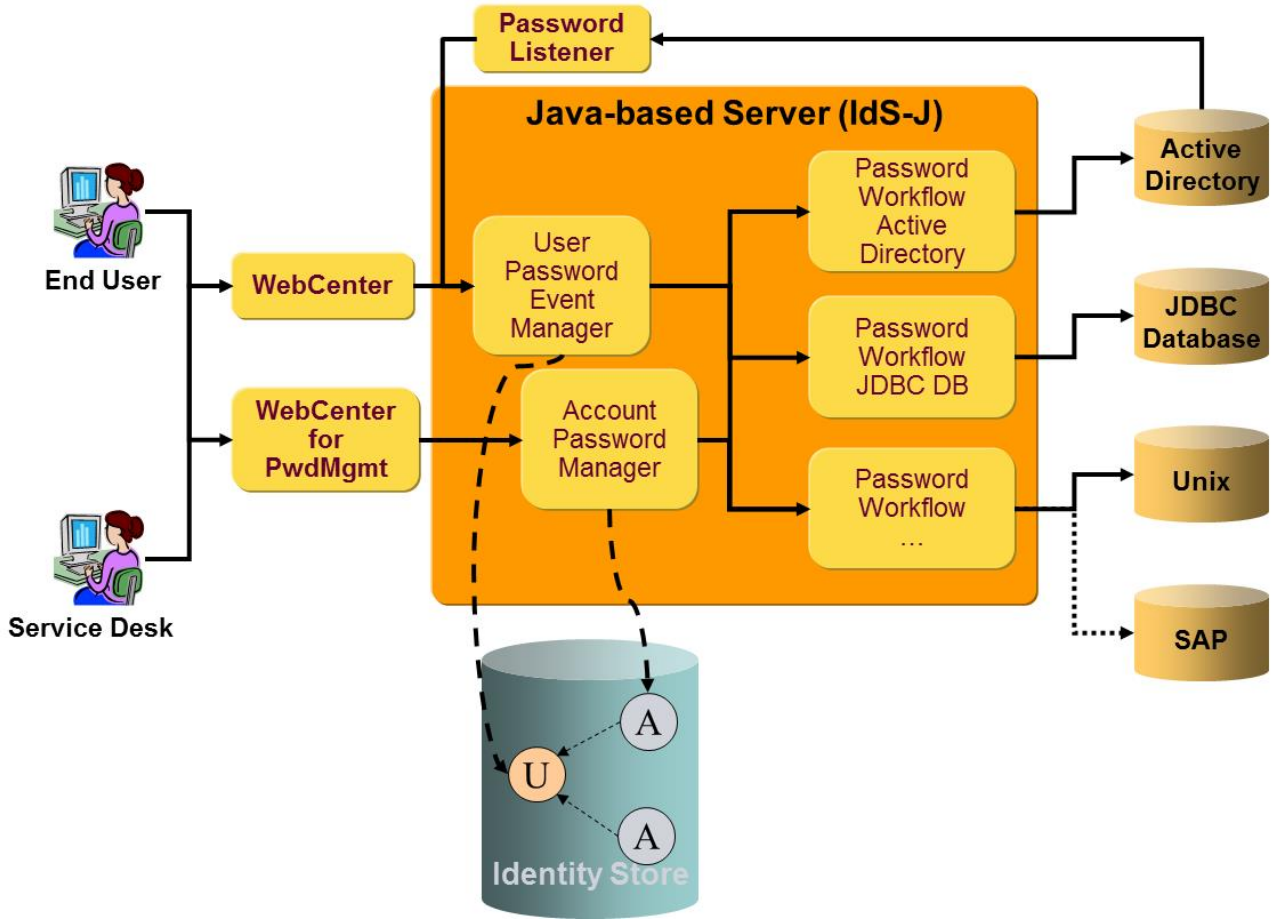

Figure 1. Users, Accounts and Password Changes

As illustrated in the figure:

- End users can change their passwords using Web Center:

  Standard Web Center sends the new password to the DirX Identity Messaging Service. The User Password Event Manager picks it up, changes it at the DirX Identity user entry, finds the user's accounts and requests the appropriate Set Password workflows to update it at the corresponding target systems in real-time.

  The enhancement in Web Center for Password Management allows users to select a subset of their accounts for password change; the message with the new password is

sent to the Account Password Manager workflow. It changes the password at the listed accounts and requests the appropriate Set Password workflows to update it at the corresponding target systems in real-time.

- End users can change their passwords in an Active Directory domain instead of using the Web Center user interface:

  The DirX Identity Password Listener obtains the changed password from the Active Directory domain controller and sends it to the DirX Identity Messaging Service. The User Password Event Manager picks it up, finds the associated user entry in DirX Identity and updates the password there. Then it finds the user's accounts - except for the Active Directory domain – and triggers the Set Password workflows for each corresponding target system. Note that in this case the new password is set for all accounts.

When end users change their passwords in an external LDAP server, they will not be synchronized to DirX Identity and thus both passwords will be different.

1.2. Related Documentation

The following documents provide additional details about the concepts and procedures referenced in this use case document:

- *DirX Identity Web Center Reference*, chapters "Configuration" and "User Interface Configuration". To secure Web Center against attacks, see especially the chapter on Security.
- *DirX Identity User Interfaces Guide*, especially the chapters on Web Center and Web Center for Password Management.
- *DirX Identity Installation Guide*, especially chapters 3 (installation) and 4 (configuration) and the section "Installing the Windows Password Listener".
- *DirX Identity Connectivity Administration Guide*, chapters/sections:
  - "Managing Connectivity Security"
  - "Managing Java-based Provisioning Workflows"
  - "Understanding Password Synchronization" in "Managing Passwords"
- *DirX Identity Tutorial*, chapter "Joining Accounts to Users" in "Getting Started / Setting up a New Target System". This chapter describes – among other things – how to set up the Policy Execution workflow to run a consistency rule.
- *DirX Identity Provisioning Administration Guide*, chapters:
  - "Managing Policies"
  - "Managing Target Systems"
- *DirX Identity Application Development Guide*, sections:
  - "Active Directory" in "Using the Source Workflows / Understanding the Java-based Source Workflows"

- "Scheduled Workflows" in "Understanding the Default Applications / Understanding Java-based Workflows / Java-based Workflow Architecture / Starting Java-based Workflows"
- "Understanding the Java-based Workflows" in "Using the Target System (Provisioning) Workflows"
- "Using Password Event Manager Workflow" in "Using the Maintenance Workflows / Understanding the Java-based Maintenance Workflows"
- "User Password Expiration Notification Workflow" in "Using the Maintenance Workflows / Understanding the Java-based Maintenance Workflows"
- "Policy Execution Workflow" in "Using the Maintenance Workflows / Understanding the Tcl-based Maintenance Workflows"

2. Configuration

This chapter provides an overview of required and optional configurations for Web Center for Password Management. Details common to both Web Centers are described in the *DirX Identity Web Center Reference Guide*.

2.1. Installation

The *DirX Identity Installation Guide* provides a detailed description of the installation procedure. This section lists only the items you should take care of when installing for Password Management.

Choose Licensed Feature Set Dialog:

Make sure that you select Password Management. If you want to use other features of DirX Identity in addition to Password Management, such as User Management, then you should also select Business Suite. If you want to work with roles or need to have approval workflows, then you must also select Professional Suite.

Choose Install Set Dialog:

For Password Management, you need at a minimum: Connectivity Schema, Provisioning Schema, C++-based Server, Message Broker, Java-based Server, Manager and Web Center.

For Password Management, you need at a minimum:

- From the Base Package: Connectivity Schema, Provisioning Schema, C++-based Server, Message Broker, Java-based Server and Manager. If you want to have User Management via Web Center or other features not supported by Web Center for Password Management, select also Web Center.
- From the Password Management Package: Web Center for Password Management.
- From the Connectivity Packages, you will most probably need Active Directory. Make sure you have selected the packages for all the other types of target systems for which you want to change passwords.

2.2. Initial Configuration Wizard

After the installation, the deployment must be configured using the Initial Configuration Wizard. For details on this task, see the *DirX Identity Installation Guide,* chapter *Configuration*.

For Password Management, you need to select and configure the following items at least once (see the **Configuration Options** dialog): Connectivity Schema, Domain Configuration, C++-based Server, Java-based Server, Manager, Web Center for Password Management.

If you also want to have User Management or other features, deploy a full Web Center in addition to Web Center for Password Management.

In the **Domain Configuration** dialog, you should select to configure a customer domain

and provide an appropriate name such as the name of your company or your organization. You can also choose to create a sample domain for testing and learning purposes. The sample domain contains a set of users, roles, business objects and policies that are ready to use. These items are the basis for the *DirX Identity Tutorial*, which guides you through important features.

In order to encrypt passwords in transit and in the DirX Identity domain, you should provide an RSA key pair for the account cn=server_admin,dxmC=DirXmetahub in the Connectivity database; otherwise the passwords are only hashed. See the chapter "Managing Connectivity Security" in the *DirX Identity Connectivity Administration Guide* for details.

2.3. Login Configuration

A login to Web Center for Password Management involves two steps:

- Finding the DirX Identity user that matches the user identification data entered into the login form.
- Authenticating the user by validating the entered password against the DirX Identity database and/or the selected external system.

The login is accepted if the identification step finds exactly one user and the subsequent authentication succeeds.

2.3.1. User Identification

The login form includes an optional authentication domain, a name field, and a password field.

Figure 2. Login form

The user is identified by authentication domain and name, while the password is only relevant for user authentication.

Web Center tries to identify the user in two ways. First, it searches for a matching DirX Identity user. If the search returns a single user, the identification has succeeded. If, on the other hand, the search yields more than one user or no user at all, Web Center checks if an authentication domain has been selected. If so, it searches again for a matching DirX Identity target system account. If that results in exactly one account, Web Center follows the account's *dxrUserLink* attribute to find the user. Otherwise, the identification has failed.

Notes

- The user identification is independent of the user authentication mode (see below).

- Web Center for Password Management does not support multiple name fields (like first name and last name) in the login form.

2.3.1.1. Searching for a DirX Identity User

By default, Web Center searches for the user in the users tree of the DirX Identity domain "`cn=Users,cn=<DXI-Domain>`".

The search filters for all users with state ENABLED, whose login form attribute match the value entered into the name field of the login form. The login form attribute is the one assigned to the name field in the login form definition.

Base object and filter can be customized in file **web.xml** via initialization parameters "`com.siemens.webMgr.auth.userBase`" and "`com.siemens.webMgr.auth.userFilter`", respectively.

Both, search base and filter, support the following placeholders:

- **%USER_ID –** is replaced with the value entered into the name field of the login form.
- **%LOGIN_ATTR** – is replaced with the attribute name assigned to the name field of the login form in file **forms-config.xml**.
- **%MASTER_TS –** is replaced with the authentication domain selected in the login form.

There's no placeholder for the DirX Identity domain; you must enter it explicitly.

In any case, whether default or customized, the filter is extended to find users in state ENABLED only.

Sample:

With login attribute *cn* and default search base and filter for the *My-Company* domain, the data entered into the login form shown above result in a search for users below

- `cn=Users,cn=My-Company`

with filter

- `(&(objectclass=dxrUser)(cn=Klarmann Bruno)(dxrState=ENABLED))`.

The filter corresponding to the data in the login form shown below is

- `(&(objectclass=dxrUser)(cn=bklarm12)(dxrState=ENABLED))`.

2.3.1.2. Searching for a DirX Identity Account

The search base for the account search is the selected target system. If no target system is selected, the search is skipped.

The search filters for all accounts with state in target system ENABLED and whose login

form attribute matches the value entered into the name field of the login form. The login form attribute can be configured per target system. The default attribute is *dxrName* for target systems of type AD and *cn* for type LDAP.

The attribute name assigned to the login form field in file **forms-config.xml** is ignored here.

Sample:

With login form attribute *dxrName* and default search base and filter for the *My-Company* domain, the following login data

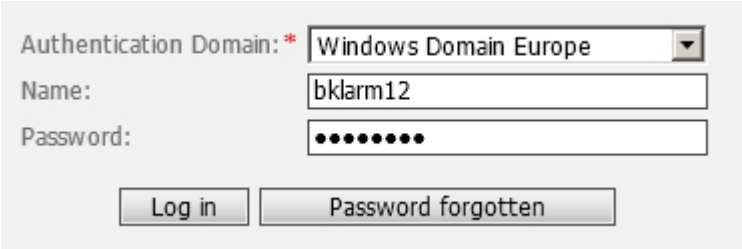

Figure 3. Login form

result in a search for accounts below

- `cn=Windows Domain Europe,cn=TargetSystems,cn=My-Company`

with filter

- `(&(objectclass=dxrTargetSystemAccount)(dxrName=bklarm12)(dxrTSState=ENABLED))`

2.3.2. User Authentication

Web Center for Password Management can combine two ways of authentication.

- **Internal (DirX Identity) authentication**
  The user is authenticated as usual with his DN and password against the DirX Identity provisioning directory. There is no additional configuration necessary.
- **External authentication**
  The user is authenticated against an external system like an LDAP or AD target system. The target system must be defined and configured as a password master via the Identity Manager's Provisioning view. You can define more than one target system for external authentication.

Authentication can work in four different modes to combine external and internal authentication:

- **DXI** – perform the **internal** authentication only. DirX Identity authentication must succeed – no other system is involved in the authentication procedure.
- **EXTERNAL** – perform the **external** authentication only.

- **ONE** – at least one authentication (**either internal or external**) must succeed, whereas both authentications are configured.
- **BOTH** – both authentications (**internal and external**) must succeed. If one of both authentications fails, the user is not successfully authenticated.

The authentication mode is configured in file **web.xml** (section of authentication modes) of Web Center for Password Management. The default mode is “DXI” (internal authentication only).

2.3.2.1. External Authentication

External authentication requires that you have defined one or more target systems as password masters.

A user is successfully authenticated against a target system if

- The user has an account in the target system.
- The account’s state in the target system is ENABLED.
- Authenticating against the connected system succeeds.

Otherwise authentication against the target system fails.

When a user logs in, Web Center performs external authentication by following the first step that applies:

- If the user has explicitly selected an authentication domain in the login form, he is authenticated against the selected target system. If the authentication succeeds, external authentication succeeds. If it fails, external authentication fails.
- If a preferred authentication domain is assigned to the user, he is authenticated against the assigned target system. If the authentication succeeds, external authentication succeeds. If it fails, external authentication fails.
- Web Center for Password Management tries to authenticate the user sequentially against all master target systems in which the user has an account. On first success external authentication succeeds. If all authentications fail, external authentication fails.
- If the user doesn’t have any account in a master target system, external authentication fails.

2.3.3. Configuring External Authentication

In external authentication, one of the target systems must act as a password master system – it performs external authentication for Web Center for Password Management.

There are two locations to configure:

- DirX Identity Manager → Provisioning → *target system* → Advanced tab → Password Management
- File system folder of Web Center for Password Management

The sample configurations described in this section provide setups of external authentication for Active Directory and the LDAP target system Intranet as master target systems for external authentication.

This section also describes how to configure Web Center for Password Management's login page for external authentication.

2.3.3.1. Configuration in Identity Manager

The configuration of an external system as password master must be done by the administrator. The configuration is located in the target system's Advanced tab under the Password Management section, as shown in the following figure.

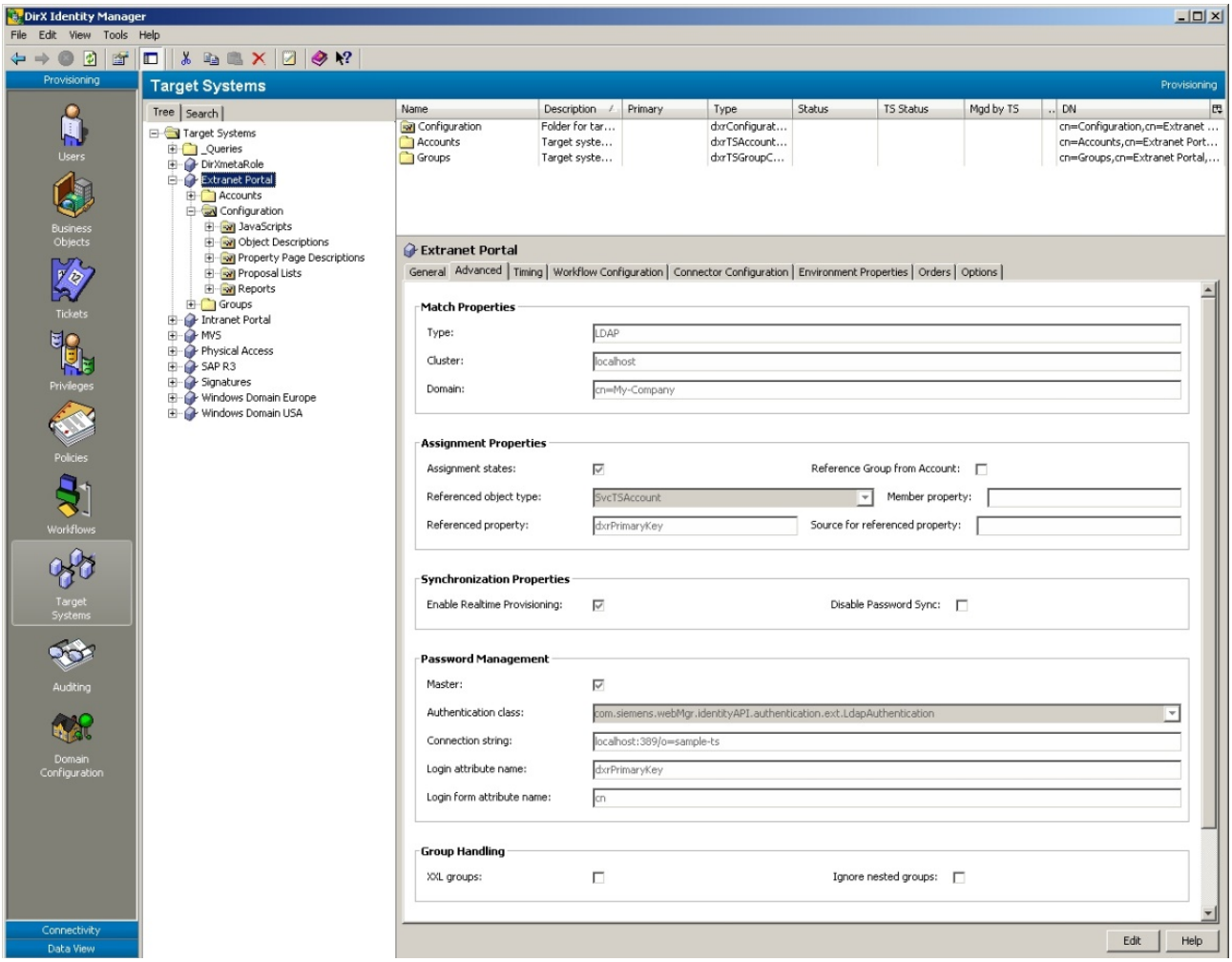

Figure 4. Customizing a Target System with DirX Identity Manager

The following parameters must be specified in DirX Identity Manager at the corresponding target system in the Advanced tab:

- **Master** - if checked, it enables external authentication. The target system is considered as the master for user authentication. Password synchronization must be enabled (Disable Password Sync unchecked).
- **Authentication class** - the class used for external authentication. The class must implement the interface

com.siemens.webMgr.identityAPI.authentication.ext.Authentication and has to be deployed in the WEB-INF/lib directory of Web Center. There are the following built-in classes for LDAP and Active Directory authentication that can be used out-of-the-box:

- **com.siemens.webMgr.identityAPI.authentication.ext.AdAuthentication**
- **com.siemens.webMgr.identityAPI.authentication.ext.LdapAuthentication**
- **Connection string** - the connection string (domain) for external authentication. For the built-in classes LDAP and Active Directory the syntax is [*protocol://*]*host*[:_port_][*/dn*], for example *localhost:389* or *ad.my-company.com* or, for SSL connections, *ldaps://ad.my-company.com*. The default protocol is *ldap*, the default ports are 389 for *ldap* and 636 for *ldaps*. For other connected systems the custom authentication class defines the syntax. The string is passed to the authentication class before authentication of a user.
- **Login attribute name** – the name of the DirX Identity account attribute that holds the login in the connected system with respect to the authentication class. This overrides the defaults in the implementation of the authentication class. Default for AD and LDAP is *dxrPrimaryKey*.
- **Login form attribute name** – the name of the DirX Identity account attribute that holds the user identification entered into the login form. This overrides the defaults in the implementation of the authentication class. Default for AD is *dxrName*, default for LDAP is *cn*.

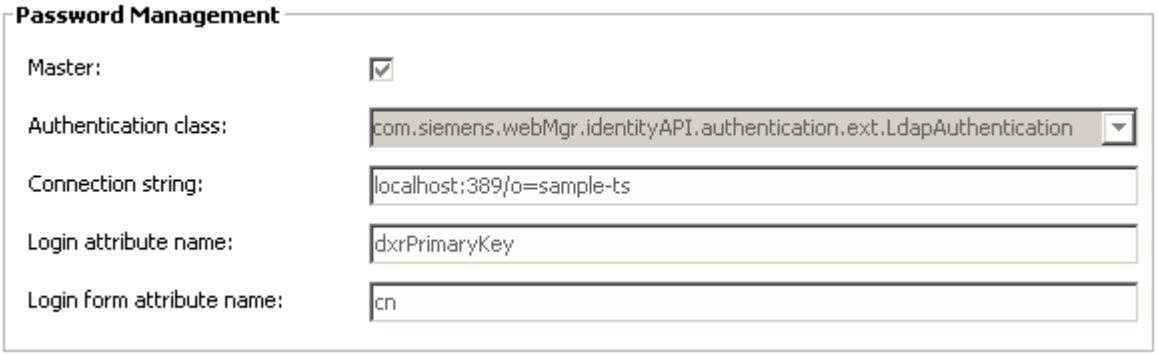

Figure 5. Identity Manager - Target System Configuration

2.3.3.2. Configuration in Web Center for Password Management Folder

You need to edit the following files:

- WEB-INF/web.xml
  - Authentication mode
- WEB-INF/config/webCenter.properties
  - Number of questions for challenge/response
- WEB-INF/configPwd/identity/forms-config.xml
  - Password master selection list on login page
  - User login attribute name

2.3.3.3. Sample Configurations

The following sample configurations describe how to set up external authentication for Active Directory, the LDAP target system Intranet Portal and a custom target system as master target systems for external authentication.

2.3.3.3.1. Active Directory as Master TS

Perform the following steps to set up Active Directory as the master target system for external authentication:

1. Set up external authentication for the target system **Active Directory**:
   In DirX Identity Manager → Provisioning, create a target system for Active Directory. In the Advanced tab, check the **Master** box of **Password Management** to enable external authentication. Enter the authentication class **com.siemens.webMgr.identityAPI.authentication.ext.AdAuthentication** in the **Authentication class** field. Enter your Active Directory domain in the **Connection string** (domain) field. For LDAP over SSL to Active Directory, enter "ldaps://", followed by the domain, and copy the certificate of the Active Directory server or an appropriate CA Root certificate into the SSL trust store of the Tomcat server. This is by default the **cacerts** truststore of the Java installation used to run Tomcat. You may define a different trust store by setting the Java system properties **javax.net.ssl.trustStore** and **javax.net.ssl.trustStorePassword** in the Tomcat configuration user interface or the Tomcat start script.
2. Set up Provisioning:
   Set up Java validation and password workflows for this target system. If you install the Active Directory controller on the same machine, change the LDAP ports of DirX Directory (for example **1389** instead of **389** and **1636** instead of **636**) and re-configure DirX Identity.
   Set up a user import workflow to import the Active Directory users into the DirX Identity users folder.
   Ensure that the DirX Identity users have the Active Directory login value in the **uid** or another attribute. The attribute name is configured in **web.xml** and **forms-config.xml**.
3. Service Desk Operators:
   Add the Service Desk operators to the DirXmetaRole group **ServiceDeskOperators**.

2.3.3.3.2. LDAP as Master TS

This section describes the steps to set up the target system Intranet Portal in the sample domain My-Company as the master target system for external authentication:

1. Create the domain **sample-ts**:
   For this sample, the domain **sample-ts** represents the LDAP server used for external authentication. In order to populate it with users, update the passwords in the file *install_path*/**basic.input.tcl** and run **Setup.bat** under *install_path**/data/schema/dirx*. Specify the userPassword **dirx** for the accounts in **sample-ts/Intranet**.
2. Set up Provisioning:
   Set up Java validation and password workflows for this target system.
   In DirX Identity Manager, run the synchronization workflows for the target systems Intranet (**Ident_Intranet_Realtime**) and Extranet (**Ident_Extranet_Realtime**).

Set up a user import workflow to import the users from the **sample-ts** folder into the DirX Identity users folder. Ensure that the DirX Identity users have the LDAP DN in the **uid** or another attribute. The attribute name is configured in **web.xml** and **forms-config.xml.**

3. Set up external authentication for the target system **Intranet Portal**:
   In the **Advanced** tab, check the **Master** box of **Password Management** to enable external authentication. Enter **com.siemens.webMgr.identityAPI.authentication.ext.LdapAuthentication** in the **Authentication class** field. Enter **localhost:389/o=sample-ts** in the **Connection string** (domain) field. For LDAP over SSL to the target system enter "ldaps://localhost:636/o=sample-ts" and copy the certificate of the LDAP server or an appropriate CA Root certificate into the SSL trust store of the Tomcat server. This is by default the **cacerts** truststore of the Java installation used to run Tomcat. You may define a different trust store by setting the Java system properties **javax.net.ssl.trustStore** and **javax.net.ssl.trustStorePassword** in the Tomcat configuration user interface or the Tomcat start script.
4. Service Desk Operators:
   Add the Service Desk operators to the DirXmetaRole group **ServiceDeskOperators**.

2.3.3.3.3. Custom Target System as Master TS

Create the target system and set up Java validation and password workflows.

Mark the target system as the master and develop and deploy a custom authentication class.

2.3.3.4. Configuring the Login Page

For external authentication, the login page for Web Center for Password Management can be configured in two modes - with or without the master target system list "Authentication Domain". The following figure shows the login page:

Figure 6. Login Page – Authentication Domain Configuration

The current mode is configured in the **WEB-INF/configPwd/identity/forms-config.xml** file

in the **loginForm** element. Follow the instructions in that file to show or hide the selection list and to enable or disable the various options.

When the list is visible, the user can select the Authentication Domain (master target system). You can define a default domain that is preselected when the login form is displayed (form property attribute “value”).

The first value in the list is <none>. If the user selects <none> the target system for external authentication is automatically determined by some other means (see the section on External Authentication above). To get the <none> option set renderer property “omitNoneOption” to false in the form property configuration. A functionally equivalent alternative to the <none> option is the empty option (renderer property “omitEmptyOption”).

The name field matches either a user attribute or an account attribute. It is used to identify the user trying to login. For details see section “User Identification” above.

Finally, the user enters a **Password** and then clicks **Log in**. If the authentication fails a couple of times, login with password is locked and the user is automatically redirected to a page prompting him to answer authentication questions. This behavior is independent of the specified authentication mode.

When a user has successfully logged in, Web Center checks if he has already entered his authentication questions. If not, Web Center displays a page where he can do that. If the user does not specify any questions, Web Center will ask him again at the next log in.

2.3.3.5. Configuring Preferred Authentication Domains

You may assign a preferred authentication domain to a user. If the user then tries to log in without specifying a domain, Web Center performs external authentication against his preferred domain only. It ignores the user’s accounts in other master domains.

Since “$pwdMasterTS” cannot be used as name of a real user attribute, you have to replace the property name “$pwdMasterTS” with the real user attribute name in some configuration files:

- Object description *user.xml
  - <property name="$pwdMasterTS” ...>
- Deployment descriptor **web.xml**
  - Value of context parameter “com.siemens.webMgr.auth.masterTsAttr”
- Forms configuration file *WEB-INF/configPwd/identity/forms-config.xml
  - Login form property "$pwdMasterTS”

2.3.3.6. Configuring Access to the Request Workflow Service

When using external authentication, access to the request workflow service usually doesn’t work out of the box since Web Center authenticates to the service with user name and password. The service verifies the presented password against the DirX Identity database. If the user has logged in against an external target system, however, the password will not

match the one in the DirX Identity database and the authentication against the request workflow service will fail.

To make this feature work, set up the connection from Web Center to the request workflow server following the procedure used for single sign-on. See the *DirX Identity Web Center Reference* for details.

2.4. Synchronizing Passwords

In authentication mode “ONE”, a user is authenticated against the DirX Identity database first. If that fails, external authentication is attempted.

If a user’s DXI password is different from his password in a master target system and the user logs in with his external password, the DXI authentication will fail while the external authentication will succeed. In this case, the external password is propagated back to his DirX Identity user entry and from there to all his master and non-master accounts (via a user password change event).

You can disable password synchronization in file **webCenter.properties**:

```
passwordManagement.login.syncUserPassword = false
```

Password synchronization does not apply to authentication modes other than “ONE“.

2.5. Locking Authentications

Locking authentications is a feature shared by all DirX Identity Web applications: Web Center for Password Management, standard Web Center and the Provisioning Web Services.

2.5.1. Locking Logins with Password

A user can authenticate to Web Center with some user name and password, or to a Provisioning Web Service application with DN and password. For security reasons, the number of attempts should be limited to prevent automated attacks. DirX Identity supports a maximum number of failed attempts after which further attempts are rejected for some period of time. Responses to password logins can also be delayed for a period of seconds depending on the number of attempts that have failed so far.

The lock mechanism is configured per domain via the following attributes:

- **dxrPwdResponseDelays** – the maximum number of failed attempts and response delays.
- **dxrPwdLockDuration** – the period of time a lock is in effect.

The following user attributes keep track of a user’s password login lock status:

- **dxrPwdFailureCount** – the number of failed attempts.

- **dxrPwdFailureTime** – the time of the last failed attempt.
- **dxrPwdAccountLockedTime** – the end time of the lock period.

A user's lock is set if his number of failed attempts hits the maximum number.

While the lock is in effect, any attempt to login with password is rejected.

The lock is released

- If a password login request is received and the lock duration has expired.
- If the user successfully logs in via another authentication mechanism, like challenge response authentication.
- Explicitly by an administrator over the Web Center for Password Management user interface.

Failure count and last failure time are cleared

- If the lock is released.
- If a password login request succeeds.
- If a password login request is received and the failure time has expired (is older than the lock duration.)

Notes:

We do not recommend defining response delays since they unnecessarily prolong request processing time on the server.

From a security point of view, defining a maximum number of attempts is sufficient. Delays add nothing to security.

The lock attributes described here are also used when a user logs in to a standard Web Center application or to the Provisioning Web Services.

2.5.2. Locking Challenge Response Authentications

A user can authenticate to a Web Center or Provisioning Web Service application by answering challenge response questions. For security reasons, the number of attempts should be limited to prevent automated attacks. DirX Identity supports a maximum number of failed attempts after which further attempts are rejected for some period of time. Responses to challenge response authentication requests can also be delayed for a period of seconds depending on the number of attempts that have failed so far.

The lock mechanism is configured per domain via the following attributes:

- **dxrChallResponseDelays** – the maximum number of failed attempts and response delays.
- **dxrChallLockDuration** – the period of time a lock is in effect.

The following user attributes keep track of a user's challenge response authentication

status:

- **dxrChallFailureCount** – the number of failed attempts.
- **dxrChallFailureTime** – the time of the last failed attempt.
- **dxrChallLockTime** – the end time of the lock period.

A user's lock is set if his number of failed attempts reaches the maximum defined.

While the lock is in effect, any attempt to authenticate by answering challenge response questions is rejected.

The lock is released

- If a challenge response authentication request is received and the lock duration has expired.
- If the user successfully logs in via another authentication mechanism, like user name and password.
- Explicitly by an administrator over the Web Center for Password Management user interface.

Failure count and last failure time are cleared

- If the lock is released.
- If a challenge response authentication request succeeds.
- If a challenge response authentication request is received and the failure time has expired (is older than the lock duration.)

Notes:

We do not recommend defining response delays since they unnecessarily prolong request processing time on the server.

From a security point of view, defining a maximum number of attempts is sufficient. Delays add nothing to security.

The lock attributes described here are also used when a user performs a challenge response authentication against a standard Web Center application or the Provisioning Web Services. They are also used for logins to the Provisioning Web Services via one-time password. This is why these attributes are grouped under general titles like "Secondary authentications" or "Other logins" in user interfaces.

2.5.3. Configuring Lock Parameters

You can view and edit the lock configuration parameters in the DirX Identity Manager Provisioning View. Select the domain object and open the "Authentication" tab:

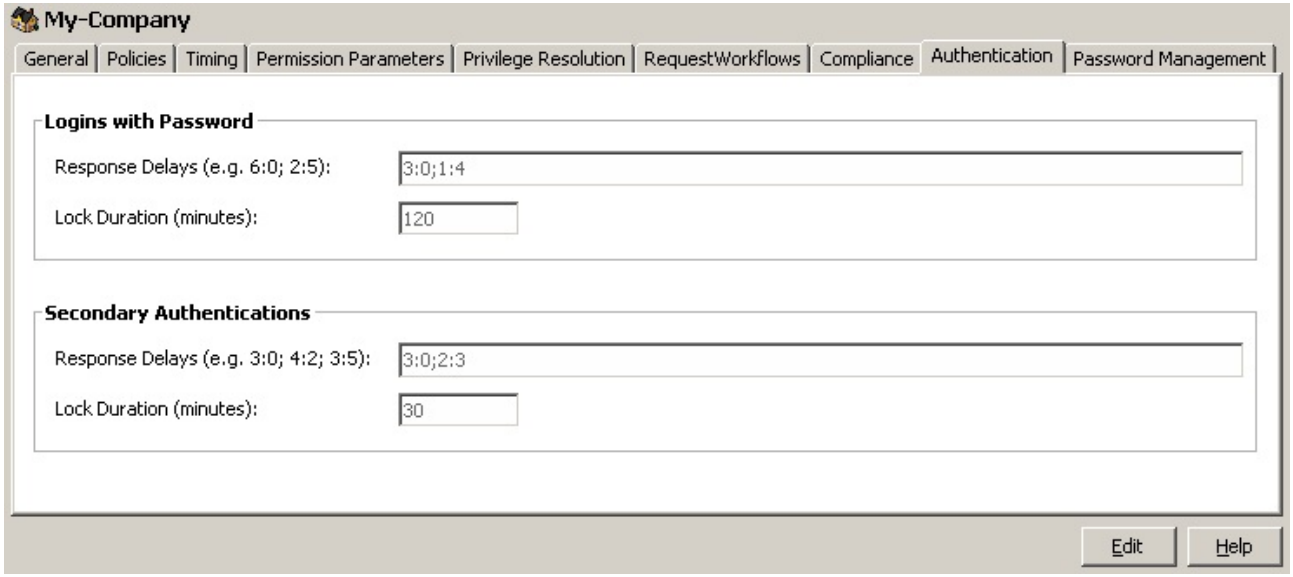

Figure 7. Identity Manager - Lock Configuration

This tab shows domain-wide settings that apply to authentications in Web Center and Provisioning Web Services applications. The configuration parameters are the same for both locks.

- **Response Delays** – A semicolon-separated list of response delays. Each delay defines the number of failed authentication attempts it applies to, and a delay time in seconds, separated by a colon. The delay "4:2", for example, applies to 4 attempts and delays each attempt by 2 seconds. The delay time 0 means no delay. The first delay in the list applies to the first number of failed attempts, the second to the next ones, and so on. Finally, if the total number of failed attempts is exceeded, further authentication attempts will be blocked for some time which means any further attempt will simply fail no matter whether it would succeed or not. To set no limit on failed attempts, leave the value for response delays empty.
- **Lock Duration (minutes)** – The period of time that a lock is valid. If the lock duration has expired, the response delay handling starts anew. Also, a user's failure count is cleared if his last failure time is older than the lock duration. The default value is 120, which means 2 hours.

Samples:

With response delays "3:0; 4:2; 5:3" and a lock duration of 60,

- The first 3 attempts are processed without any delay.
- The next 4 attempts are delayed by 2 seconds each.
- The next 5 attempts are delayed by 3 seconds each.
- After 12 (= 3+4+5) failed attempts, further attempts will be blocked for an hour.

The recommended delay configuration defines a maximum number of failed attempts without any delay, like "10:0".

2.5.4. Monitoring the Status Attributes

The Web Center for Password Management application displays the status attributes for both locks on the user summary page:

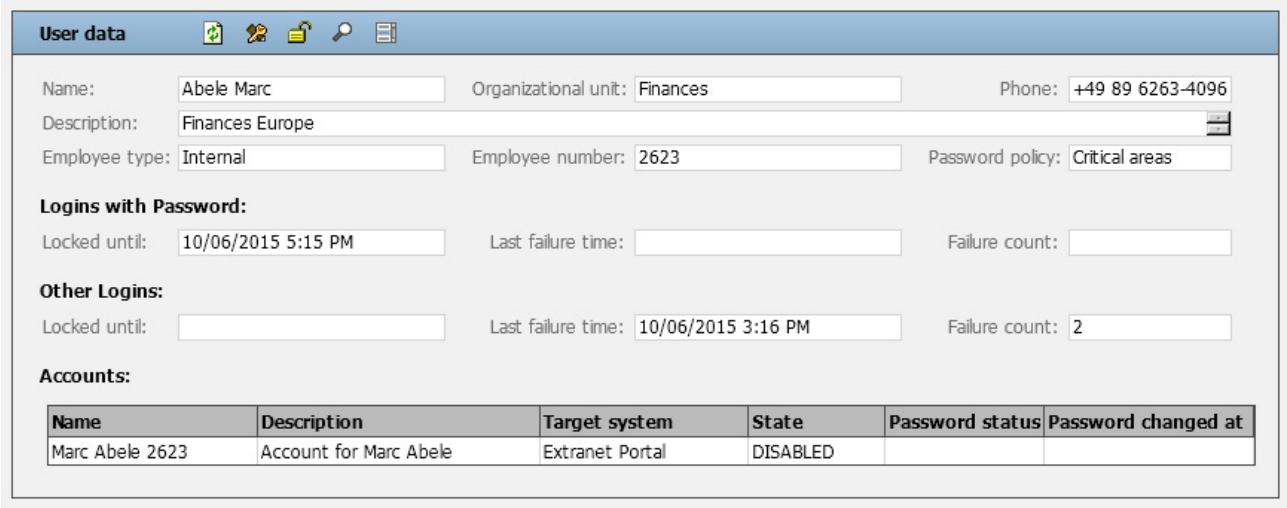

Figure 8. User Summary Page: Lock Status Attributes

2.5.5. Releasing the Locks

The Web Center for Password Management application provides the functionality to release the locks for a user. The functionality can be invoked from the user menu, the user list context menu and a tool on the user summary page (the middle tool in the toolbar of the above picture.) Note that the function releases both locks. It also clears the last failure times and the failure counts. A user can only release the locks of those users he is allowed to reset their passwords.

2.6. Workflows

The following workflows must be configured to enable the password synchronization:

- For each target system:
  - A provisioning workflow for regular validation of accounts
  - A provisioning workflow for password synchronization
- A Password Event Manager workflow for handling user password changes
- A consistency workflow to delete the password history attributes in the Identity domain

Optionally, an "import user workflow from master source" can be configured. End user entries can be imported by a user import workflow from a master source such as Active Directory or an LDAP directory. Alternatively, they can be managed completely within DirX Identity.

2.6.1. Provisioning Workflows

This section describes the provisioning workflows that can be configured for password

management.

2.6.1.1. Importing Users from a Password Master System

The standard user import workflow can be used to import the users from an Active Directory domain. For importing users from an LDAP directory, adapt the import workflow for ADS. For associating later on users and their accounts, you should store the login name of the external master system to a user attribute, e.g. uid.

After the workflow configuration is completed, define a schedule so that the users are regularly (typically: daily) imported. See the chapter on "Scheduled Workflows" in the *DirX Identity Application Development Guide*.

2.6.1.2. Validation and Password Synchronization of a Target System

If you do not manage the accounts and groups of the external system within DirX Identity and use it solely as target to change passwords, you need to make sure that the accounts in the external system are never disabled by any privilege resolution process. To do this, set the following options when running the Target System creation wizard:

- **Target System Selection** dialog - select the appropriate template from the list and DO NOT check **Accounts and Groups in common subtree** at the bottom of the dialog. Leaving this flag unchecked instructs the wizard to create separate folders for accounts and for groups (this is the default).
- **Target System Advanced** dialog - in **Assignment Properties**, check **Reference Group from Account**. As a result, the account-group references (links) are stored at the account and you can easily set them later on in the import validation workflow. Make sure that you have NOT checked **Disable Password Sync** so that password changes are performed in real time.

  If you want to use a given target system for external authentication, check the **Master** checkbox and specify the **Authentication class** and the **Connection string (domain)**. See the section "Configuring External Authentication" for details.
- **Connectivity Scenario** dialog - this dialog is displayed when you are creating your first target system. Select the **Consistency Check** and **Reports** workflows.
- **Provisioning Workflows** dialog - select the Java-based workflows for validation and password setting. Typically they are named **Validate_**type*_**Realtime* and **Set Password in** *type*. When adapting the attribute mapping in the validation workflow, make sure the login name is mapped to the account attribute that is defined as login attribute for the master target system; the default for AD is *dxrName*, the default for LDAP is *cn*.

2.6.2. Password Management Workflows

This section describes the password management workflows.

2.6.2.1. User Password Event Manager

The User Password Event Manager workflow (**UserPasswordEventManager**) processes all

password change events resulting from the Windows Password Listener and those of Web Center when it requests to change a user password. If the event references a user, the workflow performs the password change itself.

If the event is sent from Windows Password Listener, it refers to an account in the Windows target system. The account in the event is identified by the domain and its login name. The Password Event Manager searches for a target system with this domain name and finds the account in that target system by searching for the account name in the LDAP attribute **dxrName**. Make sure that the mapping in the validation workflow is appropriate.

2.6.2.2. Account Password Manager

The Account Password Manager workflow (**AccountPasswordManager**) processes password change requests for accounts from Web Center or from the Provisioning Web Services.

When started by a schedule, it searches for accounts with expired passwords and generates a new one. For more details, see the *DirX Identity Application Development Guide*.

2.6.2.3. User Password Expiration Notification

The User Password Expiration Notification workflow is optional for Password Management. It regularly checks for user passwords that are about to expire and informs the affected users by an e-mail.

The default configuration can be applied. For more details, see the *DirX Identity Application Development Guide*.

2.6.3. Consistency Workflow

To make sure that your consistency rules are applied, you need to set up a Policy Execution workflow and an appropriate schedule. The configuration options for this workflow contain a search base for the rules and a filter. Make sure that the search finds consistency rules with the object class dxrConsistencyRule and especially includes the rules to

- Remove the password history entries (**RemoveAccountPasswordChangeHistory**).
- Associate accounts to users (**assocAccount2User**). Adapt the parameter joinFilter so that it can find the user for a given account. Assuming the login name is stored in attribute dxrName of the account and in uid of the user the filter would be: (&(objectclass=dxrUser)(uid=$(subject.dxrName))).

2.7. Roles, Password and Access Policies

The administrator also needs to make sure that the appropriate policies are in place – in particular, password and access policies. Service desk members need to be allowed to reset the password for other users.

Users need to have appropriate rights to change their own or other passwords. There are two types of users in Web Center for Password Management:

- Regular end users who can only change their own passwords
- Service desk users who need to be allowed to change the password for other users.

2.7.1. User Rights

There are two kinds of users that usually work with Web Center for Password Management.

- Service Desk operators – they can list other users and reset their passwords, display reports and manage password policies. Users in the predefined DirXmetaRole group ServiceDeskOperators get these additional rights.
- Regular end users – they can only change their own passwords and define questions and answers for challenge response authentications. The users must have the right to change own passwords. This is ensured by the specific access policy.

The additional access and menu policies for password management are defined in *Password Management* folder in AccessPolicies subtree. The access and menu policies are subject of customizations. See access policies documentation for more details.

2.7.2. Service Desk Group

To define the appropriate access policies, service desk members should be identified, preferably by a group membership. We suggest that you create a group (for example, **ServiceDeskOperators**) in the DirXmetaRole target system (which represents the DirX Identity domain itself) and then populate this group with all service desk members.

2.7.3. Proposal Lists for Menu Operations

Proposal lists for menu operations help to reduce the set of operations provided in Web Center so that users see only those operations that they are allowed to use. These operations are configured in the Menus folder of the Proposal Lists section in the Domain Configuration.

For Password Management:

- End users should be able to access the operations for Self Service (especially "changePassword" and "addChallengeResponse").
- Service desk members should be able to access the operations for User Management (especially "resetPassword") and report generation ("display", "reports", "saveAsFile").

Make sure that you enable menu policies in the Domain configuration.

2.7.4. Consistency Rules

The password change workflows store the status of password changes in multi-value LDAP attributes of the respective accounts. This information must be regularly removed, which is the task of the default consistency rule **RemoveAccountPasswordChangeHistory**. Make sure this rule is active.

For external authentication, accounts have to be associated with user entries. Copy, adapt

and activate the default rule **assocAccount2User** as mentioned above (2.6.3).

2.7.5. Password Policies

You should define the password policies in the DirX Identity domain so that they match the policies defined in Active Directory and the other applications you want to synchronize.

2.7.6. Access Policies

You need several types of access policies for Password Management. The following policies allow end users and service desk members to change passwords and allow service desk members to generate reports:

- **Users can handle themselves** – users are allowed to read and modify their own entries.
- **Users handle their passwords** – all users are allowed to read and set their own passwords.
- **Users handle their accounts** – all users are allowed to read and modify their accounts.
- **Users handle passwords of their accounts** – all users are allowed to read and set the passwords of their accounts.
- **ServiceDesk can handle all users** – the service desk is allowed to read and modify all user entries.
- **ServiceDesk handles all passwords** – the service desk is allowed to read and set all user passwords.
- **ServiceDesk handles all accounts** – the service desk is allowed to read and modify all accounts. This policy is needed for assisted password reset. Service desk members are identified as members of a service desk group (e.g. ServiceDeskOperators)
- **ServiceDesk can execute user reports** – the service desk can create Password Management reports that are located in the folder for user report definitions.

The following access policies define the menu and operations that end users and the service desk can see in Web Center:

- **Users have the Self-service menu items** – all users can manage their own data, especially change their passwords.
- **ServiceDesk menus** – the service desk has menus for assisted Password Management and for report generation.

Note: menu policies only control the visibility of menu operations in Web Center! Only access policies control the actions users can perform when they are authenticated with a DirX Identity application. Therefore, the appropriate access policies must be defined.

2.8. Windows Password Listener

The Windows Password Listener captures changed passwords on Active Directory domain controllers and sends them to the Password Event Manager workflow. For details on this workflow, see the chapter "Managing Passwords" in the *DirX Identity Connectivity*

Administration Guide. The Listener needs to be installed for all domains whose users are imported into the DirX Identity domain.

This setup allows users to change their passwords in their Windows desktop and update them on all the target systems on which they have an account and which are configured to update passwords in the DirX Identity domain. See the section "Validation and Password Synchronization of a Target System" for details.

DirX Product Suite

The DirX product suite provides the basis for fully integrated identity and access management; it includes the following products, which can be ordered separately.

DirX Identity

DirX Identity provides a comprehensive, process-driven, customizable, cloud-enabled, scalable, and highly available identity management solution for businesses and organizations. It provides overarching, risk-based identity and access governance functionality seamlessly integrated with automated provisioning. Functionality includes lifecycle management for users and roles, cross-platform and rule-based real-time provisioning, web-based self-service functions for users, delegated administration, request workflows, access certification, password management, metadirectory as well as auditing and reporting functionality.

DirX Directory

DirX Directory provides a standards-compliant, high-performance, highly available, highly reliable, highly scalable, and secure LDAP and X.500 Directory Server and LDAP Proxy with very high linear scalability. DirX Directory can serve as an identity store for employees, customers, partners, subscribers, and other IoT entities. It can also serve as a provisioning, access management and metadirectory repository, to provide a single point of access to the information within disparate and heterogeneous directories available in an enterprise network or cloud environment for user management and provisioning.

DirX Access

DirX Access is a comprehensive, cloud-ready, scalable, and highly available access management solution providing policy- and risk-based authentication, authorization based on XACML and federation for Web applications and services. DirX Access delivers single sign-on, versatile authentication including FIDO, identity federation based on SAML, OAuth and OpenID Connect, just-in-time provisioning, entitlement management and policy enforcement for applications and services in the cloud or on-premises.

DirX Audit

DirX Audit provides auditors, security compliance officers and audit administrators with analytical insight and transparency for identity and access. Based on historical identity data and recorded events from the identity and access management processes, DirX Audit allows answering the “what, when, where, who and why” questions of user access and entitlements. DirX Audit features historical views and reports on identity data, a graphical dashboard with drill-down into individual events, an analysis view for filtering, evaluating, correlating, and reviewing of identity-related events and job management for report generation.

For more information: support.dirx.solutions/about

Legal remarks

On the account of certain regional limitations of sales rights and service availability, we cannot guarantee that all products included in this document are available through the Eviden sales organization worldwide. Availability and packaging may vary by country and is subject to change without prior notice. Some/All of the features and products described herein may not be available locally. The information in this document contains general technical descriptions of specifications and options as well as standard and optional features which do not always have to be present in individual cases. Eviden reserves the right to modify the design, packaging, specifications and options described herein without prior notice. Please contact your local Eviden sales representative for the most current information. Note: Any technical data contained in this document may vary within defined tolerances. Original images always lose a certain amount of detail when reproduced.