NetIQ Identity Manager Quick Start

December 2014

This document provides a task-based view of Identity Manager components and services.

1 Planning Your Deployment

Planning is key to customizing Identity Manager to meet the needs of your business environment.

Designers are information technology professionals who act in the role of a designer or architect of identity-based solutions, such as enterprise IT developers, consultants, sales engineers, architects, system designers, and system administrators. Designers should have a strong understanding of directory services, databases, and their information environment.

Components or Tools

- Designer

Library Resources

- Installing Designer for Identity Manager in the *Setup Guide*
- *Understanding Designer for Identity Manager*
- *Designer Administration Guide*
- *Policies in Designer Guide*
- *User Application Design Guide*
- *Credential Provisioning Guide*
- *Security Guide*
- *Catalog Administrator User Guide*

Key Tasks for Architects and Administrators

- ☐ Planning for, installing, and configuring Designer
- ☐ Planning your identity solution
- ☐ Securing your identity solution
- ☐ Configuring roles, resources, and workflows using Designer
- ☐ Deploying a staging environment to test your solution

2 Preparing Your Data

Analyzer helps you to analyze, clean, and prepare your data for synchronization.

Components or Tools

- Analyzer

Library Resources

- Installing Analyzer for Identity Manager in the *Setup Guide*
- *Analyzer Administration Guide*

Key Tasks

❒ Planning for, installing, and configuring Analyzer

❒ Understanding the Analyzer tool

❒ Analyzing and cleaning up data

❒ Reporting unique values in a data set

❒ Reporting matching information between data sets

❒ Security considerations

3 Installing and Configuring Identity Manager

Library Resources

- *Setup Guide*

Understanding

❒ Components

❒ Tools

❒ Data

❒ User Access

Checklists for Installation

❒ Planning

❒ Identity Vault

❒ Identity Manager Engine, Drivers, and Plug-Ins

❒ Remote Loader

❒ iManager

❒ Designer

❒ PostgreSQL and Tomcat

❒ Single Sign-on and Password Management

❒ Identity Applications - readiness

❒ Identity Applications

❒ Identity Reporting

❒ Analyzer

❒ Single Sign-on Access Configuration

❒ Activating

❒ Upgrading

❐ Migrating

❐ Using the Integrated Installer

❐ Configuring in Cluster Environments

  - General requirements
  - Identity Vault considerations and installation
  - Identity applications prerequisites and preparing for the User Application
  - Self-Service Password Reset considerations
  - User Application considerations

4 Building Policies

Identity Manager uses policies to manipulate and synchronize data to the different connected systems. Policies control how information flows from one system to another, and under what conditions.

Tools

- Policy Builder in Designer
- Policy Builder in iManager

Library Resources

- Installing Designer for Identity Manager in the *Setup Guide*
- Installing iManager in the *Setup Guide*
- *Policies in Designer Guide*
- *Policies in iManager Guide*
- *Credential Provisioning Guide*
- *User Application Administration Guide*

Key Tasks

- Understanding policy types
- Managing policies with the Policy Builder
  - In Designer
  - In iManager
- Managing credential provisioning policies
  - In Designer
  - In iManager
- Using Policies to Start Workflows Automatically
- Creating Policies to Support Entitlements

5 Building Driver Sets and Drivers

Driver sets synchronize data between connected systems according to the rules you set in them. Each driver in a driver set defines the connectivity and data exchanged between two connected systems.

Components or Tools

- Identity Manager drivers
- Your custom drivers

Library Resources

- Installing the Identity Vault in the *Setup Guide*
- Installing the Identity Manager Engine, Drivers, and Plug-ins in the *Setup Guide*
- Installing and Managing the Remote Loader in the *Setup Guide*
- *Driver Administration Guide*
- *Entitlements Guide*
- *Entitlements Service Driver Implementation Guide*
- Identity Manager Drivers Documentation website

Key Tasks for Administrators

❐ Creating and managing driver sets and drivers

❐ Configuring and managing entitlements

❐ Monitoring driver health

6 Synchronizing Your Data

NetIQ provides Identity Manager drivers to connect to and synchronize data between various identity directories, applications, and databases that run on different platforms. For each data set, you must configure its related driver to synchronize identity data.

Library Resources

- *Driver Administration Guide*
- Identity Manager Drivers Documentation website

Key Tasks

❐ Understanding data synchronization

❐ Understanding the components for synchronizing your identity data

❐ Viewing and managing associations between drivers and objects in the Identity Vault

❐ How data is synchronized between connected systems

❐ Prioritizing synchronization of certain events

7 Roles and Resources

The User Application’s Roles-Based Provisioning Module provides an easy way to assign people to privileges in target systems through their role membership. You can use the Catalog Administrator to manage roles and resources, associate resources to roles, and manage separation-of-duties conflicts between roles.

Tools

- Roles-Based Provisioning Module
- Catalog Administrator

Library Resources

- Installing the Identity Applications in the *Setup Guide*
- *Catalog Administrator User Guide*
- Configuring Roles in the *User Application: Design Guide*

Key Tasks

- ❐ Catalog Administrator tool
  - Configuring roles
  - Configuring resources
  - Configuring separation of duties constraints
  - Associating roles and resources
- ❐ Assigning users, groups, and containers to administrator roles
- ❐ Modifying the default administrator roles
- ❐ Assigning users, groups, and containers to teams
- ❐ Controlling navigation access permissions for roles and resources management interfaces
- ❐ Managing roles in the User Application
- ❐ Managing resources in the User Application
- ❐ Managing separation of duties constraints in the User Application
- ❐ Viewing reports about roles

Key Roles

- Architects
  - Analyzer
  - Designer
- Administrators
  - Identity Vault Administrator
  - User Application Administrator
  - iManager Administrator
  - Role Administrator (Role Module Administrator)
  - Role Manager (Role Module Manager)

- Roles-Based Provisioning Module
  - Domain Administrators
    - Compliance Administrator
    - Configuration Administrator
    - Provisioning Administrator
    - Report Administrator
    - Resource Administrator
    - Role Administrator
    - Security Administrator
  - Domain Manager
    - Provisioning Manager
    - Resource Manager
    - Role Manager
  - Team Manager

8 Workflows for Provisioning

Roles-based provisioning ensures that access to corporate resources complies with organizational policies and that provisioning occurs within the context of the corporate security policy. Workflows start automatically when a user starts a provisioning request by requesting a resource. The User Application driver listens for events in the Identity Vault, and can be configured to respond to events by starting the appropriate provisioning workflows.

Library Resources

- Installing the Identity Applications in the *Setup Guide*
- *User Application: Administration Guide*

Key Tasks for Administrators

❒ Configuring provisioning

❒ Configuring Provisioning Request Definitions

- Creating the definition
- Creating the request and approval forms for the definition
- Creating the workflow

❒ Managing provisioning request definitions (PRDs)

❒ Configuring and managing provisioning workflows

❒ Managing workflows in iManager

❒ Work Dashboard

- Understanding the Work Dashboard
- Permissions needed for tasks on the Work Dashboard
- Managing your work
- Managing work for users, groups, containers, roles, and teams

- ❒ Configuring a workflow for a provisioning request definition
  - Roles-based workflows
  - Resource-based workflows
  - Types of workflow activities
- ❒ Enabling and configuring support for the mobile Approvals app

Key Tasks for Approvers

- Approving or revoking requests
- Configuring the Approvals app on your iOS device

Key Tasks for Users

- ❒ *Requesting, Approving, and Managing Access to Resources and Roles*
- ❒ Permissions needed for tasks on the Work Dashboard
- ❒ Managing your work

9 Self-Service Login and Landing Page

The Login page performs robust user authentication supported by Identity Manager. The Login page redirects to the other password management pages as needed during the login process.

The landing page provides users a personal view of their permissions, tasks, and requests, as well as the ability to make a new request or search for a role or resource among their current permissions. A user can request hardware, access to a particular server, or permission to use a particular application in their environment.

Library Resources

- Installing the Single Sign-on and Password Management Components in the *Setup Guide*
- Configuring Single Sign-on Access in Identity Manager in the *Setup Guide*
- *Requesting, Approving, and Managing Access to Resources and Roles*
- *Home and Provisioning Dashboard User Guide*
- Exploring the Identity Manager Landing Page in the *User Application: User Guide*

Key Tasks for Administrators

- ❒ Securing the User Application environment
- ❒ Configuring the Login settings for password management (Password Module Setup Login Action)
- ❒ Configuring components for the users’ home landing page
- ❒ Configuring single sign-On (SSO)
- ❒ Configuring digital signatures (requires JBoss)
- ❒ Configuring anonymous or guest access for the User Application
- ❒ Configuring forgotten password
- ❒ Configuring navigation access permissions for the User Application
- ❒ Configuring users and groups with the User Application

Key Tasks for Approvers

- ❒ Approving or revoking access to resources
- ❒ Approving or revoking role assignments

Key Tasks for Users

- ❒ Accessing the User Application
- ❒ Logging in for the first time and setting up challenge response and password hint information
- ❒ Exploring the Identity Manager Landing Page
- ❒ Using the Login page for password management
- ❒ Viewing and managing your tasks
- ❒ Viewing your permissions
- ❒ Requesting access to roles or resources (browsing, requesting, checking)
- ❒ Viewing your request history
- ❒ Viewing and modifying your profile
- ❒ Changing your password
- ❒ Viewing your organization chart
- ❒ Search for users and view their identity information (limited content)
- ❒ Installing and using the mobile Approvals app

10 Self-Service Identity Management

You can display and manage user identity information in the User Application.

Library Resources

- Installing the Identity Applications in the *Setup Guide*
- Using the Identity Self-Service Tab in the *User Application: User Guide*

Key Tasks for Administrators

- ❒ Accessing the Identity Self-Service
- ❒ Creating a user or group to add to the directory service
- ❒ Customizing the user view of information in the Identity Vault
- ❒ Defining manager-employee relationships and group memberships among Identity Vault objects
- ❒ Configuring properties for searches

Key Tasks for Users

- ❒ Accessing the Identity Self-Service
- ❒ Viewing, editing, or hiding your personal information
- ❒ Searching for and viewing identity information for others
- ❒ Displaying manager-employee relationships and group memberships in an organizational chart

11 Self-Service Password Management

The self-service capabilities of Identity Manager allow users to edit their own profiles, search a directory, change their passwords (including password hints and challenge responses), review password synchronization status, and, if authorized, create accounts for new users or groups.

Library Resources

- Installing the Single Sign-on and Password Management Components in the *Setup Guide*
- *Identity Manager Password Management Guide*
- Using the Identity Self-Service tab in the *User Application: User Guide*
- Configuring forgotten password self-service
- Deploying Universal Password in the *Novell Password Management Administration Guide*

Key Tasks for Administrators

□ Understanding the Password Management Service

□ Understanding Password Self-Service

□ Configuring Password Management settings in the User Application

  - Challenge response
  - Forgotten password
  - Login
  - Password synchronization status
  - Password hint change
  - Change password
  - Generic password policy user DN
  - Configuring a PasswordManagement group with rights to view users' password synchronization status

□ Enabling the **Forgot password?** link for Identity Manager Home login page

Key Tasks for Users

- Logging in for the first time and setting up challenge response and password hint information
- Configuring your challenge response
- Changing your password hint
- Changing your password

12 Email Notification

Identity Manager provides an email notification system to notify administrators or users of actions or results that occur, such as password management, jobs status, and provisioning requests that are pending approval. You can specify triggers and the content of email messages that users receive in response to them.

Library Resources

- *Identity Manager Email Notification Guide*
- Setting Up Email Notification Templates in the *Designer Administration Guide*

- Send email and Send email template actions in the *Policies in Designer*
- Send email and Send email template actions in the *Policies in iManager*
- Working with Email Templates in the *User Application: Administration Guide*
- Administrative Users in the *User Application: Administration Guide*

Key Tasks for Administrators in Designer

- ❒ Configuring the email notification service to use your SMTP email server
- ❒ Viewing the default email notification messages
- ❒ Customizing email notification messages

Key Tasks for Administrators in iManager

- ❒ Identity Vault Administrator, understanding rights needed for the email notification service
- ❒ Configuring the email notification service to use your SMTP email server
- ❒ Viewing the default email notification messages
- ❒ Viewing the default email notification messages function
- ❒ Customizing email notification messages
- ❒ Enabling email notifications
  - For policies
  - For policies by using templates
  - For password hints
  - For password requests
  - For password synchronization status
  - For roles and resources
  - For workflow-based provisioning status and changes in the proxy, delegate, and availability settings

13 Auditing

You can audit issues of interest and troubleshoot errors.

Library Resources

- Installing the Identity Reporting Components in the *Setup Guide*
- *Reporting Guide for Sentinel*
- NetIQ Sentinel Documentation website

Key Tasks

- ❒ Enabling audit events
  - Analyzer data browser editor events
  - Digital signature events
  - Digital signature documents
  - Driver events in Designer
  - Driver set events in Designer

    - One SSO Provider (OSP) events
    - Operation events
    - Report Module events
    - Role events
    - Transformation events
    - User Application events
- □ Enabling audit events to send to Sentinel
    - Driver events in iManager
    - Driver set events in iManager
    - User Application events in the User Application
    - User-defined events in Policy Builder
    - User-defined events in Status Documents
- □ Viewing audit events from EAS in Identity Manager reports
- □ Setting up Logging
    - Setting log levels
    - Logging User Application events to Sentinel
    - Logging User Application events to OpenXDAS
    - Configuring the Event Auditing Service
    - Configuring Identity Manager for Sentinel

14 Reporting

You can generate reports to gather statistics over the appropriate periods to help you understand trends and identify issues of interest.

Tool

- Identity Reporting Module

Library Resources

- Installing the Identity Reporting Components in the *Setup Guide*
- Administrator Assignments in the *User Application: Administration Guide*
- *Using Identity Manager Reports*
- *Reporting Module Guide*
- *Reporting Guide for Sentinel*

Key Tasks

- □ Understanding predefined Identity Manager reports
- □ Defining, running, scheduling, and viewing reports with the Reporting Module
    - Viewing a report definition
    - Modifying a report definition
    - Creating a custom report definition based on an existing definition
    - Creating a custom report definition with the Report Packaging tool

    - Downloading and importing report definitions
    - Running a report on demand
    - Scheduling reports with the Calendar page
    - Viewing a list of completed and running reports
    - Viewing details of a completed report

❒ Querying and generating auditing reports using Sentinel and a Crystal Enterprise Server

15 Compliance and Attestation

Following the principle of least privilege, NetIQ Access Review helps you ensure that your users have focused access to those applications and resources that they use and cannot access resources that they do not need to access. You can collect user and access information from Identity Manager in a central location, and organize it for review. Users assigned to appropriate global, run-time, or application-specific roles can review all permissions assigned to your users, either individually or as a group, and decide whether those permission assignments are appropriate for your business environment.

Library Resources

- *NetIQ Access Review User Guide*

Key Tasks

❒ Managing Roles for Access Review

- Understanding roles
- Adding users and assigning roles
- Configuring application-specific roles

❒ Using Identity Manager with Access Review

- Integrating Access Review with Identity Manager
- Configuring automated provisioning fulfillment
- Configuring external provisioning workflow fulfillment

❒ Importing Identity Manager information into Access Review catalogs

❒ Reviewing user access and provisioning

16 Upgrading Components

You can upgrade Identity Manager components individually. You can upgrade servers one at a time. The driver sets associated with multiple servers continue to work with the different versions as you upgrade the servers.

Library Resources

- Upgrading Identity Manager in the *Setup Guide*

Key Tasks

❒ Checklist for upgrading Identity Manager

❒ Preparing to upgrade Identity Manager

❒ Upgrading Identity Manager components

17 Migrating Data to a New Installation

You can migrate existing data in Identity Manager components to a new installation when there is no upgrade path from your current setup.

Library Resources

- Migrating Identity Manager Data to a New Installation in the *Setup Guide*

Key Tasks

❒ Checklist for Performing a Migration Checklist for performing a migration

❒ Stopping the drivers

❒ Checklist for migrating Identity Manager

❒ Migrating the project, engine, and User Application driver

18 Legal Notice

THIS DOCUMENT AND THE SOFTWARE DESCRIBED IN THIS DOCUMENT ARE FURNISHED UNDER AND ARE SUBJECT TO THE TERMS OF A LICENSE AGREEMENT OR A NON-DISCLOSURE AGREEMENT. EXCEPT AS EXPRESSLY SET FORTH IN SUCH LICENSE AGREEMENT OR NON-DISCLOSURE AGREEMENT, NETIQ CORPORATION PROVIDES THIS DOCUMENT AND THE SOFTWARE DESCRIBED IN THIS DOCUMENT "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. SOME STATES DO NOT ALLOW DISCLAIMERS OF EXPRESS OR IMPLIED WARRANTIES IN CERTAIN TRANSACTIONS; THEREFORE, THIS STATEMENT MAY NOT APPLY TO YOU.

For purposes of clarity, any module, adapter or other similar material (“Module”) is licensed under the terms and conditions of the End User License Agreement for the applicable version of the NetIQ product or software to which it relates or interoperates with, and by accessing, copying or using a Module you agree to be bound by such terms. If you do not agree to the terms of the End User License Agreement you are not authorized to use, access or copy a Module and you must destroy all copies of the Module and contact NetIQ for further instructions.

This document and the software described in this document may not be lent, sold, or given away without the prior written permission of NetIQ Corporation, except as otherwise permitted by law. Except as expressly set forth in such license agreement or non-disclosure agreement, no part of this document or the software described in this document may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, or otherwise, without the prior written consent of NetIQ Corporation. Some companies, names, and data in this document are used for illustration purposes and may not represent real companies, individuals, or data.

This document could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein. These changes may be incorporated in new editions of this document. NetIQ Corporation may make improvements in or changes to the software described in this document at any time.

U.S. Government Restricted Rights: If the software and documentation are being acquired by or on behalf of the U.S. Government or by a U.S. Government prime contractor or subcontractor (at any tier), in accordance with 48 C.F.R. 227.7202-4 (for Department of Defense (DOD) acquisitions) and 48 C.F.R. 2.101 and 12.212 (for non-DOD acquisitions), the government's rights in the software and