

NetIQ® Access Review

User Guide

April 2014



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 documentation, including its rights to use, modify, reproduce, release, perform, display or disclose the software or documentation, will be subject in all respects to the commercial license rights and restrictions provided in the license agreement.

© 2014 NetIQ Corporation and its affiliates. All Rights Reserved.

For information about NetIQ trademarks, see <https://www.netiq.com/company/legal/>.

Contents

About this Book and the Library	7
About NetIQ Corporation	9
1 Overview	11
1.1 Understanding Access Review	11
1.1.1 Collecting Identity and Application Data	12
1.1.2 Publishing a Catalog of Collected Identities	12
1.1.3 Preparing Published Data for Review	12
1.1.4 Reviewing Changes	12
1.1.5 Approving a Review	13
2 Installing and Configuring Access Review	15
2.1 Checklist for Installing and Configuring Access Review	15
2.2 Considerations for Installing Access Review	16
2.2.1 Prerequisites	16
2.2.2 Hardware and Software Requirements	16
2.2.3 Understanding Authentication for Access Review	17
2.2.4 Understanding the Access Review Databases	18
2.3 Preparing to Install Access Review	18
2.4 Installing Access Review	19
2.4.1 Using a Guided Process to Install Access Review	19
2.4.2 Performing a Silent Installation of Access Review	23
2.4.3 Completing the Installation Process	24
2.5 Configuring Access Review	25
2.5.1 Understanding the AR Configuration Utility	25
2.5.2 Using the TLS/SSL Protocol for Secure Connections	26
2.5.3 Adding Users and Assigning Roles for Access Review	26
2.5.4 Configuring the Mail Server for Notifications	28
2.6 Customizing Access Review	29
2.6.1 Localizing the User Interface	30
2.6.2 Customizing the Email Templates	30
2.7 Integrating Access Review with NetIQ Identity Manager	31
2.7.1 Configuring Access Review for Integration	32
2.7.2 Configuring Identity Manager Home for Integration	33
2.7.3 Configuring an Automatic Process to Fulfill Changes	33
3 Collecting and Viewing Data	35
3.1 Importing Data into the Catalog	35
3.2 Viewing and Editing Specific Data Attributes	36
3.3 Searching for Users or Groups	36
4 Performing Reviews	37
4.1 Creating a Review	37
4.2 Completing Review Tasks	37
4.3 Manual Fulfillment	38
4.3.1 How Manual Fulfillment Works	38
4.3.2 Implementing Manual Fulfillment	38

5	Managing Access Review Users	39
5.1	Understanding Roles in Access Review	39
5.2	Global Roles.	39
5.3	Runtime Roles	40
6	Using Access Review with Identity Manager	43
6.1	Automated Fulfillment Using Identity Manager	43
6.1.1	How to Set Up Automated Identity Manager Role Based Provisioning Module Workflow Fulfillment	43
6.1.2	How Automated Fulfillment Works.	44
6.2	Custom Fulfillment Using External Provisioning Workflow.	44
6.2.1	Configuring External Identity Manager Workflow Fulfillment	44
6.2.2	Understanding External Identity Manager Workflow Fulfillment	45

About this Book and the Library

The *User Guide* provides conceptual information about the NetIQ Access Review product. This book provides installation information, and step-by-step guidance for many administrative and user-oriented tasks.

Intended Audience

This book provides information for individuals responsible for configuring, reviewing, and auditing levels of access in your organization.

Other Information in the Library

The library provides the following information resources in addition to this guide:

Release Notes

Provides detailed information on installing and configuring the NetIQ Access Review product, as well as steps for administering the product after configuration.

About NetIQ Corporation

We are a global, enterprise software company, with a focus on the three persistent challenges in your environment: Change, complexity and risk—and how we can help you control them.

Our Viewpoint

Adapting to change and managing complexity and risk are nothing new

In fact, of all the challenges you face, these are perhaps the most prominent variables that deny you the control you need to securely measure, monitor, and manage your physical, virtual, and cloud computing environments.

Enabling critical business services, better and faster

We believe that providing as much control as possible to IT organizations is the only way to enable timelier and cost effective delivery of services. Persistent pressures like change and complexity will only continue to increase as organizations continue to change and the technologies needed to manage them become inherently more complex.

Our Philosophy

Selling intelligent solutions, not just software

In order to provide reliable control, we first make sure we understand the real-world scenarios in which IT organizations like yours operate — day in and day out. That's the only way we can develop practical, intelligent IT solutions that successfully yield proven, measurable results. And that's so much more rewarding than simply selling software.

Driving your success is our passion

We place your success at the heart of how we do business. From product inception to deployment, we understand that you need IT solutions that work well and integrate seamlessly with your existing investments; you need ongoing support and training post-deployment; and you need someone that is truly easy to work with — for a change. Ultimately, when you succeed, we all succeed.

Our Solutions

- ♦ Identity & Access Governance
- ♦ Access Management
- ♦ Security Management
- ♦ Systems & Application Management
- ♦ Workload Management
- ♦ Service Management

Contacting Sales Support

For questions about products, pricing, and capabilities, contact your local partner. If you cannot contact your partner, contact our Sales Support team.

Worldwide:	www.netiq.com/about_netiq/officelocations.asp
United States and Canada:	1-888-323-6768
Email:	info@netiq.com
Web Site:	www.netiq.com

Contacting Technical Support

For specific product issues, contact our Technical Support team.

Worldwide:	www.netiq.com/support/contactinfo.asp
North and South America:	1-713-418-5555
Europe, Middle East, and Africa:	+353 (0) 91-782 677
Email:	support@netiq.com
Web Site:	www.netiq.com/support

Contacting Documentation Support

Our goal is to provide documentation that meets your needs. If you have suggestions for improvements, click **Add Comment** at the bottom of any page in the HTML versions of the documentation posted at www.netiq.com/documentation. You can also email Documentation-Feedback@netiq.com. We value your input and look forward to hearing from you.

Contacting the Online User Community

Qmunity, the NetIQ online community, is a collaborative network connecting you to your peers and NetIQ experts. By providing more immediate information, useful links to helpful resources, and access to NetIQ experts, Qmunity helps ensure you are mastering the knowledge you need to realize the full potential of IT investments upon which you rely. For more information, visit <http://community.netiq.com>.

1 Overview

The NetIQ Access Review product enables administrators and managers to easily collect all user and access information in one central location and certify that each user has only the level of access that they need to do their job. Following the principle of least privilege, this product allows you to ensure that your users have focused access to those applications and resources they use and cannot access resources they do not need to access.

For example, if you work at a company that manufactures cars, the factory workers do not require access to any Human Resources applications beyond what they might need to view their paystubs or benefit information. Similarly, the Human Resources staff does not need to have badge access to the factory floor. As a manager, you need to ensure that your employees have only the appropriate levels of access for their respective positions.

With Access Review, you can review all permissions assigned to your employees, either individually or as a group, and decide whether those permission assignments are appropriate.

Significant compliance regulations such as HIPAA, Sarbanes-Oxley, and PCI require that user access privileges align with job functions. By performing regular reviews to validate access and the appropriateness of user access assignments, organizations can reduce their risk of non-compliance. Access Review can help organizations implement, manage, and automate an access review and validation process.

1.1 Understanding Access Review

Access Review is a browser-based utility that allows you to review user access to your enterprise applications, validate whether user permission assignments are appropriate, and take action if they are not. Access Review helps organizations implement, manage, and automate the review and validation process.

Access Review collects information from various application data sources and manages the entire review and implementation process. Access Review provides tools to guide you through the key phases of the access review and validation process:

- ♦ Collecting application and identity data
- ♦ Publishing a catalog snapshot
- ♦ Reviewing accounts and permissions
- ♦ Creating a list of changes
- ♦ Approving the changes
- ♦ Implementing the changes
- ♦ Reconciling change request status

1.1.1 Collecting Identity and Application Data

During the data collection phase, Access Review collects raw data from specified identity and application data sources. Access Review supports the following access protocols by default:

- ♦ Active Directory
- ♦ CSV file
- ♦ eDirectory
- ♦ Identity Manager
- ♦ JDBC
- ♦ LDAP

Access Review provides several predefined collector templates to facilitate data collection. A collector template lets you quickly build and customize a collector. Whenever possible, the collector templates include predefined attribute mappings and value transformation policies suitable for the target data source.

For more information about collecting data, see [Section 3.1, “Importing Data into the Catalog,” on page 35](#)

1.1.2 Publishing a Catalog of Collected Identities

After collecting identity data, use Access Review to publish a catalog snapshot. The snapshot presents a consolidated view of the collected identities. Using Access Review, you can directly associate user identities and permissions. Alternatively, you can associate identities with accounts and associate the accounts with permissions.

The Access Review browser-based interface provides an easy way to resolve the mappings that exist among different user, account, and permission object types.

1.1.3 Preparing Published Data for Review

The next step is the manual process of preparing the published data for review, sometimes called “curation”. During the preparation process, one or more Access Review data administrators improve data quality by:

- ♦ Providing additional meta data
- ♦ Defining business-friendly names for various entities
- ♦ Specifying risk factors for applications, roles, and permissions

For more information about preparing data, see [Section 3.2, “Viewing and Editing Specific Data Attributes,” on page 36](#).

1.1.4 Reviewing Changes

After the data is prepared for review, Review Access users designated as Review Administrators create review definitions for particular sets of applications, groups, or users and permissions. Then Review Owners initiate review campaigns, generating tasks for reviewers, requesting that they review a set of users and decide whether the current user access should be maintained or revoked.

For more information about the review process, see [Chapter 4, “Performing Reviews,” on page 37](#).

1.1.5 Approving a Review

At the conclusion of each review campaign, the Review Owner must approve the review. After approval, a review may be optionally routed to a Review Auditor for legal acceptance. All access change requests are sent to fulfillment, which is the step where approved changes are implemented.

NOTE: Access Review provides manual and automated fulfillment of access revocation decisions. All automated fulfillment requests are routed to NetIQ Identity Manager. The fulfillment process can be further refined using delegation to a custom Identity Manager workflow.

The review and validation process that begins with data collection and publishing concludes with change request reconciliation. Access Review marks as complete all access change requests fulfilled manually or through automatic or workflow based provisioning.

For more information about implementing the changes, see [Section 4.3, “Manual Fulfillment,” on page 38](#)

2 Installing and Configuring Access Review

This section provides information about installing and configuring Access Review. NetIQ recommends that you review the installation process, including the prerequisites and requirements, before beginning.

2.1 Checklist for Installing and Configuring Access Review

Before beginning the installation process, NetIQ recommends that you review the following steps.

	Checklist Items
☐	1. Ensure that your environment meets the prerequisites and requirements for hosting Access Review. For more information, see Section 2.2, "Considerations for Installing Access Review," on page 16 .
☐	2. Ensure that the <code>JAVA_HOME</code> environment variable points to the root directory of your JDK hierarchy. For more information, see Section 2.3, "Preparing to Install Access Review," on page 18 .
☐	3. Install Access Review: ♦ For a guided installation, see Section 2.4.1, "Using a Guided Process to Install Access Review," on page 19. ♦ For an unattended installation, see Section 2.4.2, "Performing a Silent Installation of Access Review," on page 23.
☐	4. Initialize Access Review for the first time. For more information, see Section 2.4.3, "Completing the Installation Process," on page 24 .
☐	5. (Optional) Modify the SSL settings for communication with the authentication server. For more information, see Section 2.5.2, "Using the TLS/SSL Protocol for Secure Connections," on page 26 .
☐	6. (Optional) Modify the configuration settings for Access Review. For more information, see Section 2.5, "Configuring Access Review," on page 25 .
☐	7. (Optional) Add users who can log in to Access Review and assign them to roles in the application. For more information, see Section 2.5.3, "Adding Users and Assigning Roles for Access Review," on page 26 .
☐	8. (Optional) Localize the user interface or modify the templates for email notifications. For more information, see Section 2.6, "Customizing Access Review," on page 29 .
☐	9. (Optional) Create a single sign-on experience for users between Access Review and NetIQ Identity Manager Home and Provisioning Dashboard. For more information, see Section 2.7, "Integrating Access Review with NetIQ Identity Manager," on page 31 .

2.2 Considerations for Installing Access Review

This section lists the prerequisites and system requirements for installing Access Review. It also explains how Access Review handles user authentication and describes the Access Review databases.

2.2.1 Prerequisites

NetIQ recommends that you review the following prerequisites for installation:

- ♦ You must use Latin-1 characters in the installation path.
- ♦ To use eDirectory for your authentication server, the eDirectory schema must support the One SSO Provider (OSP) protocol. You can update the schema after installation. For more information about updating the schema, see [Section 2.4.3, “Completing the Installation Process,” on page 24](#). For more information about the authentication server, see [Section 2.2.3, “Understanding Authentication for Access Review,” on page 17](#).
- ♦ Before installing Access Review, you need the following information:
 - ♦ Paths to your Apache Tomcat and Java directories.
 - ♦ IP address or DNS host name and port of your Access Review server. Login users will use this information in the URL for Access Review.
 - ♦ Credentials of an administrator account for the LDAP authentication server.

NOTE: The installation process can create an authentication server, if you do not have one. For more information, see [Section 2.2.3, “Understanding Authentication for Access Review,” on page 17](#).

- ♦ The container in the LDAP authentication server where you store administrator accounts.
- ♦ The container in the LDAP authentication server where you store the accounts for users who can log in to Access Review.
- ♦ IP address and port of your Postgres database server.
- ♦ Credentials of an account that allows Access Review to access and modify data in the Postgres databases.
- ♦ Credentials of a database administrator (DBA) account that can create database tables, views, and other artifacts.

NOTE: If you do not have credentials for the DBA, the installation process can generate a sql script that the DBA runs to create and configure the databases.

2.2.2 Hardware and Software Requirements

This section provides the minimum requirements for the server where you want to install Access Review.

Category	Minimum Requirement
Processor	1 GHz
Disk Space	1 GB
Memory	512 MB (1 GB recommended)

Category	Minimum Requirement
Operating System	♦ Red Hat Enterprise Linux 6 (64-bit) ♦ Red Hat Enterprise Linux 5 (64-bit) ♦ SUSE Linux Enterprise Server 11 SP2 or SP3 (64-bit)
Operating System Hotfixes	Before installing Identity Manager, NetIQ recommends that you apply the latest operating system patches according to the manufacturer's automated update facility.
Java	Oracle Java 2 Platform Standard Edition Development version 1.7.0_51 (JDK or JRE)
Database	Postgres SQL 9.2
Application Server	Apache Tomcat 7.0.50 NOTE: (Conditional) For guaranteed delivery of email notifications, your application server must include support for Apache ActiveMQ Java Message Service (JMS) and clustering.
LDAP Authentication Server	One of the following applications, running OAuth2 protocol: ♦ Microsoft Active Directory ♦ NetIQ eDirectory
Web browser	One of the following browsers: ♦ Apple Safari 7.0.1 ♦ Google Chrome 31 ♦ Internet Explorer 9 ♦ Mozilla Firefox 21 (including the FireBug and HttpFox extensions) NOTE: The browser must have cookies enabled. If cookies are disabled, the product does not work.
Additional Software	(Conditional) Active MQ 5.9.0 for guaranteed delivery of email notifications

2.2.3 Understanding Authentication for Access Review

To verify users who log in to Access Review, you need an LDAP authentication server that uses OAuth protocol for authentication. Access Review supports Active Directory and eDirectory. You can configure more than one **authentication source**, or **identity vault**, to handle the authentication requests. Users can log in to Access Review immediately after installation if the specified containers in the identity vault have CNs and passwords for those users. Without these login accounts, only the bootstrap administrator can also log in immediately. For more information, see [“Understanding the Bootstrap Administrator for Access Review” on page 18](#).

NOTE: You do not need an authentication server to install Access Review. Instead, you can instruct the installation process to create the server.

Using One SSO Provider for Authentication

Access Review uses the authentication service, One SSO Provider (OSP), which supports the OAuth2 specification. For example, you can use a component of NetIQ Identity Manager as an authentication server, such as the Identity Vault, as long as that component also is using OAuth protocol. With OSP, you can provide single sign-on access among Access Review and other applications, such as NetIQ Identity Manager Home and Provisioning Dashboard. All requests to OSP use the http or https protocols.

Understanding the Bootstrap Administrator for Access Review

During installation, you create a **bootstrap administrator** account that can immediately log in and configure Access Review. This account is useful if you do not have an authentication server before installing Access Review, and thus do not have any specified login users. To ensure system security, NetIQ recommends that you create a text file to store the credentials for the bootstrap administrator, rather than adding this account to your LDAP container. The installation process names the file `adminusers.txt`, and places it in the `/access-review/osp` directory.

NOTE: The name for this account must be unique. Do not duplicate the name of any accounts already in the `adminusers.txt` file or in the container source or subtrees that you use for authentication. Also, do not use “admin” or “administrator” for the account name.

Understanding the Keystore for the Authentication Server

During installation, you must create a keystore for the authentication server to support Access Review. You also create a password that the Access Review service uses for authorized interactions with the authentication server.

2.2.4 Understanding the Access Review Databases

Access Review needs three databases to support operations, workflow, and data collection. By default, these databases are `arops`, `ardcs`, and `arwf`, respectively. You can establish these databases in three ways:

- ♦ Have the installation process create and configure the databases.
- ♦ Connect to existing, empty databases during installation. The databases cannot contain any data or tables before installation. During installation, ensure that you specify the correct names of your three databases.
- ♦ Have the installation process generate an SQL scripts that you or a database administrator (DBA) uses to create and configure the databases after installing Access Review. Use this method if you do not have the credentials for the DBA.

2.3 Preparing to Install Access Review

Before installing Access Review, you must ensure that the `JAVA_HOME` environment variable points to the root directory of your JDK hierarchy.

- 1 Log on to the server where you want to install Access Review.
- 2 Download and install a supported version of Java.

- 3 In a terminal, enter the following commands:

```
export JAVA_HOME=JavaInstallationDirectory
export PATH=$PATH:JavaInstallationDirectory/bin
```

- 4 Close the terminal.

2.4 Installing Access Review

You can use a guided process to install Access Review or perform a silent, unattended installation.

2.4.1 Using a Guided Process to Install Access Review

The following procedure describes how to install Access Review using an installation wizard, either in GUI format or from the console. To perform a silent, unattended installation, see [Section 2.4.2, “Performing a Silent Installation of Access Review,”](#) on page 23.

To prepare for the installation, review the prerequisites and system requirements listed in [Section 2.2, “Considerations for Installing Access Review,”](#) on page 16. Also see the Release Notes accompanying the release.

- 1 Log on to the server where you want to install Access Review.
- 2 Stop Tomcat.
- 3 Navigate to the directory containing the installation package.
- 4 At a command prompt, perform one of the following options:

- ♦ **To use the console**, enter `./access-review-install-linux.bin -i console`.
- ♦ **To use the wizard**, enter `./access-review-install-linux.bin`.

- 5 Complete the guided process, using the following parameters:

- ♦ **Tomcat Details**

Represents the home folder for the Tomcat server. For example, `/opt/apache-tomcat-7.0.50`. The installation process adds some files for Access Review to this folder.

- ♦ **Tomcat connection**

Represents the settings of the URL that users need to connect to the Access Review client. For example, `https://172.16.254.1:8080`.

Protocol

Specifies whether you want to use *http* or *https*. To use Secure Sockets Layer (SSL) for communications, specify *https*.

Host Name

Specifies the DNS name or IP address of the server hosting Access Review. Do not use `localhost`.

Port

Specifies the port that you want the server to use for communication with client computers. The default is 8080.

- ♦ **Tomcat Java Home**

Represents the home folder for the Tomcat server. For example, `/usr/lib/jvm/default-java`. The installation process adds some files for Access Review to the Tomcat home folder.

- ♦ **Authentication details**

Represents the requirements for connecting Access Review to the authentication server which contains the list of users who can log in to the application. For more information about the authentication server, see [Section 2.2.3, “Understanding Authentication for Access Review,”](#) on page 17.

Service password

Specifies the password that you want to create for Access Review to use when connecting to the authentication server. Also referred to as the client secret.

Install or connect to an authentication server

Specifies whether to install, or embed, an authentication server on the current server or connect to an existing Identity Manager server for authentication.

LDAP host

Applies only when installing a new server.

Specifies the DNS name or IP address of the LDAP authentication server. Do not use localhost.

LDAP port

Applies only when installing a new server.

Specifies the port that you want the LDAP authentication server to use for communication with Access Review.

Admin DN

Applies only when installing a new server.

Specifies the DN for an administrator account of the LDAP authentication server. For example, `cn=admin,ou=sa,o=system`.

Admin password

Applies only when installing a new server.

Specifies the password for the administrator account of the LDAP authentication server.

User container

Applies only when installing a new server.

Specifies the container in the LDAP authentication server where you store the user accounts that can log in to Access Review. For example, `o=data`.

Admin container

Applies only when installing a new server.

Specifies the container in the LDAP authentication server where you store the administrator accounts for Access Review. For example, `ou=sa,o=system`.

Host Name

Applies only when connecting to an existing server.

Specifies the name or IP address of the LDAP authentication server. Do not use localhost.

Port

Applies only when connecting to an existing server.

Specifies the port that you want the LDAP authentication server to use for communication with Access Review.

Protocol

Applies only connecting to using an existing server.

Specifies whether you want to use *http* or *https* when connecting with the external LDAP authentication server. To use Secure Sockets Layer (SSL) for communications, specify *https*.

Keystore Password

Specifies the password that you want to use for the new keystore for the LDAP authentication server. The installation process creates the keystore.

Authentication identity vault type

Specifies whether your authentication server uses eDirectory or Active Directory as its source for authentication. For more information, see [Section 2.2.3, “Understanding Authentication for Access Review,” on page 17](#).

Generate a file based bootstrap admin

Specifies whether the process adds the bootstrap administrator account to the LDAP server or generates a text file, called `adminusers.txt`, to store the account.

For more information about the bootstrap administrator account, see [Section 2.2.3, “Understanding Authentication for Access Review,” on page 17](#).

Bootstrap admin

Specifies the name of the bootstrap administrator account.

NOTE: The name of this account must be unique. Do not duplicate any accounts in the `adminusers.txt` file or in the container source or subtrees that you use for authentication.

Bootstrap password

Specifies the password for the bootstrap administrator account.

♦ Logging details

(Optional) Represents the settings for using event logging with Novell Identity Audit.

Log cache folder

Specifies the path where you want to store the cache files for logging.

Server

Specifies the DNS name or the IP address of the server that hosts Novell Identity Audit.

♦ ActiveMQ details

(Optional) Represents the settings for ActiveMQ, which guarantees delivery of email notifications from Access Review.

Host name

Specifies the DNS name or the IP address of the server that hosts the ActiveMQ instance.

Port

Specifies the port that the server uses for ActiveMQ.

♦ Database details

Represents the settings for the Access Review databases. For more information, see [Section 2.2.4, “Understanding the Access Review Databases,” on page 18](#).

If you plan to connect to an existing database instance, you must specify the names of the existing databases to match with the operations, data collection, and workflow databases.

Host

Specifies the DNS name or the IP address of the server that hosts the Postgres database.

Port

Specifies the port of the server that hosts the Postgres database.

Userid

Specifies the name of an account that allows Access Review to access and modify data in the Postgres databases.

Password

Specifies the password for the specified userid.

Database name - Operations

Specifies the name of the database that stores operations data for Access Review. The default value is arops.

Database name - Data collection

Specifies the name of the database that stores data collection information for Access Review. The default value is ardcx.

Database name - Workflow

Specifies the name of the database that stores workflow information for Access Review. The default value is arwf.

Database administrator

Specifies the account for a database administrator that can create database tables, views, and other artifacts.

Password

Specifies the password for the database administrator.

Configure databases or generate SQL

Specifies whether you want to configure your new or existing databases as part of the installation process, or afterward.

If you choose to configure after installation, the process generates a SQL script that the database administrator can run in Postgres to create the databases. For more information, see [Step 1 on page 24](#).

Create new or existing databases

Specifies whether you want to use existing, empty databases or have the installation create new ones.

NOTE: To use existing databases, they cannot contain any data or tables. Otherwise, the installation might generate errors.

- 6 Review the pre-installation summary.

NOTE: *Tomcat URL* represents the URL for Access Review.

- 7 Start the installation process.
- 8 When the installation process completes, click *Done*.
- 9 Continue to [Section 2.4.3, “Completing the Installation Process,” on page 24](#).

2.4.2 Performing a Silent Installation of Access Review

A silent (non-interactive) installation does not display a user interface or ask the user any questions. Instead, the system uses information from a `silent.properties` file, included in the installation package. You must edit the file before beginning the installation process.

To prepare for the installation, review the prerequisites and system requirements listed in [Section 2.2, “Considerations for Installing Access Review,” on page 16](#). Also see the Release Notes accompanying the release. To perform a guided installation, see [“Using a Guided Process to Install Access Review” on page 19](#).

- 1 Log in to the server where you want to install Access Review.
- 2 To specify the installation parameters, complete the following steps:
 - 2a Ensure that the `access-review-install-silent.properties` file is located in the same directory as the `./access-review-install-linux.bin` installation file.
 - 2b In a text editor, open the `silent.properties` file.
 - 2c Specify the parameter values. For a description of the parameters, see [Step 5 on page 19](#). You must specify true (enable) or false (do not enable) for the following parameters:

<code>install.authserver.authsrc.enable.file</code>	Specifies whether you want to generate the file containing the bootstrap administrator account
<code>install.ogging.enable</code>	Specifies whether you want to enable audit logging
<code>install.notification.activemq</code>	Specifies whether you want to use ActiveMQ
<code>install.db.configure</code>	Specifies whether you want to configure the databases during installation
<code>install.db.create</code>	Specifies whether you want to create new databases (you do not have existing databases)

- 2d Save and close the file.
- 3 To launch the installation program, enter the following command:

```
access-review-install-linux.bin -i silent -f access-review-install-silent.properties
```

NOTE: If the `silent.properties` file is in a different directory from the installation script, you must specify the full path to the file. The script unpacks the necessary files to a temporary directory and then launches the silent installation.

- 4 When the installation process completes, continue to [Section 2.4.3, “Completing the Installation Process,” on page 24](#).

2.4.3 Completing the Installation Process

After performing a guided or silent installation, you must initialize Access Review and verify that you can log in as the bootstrap administrator.

- 1 (Conditional) If you chose to configure the databases after installation, complete the following steps:

- 1a To find the sql script that the installation process created, navigate to the `/installation_path/access-review/sql` directory.

- 1b Have the database administrator run the sql script to create and configure the Access Review databases.

- 1c To populate the global configuration values stored in the database, enter the following command:

```
/installation_path/access-review/bin/configutil -password db_password -script /installation_path/access-review/scripts/import-configs.script
```

- 2 (Conditional) If you specified an eDirectory authentication server, ensure that the schema supports OSP. To extend the schema, use the `osp.sch` file located by default in the `access-review/osp/schema` directory.

For more information about using OSP with the authentication server, see [“Using One SSO Provider for Authentication” on page 18](#). For more information about extending the schema, see the *NetIQ eDirectory Administration* (<https://www.netiq.com/documentation/edir88/edir88/data/bookinfo.html>)

- 3 To initialize Access Review, start Tomcat.

```
./path_to_Tomcat_folder/start.sh
```

- 4 (Conditional) To observe the initialization process in Tomcat, enter the following command:

```
tail -f path_to_Tomcat_folder/logs/catalina.out
```

When the process completes, the file concludes with the following message:

```
INFO: Server startup in nnnn ms
```

- 5 (Optional) Verify that the three databases exist in Postgres.
- 6 Open a web browser and navigate to one of the following URLs, depending on how you installed Access Review:

```
http://hostname_or_IP_address:port/  
https://hostname_or_IP_address:port/
```

For example:

```
http://texasone:8080/  
https://172.16.254.1:8080/
```

- 7 (Optional) To verify installation, complete the following steps:

- 7a Log in as an administrator to the server where you installed Access Review.

- 7b In a terminal, navigate to the following directory:

```
path to installationaccess-review/logs
```

- 7c Enter the following command:

```
tail -n 1 *
```

7d Verify that .txt log files in the directory end with the following text:

```
Exit code: 0
```

NOTE

- ♦ Access_Review_InstallLog.log contains the results of all the log files. It does not have an individual exit code.
 - ♦ If a log file ends with a nonzero exit code, an error occurred in that part of the installation process.
-

8 Use the bootstrap administrator account to log in to Access Review.

9 (Conditional) If you can verify installation but cannot get Access Review in a web browser, complete the following steps:

9a Stop Access Review (and Tomcat):

```
./path_to_Tomcat_folder/shutdown.sh
```

9b Navigate to the following directory:

```
path_to_Tomcat_folder/bin
```

9c In a text editor, open setenv.sh.

This file defines global variables and exports paths needed to host Access Review under Apache Tomcat.

9d Verify that the file lists the correct host name for the authentication server and paths to Tomcat.

9e Save and close the file.

9f Start Access Review (and Tomcat):

```
./path_to_Tomcat_folder/start.sh
```

10 (Optional) Add users who can log in to Access Review, and assign roles to those users. For more information, see [Section 2.5.3, “Adding Users and Assigning Roles for Access Review,” on page 26](#).

11 (Optional) Configure the application, such as customizing the email templates and displayed labels. For more information, see [Section 2.5, “Configuring Access Review,” on page 25](#).

2.5 Configuring Access Review

NetIQ also provides the AR Configuration Utility, which allows you to modify the settings for Access Review. Also, for users to log in to Access Review, you must collect their account information from your environment.

2.5.1 Understanding the AR Configuration Utility

The AR Configuration Utility allows you to modify settings for Access Review, such as the URL for Access Review, the authentication server, OSP, and email notifications. You can also specify an external provisioning system for workflows and the settings for collection and publication.

You can run this utility in GUI or console mode. To script changes to the configuration of Access Review, use the console mode option.

In a terminal, navigate to the installation directory for Access Review, then enter one of the following commands:

- ♦ **Console mode:** `./bin/configutil.sh -password db_password -i console`
- ♦ **GUI mode:** `./bin/configutil.sh -password db_password`

2.5.2 Using the TLS/SSL Protocol for Secure Connections

You can use the Transport Layer Security/Secure Sockets Layer (TLS/SSL) protocol to ensure the following types of secure network connections for Access Review:

- ♦ HTTP, which provides end-user access to and from Access Review.
- ♦ LDAP, which ensures secure communication between Access Review and the authentication server.
- ♦ JDBC, which ensures secure communication between Access Review and the database server.

TLS/SSL protocols are not configured by default. During installation, you should specify *https* as the protocol for communication with the database and authentication server. The installation process generates a private key, certificate, and password for the SSL server. The Access Review database stores the certificate and password. After installation, you can configure Access Review to use the TLS/SSL protocol before putting the system into production.

For more information about the AR Configuration Utility, see [Section 2.5.1, “Understanding the AR Configuration Utility,” on page 25](#).

To configure secure communication with the authentication server:

- 1 Stop Access Review (and Tomcat):

```
./path_to_Tomcat_folder/shutdown.sh
```

- 2 In the AR Configuration Utility, select *OSP Settings*.
- 3 Click *Use SSL for LDAP connection*.
- 4 Ensure that the specified LDAP host and port support TLS/SSL communication.
- 5 For *AR Server Details* and *Authentication Server Details*, verify that the connection protocol for the servers is set to *https*.
- 6 Click *Save*, and then close the utility.
- 7 Start Access Review (and Tomcat):

```
./path_to_Tomcat_folder/start.sh
```

2.5.3 Adding Users and Assigning Roles for Access Review

Individuals who can log in to the Access Review application are **Access Review users**. The authentication server for Access Review must include login information for all Access Review users. The source of data, or identity source, for these users could be your Human Resources directory or a *.csv* file. To ensure that users have a fixed set of permissions in Access Review, you can assign them to one of the built-in roles.

For more information about Access Review roles, see [Section 5.1, “Understanding Roles in Access Review,” on page 39](#). For more information about the authentication server, see [Section 2.2.3, “Understanding Authentication for Access Review,” on page 17](#).

This section helps you perform the following activities:

- ♦ [“Collecting Information for Access Review Users” on page 27](#)
- ♦ [“Mapping Attributes in a Data Source to the Access Review Catalog” on page 27](#)
- ♦ [“Assigning Roles to Access Review Users” on page 28](#)

Collecting Information for Access Review Users

Until you collect data for your login users, no one can access the application without using the bootstrap administrator account. For more information about the bootstrap administrator account, see [“Understanding the Bootstrap Administrator for Access Review” on page 18](#).

NOTE: Depending on your environment, you might not need your login user data once you map your Access Review users to the Access Review attribute catalog and then start collecting data from identity and application data sources.

To add Access Review users:

- 1 Log in to Access Review as the bootstrap administrator or with an account in the Global Administrator role.
- 2 In the AR Configuration Utility, review *OSP Settings* to ensure that you have configured the authentication server to use the appropriate Admin and User containers.

NOTE: To use a .csv file as your data source, select *File* for *Authentication Source Library*.

- 3 Log in to Access Review with an Access Review administrator account, such as the bootstrap administrator.
- 4 On the *Overview* page, click *Data Collection*.
- 5 Under *Identity Sources*, select the LDAP authentication server that you specified during installation.
- 6 To add the users listed in the specified containers to the Access Review Catalog, click the icon for *Collect Now*.
- 7 Map user attributes in your containers to the attributes catalog in Access Review. For more information, see [“Mapping Attributes in a Data Source to the Access Review Catalog” on page 27](#).

Mapping Attributes in a Data Source to the Access Review Catalog

Once you collect data for Access Review users, you must map the attributes of these users to the attributes in the Access Review catalog. You can also add your own custom attributes to the catalog. For example, your identity source, an eDirectory database, contains more attributes than are built into the catalog.

By default, all Access Review users must have the *LDAP Distinguished Name* attribute mapped in the attribute catalog. Access Review uses this attribute to authenticate users who log in to the application.

- 1 Log in to Access Review as the bootstrap administrator or with an account in the Global Administrator role.
- 2 In the Access Review menu, click *Collection*.
- 3 Under *Identity Sources*, select the authentication server that you specified during installation.

- 4 Ensure that you have collected data from the identity source. For more information, see [“Collecting Information for Access Review Users” on page 27](#).
- 5 Scroll down to the *Users attribute* section.
- 6 For *LDAP Distinguished Name*, specify the attribute in your identity source that you want to map to the login attribute for Access Review users.

For example, your identity source points to a container in Active Directory. Users log in to your network with an AD attribute called *username*. For *LDAP Distinguished Name*, specify the *username* attribute. Access Review maps *username* to the *LDAP Distinguished Name* attribute in the Catalog.
- 7 (Optional) Map the other attributes in your identity source to the built-in attributes in the Access Review catalog.
- 8 (Optional) To add custom attributes, complete the following steps:
 - 8a Click *Add Attribute*.
 - 8b Click *Click to rename*.
 - 8c Specify the settings for the new attribute, and then click *Close*.
 - 8d Specify an attribute from your identity source that you want to map to the new custom attribute.
 - 8e Click *Save*.
- 9 (Optional) Add the new login users to roles in Access Review. For more information, see [“Assigning Roles to Access Review Users” on page 28](#).

Assigning Roles to Access Review Users

Access Review provides built-in roles that have a fixed set of permissions. To ensure system security and data integrity, you can assign roles to the Access Review users. For more information about Access Review roles, see [Section 5.1, “Understanding Roles in Access Review,” on page 39](#).

- 1 Log in to Access Review as the bootstrap administrator or with an account in the Global Administrator role.
- 2 Ensure that you have mapped attributes in your identity source to attributes in the Access Review catalog. For more information, see [“Mapping Attributes in a Data Source to the Access Review Catalog” on page 27](#).
- 3 In the Access Review menu, click *Settings*.
- 4 In the right panel, click *Role Assignments*.
- 5 For each role, enter the name or ID of the Access Review user account that you want to assign to that role.

For example, in the Global Administrator field, enter your own Access Review user account.
- 6 Click *Save*.

2.5.4 Configuring the Mail Server for Notifications

Access Review can notify users of tasks in their queue. To guarantee delivery of email notifications, you must have an ActiveMQ mail server. If you do not use ActiveMQ, Access Review sends the notification once, regardless of success or failure of delivery.

You can also configure Access Review to send reminders of tasks, based on the escalation timeout setting. For more information, see [REFERENCE](#).

When Access Review sends an email, the application queries the preferred language of the target user. If Access Review supports that language, the email is delivered in the preferred language. Otherwise, the emails use the default language for the system. You can customize the content in the emails. For more information, see [Section 2.6.2, “Customizing the Email Templates,” on page 30](#).

To configure the mail server for notifications:

- 1 In the AR Configuration Utility, select *Workflow Settings*.
- 2 Under *Notification System*, specify the settings for the mail server.
- 3 (Optional) To ensure guaranteed delivery of the notifications, complete the following steps:
 - 3a Select *Enable persistent notification message queue*.
 - 3b Enter the settings for the JMS broker.
 - 3c (Optional) To use TLS/SSL protocol for messaging, select *SSL* and then specify the keystore settings.
- 4 Click *Save*.
- 5 (Optional) To change the text in the email notifications, continue to [Section 2.6.2, “Customizing the Email Templates,” on page 30](#).

2.6 Customizing Access Review

You can customize the displayed names of attributes and risk levels in the Access Review interface. You can also customize the content in the templates for the email notifications. Access Review automatically localizes the attributes and email text according to the user’s preferred language:

- ♦ Chinese Simplified
- ♦ Chinese Traditional
- ♦ Danish
- ♦ Dutch
- ♦ English
- ♦ French
- ♦ German
- ♦ Italian
- ♦ Japanese
- ♦ Portuguese
- ♦ Russian
- ♦ Spanish
- ♦ Swedish

2.6.1 Localizing the User Interface

You can customize the displayed names of attributes and risk levels in the Access Review interface. The application automatically displays the information according to the user's preferred language. Access Review allows you to modify a `.properties` file that contains the strings for all built-in attributes and risk levels. You can use a text editor to customize the value that the interface displays for each attribute.

Use this feature if your organization requires special terminology for some or all attributes. For example, you might refer to *user ID* as *account name*. You can change all instances of *user ID* in the catalog.

- 1 Log in to Access Review as the bootstrap administrator or with an account in the Global Administrator role.
- 2 In the Access Review menu, click *Settings*.
- 3 In the right panel, click *Localization*.
Access Review lists the `.properties` files by language.
- 4 Select the language that you want to customize.
Depending on your browser settings, you might be prompted for the download path.

NOTE: If prompted, do not rename the `.properties` file. Access Review cannot upload a file that does not match the expected name.

- 5 In a text editor, customize the displayed text for the attributes that you want to change.
For example, you want to change all instances of *user ID* to *account name*. When you search for *user ID*, you will find the following type of string:

```
com.netiq.iac.persistence.ops.AttributeDefinition.USER.guid=LDAP User ID  
Change LDAP User ID to LDAP Account Name.
```

NOTE: Do not modify any text in the code string before the `=` sign. For example, `com.netiq.iac.persistence.ops.AttributeDefinition.USER.guid=`. Access Review might not function appropriately if you change the code string incorrectly.

- 6 Save and close the file.
- 7 To submit the modified file, click the *Upload* icon beside the language that you customized.
- 8 Click *Save*.
- 9 Refresh the browser window to view the changes.

2.6.2 Customizing the Email Templates

Access Review can notify users of tasks in their queue. The application uses default templates for the email notifications. Access Review allows you to modify an XML file that contains the email templates in the languages supported for Access Review. You can edit the XML file in one of the following programs:

- ♦ XML editor
- ♦ Text editor
- ♦ Designer for NetIQ Identity Manager

For more information about configuring Access Review to send email notifications, see [Section 2.5.4, “Configuring the Mail Server for Notifications,”](#) on page 28.

- 1 Log in to Access Review as the bootstrap administrator or with an account in the Global Administrator role.
- 2 In the Access Review menu, click *Settings*.
- 3 In the right panel, click *Localization*.
- 4 Select *email templates (all languages)*.

Depending on your browser settings, you might be prompted for the download path.

NOTE: If prompted, do not rename the `EmailTemplates.xml` file. Access Review cannot upload a file that does not match the expected name.

- 5 Modify the content in the following emails in the appropriate languages, as needed:

- ♦ Access Removal Notification
- ♦ Access Review Task Pending
- ♦ Access Review Task Reminder
- ♦ Auditor Approval Task Pending
- ♦ Auditor Approval Task Reminder
- ♦ Auto Provisioning Start Failed
- ♦ Certification External Provisioning Start Error
- ♦ Manual Fulfillment Task Pending
- ♦ Manual Fulfillment Task Reminder
- ♦ Owner Approval Task Pending
- ♦ Owner Approval Task Reminder
- ♦ Review Approval Task Start Error
- ♦ Review Error
- ♦ Review Reminder
- ♦ Review Started

NOTE: Do not modify any text in the code strings in the file. Access Review might not function appropriately if you change the code strings incorrectly.

- 6 Save and close the file.
- 7 To submit the modified file, click the *Upload* icon beside *email templates (all languages)*.
- 8 Click *Save*.

2.7 Integrating Access Review with NetIQ Identity Manager

If you have installed NetIQ Identity Manager Home and Provisioning Dashboard (Identity Manager Home), your users can log in once to access both Identity Manager Home and Access Review. NetIQ uses OSP to provide users single sign-on access from the Home page. To ensure single sign-on access, you must configure both Identity Manager Home and Access Review. Users can easily shift between the two applications without needing to enter their credentials a second time.

When you integrate Access Review with Identity Manager Home, you must change the authentication server for Access Review to the same server that Identity Manager Home uses.

Use the following checklist to ensure a proper integration between the products:

	Checklist Items
☐	1. To ensure that you have the correct software versions for integration, review the release notes for Access Review and Identity Manager Home. For more information, see the Identity Manager Documentation site (https://www.netiq.com/documentation/idm402/) .
☐	2. Ensure that users can link to Identity Manager Home from Access Review. For more information, see “Adding a Link to Home in the Access Review Menu” on page 32 .
☐	3. Determine whether you want to use the authentication server for Identity Manager Home. For more information, see “Using the Same Authentication Server as Identity Manager Home” on page 33 .
☐	4. Ensure that users can link to Access Review from Identity Manager Home. For more information, see Section 2.7.2, “Configuring Identity Manager Home for Integration,” on page 33 .
☐	5. Integrate Access Review with the workflows used in Identity Manager. For more information, see Section 2.7.3, “Configuring an Automatic Process to Fulfill Changes,” on page 33 .

For more information about Identity Manager Home, see the [User Guide for NetIQ Identity Manager Home and Provisioning Dashboard](#).

2.7.1 Configuring Access Review for Integration

For proper integration, you must link Access Review to the Identity Manager Home page. You can also choose to use the same authentication server that Identity Manager Home uses to verify login attempts. This process includes the following activities:

- ♦ [“Adding a Link to Home in the Access Review Menu” on page 32](#)
- ♦ [“Using the Same Authentication Server as Identity Manager Home” on page 33](#)

Adding a Link to Home in the Access Review Menu

This section describes how to add a link in Access Review so users can easily switch to Identity Manager Home.

- 1 Log in to Access Review as the bootstrap administrator or with an account in the Global Administrator role.
- 2 In the Access Review menu, click *Settings*.
- 3 In the right panel, click *Identity Manager Settings*.
- 4 For *Home Page URL*, specify the URL for Identity Manager Home.
- 5 Click *Save*.
- 6 Click *Refresh* beside the *Home Page URL* field.
- 7 To verify the integration, complete the following steps:
 - 7a Verify that the Access Review menu lists *Home*.
 - 7b Click *Home*, and verify that it takes you to the Identity Manager Home page.

Using the Same Authentication Server as Identity Manager Home

This section describes how to configure Access Review to use the same authentication server as Identity Manager Home for verifying users who log in to the applications.

- 1 Stop Access Review (and Tomcat):

```
./path_to_Tomcat_folder/shutdown.sh
```

- 2 In the AR Configuration Utility, click *Authentication Server Details*.
- 3 De-select *Same as AR Server*.
- 4 Specify the protocol, host name or IP address, and port that represent the authentication server for Identity Manager Home.

NOTE: To use TLS/SSL protocol for secure communications, select *https*.

- 5 Click *Save*, and then close the utility.
- 6 Start Access Review (and Tomcat):

```
./path_to_Tomcat_folder/start.sh
```

2.7.2 Configuring Identity Manager Home for Integration

You can update the Identity Manager Home page to include a link to Access Review. For more information, see “[Configuring Identity Manager Home Items](https://www.netiq.com/documentation/idm402/idmhomepage/data/b15q23lh.html)” (<https://www.netiq.com/documentation/idm402/idmhomepage/data/b15q23lh.html>) in the *User Guide for NetIQ Identity Manager Home and Provisioning Dashboard*.

NOTE

- ♦ To ensure proper integration, you might need to update your version of Identity Manager Home or Access Review. For more information, see the Release Notes for each product.
 - ♦ Ensure that you have configured single sign-on in Identity Manager Home. For more information, see “[Configuring Single Sign-On](https://www.netiq.com/documentation/idm402/idmhomepage/data/b154tjqb.html)” (<https://www.netiq.com/documentation/idm402/idmhomepage/data/b154tjqb.html>) in the *User Guide for NetIQ Identity Manager Home and Provisioning Dashboard*.
-

2.7.3 Configuring an Automatic Process to Fulfill Changes

Access Review supports a variety of data collection sources for users and their associated permissions. If the data collection source is the Roles Based Provisioning Module (RBPM) in NetIQ Identity Manager, you can set up a system where Access Review automatically processes the change set items for permission removal and RBPM fulfills the changes. For more information, see [Chapter 4, “Performing Reviews,”](#) on page 37.

You must configure Access Review to connect to the external provisioning system. You can modify the settings in the AR Configuration Utility or in Access Review. If you make the changes in Access Review, you can test the connection to the specified system.

- 1 (Conditional) In the AR Configuration Utility, navigate to *Workflow Settings > External Provisioning System*.
- 2 (Conditional) In Access Review, navigate to *Access Review menu > Settings > External Provisioning System*.
- 3 Specify the URL and login credentials for the external provisioning system.

- 4 (Optional) To verify the specified information, in Access Review, select *Test Connection*.
- 5 Click *Save*.

3 Collecting and Viewing Data

To certify that your users have the appropriate levels of access to your resources and applications, you first need to collect data on all the users, accounts, resources, and applications that exist in your environment. Access Review allows you to import identity and application data. You can import identity data from the following identity data sources:

- ♦ Active Directory
- ♦ CSV file
- ♦ eDirectory
- ♦ Identity Manager
- ♦ JDBC
- ♦ LDAP

Once you have collected the data and published it to the Identity Vault, you can view specific data by selecting the *Catalog* menu item, the type of data you want to view, then opening the detail view for that type of data. If you want to edit attributes, click the pencil icon for that data point. For example, you can edit the temporary phone number for a particular user.

3.1 Importing Data into the Catalog

You can only add a new data sources and collect data under the bootstrap account or an account with the Global Administrator role. You can only merge and publish data under the bootstrap account, an account with the Global Administrator role, or a Data Collection account.

Once you have collected data, Access Manager stores the data in the catalog. You can view the data and make specific changes to the attributes of individual items.

To collect and publish data:

- 1 (Conditional) If you are going to merge the data you collect with existing data in the data vault, set up merging rules by performing the following steps: selecting *Collection* -> *Identity Sources* -> *Set merging rules*.
- 2 Add your data sources by selecting *Overview*->*Data Collection* ->*Identity Sources*. From that point, select the type of data you want to collect and add the source. You need to add at least one identity data source, such as Active Directory, and at least one application data source.
- 3 Collect the data by selecting *Collection*, the kind of data, the source, then click the *Collect Now* icon.
- 4 Publish the data by selecting *Collection*, the kind of data, the source, set the *Publish behavior*, then click *Collect Now*.

3.2 Viewing and Editing Specific Data Attributes

Once you have published data, you can view the items, such as users and applications, along with their attributes, such as a user's phone number. To view the attributes of a specific item in the catalog, select *Catalog*, the type of data you want to view, then the details for that data type.

If you want to edit the information, select *Catalog*, the type of data you want to view, then the details for that data type, then the Edit option for that data type. When you change a value, an icon is shown next to the value. You can later reset the value to the value that was originally collected. At this point, you can also associate tags, or metadata, so you can more easily identify the information when you create and perform a review.

3.3 Searching for Users or Groups

You can search for specific users or groups in the catalog by select *Catalog*, then either *Users* or *Groups*. From there, you can browse through the list or you can use the search field to search for a particular user or group. You can search using names or attributes.

To search for users or groups:

- 1 Select *Catalog*, then the type of data you want to search across.
- 2 Enter string in search field.
- 3 Specify which attributes you want to search in *Display Options*.
- 4 Click on the interlocking rings icon to start the search.

4 Performing Reviews

Once you have data in your catalog, you can begin the review process. This is where a set of reviewers examines either the access permissions of a set of users or some other set of parameters for users or applications. The review process results in a list of changes, or **changeset** that are then implemented. Access Review refers to the implementation process as fulfillment. Fulfillment can be done in one of three ways:

1. Manual: Permissions are removed using a manual process. For information about how to perform a manual fulfillment, see [Section 4.3, “Manual Fulfillment,” on page 38](#)
2. Automated: Permissions are removed automatically by Identity Manager. This is possible if permissions came from a collection from an Identity Manager system.
3. Custom using External Workflow: Permissions are removed by an Identity Manager Roles-Based Provisioning Module workflow.

4.1 Creating a Review

When you have data published in the catalog, you start a review and select the kind of data you want to review.

To create a review:

- 1 Select Review panel and Press + icon.
- 2 Click the + icon to create a new review.
- 3 Name the review.
- 4 Select the type of user or application data that you want to review. The list comes from the names you associated with the data when you collected and edited it.
- 5 Select any attributes that you want to use to limit the review data.
- 6 Select reviewers and the review owner.
- 7 Save the review.

4.2 Completing Review Tasks

When a reviewer logs into Access Review, that reviewer will have tasks for any active review that they are assigned to.

To complete the review tasks for a typical reviewer:

- 1 Navigate to Tasks panel, and select the review that you want to perform.
- 2 Evaluate the items on the list, usually the list will be reviewers with permissions to a particular application.
- 3 Click the Remove button next to any permissions you want to remove.

4 Look over the changes to ensure accuracy.

5 Click **Certify**.

Once the reviewers have completed their tasks, the review owner must approve the changes to create a change list to be fulfilled.

4.3 Manual Fulfillment

4.3.1 How Manual Fulfillment Works

The person (or people if the fulfiller is a group) in charge of removing permissions is presented with a task that contains the list of permissions to remove. The removal is done in a domain-specific manner, based upon the actual permission. Once the permission is removed, they indicate on the task list either **Done** if they successfully removed the permission, or **Refused** if they could not remove the permission. The user continues to click **Done** or **Refused** on each permission in the list they are all resolved.

Since the process of removing permissions may be over the span of many days, and there may be many permissions to be removed, Access Review provides the following features:

1. Since the fulfiller can be a group, multiple users can work on the permission removal at the same time.
2. Customizable emails are sent to the participants to remind them that they have a manual de-provisioning task to do. The first one is sent when they first get the task, and reminders are sent periodically, namely once every escalation period/3. The email has a link which takes the directly to the task.
3. A click of *Done* or *Refused* saves the change immediately, with an option to undo.
4. A click of *Submit* locks Done/Refused permission decisions, marking them as complete.
5. There are various sort options, plus a filter option to show only incomplete items.
6. A batch mode where one can select *Done* or *Refused* for a number of items at the same time. Likewise, the same comment can be applied to a number of items.
7. When all items are marked complete, the task is automatically removed from the task list.

4.3.2 Implementing Manual Fulfillment

The type of fulfillment chosen is on an Application basis. To setup manual fulfillment, follow these steps:

- 1 Select *Catalog -> Applications*
- 2 Select the Application you want to set up.
- 3 Click *Edit Application*
- 4 In the drop down in the fulfillment area, choose *Manual*.
- 5 In the resulting type-ahead picker, choose the fulfiller for this application. You can only choose one fulfiller, but you can choose a group so more than one person can work on the fulfillment tasks.

5 Managing Access Review Users

This section discusses security configuration and authorization settings for the users who administer Access Review, as well as the users who evaluate access to applications and the users who implement the changes.

5.1 Understanding Roles in Access Review

Access Review relies on roles, defining a fixed set of roles and permissions. Access Review roles can be global or runtime:

- ♦ Global roles are constant within Access Review and assigned through the Access Review Administration and Settings. Access Review maintains the set of privileges granted by the role.
- ♦ Runtime roles are those that users assume as needed during an access review and validation cycle. Review owner, application owner, application data administrator, reviewer, and review auditor are all roles that are assigned as needed during an access review and validation cycle. They can be reassigned with each new cycle.

The options to assign global roles are under the *Setting* menu. To assign application-specific roles, such as Application Administrator, Application Owner, and Application Fulfiller, go to the catalog and edit the application. You specify review-specific roles, Review Owner, Escalation Owner, Review Auditor, and Reviewer, when you create the review.

5.2 Global Roles

Access Review defines the following global roles.

Administrator

The Administrator is the primary role and can:

- ♦ Perform all Access Review actions
- ♦ Assign all Access Review global and runtime roles

Review Administrator (RA)

The Review Administrator can access to the Access Review dashboard and has full rights to all review definitions. The Review Administrator can:

- ♦ Schedule a review
- ♦ Assign all the runtime roles as part of a review, thereby delegating certain rights pertaining to the Review to those roles
- ♦ Modify a review schedule
- ♦ Start a review

The Review Administrator has read access to the Access Review catalog.

Data Administrator (DA)

The Data Administrator can access to the Access Review dashboard and has full rights to manage identity and application data sources. The Data Administrator can:

- ♦ Execute data collection and publishing
- ♦ Review and curate collected catalog data
- ♦ Delegate certain rights for the specific application to other roles, for example, Application Administrator, Application Owner, and Application Fulfiller

Provisioning Administrator (PA)

The Provisioning Administrator has full right to provisioning real time and historical data, including fulfillment status and verification management.

Auditor (AU)

The Auditor has read-only rights to all of Access Review, including catalogs, reviews, fulfillment status, and the Access Review dashboard.

Security Officer (SO)

The Security Officer has rights to modify Access Review configuration settings, including role assignments.

5.3 Runtime Roles

Access Review defines the following runtime roles.

Review Owner (RO)

The Review Owner (RO) has full rights to the assigned Review instance. Review instance scope limits the Review Owner role authorization. The Review Owner role can launch the review or see existing history of the review campaigns.

For an active Review, the Review Owner can:

- ♦ Monitor review progress using dashboards

NOTE: The Review Owner has access to the Overview portion of the Access Review dashboard.

- ♦ Perform any certifications that are part of that review
- ♦ Resolve access policy violations in the review
- ♦ Reassign certification tasks within the review
- ♦ Run reports against the review
- ♦ Declare the review complete

The Review Owner can view the details of any user, permission or application entity within the context of the campaign, excluding catalog access rights.

The Review Administrator who initiates a review automatically assumes the role of Review Owner if no Review Owner is specified.

Reviewer (RE)

The Reviewer (RE) role has the responsibility to review a set of access permissions as part of a review campaign and decide whether each should be maintained or revoked.

The Reviewer role can:

- ♦ Decide whether to keep or remove access privileges for a user under review.

- ♦ Skip a review item.
- ♦ View user, permission, application, and account details in the context of the review

Access Review provides a set of predefined macros to select a Review Owner:

- ♦ Supervisor
- ♦ Application Owner
- ♦ Permission Owner

Escalation Reviewer (ER)

The Escalation Reviewer (ER) role is an optional participant in a review. The Escalation Reviewer can view user, permission, application, and account details in the context of the review.

If an Escalation Reviewer is configured in the review definition, all tasks not completed on time are forwarded to the Escalation Reviewer for resolution. Otherwise, the tasks are forwarded to the Review Owner.

Review Auditor (RA)

The Review Auditor (RA) role is an optional participant in a review. Each review can have its own Review Auditor.

After the Review Owner marks review complete, the Review Auditor can accept or reject the review. The Review Auditor has read-only access to the review data. A review audit is a legal stamp, accepting or rejecting of a review has no impact on the change access request fulfillment.

Change Set Fulfiller (CSF)

The Change Set Fulfiller (CSF) role has the responsibility to perform manual provisioning for requested access changes. A Change Set Fulfiller can view the change set, identity, permission, and application details for each fulfillment task.

Workflow Service (WS)

The Workflow Service role is automatically assigned to the account under which the Access Review workflow service runs. The Workflow service role is a service role that has access to the REST API and to data but has no access to the Access Review browser-based user interface.

Application Administrator (AA)

The Application Administrator role is responsible for validating published data and performing data clean-up, or “curation”, for an application. The Application Administrator has read permission to the whole catalog and write permission to the part of the catalog in the context of the application.

6 Using Access Review with Identity Manager

This chapter discusses use the specialized Identity Manager collector and features integrated into Access Review to demonstrate the full collection-review-provisioning cycle.

6.1 Automated Fulfillment Using Identity Manager

Access Review supports a variety of data collection sources for users and their associated permissions. If the data collection source is Identity Manager Roles Based Provisioning Module, it is possible to setup the system so that the change set items for permission removal are processed automatically by Access Review, and fulfilled by the Roles Based Provisioning Module.

In order for this to happen, the permission in question must be explicitly set. In Identity Manager Roles Based Provisioning Module, there are two classes of permissions: Roles and Resources. The rules for the ability for Access Review to automatically de-provision differs depending upon permission type:

- ♦ All Identity Manager Roles Based Provisioning Module Resource can be automatically deprovisioned, since all Identity Manager Roles Based Provisioning Module resources are explicitly set.
- ♦ An Identity Manager Role if the role has been explicitly set, i.e. technically if the user has an `nrfAssignedRole` attribute pointing to that Role. As an illustration, if a user had a Role indirectly, say because the Role was assigned to a container or a group, then that role cannot be automatically deprovisioned.

If the permission cannot be automatically de-provisioned, processing drops to a fallback, which is either Manual, or External Workflow, based upon how the Application was setup.

6.1.1 How to Set Up Automated Identity Manager Role Based Provisioning Module Workflow Fulfillment

Choose the Identity Manager Role Based Provisioning Module external workflow for each application you wish to use this method.

- 1 In Access Review, select *Catalog -> Applications*.
- 2 Select the application you want to set up.
- 3 Click *Edit application*.
- 4 In the drop down in the fulfillment area, choose one of the following:
 - ♦ *Automated with Manual Fallback* to choose the automated fulfillment process.
 - ♦ *Automated with Identity Manager Workflow fallback* to choose the workflow process.

6.1.2 How Automated Fulfillment Works

The following items describe how automated fulfillment works:

- ♦ When a changeset is generated on the by the Access Review server, it examines in turn each application the change items belong to. If they belong to an Application identified as having Automated fulfillment, the server identifies which permissions in that changeset are eligible to be automatically provisioned, according to the rules above, namely if it is either a Roles Based Provisioning Module Resource, or an explicitly assigned Roles Based Provisioning Module Role.
- ♦ For each of the automated group, the Access Review engine calls back to the Roles Based Provisioning Module and de-provisions them.
- ♦ For the non-automated group, de-provisioning follows the fallback path, either manual tasks that a user must complete, or using an Identity Manager Workflow that performs the tasks.

6.2 Custom Fulfillment Using External Provisioning Workflow

Using an Identity Manager Roles Based Provisioning Module external workflow would be indicated for applications where permission de---provisioning can be automated using the capabilities inherit in the Identity Manager Roles Based Provisioning Module system. Keep in mind these capabilities include REST calls, SOAP calls, and the ability to write to eDirectory, which could trigger a driver to process the deprovision. It could also prove to be an alternative to the straight manual process, where the tasks would be managed by the Roles Based Provisioning Module workflow rather than Access Review.

6.2.1 Configuring External Identity Manager Workflow Fulfillment

To set up Identity Manager Roles Based Provisioning Module workflow, you must prepare the workflow, setup Access Review to connect to the Roles Based Provisioning Module, then choose the workflow for each application you want to fulfill.

Preparing the Workflow

Any workflow is eligible to participate in this process as long as it takes as inputs the following two fields:

- ♦ String: changesetId
- ♦ String: appId

The workflow gets passed in the changesetId and the appId, and it calls back to Access Review to get the particulars of all the tasks for that changeset/app combination. It then parses these tasks, completes each one, and finally calls back to Access Review when it is complete. GCVs are typically used to hold the connection parameters.

Setting Up Access Review to Communicate with Identity Manager

Under *Settings*, your system administrator should set the userid and password of the Identity Manager Roles Based Provisioning Module Provisioning Administrator. There is a test button to make sure everything is working. Furthermore, the test also checks that you have at least one Provisioning Request Definition workflow that is eligible to be used as an external fulfillment —it does this by verifying the required inputs. Note the use of the full URL, it is pointing to the Identity Manager Roles Based Provisioning Module SOAP service. For Username, you may type in the full dn of your user, or if your system is setup with well known user containers, all you need is the cn.

Choosing the Identity Manager Workflows

To choose the external Identity Manager Roles Based Provisioning Module external workflow:

- 1 Using Access Review, go into *CatalogApplications*.
- 2 Select the Application you want to set up.
- 3 In the Application UI, click **edit application**
- 4 In the drop down in the fulfillment area, choose **Identity Manager Workflow**
- 5 In the resulting type---ahead picker, choose the Identity Manager Workflow you wish to run when the changeset of the application goes into fulfillment state.

6.2.2 Understanding External Identity Manager Workflow Fulfillment

External workflow fulfillment works as follows:

- ♦ When a changeset is generated on the by the Access Review server, it examines in turn each Application the change items belong to. If they belong to an Application identified as having an Identity Manager Workflow fulfillment, no further processing is done on those change items. Instead, the Access Review server calls back to that external workflow, expecting it to process all of those change items. The workflow is passed the changeset Id and the application Id.
- ♦ Upon start, the workflow needs to call back to Access Review using REST to get the contents of the change set. Note: Basic Authentication is not accepted for that REST call – instead, the workflow engine must first obtain an OAUTH token from the OAUTH server, and then use that token as the authentication header in subsequent REST calls. The token usually times out in 120 seconds, so a new token must be obtained if the next call takes place after that.
- ♦ Once the list of tasks is obtained, logic in the workflow must process them. The sample has a loop setup with a “TODO” step that logs the task. It is there where the custom logic will be placed.
- ♦ After all tasks are complete, the workflow needs to callback to Access Review with a status setting all those tasks to complete.
- ♦ Any other processing that needs to be done during processing is up the requirements of the customer. As an example, the sample sends an email to the users who will be losing permissions, something that the base Access Review does not.

