

NetIQ Identity Manager Quick Start

February 2018



introduction

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

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” in the *NetIQ Identity Manager Setup Guide for Linux* or “Installing Designer” in the *NetIQ Identity Manager Setup Guide for Windows*
- ◆ *Understanding Designer for Identity Manager*
- ◆ *NetIQ Designer for Identity Manager Administration Guide*
- ◆ *NetIQ Identity Manager - Using Designer to Create Policies*
- ◆ *NetIQ Identity Manager - Administrator's Guide to Designing the Identity Applications*
- ◆ *NetIQ Identity Manager Credential Provisioning Guide*
- ◆ *NetIQ Identity Manager Security Guide*
- ◆ *NetIQ Identity Manager Setup Guide for Linux* or *NetIQ Identity Manager Setup Guide for Windows*

Key Tasks for Architects and Administrators

- ☐ Planning for, installing, and configuring Designer in the *NetIQ Identity Manager Setup Guide for Linux* or Planning for, installing, and configuring Designer *NetIQ Identity Manager Setup Guide for Windows*
- ☐ Planning your identity solution

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

Preparing Your Data

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

Components or Tools

- ◆ Analyzer

Library Resources

- ◆ “Installing Designer” in the *NetIQ Identity Manager Setup Guide for Linux* or “Installing Analyzer” in the *NetIQ Identity Manager Setup Guide for Windows*
- ◆ *Analyzer for Identity Manager Administration Guide*

Key Tasks

- ☐ Planning for, installing, and configuring Analyzer in the *NetIQ Identity Manager Setup Guide for Linux* or Planning for, installing, and configuring Analyzer in the *NetIQ Identity Manager Setup Guide for Windows*
- ☐ Understanding the Analyzer tool
- ☐ Analyzing and cleaning up data
- ☐ Reporting unique values in a data set
- ☐ Reporting matching information between data sets
- ☐ Security considerations

Installing and Configuring Identity Manager

Library Resources

- ◆ *NetIQ Identity Manager Setup Guide for Linux* or *NetIQ Identity Manager Setup Guide for Windows*

Checklists for Installation

- ☐ “Planning to Install Identity Manager” in the [NetIQ Identity Manager Setup Guide for Linux](#) or “Planning to Install Identity Manager” in the [NetIQ Identity Manager Setup Guide for Windows](#)
- ☐ Identity Vault
- ☐ Identity Manager Engine, Drivers, and Plug-Ins in the [NetIQ Identity Manager Setup Guide for Linux](#) or Identity Manager Engine, Drivers, and Plug-Ins in the [NetIQ Identity Manager Setup Guide for Windows](#)
- ☐ Remote Loader in the [NetIQ Identity Manager Setup Guide for Linux](#) or Remote Loader in the [NetIQ Identity Manager Setup Guide for Windows](#)
- ☐ iManager in the [NetIQ Identity Manager Setup Guide for Linux](#) or iManager in the [NetIQ Identity Manager Setup Guide for Windows](#)
- ☐ Designer in the [NetIQ Identity Manager Setup Guide for Linux](#) or Designer in the [NetIQ Identity Manager Setup Guide for Windows](#)
- ☐ Identity Applications components in the [NetIQ Identity Manager Setup Guide for Linux](#) or PostgreSQL and Tomcat in the [NetIQ Identity Manager Setup Guide for Windows](#)
- ☐ Single Sign-on in the [NetIQ Identity Manager Setup Guide for Linux](#) or Single Sign-on in the [NetIQ Identity Manager Setup Guide for Windows](#)
- ☐ Password Management in the [NetIQ Identity Manager Setup Guide for Linux](#) or Password Management in the [NetIQ Identity Manager Setup Guide for Windows](#)
- ☐ Identity Applications - readiness in the [NetIQ Identity Manager Setup Guide for Linux](#) or Identity Applications - readiness in the [NetIQ Identity Manager Setup Guide for Windows](#)
- ☐ Identity Reporting in the [NetIQ Identity Manager Setup Guide for Linux](#) or Identity Reporting in the [NetIQ Identity Manager Setup Guide for Windows](#)
- ☐ Analyzer in the [NetIQ Identity Manager Setup Guide for Linux](#) or Analyzer in the [NetIQ Identity Manager Setup Guide for Windows](#)
- ☐ Activating in the [NetIQ Identity Manager Setup Guide for Linux](#) or Activating in the [NetIQ Identity Manager Setup Guide for Windows](#)
- ☐ Upgrading in the [NetIQ Identity Manager Setup Guide for Linux](#) or Upgrading in the [NetIQ Identity Manager Setup Guide for Windows](#)

- ☐ Migrating in the [NetIQ Identity Manager Setup Guide for Linux](#) or Migrating in the [NetIQ Identity Manager Setup Guide for Windows](#)
- ☐ Configuring in Cluster Environments
 - ♦ General requirements
 - ♦ Identity Vault [considerations](#) and [installation](#)
 - ♦ Identity applications [prerequisites](#) and [preparing a cluster for the Identity Applications](#) or Identity applications [prerequisites](#) and [preparing a cluster for the Identity Applications](#)
 - ♦ Self-Service Password Reset [considerations](#)
 - ♦ User Application [considerations](#)

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” in the [NetIQ Identity Manager Setup Guide for Linux](#) or “Installing Designer” in the [NetIQ Identity Manager Setup Guide for Windows](#)
- ♦ Installing Identity Manager in the [NetIQ Identity Manager Setup Guide for Linux](#) or Installing iManager in the [NetIQ Identity Manager Setup Guide for Windows](#)
- ♦ [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

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 and Configuring Identity Manager Components in the *NetIQ Identity Manager Setup Guide for Linux* or Installing the Identity Vault and Installing the Remote Loader in the *NetIQ Identity Manager Setup Guide for Windows*](#)
- ♦ [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](#)

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 in the *NetIQ Identity Manager Setup Guide for Linux* or Understanding data synchronization in the *NetIQ Identity Manager Setup Guide for Windows*](#)
- ☐ [Understanding the components for synchronizing data in the *NetIQ Identity Manager Setup Guide for Linux* or Understanding the components for synchronizing data in the *NetIQ Identity Manager Setup Guide for Windows*](#)

- ☐ [Viewing and managing associations between drivers and objects in the Identity Vault](#)
- ☐ [How data is synchronized between connected systems](#)
- ☐ [Prioritizing synchronization of certain events](#)

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](#)
- ♦ [Identity Applications Administration in the *NetIQ Identity Manager - Administrator's Guide to the Identity Applications*](#)

Library Resources

- ♦ [“Installing and Configuring Identity Manager Components” in the *NetIQ Identity Manager Setup Guide for Linux* or “Installing Identity Applications” in the *NetIQ Identity Manager Setup Guide for Windows*](#)
- ♦ [NetIQ Identity Manager - Administrator's Guide to the Identity Applications](#)
- ♦ [Configuring Roles in the *User Application: Design Guide*](#)

Key Tasks

- ☐ [Catalog Administrator tool](#)
 - ♦ [Creating and Managing Roles](#)
 - ♦ [Creating and Managing Resources](#)
 - ♦ [Separation of Duties Constraints](#)
 - ♦ [Mapping Resources to Roles](#)
- ☐ [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](#)

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 and Configuring Identity Manager Components” in the [NetIQ Identity Manager Setup Guide for Linux](#) or “Installing Identity Applications” in the [NetIQ Identity Manager Setup Guide for Windows](#)
- ♦ [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

- ☐ [NetIQ Identity Manager Home and Provisioning Dashboard User Guide](#)
- ☐ [Permissions needed for tasks on the Work Dashboard](#)
- ☐ [Managing your work](#)

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 Identity Applications” in the *NetIQ Identity Manager Setup Guide for Linux* or “Installing the Single Sign-on Component” and Installing the Password Management Component in the *NetIQ Identity Manager Setup Guide for Windows*
- ♦ Configuring Single Sign-on Access in the *NetIQ Identity Manager Setup Guide for Linux* or Configuring Single Sign-on Access in the *NetIQ Identity Manager Setup Guide for Windows*.
- ♦ *NetIQ Identity Manager - Administrator's Guide to the Identity Applications*
- ♦ Managing Your Permissions and Identity Profile in the *NetIQ Identity Manager - User's Guide to the Identity Applications*
- ♦ Exploring the Identity Manager Landing Page in the *User Application: User Guide*

Key Tasks for Administrators

- ☐ Securing the Identity Applications 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 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 Single Sign-on Access in Identity Manager
- ☐ 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 other users in your organization
- ☐ Displaying detailed information about users
- ☐ Installing and using the mobile Approvals app

Self-Service Identity Management

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

Library Resources

- ♦ “Installing Identity Applications” in the *NetIQ Identity Manager Setup Guide for Linux* or “Installing Identity Applications” in the *NetIQ Identity Manager Setup Guide for Windows*
- ♦ Managing Your Profile in the *User's Guide to the Identity Applications*

Key Tasks for Administrators

- ☐ Accessing the Identity Self-Service
- ☐ Creating a user or a group
- ☐ 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

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 Identity Applications” in the *NetIQ Identity Manager Setup Guide for Linux* or “Installing the Single Sign-on Component” and Installing the Password Management Component in the *NetIQ Identity Manager Setup Guide for Windows*

- ♦ [NetIQ Identity Manager Password Management Guide](#)
- ♦ [Configuring forgotten password self-service](#)
- ♦ [Deploying Universal Password in the *Identity Manager Password Management Administration Guide*](#)

Key Tasks for Administrators

- ☐ [Understanding the Password Management Service](#)
- ☐ [Understanding Password Self-Service](#)
- ☐ [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](#)

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](#)

Auditing

You can audit issues of interest and troubleshoot errors.

Library Resources

- ♦ [“Installing Identity Reporting” in the *NetIQ Identity Manager Setup Guide for Linux* or *Installing Identity Reporting in the NetIQ Identity Manager Setup Guide for Windows*](#)
- ♦ [Administrator Guide to NetIQ Identity Reporting](#)
- ♦ [NetIQ Sentinel Documentation website](#)

Key Tasks

- ☐ [Enabling audit events](#)
 - ♦ [Analyzer data browser editor events](#)
 - ♦ [Driver events in Designer](#)
 - ♦ [Driver set events in Designer](#)
 - ♦ [One SSO Provider \(OSP\) events in the *NetIQ Identity Manager Setup Guide for Linux* or *One SSO Provider \(OSP\) events in the NetIQ Identity Manager Setup Guide for Windows*](#)
 - ♦ [Operation 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

☐ Setting up Logging

- ♦ Setting log levels
- ♦ Logging User Application events to Sentinel
- ♦ Configuring Sentinel Log Management for Identity Governance and Administration for Event Auditing
- ♦ NetIQ Identity Manager - Configuring Auditing in Identity Manager

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

Library Resources

- ♦ “Installing Identity Reporting” in the *NetIQ Identity Manager Setup Guide for Linux* or “Installing Identity Reporting” in the *NetIQ Identity Manager Setup Guide for Windows*
- ♦ Administrator Assignments in the *Administrator's Guide to the Identity Applications*
- ♦ *Using Identity Manager Reports*
- ♦ *Administrator Guide to NetIQ Identity Reporting*
- ♦ *NetIQ Identity Manager - Configuring Auditing in Identity Manager*

Key Tasks

- ☐ Understanding predefined Identity Manager reports
- ☐ Defining, running, scheduling, and viewing reports with Identity Reporting
 - ♦ Viewing a report definition
 - ♦ Modifying a report definition
 - ♦ Creating a custom report definition based on an existing definition
 - ♦ 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

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

- ☐ Using Identity Manager with Access Review
 - ♦ Integrating Access Review with Identity Manager
 - ♦ Configuring fulfillment

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 *NetIQ Identity Manager Setup Guide for Linux* or “Upgrading Identity Manager” in the *NetIQ Identity Manager Setup Guide for Windows*

Key Tasks

- ☐ “Checklist for Upgrading Identity Manager” in the *NetIQ Identity Manager Setup Guide for Linux* or “Checklist for Upgrading Identity Manager” in the *NetIQ Identity Manager Setup Guide for Windows*
- ☐ “Preparing to Upgrade Identity Manager” in the *NetIQ Identity Manager Setup Guide for Linux* or “Preparing to Upgrade Identity Manager” in the *NetIQ Identity Manager Setup Guide for Windows*
- ☐ “Upgrading Identity Manager Components” in the *NetIQ Identity Manager Setup Guide for Linux* or “Upgrading Identity Manager Components” in the *NetIQ Identity Manager Setup Guide for Windows*

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 [NetIQ Identity Manager Setup Guide for Linux](#) or “Migrating Identity Manager Data to a New Installation” in the [NetIQ Identity Manager Setup Guide for Windows](#)

Key Tasks

- ☐ [Checklist for Migrating Identity Manager](#)
- ☐ Stopping and Starting Identity Manager Drivers during Migration in the [NetIQ Identity Manager Setup Guide for Linux](#) or “Checklist for Performing a Migration” in the [NetIQ Identity Manager Setup Guide for Windows](#)
- ☐ Preparing Your Designer Project for Migration in the [NetIQ Identity Manager Setup Guide for Linux](#) or “Preparing Your Designer Project for Migration” in the [NetIQ Identity Manager Setup Guide for Windows](#)
- ☐ Migrating Identity Manager to a New Server in the [NetIQ Identity Manager Setup Guide for Linux](#) or Migrating Identity Manager to a New Server in the [NetIQ Identity Manager Setup Guide for Windows](#)
- ☐ Migrating the User Application Driver in the [NetIQ Identity Manager Setup Guide for Linux](#) or Migrating the User Application Driver in the [NetIQ Identity Manager Setup Guide for Windows](#)

Contact Information

Our goal is to provide documentation that meets your needs. If you have suggestions for improvements, please email Documentation-Feedback@netiq.com (<mailto:Documentation-Feedback@netiq.com>). We value your input and look forward to hearing from you.

For detailed contact information, see the [Support Contact Information](#) website (<http://www.netiq.com/support/process.asp#phone>).

For general corporate and product information, see the [NetIQ Corporate](#) website (<http://www.netiq.com/>).

For interactive conversations with your peers and NetIQ experts, become an active member of our [community](#) (<https://www.netiq.com/communities/>). The NetIQ online community provides product information, useful links to helpful resources, blogs, and social media channels.

Legal Notice: For information about legal notices, trademarks, disclaimers, warranties, export and other use restrictions, U.S. Government rights, patent policy, and FIPS compliance, see <https://www.netiq.com/company/legal/>.

Copyright © 2018 NetIQ Corporation. All Rights Reserved.