EVIDEN

Identity and Access Management

DirX Identity

Enabling Smart Card Login for DirX Identity Manager

Version 8.10.12, Edition August 2025

Table of Contents

Preface

This document presents a use case that illustrates how to set up smart card login for DirX Identity Manager when DirX Directory is used as the LDAPv3 directory server for the Identity Store. It describes two scenarios for setting up smart card login and consists of the following chapters:

- Chapter 1 provides general information about the use case and the two configurations.
- Chapter 2 describes how to set up the recommended configuration.
- Chapter 3 describes how to set up the alternate configuration.
- Chapter 4 describes how to create a personalized DomainAdmin for representing the smart card user.

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

DirX Identity allows for extensive customization of its features using various methods; for example, with schema extensions and object descriptions and by setting options and parameters through wizards or object pages.

DirX Identity provides for smart card login to DirX Identity Manager to connect to the Provisioning and Connectivity databases. It is based on the SASL EXTERNAL bind authentication method and is intended for use by a small subset of administrators whose access to DirX identity data requires a very strong level of security.

This chapter describes some general aspects of smart card login related to DirX Directory and DirX Identity configuration and introduces the two configuration scenarios for enabling its use with DirX Identity Manager.

1.1. Related Documentation

The following documents contain additional information related to this use case. We recommend that you become familiar with the information in these documents before proceeding with the tasks described in this use case document.

You can also consult the online help provided with DirX Manager and DirX Identity Manager (click **Help** in a dialog or topic to access the online help).

DirX Directory Manager Guide

- **What is DirX Manager?** → **Configuration View** → **LDAP Configuration Subentry** and → **LDAP SSL Configuration Subentry** provide detailed information about these subentries and how to manage them with DirX Manager.
- **Schema Management** provides detailed information about directory schema attribute and object class structure and describes how to manage these elements with DirX Manager.
- **Database** → **Indices** provides detailed information about attribute indexes and describes how to manage them with DirX Manager.
- **Core Component** → **Using LDAP** → **Smart Card Login** describes the prerequisites and procedure for setting up smart card login for DirX Manager. All the principles and most steps given in this document also apply to setting up smart card login for DirX Identity Manager.
- **Core Component** → **Basic Patterns/LDAP Functionality** provides detailed information about how to use DirX Manager's core user interface. You will need to use this interface as part of the smart card login configuration process.

DirX Directory Administration Reference

- **DirX Attributes** → **X.500 User Application Attributes** → **Attributes for LDAP Server Configuration** → **Attributes Controlling LDAP Extended Operations** describes the attributes that specify groups of users that are allowed to perform specific extended operations and groups of operations. You will need to configure the LDAP Extended

Operations Read Users attribute as part of the smart card login configuration process.

- **DirX String Representation for DAP Binds → Distinguished Names** describes X.500 distinguished name format.

DirX Identity User Interfaces Guide

- **Using DirX Identity Manager** describes how to use DirX Identity Manager's login, Provisioning, Connectivity and Data Views. See also the "Basic Patterns" topics in the "Core Components" section of the DirX Identity Manager online help for detailed information about the Data View and managing LDAP server profiles for the login dialog. You will need to understand how to use these views when following the instructions for setting up smart card login given in this use case.
- **Using DirX Identity Manager → Customizing DirX Identity Manager → Customizing the Property File (dxi.cfg)** describes the DirX Identity Manager **dxi.cfg** property file. You will need to update this file as part of the smart card login configuration process.

DirX Identity Connectivity Administration Guide:

- **Managing DirX Identity Servers → Managing the Java-based Server → Server Processes → Configuring the Processes → Java-based Server Password Parameters** describes the Java-based Server password properties file. You will need to provide a similar password properties file in the DirX Identity Manager environment as part of the smart card login configuration process.

DirX Identity Customization Guide

1.2. General Information

This section provides general information about configuring DirX Directory and DirX Identity for smart card login and introduces the two smart card login configuration scenarios.

1.2.1. DirX Directory Configuration Requirements

Configuring DirX Directory for smart card login to DirX Identity Manager has the following requirements:

- Smart card login requires the LDAP server to be configured (in the LDAP server profile) for SASL external bind authentication. When an LDAP server is configured for SASL external binds, it cannot support normal SSL binds; the two forms are mutually exclusive per LDAP server. If you want to support both SASL external binds (for example, for DirX Manager binds) and SSL binds (for example, for Java-based Server binds), your DirX Directory configuration will require two LDAP servers: one for SASL external binds, and one for SSL binds. Figures 2 and 4 illustrate this configuration. A single LDAP server can support both SASL and simple bind and/or both SASL and anonymous bind.
- Mapping the smart card to an LDAP user requires using the mapping option that instructs the DSA to map to the user directory entry that owns the certificate specified in the SASL external bind (exactly one entry). This mapping option requires the **userCertificate** attribute to have an initial index.

- The smart card LDAP user must have the right to perform the extended LDAP operation (OID=1.3.12.2.1107.1.3.2.11.38) that retrieves the mapped user (the bind DN).

1.2.2. DirX Identity Configuration Requirements

Configuring DirX Identity for smart card login to DirX Identity Manager has the following requirements:

- The smart card LDAP user is represented as a "personalized DomainAdmin" that holds the smart card certificate and is used for external SASL binds. The personalized DomainAdmin needs to be configured in DirX Identity as part of the smart card login setup process.
- The authentication mechanism for starting request workflows needs to be configured for SASL authentication instead of user/password authentication. The following figure illustrates the configuration files and scripts for setting up request workflow service SASL authentication and the authentication control flow:

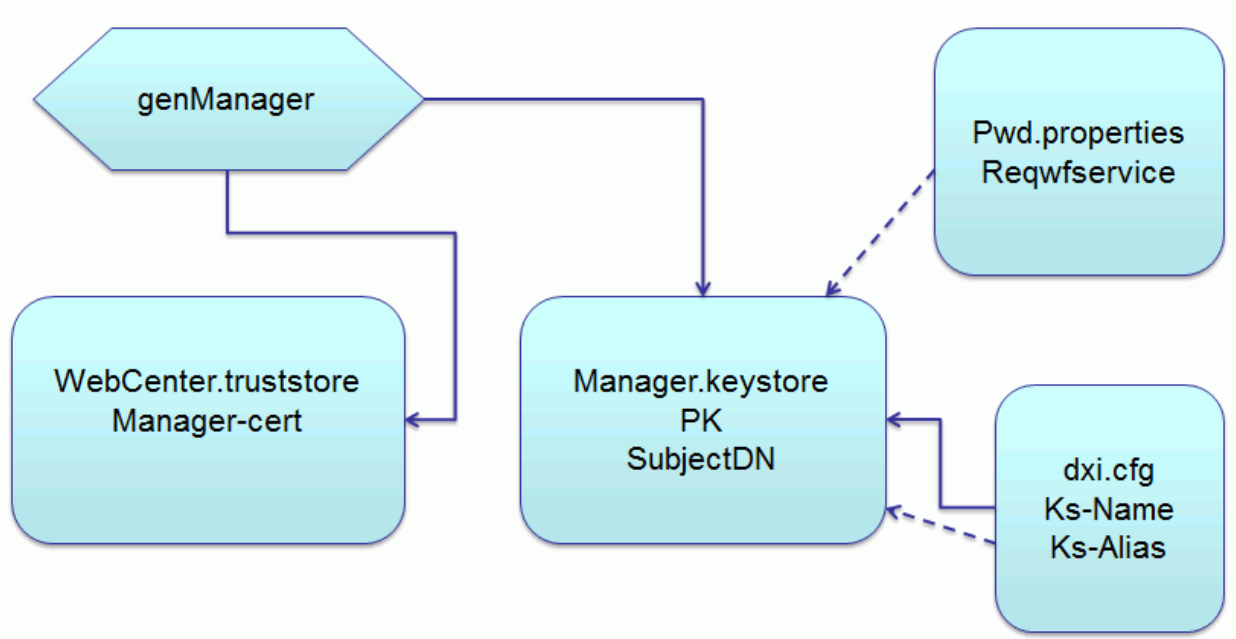


Figure 1. Request Workflow Service SASL Authentication Files

As shown in the figure:

  - The **genManager** script generates a keystore with a private key for DirX Identity Manager (**Manager.keystore PK SubjectDN** in the figure) or it appends a private key to an existing keystore and adds (or appends) a certificate for this key to the Java-based Server's truststore (**WebCenter.truststore Manager-cert** in the figure). You need to copy the generated keystore (**Manager.keystore** in the figure) to the machine where DirX Identity Manager runs.
  - To access the keystore, you need to specify a request workflow service password, the name of the keystore, and an alias for the keystore:
    - You specify the keystore name and alias in DirX Identity Manager's Java properties file *dxi_install_path*/GUI/bin/dxi.cfg* file in the **keystoreName** and **keystoreAlias** parameters.

- The request workflow service password is stored in a password properties file (file name:*password.properties*) in DirX Identity Manager's runtime environment (shown as **Pwd.properties Reqwfservice** in the figure). This file is similar to the Java-based Server's password properties file. It needs to reside in the DirX Identity Manager environment because the Java-based Server may be running on a different host from Identity Manager and thus may not be available, and DirX Identity Manager needs the request workflow service password to access the keystore. You need to supply the password properties file in DirX Identity Manager's *dxi_install_path*/GUI/bin* subdirectory and provide the request workflow service password in this file. This password must be identical to the password you provide in the **keystorePassword** parameter of the **genManager** script.

◦ DirX Identity Manager uses the password properties file and **dxi.cfg** to read the private key from the keystore. It then encrypts the name to be used to start the request workflow service and sends it to the Java-based Server as an encrypted key.

◦ The Java-based Server uses its truststore (**WebCenter.truststore** in the figure) and tries to decrypt the username, and then checks it.

1.3. Recommended Smart Card Login Scenario

In the recommended configuration, Connectivity and Provisioning are located in one database, as shown in the following figure.

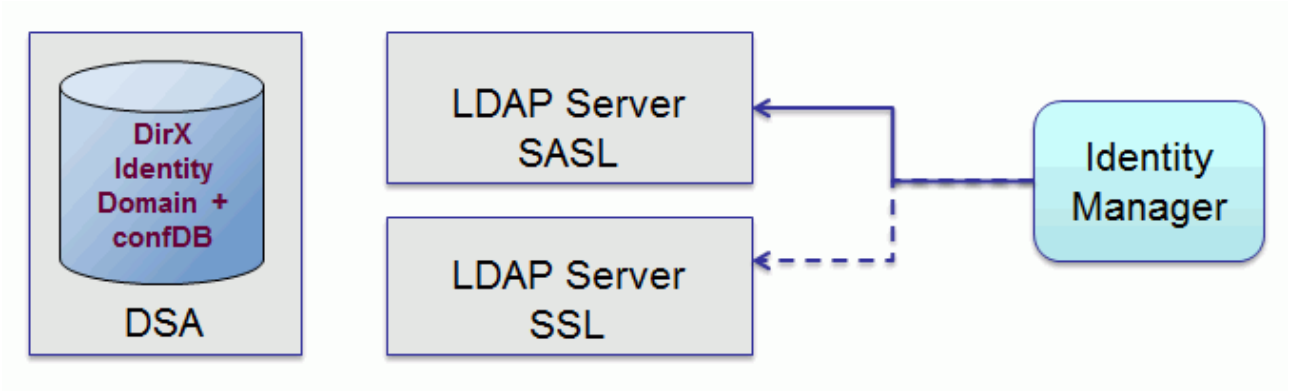


Figure 2. Recommended Configuration - Component View

For this scenario, you need to create and configure a personalized DomainAdmin that stores your certificate in the **Certificate** attribute. This user is used for both Provisioning and Connectivity connection, as shown in the following figure:

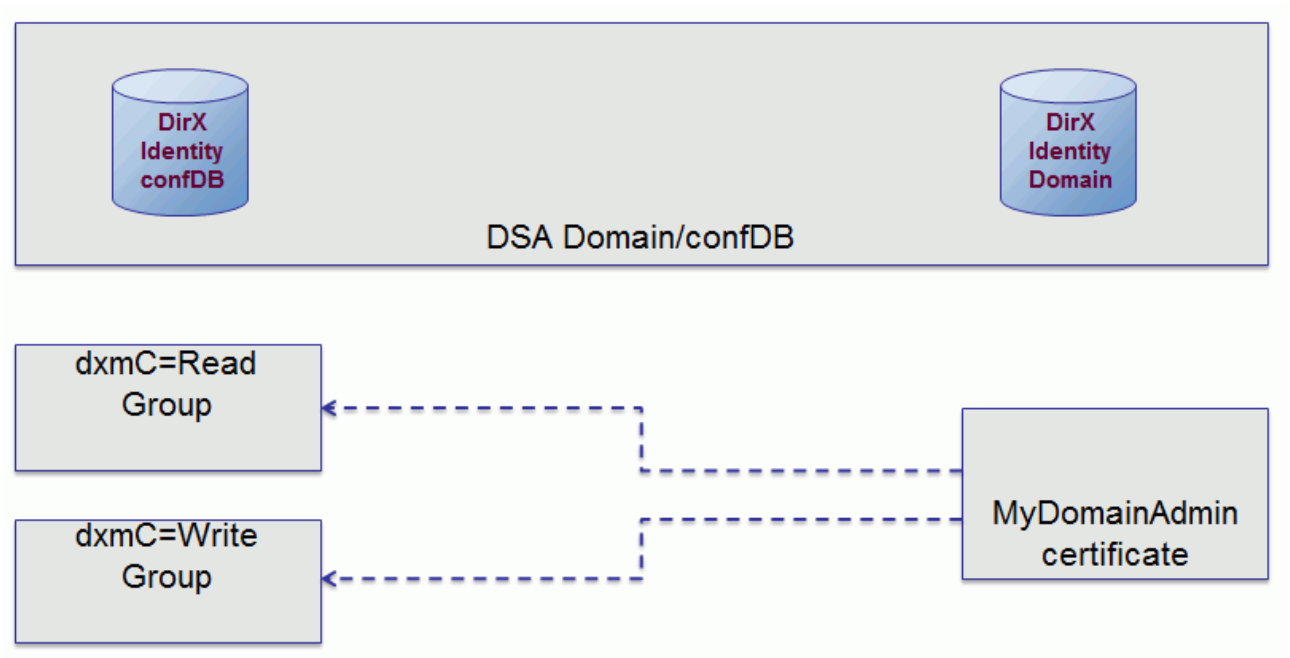


Figure 3. Recommended Configuration - DirX Identity Access View

We recommend using this smart card login scenario because it is simpler to configure than the alternate scenario.

1.4. Alternate Smart Card Login Scenario

In the alternate smart card login scenario, Connectivity and Provisioning are located in separate DirX databases, as shown in the following figure.

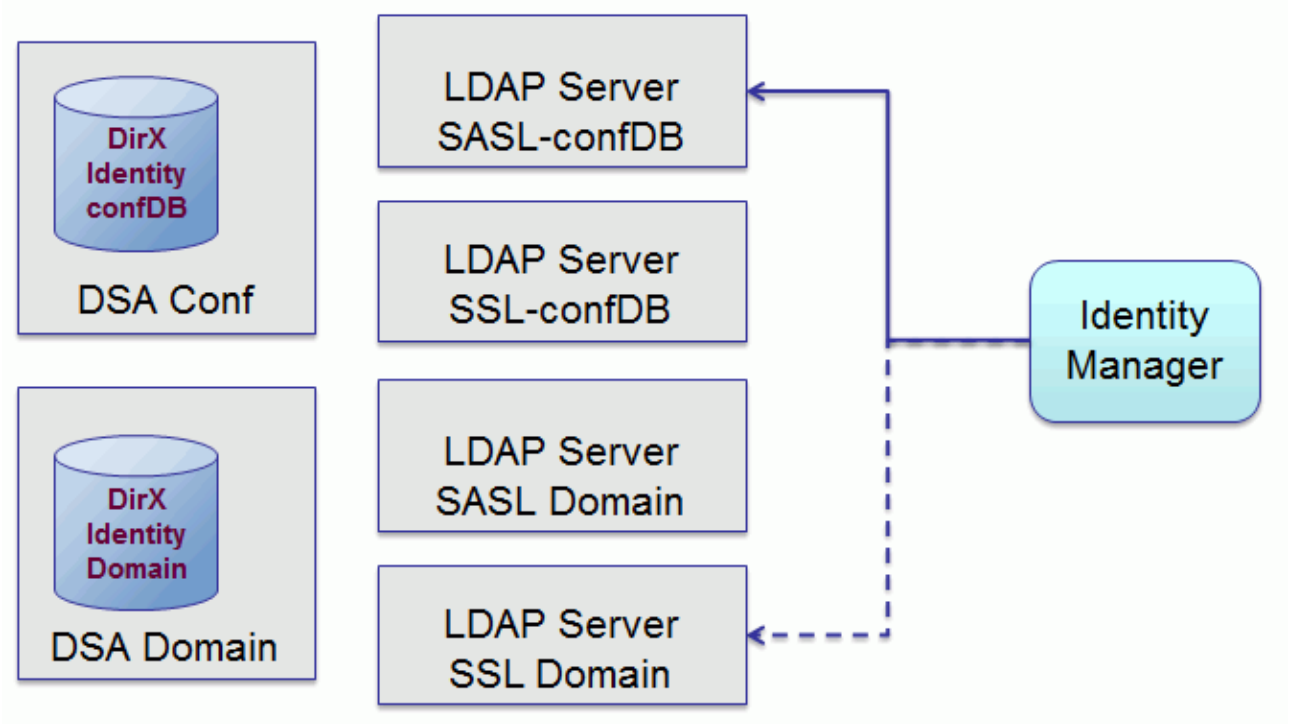


Figure 4. Alternate Scenario - Component View

As shown in the figure, there are two different DirX databases on two different machines.

One DirX database hosts the Connectivity data, and the other database hosts the Provisioning domain data.

For this scenario, you need to set up two personalized user objects:

- A personalized DomainAdmin (shown as **myDomainAdmin** in the next figure) that stores the smart card certificate in the **Certificate** attribute and is used for smart card login to the Provisioning domain.
- A personalized metahubAdmin (shown as **myMetahubAdmin** in the next figure) that stores the smart card login certificate in the **userCertificate** attribute and is used for smart card login to the Connectivity database.

You also need to set up two "mirror" user objects for the personalized DomainAdmin to support authenticated connection between the Provisioning and Connectivity databases for access to target system data (for example, running target system workflows or wizards):

- A mirrored personalized DomainAdmin on the Provisioning side (shown as **MyMirrorAdmin** in the following figure) that links to the personalized DomainAdmin and holds the encrypted password for authenticating with the mirrored DomainAdmin on the Connectivity side.
- A mirrored personalized DomainAdmin on the Connectivity side (shown as **Mirrored MyDomainAdmin** in the following figure) that holds the same password as the mirrored DomainAdmin on the Provisioning side.

The following figure illustrates this scenario:

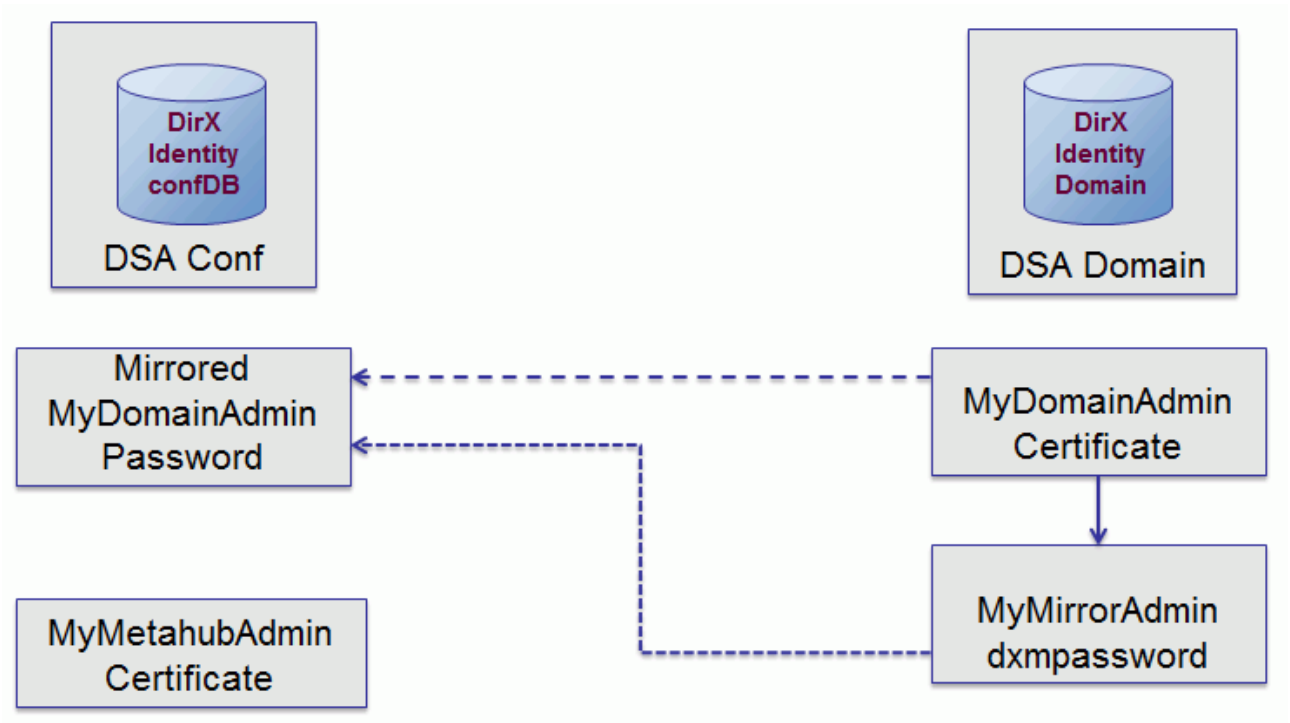


Figure 5. Alternate Scenario - DirX Identity Access View

2. Configuring the Recommended Scenario

This chapter describes how to configure the recommended smart card login scenario and add additional administrators to it.

2.1. Configuration Procedure

Configuring the recommended smart card login scenario consists of the following tasks:

- Configuring the DSA and LDAP Server
- Configuring DirX Identity Manager
- Configuring DirX Identity

The next sections describe each configuration task.

2.1.1. Prerequisites

The recommended smart card login scenario has the following prerequisites:

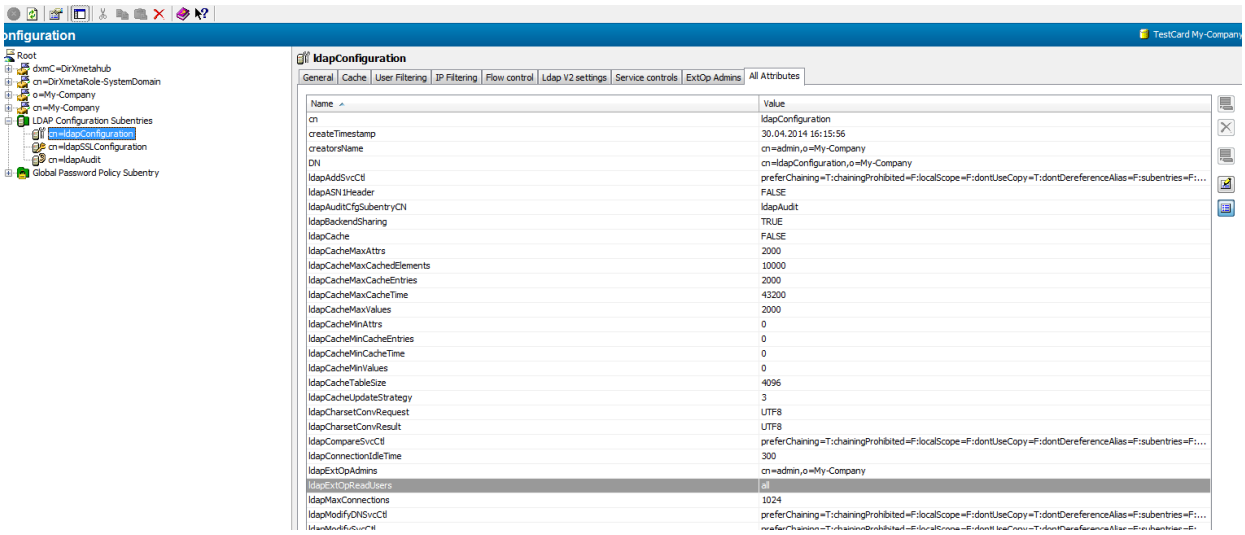
- Atos CardOS API V 5.5 64-bit (see *DirX Directory Manager Guide*: **Core component** → **Using LDAP** → **Smart Card Login** → **Software Requirements**)
- DirX Directory Server V8.9 or newer
- DirX Manager V2.3 build 110 or newer
- Java 11 64-bit Java Runtime Environment (JRE)

2.1.2. Configuring the DSA and LDAP Server

To configure the DSA and LDAP Server for smart card login:

- Using DirX Manager, follow the instructions in the document *DirX Directory Manager Guide* → **Core component** → **Using LDAP** → **Smart Card Login** → **Setting up the LDAP Server and the DSA for Smart Card Login**, with the following exceptions:
  - In the Client Authentication tab of the LDAP server SSL configuration subentry, select **client authentication required** and then select **Use the directory entry that owns the Certificate as bind initiator** from the drop-down list.
  - The selection **Use the directory entry that owns the Certificate as bind initiator** requires that you configure an initial index for the **userCertificate** attribute. You can use the Database node in DirX Manager's Schema View to perform this task.
- In the LDAP Configuration subentry, add the distinguished name provided in the subject field of your smart card certificate to the LDAP Extended Operations Read Users attribute (or use the value **all**) to allow the personalized DomainAdmin to perform all extended LDAP read operations. The following figure shows the subentry and the attribute:

LDAP Server Configuration Subentry and the ldapExtOpReadUsers Attribute



Because the client (Identity Manager) will use SASL external binding for the personalized DomainAdmin, you need to specify the DN attribute values in X.500 syntax prefixed with **X500DN:**. For example:

X500DN:/C=DE/O=Atos/SURNAME=Schwinn/GIVENNAME=Ignaz/SERIALNUMBER=A987/CN=Ignaz Schwinn/UID=Z1234)

See the *DirX Administration Reference* → **DirX String Representation for DAP Binds** → **String Representations for Structured Attribute Syntaxes** → **Certificate Attribute** for a description of this syntax. See the *DirX Administration Reference* → **DirX Attributes** → **X.500 User Application Attributes** → **LDAP Extended Operations Admins** for more information about access policies for LDAP extended operations.

2.1.3. Configuring DirX Identity Manager

To configure DirX Identity Manager for smart card login:

- Configure it to use:
- The PKCS#11 library
- The Java 11 JRE (64-bit)
- Set up the login profiles for the Provisioning and Connectivity views.

2.1.3.1. Configure the PKCS#11 Library

In DirX Identity Manager's **Tools** → **Options** menu, select to manage Java keystores and then specify the path to the PKCS#11 library in the **Smart Card** frame, as shown in the *DirX Directory Manager Guide* → **Core Component** → **Using LDAP** → **Smart Card Login** → **Configuring the PKCS**#1 **Library for DirX Manager**.

2.1.3.2. Configure Java 11 JRE (64-bit)

To ensure that DirX Identity Manager uses Java 11 JRE (64-bit), you can set it up to use existing Java 11 JRE (64-bit) installation:

- Open the file *dxi_install_path***setdxienv.bat**.
- Check to make sure the **set DXI_JAVA_HOME=** directive is present in the file and is set to the valid path to the JRE installation. For example:

```
…
@ECHO OFF
set DXI_JAVA_HOME=C:\Program Files\AdoptOpenJDK\jre-11.0.11.9-
hotspot
SET PATH=%DXI_JAVA_HOME%\bin;%PATH%
…
```

2.1.3.3. Set up the Login Profiles

To set up the login profiles for Connectivity and Provisioning, follow the instructions given in the *DirX Directory Manager Guide* → **Core Component** → **Using LDAP** → **Smart Card Login** → **Setting up the Client**. In the **Authentication** frame, select **SASL EXTERNAL bind** and then select **Smart Card PKCS#11** from the drop-down list in **Client Keystore**.

2.1.4. Configuring DirX Identity

Configuring DirX Identity for smart card login in the recommended scenario consists of the following tasks:

- Creating the personalized DomainAdmin in the Provisioning view.
- Storing the smart card certificate in the personalized DomainAdmin.
- Adding the personalized DomainAdmin to DirXmetahub read and write groups in the Connectivity view.
- Setting up the request workflow service for SASL authentication.

2.1.4.1. Create the Personalized DomainAdmin

To set up the personalized DomainAdmin, follow the instructions in the chapter "Creating a Personalized DomainAdmin".

2.1.4.2. Store the Smart Card Certificate in the Personalized DomainAdmin

To store the smart card certificate in the personalized DomainAdmin:

- In DirX Identity Manager's **Provisioning** → **Users** view, open the personalized DomainAdmin user you created (for example, **MyDomainAdmin**).
- In this user's Authentication tab, edit the **Certificate** attribute to add the smart card certificate.

2.1.4.3. Add the Personalized DomainAdmin to DirXmetahub Read and Write Groups

To add the personalized DomainAdmin to the DirXmetahub read and write groups:

- Change to the Identity Manager's Data View and then open the Connectivity view.
- Add the personalized DomainAdmin you created (for example, **MyDomainAdmin**) as a member of the following groups:

  dxmC=dirxmetahub,dxmc=groups,cn=Write

  dxmC=dirxmetahub,dxmc=groups,cn=Read

Here is a sample entry in LDIF format that show the update for **MyDomainAdmin** to the Write group:

dn: cn=Write,dxmC=Groups,dxmC=DirXmetahub
objectClass: top
objectClass: groupOfUniqueNames
cn: Write
description: Default Administrator Group (with Write permissions)
uniqueMember: cn=admin,dxmC=DirXmetahub
uniqueMember: cn=MyDomainAdmin,cn=Users,cn=My-Company

2.1.4.4. Set up Request Workflow Service SASL Authentication

To set up request workflow service authentication:

- Navigate to the **/utils/ssl** subdirectory in the directory of the Java-based Server that runs the request workflows; for example, *dxi_install_path***/ids-j-My-Company-S1/utils/ssl**. You can use DirX Manager's **Connectivity** → **Expert** view to check for request workflow support: open the **Manage Ids-J Configuration** context menu on a Java-based Server (right-click the server entry) and then select **requestworkflow Types**.
- Edit the following **genManager.bat** (or **.sh**) script parameters to your requirements:

set dname - specifies the host name; for example, **dxi-w-2012-03**.

set alias - specifies the keystore alias; for example, **dxi-w-2012-03**.

set keystorePassword - specifies the keystore password. The default is **alpha123**.

set truststorePassword - specifies the truststore password. The default is **changeme**.

- Run the **genManager.bat** (or **.sh**) script.
- Copy the generated keystore file to *dxi_install_path**/GUI/bin* on the machine that hosts DirX Identity Manager.
- In *dxi_install_path**/GUI/bin*, edit the **dxi.cfg** property file: uncomment the following lines and then set the keystoreName and keystoreAlias values:

```
#keystoreName=manager-keystore-<alias>
```

```
#keystoreAlias=<alias>
```

For example:

```
#keystoreName=manager-keystore-dxi-w2012-03
#keystoreAlias=dxi-w2012-03
```

2.2. Enabling Additional Administrators – Recommended Scenario

If you have already set up smart card login for one administrator, you can define additional administrators by performing a subset of the configuration tasks.

To enable additional administrators for the recommended configuration:

- Add this administrator to the LDAP Extended Operations Read Users attribute as described in "Configuring the DSA and LDAP Server".
- Prepare the personalized DomainAdmin as described in "Creating a Personalized DomainAdmin".
- Store the certificate in this personalized DomainAdmin as described in "Store the Smart Card Certificate in the Personalized DomainAdmin".
- Add the personalized DomainAdmin to DirXmetahub read and write groups as described in "Add the Personalized DomainAdmin to DirXmetahub Read and Write Groups".

3. Configuring the Alternate Scenario

This chapter describes how to configure the alternate smart card login scenario and add additional administrators to it.

3.1. Configuration Procedure

Configuring the alternate smart card login scenario consists of the following tasks:

- Configuring the LDAP server on the DirX Identity Provisioning domain side for smart card login.
- Configuring the Provisioning domain for smart card login.
- Configuring the LDAP server on the Connectivity database side for smart card login.
- Configuring the Connectivity database for smart card login from the Provisioning domain.

The next sections describe how to perform these tasks.

3.1.1. Prerequisites

The alternate scenario has the same prerequisites as the recommended scenario. See the section "Prerequisites" in the chapter "Configuring the Recommended Scenario".

3.1.2. Configure the LDAP Server - Provisioning

To configure the LDAP server on the Provisioning domain side for smart card login, follow the steps given in "Configuring the DSA and LDAP Server".

3.1.3. Configure DirX Identity - Provisioning

To configure the DirX Identity Provisioning domain for smart card login:

- Create the personalized DomainAdmin as described in the chapter "Creating a Personalized DomainAdmin".
- Store the smart card certificate in this personalized DomainAdmin as described in the section "Store the Smart Card Certificate in the Personalized DomainAdmin".
- In the **Provisioning** → **Users** view, create a mirror of the personalized DomainAdmin object you just created - for example, **MyMirrorAdmin** - to hold the encrypted password (dxmPassword attribute). This user object only needs to hold the encrypted password; no group assignments are necessary.
- Change to the **Data View** and then edit the **userpassword** field of your mirror personalized DomainAdmin user object to set the password.
- In the **Provisioning** → **Users** view, link the personalized DomainAdmin user object to the mirror personalized DomainAdmin user object using the **Mirrored User** field in the **SASL external bind** section of the Authentication tab of the personalized DomainAdmin user.

- Change to **Data View** → **Connectivity**.
- Create the mirrored user for the personalized DomainAdmin - for example, **Mirrored MyDomainAdmin** - with the same password as the mirror personalized DomainAdmin you previously created in the Provisioning view (for example, **MyMirrorAdmin**). See step 7 in the chapter "Creating a Personalized DomainAdmin".
- In **Data View** → **Connectivity**, add the mirrored user for the personalized domainAdmin - for example, **Mirrored MyDomainAdmin** - to the DirXmetahub read and write groups as described in "Add the Personalized DomainAdmin to DirXmetahub Read and Write Groups".
- Ensure that the DirX Identity Manager runtime uses the Java 11 JRE (64 bit) as described in "Configure Java 11 JRE (64-bit)".
- Set up the login profile for Provisioning as described in "Set up the Login Profiles".
- Set up SASL authentication to the request workflow service as described in "Set up Request Workflow Service SASL Authentication".

3.1.4. Configure the LDAP Server - Connectivity

To configure the LDAP server for the DirX Identity Connectivity database, follow the steps given in "Configuring the DSA and LDAP Server".

3.1.5. Configure DirX Identity - Connectivity

To configure the DirX Identity Connectivity database for smart card login:

- In DirX Identity Manager's **Data View** → **Connectivity**:
- Create a personalized DomainAdmin for smart card login to the Connectivity side - for example, **MyMetahubAdmin** - and then store the smart card certificate in the **userCertificate** attribute for this use. This user must have the inetOrgPerson object class, because this object class contains the **userCertificate** attribute. To create this user, right-click in the **cn=Users** tree and then select **New** → **Internet Organizational Person**.
- Add this personalized DomainAdmin to the DirXmetahub read and write groups as described in "Add the Personalized DomainAdmin to DirXmetahub Read and Write Groups".
- Ensure that the DirX Identity Manager runtime uses Java 11 JRE (64-bit) as described in the section "Configure Java 11 JRE (64-bit)".
- Set up the login profile for Connectivity as described in "Set up the Login Profiles".

3.2. Enabling Additional Administrators - Alternate Scenario

If you have already set up the smart card login for one administrator, you can define additional administrators by performing a subset of the configuration tasks. The next sections describe this subset.

3.2.1. Configure the LDAP Servers - Provisioning and Connectivity

In the LDAP Configuration subentry for both LDAP servers, add the distinguished name of the new personalized DomainAdmin to the LDAP Extended Operations Read Users attribute (or use the value **all**) to allow the new personalized DomainAdmin to perform all extended LDAP read operations. See the section "Configuring the DSA and LDAP Server" for details.

3.2.2. Configure DirX Identity - Provisioning

To add new personalized DomainAdmins to the Provisioning side:

- Create the new personalized DomainAdmin as described in the chapter "Creating a Personalized DomainAdmin".
- Store the smart card certificate in this new personalized DomainAdmin as described in the section "Store the Smart Card Certificate in the Personalized DomainAdmin".
- In the **Provisioning** → **Users** view, create a mirror personalized DomainAdmin user object for the new personalized DomainAdmin to hold the encrypted password.
- Change to the **Data View** and then set this password (edit the mirrored user object's **userpassword** attribute).
- In the new personalized DomainAdmin, use the **Mirrored User** field (**Provisioning** → **Users** → *new personalized DomainAdmin* → **Authentication** tab → **SASL external bind** section) to link the mirror personalized DomainAdmin to the new personalized DomainAdmin.
- Change to **Data View** → **Connectivity**. In this view, create another mirrored user for the personalized DomainAdmin with the same password as the mirror personalized DomainAdmin you created in the Provisioning view and then add it to the DirXmetahub read and write groups (See step 7 in the chapter "Creating a Personalized DomainAdmin").
- Set up the login profile for Provisioning as described in the section "Set up the Login Profiles".

3.2.3. Configure DirX Identity - Connectivity

To add new personalized DomainAdmins for smart card logins to the Connectivity side, follow the instructions in the section "Configure DirX Identity - Connectivity".

4. Creating a Personalized DomainAdmin

To create a personalized DomainAdmin in the Provisioning view:

1. Log in with DirX Identity Manager to your Provisioning domain.
2. In the **Provisioning** → **Domain Configuration** view, copy **DomainAdmin**.
3. In the **Provisioning** → **Users** view, paste the copy into the Users subtree at the desired location. Copy the object in the TEMPLATE state (same groups, same password, and so on).
4. In the DirX Identity Manager **Data View**, change the password.
5. In the **Data View**, rename your copied **DomainAdmin** to a name of your choice.
6. In the **Provisioning** → **Users** view, reset the **Use as Template** operational parameter for your personalized DomainAdmin.
7. (Alternate scenario only):
   a. Change to the **Connectivity** view.
   b. Create the mirrored users in **dxmC=dirxmetahub,dxmc=users,cn=** *Domain*,**cn=Users,***same_substructure_as_in_provisoning*,**cn=***new name*.
   c. The password of the mirrored user(s) in the Connectivity view must be identical to the password of the mirrored user(s) in the Provisioning view.
   d. Append the mirrored user(s) to **dxmC=dirxmetahub,dxmc=groups,cn=Write** and **dxmC=dirxmetahub,dxmc=groups,cn=Read**.
8. In the **Provisioning** → **Users** view, append the following groups to the personalized DomainAdmin you created in steps 1-6.
   - AuditAdmins
   - BusinessObjectAdmins
   - PolicyAdmins
   - ServerAdmins
   - ServiceDeskOperators

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.