Technical Data Sheet

DirX Identity V8.5

Secure and flexible Password Management

DirX Identity provides a comprehensive password management solution for enterprises and organizations. It delivers self-service and assisted password reset, password expiration management, user enrollment, password listener for Windows, password synchronization, password policy management, privileged account password management and audit and reporting functionality. Providing end users with a quick and flexible way to reset their password based on strong password policies or to unlock their account DirX Identity password management helps organizations to significantly reduce helpdesk costs and to strengthen security of password-related authentication processes.

Bull
atos technologies

Secure and flexible Password Management

The challenges of password usage

Due to the increasing password proliferation users will have to remember more and more passwords with the risk that passwords are forgotten frequently. When a password is forgotten the password reset is most often done via the service desk. This results in high service desk costs especially when the password reset is requested outside office hours. Also password resets cause major service desk call spikes after public holidays or after the weekend.

For security and compliancy reasons organizations tend to introduce stronger password policies resulting in increasing password complexity with the consequence that password are forgotten more often. So there is a delicate balance between security and compliancy on one hand and the number of password reset and related service desk costs on the other hand.

For this reason there is a very strong demand for self-service password reset that allows an organization to enforce stronger password policies but takes away the password related service desk costs. From the user side there is a strong demand to have an instant password reset function anytime, anywhere.

In case users do not have direct access to target systems to reset their passwords, a password management solution should support service desk staff to perform an assisted password reset on request of the user. This requires that service desks agents are supported to properly authenticate users.

As users are required to login with one password per each IT application users must remember a lot of different passwords, one for each system they need to use. As a result, users tend to write down their passwords or to select easy-to-guess passwords which in turn puts system security at risk. To reduce the number of passwords users have to manage, there is also a strong need to synchronize passwords. This helps users to manage only one single password based on a single password policy across multiple IT systems.

Shared, privileged accounts have additional requirements in terms of password management and password usage as privileged accounts are not related to one specific user. Privileged accounts are often used by different administrators. Passwords of privileged accounts should be set by the system, disclosed to administrators when needed and changed after use.

In order to manage consistent password policies a password management solution requires password policy management functionality that also enforces the defined policies when users select new passwords.

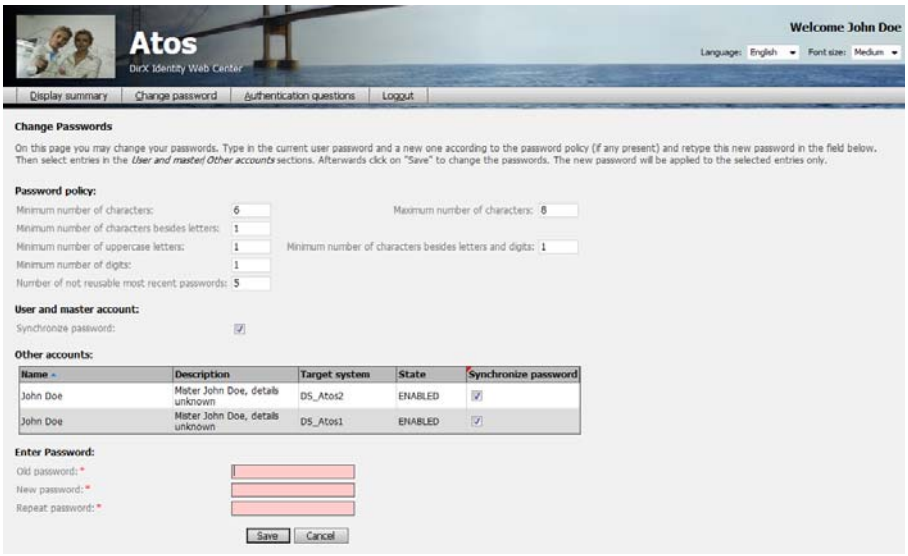

Figure 1 - DirX Identity Password Reset – User Dialog via Web Center

To help ensure and document regulatory compliance or to support billing requirements, audit and reporting functionality is needed to support both administrators and service desk staff.

DirX Identity addresses these challenges by providing a password management solution with a comprehensive feature set.

Feature Overview

DirX Identity Password Management offers the following features:

- Self-service password reset: Users reset forgotten passwords or unlock accounts using alternative credentials.
- Assisted password reset: Administrators or service desk staff reset forgotten passwords or unlock accounts for users.
- Password expiration: Remind users to change their passwords before they expire.
- User enrollment: Users select and answer security questions (also known as authentication or challenge questions) as alternative credentials.
- Password Listener for Windows: Catch password changes from Windows desktop.
- Password synchronization: Synchronize password changes to target systems in real-time.
- Password policy management: Manage and enforce rules for complexity, expiration and history of passwords.
- Privileged account password management: Manage and control access to passwords for shared privileged accounts.
- Audit and reporting: Keep track records of password-related actions and generate reports.

Atos also offers Password Reset as a Service to provide end users a simple and instant way to reset their password or to unlock their account.

Benefits

DirX Identity Password Management provides the following benefits for users and organizations:

- Provides end users with a quick and flexible way to reset their password or to unlock their account.
- Significant reduction of service desk costs through self-service and assisted password reset and password synchronization.
- Strengthened security through fewer passwords for users to remember, enforcement of strong password policies, various authentication options, documentation of password-related actions via audit and reporting.
- Reduced number of passwords to be managed by users through password synchronization.
- Improved user productivity due to fewer service desk calls and fewer login problems.
- Enhanced user experience, i.e. fewer passwords to remember, only a single user interface to deal with, consistent password policies, early password expiration notifications.
- Seamlessly fits in the enterprise Identity and Access Management landscape.

Self-Service Password Reset

DirX Identity Password Management offers password reset functionality to users via a Web user interface and a Windows client.

By default DirX Identity Password Reset is provided for Microsoft Active Directory. Optionally, other target environments can be supported.

In order to reset a password, a user is required to authenticate using alternative credentials. After a positive authentication the password can be changed for the account(s) that the user is authorized to. The new password that is entered will be validated against the password policy of the respective target systems.

Authentication Options

DirX Identity Password Reset supports the following options for alternative authentication:

- ▶Smart card authentication
- ▶Answering security questions
- ▶Mobile OTP (One-Time Password)

If security questions are used for alternative authentication, a user first needs to define the personal set of security questions. After that, the self-service password reset can be used. The number of questions that need to be set up and the number of questions that need to be answered is flexible and depends on the security policy of the organization.

Password Reset via Web Center

The Password Reset Web Center can be accessed via a standard browser. In the case of a forgotten password, users may no longer be able to login to use a browser. In this case, a kiosk system or a browser session from a colleague must be used.

Through the Web Center interface, users can:

- ▶Change their own passwords.
- ▶Reset forgotten passwords by authenticating with security questions.
- ▶Manage the personal set of security questions.
- ▶First time users can register and logon with their AD password and setup security questions.
- ▶Change or reset the passwords for only a subset of their accounts they have in target systems.
- ▶Monitor the password change status (pending, succeeded or failed) for each of the accounts they have selected.

Password Reset via Atos Password Reset Client

The Atos Password Reset Client (APRC) is a Windows client that must be deployed on a user's Microsoft Windows system.

APRC can be accessed and used before logon to Windows (after ctrl-alt-del) via an extra option in the login screen. The advantage of this user interface is that the password reset can be done directly from the workstation of the user. It can be used from within the corporate network or from outside by roaming users.

The Atos Password Reset Client (APRC) offers a configurable deployment mode for selecting alternative authentication methods:

- ▶Smart card authentication
- ▶Security questions
- ▶Mobile OTP
- ▶Any combination of these options.

APRC provides the following functionality:

- ▶Validation of new passwords against the password policy of Microsoft Active Directory.
- ▶The dialog language is set according to the Windows system language setting. For languages that are not supported by APRC, the dialogs show up in English.
- ▶The password reset uses the combination of account and domain name as user ID, not the user name.
  Smart card option only: In case a user (real person) has multiple accounts or the same account name in multiple domains, the password reset detects the correct account based on the combination of domain name, account name and a unique ID (UID).
- ▶Smart card option only: The UID 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 UID string contains the client certificate UID. Therefore functional users with ID string like <prefix>-<UID>-<suffix> are able to reset their account password as well.
- ▶Smart card option only: The certificate provided on the smart card must be applicable for digital signatures. The APRC will display only such certificates.

Assisted Password Reset

For the service desk, DirX Identity provides additional features to support users who do not have direct access to IT systems. Through the Web Center interface, service desk agents can:

- ▶Reset users' passwords on request. They can validate users by challenging their attributes or security questions.
- ▶Create and maintain password policies that control how passwords are used and administered in the enterprise, such as password length and complexity, password aging, and password reuse after expiration.
- ▶Create reports on password changes and resets.

Figure 2 - DirX Identity Password Reset using the Atos Password Reset Client

Password Expiration

DirX Identity Password Management optionally reminds users to change their passwords before they expire by regularly checking for user passwords that are about to expire and by informing the affected users by e-mail notification. The number of notifications to be sent is configurable.

User Enrollment

First time users enroll to the system by registering with their Active Directory account and by selecting security questions and providing answers via the Web Center user interface. Administrators can configure whether users can define their own security questions or just select from the list of predefined questions.

Onboarding/offboarding of users

Both onboarding of users i.e. initial load of the user population to the DirX Identity system and adding users to the system and offboarding i.e. deleting users from the system is accomplished via the identity management functionality of DirX Identity. Synchronization services maintain an accurate and up-to-date identity store of identities which are allowed to use password reset functionality.

Windows Password Listener

The Windows Password Listener catches the user password changes in a Windows domain, encrypts the information and generates password change events. These trigger the event manager and the corresponding password change workflows to synchronize changed password to the connected target systems.

The Windows Password Listener is suitable for Microsoft Windows 2008 R2 and 2012 servers.

Password Synchronization

DirX Identity Password Management allows users to maintain a single password that will be automatically synchronized with Microsoft Active Directory and optionally to other relevant IT systems, where the user has accounts.

This event-driven, real-time password synchronization service ensures that password changes made from the Web Center interface or from the Windows system are immediately synchronized to the users' accounts in the appropriate target systems. Preconfigured password synchronization workflows are provided to perform the password synchronization.

Password Policy Management

Administrators or service desk staff can define password policies compliant with application password policies in the enterprise. They determine password length and complexity, password aging, password history, behavior of the system after failed logins and password reuse after expiration.

Privileged Account Password Management

In addition to accounts that are related to just one specified identity (user), target systems typically hold a small number of privileged accounts that are entitled to target system management. Such accounts, as for example the root account in UNIX systems, are allowed to perform critical actions in the target system with a high security risk. Privileged accounts are not related to a specific user. A number of persons can use them in parallel.

DirX Identity provides means to control and audit password usage of privileged accounts:

- Users that are assigned to privileged accounts can read the password in clear text to perform the login action.
- They are also entitled to change the password of privileged accounts.
- Removal of a user from a privileged account automatically enforces a password change.
- Alternatively one can define that assignment of a user to a privileged account copies his certificates to the account. This allows authentication via certificates at the target system side.
- DirX Identity automatically changes all expired privileged account passwords.

Audit and Reporting

To help ensure and document regulatory compliance and to support billing, DirX Identity keeps track records of password-related actions via its audit trail mechanism. Standard reports are provided, such as:

- Number of registered users for password management
- Users with all properties
- Users with compact password management history
- Users with password management
- Users with password management history
- Users with privilege hierarchy
- Users without privileges

Both the audit trails and reports are configurable and customizable to best suit customer requirements.

Architecture

DirX Identity Password Management builds on the core features of the product DirX Identity and on the product DirX Directory that serves as the configuration and user repository. DirX Identity Password Management uses the agents and connectors of the connectivity framework of DirX Identity to implement the password reset functionality for the connected systems. DirX Audit can be used for centralized, secure storage, analysis, correlation and review of password-related audit logs.

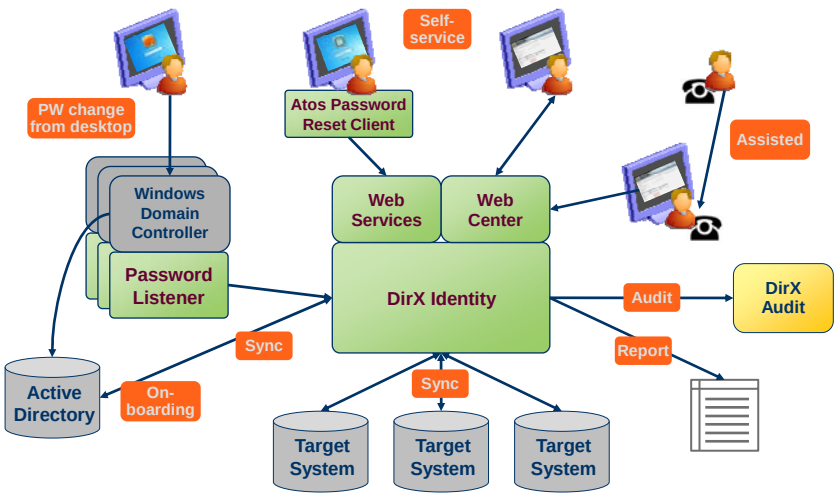

Figure 3 - DirX Identity Password Management Architecture

DirX Identity

DirX Identity provides a comprehensive, process-driven, customizable, cloud-ready, scalable and highly-available identity management solution for enterprises and organizations. It delivers overall identity and access governance functionality seamlessly integrated with automated provisioning. Features include life-cycle management for users and roles, cross-platform and rule-based provisioning in real-time, Web-based user self-service and delegated administration, request workflows, access certification, password management, metadirectory and auditing and reporting.

DirX Directory

DirX Directory provides a standards-compliant, high-performance, highly available, highly reliable and secure LDAP and X.500 directory server with very high linear scalability. DirX Directory can act as the identity store for employees, customers, trading partners, subscribers, and other e-business entities.

DirX Audit

DirX Audit provides auditors, security compliance officers and 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, a monitor for identity-related events and job management for report generation. With its analytical features, DirX Audit helps enterprises and organizations to ensure sustainable compliance and provide business intelligence for the identity and access management processes.

Security

The authentication and authorization mechanisms of the respective LDAP directory allow protecting attributes and passwords. DirX Identity provides additional security features:

- All components can optionally work in SSL/TLS mode when using LDAP connections.
- Data transfer via the messaging service can be encrypted to provide high security during network transfer.
- Passwords, security questions and their related answers can be stored in strong

encrypted mode in the Identity store. DirX Identity guarantees that data transfer and logging is secure up to the interface of the connected target directory.

Password Reset as a Service

In addition to the password management functionality provided with the product DirX Identity, Atos also offers Password Reset as a Service to provide end users a simple and instant way to reset their password or to unlock their account.

The Password Reset Service can be offered as a

- ▶Shared service
- ▶Customer dedicated service on Atos premise
- ▶Customer dedicated service on customer premise

The Atos Password Reset Services is provided for both Microsoft Active Directory and optionally for other environments.

Password Reset as a Service provides a number of additional benefits to customers:

- ▶Provides a high level of agility - rapid deployment
- ▶All inclusive approach – avoids upfront HW / SW investments - no CAPEX
- ▶Technology agnostic – customer can focus on functionality instead of technology
- ▶External and internal access
- ▶Multiple target platforms supported
- ▶Password reset and unlock
- ▶24*7*365 available: anytime-anywhere

System Requirements

Hardware

- ▶Intel server platform for Microsoft Windows Server 2008 R2, Microsoft Windows Server 2012 R2, Red Hat Enterprise Linux, SUSE Linux Enterprise Server
- ▶Sparc processor servers for Oracle Solaris

Memory requirements:

Main memory: minimum 4 GB

Disk Space: minimum 4 GB plus disk space for data

Software

- ▶DirX Identity V8.5
- ▶DirX Directory V8.3/V8.4
- ▶DirX Audit V4.0/V5.0

For the DirX Identity Web Center

- ▶Microsoft Internet Explorer 8 or newer
- ▶Mozilla Firefox 38 or newer
- ▶Google Chrome 45 or newer
- ▶Microsoft Edge

For the Atos Password Reset Client (APRC)

- ▶Microsoft Windows 7 64-bit

User interface

English

Web Center: English / German / customizable

APRC: English / German / customizable

Documentation

- ▶DirX Identity documentation
- ▶DirX Directory documentation
- ▶APRC documentation

F-DirX Identity 8.5pw en1

For more information: Please contact security@atos.net or visit www.atos.net/identity

atos.net

Atos