

Identity Provisioning

Automation and control of identity management

Overview

Many organizations are dependent on their identity data to be correct so authentication and data access works securely and successfully. User objects are most likely to exist in several user stores, both local and cloud. PhenixID Identity Provisioning (PIP) provides an easy to use application to automatically handle creation, change and deletion of user object in different user stores.

Features

Provision, synchronize and de-provision user objects.
Several user store connectors included.
Create status reports and send them scheduled to stakeholders.

Get in control

With PhenixID Identity Provisioning (PIP) you will have optimal control over the status of your user accounts. With PIP you can create status reports for managers or IT regarding user status and have them emailed e.g. first monday each month. You can also create alerts when security policies are breached. Inactive and unauthorized user accounts are not only a security risk, but also affects license costs.

Reduce costs

Automate your manual processes regarding user management. Easy to get started with a user friendly and easy to work with tool. Get in control, does the number of active users match the number of licenses?

phenixid.se/try-it

PhenixID - Provider of secure identity and authentication solutions

PhenixID, Cylindervägen 12, SE-131 52 Nacka Strand, Sweden · Phone: +46 (0)8 667 75 55 Email: info@phenixid.se Web: www.phenixid.se



Overview

PhenixID Identity Provisioning (PIP) is a service that can leverage corporate rules and policies regarding the handling of electronic identity and information

Several connectors supported

PIP includes several connectors to simplify the integration to your user stores:

- LDAP directory
- ODBC or JDBC database connection
- Imported LDIF or comma-separated files
- Web/REST services interface

User friendly and easy to use tool

PIP includes a tool that does not require developing skills to perform different tasks. The tool offers graphical components that easily can be used together to create e.g. different user provisioning scenarios.

Password reset through mobile app

Using PhenixID One Touch, a user can easily reset a forgotten password just by tapping "Reset password" using the app. The user does not need to remember a URL to the Password Reset web page, they just need to remember using the app to reset their forgotten password.

Architecture

The architecture consists of a server engine and components such as Policies, Data Sources, Actions and Schedules.

Policy based

A policy has multiple functions and is the component that holds the logical concept by which policies are constructed:

- Data source connection and configuration to use for obtaining information
- A schedule is set to start and execute the desired process
- Actions are defined in the policy and the order, in which these actions shall be executed, is set

Synchronization

Data can be synchronized to one data source or distributed to multiple data repositories simultaneously.

Reporting

Create status reports and send them scheduled to stakeholders.

Actions

The obtained information can be modified by the Actions configured in the policy.

- | | |
|---------|---|
| Input | Adds data from one or more Data Sources to the objects virtual image by creating new session objects or attributes. |
| Process | Updates existing session objects and their attributes. |
| Output | Saves data from existing session objects and their attributes by writing to one or more data repositories or export to a supported file format. |

Scheduler

There are three types of Schedulers.

- Scheduled policies are configured in the administrative user interface to be executed at a specified time or interval.
- Manual policies can only be executed in the administrative user interface or triggered by an Action configured in the administrative user interface.
- Persistent Search Policies can be configured for an LDAP directory that supports Persistent Search or an Active Directory with DirSync control. Policies of this type start a separate thread that listens to the directory. When the thread notifies the Policy of specified events, the Policy automatically executes its configured actions.

API

The service includes an API that lets you develop custom Actions as needed in case the enclosed actions are not sufficient.

Alerts

Send alerts/notifications as mobile text messages or email if for example:

Key user account changed its password. A text message will be sent to Security Officers.

Sudden change of group membership for groups with high security access. A text message will be sent to Security Officers.

Why PhenixID?

We are a Swedish company based in Stockholm.

Our focus is to create applications that solve customer challenges while at the same time keep the cost at a low level. All our products are built on open standards.

All methods for delivering one-time passwords are included in the license. Technical training is available at request.

Third line support, with highly experienced technicians.