EVIDEN

Identity and Access Management

DirX Identity

DirX Password Reset Client - Installation and Configuration

Version 8.10.13, Edition October 2025

Table of Contents

Preface

This manual provides information about installing and configuring the DirX Password Reset Client and partly of the corresponding Web Services.

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. DirX Password Reset Client - Installation and Configuration

This chapter describes the installation and configuration of the DirX Password Reset Client and partly of the corresponding Web Service.

The back end site consists of

- Provisioning Servlet (deployed in a Tomcat server)
- DirX Identity system with at least Java-based server and messaging server (Active MQ)
- Active Directory (as a connected directory; could be several ones)

Abbreviations used in this document:

DPRS
: DirX Password Reset Server (backend server connected to the customer Active Directory)

DPRC
: DirX Password Reset Client (Windows credential provider on customer client PC)

Supported modes:

DPRC supports two different modes:

- Kiosk mode: In this mode a pre-configured local account is used to setup the VPN connection to the corporate Domain controller to set the password in Active Directory and to cache the password on the client side. This mode supports corporate and Internet LAN/WLAN environments (no hotel scenarios). As VPN software the customer-specific VPN software can be used.
- Pure credential provider mode: In this mode no local account is used. This mode also supports corporate and Internet LAN/WLAN environments (no hotel scenarios). The difference to the kiosk mode is that the VPN software must allow setting up a connection at pre-login state. So far, only Juniper Pulse does allow that. This mode also supports smart card authentication in corporate networks.

Prerequisites:

- DPRS is set up
- Client PC is installed with Windows 10.
- Client PC is connected to internal corporate LAN or to external LAN (Internet) or pre-defined WLAN
- If the smart card option is used: PKI base client 5.7 or 5.8 with Atos Card OS API V5.2 or higher is installed on the PC.
  Note: The smart card option is possible only in corporate networks.
- If VPN is used: For pure credential provider mode, Juniper Pulse version 5 is installed

and pre-configured. For kiosk mode, the relevant VPN software is installed and pre-configured.

Functional information:

- The DPRC offers three operation modes that can be combined:
- Smart card option (in corporate networks only)
- Authentication questions option
- Mobile OTP (one-time password) option
- A combination of these 3 options
- The dialog language corresponds to the Windows system language setting. If the current Windows 7 language is not supported by the password reset client, the dialogs are displayed in English.
- The password reset uses the combination of account and domain name – not the username.
  Smart card option only: If a user (real person) has multiple accounts or the same account name across multiple domains, the password reset detects the correct account based on the combination of domain name, account name and GID (serial number from smart card).
- Smart card option only: The email address from the certificate is always extracted and sent in the request.
- Smart card option only: The GID is extracted from the certificate (on client side) and the AD account import (server side). The validation on server side checks that the AD account GID string contains the client certificate GID. Therefore, functional users with a GID string like *prefix-GID-suffix* can reset their account password as well.
- Smart card option only: The certificate on the smart card must be applicable for digital signatures. The DPRC will display only such certificates.
- Smart card option only: The issuer of the root CA certificate must be in the local computer store of the client.
- Authentication questions only and Password dialog: The password reveal button and an informal note on which keyboard layout is activated is integrated.
- Authentication questions only: Hostname check can be configured. If activated, the hostname and the domain of the host (which can be a different domain than the one from the account) is sent in each request to the back end. On the backend, an additional check on these attributes can be configured (registry key: computerSIDoption).

License information:

- The Visual C++ Redistributable Package for Visual Studio 2017 is Microsoft license-free software
- The Microsoft .NET Framework 4.7.2 package is Microsoft license-free software
- The DPRC itself is licensed within the DirX Identity Product
- License relevant DPRC build regarding 3rd party SW:

- JavaProperties reader license: Apache
  (http://www.apache.org/licenses/LICENSE-2.0.html)
- NSpring for Logging
  (see section “NSpring terms of use” at the end of the document)

1.1. DPRC Installation

Installation Files

The DPRC installation consists of following files:

- AtosPasswordResetClient.msi - the DPRC application package
- AtosPasswordResetClient.reg – configuration file for customizing registry settings

Prerequisites are:

- Microsoft Visual C++ 2017 Redistributable - x64 - 14.16.27029 or higher
- Microsoft .NET Framework 4.7.2 or higher

Both prerequisites must be installed beforhand.

DPRCInstaller

The **AtosPasswordResetClient.msi** is a standard MSI installer file that can install DPRC without the bootstrapper if the prerequisites are already met. The default folder where DPRC is installed is C:\Program Files\Atos\Password Reset Client.

The installer supports 2 modes to install:

1) Kiosk mode

The kiosk mode uses client-side SSL connection to the Password reset service. Therefore, the relevant certificates must be installed.

The following must be pre-installed or prepared:

- Microsoft Visual C++ 2017 Redistributable x64 or higher
- Microsoft .NET Framework 4.7.2 or higher
- VPN software, e.g. Junos Pulse 5.0 (Juniper Networks)
- The root CA certificate of the Password reset service is installed in the Trusted Root Certification Authorities folder in the computer store.

The kiosk mode must be installed in the following sequence

- Stop msiserver service:
  sc stop msiserver
- Set SEBackupPrivilege for msiserver service:

```
sc privs msiserver
SeTcbPrivilege/SeCreatePagefilePrivilege/SeLockMemoryPrivilege/SeI
ncreaseBasePriorityPrivilege/SeCreatePermanentPrivilege/SeAuditPri
vilege/SeSecurityPrivilege/SeChangeNotifyPrivilege/SeProfileSingle
ProcessPrivilege/SeImpersonatePrivilege/SeCreateGlobalPrivilege/Se
AssignPrimaryTokenPrivilege/SeRestorePrivilege/SeIncreaseQuotaPriv
ilege/SeShutdownPrivilege/SeTakeOwnershipPrivilege/SeLoadDriverPri
vilege/SeBackupPrivilege
```

this is one command line!.

- Call the installer:
  msiexec /I AtosPasswordResetClient.msi KIOSKMODE=1
- Reset privileges for msiserver service:

```
sc privs msiserver
SeTcbPrivilege/SeCreatePagefilePrivilege/SeLockMemoryPrivilege/SeI
ncreaseBasePriorityPrivilege/SeCreatePermanentPrivilege/SeAuditPri
vilege/SeSecurityPrivilege/SeChangeNotifyPrivilege/SeProfileSingle
ProcessPrivilege/SeImpersonatePrivilege/SeCreateGlobalPrivilege/Se
AssignPrimaryTokenPrivilege/SeRestorePrivilege/SeIncreaseQuotaPriv
ilege/SeShutdownPrivilege/SeTakeOwnershipPrivilege/SeLoadDriverPri
vilege
```

- Call DPRCCertUtil utility to import the client certificate into a new folder in the computer store and to grant access to the certificate for the local account:

```
DPRC_INST_PATH\APRCCertUtil.exe -install -f <clientstore.p12> -p
<p12password>
```

- Exchange the installed VPN scripts in folder DPRC_INST_PATH\VPN. In the scripts the path to the VPN command-line executable, the VPN service URL, and the realm name must be adopted.

In the event log 2 informational entries from Source “AtosPasswordResetClient” should be seen (one for the local account and one for the reg file).

2) Pure credential provider mode

The following must be pre-installed or prepared:

- Microsoft Visual C++ 2017 Redistributable x64 or higher

- Microsoft .NET Framework 4.7.2 or higher
- Junos Pulse 5.0 VPN software
- Prepare the AtosPasswordResetClient.reg file

The pure credential provider mode must be installed in the following sequence

- Calling installer:
  msiexec /I AtosPasswordResetClient.msi KIOSKMODE=0

To reinstall the same DPRC version or install this version over a previous version, the previous instance must be uninstalled. This is because of an issue in the Microsoft Studio Installer extension in use. It means that a higher version of the DPRC cannot be installed without uninstalling the previous version.

De-installation

For the kiosk mode, the uninstallation must be done in the following order:

- Call DPRCCertUtil utility to delete the client certificate from the Atos folder in the computer store and to revoke access to the certificate for the local account:
  DPRC_INST_PATH\APRCCertUtil.exe -uninstall
- Call the standard Windows package uninstallation routine. The uninstallation will delete the local account.

For the pure credential provider, there is no extra step to perform.

DPRC Registry Configuration File

The following table contains all configuration parameters in the registry. The option column shows which entry is relevant for ALL options (ALL), smart card option (SC), authentication questions option (AQ). If both options are set in the registry then both SC and AQ are relevant.

This version fetches the password policy from the domain (via the web service) or takes it from registry. This is defined via two registry options.

Note that this version supports the domain setting "Windows compatible policy" which only makes sense together with the password length setting.

Name	Type	Option	Default value	Remarks
SmartCardOption	DWORD	ALL	1	Smart card option; possible values 1 or 0
ChallengesOption	DWORD	ALL	1	Authentication questions option; possible values 1 or 0
OTPOption	DWORD	All	1	Mobile OTP option; possible values 1 or 0

Name	Type	Option	Default value	Remarks
DefaultOption	String	ALL	SmartCardOption	Defines which option is first in drop-down list to choose from.
VPNOption	DWORD	ALL	1	Defines if VPN scripts should be called
KioskModeOption	DWORD	ALL	1	Defines the kiosk mode option when set to 1 otherwise pure credential provider mode
ClientCertificateSubject	String	ALL	empty	Subject of the client certificate
ClientCertificateStoreName	String	ALL	Atos Password Reset	Name of the folder in which the client certificate is searched in
ComputerSIDOption	DWORD	ALL	0	Defines if the long hostname and computer domain name is put in every request.
KioskModeParam	String	ALL	empty	Internally used for kiosk mode
InstallDir	String	ALL	C:\\Program Files\\Atos\\Password Reset Client\\	Installation directory (do not change)
RootCAIssuer	String	SC	Identity	String value that must match issuer in the chain of CA certificates; can be left empty
ServerCertIssuer	String	SC	Identity	String value that must match issuer in the web service certificate (https); can be left empty
SslServerCertificateSubject	String	SC	<empty>	String value that must be in the subject of the web service certificate; can be left empty
CompanyName	String	ALL	Atos	String value that is not allowed in passwords; can be left empty

Name	Type	Option	Default value	Remarks
Vendor	String	ALL	Atos IT Solutions and Services GmbH	Vendor (do not change)
EndpointURL	String	ALL	https://*host:port/servlet-name*/services/Spmlv2RequestService	URL of the corporate web service; host, port and servlet-name must be customized
EndpointURLExternal	String	ALL	https://*external-host:external-port/ servlet-name*/services/Spmlv2RequestService	URL of the external web service; host, port and servlet-name must be customized
WildcardCertificate	DWORD	ALL	0	Defines if the server certificate can be a wildcard certificate
VerifyCorporateURL	String	ALL	http://*corporate-host:corporate-port*	URL of a second internal accessible web site or service (used to verify internal network connectivity even if internal reset service is down)
InactivityTimeout	DWORD	ALL	180	Set the timeout (in seconds) after which DPRC will be closed if no input from the user occurs (mouse move or keyboard). If set to 0 then this is disabled.
BindingSendTimeout	DWORD	ALL	60	Sets the interval of time (in seconds) provided for a write operation to complete before the transport raises an exception.
BindingOpenTimeout	DWORD	ALL	60	Sets the interval of time (in seconds) provided for a connection to open before the transport raises an exception.

Name	Type	Option	Default value	Remarks
BindingReceiveTimeout	DWORD	ALL	600	Sets the interval of time (in seconds) that a connection can remain inactive, during which no application messages are received, before it is dropped.
GetStatusInterval	DWORD	ALL	5	Interval (in seconds) that the GetStatus request is executed as long as “pending” is returned.
GetStatusTimeout	DWORD	ALL	60	Timeout value (in seconds) for the GetStatus request.
LogLevel	String	ALL	INFO	Defines which kind of log messages is written. Possible values in order: DEBUG, INFO, WARNING, ERROR. If set to INFO then informal and higher messages are written.
LastLoggedOnSAMUserBackup	String	ALL	empty	Used for kiosk mode to save the last logged on username
PwdMinCharLength	DWORD	ALL	8	The minimum length of the password.
PwdMaxCharLength	DWORD	ALL	20	The maximum length of the password.
PwdMinLowerChar	DWORD	ALL	0	The number of lowercase characters required for the password.
PwdMinUpperChar	DWORD	ALL	0	The number of uppercase characters required for the password.
PwdMinNonAlphaNum	DWORD	ALL	0	The number of non-alphanumeric characters required for the password. Non-alphanumeric characters comprise all characters that are not letters and numbers.

Name	Type	Option	Default value	Remarks
PwdMinSpecialChar	DWORD	ALL	0	The number of special characters required for the password. Special characters comprise all characters besides letters.
PwdMinNumeric	DWORD	ALL	0	The number of numeric characters required for the password.
PwdProhibitChars	String	ALL	""	Defines prohibited characters ,e.g. äöü
PwdInHistory	DWORD	ALL	3	Defines the number of passwords that are stored in the history record (in DirX Identity).
PwdWindowsCompatible	DWORD	ALL	1	Defines the Windows password complexity requirements.
AutoSelectSingleCertificate	DWORD	ALL	0	In case of smart card option, defines whether the list of valid and useable certificates on the smart card is shown (with selection option).
UsePoliciesFromService	DWORD	ALL	1	Defines if policies are fetched from service. Only one of these values must be “1”.
UsePoliciesFromRegistry	DWORD	ALL	0	Defines if policies are taken from registry (not from service) Only one of these values must be “1”.

Detailed configuration:

1. The root CA certificate including any intermediate certificates of the DPRS server must be present in the local computer store under Trusted Root Certification Authorities of the Windows 7 client.
2. Configure correct web service URLs in windows registry of the client in path HKEY_LOCAL_MACHINE\SOFTWARE\Atos\Password Reset Client keys EndpointUrl, EndpointURLExternal, and VerifyCorporateURL.
   Server name in URL must match the server certificate DN used for SSL; given as fully qualified domain name (FQDN); names are case-sensitive.
   This can be done via the reg configuration file.

3. Configure correct Root CA issuer name string in windows registry of the client (HKEY_LOCAL_MACHINE\SOFTWARE\Atos\Password Reset Client\RootCAIssuer). This depends on the root CA issuer of the customer e.g. for Siemens the wildcard string is “Siemens”. The DPRC client checks if the issuer of the root CA certificate (must be in local computer store) contains this string (string compare is done both in upper case). This can be done via the reg configuration file.
4. Configure correct Root CA issuer name string in windows registry of the client (HKEY_LOCAL_MACHINE\SOFTWARE\Atos\Password Reset Client\ServerCertIssuer). For example, for Siemens the wildcard string is “Siemens”. The client checks if the issuer of the server certificate contains this string (string compare is done both in upper case). This can be done via the reg configuration file.
5. Using kiosk mode: set VPNOption, KioskModeOption, and ChallengesOption to 1 (and/or OTPOption), SmartCardOption to 0. This mode uses client-side SSL connection if connected to the Internet. So set the ClientCertificateSubject and ClientCertificateStoreName. For installing the client certificate and creating the store folder the utility DPRCCertUtil must be used.
6. Using pure credential provider mode: set VPNOption to 1, KioskModeOption to 0. ChallengesOption, OTPOption and SmartCardOption can all be set to 1 (or to 1 and 0). Smart card option does only work in corporate networks. This mode uses client-side SSL connection if connected to the Internet. So set the ClientCertificateSubject and ClientCertificateStoreName. For installing the client certificate and creating the store folder the utility DPRCCertUtil must be used.
7. The computer SID option can be used in both modes. This must be configured on both sides, DPRC and DPRS. In this case, DPRC is sending the long hostname and the computer domain name in each request. On the backend side this can then be verified. (It was intended to use the computer SID but then changed to hostname as the computer SID from the DC is not stored on the computer locally; the name of the registry key has not been changed).

1.1.1. DPRC Smoke Test

After DPRC is installed, logout or restart the system and press Switch user in the login screen. The DirX Password Reset logon tile should now be visible.

1.1.2. DPRC Troubleshooting

To resolve potential DPRC problems (no login tiles displayed) reboot in safe mode. The safe mode activates only the built-in credential providers and the logonUI is not influenced by any custom plug-ins. Then it is possible to login as usual and uninstall the DPRC application.

In case of errors, provide the log files DPRC located in C:\Windows\Temp (or path defined by system environment variable TEMP) or C:\Users\Public\DirX Password Reset Client:

AtosPasswordResetClient.log and AtosPasswordResetClient-bak.log.

The client alternates these log files.

In the registry the configuration is under the key
HKEY_LOCAL_MACHINE\SOFTWARE\Atos\Password Reset Client

For more logging set LogLevel to DEBUG (default is INFO).

The installation writes entries in the application event log. Look for Sources “AtosPasswordResetClient” and “MsiInstaller”. For kiosk mode, two informational entries are created if successful. For pure credential provider, one informational entry is created. Otherwise error entries are created.

1.1.3. DPRC Known Issues

Smart card only: Clients and server machine should use time synchronization. If the client time (creation timestamp of request) is more than 60 seconds in the future compared to the server then the request will fail. Also note that a request expires after 300 seconds.

1.1.4. DPRC 3rd Party Software Licenses

1.1.4.1. NSpring

The NSpring Framework for .NET

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

- Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
- Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
- Neither the name of the NSpring project nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission from the copyright owner.
- No product derived from this software may be called "NSpring", nor may "NSpring" appear in the name of such a product, without specific prior written permission from the copyright owner.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED.IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY,

WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

1.2. Implementation Details

1.2.1. Smart Card Option

In the smart card mode the following sequence of requests are sent to the back end service:

1. GetPasswordPolicy
2. SetPassword
3. Status (one or more times)

The first two requests are signed with the selected smart card certificate. The Status request is not signed.

The following identifying attributes are sent in the signed requests:

- Domain\account as ts.dxrtsdomainname\dxrname from user input OR
- UPN as principalName from user input if this is given
- Serialnumber from the smart card as serialnumber (not configurable)
- RFC822 name from the smart card as user.mail (not configurable)
- Hostname (long form) and computer domain name as computer.machineSID, computer.domain if ComputerSIDoption in registry is enabled (obtained via Win32 API functions).

The Status request just contains the syncRequestID from the SetPassword request. No part of any request is encrypted. In corporate networks server-side SSL/TLS protocol is used, in non-corporate networks client-side SSL/TLS protocol.

Smart card mode does not need any user entries in the provisioning domain just accounts. The GetPasswordPolicy request will return in this order if available the policy of the account, the target system, or the default policy.

1.2.2. Authentication Question Option

In the authentication question mode the following sequence of requests are sent to the back end service:

1. GetChallenges
2. CheckChallengeResponses (this contains in the response also the password policies)
3. SetPassword
4. Status (one or more times)

No request is signed.

The following identifying attributes are sent in the requests:

- Domain\account as ts.dxrtsdomainname\dxrname from user input OR
- UPN as principalName from user input if this is given
- Hostname (long form) and computer domain name as computer.machineSID, computer.domain if ComputerSIDoption in registry is enabled (obtained via Win32 API functions).
- Challenges and responses in the CheckChallengeResponses and SetPassword request.

The Status request just contains the syncRequestID from the SetPassword request. No part of any request is encrypted. In corporate networks server-side SSL/TLS protocol is used, in non-corporate networks client-side SSL/TLS protocol.

Authentication question mode needs user entries in the provisioning domain. So the drxUserLink attribute in the account must be set and link to a user. The challenges and responses are stored at the user. The CheckChallengeResponses request will return in this order if available the policy of the user, the target system, or the default policy.

1.2.3. Mobile OTP Option

In the mobile OTP mode the following sequence of requests are sent to the back end service:

1. SendOTP (this contains in the response also the password policies)
2. SetPassword
3. Status (one or more times)

No request is signed.

The following identifying attributes are sent in the requests:

- Domain\account as ts.dxrtsdomainname\dxrname from user input OR
- UPN as principalName from user input if this is given
- Hostname (long form) and computer domain name as computer.machineSID, computer.domain if ComputerSIDoption in registry is enabled (obtained via Win32 API functions).
- OTP password in the SetPassword request.

The Status request just contains the syncRequestID from the SetPassword request. No part of any request is encrypted. In corporate networks server-side SSL/TLS protocol is used, in non-corporate networks client-side SSL/TLS protocol.

Mobile OTP mode doesn’t need user entries in the provisioning domain. So the drxUserLink attribute in the account can be set and link to a user. The hashed OTP is stored at the account. The SendOTP request will return the policy in this order: if available the policy of the account, the target system or the default policy.

1.3. DPRS Configuration

1.3.1. DPRS Prerequisites

- AD Target systems with imported AD accounts that should support the DPRC. If authentication questions mode is used then accounts must have a user link and the user should have configured authentication questions.
- AD password reset workflows bound to the above target systems. The AD target system should for clustered set Password workflows have the connector configuration parameter “check_password_history” set to true (AD policy is observed).

1.3.2. DPRS Configuration

The server side configuration depends on the configured authentication mode scenario of the DPRC (smart card option, authentication questions option, OTP option). Depending on which mode is configured then you have to do the configuration according to this or these options.

General steps:

- Configure provisioning servlet on Tomcat with SSL
- In the Tomcat installation folder create a text file named **dxi.cfg** with the content: *cache.update=**timestamp*
- Adjust the following configuration files under *install_path***\provisioningServlet\WEB-INF**. See the “SPML Provisioning Web Services” in the *Integration Framework Guide* for more information:
- accountContext.xml
- applicationContext.xml
- server-config.wsdd
- config.xml
- identifierMatcherConfig.xml
- classes\crypto.properties and classes\password.properties
- Configure the trust store path in *install_path***\provisioningServlet\WEB-INF\classes\crypto.properties** (key name org.apache.ws.security.crypto.merlin.file). Ensure that the trust store contains the CA certificate (or chain of CA certificates) of the user’s certificate (smart card) used to sign the password reset requests. Key org.apache.ws.security.crypto.merlin.load.cacerts has to be set to false even if JRE cacerts is used.
- Configure the trust store password in *install_path***\provisioningServlet\WEB-INF\password.properties** as *signatureTruststore=<password>*
- Uncomment the element tags for the WsTrustHandler in *install_path**\provisioningServlet\WEB-INF\server-config.wsdd* <handler type="java:com.siemens.idm.service.provisioning.wssecurity.WsTrustHandler" >

<parameter name="signatureIsOptional" value="true"/>
<parameter name="action" value="Signature Timestamp"/>
<parameter name="signaturePropFile" value="crypto.properties" />
</handler>
You must use signatureIsOptional=true even if just use smart card option. The status request in not signed in both options.

- File *install_path***provisioningServlet\WEB-INF\identifierMatcherConfig.xml** has to be present and should contain match rules (security issue otherwise). The predefined match rules are email address and serialnumber (GUID).

Authentication questions steps:

- Maintain the number of returned challenges in parameter "numberOfChallenges"
<bean id="GetChallengesAccountsHandler"...,
in parameter "minimumNumberOfResponses" in section <bean id="CheckChallengeResponsesAccountsHandler"...,
and in parameter "minimumNumberOfResponses" in section <bean id="SetPasswordAccountsHandler"...
and in parameter "minimumNumberOfResponses" in section <bean id="GetPasswordPolicyAccountsHandler
in file *install_path***provisioningServlet\WEB-INF\accountsContext.xml**. The number must be the same in all sections.

Mobile OTP steps:

- Configure the OTP parameters, like policy of the one-time password (character sets, length), time-to-live attribute, attribute name of the attribute which holds the mobile number, nationalization placeholder of content of text message in file *install_path***provisioningServlet\WEB-INF\accountsContext.xml**.
- Configure the SMS gateway plug-in for the Send Text Message workflow.

  If you use the smart card option, you need to copy the additional jar file **xalan-2.7.1.jar** to the folder *install_path***provisioningServlet\WEB-INF\lib**. The file **xalan-2.7.1.jar** is provided in the folder *install_path**\provisioningServlet.org\endorsed\extralib*. Note that if you use the smart card option, you cannot use this deployment with this extra jar file for other non DPRC-specific SPML services.

Other Identity-related customizations are outside the scope of this document.

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.