
NetIQ® Identity Governance

User Guide

April 2018

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.

Contents

About this Book and the Library	13
About NetIQ Corporation	15
1 Overview	17
Understanding Installation and Configuration	17
Understanding Data Collection and Publication	18
Understanding Data Sources	18
Collecting Identity and Application Data	19
Publishing a Catalog of Collected Identities	20
Preparing Published Data for Review	20
Understanding the Review Process	20
Reviewing Access and Permissions	21
Fulfilling Changes Requested in the Review	21
Completing and Approving a Review	22
Understanding Reporting	22
Part I Installing Identity Governance	23
2 Planning to Install Identity Governance	25
Checklist for Installing Identity Governance	25
Understanding Authentication for Identity Governance	27
Using One SSO Provider for Authentication	27
Understanding Authentication with One SSO Provider	28
Understanding the Bootstrap Administrator for Identity Governance	29
Understanding the Keystore for the Authentication Server	29
Understanding Password Management in Identity Governance	30
Understanding Identity Reporting	30
Understanding the Identity Governance and Reporting Databases	31
Understanding the Identity Governance Databases	31
Understanding the Identity Reporting Database	33
Recommended Installation Scenarios and Server Setup	33
Identity Governance in a New Environment	33
Identity Governance and Identity Manager	34
Identity Governance and Existing Components	34
Component Installation Order	35
Recommended Server Setup	35
Selecting an Operating System Platform for Identity Governance	36
Ensuring High Availability for Identity Governance	37
Prerequisites for Installing Identity Governance	38
General Prerequisites for Identity Governance	38
Prerequisites for the Identity Governance Databases	39
Prerequisites for the Tomcat Application Server	40
Prerequisites for One SSO Provider	40
Prerequisites for Identity Reporting	40
Hardware and Software Requirements	41
Identity Governance Server System Requirements	41
Database Server System Requirements	43
Identity Reporting Server System Requirements	43
Identity Governance and Reporting Browser Requirements	44

Auditing Server System Requirements	45
3 Installing Tomcat, PostgreSQL, and ActiveMQ for Identity Governance	47
Checklist for Installing Tomcat, PostgreSQL, and ActiveMQ	48
Using the Wizard to Install Tomcat, PostgreSQL, and ActiveMQ	48
Silently Installing Tomcat, PostgreSQL, and ActiveMQ	51
Safeguarding the Passwords for a Silent Installation	51
Installing Tomcat, PostgreSQL, and ActiveMQ Using a Silent Properties File	51
Stopping, Starting, and Restarting Tomcat	52
Linux Examples for Tomcat	52
Windows Examples for Tomcat	52
Stopping, Starting, and Restarting ActiveMQ	53
Linux Examples for ActiveMQ	53
Windows Examples for ActiveMQ	53
4 Installing One SSO Provider	55
Checklist for Installing One SSO Provider	55
Using the Wizard to Install One SSO Provider	55
Silently Installing One SSO Provider	59
Creating a Silent Properties File for Installing on a Secondary Node	59
Running a Silent Installation	60
5 Installing Identity Governance	63
Checklist for Installing and Configuring Identity Governance	63
Preparing a PostgreSQL Database for Identity Governance	65
Adding the JDBC File to the Application Server	65
Creating the PostgreSQL Databases Before Installation	65
Creating a Temporary PostgreSQL Database Administrator for the Installation Process	66
Preparing an Oracle Database for Identity Governance	67
Adding the Oracle JDBC File to the Application Server	67
Creating the Schemas for the Oracle Database before Installation	68
Creating a Temporary Oracle Database Administrator for the Installation Process	69
Preparing an MS SQL Server Database for Identity Governance	70
Adding the JDBC File to the Application Server	70
Creating the MS SQL Server Databases Before Installation	70
Creating a Temporary MS SQL Server Database Administrator for the installation process	72
Using a Guided Process to Install Identity Governance and Identity Reporting	73
Performing a Silent Installation of Identity Governance	79
Understanding the Passwords that Identity Governance Reads from Environment Variables	
During the Installation Process	80
Creating a Silent Properties File for Installing on a Secondary Node	80
Running the Silent Installation	81
6 Installing Identity Reporting	83
Checklist for Installing Identity Reporting	83
Understanding the Installation Process for the Identity Reporting Components	84
Understanding the Installation Process for Identity Reporting	84
Understanding the Users that the Installation Process Creates	85
Preparing the Database Environment for Identity Reporting	85
Preparing MS SQL Server	85
Preparing Oracle	86
Preparing PostgreSQL	86
Installing Identity Reporting	87

Using the Guided Process to Install Identity Reporting	87
Installing Identity Reporting Silently	94
7 Completing the Installation Process	97
Configuring the Databases after Installation	97
Configuring the PostgreSQL Databases for Identity Governance	98
Configuring the Oracle Database for Identity Governance	99
Configuring the MS SQL Database for Identity Governance	100
Configuring the Identity Reporting Databases	100
Preparing One SSO Provider for Use	101
Ensuring the Configuration Update Utility Can Run OSP	101
Preparing OSP to Use an Active Directory LDAP Server	102
Enabling Auditing for the OSP after the Installation	103
Completing the Cluster Configuration for Identity Governance	103
Configuring the Nodes in the Tomcat Cluster	103
Configuring ActiveMQ Failover in the Tomcat Cluster	104
Cleaning Up Unfinished Data Production Jobs	105
Ensuring Rapid Response to Authentication Requests	105
Enabling Auditing	106
Enabling Auditing for Identity Governance	106
Enabling Auditing for Identity Reporting	108
Enabling Auditing for OSP after the Installation	109
Starting and Initializing Identity Governance	110
Configuring Identity Governance for Two-Factor Authentication	112
Prerequisites for Configuring Two-Factor Authentication	112
Configure the Advanced Authentication Server for Two-Factor Authentication	112
Configure OSP for Two-Factor Authentication	114
Testing the Enrolled Methods	116
Updating the License Key	116
8 Upgrading Identity Governance	119
Planning to Upgrade Identity Governance	119
Saving Customized Settings for Attributes in the Catalog	120
Running the Cleanup Utility	121
Changes to Passwords Stored in Environment Variables	121
Upgrading Procedure	121
9 Uninstalling Identity Governance	125
Part II Configuring and Managing Identity Governance	127
10 Configuring Identity Governance Settings	129
Running the Identity Governance Configuration Utility	129
Identity Governance Server Details	130
Authentication Server Details	130
Security Settings	131
Network Topology Settings	132
Miscellaneous Settings	132
Bulk Data Update Settings	134
Workflow Settings	134
Using the TLS/SSL Protocol for Secure Connections	136
Configuring the Mail Server for Notifications	137
Configuring Fulfillment	138

Configuring Multiple Fulfillment Targets for an Application	139
Transforming Data from Fulfillment Targets	140
Configuring Identity Manager and Manual Fulfillment Methods	140
Configuring Service Desk Fulfillment	141
Understanding Fulfillment Status	146
Configuring Analytics and Role Mining Settings	148
Understanding Role Mining Settings	150
Creating Custom Metrics	150
Viewing Entitlement Assignments Statistics to Leverage Roles	151
Viewing Account Statistics and Details	151

11 Customizing Identity Governance for Your Enterprise 153

Localizing to the User's Preferred Language	153
Customizing the User Interface	154
Customizing the Labels in the Identity Governance Interface	154
Customizing Strings in the JAR Properties Files	155
Translating Content for Identity Governance and One SSO Provider	156
Preparing Files for Translation	157
Ensuring that Identity Governance Recognizes the New Language	158
Adding the Translated Labels to the Identity Governance Interface	159
Adding Translated Content to Identity Governance and OSP	159
Verifying the New Translations	160
Customizing the Email Notification Templates	160
Modifying Email Templates	161
Adding an Image to the Email Template	163
Customizing the Identity Governance Style Sheet	163
Customizing the Collector Templates for Data Sources	164
Customizing Fulfillment Target Templates	165
Specifying Additional Fulfillment Context Attributes	165
Using Coverage Maps	165
Creating Coverage Map	166
Loading Coverage Map	170
Customizing Categories	171
Customizing Review Display	171
Configuring Reasons for Review Actions	172
Disabling Review Email Notifications	172
Extending the Identity Governance Schema	173
Adding or Editing Attributes to Extend the Schema	173
Adding Attributes to a Collector	175
Viewing Available Attributes in Business Roles	176

12 Changing Passwords for Administrative Users 177

How to Change the Password for the Bootstrap Administrator	177
How to Change the Password for the Database Users	178

13 Adding Identity Governance Users and Assigning Authorizations 179

Understanding Authorizations in Identity Governance	179
Global Authorizations	179
Runtime Authorizations	181
Adding Identity Governance Users	184
Assigning Authorizations to Identity Governance Users	184

14 Integrating Single Sign-on Access with Identity Manager	187
Checklist for Integrating Identity Governance with Identity Manager	187
Configuring Identity Governance for Integration	188
Adding a Link to Identity Manager Home in the Identity Governance Menu	188
Using the Same Authentication Server as Identity Manager	188
Configuring Identity Manager for Integration.	189
Configuring a File Authentication Source for the Bootstrap Administrator	190
 Part III Managing the Identity Governance Catalog	 193
 15 Creating and Managing Data Sources	 195
Understanding Collector Configuration	195
Understanding the Common Elements in a Collector	196
Understanding Collector Templates for Identity Sources	197
Understanding Collector Templates for Application Sources	197
Understanding the Variations for Data Sources	199
Transforming Data During Collection	201
Creating Identity and Application Sources	201
Understanding Change Event Collection Status	204
Supported Attribute Syntaxes for eDir and IDM Change Events Collection.	204
Managing Identity and Application Sources	205
Exporting and Importing Collectors	205
Comparing Collections and Publications	206
Testing Collections	206
Creating Emulation Packages	207
Migrating an Identity Collector to a Change Event Identity Collector.	207
 16 Creating and Monitoring Scheduled Collections	 211
Creating a Scheduled Collection.	211
Monitoring Scheduled Collections.	212
Understanding the Cron Expression for a Custom Interval of Collection	212
 17 Integrating Collected Data with Identity Manager	 215
Understanding Synchronization and Reflection	215
Reflecting Application Permissions in Identity Manager.	215
Synchronizing Data Changes between Identity Governance and Identity Manager	216
Ensuring Best Performance for Identity Matching.	217
Reflecting Permissions and Assignments from Applications Not Connected to Identity Manager	217
Synchronizing Changes in Identity Governance Data with Objects in the Identity Vault.	218
Synchronizing New User Objects.	218
Synchronizing Resource Objects	219
Migrating User Objects to the Identity Vault	219
Targeting Identities that Do Not Exist in Identity Manager	220
Adding Application Permissions after Migrating Identities	220
 18 Publishing the Collected Data	 221
Publishing Identity Sources.	221
Understanding Publication Behavior	221
Setting the Merge Rules for Publication.	222
Publishing the Identity Sources	222
Publishing Application Sources.	223

19 Managing Data in the Catalog	225
Configuring the Data Source for Post Authentication Matching	225
Understanding Identity, Application, and Permission Management	226
Managing Identity Information	226
Managing Application Information	226
Reviewing Application Fulfillment Settings	227
Managing Permission Information	227
Editing Attribute Values on Objects in the Catalog	228
Editing Data	229
Editing Attribute Values in Bulk	229
Searching for Users or Groups	230
Managing Technical Roles	231
Understanding Technical Role States	231
Understanding Technical Role Mining	231
Creating Technical Roles	232
Activating Technical Roles	234
Editing and Deleting a Technical Role	234
Downloading and Importing Technical Roles	234
20 Grooming the Identity Governance Databases	237
Understanding the Data Purge Utility	237
Identifying Purgeable Data	237
Purging Data from the Operations Database	240
Creating a Parameters File to Run the Data Purge Utility	241
Part IV Creating and Running Reviews	245
21 Creating and Modifying Review Definitions	247
Viewing the Catalog	247
Understanding the Review Process	248
Creating a Review Definition	248
Previewing a Review	248
Reviewing Items	249
Setting Up Review Notifications	249
Escalating Review Items	249
Setting Review Expiration Policy	250
Completing or Terminating a Review	250
Fulfilling Changes and Audit Acceptance	251
Selecting a Review Type	251
Creating a Review Definition	252
Expanding and Restricting Review Items	256
Modifying a Review Definition	256
Specifying Reviewers	256
Downloading and Importing Review Definitions	257
Improving Performance in Large Scale Reviews	258
22 Running a Review Instance	259
Completing Review Tasks	259
Verifying and Approving a Review Instance	259
Fulfilling the Changeset for a Review Instance	260
Manually Fulfilling the Changeset	260
Using Workflows to Fulfill the Changeset	261

Automatically Fulfilling the Changeset	261
Using Service Desk Fulfillment	261
Confirming the Fulfillment Activities	261

Part V Using Policies in Identity Governance 263

23 Creating and Managing Separation of Duties Policies 265

Understanding Separation of Duties	265
Creating and Editing Separation of Duties Policies	265
Understanding the Separation of Duties Policy Options	266
Providing Resolution Instructions for the Separation of Duties Policies	266
Deciding what Occurs when the Separation of Duties Policy is Violated	267
Defining Separation of Duties Conditions	267
Importing Separation of Duties Policies	268
Downloading Separation of Duties Policies	268

24 Managing Separation of Duties Violations 269

Understanding SoD Violation versus SoD Case	269
Listing SoD Violations or SoD Cases	269
Viewing SoD Case Details	270
Understanding SoD Case Status	270
Approving and Resolving an SoD Violation	271
Closing an SoD Case	272

25 Creating and Managing Business Roles 273

Overview of Roles	273
Understanding Business Role States	274
Understanding Business Role Mining	275
Managing Business Roles	276
Defining Business Roles	277
Authorizing User Access Through Business Roles	281
Adding Authorizations to a Business Role	281
Adding a Business Role Approval Policy	282
Publishing or Deactivating Business Roles	283
Analyzing Business Roles	284
Editing Business Roles	284
Approving Business Roles	285
Downloading and Importing Business Roles and Approval Policies	286
Automated Access Provisioning and Deprovisioning	287
Automatic Provisioning Requests	287
Automatic Deprovisioning Requests	287

26 Calculating and Customizing Risk 289

Understanding Risk Levels and Risk Scoring	289
Risk Levels	290
Risk Scoring	290
Risk Factors	290
Risk Score Calculation Details	292
Visualizing Risk	293
Configuring Risk Levels	294
Configuring Risk Scores	294

Setting and Viewing Risk Calculation Schedules and Status	295
Viewing Calculated Risk Scores	295
27 Administering Access Request	297
Understanding Access Request	297
Configuring Access Request	297
Creating Request Policies	298
Creating Request Approval Policies	299
Assigning Resources to Request and Approval Policies	299
Assigning Request to Identity Governance Users	300
Disabling the Access Request Service	301
28 Creating and Managing Certification Policies	303
Understanding Certification Policies	303
Creating and Editing Certification Policies	303
Scheduling and Calculating Certification Policy Violations	304
Managing Certification Policy Violations	305
Resolving Certification Policy Violations	305
29 Creating and Managing Delegation	307
Understanding Delegation	307
Assigning and Managing Delegates	307
30 Creating and Managing Data Policies	309
Creating and Editing Data Policies	309
Part VI Reporting for Identity Governance	311
31 Setting Up Identity Reporting	313
Manually Generating the Database Schema	313
Preparing Identity Reporting for Use	314
Starting Identity Reporting	315
Assigning the Report Administrator Authorization	315
Testing the Integration with Identity Governance	316
Adding Data Sources to Identity Reporting	316
Enabling Auditing for Identity Reporting after Installation	317
32 Managing Identity Governance Reports	319
Understanding the Provided Reports	319
Running Identity Governance Reports	322
Part VII Instructions for Identity Governance Users	325
33 Instructions for Access Requesters and Approvers	327
Understanding the Access Request Process	327
Reviewing Current Access	328
Requesting Access and Viewing Timeline	328

Approving Access Requests	330
Comparing Access of Multiple Users	330
Retracting Access Request	331
Restarting Failed Access Request	331
34 Instructions for Reviewers	333
Understanding Reviews	333
Understanding the Steps in a Review Run	333
Understanding the Reviewer's Authorization	334
Performing a Review.	335
Viewing Completed Reviews.	336
35 Instructions for Review Owners	337
Understanding the Review Process for Review Owners.	337
Understanding the Review Definition	337
Understanding Reviewers and Escalation	338
Understanding the Fulfillment Process	338
Managing a Review in Preview Mode.	338
Managing a Review in Live Mode	339
Checklist for Managing a Review in Live Mode	340
Starting a Review Run	341
Managing a Review Run	341
Modifying the Settings of a Review Run	342
Managing the Progress of Reviewers	342
Approving the Review	343
Viewing Fulfillment Status	343
Managing the Audit Process	344
Viewing Run History	344
36 Instructions for Fulfillers	345
Understanding the Fulfillment Process	345
Managing the Fulfillment Process	345
Understanding the Fulfiler's Authorization	346
Performing a Manual Change	346

About this Book and the Library

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

Intended Audience

This book provides information for a variety of users involved in collecting, reviewing, and updating identities in your environment:

Identity architect

Design a catalog of identities that can merge attributes from multiple sources of identity data, such as applications and LDAP directories. Help with the initial set up and configuration of the catalog, data sources, and identity mapping.

Data administrator

Create identity and application sources in the Identity Governance catalog that correlate with existing sources in the organization. Configure roles and security for Identity Governance. Help business administrators and application owners to create scheduled collections and reviews. Set up manual or automated fulfillment workflows.

Business administrator

Collect and publish identity and application data for review.

Application owner or supervisor

Review identity and application data to ensure that users have only the access that they need to accomplish their assigned functions.

Auditor

Verify that changes to identities have been fulfilled and that users have only the access that they need.

Other Information in the Library

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

Release Notes

Provides information specific to this release of the Identity Governance product, such as known issues.

NetIQ Identity Manager Driver for Identity Governance

Provides information about how to install and configure the Identity Manager Driver for NetIQ Identity Governance. The Identity Governance driver allows you to provision application-specific permission catalog data from Identity Governance to Identity Manager, giving you the ability to review and certify permission assignments using Identity Governance, as well as to request and

provision these permissions using Identity Manager. The driver also can provision users in the Identity Vault for Identity Manager. For more information, see [NetIQ Identity Manager Driver for Access Review Installation and Configuration Guide](#).

Videos

Provide supplemental information about using Identity Governance. For more information, see the [NetIQ Youtube site \(https://www.youtube.com/user/netiqTV\)](https://www.youtube.com/user/netiqTV).

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
Website:	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
Website:	www.netiq.com/support

Contacting Documentation Support

Our goal is to provide documentation that meets your needs. The documentation for this product is available on the NetIQ Web site in HTML and PDF formats on a page that does not require you to log on. If you have suggestions for documentation improvements, select **comment on this topic** at the bottom of any page in the HTML version 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

NetIQ Communities, 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, NetIQ Communities 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 community.netiq.com.

1 Overview

The Identity Governance product enables administrators and managers to easily collect all user and access information in one central location and certify that users have only the level of access that they need to do their jobs. 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.

With Identity Governance, administrators and business managers can ensure that your employees, either individually or as a group, have the appropriate set of permissions. Identity Governance collects information from various identity and application data sources and manages the entire review and certification process. Identity Governance provides tools to guide you through the key phases of the access or account review, audit case management, and validation process.

- ♦ Collecting identity and application data
- ♦ Publishing identities, accounts, permissions, and groups
- ♦ Highlighting policy violations
- ♦ Grouping common permission sets into technical roles
- ♦ Establishing business role policies to describe what is authorized
- ♦ Preparing published data for review
- ♦ Previewing review data
- ♦ Reviewing user access
- ♦ Approving the review
- ♦ Fulfilling the access changes
- ♦ Verifying that the access changes were made

Understanding Installation and Configuration

You can install the components for Identity Governance in a distributed environment. Several of the components can also run in a high-availability cluster. For more information about where you should install these components, see [“Recommended Installation Scenarios and Server Setup” on page 33](#).

Identity Governance requires a relational database to operate and the data storage is grouped into four logical partitions:

- ♦ Data collection
- ♦ Operational data
- ♦ Provisioning workflow
- ♦ Analytics

Identity Governance provides authentication and Single Sign On (SSO) through the One SSO Provider service (OSP). After the client **authenticates** to OSP (with basic authentication, Kerberos or SAML), it can optionally implement a multi-factor authentication method when used with the optional Advanced Authentication Service. The OSP can be a shared service providing Single Sign On, across Identity Governance, Identity Manager and Identity Reporting services.

For more information about installation and configuration, see [Part I, “Installing Identity Governance,” on page 23](#).

Understanding Data Collection and Publication

Identity Governance processes require clean, up-to-date data obtained from a variety of sources such as Identity Manager, Active Directory, and other enterprise applications in the data center and the cloud. Identity Governance can obtain the data by directly connecting to the systems through protocols such as LDAP and JDBC, or it can simply load the data from a periodically extracted data file such as a Comma Separated Value (CSV) formatted file.

Identities are the first part of the Entitlement Catalog. Identity Governance can collect, correlate, and publish the identities. Plus, if you integrate with Identity Manager, you can leverage all the capabilities of Identity Manager to provide a synchronized, composite view of the people or things in your organization from multiple changing systems of record. Identity Governance can collect identities from multiple sources but it logically publishes the identities to a single name space in the Catalog.

Identity Governance maps the identity and entitlement data to a minimum standard schema. The schema can be extended to include custom attributes to match the shape of your identity and entitlement data.

Permissions are the next major part of the Entitlement Catalog. Applications have their own namespaces and Identity Governance can collect and publish the permissions per application in parallel. Identity Governance uses the latest published Identity Catalog to map who has what access to permissions in each application when it is published.

Collection templates are the default mappings of data from identity and application sources to the core Identity Governance standard schema. At a minimum, connection specific information such as accounts and passwords or API keys and access tokens must be provided to save the template and collect the data.

Identity Governance provides templates to simplify the collection of data from the applications. For more information about the templates, see [“Collecting Identity and Application Data” on page 19](#).

Understanding Data Sources

Identity Governance has two categories of data sources: identity and application. An **identity source**, such as SAP User Management or Active Directory, provides attributes of an identity. For example, you import employee names, titles, and human resources attributes. **Identities**, also referred to as users in the user interface and in this document, represent the people who are at the core of the processes within Identity Governance. They are the *who* in the review process of “*who* has access to *what*.” Identities are also the people who manage and perform the reviews, or who serve as the administrators of Identity Governance. **Identity sources with change events** enable incremental changes to the user and group data without having to frequently collect and publish identities.

To review the access for an application, such as Salesforce, you can create an **application source**. The application source can collect data for accounts and permissions. Accounts and permissions are the *what* in the review process of “*who* has access to *what*.” In general, **accounts** represent entities, such as a system, application, or data source, that an identity might access. For example, your employees might have an account that lets them log in to a self-service human resources application. Accounts often specify the type of permissions granted to the user. **Permissions** can describe any of the following:

- ♦ Actions that you can take within an application, such as running reports

- ♦ Items that you possess, such as an identity badge
- ♦ Things that you can access, such as a building

Your organization might also have a hierarchy of permissions based on **roles**. For example, a corporate role called *Sales Employee* might consist of various child permissions that apply to all employees, such as *Garage Access*, *Building Access*, and *Read Access to Company Intranet*. The role might also have permissions associated with sales software applications and financial data.

Each application source can contain separate **collectors** for gathering specific account and permission data. Account collectors help you discover accounts that have been added or deleted since the previous data collection. You can also determine whether accounts are being used, such as identifying the last login for that account. When you collect permission data, you can review changes to permissions, such as new groups or roles. You can also view changes in the assignments of permissions to users or accounts.

Collecting Identity and Application Data

During the data collection phase, Identity Governance collects raw data from specified identity and application data sources. Identity Governance can collect data from the following types of sources:

- ♦ Active Directory
- ♦ Azure
- ♦ CSV file
- ♦ eDirectory
- ♦ Google Apps
- ♦ Identity Manager
- ♦ JDBC
- ♦ RACF
- ♦ Salesforce.com
- ♦ SAP User Management
- ♦ ServiceNow

NOTE: Active Directory, eDirectory, and Identity Manager identity sources can be configured to generate incremental change events.

Identity Governance 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. To automate the collection process, you can create **scheduled collections** that define the interval and data sources that you want to collect.

For more information about collecting data, see [Part III, “Managing the Identity Governance Catalog,” on page 193](#).

Publishing a Catalog of Collected Identities

After collecting identity data, you can publish a snapshot of the Identity Governance catalog. The snapshot presents a consolidated view of the collected identities. Using Identity Governance, you can directly associate user identities and permissions. Alternatively, you can associate identities with accounts and associate the accounts with permissions. For more information about publishing, see [Chapter 18, “Publishing the Collected Data,” on page 221](#).

If you use the Identity Manager Driver for Identity Governance (Identity Governance driver), you can **synchronize** data that Identity Governance has collected from application sources with identities, roles, and resources in Identity Manager. For example, the Identity Vault for Identity Manager contains information related to the roles and resources assigned to Joe Smith for applications A, B, and C. Identity Governance collects Joe’s roles and permissions from applications D, E, and F. When you publish the Identity Governance catalog to Identity Manager, the driver allows you to **reflect** Joe’s roles, resources, and permissions in the Identity Vault. This option ensures that you do not have duplicate information for Joe Smith. Also, Joe can now request access to resources in applications that Identity Manager does not manage. For more information about synchronizing and reflecting user data, see [“Understanding Synchronization and Reflection” on page 215](#). For more information about the driver, see the [NetIQ Identity Manager Driver for Access Review Installation and Configuration Guide](#).

Preparing Published Data for Review

The next step is the manual process of preparing the published data for review. During the manual process, you can improve data quality by:

- ♦ Defining technical roles
- ♦ Defining business role policies
- ♦ Setting policies, such as Separation of Duties
- ♦ Providing additional meta data
- ♦ Defining business-friendly names for various entities
- ♦ Specifying risk factors for applications, roles, authorizations, and permissions

You can also **edit** the data by changing the collected values. The Identity Governance browser-based interface provides an easy way to resolve the mappings that exist among different user, account, and permission object types. For more information about preparing data, see [“Editing Attribute Values on Objects in the Catalog” on page 228](#).

Understanding the Review Process

After you edit and publish the data, you can review particular sets of applications, groups, accounts, roles, or users and permissions. You can focus reviews on selected permissions for all or selected users or accounts, or on the ongoing presence of **unmapped accounts**, which are accounts in an application without an assigned user.

In addition, Identity Governance allows you to review business role policies and memberships. Business roles organize people by their business function and user based attributes, to solve questions of what users should have access to because of who they are or what they need or might have an option to request without additional approval. For more information, see [Chapter 25, “Creating and Managing Business Roles,” on page 273](#).

To run the same review at regular intervals, you create a **review definition** with an optional schedule to automatically start at the intervals you define. Users with the Review Administrator authorization can create review definitions. For more information, see [Chapter 21, “Creating and Modifying Review Definitions,” on page 247](#).

For each review, you assign users to specific Identity Governance roles, such as:

- ♦ Owner of the review who previews, initiates and completes the review
- ♦ Users who review the sets of data
- ♦ (Optional) User who reviews escalated items
- ♦ (Optional) User who audits the review

When a reviewer or fulfiller marks an item complete, Identity Governance automatically removes the item from the task list.

Reviewing Access and Permissions

After you have a review definition, the Review Owner can preview, and initiate a **review run** or it starts automatically if you set the schedule. The review run generates tasks for reviewers, requesting that they review a set of users and decide whether the current user access should be maintained or revoked. When the Review Owner initiates a review run, Identity Governance automatically generates tasks for assigned Reviewers and notifies them as specified in the review definition. To help Review Owners ensure that the review process proceeds in a timely manner, you can specify the length of the review period, such as three weeks. In addition, you can set the schedule to run in preview mode so that the Review Owner can preview review definition and items, and change review options, review monitors, duration, and reviewers. You can also instruct Identity Governance to **escalate the process** and move the tasks to Escalation Reviewers, if specified in the review definition, or to the Review Owner if the Reviewer does not complete all tasks. For more information, see [“Escalating Review Items” on page 249](#). For more information about the review process including preview mode, see [Chapter 22, “Running a Review Instance,” on page 259](#).

Fulfilling Changes Requested in the Review

The review process results in a list of changes, or **changeset** that are then implemented. Identity Governance refers to the implementation process as **fulfillment**. You can fulfill the changeset in the following ways:

Manual

Use a manual process to modify and remove permissions. For more information about manual fulfillment, see [“Fulfilling the Changeset for a Review Instance” on page 260](#).

Automated

Use Identity Manager to automatically remove permissions. You can use this option if the permissions were collected from an Identity Manager system.

Custom using External Workflow

Use a workflow defined in Identity Manager identity applications to remove permissions.

Service Desk

Identity Governance includes connectors to various service desk products to enable fulfillment integration with your incident management applications. When you connect to an application for fulfillment, you must configure the connector to map the data fields in the change item to the input fields of the application. For more information, see [“Configuring Service Desk Fulfillment” on page 141](#).

For more information, see [“Configuring Fulfillment” on page 138](#).

Completing and Approving a Review

Review Owners can complete, terminate, review, or partially approve the decisions at any time during a review run. If they want to change the review, all access change requests are sent to fulfillment, which is the step where approved changes are implemented. After approval, a review can be optionally routed to a Review Auditor for legal acceptance.

The review and validation process that begins with data collection and publishing concludes with change request reconciliation. Identity Governance can track the status of change requests fulfilled manually or through automatic or workflow-based provisioning.

For more information, see [Chapter 22, “Running a Review Instance,” on page 259](#).

Understanding Reporting

If you install Identity Reporting with Identity Governance, you can generate reports about identity and application data, data collection and publication, reviews, and fulfillment status. Users with the Global or Report Administrator role can create, run, and view the reports. For more information, see [Part VI, “Reporting for Identity Governance,” on page 311](#).

Installing Identity Governance

This section guides you through the process of installing the components and framework required for Identity Governance:

- ♦ Application server
- ♦ Databases for Identity Governance and Identity Reporting
- ♦ Authentication service
- ♦ Identity Governance
- ♦ Identity Reporting

It is important to review the installation process before beginning.

- ♦ [Chapter 2, “Planning to Install Identity Governance,” on page 25](#)
- ♦ [Chapter 3, “Installing Tomcat, PostgreSQL, and ActiveMQ for Identity Governance,” on page 47](#)
- ♦ [Chapter 4, “Installing One SSO Provider,” on page 55](#)
- ♦ [Chapter 5, “Installing Identity Governance,” on page 63](#)
- ♦ [Chapter 6, “Installing Identity Reporting,” on page 83](#)
- ♦ [Chapter 7, “Completing the Installation Process,” on page 97](#)
- ♦ [Chapter 8, “Upgrading Identity Governance,” on page 119](#)
- ♦ [Chapter 9, “Uninstalling Identity Governance,” on page 125](#)

2 Planning to Install Identity Governance

To run the Identity Governance product, you need the following components:



- ♦ Databases for Identity Governance and Identity Reporting
You can use Microsoft SQL Server, PostgreSQL, or Oracle.
- ♦ An application server
Identity Governance requires Apache Tomcat.
- ♦ One SSO Provider (OSP)
- ♦ LDAP authentication server (NetIQ eDirectory or Microsoft Active Directory)
- ♦ (Optional) ActiveMQ
- ♦ (Optional) Identity Reporting
- ♦ (Optional) Audit Server

You can get the components from the [NetIQ Downloads site](#). For your convenience, Apache ActiveMQ, Apache Tomcat and PostgreSQL are bundled in the same installation program. Oracle Java SE Runtime Environment (JRE) is installed if Tomcat, ActiveMQ, or both are installed. If you already have the appropriate versions of PostgreSQL, ActiveMQ and Tomcat, you do not need to install the applications again. For a list of the appropriate versions to use with Identity Governance, see [“Hardware and Software Requirements” on page 41](#).

- ♦ [“Checklist for Installing Identity Governance” on page 25](#)
- ♦ [“Understanding Authentication for Identity Governance” on page 27](#)
- ♦ [“Understanding Password Management in Identity Governance” on page 30](#)
- ♦ [“Understanding Identity Reporting” on page 30](#)
- ♦ [“Understanding the Identity Governance and Reporting Databases” on page 31](#)
- ♦ [“Recommended Installation Scenarios and Server Setup” on page 33](#)
- ♦ [“Prerequisites for Installing Identity Governance” on page 38](#)
- ♦ [“Hardware and Software Requirements” on page 41](#)

Checklist for Installing Identity Governance

Before beginning the installation process, review the following steps and the linked information. Understanding the various components and how they fit in the overall environment helps you make decisions during installation and troubleshoot issues following installation.

	Checklist Items
	1. Learn about the collection, publication, and review process. For more information, see Chapter 1, “Overview,” on page 17 .
	2. Learn about the relationship between the LDAP authentication server and the OSP authentication service. For more information, see “Understanding Authentication for Identity Governance” on page 27 .

	Checklist Items
<input type="checkbox"/>	3. Decide which servers you want to use for your Identity Governance components. For more information, see “Recommended Installation Scenarios and Server Setup” on page 33.
<input type="checkbox"/>	4. (Conditional) To add Identity Governance to an existing Identity Manager environment, review the scenarios. For more information, see “Identity Governance and Identity Manager” on page 34.
<input type="checkbox"/>	5. Decide whether you want to run OSP, ActiveMQ, and Identity Governance in a clustered environment. For more information, see “Ensuring High Availability for Identity Governance” on page 37.
<input type="checkbox"/>	6. Install the Tomcat application server: <ul style="list-style-type: none"> ♦ To review the prerequisites for Tomcat, see “Prerequisites for the Tomcat Application Server” on page 40. ♦ The Tomcat server has the same server requirements as the Identity Governance server. For more information, see “Identity Governance Server System Requirements” on page 41. ♦ To install Tomcat using the convenience installer included with Identity Governance, see Chapter 3, “Installing Tomcat, PostgreSQL, and ActiveMQ for Identity Governance,” on page 47.
<input type="checkbox"/>	7. Install or configure the Identity Governance databases: <ul style="list-style-type: none"> ♦ To learn about the databases, see “Understanding the Identity Governance and Reporting Databases” on page 31. ♦ To review the prerequisites for the databases, see “Prerequisites for the Identity Governance Databases” on page 39. ♦ To review the server requirements for the databases, see “Database Server System Requirements” on page 43. ♦ (Conditional) To use PostgreSQL as the database platform, see Chapter 3, “Installing Tomcat, PostgreSQL, and ActiveMQ for Identity Governance,” on page 47. ♦ (Conditional) To use Oracle as the database platform, see “Preparing an Oracle Database for Identity Governance” on page 67. ♦ (Conditional) To use Microsoft SQL Server as the database platform, see “Preparing an MS SQL Server Database for Identity Governance” on page 70.
<input type="checkbox"/>	8. Install OSP for an authentication service: <ul style="list-style-type: none"> ♦ To review the prerequisites, see “General Prerequisites for Identity Governance” on page 38. <p>The OSP server has the same requirements as the Identity Governance server. For more information, see “Identity Governance Server System Requirements” on page 41.</p> <ul style="list-style-type: none"> ♦ To install the OSP server, see Chapter 4, “Installing One SSO Provider,” on page 55.
<input type="checkbox"/>	9. Install Identity Governance: <ul style="list-style-type: none"> ♦ To review the prerequisites, see “General Prerequisites for Identity Governance” on page 38. ♦ To review the server requirements, see “Identity Governance Server System Requirements” on page 41. ♦ To install the Identity Governance server, see Chapter 5, “Installing Identity Governance,” on page 63.

	Checklist Items
<input type="checkbox"/>	10. (Conditional) Complete the database configuration if you chose Generate SQL for later during installation. For more information, see “Configuring the Databases after Installation” on page 97 .
<input type="checkbox"/>	11. (Conditional) Complete the configuration of the Tomcat cluster: <ul style="list-style-type: none"> ♦ “Configuring the Nodes in the Tomcat Cluster” on page 103 ♦ “Configuring ActiveMQ Failover in the Tomcat Cluster” on page 104
<input type="checkbox"/>	12. (Optional) Install Identity Reporting if you did not install it as part of the Identity Governance installation: <ul style="list-style-type: none"> ♦ To learn about reporting, see “Understanding Identity Reporting” on page 30. ♦ To review the prerequisites, see “Prerequisites for Identity Reporting” on page 40. ♦ To review the server requirements, see “Identity Reporting Server System Requirements” on page 43. ♦ To install Identity Reporting, see Chapter 6, “Installing Identity Reporting,” on page 83.
<input type="checkbox"/>	13. (Optional) Add a valid license key to continue using Identity Governance after the 90-day trial period. For more information, see “Updating the License Key” on page 116 .

Understanding Authentication for Identity Governance

To verify the identity of users who log in to Identity Governance, you need an LDAP authentication server. Identity Governance supports Active Directory and eDirectory. For example, you can use the Identity Vault for Identity Manager as an authentication server. Users can log in to Identity Governance immediately after installation if the users in the specified containers of the authentication server have passwords. Without these login accounts, only the bootstrap administrator can log in immediately.

- ♦ [“Using One SSO Provider for Authentication” on page 27](#)
- ♦ [“Understanding Authentication with One SSO Provider” on page 28](#)
- ♦ [“Understanding the Bootstrap Administrator for Identity Governance” on page 29](#)
- ♦ [“Understanding the Keystore for the Authentication Server” on page 29](#)

Using One SSO Provider for Authentication

Identity Governance uses the One SSO Provider (OSP) authentication service, which supports the OAuth2 specification. With OSP, you can provide single sign-on access among Identity Governance and other applications, such as Identity Manager Home and Provisioning Dashboard. All requests to OSP use the http or https protocols.

NOTE: OSP is always the login mechanism for Identity Governance even in a non-SSO environment.

Understanding Authentication with One SSO Provider

The OSP authentication service supports the OAuth2 specification and requires an LDAP authentication server. Identity Governance works with eDirectory and Microsoft Active Directory. You must create the LDAP server before you install Identity Governance.

You can configure the type of authentication that you want OSP to use: userID and password, Kerberos, or SAML 2.0. However, OSP does not support MIT-style Kerberos or SAP login tickets.

How do OSP and SSO work?

If you use the Identity Vault as your authentication service, users with the CNs and passwords in the specified container can log in to Identity Governance immediately after installation. Without these login accounts, only the administrator that you specify during installation can log in immediately.

When a user directs the browser to one of the browser-based components, the component determines that authentication is required and temporarily redirects the browser to the OSP service. The OSP service authenticates the user, either by asking the user for a name/password or, if so configured, by asking the Kerberos or SAML provider to authenticate the user. OSP then issues an OAuth2 access token and redirects the browser back to the browser-based component. The component uses the token during the user's session to provide SSO access to any of the browser-based components.

How does OSP work with Kerberos?

OSP and Kerberos ensure that users only need to log in once to create a session with Identity Governance and Identity Reporting. If the user's session times out, authorization occurs automatically and without user intervention.

Identity Governance allows you to configure the user logout experience. If the option **Use Logout Landing page** is set to **True**, the user in a Kerberos environment can logout and OSP does not reauthorize the user. The user is presented with the landing page.

If the option is set to **False**, after logging out, users should always close the browser to ensure that their sessions end. Otherwise, the application redirects the user to the login window and OSP reauthorizes the user session.

How does OSP work with SAML?

Using a SAML 2.0 Identity Provider (IDP) with OSP can provide SSO for multiple applications, such as applications beyond just Identity Governance and Identity Manager.

When a browser-based component requests that OSP provide an OAuth2 token to the component, OSP first contacts the SAML IDP to authenticate the user. If the user is not yet authenticated with the IDP, the IDP requires the user to enter credentials. The IDP then responds to OSP that the user is authenticated and the OAuth2 token is issued. If the user is already authenticated with the IDP, the IDP skips the request for the user's credentials.

When the user logs out using a browser-based component, the component first informs OSP of the logout request. OSP then informs the SAML IDP of the logout request. In most cases this will result in the browser displaying the IDP's "logged out" page.

How do I set up authentication and single sign-on access?

For OSP and SSO to function, you must install OSP. Then specify the URLs for client access to each component, the URL that redirects validation requests to OSP, and settings for the authentication server. You can provide this information during installation or afterward with the Identity Governance Configuration Utility, or the Roles Based Provisioning Module (RBPM) configuration utility if you integrate with Identity Manager. You can also specify the settings for your Kerberos ticket server or SAML IDP.

Understanding the Bootstrap Administrator for Identity Governance

During installation, you create a **bootstrap administrator** account that can immediately log in and configure Identity Governance. This account is useful if you do not have an authentication server before installing Identity Governance, and thus do not have any specified login users. The bootstrap administrator can access all items in the administration console, except for **Reviews** and **Access Request**.

The installation process creates a text file that stores the credentials for the bootstrap administrator. The file name is `adminusers.txt`, and places it in the following directory:

- ♦ **Linux:** Default location in `/opt/netiq/idm/apps/idgov/osp`
- ♦ **Windows:** Default location in `c:\netiq\idm\apps\idgov\osp`

IMPORTANT: To ensure system security, it is important that you use this text file, rather than adding this account to your LDAP container.

The bootstrap administrator account does not link to an account for a real person. You should not continue using this account after you have Identity Governance running in a production environment. Instead, as soon as you have collected user accounts, assign one of the collected accounts as a global administrator. For more information about assigning authorizations, see [“Understanding Authorizations in Identity Governance” on page 179](#).

NOTE: The name for the bootstrap administrator 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 provide a password that the Identity Governance service uses for authorized interactions with the authentication server. The installation process assumes that you want to use OSP with an LDAP server. By default, the installation program places the TLS/SSL trust certificates in the `cacerts` keystore file of the Java Runtime Environment (JRE) for the Apache Tomcat instance that hosts OSP. To use SAML 2.0 authentication, you must manually install the SAML Identity Provider's TLS/SSL certificate in the truststore that you want to use. Also, when using a Certificate Authority (CA) to issue certificates for the LDAP server, SAML IDP, or Advanced Authentication Framework servers, you can install the CA's trusted root certificate into the truststore and remove any server-specific certificates. For more information, see [“Prerequisites for One SSO Provider” on page 40](#).

To use a non-default trust store or to change the password of the default trust store, use the Identity Governance Configuration Update utility.

- ♦ **Linux:** `configupdate.sh`
- ♦ **Windows:** `configupdate.bat`

Then modify the keystore settings in the configuration utility. For more information, see [“Running the Identity Governance Configuration Utility” on page 129](#).

Understanding Password Management in Identity Governance

Self Service Password Reset (SSPR) is an optional program that helps users to reset their passwords without administrative intervention. When you run Identity Governance with SSPR in a non-Identity Manager environment, SSPR uses a proprietary protocol for managing authentication methods. However, if you integrate Identity Governance with Identity Manager, you can instruct SSPR to use the NetIQ Modular Authentication Services (NMAS), which Identity Manager has traditionally used for its password management program.

SSPR automatically integrates with OSP, the single sign-on process for Identity Governance and Identity Reporting. It is the default password management program for Identity Manager, even when you do not install SSPR. When a user requests a password reset, SSPR requires the user to answer the challenge-response question. If the answer is correct, SSPR responds in one of the following ways:

- ♦ Allows the user to create a new password
- ♦ Creates a new password and sends it to the user
- ♦ Creates a new password, sends it to the user, and marks the old password as expired

You configure this response in the SSPR Configuration Editor.

The Identity Governance installation package does not include an installation program for SSPR. To install and manage SSPR, see the [Self Service Password Reset 4.2 Administration Guide](#).

Understanding Identity Reporting

Identity Reporting generates a snapshot of the catalog and the state of permissions or reviews. You can use the reports to help meet compliance regulations for your business. You can also create custom reports if the predefined reports do not meet your needs. The user interface for Identity Reporting makes it easy to schedule reports to run at off-peak times for optimized performance.

There are two different versions of Identity Reporting you can install. You can install the version that comes with Identity Governance and it is configured only to run with Identity Governance. This version uses the Identity Governance security module to determine who has access to the reports. Installed this way you can run both Identity Manager and Identity Governance reports by configuring an external data source to where you store the data. However, Identity Reporting cannot be utilized for Data Collection in Identity Manager.

The second version of Identity Reporting ships with Identity Manager. If you already have an Identity Manager environment and you want to utilize Data Collection, you must use this version of Identity Reporting. It uses the Identity Manager security module to determine who has access to the reports. It can run both the Identity Manager and Identity Governance reports by configuring an external data source to where you store the data.

You can also install both versions of Identity Reporting in the Identity Governance environment and in the Identity Manager environment so that each system has its own reporting environment. However, installing Identity Reporting this way, requires that you deploy, configure, and run reports on two different systems. For more information about Identity Reporting, see the [Administrator Guide to NetIQ Identity Reporting](#).

Understanding the Identity Governance and Reporting Databases

Identity Governance and Identity Reporting databases run on Microsoft SQL Server, Oracle, and PostgreSQL platforms. You can have the installation program to do most of the work for building the databases, schemas, tables, and views for each component. For more information, see the following sections:

- ♦ [“Understanding the Identity Governance Databases” on page 31](#)
- ♦ [“Understanding the Identity Reporting Database” on page 33](#)

This section assumes that you intend to use Identity Reporting with Identity Governance in an environment without Identity Manager. For more information about installing and using Identity Reporting in an Identity Manager environment, see:

- ♦ **Linux:** [“Planning to Install Identity Reporting”](#) in the *NetIQ Identity Manager Setup Guide for Linux*.
- ♦ **Windows:** [“Considerations for Installing Identity Manager Components”](#) in the *NetIQ Identity Manager Setup Guide for Windows*.

Understanding the Identity Governance Databases

Identity Governance uses four databases: operations, data collection, workflow, and analytics. By default, these databases are `igops`, `igdc`, `igwf`, and `igara`, respectively. You can establish these databases in the following ways:

- ♦ Have the installation program create the databases, including all schemas, tables, and views.
- ♦ Create the databases before installation. The databases cannot contain any data or tables before installation. They can include the user schemas. The Identity Governance installation program then creates the tables, views, and artifacts in the databases. During installation, ensure that you specify the correct names of your databases.

IMPORTANT

- ♦ For Oracle, you must create the database (SID) before installation, and the installation program can create the schemas, tables, and views for you. Alternatively, you can add the schemas to the database before installing Identity Governance.
 - ♦ For Oracle, Identity Governance supports Pluggable and Container type databases. If you use a Container type database, you must prepend `C##` to the common user name. Identity Governance requires a common user to function, so the user name must start with `C##`.
-
- ♦ Have the installation program generate a SQL file instead of creating schemas, tables, views, and artifacts in the databases. The installation program generates a SQL file for each schema, which your database administrator can run to update the database for Identity Governance. You might use this method if you do not have the credentials for the database administrator.
 - ♦ Ensure that the database runs in the same subnetwork as your Identity Governance server.
 - ♦ Set up schemas and users for the databases, then you can initialize (or reset) the database with the following command:
 - ♦ **Linux:** Default location in `/opt/netiq/idm/apps/idgov/bin`

```
./db-init.sh -password *****
```


- ♦ **Windows:** Default location in c:\netiq\idm\apps\idgov\bin

```
db-init.bat -password *****
```

The command uses Liquibase commands to initialize the database.

Next, you must import (or re-import) the global configuration for Identity Governance to the database.

- ♦ **PostgreSQL:** Use the following command:

```
"/opt/netiq/idm/apps/jre/bin/java" -Djava.util.logging.config.file="/opt/netiq/idm/apps/idgov/conf/logging.properties" -Djava.security.egd=file:///dev/urandom -Dcom.netiq.ism.config="/opt/netiq/idm/apps/idgov/conf/unused.props" -classpath "/opt/netiq/idm/apps/idgov/lib/igconfigutil.jar":"/opt/netiq/idm/apps/idgov/lib/ojdbc.jar" com.netiq.iac.config.util.IacConfigUtil -dbDriver oracle.jdbc.OracleDriver -dbUser %igops-user% -dbPassword %password% -dbUrl "jdbc:oracle:thin:@%oracle-server%:%port%/%sid%" -script "/opt/netiq/idm/apps/idgov/scripts/all-import-configs.script"
```

- ♦ **Oracle:** Use the following command:

```
"/opt/netiq/idm/apps/jre/bin/java" -Djava.util.logging.config.file="/opt/netiq/idm/apps/idgov/conf/logging.properties" -Djava.security.egd=file:///dev/urandom -Dcom.netiq.ism.config="/opt/netiq/idm/apps/idgov/conf/unused.props" -classpath "/opt/netiq/idm/apps/idgov/lib/igconfigutil.jar":"/opt/netiq/idm/apps/idgov/lib/ojdbc.jar" com.netiq.iac.config.util.IacConfigUtil -dbDriver oracle.jdbc.OracleDriver -dbUser %igops-user% -dbPassword %password% -dbUrl "jdbc:oracle:thin:@%oracle-server%:%port%/%sid%" -script "/opt/netiq/idm/apps/idgov/scripts/all-import-configs.script"
```

NOTE: This commands contains the default installation path of /opt/netiq/idm/apps.

- ♦ **MS SQL:** Use the following commands:

```
"/opt/netiq/idm/apps/jre/bin/java" -Djava.util.logging.config.file="/opt/netiq/idm/apps/idgov/conf/logging.properties" -Dcom.netiq.ism.config="/opt/netiq/idm/apps/idgov/conf/unused.props" -classpath "/opt/netiq/idm/apps/idgov/lib/ig-configutil.jar":"/opt/netiq/idm/apps/idgov/lib/msjdbc.jar" com.netiq.iac.config.util.IacConfigUtil -dbDriver com.microsoft.sqlserver.jdbc.SQLServerDriver -dbUser igops -dbPassword %igops-password% -dbUrl "jdbc:sqlserver://%server%:%port%;databaseName=igops" -script "/opt/netiq/idm/apps/idgov/scripts/all-import-configs.script"
```

For more information about preparing and configuring the databases, see the following sections:

- ♦ [“Preparing an MS SQL Server Database for Identity Governance” on page 70](#)
- ♦ [“Preparing an Oracle Database for Identity Governance” on page 67](#)
- ♦ [“Preparing a PostgreSQL Database for Identity Governance” on page 65](#)
- ♦ [“Configuring the Databases after Installation” on page 97](#)

Understanding the Identity Reporting Database

Identity Reporting uses one database. It is important that you allow the installation program for Identity Governance to create the schema, tables, and views for the PostgreSQL database. For Oracle, you must create the database (SID) in AL32UTF-8 (Unicode UTF-8 Universal character set) before installing Identity Reporting.

The Identity Reporting database must run in the same subnetwork as your Identity Governance server. You can establish the Identity Reporting database in the same way as you do for the Identity Governance database. For more information, see [“Understanding the Identity Governance Databases” on page 31](#).

Recommended Installation Scenarios and Server Setup

You can install Identity Governance in many different configurations, depending on network topology and the identity management products with which it will integrate. Regardless of installation scenario, Identity Governance incorporates the following components:

- ♦ ActiveMQ
- ♦ Tomcat application server
- ♦ Microsoft SQL Server, Oracle, or PostgreSQL database (must be on the same subnetwork as the Identity Governance server)
- ♦ OSP
- ♦ (Optional) SSPR
- ♦ (Optional) Identity Reporting

This section presents a few common installation scenarios and recommendations to inform your installation choices:

- ♦ [“Identity Governance in a New Environment” on page 33](#)
- ♦ [“Identity Governance and Identity Manager” on page 34](#)
- ♦ [“Identity Governance and Existing Components” on page 34](#)
- ♦ [“Component Installation Order” on page 35](#)
- ♦ [“Recommended Server Setup” on page 35](#)
- ♦ [“Selecting an Operating System Platform for Identity Governance” on page 36](#)
- ♦ [“Ensuring High Availability for Identity Governance” on page 37](#)

Identity Governance in a New Environment

The Identity Governance installer installs the different required components if you do not have any or all of them in your environment. The Identity Governance installer includes an installer for Identity Reporting. In addition to the Identity Governance installer, the software download web page provides installers for ActiveMQ, Tomcat web server, PostgreSQL server, and OSP.

For best performance, do not install Identity Governance on the same server the databases, however, ensure that the databases and Identity Governance run in the same subnetwork. Also, you must ensure that the database include the supported versions of Java and the Tomcat application server.

It is important that you review all the prerequisites, requirements, and installation procedures in this chapter. Also, review the following topics as you prepare to install the Identity Governance components in a new environment:

- ♦ [“Component Installation Order” on page 35](#)
- ♦ [“Recommended Server Setup” on page 35](#)

Identity Governance and Identity Manager

To integrate Identity Governance with Identity Manager Advanced Edition, you can use some of the components that you installed with Identity Manager: OSP, SSPR, and Identity Reporting. The Identity Governance installation program will need the accounts and permissions to access, configure, and modify the existing Identity Manager components.

If you want to use Identity Reporting as part of your Identity Governance solution, but you already have Identity Manager installed and running, you must install the version Identity Reporting that comes with Identity Manager. Identity Reporting that comes with Identity Manager utilizes the Identity Manager security module to determine who has access the reports.

You will also need to perform the following tasks:

- ♦ Update the `configupdate.sh` or `configupdate.bat` file to include a configuration variable for the Tomcat server
- ♦ Create the databases for Identity Governance
- ♦ Integrate OSP to define and provision Identity Governance user accounts
- ♦ (Optional) Integrate with Identity Reporting

For more information about these activities, see [Chapter 14, “Integrating Single Sign-on Access with Identity Manager,” on page 187](#) and [Chapter 6, “Installing Identity Reporting,” on page 83](#).

It is important that you review the prerequisites and requirements for Identity Governance and gather the server and account information necessary to complete the installation process. For more information, see the following:

- ♦ [“General Prerequisites for Identity Governance” on page 38](#)
- ♦ [“Prerequisites for the Identity Governance Databases” on page 39](#)
- ♦ [“Identity Governance Server System Requirements” on page 41](#)
- ♦ [“Database Server System Requirements” on page 43](#)
- ♦ [Chapter 5, “Installing Identity Governance,” on page 63](#)

Identity Governance and Existing Components

If you are installing Identity Governance into an environment that already has a supported version of Tomcat, PostgreSQL, and ActiveMQ, you can use those components. Ensure that you review the prerequisites and requirements provided in this chapter for each existing component. You should also consider the following:

- ♦ Availability and suitability of existing components for Identity Governance use, including capacity, throughput, and utilization.
- ♦ Additional processing load Identity Governance can place on existing components.
- ♦ Resources needed to host Identity Governance components you must install in the environment.
- ♦ OWASP best practices for securing your Tomcat environment at https://www.owasp.org/index.php/Securing_tomcat.

Component Installation Order

You must install the Identity Governance components in a specific order, which depends on whether you plan to integrate Identity Governance with Identity Manager.

- ♦ [“Using Identity Governance without Identity Manager” on page 35](#)
- ♦ [“Using Identity Governance with Identity Manager” on page 35](#)

Using Identity Governance without Identity Manager

To use Identity Governance without integrating with Identity Manager Advanced Edition, install the components in the following order:

1. (Conditional) LDAP authentication server with admin and user containers

To use an authentication server for the data source, ensure that you have Active Directory or eDirectory already installed.

2. Database and Tomcat

NOTE

- ♦ You must install Identity Governance on a Tomcat application server. For your convenience, there is an installation program for Tomcat. Alternatively, you can use your installation of Tomcat if it is a version supported by Identity Governance.
 - ♦ For your convenience, there is an installation program for PostgreSQL. Alternatively, you can use your installation of MS SQL Server, Oracle, or PostgreSQL if it is a version supported by Identity Governance.
-

3. OSP
4. (Optional) SSPR
5. Identity Governance and Identity Reporting
6. (Optional) Identity Reporting, if not installed at the same time as Identity Governance

Using Identity Governance with Identity Manager

To use Identity Governance with Identity Manager Advanced Edition, install the components in the following order:

1. Identity Manager Advanced Edition
2. Identity Governance

You can install Identity Reporting as part of the Identity Manager installation or after installing Identity Governance.

Recommended Server Setup

In a typical production environment, you might install Identity Governance components on three or more servers, as well as on client workstations.

The following table provides examples for an Identity Governance setup.

	Case 1	Case 2	Case 3	Case 4
Server 1	(can be clustered) OSP SSPR Identity Governance	(can be clustered) OSP Identity Governance Identity Reporting	(can be clustered) OSP Identity Governance	(can be clustered) OSP
Server 2	(can be clustered) Identity Reporting	(can be clustered) SSPR	(can be clustered) Identity Reporting	(can be clustered) Identity Governance
Server 3	Database server	Database server	SSPR	(can be clustered) Identity Governance
Server 4	Authentication server	Authentication server	Database server	Identity Reporting
Server 5			Authentication server	SSPR
Server 6				Database server
Server 7				Authentication server
Server 8	Audit server	Audit server	Audit server	Audit server

Selecting an Operating System Platform for Identity Governance

You can install Identity Governance components on a variety of operating system platforms. The following table helps you determine which servers you might want to use for your Identity Governance components. For more information about supported operating system versions, see [“Hardware and Software Requirements” on page 41](#).

Platform	Component
Red Hat Enterprise Linux (RHEL), SUSE Linux Enterprise Server (SLES) Windows Server	Identity Governance Identity Reporting One SSO Provider ActiveMQ Self Service Password Reset Tomcat Browser access to Identity Governance
Windows desktop	Browser access to Identity Governance Browser access to Identity Reporting

See the audit server documentation for supported platforms. Identity Governance supports the following auditing servers:

- ♦ NetIQ Sentinel

- ♦ ArcSight
- ♦ Splunk

Ensuring High Availability for Identity Governance

High availability ensures efficient manageability of critical network resources including data, applications, and services. Identity Governance supports high availability through stateless clustering or Hypervisor clustering, such as VMware Vmotion. When planning a high-availability environment, the following considerations apply:

- ♦ To manage the availability of your network resources for Identity Governance, use the SUSE Linux Enterprise High Availability Extension with SUSE Linux Enterprise Server (SLES) 12 with the latest patches installed.
- ♦ You can run Identity Governance in a stateless cluster where the load balancers shift authentication requests among the various OSP servers. During installation, you must specify a URL that drives client access through your L4 switch or load balancer rather than specifying the hostname and port for the Tomcat server.
- ♦ Each node in the cluster must have a unique `runtime_identifier`. For example, `node1` or `ProdNode1`. For more information, see [“Configuring the Nodes in the Tomcat Cluster” on page 103](#).

Each Identity Governance runtime uses this identifier to claim and identify tasks that it processes. Some of these tasks are long-running, so the identifier should be able to remain unique after a restart of the environment, where an IP address or other identifier might not be guaranteed to remain the same.

- ♦ The configuration settings for OSP and Identity Governance must be identical for all nodes in the cluster.
- ♦ When installing OSP, consider the following requirements:
 - ♦ Configure a load balancer with a DNS host name and port for the authentication server (OSP server).
The OSP server can use the same load balancer specified for Identity Governance, a dedicated load balancer, or a single Tomcat instance.
 - ♦ Specifying the values for the appropriate load balancer instead of the connection settings to the Tomcat instance. For more information, see [Application address](#) in [Step 6 on page 56](#).
 - ♦ The `osp.war` and configuration files must be on each deployment of OSP in the environment. Use the same Keystore file for all deployments. For more information, see [Chapter 4, “Installing One SSO Provider,” on page 55](#).
- ♦ When installing Identity Governance, consider the following requirements:
 - ♦ Configure a load balancer with a DNS host name and port for Identity Governance use.
Identity Governance can use a dedicated load balancer or the same load balancer as for the OSP server.
 - ♦ Specify the values for the load balancer instead of the host and port for the Tomcat connection. For more information, see [Application address](#) in [Step 7 on page 73](#).
 - ♦ On the primary (or master) node, perform the steps for configuring the databases. For more information, see [Database details](#) in [Step 7 on page 73](#).
 - ♦ For each installation on a secondary node, do not perform any database configuration steps. Instead, specify the settings for connecting to the previously configured databases. For more information, see [Database details](#) in [Step 7 on page 73](#).

- ♦ To silently install OSP and Identity Governance on the secondary nodes in the cluster, use the content from the installation log files. The log files are:
 - ♦ `Identity_Governance_InstallLog.log`
 - ♦ `osp_install_log.log`

For more information, see [“Creating a Silent Properties File for Installing on a Secondary Node” on page 59](#).

For each component, copy the parameter values from the log to the `silent.properties` file.

NOTE: In the `silent.properties` file for Identity Governance, change the following settings:

- ♦ `install.db.configure=false`
 - ♦ `install.tomcat.runtime.id=`
-

Prerequisites for Installing Identity Governance

Before installing Identity Governance, it is important that you review the prerequisites and considerations.

- ♦ [“General Prerequisites for Identity Governance” on page 38](#)
- ♦ [“Prerequisites for the Identity Governance Databases” on page 39](#)
- ♦ [“Prerequisites for the Tomcat Application Server” on page 40](#)
- ♦ [“Prerequisites for One SSO Provider” on page 40](#)
- ♦ [“Prerequisites for Identity Reporting” on page 40](#)

General Prerequisites for Identity Governance

- ♦ You can install Identity Governance and OSP in a stateless cluster. For more information about the installation requirements, see [“Ensuring High Availability for Identity Governance” on page 37](#).
- ♦ For best performance, do not install Identity Governance on the same server as its databases. However, the Identity Governance server should include the supported versions of Java, and Tomcat application server.
- ♦ Do not install Identity Governance or its database on a server that is already running components for Identity Manager. For example, do not install on the same server as Identity Manager Home and Provisioning Dashboard.
- ♦ You must use Latin-1 characters in the installation path.
- ♦ Do not use mixed case domains. Identity Governance utilizes OAuth for authentication. OAuth does not support mixed case domains. For more information, see [“RCF 3986 Section 6.2.1 Simple String Comparison”](#).
- ♦ To use an authentication server as your data source for Identity Governance users, ensure that you have Active Directory or eDirectory already installed. For more information, see [“Adding Identity Governance Users” on page 184](#).
- ♦ When you point to the installation directory for Java, it must be a supported Oracle Java instance used by the Tomcat server. The application does not work with IBM Java.
- ♦ Ensure that the communication ports that you want to use are open in the firewall.
- ♦ To integrate Identity Governance with Identity Manager, the Identity Manager component must already be installed and configured with OSP.

- ♦ To use TLS auditing, the audit server should be up and running when you install Identity Governance so that the installer can connect to the audit server and retrieve the certificate to add to the keystore.
- ♦ Before installing Identity Governance, you need the following information:
 - ♦ Paths to your Apache Tomcat and Java directories.
 - ♦ Credentials of a database administrator (DBA) account that can access and modify data in the databases to 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 configure the databases.

- ♦ IP address or DNS host name and port of your Identity Governance server. Login users will use this information in the URL for Identity Governance.
- ♦ (Conditional) When using an LDAP authentication server, you need the following information:
 - ♦ Credentials of an administrator account for the server.
 - ♦ The container in the server where you store administrator accounts.
 - ♦ The container in the server where you store the accounts for users who can log in to Identity Governance.
- ♦ (Conditional) To use an Identity Manager authentication server, you must have the DN, password, user container, and admin container of an administrator account for the server.
- ♦ (Conditional) To use an Identity Manager authentication server or TLS auditing, you must have the keystore password for the server.
- ♦ For best performance, do not install Identity Governance on the database server, however, the database server and the Identity Governance server must run in the same subnetwork. Also, ensure that the database is running the supported versions of Java and the Tomcat application server.
- ♦ IP address or DNS host name and port of your database server.
- ♦ IP address or DNS host name and port of your ActiveMQ server. If it is installed on a separate server.

Prerequisites for the Identity Governance Databases

Review the following considerations before installing Identity Governance:

- ♦ For best performance, do not install Identity Governance on the database server, however, the database server and the Identity Governance server must run in the same subnetwork. Also, ensure that the database is running the supported versions of Java and the Tomcat application server.
- ♦ You can install the version of PostgreSQL bundled with Identity Governance in an environment that runs an older version of the database program. To ensure that the new installation does not overwrite the previous version, specify a different directory for the files.
- ♦ (Conditional) To use an Oracle database with Identity Governance, you must install the database with the Identity Governance admin user for the database before installing Identity Governance. For more information, see [Section 7, “Completing the Installation Process,” on page 97](#).
- ♦ (Conditional) To install the databases in a clustered environment, see [“Ensuring High Availability for Identity Governance” on page 37](#).

Prerequisites for the Tomcat Application Server

Review the following considerations before installing Tomcat:

- ♦ We highly recommend that you configure Tomcat to use https with either TLSv1.2 or TLS1.1. Any prior version of TLS should not be used. For more information, see [“Securing Tomcat”](#).
- ♦ You can install Tomcat, PostgreSQL, and ActiveMQ on the same server or on separate servers.
- ♦ If selected, the installation process installs supported version of Apache ActiveMQ
- ♦ If Tomcat or ActiveMQ is installed, the Oracle JRE is automatically included.
- ♦ You can use your own Tomcat installation program instead of the one provided in the Identity Governance installation kit.
- ♦ To use ActiveMQ, which guarantees that notifications are sent using SMTP, install MQServer.
- ♦ The installation process sets the JRE location in the `setenv.sh` file.
 - ♦ **Linux:** Default location in `/opt/netiq/idm/apps/tomcat/bin/`
 - ♦ **Windows:** Default location in `c:\netiq\idm\apps\tomcat\bin\`
- ♦ (Conditional) If you use Linux, do not run Tomcat as `root`. The installation process creates a user account for the Tomcat service, which should not be `root`.

Prerequisites for One SSO Provider

Before installing OSP, it is important that you review the following considerations:

- ♦ (Conditional) Even if you installed OSP with Identity Manager 4.5 or later, you must install OSP with Identity Governance.
- ♦ (Conditional) OSP requires trust certificates configured for secure communication for user authentication in a production environment. Depending on your Identity Governance solution, OSP might need to communicate with an authentication server, a SAML provider, or one or more Advanced Authentication Framework servers. For more information, see [“Understanding the Keystore for the Authentication Server” on page 29](#).
- ♦ OSP requires a public/private key pair for use during normal operations to generate other key material. The installation program automatically creates the keypair and places it in the `osp.jks` file.
- ♦ (Conditional) If you set up multiple instances of OSP for use in a high availability cluster, copy the `osp.jks` file from the installed location on the first server to the same location on the other member servers in the cluster. OSP must use the same key material.

Prerequisites for Identity Reporting

It is important that you review the following prerequisites and considerations before starting the installation process.

When installing Identity Reporting, consider the following prerequisites and considerations:

- ♦ This guide provides information about installing Identity Reporting for use with Identity Governance only. If you have already installed Identity Reporting with Identity Manager 4.5 or later, you might not need to install it again for Identity Governance. Ensure that you have the

appropriate version of Identity Reporting. For more information, see the [NetIQ Identity Governance 3.0.1 Release Notes](#). For more information about installing with Identity Manager, see:

- ♦ **Linux:** “Planning to Install Identity Reporting” in the [NetIQ Identity Manager Setup Guide for Linux](#).
- ♦ **Windows:** “Considerations for Installing Identity Manager Components ” in the [NetIQ Identity Manager Setup Guide for Windows](#).
- ♦ You can install Identity Reporting on the same server as Identity Governance, and the two products use the same Tomcat instance, or you can install it on a separate server running Tomcat.
- ♦ (Conditional) To run reports against a Microsoft SQL Server database, you must install the appropriate JDBC file. For example, `sqljdbc42.jar`.
- ♦ (Conditional) To run reports against an Oracle 12c database, you must install the appropriate JDBC file. For example, `ojdbc7.jar`.
- ♦ Assign the Report Administrator authorization to any users that you want to be able to access reporting functionality.
- ♦ Ensure that all servers in your Identity Governance environment are set to the same time, particularly the servers for the database and events auditing components. If you do not synchronize the time on your servers, some reports might be empty when executed. For example, this issue can affect data related to new users when the servers hosting Identity Governance and the reporting databases have different time stamps.

Hardware and Software Requirements

It is important that you review the hardware and software requirements for the servers and devices for use with Identity Governance.

- ♦ “Identity Governance Server System Requirements” on page 41
- ♦ “Database Server System Requirements” on page 43
- ♦ “Identity Reporting Server System Requirements” on page 43
- ♦ “Identity Governance and Reporting Browser Requirements” on page 44
- ♦ “Auditing Server System Requirements” on page 45

Identity Governance Server System Requirements

This section provides the minimum requirements for the server(s) where you want to install Identity Governance.

These system requirements provide server settings according to the size of your Identity Governance catalog. In a small catalog, you might collect fewer than 100,000 identities with 100,000 permissions and 80,000 groups.

If you are running virtual machines, set up the VM as Thick Provisioned.

Category	Minimum Requirement
Processor	<ul style="list-style-type: none">♦ 4.0 GHz, single processor (small catalog)♦ 8.0 GHz, single processor

Category	Minimum Requirement
Disk Space	50 GB
Memory	<ul style="list-style-type: none"> ◆ 16 GB (small catalog) ◆ 32 GB
Operating System	<ul style="list-style-type: none"> ◆ Red Hat Enterprise Linux 7.4 (64-bit) ◆ SUSE Linux Enterprise Server 12 SP3 (64-bit) ◆ Microsoft Windows Server 2012 R2 (64-bit) ◆ Microsoft Windows Server 2016 (64-bit) <p>IMPORTANT: Before installing Identity Governance, apply the latest operating system patches.</p>
Java	Oracle Java 2 Platform Standard Edition Development Kit 8 (jdk8u152) or Java Runtime Environment 8 (jre8u152)
Application Server	<p>Apache Tomcat 8.5.23</p> <p>NOTE: (Conditional) For guaranteed delivery of email notifications, your application server must include support for Apache ActiveMQ Java Message Service (JMS) and clustering.</p>
LDAP Authentication Server	<ul style="list-style-type: none"> ◆ Microsoft Active Directory ◆ NetIQ eDirectory 9.0 Service Pack 3 ◆ NetIQ Identity Manager 4.6
Third-Party Connector Libraries	<p>(Optional) The Identity Governance JDBC Collectors and SAP User Management Collector use third-party client connector software that is not distributed with the product.</p> <ul style="list-style-type: none"> ◆ DB2: <code>com.ibm.db2.jcc.DB2Driver</code> ◆ Generic JTDS: <code>net.sourceforge.jtds.jdbc.Driver</code> ◆ Microsoft SQL Server: <code>com.microsoft.sqlserver.jdbc.SQLServerDriver</code> ◆ MySQL: <code>com.mysql.jdbc.Driver</code> ◆ Oracle Thin Client: <code>oracle.jdbc.driver.OracleDriver</code> ◆ PostgreSQL: <code>org.postgresql.Driver</code> ◆ SAP: <code>sapjco3.jar</code> <p>NOTE: Ensure that all required SAP Java Connector Native library components are installed on the host system. For more information, refer to the vendor documentation.</p> <ul style="list-style-type: none"> ◆ Sybase: <code>com.sybase.jdbc3.jdbc.SybDriver</code> <p>To gather identity and application data from one of these sources, put one or more of the these client <code>jar</code> files into the Apache Tomcat <code>/lib</code> folder, then restart the Tomcat server.</p> <ul style="list-style-type: none"> ◆ Linux: Default location of Apache Tomcat is <code>/opt/netiq/idm/apps/tomcat</code> ◆ Windows: Default location of Apache Tomcat is <code>c:\netiq\idm\apps\tomcat</code>

Category	Minimum Requirement
Additional Software	(Optional) Apache ActiveMQ 5.15.1, which guarantees that notifications are sent using SMTP

Database Server System Requirements

This section provides the minimum requirements for the server where you want to install the databases for Identity Governance.

These system requirements provide server settings according to the size of your Identity Governance catalog. In a small catalog, you might collect fewer than 100,000 identities with 100,000 permissions and 80,000 groups.

On a virtual machine, set up the VM as Thick Provisioned.

Category	Minimum Requirement
Processor	<ul style="list-style-type: none"> ◆ 4.0 GHz, single processor (small catalog) ◆ 8.0 GHz, single processor
Disk Space	<ul style="list-style-type: none"> ◆ 60 GB (small catalog) ◆ 100 GB
Memory	<ul style="list-style-type: none"> ◆ 16 GB (small catalog) ◆ 32 GB
Operating System	<ul style="list-style-type: none"> ◆ Red Hat Enterprise Linux 7.4 (64-bit) ◆ SUSE Linux Enterprise Server 12 SP3 (64-bit) ◆ Microsoft Windows Server 2012 R2 (64-bit) ◆ Microsoft Windows Server 2016 (64-bit) <p>IMPORTANT: Before installing Identity Governance, apply the latest operating system patches.</p>
Database	<p>One of the following:</p> <ul style="list-style-type: none"> ◆ Microsoft SQL Server 2016 SP1 with JDBC driver 6.0 (<code>sqljdbc42.jar</code> for jre8) ◆ Oracle 12c SP2 with JDBC driver <code>ojdbc7.jar</code> <p>NOTE: If using Oracle 12c SP2, Identity Governance requires that you install all patches available from Oracle.</p> <ul style="list-style-type: none"> ◆ PostgreSQL 9.6.5 with JDBC driver <code>postgresql-42.1.4.jar</code>

Identity Reporting Server System Requirements

This section lists the requirements for the server that hosts Identity Reporting when installed only for Identity Governance. For more information about whether to install the components on the same server, see [“Recommended Installation Scenarios and Server Setup” on page 33](#). For more information about the system requirements for installing in an Identity Manager environment that includes Identity Governance, see:

- ◆ **Linux:** [“Auditing and Reporting Guidelines”](#) in the *NetIQ Identity Manager Setup Guide for Linux*.

- ♦ **Windows:** “[Considerations for Installing Identity Manager Components](#)” in the *NetIQ Identity Manager Setup Guide for Windows*.

Category	Minimum Requirement
Processor	Pentium 4
Disk Space	50 GB
Memory	16 GB
Operating System	<ul style="list-style-type: none"> ♦ Red Hat Enterprise Linux 7.4 (64-bit) ♦ SUSE Linux Enterprise Server 12 SP3 (64-bit) ♦ Microsoft Windows Server 2012 R2 (64-bit) ♦ Microsoft Windows Server 2016 (64-bit) <p>IMPORTANT: Before installing Identity Governance, apply the latest operating system patches.</p>
Virtualization Systems	<p>VMWare ESX 6.5 U1</p> <p>IMPORTANT: NetIQ supports Identity Reporting on enterprise-class virtualization systems that provide official support for the operating systems where NetIQ products are running. As long as the vendors of the virtualization systems officially support these operating systems, NetIQ supports the Identity Reporting stack on them.</p>
Application Server	Apache Tomcat 8.5.23
Java	Tomcat: Java Development Kit 8 (jdk8u152) or Java Runtime Environment 8 (jre8u152) from Sun (Oracle)
Databases	<p>Identity Reporting database runs on the following platforms:</p> <ul style="list-style-type: none"> ♦ Microsoft SQL Server 2016 SP 1 ♦ Oracle 12c <p>NOTE: If using Oracle 12c SP 2, Identity Governance requires that you install all patches available from Oracle.</p> <ul style="list-style-type: none"> ♦ PostgreSQL 9.6.5 <p>You can run reports against the following databases:</p> <ul style="list-style-type: none"> ♦ Microsoft SQL Server 2016 SP 1 ♦ Oracle 12c ♦ PostgreSQL 9.6.5

Identity Governance and Reporting Browser Requirements

To log in to Identity Governance on their local devices, users must have one of the following browser versions, at a minimum:

Computers

- ♦ Apple Safari 11.0.1 (12604.3.5.1.1)
- ♦ Google Chrome 62.0.3202.94
- ♦ Microsoft Edge Browser 40.15063.674.0
- ♦ Microsoft Internet Explorer 11.608.15063.0

- ♦ Mozilla Firefox 62.0.3202.94
- ♦ Mozilla Firefox (Mac) 57

iPad (iOS 10.3.3)

- ♦ Safari 10.0
- ♦ Chrome 62.0.3202.70
- ♦ Firefox 10.3

NOTE: The browser must have cookies enabled. If cookies are disabled, the product does not work.

Auditing Server System Requirements

This section provides the minimum requirements for the server where you want to send audit events from Identity Governance. The following audit servers using sysloger are certified for use with Identity Governance:

- ♦ Splunk 6.6.3 (build e21ee54bc796)
- ♦ ArcSight ESM Suite-6.11.0.2149.0
- ♦ Sentinel 8.0.0.1_3404

3 Installing Tomcat, PostgreSQL, and ActiveMQ for Identity Governance

For your convenience, Apache Tomcat, PostgreSQL, and Apache ActiveMQ are bundled in the same installation program and available on the Identity Governance download site. If your company does not already provide an application server and a database server, you can use this convenience installer to install an Open Source version of these components. This installer provides a Java JRE from Oracle, open source versions of Apache Tomcat web server, ActiveMQ, and PostgreSQL database server as a basis for Identity Governance.

NOTE: To use a Microsoft SQL Server database, install Tomcat, then continue to [“Preparing an MS SQL Server Database for Identity Governance” on page 70.](#)

To use an Oracle database, install Tomcat, then continue to [“Preparing an Oracle Database for Identity Governance” on page 67.](#)

This installer lets you install these applications without downloading them separately. It is important to use an enterprise application server for staging and production environments, and create a development environment by using this convenience installer. If you need applications support, go to the provider of the component. Identity Governance does not provide updates for these components, or administration, configuration, or tuning information beyond what it is outlined in the Identity Governance documentation.

By default, the installation program installs the applications in the following directories:

- ♦ **Linux:** Default location of `/opt/netiq/idm/apps/`
- ♦ **Windows:** Default location of `C:\netiq\idm\apps\`

It is important that you review the installation process before beginning:

- ♦ [“Checklist for Installing Tomcat, PostgreSQL, and ActiveMQ” on page 48](#)
- ♦ [“Using the Wizard to Install Tomcat, PostgreSQL, and ActiveMQ” on page 48](#)
- ♦ [“Silently Installing Tomcat, PostgreSQL, and ActiveMQ” on page 51](#)
- ♦ [“Stopping, Starting, and Restarting Tomcat” on page 52](#)
- ♦ [“Stopping, Starting, and Restarting ActiveMQ” on page 53](#)

Checklist for Installing Tomcat, PostgreSQL, and ActiveMQ

It is important to complete the steps in the following checklist:

	Checklist Items
<input type="checkbox"/>	1. Learn about the interaction among Identity Governance components. For more information, see the following sections: <ul style="list-style-type: none">♦ “Understanding Authentication for Identity Governance” on page 27♦ “Understanding Password Management in Identity Governance” on page 30
<input type="checkbox"/>	2. Decide which servers you want to use for your Identity Governance components. For more information, see “Recommended Server Setup” on page 35 .
<input type="checkbox"/>	3. Review the considerations for installing the applications to ensure that the computers meet the requirements: <ul style="list-style-type: none">♦ “Prerequisites for the Tomcat Application Server” on page 40♦ “Prerequisites for the Identity Governance Databases” on page 39
<input type="checkbox"/>	4. Install supported versions of Tomcat, PostgreSQL, and ActiveMQ. If using the convenience installer from the Identity Governance download site: <ul style="list-style-type: none">♦ For a guided installation, see “Using the Wizard to Install Tomcat, PostgreSQL, and ActiveMQ” on page 48.♦ For a silent installation, see “Silently Installing Tomcat, PostgreSQL, and ActiveMQ” on page 51.
<input type="checkbox"/>	5. (Conditional) To use a Microsoft SQL Server or Oracle database, see one of the following sections: <ul style="list-style-type: none">♦ “Preparing an MS SQL Server Database for Identity Governance” on page 70♦ “Preparing an Oracle Database for Identity Governance” on page 67
<input type="checkbox"/>	6. Install the rest of the Identity Governance components.

Using the Wizard to Install Tomcat, PostgreSQL, and ActiveMQ

The following procedure describes how to install Tomcat, PostgreSQL, and ActiveMQ using a guided process, either in the GUI format or from the console. To prepare for the installation, review the considerations and system requirements listed in the following sections:

- ♦ [“Prerequisites for the Tomcat Application Server” on page 40](#)
- ♦ [“Database Server System Requirements” on page 43](#)
- ♦ [NetIQ Identity Governance 3.0.1 Release Notes](#)

To perform a silent, unattended installation, see [“Silently Installing Tomcat, PostgreSQL, and ActiveMQ” on page 51](#).

To perform a guided installation:

- 1 Log in as `root` on Linux server or an administrator on Windows server where you want to install the applications.
- 2 Ensure that the planned installation path does not include directories with any of the following names:
 - ♦ `tomcat`
 - ♦ `postgres`
 - ♦ `activemq`
 - ♦ `jre`

For example, if you want to add this version of Postgres to a server while keeping a previous version of Postgres, create an installation path separate from the other version.

- 3 From the directory that contains the installation files, complete one of the following actions:
 - ♦ **Linux (console):** Enter `./TomcatPostgreSQL.bin -i console`
 - ♦ **Linux (GUI):** Enter `./TomcatPostgreSQL.bin`
 - ♦ **Windows (console):** Enter `cmd /c "TomcatPostgreSQL.exe -i console"`
 - ♦ **Windows (GUI):** Double-click `TomcatPostgreSQL.exe`

NOTE: To execute the file, you might need to use the `chmod +x` or `sh` command for Linux or log in to your Windows server as an administrator.

- 4 Review the introductory information, and then select **Next**.
- 5 Accept the License Agreement, and then select **Next**.
- 6 Specify the components that you want to install: Tomcat, PostgreSQL, and ActiveMQ.
- 7 To complete the guided process, specify values for the following parameters:

- ♦ **Tomcat install folder**

Applies only when installing Tomcat.

Specifies the parent directory where you want to install the Tomcat files.

- ♦ **Tomcat details**

Applies only when installing Tomcat.

Specifies the ports needed for running Tomcat.

Tomcat shutdown port

Specifies the port that you want to use for cleanly shutting down all web applications and Tomcat. The default is 8005.

Tomcat http port

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

NOTE: By default on Linux, a non-root user cannot open a port under 1024. NetIQ recommends running Tomcat as non-root. Therefore, if you change the port from the default, you should use a port above 1024.

Tomcat redirect port

(Conditional) When you do not use TLS/SSL protocols, specifies the port to which the application server redirects requests that require SSL transport. The default value is 8443. For more information, see [SSL/TLS Configuration HOW-TO](#) in the Tomcat documentation.

Tomcat ajp port

(Optional) Specifies the port that you want the application server to use for communication with a web connector using the AJP protocol instead of `http`. The default value is 8009.

Use this parameter when you want the application server to manage the static content contained in the web application, and/or utilize the application server's SSL processing.

- ◆ **ActiveMQ install folder**

Applies only when installing ActiveMQ.

Specifies the parent directory where you want to install the ActiveMQ files.

- ◆ **PostgreSQL install folder**

Applies only when installing PostgreSQL.

Specifies the parent directory where you want to install the PostgreSQL files.

- ◆ **PostgreSQL details**

Applies only when installing PostgreSQL.

Specifies the settings for the PostgreSQL database for the identity applications.

NOTE: If you already have a supported version of PostgreSQL running on the server, the installation program prompts you for the password for the default `postgres` user. The program then creates the database admin user and assigns it the same password as for `postgres`.

Password for postgres user

Specifies the password for the default `postgres` user and database login account, if created.

PostgreSQL port

Specifies the port of the server that hosts the Postgres database. The default value is 5432.

Login account

*Applies only when you select **Create database login account**.*

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

The default value is `idmadmin`, which corresponds with the default database administrator for the identity applications component of Identity Manager.

This account is not the same as the default `postgres` user.

Database name

*Applies only when you select **Create empty database**.*

Specifies the name of the database.

The default value is `idmuserappdb`, which corresponds with the default database for the identity applications component of Identity Manager.

8 Review the pre-installation summary.

- 9 Start the installation process.
- 10 When the installation process completes, select **Done**.

Silently Installing Tomcat, PostgreSQL, and ActiveMQ

A silent (non-interactive) installation does not display a user interface or ask the user any questions. Instead, InstallAnywhere uses information from the `TomcatPostgreSQL-install-silent.properties` file. To run the silent installation, you must edit the file for your environment.

To prepare for the installation, review the considerations and system requirements listed in the following sections:

- ♦ [“Prerequisites for the Tomcat Application Server” on page 40](#)
- ♦ [“Prerequisites for the Identity Governance Databases” on page 39](#)
- ♦ [“Safeguarding the Passwords for a Silent Installation” on page 51](#)
- ♦ [NetIQ Identity Governance 3.0.1 Release Notes](#)

For a guided installation, see [“Using the Wizard to Install Tomcat, PostgreSQL, and ActiveMQ” on page 48](#).

Safeguarding the Passwords for a Silent Installation

You must specify `NETIQ_DB_PASSWORD` for the PostgreSQL installation:

```
export NETIQ_DB_PASSWORD=myPassWord
```

Installing Tomcat, PostgreSQL, and ActiveMQ Using a Silent Properties File

If the `TomcatPostgreSQL-install-silent.properties` file resides 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.

- 1 Log in as `root` on Linux server or an administrator on Windows server where you want to install the applications.
- 2 Navigate to the directory containing the installation files.
- 3 To specify the installation parameters, complete the following steps:
 - 3a Ensure that the silent properties file is located in the same directory as the execution file for installation.
 - 3b In a text editor, open the silent properties file.

- 3c Specify the parameter values. For a description of the parameters, see [Step 7 on page 73](#) in “Using the Wizard to Install Tomcat, PostgreSQL, and ActiveMQ”.

NOTE: To use an existing PostgreSQL database for Identity Governance on a Linux server, specify `installed` for `NETIQ_USE_INSTALLED_POSTGRES`. The database instance must be run by a supported version of PostgreSQL. Also, you do not need to configure the database.

- 3d Save and close the file.

- 4 To launch the installation process, enter one of the following commands:

- ♦ **Linux:** Enter `./TomcatPostgreSQL.bin -i silent -f path_to_silent_properties_file`
- ♦ **Windows:** `cmd /c ".\TomcatPostgreSQL.exe -i silent -f path_to_silent_properties_file"`
- ♦ **Windows (PowerShell):** `./TomcatPostgreSQL.exe -i silent -f path_to_silent_properties_file"`

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.

Stopping, Starting, and Restarting Tomcat

Identity Governance runs the Tomcat server running on Linux as a service instead of starting it using an initialization script. Some installation and configuration tasks require stopping Tomcat before completing the steps and then starting it afterwards. Other tasks require reloading Tomcat. The following examples guide these processes.

Linux Examples for Tomcat

To stop Tomcat:

```
systemctl stop identity_tomcat.service
```

To start Tomcat:

```
systemctl start identity_tomcat.service
```

To restart Tomcat:

```
systemctl restart identity_tomcat.service
```

To show the status of Tomcat.service:

```
systemctl status identity_tomcat.service
```

Windows Examples for Tomcat

To stop, start, or restart Tomcat, use one of the following methods:

To use the Services window:

- 1 Open the **Services** window (`C:\Windows\system32\services.msc`).

2 Locate **IDM Apps Tomcat Service**.

3 Select **Start**, **Stop**, or **Restart**.

To use Task Manager:

1 Open Task Manager, and select **More details** if not already expanded.

2 Select the **Services** tab.

3 Locate **IDM Apps Tomcat Service** and right-click over it.

4 Select **Start**, **Stop**, or **Restart**.

NOTE: If the Task Manager Services does not restart, it could be due to the time it takes for **Stop** to finish. Wait a minute and then try **Start** again.

To use a command prompt:

1 Open a command prompt using `cmd.exe`.

2 Enter the following command:

```
NET STOP|START|RESTART "IDM Apps Tomcat Service"
```

3 (Conditional) If Windows responds that it could not stop the service, use another method to check the status.

Stopping, Starting, and Restarting ActiveMQ

Identity Governance installs ActiveMQ and starts it from within the Tomcat service. Some installation and configuration tasks require stopping ActiveMQ before completing the steps and then starting it afterwards.

Linux Examples for ActiveMQ

To stop ActiveMQ:

```
systemctl stop identity_activemq.service
```

To start ActiveMQ:

```
systemctl start identity_activemq.service
```

To restart ActiveMQ:

```
systemctl restart identity_activemq.service
```

To show the status of the ActiveMQ service:

```
systemctl status identity_activemq.service
```

Windows Examples for ActiveMQ

On Windows you start, stop, and restart ActiveMQ by starting, stopping, and restarting Tomcat. For more information, see [“Windows Examples for Tomcat” on page 52](#).

4 Installing One SSO Provider

This section provides information about installing One SSO Provider (OSP), which allows you to configure Identity Governance for single sign-on access.

NOTE: If you have not already installed the minimum version of OSP in your environment, you must install OSP for Identity Governance.

The installation program installs the components in the following default directory:

- ♦ **Linux:** /opt/netiq/idm/apps/osp
- ♦ **Windows:** C:\netiq\idm\apps\osp

It is important that you review the installation process before beginning:

- ♦ [“Checklist for Installing One SSO Provider” on page 55](#)
- ♦ [“Using the Wizard to Install One SSO Provider” on page 55](#)
- ♦ [“Silently Installing One SSO Provider” on page 59](#)

Checklist for Installing One SSO Provider

It is important that you complete the steps in the following checklist:

	Checklist Items
<input type="checkbox"/>	1. Decide which servers you want to use for your Identity Governance components. For more information, see “Recommended Installation Scenarios and Server Setup” on page 33 .
<input type="checkbox"/>	2. Ensure that Tomcat has been installed. For more information, see Chapter 3, “Installing Tomcat, PostgreSQL, and ActiveMQ for Identity Governance,” on page 47 .
<input type="checkbox"/>	3. Decide whether you want to install Identity Governance in a clustered environment. For more information about the requirements, see “Ensuring High Availability for Identity Governance” on page 37 .
<input type="checkbox"/>	4. Install the components: <ul style="list-style-type: none">♦ For a guided installation, see “Using the Wizard to Install One SSO Provider” on page 55.♦ To install the components silently, see “Silently Installing One SSO Provider” on page 59.

Using the Wizard to Install One SSO Provider

The following procedure describes how to install OSP using an installation wizard, either in the GUI format or from the console. To prepare for the installation, review the considerations and system requirements listed in the following sections:

- ♦ [“Prerequisites for One SSO Provider” on page 40](#)

- ♦ [“Identity Governance Server System Requirements” on page 41](#)
- ♦ Release Notes accompanying the release

To perform a silent, unattended installation, see [“Silently Installing One SSO Provider” on page 59](#).

To install OSP:

- 1 Log in as `root` on Linux server or an administrator on Windows server where you want to install OSP.
- 2 Stop Tomcat. For examples, see [“Stopping, Starting, and Restarting Tomcat” on page 52](#).
- 3 From the directory that contains the installation files, complete one of the following actions:
 - ♦ **Linux (console):** Enter `./osp-install-linux.bin -i console`
 - ♦ **Linux (GUI):** Enter `./osp-install-linux.bin`
 - ♦ **Windows (console):** Enter `cmd /c "osp-install-win.exe -i console"`
 - ♦ **Windows (GUI):** Double-click `osp-install-win.exe`

NOTE: To execute the file, you might need to use the `chmod +x` or `sh` command for Linux or log in to your Windows server as an administrator.

- 4 Accept the license agreement, and then select **Next**.
- 5 Specify a path for the installed files.
- 6 Complete the guided process, using the following parameters:

- ♦ **Tomcat details**

Represents the home directory for the Tomcat server. The installation process adds some files for OSP to this folder.

- ♦ **Linux:** Default location of `/opt/netiq/idm/apps/tomcat`
- ♦ **Windows:** Default location of `c:\netiq\idm\apps\tomcat`

- ♦ **Tomcat Java home**

Represents the home directory for Java on the Tomcat server. The installation process adds some files for OSP to the directory.

- ♦ **Linux:** Default location of `/opt/netiq/idm/apps/jre`
- ♦ **Windows:** Default location of `c:\netiq\idm\apps\jre`

- ♦ **Application address**

Represents the settings of the URL that users need to connect to OSP. For example, `https://myserver.mycompany.com:8443`.

The installation program creates a certificate in the `osp.jks` file that uses the specified host name.

Protocol

Specifies whether you want to use `http` or `https`. To use SSL for communications, specify `https`.

If you specify `https`, ensure that you have configured your server for SSL communications. For more information, see [“Understanding the Keystore for the Authentication Server” on page 29](#).

Host Name

Do not use `localhost`.

In a non-clustered environment, specifies the DNS name or IP address of the Tomcat server where you are installing OSP.

In a clustered environment, specifies the DNS name of the server that hosts the load balancer that you want to use. For more information about installing in a clustered environment, see [“Ensuring High Availability for Identity Governance” on page 37](#).

Port

Specifies the port that you want the server to use for communication with users' computers.

When installing in a clustered environment, specify the port for the load balancer.

◆ Login screen customization

(Optional) Represents the organization name displayed on the login screen for users. The default value is `NetIQ Access`. Keep in mind the following points:

- ◆ Allows the ASCII character set (0x20 - 0x7E)
- ◆ Must add escape character for dollar signs (\\$) and backslashes (\\)
- ◆ Escaped backslashes do not appear
- ◆ Apostrophes and spaces are converted into pseudo-tags [apos] and [nbsp], respectively
- ◆ Installer stores result in `oidp_enduser_custom_resources_en_US.properties`.

◆ Authentication details

Represents the requirements for connecting to an authentication server that contains the list of users who can log in to the application. For more information about the authentication server, see [“Understanding Authentication with One SSO Provider” on page 28](#).

LDAP host

Specifies the DNS name or IP address of the LDAP authentication server, your directory server that contains the distinguished names of your user accounts.

Do not use `localhost` unless you want to specify a CSV file instead of an authentication server. (Test environment only)

LDAP port

Specifies the port that you want the LDAP authentication server to use for communication with Identity Governance. For example, specify `389` for a non-secure port or `636` for SSL connections.

Use SSL

Specifies whether you want to use Secure Sockets Layer protocol for connections between the Identity Governance and the authentication server.

JRE Trust store (cacerts) file

Applies only when you want to use SSL for the LDAP connection or TLS for audit events.

Specifies the path to the certificate.

- ◆ **Linux:** For example, `/opt/netiq/idm/apps/jre/lib/security/cacerts`
- ◆ **Windows:** For example, `c:\netiq\idm\apps\jre\lib\security\cacerts`

JRE Trust store password

Applies only when you want to use SSL for the LDAP connection or TLS for audit events.

Specifies the password for the `cacerts` file.

Admin DN

Applies only when installing a new authentication 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 authentication server.

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

User container

Applies only when installing a new authentication server.

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

Admin container

Applies only when installing a new authentication server.

Specifies the search context for the Identity Governance administrator accounts in the LDAP authentication server. In most cases, this value is the same as the container in the **Admin DN** field. For example, `ou=sa,o=system`.

Keystore Password

Applies only when installing a new authentication server.

Specifies the password that you want to create for the new keystore for the LDAP authentication server.

The password must be a minimum of six characters.

NOTE: After retrieving the authentication details, the installer uses the gathered information to connect to the LDAP server and attempt to determine whether the server is Active Directory (AD) or eDirectory (eDir). If this test is unsuccessful, then the installer prompts you to select the LDAP server type.

♦ **Auditing details**

Represents the settings for auditing OSP events that occur in the authentication server.

Enable auditing for OSP

Specifies whether you want to send OSP events to an auditing server.

If you select this setting, also specify the location for the audit log cache.

Protocol

Applies only when you enable auditing for OSP.

Specifies whether to use TCP (default), TLS (TCP using SSL), or UDP.

Audit server

Applies only when you enable auditing for OSP.

Specifies name of the auditing server.

Audit port

Applies only when you enable auditing for OSP.

Specifies the port to use for communication using the selected protocol.

Audit events cache

Applies only when you enable auditing for OSP.

Specifies the location of the cache directory that you want to use for auditing.

- ♦ **Linux:** For example, `/opt/netiq/idm/apps/audit`
- ♦ **Windows:** For example, `c:\netiq\idm\apps\audit`

- 7 Review the pre-installation summary.
- 8 Start the installation process.
- 9 When the installation process completes, select **Done**.

Silently Installing One SSO Provider

A silent (non-interactive) installation does not display a user interface or ask the user any questions. The installation kit provides the `osp-install-silent.properties` file. To prepare for the installation, review the considerations and system requirements listed in the following sections:

- ♦ [“Prerequisites for One SSO Provider” on page 40](#)
- ♦ [“Identity Governance Server System Requirements” on page 41](#)
- ♦ Release Notes accompanying the release

To perform a guided installation, see [“Using the Wizard to Install One SSO Provider” on page 55](#).

Creating a Silent Properties File for Installing on a Secondary Node

In a clustered environment, you can use the same silent properties file for each node. However, you might choose to run the guided installation on the primary node, then silently install on the secondary nodes. You can quickly create a silent properties file from the `OSP_Install.log` file that the guided installation creates.

- 1 After installing OSP on the primary node, locate the `osp_install_log.log` file.
 - ♦ **Linux:** Default location of `/opt/netiq/idm/apps/osp/logs`
 - ♦ **Windows:** Default location of `c:\netiq\idm\apps\osp\logs`
- 2 Locate the sample `osp-install-silent.properties` file, by default in the same directory as the installation scripts for OSP.
- 3 Open the files in a text editor.
- 4 Copy the parameter values from the log file to their corresponding parameters in the silent properties file.

Your silent properties file should contain all the parameters listed between `User Interactions` and `Summary` in the log file.
- 5 Change the values that represent true/false settings:

Log file	Silent.properties file
0	false
1	true

- 6 Change the values for the NetIQ servlet and auditing protocols as specified in the following table:

Log file	Silent.properties file
NETIQ_SERVLET_PROTOCOL_HTTP=1 NETIQ_SERVLET_PROTOCOL_HTTPS=0	NETIQ_SERVLET_PROTOCOL=http
NETIQ_SERVLET_PROTOCOL_HTTP=0 NETIQ_SERVLET_PROTOCOL_HTTPS=1	NETIQ_SERVLET_PROTOCOL=https
NETIQ_OSP_AUDIT_PROTOCOL_TCP=1 NETIQ_OSP_AUDIT_PROTOCOL_TLS=0 NETIQ_OSP_AUDIT_PROTOCOL_UDP=0	NETIQ_OSP_AUDIT_PROTOCOL=tcp
NETIQ_OSP_AUDIT_PROTOCOL_TCP=0 NETIQ_OSP_AUDIT_PROTOCOL_TLS=1 NETIQ_OSP_AUDIT_PROTOCOL_UDP=0	NETIQ_OSP_AUDIT_PROTOCOL=tls
NETIQ_OSP_AUDIT_PROTOCOL_TCP=0 NETIQ_OSP_AUDIT_PROTOCOL_TLS=0 NETIQ_OSP_AUDIT_PROTOCOL_UDP=1	NETIQ_OSP_AUDIT_PROTOCOL=udp

- 7 Save and close the files.

Running a Silent Installation

- 1 Log in as `root` on Linux server or an administrator on Windows server where you want to install OSP.
- 2 Stop Tomcat. For examples, see [“Stopping, Starting, and Restarting Tomcat” on page 52](#).
- 3 (Conditional) If you have the `.iso` image file for the Identity Governance installation package, navigate to the directory containing the OSP installation files, located by default in the `osp` directory.
- 4 (Conditional) If you downloaded the installation files from the [NetIQ Downloads website](#), complete the following steps:
 - 4a Navigate to the `.zip` file for the downloaded image.
 - 4b Extract the contents of the file to a folder on the local computer.
- 5 Locate the `osp-install-silent.properties` file, by default in the same directory as the OSP installation file
- 6 (Conditional) In a non-clustered environment or when installing on the primary node, complete the following steps:
 - 6a In a text editor, open the silent properties file.
 - 6b Specify the parameter values.
For more information about the settings for installation, see [Step 5 through Step 6 on page 56](#).
 - 6c Save and close the file.
- 7 (Conditional) When installing on a secondary node in a cluster, you can modify the silent properties file using the steps in [“Creating a Silent Properties File for Installing on a Secondary Node” on page 59](#).
- 8 To run the silent installation:
 - ♦ **Linux:** Issue the following command:

```
./osp-install-linux.bin -i silent -f path_to_silent_properties_file
```

- ♦ **Windows:** From a command prompt enter, `osp-install-win.exe -i silent -f path_to_silent_properties_file`

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.

5 Installing Identity Governance

This section provides information about installing and configuring Identity Governance. It is important that you review the installation process, including the prerequisites and requirements, before beginning:

- ♦ [“Checklist for Installing and Configuring Identity Governance” on page 63](#)
- ♦ [“Preparing a PostgreSQL Database for Identity Governance” on page 65](#)
- ♦ [“Preparing an Oracle Database for Identity Governance” on page 67](#)
- ♦ [“Preparing an MS SQL Server Database for Identity Governance” on page 70](#)
- ♦ [“Using a Guided Process to Install Identity Governance and Identity Reporting” on page 73](#)
- ♦ [“Performing a Silent Installation of Identity Governance” on page 79](#)

Checklist for Installing and Configuring Identity Governance

Before beginning the installation process, it is important that you review the following steps.

	Checklist Items
<input type="checkbox"/>	1. Ensure that your environment meets the prerequisites and requirements for hosting Identity Governance. For more information, see “Prerequisites for Installing Identity Governance” on page 38 and “Hardware and Software Requirements” on page 41 .
<input type="checkbox"/>	2. Decide whether you want to install Identity Governance in a clustered environment. For more information about the requirements, see “Ensuring High Availability for Identity Governance” on page 37 .
<input type="checkbox"/>	3. Ensure that your environment has a supported version of Tomcat already installed. For more information about installing Tomcat, see Chapter 3, “Installing Tomcat, PostgreSQL, and ActiveMQ for Identity Governance,” on page 47 .
<input type="checkbox"/>	4. Ensure that your environment has a supported version of OSP. For more information about installing OSP, see Chapter 4, “Installing One SSO Provider,” on page 55 .
<input type="checkbox"/>	5. (Conditional) To use a Microsoft SQL Server database, ensure that your environment has a supported version already installed. For more information, see the following sections: <ul style="list-style-type: none">♦ “Understanding the Identity Governance and Reporting Databases” on page 31♦ “Preparing an MS SQL Server Database for Identity Governance” on page 70
<input type="checkbox"/>	6. (Conditional) To use an Oracle database, ensure that your environment has a supported version already installed. For more information, see the following sections: <ul style="list-style-type: none">♦ “Understanding the Identity Governance and Reporting Databases” on page 31♦ “Preparing an Oracle Database for Identity Governance” on page 67

	Checklist Items
<input type="checkbox"/>	<p>7. (Conditional) To use a PostgreSQL database, ensure that your environment has a supported version already installed. For more information, see the following sections:</p> <ul style="list-style-type: none"> ♦ “Understanding the Identity Governance and Reporting Databases” on page 31 ♦ Chapter 3, “Installing Tomcat, PostgreSQL, and ActiveMQ for Identity Governance,” on page 47 ♦ “Preparing a PostgreSQL Database for Identity Governance” on page 65
<input type="checkbox"/>	<p>8. (Conditional) To use TLS auditing, the audit server should be up and running when you install Identity Governance so that the installer can connect to the audit server and retrieve the certificate to add to the keystore.</p>
<input type="checkbox"/>	<p>9. Install Identity Governance and Identity Reporting (optional):</p> <ul style="list-style-type: none"> ♦ For a guided installation, see “Using a Guided Process to Install Identity Governance and Identity Reporting” on page 73. ♦ For an unattended installation, see “Performing a Silent Installation of Identity Governance” on page 79.
<input type="checkbox"/>	<p>10. To use third-party client connector software for gathering identity and application data, ensure that you add the appropriate .jar files. For more information, see “Identity Governance Server System Requirements” on page 41.</p>
<input type="checkbox"/>	<p>11. Complete the setup for Identity Governance and its database. For more information, see Section 7, “Completing the Installation Process,” on page 97.</p>
<input type="checkbox"/>	<p>12. (Optional) Modify the SSL settings for communication with the authentication server. For more information, see “Using the TLS/SSL Protocol for Secure Connections” on page 136.</p>
<input type="checkbox"/>	<p>13. (Optional) Modify the configuration settings for Identity Governance. For more information, see Chapter 10, “Configuring Identity Governance Settings,” on page 129.</p>
<input type="checkbox"/>	<p>14. (Optional) Add users who can log in to Identity Governance and assign them to authorizations in the application. For more information, see “Adding Identity Governance Users” on page 184.</p>
<input type="checkbox"/>	<p>15. (Optional) Customize the user interface or the templates for email notifications and collectors. For more information, see Chapter 11, “Customizing Identity Governance for Your Enterprise,” on page 153.</p>
<input type="checkbox"/>	<p>16. (Optional) Create a single sign-on experience for users between Identity Governance and Identity Manager Home and Provisioning Dashboard. For more information, see “Checklist for Integrating Identity Governance with Identity Manager” on page 187.</p>

Preparing a PostgreSQL Database for Identity Governance

You can install PostgreSQL and create the databases for Identity Governance if you do not want the installation program to create these. The installation program can create the databases, tables, views, and other artifacts in the databases. The program needs the name of the databases to represent the operations, data collection, provisioning workflow, and analytics databases for Identity Governance.

However, your database administrator might prefer to create the schemas, as well as the database artifacts, rather than allowing the installation process to do so. Your database administrator can choose to complete the following actions before you install Identity Governance:

- ♦ [“Adding the JDBC File to the Application Server” on page 65](#)
- ♦ [“Creating the PostgreSQL Databases Before Installation” on page 65](#)
- ♦ [“Creating a Temporary PostgreSQL Database Administrator for the Installation Process” on page 66](#)

Adding the JDBC File to the Application Server

To run queries against the database, add the JDBC file to the application server.

- 1 Ensure that you do not have an older version of the JDBC file in the:
 - ♦ **Linux:** /opt/netiq/idm/apps/tomcat/lib directory
 - ♦ **Windows:** c:\netiq\idm\apps\tomcat\lib directory
- 2 When you install Identity Governance, the installation program places the correct JDBC file in the:
 - ♦ **Linux:** /opt/netiq/idm/apps/tomcat/lib directory
 - ♦ **Windows:** c:\netiq\idm\apps\tomcat\lib directory

Creating the PostgreSQL Databases Before Installation

Your database administrator can choose to create the databases for Identity Governance before you run the installation. Otherwise, the installation program can generate the databases.

- 1 Install a supported version of PostgreSQL. For more information, see [“Database Server System Requirements” on page 43](#).
- 2 Create the databases and roles for igops, igdcs, igwf, and igara using the following commands:

```
CREATE ROLE operations_db_name LOGIN password 'password';
CREATE ROLE data_collection_db_name LOGIN password 'password';
CREATE ROLE workflow_db_name LOGIN password 'password';
CREATE ROLE analytics_db_name LOGIN password 'password';
CREATE ROLE ig_report_role NOLOGIN;
CREATE DATABASE igops WITH OWNER = operations_db_name ENCODING = 'UTF8';
CREATE DATABASE igdcs WITH OWNER = data_collection_db_name ENCODING = 'UTF8';
CREATE DATABASE igwf WITH OWNER = workflow_db_name ENCODING = 'UTF8';
CREATE DATABASE igara WITH OWNER = analytics_db_name ENCODING = 'UTF8';
GRANT EXECUTE ON igops.max_risk_level to igrptuser;
GRANT EXECUTE ON igops.min_risk_level to igrptuser;
GRANT EXECUTE ON igops.risk_value to igrptuser;
```

- 3 Specify the same password for all databases.

NOTE: The installation process for Identity Governance requires you to specify one password that applies to all databases. After installing Identity Governance, you can modify the passwords to be unique for each database.

- 4 Create the reporting user `igrptuser`.

```
CREATE ROLE "igrptuser" PASSWORD 'igrptuser_password' LOGIN;
```

- 5 Grant the reporting role to the reporting user.

```
GRANT IG_REPORT_ROLE TO "igrptuser";
```

- 6 When you install Identity Governance, specify one of the following settings:

- ♦ **Configure database now > Update**, if you want the installation program to generate or update the schemas, tables, and views when you migrate from Identity Governance 2.5 to 3.0
- ♦ **Configure database now > Use only existing**, if your database is already set up correctly with all schemas, roles, and users
- ♦ **Generate SQL for later**, if your database administrator wants to generate the schemas, tables, and views
- ♦ **No database configuration**, for using two or more nodes in clustered environment

For more information about using SQL statements after installation, see [“Configuring the Databases after Installation” on page 97](#).

Creating a Temporary PostgreSQL Database Administrator for the Installation Process

The installation process requires the password for an administrator account in PostgreSQL that can create databases, roles, tables, views, and other artifacts in the databases. You can avoid specifying the password for the `postgres` account by creating a temporary administrator for the installation process to use.

The temporary account must have the following properties:

- ♦ LOGIN
- ♦ SUPERUSER
- ♦ CREATEDB
- ♦ CREATEROLE

The temporary account must have privileges to complete the following tasks:

- ♦ create databases
- ♦ create roles
- ♦ assign ownership of each database to a role so that this role can then create tables, views, and other artifacts within the databases that it owns
- ♦ grant connect on a database to a role
- ♦ grant one role to another.

During installation, you can also select **Generate SQL for later**, which prevents the installation program from creating the tables, views, and artifacts in the Identity Governance or Identity Reporting databases. Instead, the program generates a SQL file for each database, which your database administrator can run to update each database. For more information about using the SQL files, see [“Configuring the Databases after Installation” on page 97](#).

Preparing an Oracle Database for Identity Governance

Before installing, you need an Oracle JDBC file for the application server and an existing database for Identity Governance to use. You can create existing schemas if you do not want the installation program to create these. The installation program will create the schemas, tables, views, and other artifacts in the database unless you select **Generate SQL for later** in the **Database details** section of the installation program. The program needs the name of the database, user tablespace (**USERS** by default), temporary tablespace (**TEMP** by default), and the user schemas to represent the operations, data collection, provisioning workflow, and analytics tables for Identity Governance.

IMPORTANT: You must turn on the SQL Tuning Advisor to optimize queries in the Oracle database.

However, your database administrator might prefer to create the schemas, as well as the database artifacts, rather than allowing the installation process to do so. Your database administrator can choose to complete the following actions before you install Identity Governance:

- ♦ [“Adding the Oracle JDBC File to the Application Server” on page 67](#)
- ♦ [“Creating the Schemas for the Oracle Database before Installation” on page 68](#)
- ♦ [“Creating a Temporary Oracle Database Administrator for the Installation Process” on page 69](#)

After you install Identity Governance, the database administrator might need to update the schemas and global configuration values. For more information, see [Chapter 7, “Completing the Installation Process,” on page 97](#).

Adding the Oracle JDBC File to the Application Server

To run queries against the databases, you must add an Oracle JDBC file to the Tomcat library.

- 1 Download the `ojdbc7.jar` file from the [Oracle website](#).
- 2 Copy the file to a temporary directory on the `tomcat_install` server.

The installation process then places the file in the:

- ♦ **Linux:** `/opt/netiq/idm/apps/tomcat/lib` directory
- ♦ **Windows:** `c:\netiq\idm\apps\tomcat\lib` directory

NOTE: Ensure that you do not have an older version of the Oracle JDBC file in the directory or the installation fails.

Creating the Schemas for the Oracle Database before Installation

Your database administrator can choose to create the schemas in the Identity Governance database before you run the installation. Otherwise, the installation program can generate the schemas.

This procedure assumes that you will use the default names for the schemas:

- ♦ Identity Governance: `igops`, `igdcs`, `igwf`, and `igara`
- ♦ Identity Reporting: `idm_rpt_cfg`

To create the schemas:

- 1 Install a supported version of Oracle.
For more information, see [“Database Server System Requirements” on page 43](#).
- 2 Create or identify the database that you want Identity Governance to use.
- 3 In the database, create the schema for `igops`, `igdcs`, `igwf`, and `igara` with the following privileges:
 - ♦ `select_catalog_role`
 - ♦ Create session
 - ♦ Create table
 - ♦ Create view
 - ♦ Create sequence
 - ♦ Create procedure
 - ♦ Create trigger
 - ♦ Analyze any (`igops` only)
 - ♦ Create public synonym (`igops` only)
 - ♦ Drop public synonym (`igops` only)
- 4 Specify the same password for all schemas.

NOTE: The installation process for Identity Governance requires you to specify one password that applies to all schemas. After installing Identity Governance, you can modify the passwords to be unique for each schema.

- 5 Issue the following commands:

NOTE: If you use the default values of `users` and `temp`, skip the following commands:

```
alter user dbName default tablespace users;  
alter user dbName temporary tablespace temp;
```

```

alter user igops default tablespace users;
alter user igops temporary tablespace temp;
alter user igops quota unlimited on users;
alter user igdcs default tablespace users;
alter user igdcs temporary tablespace temp;
alter user igdcs quota unlimited on users;
alter user igwf default tablespace users;
alter user igwf temporary tablespace temp;
alter user igwf quota unlimited on users;
alter user igara default tablespace users;
alter user igara temporary tablespace temp;
alter user igara quota unlimited on users;
CREATE USER idm_rpt_cfg IDENTIFIED BY "<password>";
GRANT CREATE SESSION, CREATE TABLE, CREATE VIEW, CREATE PROCEDURE, CREATE
SEQUENCE, CREATE TRIGGER, UNLIMITED TABLESPACE TO idm_rpt_cfg;
create role ig_report_role not identified;
grant EXECUTE ON igops.max_risk_level to igrptuser;
grant EXECUTE ON igops.min_risk_level to igrptuser;
grant EXECUTE ON igops.risk_value to igrptuser;

```

6 Create the reporting user igrptuser.

```
CREATE USER igrptuser IDENTIFIED BY "igrptuser_password";
```

7 Grant the reporting role to the reporting user plus additional privileges.

```

GRANT IG_REPORT_ROLE TO igrptuser;
GRANT CREATE SESSION TO igrptuser;
ALTER USER igrptuser DEFAULT TABLESPACE USERS;
ALTER USER igrptuser TEMPORARY TABLESPACE TEMP;

```

8 When installing Identity Governance, specify one of the following settings:

- ♦ **Configure database now > Update**, if you want the installation program to generate or update the schemas, tables, and views when you migrate from Identity Governance 2.5 to 3.0
- ♦ **Configure database now > Use only existing**, if your database is already set up correctly with all schemas, roles, and users
- ♦ **Generate SQL for later**, if your database administrator wants to generate the schemas, tables, and views
- ♦ **No database configuration**, for using two or more nodes in clustered environment

For more information about using SQL statements after installation, see [“Configuring the Databases after Installation” on page 97](#).

Creating a Temporary Oracle Database Administrator for the Installation Process

The installation process requires the password for an administrator account in Oracle that can create tables, views, and other artifacts in the databases. You can avoid specifying the password for the Oracle `system` account by creating a temporary administrator for the installation process to use.

The temporary account must have the `CONNECT` role and the following system privileges:

- ♦ Alter user
- ♦ Create public synonym
- ♦ Create user

- ♦ Drop public synonym
- ♦ Drop user
- ♦ Grant any object privilege
- ♦ Grant any privilege
- ♦ Grant any role

During installation, you can also select **Generate SQL for later**, which prevents the installation program from creating the tables, views, and artifacts in the Identity Governance or Identity Reporting database. Instead, the program generates a SQL file for each schema, which your database administrator can run to update the database. For more information about using the SQL files, see [“Configuring the Databases after Installation” on page 97](#).

Preparing an MS SQL Server Database for Identity Governance

Before installing, you need an MS SQL Server JDBC file for the application server and an existing database for Identity Governance to use. You can install MS SQL Server and create the databases for Identity Governance if you do not want the installation program to create these. The installation program can create the databases, tables, views, and other artifacts in the databases. The program needs the name of the databases to represent the operations, data collection, provisioning workflow, and analytics databases for Identity Governance.

However, your database administrator might prefer to create the schemas, as well as the database artifacts, rather than allowing the installation process to do so. Your database administrator can choose to complete the following actions before you install Identity Governance:

- ♦ [“Adding the JDBC File to the Application Server” on page 70](#)
- ♦ [“Creating the MS SQL Server Databases Before Installation” on page 70](#)
- ♦ [“Creating a Temporary MS SQL Server Database Administrator for the installation process” on page 72](#)

Adding the JDBC File to the Application Server

To run queries against the database, add the JDBC file to the application server.

- 1 Ensure that you do not have an older version of the JDBC file in the:
 - ♦ **Linux:** /opt/netiq/idm/apps/tomcat/lib directory
 - ♦ **Windows:** c:\netiq\idm\apps\tomcat\lib directory
- 2 When you install Identity Governance, the installation program places the correct JDBC file in the directory.

Creating the MS SQL Server Databases Before Installation

Your database administrator can choose to create the databases for Identity Governance before you run the installation. Otherwise, the installation program can generate the databases.

- 1 Install a supported version of SQL Server. For more information, see [“Database Server System Requirements” on page 43](#).
- 2 Create the databases, logins, users, and roles using the following commands:

```

USE [master];
CREATE DATABASE [igops];
CREATE DATABASE [igdcs];
CREATE DATABASE [igwf];
CREATE DATABASE [igara];

ALTER DATABASE [igops] SET READ_COMMITTED_SNAPSHOT ON WITH NO_WAIT;
ALTER DATABASE [igdcs] SET READ_COMMITTED_SNAPSHOT ON WITH NO_WAIT;
ALTER DATABASE [igwf] SET READ_COMMITTED_SNAPSHOT ON WITH NO_WAIT;
ALTER DATABASE [igara] SET READ_COMMITTED_SNAPSHOT ON WITH NO_WAIT;

CREATE LOGIN [igops] WITH PASSWORD = 'password';
CREATE LOGIN [igdcs] WITH PASSWORD = 'password';
CREATE LOGIN [igwf] WITH PASSWORD = 'password';
CREATE LOGIN [igara] WITH PASSWORD = 'password';
GO

USE [igops];
CREATE USER [igops] FOR LOGIN [igops];
ALTER ROLE [db_owner] ADD MEMBER [igops];
CREATE ROLE [IG_REPORT_ROLE];
CREATE LOGIN [igrptuser] WITH PASSWORD = 'password';
CREATE USER [igrptuser] FOR LOGIN [igrptuser];
ALTER ROLE [IG_REPORT_ROLE] ADD MEMBER [igrptuser];
GO

USE [igdcs];
CREATE USER [igdcs] FOR LOGIN [igdcs];
ALTER ROLE [db_owner] ADD MEMBER [igdcs];
GO

USE [igwf];
CREATE USER [igwf] FOR LOGIN [igwf];
ALTER ROLE [db_owner] ADD MEMBER [igwf];
GO

USE [igara];
CREATE USER [igara] FOR LOGIN [igara];
ALTER ROLE [db_owner] ADD MEMBER [igara];
GO

```

3 (Optional) If you are installing Identity Reporting, also use the following commands:

```

USE [master];
CREATE DATABASE [reports];
ALTER DATABASE [reports] SET READ_COMMITTED_SNAPSHOT ON WITH NO_WAIT;
CREATE LOGIN [idm_rpt_cfg] WITH PASSWORD = 'password';
GO

USE [reports];
CREATE USER [idm_rpt_cfg] FOR LOGIN [idm_rpt_cfg];
GO

USE [reports];
GRANT EXECUTE ON [igops.max_risk_level] TO [IG_REPORT_ROLE];
GRANT EXECUTE ON [igops.min_risk_level] TO [IG_REPORT_ROLE];
GRANT EXECUTE ON [igops.risk_value] TO [IG_REPORT_ROLE];
GO

```

Then log into [reports] database directly and execute the following commands:

```
CREATE SCHEMA [idm_rpt_cfg] AUTHORIZATION [idm_rpt_cfg];
GO
ALTER AUTHORIZATION ON SCHEMA::[idm_rpt_cfg] TO [idm_rpt_cfg];
GO
```

4 Specify the same password for all databases.

NOTE: The installation process for Identity Governance requires you to specify one password that applies to all databases. After installing Identity Governance, you can modify the passwords to be unique for each database.

5 Create the reporting user igrptuser.

```
USE [igops]; CREATE LOGIN [igrptuser] WITH PASSWORD = 'igrptuser_password';
CREATE USER [igrptuser] FOR LOGIN [igrptuser];
```

6 Grant the reporting role to the reporting user.

```
USE [igops]; ALTER ROLE [IG_REPORT_ROLE] ADD MEMBER [igrptuser];
```

7 When installing Identity Governance, specify one of the following settings:

- ♦ **Configure database now > Update**, if you want the installation program to generate or update the schemas, tables, and views when you migrate from Identity Governance 2.5 to 3.0
- ♦ **Configure database now > Use only existing**, if your database is already set up correctly with all schemas, roles, and users
- ♦ **Generate SQL for later**, if your database administrator wants to generate the schemas, tables, and views
- ♦ **No database configuration**, for using two or more nodes in clustered environment

For more information about using SQL statements after installation, see [“Configuring the Databases after Installation” on page 97](#).

Creating a Temporary MS SQL Server Database Administrator for the installation process

The installation process requires the password for an administrator account in MS SQL Server that can create databases, tables, views, and other artifacts in the databases. You can avoid specifying the password for the admin account by creating a temporary administrator for the installation process to use.

The temporary account must have the following properties:

- ♦ Create any database
- ♦ Alter any login
- ♦ Alter any user
- ♦ Create role

During installation, you can also select **Generate SQL for later**, which prevents the installation program from creating the tables, views, and artifacts in the Identity Governance or Identity Reporting database. Instead, the program generates a SQL file for each schema, which your database administrator can run to update the database. For more information about using the SQL files, see [“Configuring the Databases after Installation” on page 97](#).

Using a Guided Process to Install Identity Governance and Identity Reporting

The following procedure describes how to install Identity Governance and Identity Reporting using an installation wizard, either in GUI format or from the console. To prepare for the installation, review the considerations and system requirements listed in the following sections:

- ♦ [“Prerequisites for Installing Identity Governance” on page 38](#)
- ♦ [“Identity Governance Server System Requirements” on page 41](#)
- ♦ Release Notes accompanying the release

To perform a silent, unattended installation, see [“Performing a Silent Installation of Identity Governance” on page 79](#).

To install Identity Governance:

- 1 Log in as `root` on Linux server or as an administrator on Windows server to the server where you want to install Identity Governance.
- 2 Stop Tomcat. For examples, see [“Stopping, Starting, and Restarting Tomcat” on page 52](#).
- 3 From the directory that contains the installation files, complete one of the following actions:
 - ♦ **Linux:** Use one of the following commands to install Identity Governance on Linux.
 - ♦ **To use the console:** enter `./identity-governance-install-linux.bin -i console`
 - ♦ **To use the wizard:** enter `./identity-governance-install-linux.bin`
 - ♦ **Windows:** Use one of the following commands to install Identity Governance on Windows.
 - ♦ **To use the console:** enter `cmd /c "identity-governance-install-win.exe -i console"`
 - ♦ **To use the wizard:** double-click `identity-governance-install-win.exe`

NOTE: To execute the file, you might need to use the `chmod +x` or `sh` command for Linux or log in to your Windows server as an administrator.

- 4 Accept the license agreement, and then select **Next**.
- 5 Select whether to install Identity Governance, Identity Reporting, or both.
- 6 Specify an installation path for each installed feature.
- 7 Complete the guided process, using the following parameters:

- ♦ **Tomcat installation**

Represents the settings for the Tomcat installation that hosts Identity Governance. In a clustered environment, specify runtime values for each node where you install Identity Governance.

Specify the Tomcat folder

Specifies the path to the Tomcat installation. The installation process adds or modifies some files for Identity Governance to this folder.

- ♦ **Linux:** `/opt/apache-tomcat-x.x.xx`
- ♦ **Windows:** `c:\netiq\idm\apps\tomcat-x.x.xx`

Runtime host name

Specifies the DNS name or IP address for the Tomcat installation.

Runtime port

Specifies the port that Tomcat uses to listen for communication from Identity Governance or the load balancers.

Runtime identifier

In a non-clustered environment, you can specify the local server name.

In clustered environment, specifies the unique name for the current node. For example, `node1` or `ProdNode1`. Do not use the server's name, which might change according to a DHCP assignment.

♦ Tomcat Java Home

Represents the path to the Oracle Java instance that Tomcat uses. For example, `/root/jdk1.x.x_xx`. The installation process adds some files for Identity Governance to the Tomcat home folder.

♦ Application address

Represents the settings of the URL that users need to connect to the Identity Governance. For example, `https://myserver.mycompany.com:8443`.

Protocol

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

Host Name

Do not use `localhost`.

In a non-clustered environment, specifies the DNS name or IP address of the server hosting Identity Governance.

In a clustered environment, specifies the DNS name of the server that hosts the load balancer that you want to use. For more information about installing in a clustered environment, see [“Ensuring High Availability for Identity Governance” on page 37](#).

Port

Specifies the port that you want the server to use for communication with client computers. The default is 8080. To use SSL, the default is 8443.

When installing in a clustered environment, specify the port for the load balancer.

♦ Authentication details

Represents the requirements for connecting Identity Governance to the LDAP authentication server (for example, OSP) that contains the list of users who can log in to the application. For more information about the authentication server, see [“Understanding Authentication for Identity Governance” on page 27](#).

NOTE: In a clustered environment where the `osp.war` file resides behind the load balancer, specify the host and port for the load balancer's server rather than the authentication server.

Service password

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

Protocol

Change this only when you choose to connect to an external authentication 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*.

Host

Change this only when you choose to connect to an external authentication server.

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

Port

Change this only when you choose to connect to an external authentication server.

Specifies the port that you want the LDAP authentication server or load balancer to use for communication with Identity Governance.

◆ Bootstrap administrator details

Represents the credentials for the bootstrap administrator. For more information, see [“Understanding the Bootstrap Administrator for Identity Governance” on page 29](#).

Bootstrap admin name

Specifies the name of the bootstrap administrator account. The default value is `igadmin`.

(Conditional) When connecting to an existing Identity Manager authentication server, specify the full DN of a unique identity that already exists and can access Identity Manager Home as a bootstrap administrator. For example,
`cn=uaadmin,ou=sa,o=data`.

NOTE

- ◆ If you use an Identity Vault user as a bootstrap administrator, you must configure Identity Governance to use Identity Vault instead of File in the Identity Governance Configuration Utility (`/idgov/bin/configutil.sh` or `\idgov\bin\configutil.cmd`). The **Bootstrap Administrator** section on the Authentication Server Details tab contains this setting.
 - ◆ 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.
-

Password

Specifies the password for the bootstrap administrator account.

◆ ActiveMQ details

(Optional) Represents the settings for ActiveMQ, which guarantees that notifications are sent using SMTP from Identity Governance.

For more information about configuring ActiveMQ in a clustered environment, see [“Configuring ActiveMQ Failover in the Tomcat Cluster” on page 104](#).

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 Type

Specifies the platform you want to use for the Identity Governance databases.

For more information about supported versions, see [“Database Server System Requirements” on page 43](#).

- ◆ **Database details**

Represents the settings for the Identity Governance databases. For more information, see [“Understanding the Identity Governance and Reporting Databases” on page 31](#).

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

In a clustered environment, perform the configuration steps only on the primary node in the cluster. For more information about installing in a clustered environment, see [“Ensuring High Availability for Identity Governance” on page 37](#).

Configure database now

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

NOTE: Ensure that you specified the correct names for the existing databases.

Generate SQL for later

Specifies that you want to generate the SQL scripts that the database administrator can run in your database platform to create the databases and other artifacts.

The installation process stores the scripts in the `./idgov/sql` directory. If you are installing Identity Reporting at this time, the installation process stores the scripts in the `./idrpt/sql` directory. For more information about using the files, see [Section 7, “Completing the Installation Process,” on page 97](#).

No database configuration

Specifies that you do not want to configure a new or existing database.

Use this setting when you install Identity Governance on a secondary node in the cluster. For more information, see [“Ensuring High Availability for Identity Governance” on page 37](#).

Host

Specifies the DNS name or the IP address of the server that hosts the Identity Governance databases.

Port

Specifies the port of the server that hosts the Identity Governance databases. The default values are 1433 for MS SQL Server, 1521 for Oracle and 5432 for PostgreSQL.

Microsoft SQL Server JDBC Jar

Applies only when using an MS SQL Server database

Specifies the path to the JAR file for the MS SQL Server JDBC driver. Microsoft provides this file.

Oracle JDBC Jar

Applies only when using an Oracle database

Specifies the path to the JAR file for the Oracle JDBC driver. For example, `/opt/oracle/ojdbc7.jar`.

Oracle provides the driver JAR file, which represents the Thin Client JAR for the database server.

Database name

Applies only when using an Oracle database

Specifies the name of the database to which you want to add the Identity Governance databases. For example, `Orclidentitygovernance`.

User tablespace

Applies only when using an Oracle database

Specifies the name of the database storage unit for storing the schema for the Identity Governance databases. The default is `USERS`.

Temporary tablespace

Applies only when using an Oracle database

Specifies the name of the temporary database storage unit for storing the schema. The default is `TEMP`.

Operations

Specifies the name of the database that stores operations data for Identity Governance. The default value is `igops`.

NOTE: If you created a blank database for the operations data, ensure that you specify the exact name of the existing, empty database.

Data collection

Specifies the name of the database that stores data collection information for Identity Governance. The default value is `igdc`.

NOTE: If you created a blank database for the data collection information, ensure that you specify the exact name of the existing, empty database.

Workflow

Specifies the name of the database that stores workflow information for Identity Governance. The default value is `igwf`.

NOTE: If you created a blank database for the workflow data, ensure that you specify the exact name of the existing, empty database.

Analytics

Specifies the name of the database that stores analytics information for Identity Governance. The default value is `igara`.

NOTE: If you created a blank database for the analytics data, ensure that you specify the exact name of the existing, empty database.

Password (for database owners)

Specifies the password for the database account administrator that can create database tables, views, and other artifacts in the Identity Governance databases.

Reporting user

Specifies the account for a database user that has rights to the views related to reporting for Identity Governance. The default value is `igrptuser`.

The installation process creates this account if you select **Configure database now** and **Update** (rather than **Use only existing**).

Reporting user password

Specifies the password for the reporting user specified above.

Administrator user

Specifies the account for a database administrator that the installation process can use to configure the databases for Identity Governance.

WARNING: Do not use the default database administrator account (`idmadmin`) if that account was created when you installed PostgreSQL and Tomcat.

Administrator password

Specifies the password for the database administrator.

Update / Use only existing

Applies only when you choose to configure the database during the installation.

Specifies whether you want to have the installation process migrate or create new databases or use existing, empty databases. Select **Update** if you are installing or upgrading Identity Governance.

NOTE: To use existing databases, the installation program drops known tables and views within each schema and then adds the needed tables and views that it needs for the current version.

♦ Identity Audit

Represents the settings for collecting auditing events that occur in the Identity Governance server.

Enable auditing

Specifies whether you want to send Identity Governance log events to an auditing server.

If you select this setting, also specify the audit server details.

Audit server

Applies only when you enable identity auditing.

Specifies the IP address or DNS name of the audit server.

Audit port

Applies only when you enable identity auditing.

Specifies the port to use for sending log events to the audit server.

Audit cache location

Applies only when you enable identity auditing.

Specifies the location of the cache directory on the Identity Governance server that you want to use to store log events. For example:

- ♦ **Linux:** `/opt/netiq/idm/apps/audit`
- ♦ **Windows:** `C:\netiq\idm\apps\audit`

Secure layer

Applies only when you enable identity auditing.

Specifies whether to use TLS (TCP using SSL). If not selected, events are sent using TCP.

Trust store location

Applies only when you want to use TLS for audit events.

Specifies the path to the keystore file location for trusting the audit server certificate. For example:

- ♦ **Linux:** `/opt/netiq/idm/apps/jre/lib/security/cacerts`
- ♦ **Windows:** `C:\netiq\idm\apps\jre\lib\security\cacerts`

Trust store password

Applies only when you want to use TLS for audit events.

Specifies the password for the trust store file.

Test certificate trust

Applies only when you want to use TLS for audit events.

Specifies whether to attempt to connect to the audit server and trust the retrieved certificate within a copy of the trust store file. The actual trust occurs during the installation process.

NOTE: Attempting a TLS connection on a TCP port results in a timeout after 5 seconds. Be sure to specify a secure audit port if you select to use TLS.

- 8 Review the pre-installation summary.

NOTE: **Application URL** represents the URL that connects users to Identity Governance.

- 9 Start the installation process.
- 10 When the installation process completes, select **Done**.
- 11 Continue to [Section 7, “Completing the Installation Process,” on page 97](#).

NOTE: Do **not** start Tomcat.

Performing a Silent Installation of Identity Governance

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

This section provides guidances for the following activities:

- ♦ [“Understanding the Passwords that Identity Governance Reads from Environment Variables During the Installation Process” on page 80](#)
- ♦ [“Creating a Silent Properties File for Installing on a Secondary Node” on page 80](#)
- ♦ [“Running the Silent Installation” on page 81](#)

To prepare for the installation, review the considerations and system requirements listed in the following sections:

- ♦ [“Prerequisites for Installing Identity Governance” on page 38](#)
- ♦ [“Identity Governance Server System Requirements” on page 41](#)
- ♦ Release Notes accompanying the release

To perform a guided installation, see [“Using a Guided Process to Install Identity Governance and Identity Reporting” on page 73](#).

Understanding the Passwords that Identity Governance Reads from Environment Variables During the Installation Process

Identity Governance reads in the following passwords from environment variables during the silent installation process. You must set these in the silent properties file.

- ♦ `install_authserver_client_secret`: It is the password for OSP.
- ♦ `install_bootstrap_secret`: It is the password for the bootstrap administrator.
- ♦ `install_db_admin_secret`: It is the password for the database administrator.
- ♦ `install_db_secret`: It is the password for `igops`, `igdc`s, `igwf`, and `igara`.
- ♦ `install_db_rpt_secret`: It is the password for `igrptuser`.
- ♦ `install_db_reporting_secret`: It is the password for `idm_rpt_cfg`.
- ♦ `install_truststore_secret`: It is the password for `cacerts`.
- ♦ `install_smtp_password_auth_user`: It is the password for the SMTP authentication user. If you SSL for SMTP, then you can enter it in the silent properties file or leave it empty and enter it later.

Creating a Silent Properties File for Installing on a Secondary Node

In a clustered environment, you can use the same silent properties file for each node. However, you might choose to run the guided installation on the primary node, then silently install on the secondary nodes. You can quickly create a silent properties file from the `Identity_Governance_InstallLog.log` file that the guided installation creates.

- 1 Locate the `Identity_Governance_InstallLog.log` file:
 - ♦ **Linux:** Default location of `/opt/netiq/idm/apps/idgov/logs`
 - ♦ **Windows:** Default location of `c:\netiq\idm\apps\idgov\logs`
- 2 Locate the sample `identity-governance-install-silent.properties` file, by default in the same directory as the installation scripts for Identity Governance.
- 3 Open the files in a text editor.
- 4 Copy the parameter values from the log file to their corresponding parameters in the silent properties file.

The silent properties file should contain all the parameters listed between `User Interactions` and `Summary` in the log file. Do not delete `INSTALLER_UI=silent` or any content after `# When to Configure DB?`.

- 5 Change the values that represent the true/false settings:

Log file	Silent.properties file
0	false
1	true

- 6 Change the values as specified in the following table:

Log file	Silent.properties file
install_servlet_protocol_http=1 install_servlet_protocol_https=0	install_servlet_protocol=http
install_servlet_protocol_http=0 install_servlet_protocol_https=1	install_servlet_protocol=https
install_authserver_protocol_http=1 install_authserver_protocol_https=0	install_authserver_protocol=http
install_authserver_protocol_http=0 install_authserver_protocol_https=1	install_authserver_protocol=https

- 7 To prevent the installation process from creating or configuring the database, specify `no` for `install_db_configure` and leave `install_db_create` blank.

For example:

```
# When to Configure DB?
# Allowable values:
#   during - Perform configuration during installation
#   after  - Perform configuration post install, via a generated SQL script
#   no     - Do not perform DB configuration
install_db_configure=no

# Create DB?
# If performing the DB configuration during installation,
# should the installer also create the database
# or should it use an existing database.
#
# Allowable values:
#   true  - Create the database.
#   false - Use an existing database.
install_db_create=
```

The installation process only needs the values for the databases under `#Database details`.

- 8 Save and close the file.

Running the Silent Installation

- 1 Log in as `root` on Linux server or an administrator on Windows server where you want to install Identity Governance.
- 2 Stop Tomcat. For examples, see [“Stopping, Starting, and Restarting Tomcat” on page 52](#).
- 3 Locate the sample `identity-governance-install-silent.properties` file, by default in the same directory as the installation scripts for Identity Governance.
- 4 (Conditional) In a non-clustered environment or when installing on the primary node, complete the following steps:
 - 4a In a text editor, open the `identity-governance-install-silent.properties` file.
 - 4b Specify the parameter values. For a description of the parameters, see [Step 7 on page 73](#).
 - 4c Save and close the file.

5 (Conditional) When installing on a secondary node in a cluster, you can create the `.properties` file using the steps in [“Creating a Silent Properties File for Installing on a Secondary Node” on page 80](#).

6 To launch the installation program, enter the following command:

- ♦ **Linux:** `./identity-governance-install-linux.bin -i silent -f path_to_silent_properties_file`
- ♦ **Windows:** From a command line, enter: `identity-governance-install-win.exe -i silent -f path_to_silent_properties_file`.

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.

7 When the installation process completes, continue to [Section 7, “Completing the Installation Process,” on page 97](#).

NOTE: Do **not** start Tomcat.

6 Installing Identity Reporting

Before you install Identity Reporting, you must decide if you want Identity Reporting to use the Identity Governance security module or the Identity Manager security module. For more information, see [“Understanding Identity Reporting” on page 30](#).

You can install Identity Reporting when you install Identity Governance, or you can install it at a later time. This chapter guides you through the process of installing the required components for running reports with the assumption that you do not intend to use Identity Reporting as part of an Identity Manager environment. For more information about installing reporting for Identity Manager, see:

- ♦ **Linux:** [“Planning to Install Identity Reporting”](#) in the *NetIQ Identity Manager Setup Guide for Linux*.
- ♦ **Windows:** [“Considerations for Installing Identity Manager Components”](#) in the *NetIQ Identity Manager Setup Guide for Windows*.

The Identity Reporting installation files are included with the Identity Governance installation program. By default, the installation program installs the components in the following location:

- ♦ **Linux:** `/opt/netiq/idm/apps/idrpt`
- ♦ **Windows:** `c:\netiq\idm\apps\idrpt`

It is important that you review the installation process before beginning.

- ♦ [“Checklist for Installing Identity Reporting” on page 83](#)
- ♦ [“Understanding the Installation Process for the Identity Reporting Components” on page 84](#)
- ♦ [“Preparing the Database Environment for Identity Reporting” on page 85](#)
- ♦ [“Installing Identity Reporting” on page 87](#)

Checklist for Installing Identity Reporting

It is important that you complete the steps in the following checklist.

	Checklist Items
<input type="checkbox"/>	1. Learn about the interaction among Identity Reporting components. For more information, see “Understanding Identity Reporting” on page 30 .
<input type="checkbox"/>	2. Decide which server you want to use for your Identity Reporting components. For more information, see “Recommended Installation Scenarios and Server Setup” on page 33 .
<input type="checkbox"/>	3. Review the considerations for installing Identity Reporting. For more information, see “Prerequisites for Identity Reporting” on page 40 .
<input type="checkbox"/>	4. Review the hardware and software requirements for the computer that will host Identity Reporting. For more information, see “Identity Reporting Server System Requirements” on page 43 .
<input type="checkbox"/>	5. Ensure that the server where you want to install Identity Reporting has the Tomcat application server. For more information, see Chapter 3, “Installing Tomcat, PostgreSQL, and ActiveMQ for Identity Governance,” on page 47 .

	Checklist Items
<input type="checkbox"/>	6. Ensure that you have a database to which the installation process can connect. For more information, see “Preparing the Database Environment for Identity Reporting” on page 85.
<input type="checkbox"/>	7. (Conditional) To use an Oracle database, ensure that the schema exists for the reporting user. For more information, see “Preparing an Oracle Database for Identity Governance” on page 67 and “Understanding the Users that the Installation Process Creates” on page 85.
<input type="checkbox"/>	8. Install Identity Reporting: <ul style="list-style-type: none"> ♦ For a guided installation, see “Using the Guided Process to Install Identity Reporting” on page 87. ♦ To install reporting silently, see “Installing Identity Reporting Silently” on page 94.
<input type="checkbox"/>	9. Complete the installation and setup for Identity Reporting. For more information, see the following sections: <ul style="list-style-type: none"> ♦ “Configuring the Identity Reporting Databases” on page 100 ♦ “Preparing Identity Reporting for Use” on page 314

Understanding the Installation Process for the Identity Reporting Components

You can install Identity Reporting and the reporting drivers on the same server. For more information, see [“Recommended Installation Scenarios and Server Setup” on page 33.](#)

- ♦ [“Understanding the Installation Process for Identity Reporting” on page 84](#)
- ♦ [“Understanding the Users that the Installation Process Creates” on page 85](#)

Understanding the Installation Process for Identity Reporting

The installation program for Identity Reporting performs the following functions:

- ♦ Deploys the client WAR file, which contains the user interface components for reporting, to the application server
- ♦ Deploys the core WAR file, which contains the core REST services needed for reporting
- ♦ Deploys the RPTDOC WAR file, which contains the documentation of REST services needed for reporting
- ♦ Installs, updates, or positions the JDBC driver that connects to the reporting database
- ♦ Configures the authentication services for Identity Reporting
- ♦ Configures the email delivery system for Identity Reporting
- ♦ Configures the core reporting services for Identity Reporting
- ♦ (Optional) Creates the user accounts for Identity Reporting

Understanding the Users that the Installation Process Creates

Identity Reporting requires a specific set of users and schema for each reporting database, which the installation program creates for you. The installation process uses the database administration credentials specified during the installation to create these users.

The following are the default names of these users:

User name	Description
postgres	Administrator of the PostgreSQL server
igrptuser	Has the credentials to access the report views and run the reports for Identity Governance
idm_rpt_cfg	Owns the reporting configuration data and the Identity Manager reporting views

Preparing the Database Environment for Identity Reporting

When using PostgreSQL, the installation process for Identity Reporting can create the `RPT` database. For MS SQL Server and Oracle, the installation process needs to connect to an existing, empty database. Create the database before installing Identity Reporting if you use MS SQL Server or Oracle for the reporting database platform.

- ♦ [“Preparing MS SQL Server” on page 85](#)
- ♦ [“Preparing Oracle” on page 86](#)
- ♦ [“Preparing PostgreSQL” on page 86](#)

Preparing MS SQL Server

If you are using MS SQL Server, you must provide the latest JDBC file and create a database for the installation program to use.

Obtaining the MS SQL Server JDBC File for the Application Server

To run queries against an MS SQL Server database, you must add an MS SQL Server JDBC file to the library for your application server. The installation program copies it there for you, but you must download and have the file ready during the installation.

- 1 Download the `sqljdbc42.jar` file from the Microsoft website.
- 2 Copy the file so that it is accessible during the installation.

Creating an MS SQL Server Database for Reporting

As a system administrator, create a database, such as `reporting`. Alternatively, you can allow the installation program to create a database for you. Specify an account for the database owner that the installation process can use. For more information, see [“Creating a Temporary MS SQL Server Database Administrator for the installation process” on page 72](#).

Preparing Oracle

If you are using Oracle, you must provide the latest JDBC file and create a database for the installation program to use.

Obtaining the Oracle JDBC File for the Application Server

To run queries against an Oracle database, you must add an Oracle JDBC file to the library for your application server. The installation program copies it there for you, but you must download and have the file ready during the installation.

- 1 Download the `ojdbc7.jar` file from the [Oracle website](#).
- 2 Copy the file so that it is accessible during the installation.

Creating an Oracle Database for Reporting

The schema names for Identity Reporting must be exactly as listed in the following procedure. This requirement means you can only have one instance of Identity Reporting within an Oracle database (SID). If you are going to have multiple environments of development, staging, and production, you can only have one Oracle server for all three environments with three separate SIDs for each instance.

Your database administrator can choose to create the schemas in the Identity Reporting database before you run the installation. Otherwise, the installation program can generate the schemas.

- 1 Install a supported version of Oracle.

For more information, see [“Database Server System Requirements” on page 43](#).

IMPORTANT: You must create the database (SID) in AL32UTF-8 (Unicode UTF-8 Universal character set) before installing Identity Reporting.

- 2 To prepare the database, complete the following steps:
 - 2a Create or identify the database that you want Identity Reporting to use.
 - 2b In the database, create the schema for `idm_rpt_cfg` with the `connect` privilege.
or
You can allow the installation program to create the schema for you.
 - 2c Specify a password for the schema.
- 3 When installing Identity Reporting, specify **Configure database now or at startup** if you want the installation program to generate the schema, tables, and views.

For more information about using SQL statements after installation, see [“Configuring the Databases after Installation” on page 97](#).

Preparing PostgreSQL

If you are using PostgreSQL, the installation program removes existing PostgreSQL JDBC jars and installs the latest PostgreSQL JDBC file. If you want to create the reporting database for the installation program to use, you can do that before installing reporting.

Creating a PostgreSQL Database for Reporting

As a Postgres administrator, create a database, such as `reporting`. Alternatively, you can allow the installation program to create a database for you. Specify an account for the database owner that the installation process can use. For more information, see [“Creating a Temporary PostgreSQL Database Administrator for the Installation Process” on page 66](#).

Installing Identity Reporting

This section describes the process for installing Identity Reporting if you did not install it when you installed Identity Governance.

- ♦ [“Using the Guided Process to Install Identity Reporting” on page 87](#)
- ♦ [“Installing Identity Reporting Silently” on page 94](#)

Using the Guided Process to Install Identity Reporting

This procedure describes how to install Identity Reporting for Identity Governance using an installation wizard, either in GUI format or from the console. To perform a silent, unattended installation, see [“Installing Identity Reporting Silently” on page 94](#).

To prepare for the installation, review the prerequisites and system requirements listed in [“Identity Reporting Server System Requirements” on page 43](#). Also see the Release Notes accompanying the release.

- 1 Log in as `root` on Linux server or an administrator on Windows server where you want to install Identity Reporting.

NOTE: Identity Reporting requires you to log in as `root` on Linux server or an administrator on Windows server to complete the installation successfully.

- 2 Stop Tomcat. For examples, see [“Stopping, Starting, and Restarting Tomcat” on page 52](#).
- 3 From the directory that contains the installation files, complete one of the following actions:

NOTE: To execute the file, you might need to use the `chmod +x` or `sh` command for Linux or log in to your Windows server as an administrator.

- ♦ **Linux:** Use the following commands for Linux:
 - ♦ **Console:** Enter `./identity-governance-install-linux.bin -i console`
 - ♦ **GUI:** Enter `./identity-governance-install-linux.bin`
 - ♦ **Windows:** Use the following commands for Windows:
 - ♦ **Console:** Enter `cmd /c "identity-governance-install-win.exe -i console"`
 - ♦ **GUI:** Double-click `identity-governance-install-win.exe`
- 4 Accept the License Agreement, and then select **Next**.
 - 5 Select the Identity Reporting install set.
 - 6 To complete the guided process, specify values for the following parameters:
 - ♦ **Select install location**
Specifies the location for the installation files.

- ◆ **Tomcat installation**

Represents the settings for the Tomcat installation that hosts Identity Governance. In a clustered environment, specify runtime values for each node where you install Identity Governance.

Specify the Tomcat folder

Specifies the path to the Tomcat installation. The installation process adds or modifies some files for Identity Governance to this folder. For example:

- ◆ **Linux:** `/opt/apache-tomcat-x.x.xx`
- ◆ **Windows:** `c:\path\to\tomcat-x.x.xx`

Runtime host name

Specifies the DNS name or IP address for the Tomcat installation.

Runtime port

Specifies the port that Tomcat uses to listen for communication from Identity Governance or the load balancers.

Runtime identifier

In a non-clustered environment, you can specify the local server name.

In clustered environment, specifies the unique name for the current node. For example, `node1` or `ProdNode1`. Do not use the server's name, which might change according to a DHCP assignment.

- ◆ **Tomcat Java Home**

Represents the path to the Oracle Java instance that Tomcat uses. The installation process adds some files for Identity Governance to the Tomcat home folder. For example:

- ◆ **Linux:** `/root/jdk1.x.x_xx`
- ◆ **Windows:** `c:\path\to\jdk1.x.x.xx`

- ◆ **Application address**

Represents the settings of the URL that users need to connect to Identity Reporting on the application server. For example, `https://myserver.mycompany.com:8443`.

NOTE: If OSP runs on a different instance of the application server, you must also select **Connect to an external authentication server** and specify values for the OSP server.

Protocol

Specifies whether you want to use `http` or `https`. To use SSL for communication, specify `https`.

Host name

Specifies the DNS name or IP address of the application server. Do not use `localhost`.

Port

Specifies the port that you want the application server to use for communication with Identity Governance.

Connect to an external authentication server

Specifies whether a different instance of the application server that hosts the authentication server (OSP). The authentication server contains the list of users who can log in to Identity Reporting.

If you select this setting, also specify values for the authentication server's **Protocol**, **Host name**, and **Port**.

- ◆ **Application address**

Applies only when the Identity Governance server location is unknown.

Represents the settings of the URL that users need to connect to the Identity Governance. For example, `https://myserver.mycompany.com:8443`.

Protocol

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

Host Name

Do not use `localhost`.

In a non-clustered environment, specifies the DNS name or IP address of the server hosting Identity Governance.

In a clustered environment, specifies the DNS name of the server that hosts the load balancer that you want to use. For more information about installing in a clustered environment, see [“Ensuring High Availability for Identity Governance” on page 37](#).

Port

Specifies the port that you want the server to use for communication with client computers. The default is 8080. To use SSL, the default is 8443.

When installing in a clustered environment, specify the port for the load balancer.

- ◆ **Authentication details**

Represents the requirements for connecting Identity Governance to the LDAP authentication server (for example, OSP) that contains the list of users who can log in to the application. For more information about the authentication server, see [“Understanding Authentication for Identity Governance” on page 27](#).

NOTE: In a clustered environment where the `osp.war` file resides behind the load balancer, specify the host and port for the load balancer’s server rather than the authentication server.

Service password

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

Protocol

Change this only when you choose to connect to an external authentication 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*.

Host

Change this only when you choose to connect to an external authentication server.

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

Port

Change this only when you choose to connect to an external authentication server.

Specifies the port that you want the LDAP authentication server or load balancer to use for communication with Identity Governance.

- ◆ **Database Type**

Specifies the platform you want to use for the Identity Governance and reporting databases.

For more information about supported versions, see [“Database Server System Requirements” on page 43](#).

◆ **Database details**

Represents the settings for the Identity Governance and reporting databases. For more information, see [“Understanding the Identity Governance and Reporting Databases” on page 31](#).

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

In a clustered environment, perform the configuration steps only on the primary node in the cluster. For more information about installing in a clustered environment, see [“Ensuring High Availability for Identity Governance” on page 37](#).

Configure database now

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

NOTE: Ensure that you specified the correct names for the existing databases.

Generate SQL for later

Specifies that you want to generate the SQL scripts that the database administrator can run in your database platform to create the databases and other artifacts.

The installation process stores the scripts in the following directory:

- ◆ **Linux:** /opt/netiq/idm/apps/idgov/sql
- ◆ **Windows:** c:\netiq\idm\apps\idgov\sql

If you are installing Identity Reporting at this time, the installation process stores the scripts in the following directory:

- ◆ **Linux:** /opt/netiq/idm/apps/idrpt/sql
- ◆ **Windows:** c:\netiq\idm\apps\idrpt\sql

For more information about using the files, see [Section 7, “Completing the Installation Process,” on page 97](#).

No database configuration

Specifies that you do not want to configure a new or existing database.

Use this setting when you install Identity Governance on a secondary node in the cluster. For more information, see [“Ensuring High Availability for Identity Governance” on page 37](#).

Host

Specifies the DNS name or the IP address of the server that hosts the Identity Governance databases.

Port

Specifies the port of the server that hosts the Identity Governance databases. The default values are 1433 for MS SQL Server, 1521 for Oracle and 5432 for PostgreSQL.

Microsoft SQL Server JDBC Jar

Applies only when using an MS SQL Server database

Specifies the path to the JAR file for the MS SQL Server JDBC driver. Microsoft provides this file.

Oracle JDBC Jar

Applies only when using an Oracle database

Specifies the path to the JAR file for the Oracle JDBC driver. For example: /.

- ♦ **Linux:** opt/oracle/ojdbc7.jar
- ♦ **Windows:** c:\ProgramFiles\Oracle\ojbc7.jar

Oracle provides the driver JAR file, which represents the Thin Client JAR for the database server.

Database name

Applies only when using an Oracle database

Specifies the name of the database to which you want to add the Identity Governance databases. For example, Orclidentitygovernance.

User tablespace

Applies only when using an Oracle database

Specifies the name of the database storage unit for storing the schema for the Identity Governance databases. The default is USERS.

Temporary tablespace

Applies only when using an Oracle database

Specifies the name of the temporary database storage unit for storing the schema. The default is TEMP.

Operations

Specifies the name of the database that stores operations data for Identity Governance. The default value is igops.

NOTE: If you created a blank database for the operations data, ensure that you specify the exact name of the existing, empty database.

Data collection

Specifies the name of the database that stores data collection information for Identity Governance. The default value is igdcs.

NOTE: If you created a blank database for the data collection information, ensure that you specify the exact name of the existing, empty database.

Workflow

Specifies the name of the database that stores workflow information for Identity Governance. The default value is igwf.

NOTE: If you created a blank database for the workflow data, ensure that you specify the exact name of the existing, empty database.

Analytics

Specifies the name of the database that stores analytics information for Identity Governance. The default value is igara.

NOTE: If you created a blank database for the analytics data, ensure that you specify the exact name of the existing, empty database.

Password (for database owners)

Specifies the password for the database account administrator that can create database tables, views, and other artifacts in the Identity Governance databases.

Reporting user

Specifies the account for a database user that has rights to the views related to reporting for Identity Governance. The default value is `igrptuser`.

The installation process creates this account if you select **Configure database now** and **Update** (rather than **Use only existing**).

Reporting user password

Specifies the password for the reporting administrator.

Administrator user

Specifies the account for a database administrator that the installation process can use to configure the databases for Identity Governance.

WARNING: Do not use the default database administrator account (`idmadmin`) if that account was created when you installed PostgreSQL and Tomcat.

Administrator password

Specifies the password for the database administrator.

Update / Use only existing

Applies only when you choose to configure the database during the installation.

Specifies whether you want to have the installation process migrate or create new databases or use existing, empty databases. Select **Update** if you are installing or upgrading Identity Governance.

NOTE: To use existing databases, the installation program drops known tables and views within each schema and then adds the needed tables and views that it needs for the current version.

- ◆ **Report default language**

Specifies the language that you want to use for Identity Reporting.

Target locale

Specifies the locale. Default selection is English.

- ◆ **Report email delivery**

Represents the settings for the SMTP server that sends report notifications. To modify these settings after installation, use the configuration utility for Identity Governance.

Default email address

Specifies the email address that you want Identity Reporting to use as the origin for email notifications.

SMTP server

Specifies the IP address or DNS name of the SMTP email host that Identity Reporting uses for notifications. Do not use `localhost`.

SMTP server port

Specifies the port number for the SMTP server. The default value is 465.

Use SSL for SMTP

Specifies whether you want to use SSL protocol for communication with the SMTP server.

Require server authentication

Specifies whether you want to use authentication for communication with the SMTP server.

If you select this setting, also specify the credentials for the email server.

SMTP user name

*Applies only when you select **Requires server authentication**.*

Specifies the name of a login account for the SMTP server.

SMTP password

*Applies only when you select **Requires server authentication**.*

Specifies the password of a login account for the SMTP server.

♦ **Report retention details**

Represents the settings for maintaining completed reports.

Keep finished reports for

Specifies the amount of time that Identity Reporting will retain completed reports before deleting them. For example, to specify six months, enter 6 and then select **Month**.

Location of report definitions

Specifies a path where you want to store the report definitions. For example:

- ♦ **Linux:** /opt/netiq/IdentityReporting
- ♦ **Windows:** c:\netiq\IdentityReporting

♦ **Identity Audit**

Represents the settings for collecting auditing events that occur in the Identity Governance server. For more information, see [“Enabling Auditing” on page 106](#).

Enable auditing

Specifies whether you want to send Identity Governance log events to an auditing server.

If you select this setting, also specify the audit server details.

Audit server

Applies only when you enable identity auditing.

Specifies the IP address or DNS name of the audit server.

Audit port

Applies only when you enable identity auditing.

Specifies the port to use for sending log events to the audit server.

Audit cache location

Applies only when you enable identity auditing.

Specifies the location of the cache directory on the Identity Governance server that you want to use to store log events. For example:

- ♦ **Linux:** /opt/netiq/idm/apps/audit
- ♦ **Windows:** C:\netiq\idm\apps\audit

Secure layer

Applies only when you enable identity auditing.

Specifies whether to use TLS (TCP using SSL). If not selected, events are sent using TCP.

Trust store location

Applies only when you want to use TLS for audit events.

Specifies the path to the keystore file location for trusting the audit server certificate.
For example:

- ♦ **Linux:** `/opt/netiq/idm/apps/jre/lib/security/cacerts`
- ♦ **Windows:** `C:\netiq\idm\apps\jre\lib\security\cacerts`

Trust store password

Applies only when you want to use TLS for audit events.

Specifies the password for the trust store file.

Test certificate trust

Applies only when you want to use TLS for audit events.

Specifies whether to attempt to connect to the audit server and trust the retrieved certificate within a copy of the trust store file. The actual trust occurs during the installation process.

NOTE: Attempting a TLS connection on a TCP port results in a timeout after 5 seconds. Be sure to specify a secure audit port if you select to use TLS.

- 7 Review the information in the Pre-Installation Summary window, and then select **Install**.
- 8 When the installation process completes, continue to [Section 7, “Completing the Installation Process,” on page 97](#).

Installing Identity Reporting Silently

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. You can run the silent installation after editing the file to customize the installation process for your environment. To perform a guided installation, see [“Using the Guided Process to Install Identity Reporting” on page 87](#).

To prepare for the installation, review the prerequisites and system requirements listed in [“Identity Reporting Server System Requirements” on page 43](#). Also see the Release Notes accompanying the release.

- 1 Log in as `root` on Linux server or an administrator on Windows server where you want to install Identity Reporting.
- 2 (Conditional) To avoid specifying passwords for the installation in the silent properties file for a silent installation, use the `export` or `set` command. For example:

```
export install_db_reporting_secret=myPassWord
```

The silent installation process reads the passwords from the environment, rather than from the silent properties file.

Specify the following passwords:

Database users

The installation program creates the user `idm_rpt_cfg` for the reporting schema.

The following are the default administrators installed with your database:

- ♦ **MS SQL Server:** `sa`
- ♦ **Oracle:** `SYSTEM`
- ♦ **PostgreSQL:** `postgres`

install_db_admin_secret

Specify the password for the administrator for the reporting database.

install_db_reporting_secret

Specify the password for `idm_rtp_cfg` which is used internally to support report administration during runtime.

install_smtp_password_auth_user

(Conditional) To use authentication for email communications, specify the password for the default SMTP email user.

install_authserver_client_secret

Specify the client ID password for authenticating using OSP.

install_truststore_secret

(Conditional) Applies only when you are using secure communications.

Specify the password for the trust store.

- 3 To specify the installation parameters, complete the following steps:
 - 3a Locate the sample `identity-governance-install-silent.properties` silent properties file, by default in the same directory as the installation scripts for Identity Governance.
 - 3b In a text editor, open the silent properties file.
 - 3c Specify the parameter values. For a description of the parameters, see [Step 6 on page 87](#).
 - 3d Save and close the file.
- 4 Stop the application server, such as Tomcat. For examples, see [“Stopping, Starting, and Restarting Tomcat” on page 52](#).
- 5 To launch the installation process, enter the following command:
 - ♦ **Linux:** `./identity-governance-install-linux.bin -i silent -f path_to_silent_properties_file`
 - ♦ **Windows:** From a command line enter: `identity-governance-install-win.exe -i silent -f path_to_silent_properties_file`

NOTE: If the silent properties file resides 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.

- 6 When the installation process completes, continue to [Section 7, “Completing the Installation Process,” on page 97](#).

7 Completing the Installation Process

After performing a guided or silent installation, you must initialize Identity Governance and verify that you can log in to the product as the bootstrap administrator. In a cluster, ensure that the Tomcat configuration file on each node specifies a unique runtime identifier.

- ♦ [“Configuring the Databases after Installation” on page 97](#)
- ♦ [“Preparing One SSO Provider for Use” on page 101](#)
- ♦ [“Completing the Cluster Configuration for Identity Governance” on page 103](#)
- ♦ [“Ensuring Rapid Response to Authentication Requests” on page 105](#)
- ♦ [“Enabling Auditing” on page 106](#)
- ♦ [“Starting and Initializing Identity Governance” on page 110](#)
- ♦ [“Configuring Identity Governance for Two-Factor Authentication” on page 112](#)
- ♦ [“Updating the License Key” on page 116](#)

Configuring the Databases after Installation

During the installation process, you might have specified **Generate SQL for later** to configure the databases or schema after installation. Your database administrator needs to run the SQL scripts that the installation created to populate the databases. For PostgreSQL, the administrator also needs to create the roles for the Identity Governance databases. For MS SQL, the administrator also needs to create the logins, users, and roles for the Identity Governance databases. If you selected **Configure Database Now** during the installation, you can skip this section.

Identity Governance needs the following SQL scripts, located by default in:

- ♦ **Linux:** `/opt/netiq/idm/apps/idgov/sql`
- ♦ **Windows:** `c:\netiq\idm\apps\idgov\sql`

These are files for the specific database or schema:

- ♦ `ops-init.sql` for the `igops` database or schema
- ♦ `dcs-init.sql` for the `igdcs` database or schema
- ♦ `wf-init.sql` for the `igwf` database or schema
- ♦ `ara-init.sql` for the `igara` database or schema

To configure the Identity Governance and Identity Reporting databases, see the following sections:

- ♦ [“Configuring the PostgreSQL Databases for Identity Governance” on page 98](#)
- ♦ [“Configuring the Oracle Database for Identity Governance” on page 99](#)
- ♦ [“Configuring the MS SQL Database for Identity Governance” on page 100](#)
- ♦ [“Configuring the Identity Reporting Databases” on page 100](#)

Configuring the PostgreSQL Databases for Identity Governance

The database administrator must create the appropriate roles in the database for Identity Governance. The database administrator or database owners must run the SQL scripts that the installation program generated. It is best practice to have the database administrator review the SQL scripts. Also, you must populate the global configuration values in the database.

NOTE: You must create the roles with the `igops`, `igdcs`, `igwf`, and `igara` database passwords rather than the database administrator password.

- 1 To populate the user schema in the database, have the database administrator run a command similar to the following:

```
CREATE ROLE operations_db_name LOGIN password 'password';
CREATE ROLE data_collection_db_name LOGIN password 'password';
CREATE ROLE workflow_db_name LOGIN password 'password';
CREATE ROLE analytics_db_name LOGIN password 'password';
CREATE ROLE ig_report_role NOLOGIN;
CREATE DATABASE igops WITH OWNER = operations_db_name ENCODING = 'UTF8';
CREATE DATABASE igdcs WITH OWNER = data_collection_db_name ENCODING = 'UTF8';
CREATE DATABASE igwf WITH OWNER = workflow_db_name ENCODING = 'UTF8';
CREATE DATABASE igara WITH OWNER = analytics_db_name ENCODING = 'UTF8';
```

For example:

```
CREATE ROLE igops LOGIN PASSWORD 'netiq';
CREATE ROLE igdcs LOGIN PASSWORD 'netiq';
CREATE ROLE igwf LOGIN PASSWORD 'netiq';
CREATE ROLE igara LOGIN PASSWORD 'netiq';
CREATE ROLE ig_report_role NOLOGIN;

CREATE DATABASE igops WITH OWNER = igops ENCODING = 'UTF8';
CREATE DATABASE igdcs WITH OWNER = igdcs ENCODING = 'UTF8';
CREATE DATABASE igwf WITH OWNER = igwf ENCODING = 'UTF8';
CREATE DATABASE igara WITH OWNER = igara ENCODING = 'UTF8';
```

- 2 Have the database administrator run the SQL scripts to create and configure the Identity Governance databases. These are located by default in the following directory:

- ♦ **Linux:** `/opt/netiq/idm/apps/idgov/sql`
- ♦ **Windows:** `c:\netiq\idm\apps\idgov\sql`

- 3 (Optional) To use non-default settings, change the owner and the database name.

```
"/opt/netiq/idm/apps/jre/bin/java" -Djava.util.logging.config.file="/opt/netiq/idm/apps/idgov/conf/logging.properties" -Dcom.netiq.ism.config="/opt/netiq/idm/apps/idgov/conf/unused.props" -classpath "/opt/netiq/idm/apps/idgov/lib/ig-configutil.jar":"/opt/netiq/idm/apps/idgov/lib/postgresql-42.1.4.jar" com.netiq.iac.config.util.IacConfigUtil -dbDriver org.postgresql.Driver -dbUser igops -dbPassword %igops-password% -dbUrl "jdbc:postgresql://%server%:%port%/igops" -script "/opt/netiq/idm/apps/idgov/scripts/import-configs.script"
```

- 4 To populate the global configuration values in the database, enter the following command:

```
"/opt/netiq/idm/apps/jre/bin/java" -Djava.util.logging.config.file="/opt/
netiq/idm/apps/idgov/conf/logging.properties" -Djava.security.egd=file:///dev/
urandom -Dcom.netiq.ism.config="/opt/netiq/idm/apps/idgov/conf/unused.props" -
classpath "/opt/netiq/idm/apps/idgov/lib/ig-configutil.jar":"/opt/netiq/idm/
apps/idgov/lib/ojdbc.jar" com.netiq.iac.config.util.IacConfigUtil -dbDriver
oracle.jdbc.OracleDriver -dbUser %igops-user% -dbPassword %password% -dbUrl
"jdbc:oracle:thin:@%oracle-server%:%port%/%sid%" -script "/opt/netiq/idm/apps/
idgov/scripts/import-configs.script"
```

For example:

```
"/opt/netiq/idm/apps/jre/bin/java" -Djava.util.logging.config.file="/opt/
netiq/idm/apps/idgov/conf/logging.properties" -Dcom.netiq.ism.config="/opt/
netiq/idm/apps/idgov/conf/unused.props" -classpath "/opt/netiq/idm/apps/idgov/
lib/ig-configutil.jar":"/opt/netiq/idm/apps/idgov/lib/postgresql-42.1.4.jar"
com.netiq.iac.config.util.IacConfigUtil -dbDriver org.postgresql.Driver -
dbUser igops -dbPassword netiq -dbUrl "jdbc:postgresql://localhost:5432/igops"
-script "/opt/netiq/idm/apps/idgov/scripts/import-configs.script"
```

Configuring the Oracle Database for Identity Governance

Your database administrator must run the SQL scripts to create the tables and views. Also, you must populate the global configuration values in the database.

- 1 (Conditional) If you chose to generate SQL scripts, complete the following steps:

- 1a Locate the scripts for each schema to create the tables and views.

The scripts are located by default in the following default directory:

- ♦ **Linux:** /opt/netiq/idm/apps/idgov/sql
- ♦ **Windows:** c:\netiq\idm\app\idgov\sql

- 1b To run the scripts, have the database administrator copy the SQL files where they can be run directly on the database.

- 2 To populate the global configuration values in the database, enter the following command:

```
"/opt/netiq/idm/apps/jre/bin/java" -Djava.util.logging.config.file="/opt/
netiq/idm/apps/idgov/conf/logging.properties" -Djava.security.egd=file:///dev/
urandom -Dcom.netiq.ism.config="/opt/netiq/idm/apps/idgov/conf/unused.props" -
classpath "/opt/netiq/idm/apps/idgov/lib/ig-configutil.jar":"/opt/netiq/idm/
apps/idgov/lib/ojdbc.jar" com.netiq.iac.config.util.IacConfigUtil -dbDriver
oracle.jdbc.OracleDriver -dbUser %igops-user% -dbPassword %password% -dbUrl
"jdbc:oracle:thin:@%oracle-server%:%port%/%sid%" -script "/opt/netiq/idm/apps/
idgov/scripts/import-configs.script"
```

NOTE: This commands contains the default installation path of /opt/netiq/idm/apps.

For example:

```
"/opt/netiq/idm/apps/jre/bin/java" -Djava.util.logging.config.file="/opt/
netiq/idm/apps/idgov/conf/logging.properties" -Djava.security.egd=file:///dev/
urandom -Dcom.netiq.ism.config="/opt/netiq/idm/apps/idgov/conf/unused.props" -
classpath "/opt/netiq/idm/apps/idgov/lib/ig-configutil.jar":"/opt/netiq/idm/
apps/idgov/lib/ojdbc.jar" com.netiq.iac.config.util.IacConfigUtil -dbDriver
oracle.jdbc.OracleDriver -dbUser igops -dbPassword netiq -dbUrl
"jdbc:oracle:thin:@myoracle.mycompany.com:1521/mysid" -script "/opt/netiq/idm/
apps/idgov/scripts/import-configs.script"
```

Configuring the MS SQL Database for Identity Governance

The database administrator must create the appropriate logins, users, and roles in the database for Identity Governance. The database administrator or database owners must run the SQL scripts that the installation program generated. It is best practice to have the database administrator review the SQL scripts. Also, you must populate the global configuration values in the database.

NOTE: You must create the roles with the `igops`, `igdc`s, `igwf`, and `igara` database passwords rather than the database administrator password.

- 1 Create the appropriate logins, users, and roles in the database.
- 2 Have the database administrator run the SQL scripts to create and configure the Identity Governance databases. These are located by default in the following directory:
 - ♦ **Linux:** `/opt/netiq/idm/apps/idgov/sql`
 - ♦ **Windows:** `c:\netiq\idm\apps\idgov\sql`
- 3 To populate the global configuration values in the database, enter the following command:

```
"/opt/netiq/idm/apps/jre/bin/java" -Djava.util.logging.config.file="/opt/netiq/idm/apps/idgov/conf/logging.properties" -Dcom.netiq.ism.config="/opt/netiq/idm/apps/idgov/conf/unused.props" -classpath "/opt/netiq/idm/apps/idgov/lib/ig-configutil.jar":"/opt/netiq/idm/apps/idgov/lib/msjdbcm.jar" com.netiq.iac.config.util.IacConfigUtil -dbDriver com.microsoft.sqlserver.jdbc.SQLServerDriver -dbUser igops -dbPassword %igops-password% -dbUrl "jdbc:sqlserver://%server%:%port%;databaseName=igops" -script "/opt/netiq/idm/apps/idgov/scripts/import-configs.script"
```

For example:

```
"/opt/netiq/idm/apps/jre/bin/java" -Djava.util.logging.config.file="/opt/netiq/idm/apps/idgov/conf/logging.properties" -Dcom.netiq.ism.config="/opt/netiq/idm/apps/idgov/conf/unused.props" -classpath "/opt/netiq/idm/apps/idgov/lib/ig-configutil.jar":"/opt/netiq/idm/apps/idgov/lib/msjdbcm.jar" com.netiq.iac.config.util.IacConfigUtil -dbDriver com.microsoft.sqlserver.jdbc.SQLServerDriver -dbUser igops -dbPassword netiq -dbUrl "jdbc:sqlserver://myserver.netiq.com:1433;databaseName=igops" -script "/opt/netiq/idm/apps/idgov/scripts/import-configs.script"
```

Configuring the Identity Reporting Databases

If you chose **Generate SQL for later** during installation, have the database administrator run the SQL script to configure the Identity Reporting database. The script is located by default in the following directory:

- ♦ **Linux:** `/opt/netiq/idm/apps/idrpt/sql`
- ♦ **Windows:** `c:\netiq\idm\apps\idrpt\sql`

If you cannot access the SQL scripts, see [“Manually Generating the Database Schema” on page 313](#).

Preparing One SSO Provider for Use

In some installation scenarios, you must take additional steps to prepare OSP for use with Identity Governance. For example, running OSP in an environment without Identity Manager or using Active Directory as your LDAP authentication server require some additional steps. Also, if you did not enable auditing during the installation process, you must run some additional steps.

- ♦ “Ensuring the Configuration Update Utility Can Run OSP” on page 101
- ♦ “Preparing OSP to Use an Active Directory LDAP Server” on page 102
- ♦ “Enabling Auditing for the OSP after the Installation” on page 103

Ensuring the Configuration Update Utility Can Run OSP

When you run OSP on a different Tomcat server than Identity Governance, and you do not have Identity Manager in your environment, you must ensure that the OSP Configuration Update utility has the appropriate values to run OSP. The OSP Configuration Update utility (`configupdate.sh` or `configupdate.bat`) contains the settings that allow OSP to function and it is a separate utility from the Configuration Update utility for Identity Governance. After installing Identity Governance, you must update several settings in both utilities. see “SSO Clients Parameters” in the *NetIQ Identity Manager Setup Guide for Linux*.

- 1 Create a backup copy of the `ism-configuration.properties` file.
 - ♦ **Linux:** Default location in `/opt/netiq/idm/apps/tomcat/conf`
 - ♦ **Windows:** Default location in `C:\opt\netiq\idm\apps\tomcat\conf`
- 2 In a text editor, open the `configupdate.sh.properties` or `configupdate.bat.properties` to update values.
 - ♦ **Linux:** Default location in `/opt/netiq/idm/apps/osp/bin`
 - ♦ **Windows:** Default location in `c:\netiq\idm\apps\osp\bin`
- 2a In the file, modify the properties to the following values:
 - ♦ Change `is_prov` to `false`
 - ♦ (Conditional) Change `use_ssl` to `false`, if your LDAP server is not set up for SSL communication
 - ♦ (Option) Change `use_console` to `true`, if you want to run the utility in console mode, otherwise change `use_console` to `false` for opening in the console in GUI mode
- 2b Save and close the file.
- 3 Update settings in the OSP Configuration Update utility.
 - 3a Launch the Configuration Update utility.
 - ♦ **Linux:** Default location in the `/opt/netiq/idm/apps/osp/bin`
`./configupdate.sh edition=none`
 - ♦ **Windows:** Default location in `C:\netiq\idm\apps\osp\bin`
`configupdate.bat edition=none`

NOTE: Adding `edition=none` on the command line avoids needing to modify this value within `configupdate.sh.properties` or the `configupdate.bat.properties` file. It also avoids certain unnecessary fields which the config update utility would otherwise require values for in order to save.

3b Select **SSO Clients**.

3c Under **Reporting**, specify values for the following parameters:

NOTE: Regardless whether you use Identity Reporting, the utility requires values in these fields.

- ♦ **OAuth client ID**

For example, `rpt`.

- ♦ **OAuth client secret**

- ♦ **URL link to landing page**

For example, `http://123.456.78.90:8180/#/landing`

- ♦ **URL link to Identity Governance**

For example, `http://123.456.78.90:8080/#/nav`

- ♦ **OSP OAuth redirect url**

For example, `http://123.456.78.90:8180/IDMRPT/oauth.html`

3d Under **DCS Driver**, specify values for the following parameters:

NOTE: Regardless whether you use Identity Reporting, the utility requires values in these fields.

- ♦ **OAuth client ID**

For example, `dcdriver`.

- ♦ **OAuth client secret**

3e To save your changes, select **OK**.

3f Update the settings for **Identity Vault** and **Authentication**, as needed.

Preparing OSP to Use an Active Directory LDAP Server

To use Active Directory for your LDAP authentication server, you need to update the settings using the OSP Configuration Update utility and in the Identity Governance configuration utility.

- 1 Ensure that you have prepared the Configuration Update utility for OSP. For more information, see [“Ensuring the Configuration Update Utility Can Run OSP” on page 101](#).
- 2 Stop Tomcat, if it is running. For examples, see [“Stopping, Starting, and Restarting Tomcat” on page 52](#).
- 3 Update settings in the Configuration Update utility.

3a Launch the Configuration Update utility.

- ♦ **Linux:** Default location in the `/opt/netiq/idm/apps/osp/bin`

`./configupdate.sh edition=none`

- ♦ **Windows:** Default location in `C:\netiq\idm\apps\osp\bin`

`configupdate.bat edition=none`

NOTE: Adding `edition=none` on the command line avoids needing to modify this value within `configupdate.sh.properties` or `configupdate.bat.properties` file. It also avoids certain unnecessary fields which the config update utility would otherwise require values for in order to save.

- 3b Select **Reporting > Identity Vault Settings > Identity Vault User Identity > Login Attribute**.
- 3c For **Login Attribute**, specify the attribute in Active Directory that you want to use for logging in to Identity Governance. For example, `sAMAccountName`.

NOTE: This value is case-sensitive.

- 3d To save your change, select **OK**.
- 4 Update settings in the Identity Governance Configuration utility:
 - 4a Launch the Identity Governance Configuration utility.
 - ♦ **Linux:** Default location in `/opt/netiq/idm/apps/idgov/bin`

`./configutil -password database_password`
 - ♦ **Windows:** Default location in `c:\netiq\idm\apps\idgov\bin`

`configutil -password database_password`
 - 4b Select **Security Settings**.
 - 4c For **Auth Matching Rules**, add the same attribute from Active Directory that you specified for **Login Attribute** in [Step 3c](#).

Do not delete `dn`. For example, the setting should now list `dn` and `sAMAccountName`.
 - 4d Select **Save**.
- 5 Continue with the post-installation tasks, as required.

Enabling Auditing for the OSP after the Installation

If during the OSP installation process you did not enable auditing, you can enable it at anytime. For more information, see [“Enabling Auditing for OSP after the Installation” on page 109](#).

Completing the Cluster Configuration for Identity Governance

The Tomcat cluster needs to know the unique runtime identifier for each node. Also, to use ActiveMQ in a Tomcat cluster, Identity Governance needs the host name or IP address and port for each ActiveMQ server.

- ♦ [“Configuring the Nodes in the Tomcat Cluster” on page 103](#)
- ♦ [“Configuring ActiveMQ Failover in the Tomcat Cluster” on page 104](#)
- ♦ [“Cleaning Up Unfinished Data Production Jobs” on page 105](#)

Configuring the Nodes in the Tomcat Cluster

To run Identity Governance in a Tomcat cluster, each node in the cluster must have a unique runtime identifier. Also, the Tomcat instance should run on the same port as the port exposed by the load balancer. However, the instance might need to use a different port.

NOTE: It is possible for two clustered nodes to simultaneously attempt to claim a data processing task. When this occurs, one of the nodes will report a “stale object” exception, which you can ignore since the work will still be carried out.

For more information, see [“Ensuring High Availability for Identity Governance” on page 37](#).

- 1 Stop Tomcat, if the application server is running. For examples, see [“Stopping, Starting, and Restarting Tomcat” on page 52](#).
- 2 To specify a unique runtime identifier, complete the following steps:
 - 2a Log in to primary node in the cluster.
 - 2b In a text editor, open the `ism-configuration.properties` file.
 - ♦ **Linux:** Default location in `/opt/netiq/idm/apps/tomcat/conf`
 - ♦ **Windows:** Default location in `c:\netiq\idm\apps\tomcat\conf`
 - 2c Ensure that `com.netiq.iac.runtime.id` is a unique value that represents the node.
For example, `node1` or `ProdNode1`.
 - 2d Save and close the file.
 - 2e Repeat this procedure for each node in the cluster.
- 3 To specify a different port for a node than the port exposed by the load balancer, complete the following steps:
 - 3a Log in to the node where you want to change the port.
 - 3b In a text editor, open the `ism-configuration.properties` file.
 - ♦ **Linux:** Default location in `/opt/netiq/idm/apps/tomcat/conf`
 - ♦ **Windows:** Default location in `c:\netiq\idm\apps\tomcat\conf`
 - 3c For `com.netiq.iac.url.local.port`, specify the Tomcat port for the local node.
 - 3d Save and close the file.

Configuring ActiveMQ Failover in the Tomcat Cluster

To represent the host name and port for the ActiveMQ server, the installation process creates the **JMS broker URI** parameter in the Identity Governance Configuration Utility. This parameter has a `tcp://` prefix by default. However, in a clustered environment, the parameter needs a `failover` prefix and a comma-separated list of the ActiveMQ hosts.

For more information, see the ActiveMQ documentation, such as [The Failover Transport](#) and [Introduction to Master/Slave](#).

- 1 For each instance of Identity Governance, run the Identity Governance Configuration utility. The default installation location is .
 - ♦ **Linux:** Default location in `/opt/netiq/idm/apps/idgov/bin/`
 - ♦ **Console mode:** `./bin/configutil.sh -password db_password -console`
 - ♦ **GUI mode:** `./bin/configutil.sh -password db_password`
 - ♦ **Windows:** Default location in `c:\netiq\idm\apps\idgov\bin\`
 - ♦ **Console mode:** `configutil.bat -password db_password -console`
 - ♦ **GUI mode:** `configutil.bat -password db_password`

For more information, see [“Running the Identity Governance Configuration Utility” on page 129](#).

- 2 Select **Workflow Settings**.
- 3 (Conditional) Select **Enable persistent notification message queue** to ensure guaranteed message delivery.

If you specified ActiveMQ during installation, this setting should already be enabled.

- 4 For **JMS broker URI**, add `failover:` to the prefix, then add the host name or IP address and port for each ActiveMQ server.

Use commas to separate the server values. For example:

```
failover:tcp://amq1.mycompany.com:61616,tcp://amq2.mycompany.com:61616
```

- 5 Save the changes then close the utility.

Cleaning Up Unfinished Data Production Jobs

When running IG in a clustered environment, a node could go down while a data production job is running on it. In some configurations, these jobs could become orphaned processes that do not complete. When this happens, you might need to clean up these processes to ensure health and performance of your system.

Data production jobs are tied to specific runtime instances, identified by their `runtime_identifier`. Do not use a hostname or other identifier that might change if a runtime instance is restarted so that jobs do not become orphaned. When you start a new instance and control the identifier it is using, you can use a previously used identifier to make sure IG can clean up jobs correctly. If you do not have an option to start a new node with the same identifier, you can reassign data production jobs through the following manual process.

- 1 Find the node identifier from the local configuration property file on a node. Look for the line `property key is:` to locate the identifier.
- 2 Run a SQL statement against the arops database to retrieve the production records you want to clean up. For example:

```
select * from data_production where runtime_identifier = '<node runtime identifier>' and status != 'COMPLETED' and status != 'ERROR'
```

- 3 For each production record from the SQL statement results do the following:
 - 3a Execute a REST API call `GET /dataprod/mgt/id` using the production ID.
 - 3b Modify the payload by setting the runtime identifier in the payload to the node identifier where you want to reassign the production process.
 - 3c Execute a REST API call `PUT /dataprod/mgt/id` using the production ID and modified payload from step 3b.

Ensuring Rapid Response to Authentication Requests

You can configure OSP so users can log in with an email address or another attribute available in the LDAP authentication server. If you use a non-default attribute, the server might take longer to respond to authentication requests, particularly when running workflows for a review definition. Also, OSP automatically times out LDAP connections after 15 seconds. To ensure a rapid response time, the LDAP authentication server should have an index for the login attribute. If using Identity Governance with Identity Manager, you also must specify that attribute in the RBPM Configuration Utility.

NOTE: Active Directory automatically creates an index for the "mail" attribute.

- 1 If using with Identity Manager, to specify the login attribute, complete the following steps:
 - 1a Run the RBPM Configuration utility.

For more information, see “[Planning to Install Identity Applications](#)” in the *NetIQ Identity Manager Setup Guide for Linux*.

1b Select **Authentication > Show Advanced Options**.

For more information, see “[Authentication Configuration](#)” in the *NetIQ Identity Manager Setup Guide for Linux*.

1c For **Duplicate resolution naming attribute**, specify the attribute that you want to use for login activities. For example, Internet Email Address.

1d Save your changes.

2 (Conditional) If using with Identity Manager, to create an index for the login attribute in eDirectory, complete the following steps:

2a Create the index.

For more information, see “[Creating an Index](#)” in the *NetIQ eDirectory Administration Guide*.

2b For the attribute, select the same attribute that you specified for **Duplicate resolution naming attribute** in the configuration utility.

2c For the index rule, specify **Value**.

2d Complete the process for creating the index.

Enabling Auditing

You can enable auditing during the installation of Identity Governance or you can enable auditing any time after you have installed Identity Governance. If you have enabled auditing during the installation, you can also increase the level of audit information gathered by editing the `ig-server.logging.xml` file.

Identity Governance provides auditing for the following components:

- ♦ Identity Governance
- ♦ Identity Reporting
- ♦ OSP

Identity Governance allows you audit the different services it provides by enabling auditing for the specific service. Identity Governance uses REST calls for auditing. You must use the following information to enable auditing for the different components.

- ♦ “[Enabling Auditing for Identity Governance](#)” on page 106
- ♦ “[Enabling Auditing for Identity Reporting](#)” on page 108
- ♦ “[Enabling Auditing for OSP after the Installation](#)” on page 109

Enabling Auditing for Identity Governance

Use the following information to enable auditing for Identity Governance. The steps for enabling auditing are the same whether you installed Identity Governance and Identity Reporting on the same server or different servers.

1 If you enabled auditing during the install, proceed to [Step 5](#).

or

If you want to enable auditing after the installation, proceed to [Step 2](#).

2 Create an audit directory to store the audit information.

- ♦ **Linux:** /opt/netiq/idm/apps/audit
- ♦ **Windows:** C:\netiq\idm\apps\audit

3 (Optional) Create the Identity Governance log file if it does not exist.

- ♦ **Linux:** /opt/netiq/idm/apps/audit/ig-server
- ♦ **Windows:** C:\netiq\idm\apps\audit\ig-server

4 (Linux only) Assign ownership to the audit directory.

```
chown -R novlua.users /opt/netiq/idm/apps/audit
```

NOTE: The novlua.users is the same ownership as the tomcat directory. It allows the Tomcat service to modify files within the audit logs directory.

5 Modify the Identity Governance logging file to enter the syslog server information.

5a Open the logging file in a text editor.

- ♦ **Linux:** /opt/netiq/idm/apps/tomcat/conf/ig-server-logging.xml
- ♦ **Windows:** C:\netiq\idm\apps\tomcat\conf\ig-server-logging.xml

5b Make the following changes specific for your syslog server:

```
<enabled>true</enabled>
<protocol>TCP/TLS</protocol>
<host>123.456.78.90</host>
<port>6514</port>
<cache-dir>/opt/netiq/idm/apps/audit</cache-dir>
<cache-file>ig-server</cache-file>
<application>Identity Governance</application>
<vendor>Micro Focus</vendor>
<version>3.0</version>
```

NOTE: To disable auditing, ensure that the <enabled> line is set to false. For example:

```
<enabled>>false</enabled>
```

6 Modify the Identity Governance logging file ig-server-logging.xml to enabling auditing for each specific service.

- ♦ **Linux:** /opt/netiq/idm/apps/tomcat/conf/ig-server-logging.xml
- ♦ **Windows:** C:\netiq\idm\apps\tomcat\conf\ig-server-logging.xml

6a In a text editor change each Identity Governance service you want to audit from OFF to INFO. Instead of INFO, you can set the value to DEBUG, TRACE, or ALL.

There are currently 46 available services listed in the ig-server.logging.xml file that you can enable for the auditing service.

6b (Optional) You can also filter the Audit Logger for REST services by HTTP method, by adding the method to the end of the logger name. This enables more finely-grained auditing of updates for example (PUT and POST methods), or deletes (DELETE method).

For example, change **OFF** to **INFO** for whichever service you want the Audit Logger to gather additional information.

```
<logger name="audit.com.netiq.iac.server.rest.CollectionService.GET"
additivity="false" level="INFO"/>
<logger name="audit.com.netiq.iac.server.rest.CollectionService.PUT"
additivity="false" level="INFO"/>
<logger name="audit.com.netiq.iac.server.rest.CollectionService.POST"
additivity="false" level="OFF"/>
<logger name="audit.com.netiq.iac.server.rest.CollectionService.DELETE"
additivity="false" level="OFF"/>
```

- 7 (Conditional) If you are using TLS, add the certificate (public key) for the `syslog` server (at the provided port) to the Identity Governance and Identity Reporting trusted certificates files.
- 8 Restart Tomcat. For more information, see [“Stopping, Starting, and Restarting Tomcat” on page 52](#).

You can see a list of the audit events here [AuditEventTable.pdf](https://www.netiq.com/documentation/identity-governance-30/references/AuditEventTable.pdf) (<https://www.netiq.com/documentation/identity-governance-30/references/AuditEventTable.pdf>).

Enabling Auditing for Identity Reporting

Use the following information to enable auditing for Identity Reporting. The steps for enabling auditing are the same whether you installed Identity Reporting and Identity Governance on the same server or different servers.

- 1 (Conditional) If you enabled auditing during the install, proceed to [Step 3](#).
- 2 (Conditional) If you want to enable auditing after the installation, complete the following steps.

2a Create an audit directory to store the audit information.

- ♦ **Linux:** `/opt/netiq/idm/apps/audit`
- ♦ **Windows:** `C:\netiq\idm\apps\audit`

2b Create the Identity Reporting log file.

- ♦ **Linux:** `../tomcat/conf/idmrptcore_logging.xml`
- ♦ **Windows:** `C:\netiq\idm\apps\tomcat\conf\idmrptcore_logging.xml`

2c (Linux only) Assign ownership to the audit directory.

```
chown -R novlua.users /opt/netiq/idm/apps/audit
```

NOTE: The `novlua.users` is the same ownership as the `tomcat` directory. It allows the Tomcat service to modify files within the audit logs directory.

- 3 Modify the Identity Governance logging file to enter the `syslog` server information.

3a Open the logging file in a text editor.

- ♦ **Linux:** `/opt/netiq/idm/apps/tomcat/conf/idmrptcore_logging.xml`
- ♦ **Windows:** `C:\netiq\idm\apps\tomcat\conf\idmrptcore_logging.xml`

3b Make the following changes specific for your `syslog` server:

```
<enabled>true</enabled>
<protocol>TCP/TLS</protocol>
<host>123.456.78.90</host>
<port>6514</port>
<cache-dir>/opt/netiq/idm/apps/audit</cache-dir>
<cache-file>idm-rpt</cache-file>
<application>Reporting Core</application>
<vendor>Micro Focus</vendor>
<version>6.0</version>
```

NOTE: To disable auditing, ensure that the `<enabled>` line is set to `false`. For example:

```
<enabled>false</enabled>
```

- 4 (Conditional) If you are using TLS, add the certificate (public key) for the `syslog` server (at the provided port) to the Identity Governance and Identity Reporting trusted certificates files. For example:
 - ♦ **Linux:** `jre/lib/security/cacerts`
 - ♦ **Windows:** `c:\netiq\jre\cacerts`
- 5 Restart Tomcat. For more information, see “Stopping, Starting, and Restarting Tomcat” on page 52.

Enabling Auditing for OSP after the Installation

The steps to enable auditing for OSP are different from enabling auditing for the other components.

You can see a list of the audit events here [OSP CEF Events.pdf \(https://wwwtest.netiq.com/documentation/identity-governance-30/references/OSP%20CEF%20Events.pdf\)](https://wwwtest.netiq.com/documentation/identity-governance-30/references/OSP%20CEF%20Events.pdf).

Use the following information to enable auditing for OSP.

- 1 Create the audit directory.
 - ♦ **Linux:** `/opt/netiq/idm/apps/audit`
 - ♦ **Windows:** `C:\netiq\idm\apps\audit`
- 2 Create the OSP log file.
 - ♦ **Linux:** `/opt/netiq/idm/apps/audit/osp.log`
 - ♦ **Windows:** `C:\netiq\idm\apps\audit\osp.log`
- 3 (Linux only) Set the ownership on the audit directory.

```
/bin/chown -R novlua.idvadmin /opt/netiq/idm/apps/audit
/bin/chmod -R g+s /opt/netiq/idm/apps/audit
```

NOTE: The `novlua` is the same ownership as the `tomcat` directory. It allows the Tomcat service to modify files within the audit logs directory.

- 4 Use the Identity Governance Configuration Update utility to set properties for your environment in OSP.
 - 4a Execute the Identity Governance Configuration Update utility.
 - ♦ **Linux:** The utility is `configupdate.sh` on Linux.

```
/opt/netiq/idm/apps/osp/bin/configupdate.sh edition=none
```

- ♦ **Windows:** The utility is `configupdate.bat` on Windows.

```
C:\netiq\idm\apps\osp\bin\configupdate.bat edition=none
```

NOTE: Adding `edition=none` on the command line avoids needing to modify this value within `configupdate.sh.properties` or `configupdate.bat.properties` file. It also avoids certain unnecessary fields which the config update utility would otherwise require values for in order to save.

4b Access the **CEF Auditing** tab.

4c Select the **Send audit events** option.

4d Specify the values for your environment:

- ♦ **Destination host:** Specify `localhost`
- ♦ **Destination port:** Specify the port. The default value is `6514`.
- ♦ **Network protocol:** Select **TCP** or **UDP**.
- ♦ **Use TLS:** Select this option to secure communication over TCP. By default, this option is not selected.
- ♦ **Intermediate event store directory:** Specify the audit directory you created in [Step 1](#). The default directory is:
 - ♦ **Linux:** `/opt/netiq/idm/apps/audit`
 - ♦ **Windows:** `C:\netiq\idm\apps\audit`

4e Restart Tomcat. For more information, see [“Stopping, Starting, and Restarting Tomcat” on page 52](#).

Starting and Initializing Identity Governance

To verify installation and to initialize the Identity Governance databases, you must start Tomcat. In a clustered environment, start the primary node first to ensure that the initial database load occurs before the other nodes start.

- 1 (Optional) Verify that the schemas (Oracle) or databases (MS SQL or PostgreSQL) exist in your database platform.
- 2 To initialize Identity Governance and its databases, start Tomcat. For examples, see [“Stopping, Starting, and Restarting Tomcat” on page 52](#).

NOTE: In a clustered environment, start Tomcat only on the primary (or master) node.

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

```
tail -f path_to_Tomcat_folder/logs/catalina.yyyy.mm.dd.log
```

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

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

- 4 Open a web browser and navigate to one of the following URLs, depending on how you installed Identity Governance:

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

For example:

http://texasone:8080/
https://172.16.254.1:8443/

The browser should display the login page for Identity Governance.

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

5a Log in as an administrator to the server where you installed Identity Governance.

5b In a terminal, navigate to the following directory:

- ♦ **Linux:** /opt/netiq/idm/apps/idgov/logs
- ♦ **Windows:** c:\netiq\idm\apps\idgov\logs

5c Enter the following command:

```
tail -n 1 *
```

5d Verify that all .txt log files in the directory end with the following text:

```
Exit code: 0
```

NOTE

- ♦ Identity_Governance_InstallLog.log contains the results of all the log files. It does not have an individual exit code.
 - ♦ The checksums-log.txt file contains multiple command and multiple Exit code: 0 for each command.
 - ♦ If a log file ends with a nonzero exit code, an error occurred in that part of the installation process.
-

6 Use the bootstrap administrator account to log in to Identity Governance.

Until you collect and publish data from an identity source that contains login accounts for Identity Governance, you must use the bootstrap administrator account. For more information, see [“Adding Identity Governance Users” on page 184](#).

7 (Conditional) If you can verify installation but cannot get Identity Governance to load in a web browser, complete the following steps:

7a Stop Identity Governance (and Tomcat). For examples, see [“Stopping, Starting, and Restarting Tomcat” on page 52](#).

7b Navigate to the following directory:

- ♦ **Linux:** /opt/netiq/idm/apps/tomcat/bin
- ♦ **Windows:** c:\netiq\idm\apps\tomcat\bin

7c In a text editor, open setenv.sh.

This file defines global variables and export paths needed to host Identity Governance under Apache Tomcat.

7d Verify that the file lists the correct host name for the authentication server and paths to Tomcat.

7e Save and close the file.

7f Start Identity Governance (and Tomcat). For examples, see [“Stopping, Starting, and Restarting Tomcat” on page 52](#).

8 (Conditional) In a clustered environment, start Tomcat on the secondary nodes.

9 (Conditional) To configure Identity Reporting, continue to [Chapter 31, “Setting Up Identity Reporting,” on page 313](#).

10 (Conditional) To integrate Identity Governance with Identity Manager, continue to [Chapter 14, “Integrating Single Sign-on Access with Identity Manager,” on page 187](#).

- 11 Add users who can log in to Identity Governance, and assign authorizations to those users. For more information, see [“Adding Identity Governance Users” on page 184](#).
- 12 (Optional) Configure Identity Governance, such as customizing the email templates and displayed labels. For more information, see [Chapter 10, “Configuring Identity Governance Settings,” on page 129](#).

Configuring Identity Governance for Two-Factor Authentication

If you want to configure Identity Governance to use two-factor authentication, this section shows how to configure OSP on your Identity Governance server with NetIQ Advanced Authentication. For more information, see the [Advanced Authentication](#) documentation.

After you have an Identity Governance server and an Advanced Authentication server running and reachable in your environment, use the following sections to configure the two-factor authentication:

- ♦ [“Prerequisites for Configuring Two-Factor Authentication” on page 112](#)
- ♦ [“Configure the Advanced Authentication Server for Two-Factor Authentication” on page 112](#)
- ♦ [“Configure OSP for Two-Factor Authentication” on page 114](#)
- ♦ [“Testing the Enrolled Methods” on page 116](#)

Prerequisites for Configuring Two-Factor Authentication

Before configuring the servers for two-factor authentication, ensure the following conditions exist:

- ☐ Server time is in sync for the Identity Governance and Advanced Authentication servers
- ☐ Each server can correctly resolve the DNS name of the other server
- ☐ You must have OSP installed and running on the Identity Governance server

Configure the Advanced Authentication Server for Two-Factor Authentication

Advanced Authentication allows you to increase security in your environment by providing multiple ways for advanced authentication. This solution allows you to add two-factor authentication to Identity Governance to add an additional layer of security. You must configure Advanced Authentication to communicate with the Identity Vault Identity Governance uses for authentication for the two-factor authentication to work.

This section assumes you have a good working knowledge and understanding of Advanced Authentication. For more information, see the [Advanced Authentication](#) documentation.

- 1 Log in with administrator credentials to the Advanced Authentication Administration portal.
- 2 Click **Repositories**, then click **Add**.
- 3 Complete the guided process, using the following parameters:

LDAP type

Select the appropriate type for the Identity Vault you use with your Identity Governance server.

Name

Specify a name for this repository.

Base DN

Specify the base DN where Advances Authentication searches for the users in the Identity Vault. For example, `o=data`.

User

Specify the administrator user name in LDAP format. For example,
`cn=admin,ou=sa,o=system`.

Password

Specify the password for the administrative user.

Group DN

(Optional) Specify a group DN if you want to collect groups.

- 4 Under **LDAP Servers**, click **Add Server**, then specify the DNS name of the LDAP server and the port.
- 5 Save the server details.
- 6 (Optional) To change default attributes or collect a new attribute, click **Advanced settings** and then edit the following settings:

User Lookup Attributes

These attributes specify the LDAP attributes Advanced Authentication uses to find a user object in the directory. The attribute names used must match the names configured in the Identity Governance Configuration Update utility. **Identity Vault:Login** attribute (by default, `cn`) and **Authentication:Duplicate** resolution naming attribute (by default, `mail`).

IMPORTANT: Expand **Advanced settings** and ensure that the **User lookup** attribute is configured. If you are using the **Email OTP** method, then you must configure the **User mail** attributes.

If using Active Directory with Identity Governance, use `sAMAccountName` instead of `cn`.

User Mail Attributes

This option must contain the names of LDAP attributes used to hold a user's email address. The default values are typically sufficient.

IMPORTANT: Ensure that all users in your Repository have unique email IDs.

- 7 Click **Save** to save the repository details.
For more information, see “[Adding a Repository](#)” in the *Advance Authentication Administration Guide*.
- 8 Find the new repository that you just created, then click **Edit > Full sync** to sync the users and groups from the LDAP server.
- 9 Define the method for two-factor authentication of **Email OTP** and **LDAP Password**.
 - 9a Click **Methods > Email OTP** to edit this method.
 - 9b Change the different setting for your environment. For example, change **OTP Period**, **OTP Format**, **Sender Email**, and **Subject**.
 - 9c Click **Save** to save the **Email OTP** method.
 - 9d Click **LDAP Password**.

- 9e Change the different settings for the LDAP Identity Vault Identity Governance uses, then click **Save**.
For more information, see “[Configuring Methods](#)” in the *Advance Authentication Administration Guide*.
- 10 Configure the mail sender for the **Email OTP** method.
 - 10a Under **Policies**, click **mail sender**.
 - 10b Specify the host, port, user name, password, and whether you want to enable TLS/SSL.
 - 10c Click **Save** to save the changes for your environment.
- 11 Create a chain to make the authentication methods available for OSP.
 - 11a Click **Chains** to make the chain available to the users.
 - 11b Click **Add** to create a new chain.
 - 11c In the **Name** field, specify a name for this new chain.
 - 11d Set **Is enable** to **On**.
 - 11e Select the methods you created in [Step 9](#). This allows the users to enter their LDAP password and then perform an OTP validation.
 - 11f In the **Roles and Group** field, type **A** to find the **ALL USERS** group, then select the **ALL USERS** group.
 - 11g Set any additional option that you require, then click **Save**.
For more information, see “[Creating a Chain](#)” in the *Advance Authentication Administration Guide*.
- 12 Create an event to define the type of authentication event you use.
 - 12a Click **Events**.
 - 12b Click the **Edit** icon next to the authentication event.
 - 12c Ensure that **Is enabled** is set to **ON**.
 - 12d Select the event type.
For example, you would select **Windows login** if your Identity Vault is Active Directory.
 - 12e Select the chain you created in [Step 11](#).
 - 12f Set any additional options that you require, then click **Save**.
For more information, see “[Configuring Events](#)” in the *Advanced Authentication Administration Guide*.

Configure OSP for Two-Factor Authentication

Ensure that you have created the methods, chain, and events in Advanced Authentication before proceeding. You must configure OSP to accept the authentications from Advance Authentication.

- 1 Execute the Identity Governance Configuration Update utility.
 - ♦ **Linux:** The utility is `configupdate.sh` on Linux.

`/opt/netiq/idm/apps/osp/bin/configupdate.sh edition=none`
 - ♦ **Windows:** The utility is `configupdate.bat` on Windows.

`C:\netiq\idm\apps\osp\bin\configupdate.bat edition=none`

NOTE: Adding `edition=none` on the command line avoids needing to modify this value within `configupdate.sh.properties` or `configupdate.bat.properties` file. It also avoids certain unnecessary fields which the config update utility would otherwise require values for in order to save.

- 2 Click the **Authentication** tab, then click **show advanced options**.
- 3 Under **Authentication method**, select the **Enable two factor authentication** option.
- 4 Click the **Second factor** tab, then fill out the following fields:

Advanced Authentication Administrator > Admin Name

Specify the repository-qualified name of the Advanced Authentication administrator account that OSP uses to interface with Advanced Authentication. Typically, the account is in the `LOCAL` repository.

The default Advanced Authentication administrator account is named `admin`. If you used this account, then the **Admin name** value is:

`LOCAL\admin` (repository name + \ + user name)

Advanced Authentication Administrator > Admin Password

Specify the password of the Advanced Authentication administrative user you specified above.

Advanced Authentication Repository > User repository name

Specify the name of the repository in Advanced Authentication you created in [“Configure the Advanced Authentication Server for Two-Factor Authentication” on page 112](#). This repository corresponds to the Identity Vault for Identity Governance.

Advanced Authentication Servers

Click **Add**, then specify the DNS name or IP address of the Advanced Authentication server. If you use a different port than 443, specify that port as well.

(Conditional) If you have clustered the Advanced Authentication server, then click **Add** again, and specify each DNS name or IP address for each server in the cluster.

Advanced Authentication Endpoint

An Advanced Authentication endpoint is an identifier and secret that ensures that the entity performing authentication with the Advanced Authentication server is authorized to do so.

If no endpoint data is found in the configuration (or if the endpoint data in the configuration cannot be resolved with the Advanced Authentication server) then the **Create new endpoint** box is checked. Specify a name and description for the new endpoint you want to create. The name and description appear in the **Endpoints** section of the Advanced Authentication administrator interface.

If you have already created an endpoint, and the endpoint information is in the configuration, and Identity Governance the endpoint data can resolve with the Advanced Authentication server, then the Identity Governance Configuration Update utility does not select **Create new endpoint box** and it displays the endpoint identifier and a representation of the endpoint secret.

Second Factor Conditions

If you want to require all users to supply a second authentication factor at all times then check **All users, all the time**.

Otherwise deselect the option, then specify conditions for your environment using the following information:

User Login Condition

When you deselect **All users, all the time**, the **User Login Condition** editor appears. This editor allows you to configure an expression that defines under which conditions Identity Governance uses the second factor authentication.

For example, if users do not have mobile devices then you should use **Email OTP** as a second factor authentication.

You build a login condition of expressions that evaluate various operands including user LDAP attributes, server attributes like time-of-day, and date, and HTTP request values like originating IP address, session attributes like session age and so forth. You can negate the expressions and combine the expressions using logical AND and OR operators.

Second Factor Authentication Methods

Use this advanced option to enable and disable the available second factor methods and define the relative priority of each method you want to set.

If you disable a method by deselecting the box next to the method name, then that method is not available for authentication even if a user is enrolled in that method.

Identity Governance uses the relative priority of second factor methods to determine which method it should use if a user is enrolled in more than one method.

For example, using the default values configuration the **Email OTP** has a higher priority than the **LDAP password** method. Therefore, even if a user has enrolled in both methods, Identity Governance selects the **Email OTP** method for that user. You can change the behavior such that Identity Governance selects the LDAP Password by making the **TOTP** priority higher than **Email OTP**.

NOTE: **Email OTP** methods do not need enrollment to be available for a user. It is enabled by default.

- 5 Click **OK** to save the configuration, then exit out of the Identity Governance Configuration Update utility.

Testing the Enrolled Methods

After you have configure Advanced Authentication and Identity Governance for two-factor authentication, you can test the methods to ensure that they work.

- 1 Log in to the Advanced Authentication server as an end user.
- 2 View the **Enrolled** and **Not Enrolled** methods.
- 3 Enroll the methods for the test user by clicking on the appropriate method, then click **Test**.
- 4 Ensure that the test is successful, then save the method for the user.
- 5 Log in to Identity Governance and OSP redirects you to use the second factor authentication.

Updating the License Key

You must enter a valid license key to continue using Identity Governance past the 90-day trial period.

- 1 Log in as a Global Administrator.
- 2 Select your user name, and then select **About**.
- 3 Enter a license key in the appropriate field.

- 4 Select **Submit license**.
- 5 Close the window.

8 Upgrading Identity Governance

You can upgrade to Identity Governance 3.0.x from Identity Governance 2.5. As part of the upgrade process, you must also migrate data because some of the collector templates and database tables and views changed between the releases.

NOTE: If you are upgrading and changing database platforms, you cannot migrate your existing data to the new platform. For example, if you are running Identity Governance with PostgreSQL as your database and you plan to upgrade and use Microsoft SQL Server as your database, your existing data cannot move to the new database.

Upgrading to the latest Identity Governance version is a process you must follow. You must backup your current data, uninstall the current version of Identity Governance and Identity Reporting, if you installed it, and then reinstall the current version of Identity Governance. With the Identity Governance 3.0 release, Identity Reporting is part of the installation process instead of running a separate installer.

- ♦ [“Planning to Upgrade Identity Governance” on page 119](#)
- ♦ [“Saving Customized Settings for Attributes in the Catalog” on page 120](#)
- ♦ [“Running the Cleanup Utility” on page 121](#)
- ♦ [“Changes to Passwords Stored in Environment Variables” on page 121](#)
- ♦ [“Upgrading Procedure” on page 121](#)

Planning to Upgrade Identity Governance

As you plan your upgrade, keep in mind the following considerations:

- ☐ Only review owners and administrators can view in Identity Governance the review runs that were completed in a previous version. If you have reporting installed, you can run reports before you upgrade to capture these details and make them available to other users after the upgrade.
- ☐ Open fulfillment requests will be available after the upgrade.
- ☐ Before you upgrade, make a note of the values for the following settings. The installation process fails to restore or adversely modifies these settings:

Location of settings	Affected Settings
Administration settings in Identity Governance	All settings in the following areas: <ul style="list-style-type: none">♦ Risk Level Configuration♦ General Settings♦ Identity Manager System Connection Information
Reviews > Definitions in Identity Governance	<ul style="list-style-type: none">♦ Escalation timeout♦ Reminder notification

Location of settings	Affected Settings
Workflow Setting > Notification System in the Configuration utility	<ul style="list-style-type: none"> ♦ Mail Server ♦ From Address
Administration > Risk Level Configuration in Identity Governance	Customized risk settings

- ☐ (Conditional) If you customized attributes in the Identity Governance catalog, save those settings before you upgrade. For more information, see [“Saving Customized Settings for Attributes in the Catalog” on page 120](#).
- ☐ (Conditional) To upgrade your Identity Governance Oracle database, you must grant the CREATE PUBLIC SYNONYM and DROP PUBLIC SYNONYM privileges to the igops schema.

Saving Customized Settings for Attributes in the Catalog

Identity Governance allows you to customize some of the attributes, such as email or Account name, in the Catalog. However, when you migrate collected data from a previous version of Identity Governance to this release, all customizations that you applied in the Catalog will be lost. For example, you changed the displayed name of the user attribute Title to Job Title and specified that it is an editable value. The migration process overrides this type of customization.

To maintain your custom settings, you must save those settings before upgrading to Identity Governance or migrating your collections for this release.

- 1 Before upgrading Identity Governance, run the following query against the igops database for the USER entity type:

```
postgres sql:
select attribute_key as attrKey,
attribute_type as attrType,
curatable as editable,
entity_type as entityType,
listable as displayable,
quick_info as quickInfo,
searchable as advanceSearch
from attribute_definition
where extended = false and (attribute_type = 'ARC_MANAGED' or attribute_type =
'COLLECTED') and entity_type = 'USER';
```

```
oracle sql:
select attribute_key as attrKey,
attribute_type as attrType,
curatable as editable,
entity_type as entityType,
listable as displayable,
quick_info as quickInfo,
searchable as advanceSearch
from attribute_definition
where extended = '0' and (attribute_type = 'ARC_MANAGED' or attribute_type =
'COLLECTED') and entity_type = 'USER';
```

- 2 Save the output from the query.

- 3 Run the same query for the other entity types in the Catalog. For each query, change the two instances of `entity_type = USER` to specify the type of attribute that you want to query: `GROUP`, `ACCOUNT`, or `PERMISSION`.
- 4 Save the output from each query that you run.
- 5 After migrating your collected data to the new release, manually reapply your customized settings to the affected attributes based on the query output.

Running the Cleanup Utility

If you extended the schema in the Identity Governance databases, you should clean up the data in the databases. The cleanup utility ensures that you have no schema extension conflicts between your custom attributes and attributes to be added in this version. For more information about migrating your data, contact [Technical Support](#).

Changes to Passwords Stored in Environment Variables

To allow the silent installation of Identity Governance to work, Identity Governance reads passwords stored in environment variables. For more information, see [“Understanding the Passwords that Identity Governance Reads from Environment Variables During the Installation Process”](#) on page 80.

In prior versions of Identity Governance, some of these environment variables had different names. Here is a list of the changes:

Current Name	Prior Name
<code>install_authserver_client_secret</code>	<code>NETIQ_RPT_OSP_PWD</code>
<code>install_db_admin_secret</code>	<code>NETIQ_DB_USER_PASSWORD</code>
<code>install_db_reporting_secret</code>	<code>NETIQ_DB_CFG_PWD</code>
<code>install_truststore_secret</code>	<code>NETIQ_SSL_KEYSTORE_PWD</code>
<code>install_smtp_password_auth_user</code>	<code>NETIQ_SMTP_PASSWORD</code>

Upgrading Procedure

Before starting the upgrade procedure, ensure that you review the consideration in [“Planning to Upgrade Identity Governance”](#) on page 119.

- 1 (Optional) Run reports for any review run details you want to make available after the upgrade.
- 2 Complete or stop all scheduled items, running reports, and running reviews before starting the upgrade process.
- 3 Stop Identity Governance (and Tomcat). For more information, see [“Stopping, Starting, and Restarting Tomcat”](#) on page 52.
- 4 Back up and export (PostgreSQL only) your full Identity Governance data and confirm that you can restore it with no problems.

Include the following databases:

- ♦ `igara`

- ♦ igdcs
- ♦ igops
- ♦ igwf
- ♦ idm_rpt_cfg
- ♦ idm_rpt_data

For more information, see “[Backup and Restore](#)” in the *PostgreSQL Documentation*.

5 (Conditional) If you have an Oracle database, perform the following steps:

5a Backup the igops schema.

5b Run the following command to identify invisible columns:

```
select c.table_name, e.extension_name
  from sys.user_tab_cols c
       inner join sys.user_stat_extensions e on e.table_name = c.table_name
 where c.virtual_column = 'YES' and e.droppable = 'YES'
```

Script that should drop extended statistics and so the virtual column
declare

```
v_sql varchar2(255);
v_owner varchar2(255);
begin
  select SYS_CONTEXT('USERENV', 'SESSION_USER') into v_owner from DUAL;
  for rec in (
    select c.table_name, e.extension_name
      from sys.user_tab_cols c
           inner join sys.user_stat_extensions e on e.table_name = c.table_name
    where c.virtual_column = 'YES' and e.droppable = 'YES'
  )
  loop
    --v_sql := 'alter table '||v.table_name||' drop '||v.column_name;
    v_sql := 'exec dbms_stats.drop_extended_stats('' '|| v_owner ||'',
    ''|| rec.table_name ||'', ''|| rec.extension_name ||'')';
    execute immediate v_sql;
  end loop;
end;
```

5c Remove the hidden columns. For more information, see “[Tips and Tricks Invisible Columns in Oracle Database 12c](#)”.

6 Move your generated reports (pdf and csv) from the Reporting home folder to a backup directory.

7 Use the Data Purge utility to delete unwanted data before upgrading. For more information, see [Chapter 20, “Grooming the Identity Governance Databases,” on page 237](#).

8 Uninstall Identity Governance and Identity Reporting. For more information, see [Chapter 9, “Uninstalling Identity Governance,” on page 125](#).

9 Uninstall OSP and clean up any remaining files and folders. The default installation directory is:

- ♦ **Linux:** /opt/netiq/idm/apps/osp
- ♦ **Windows:** C:\netiq\idm\apps\osp

10 Uninstall Tomcat and clean up any remaining files and folder.

11 (Conditional) If using PostgreSQL, uninstall PostgreSQL. For more information, see [PostgreSQL Installation Procedure](#) in the PostgreSQL documentation. The uninstall information is at the end of the section.

12 (Conditional) If you are running on Windows, reboot the Windows server.

- 13 (Conditional) Upgrade the database server if you are running Microsoft SQL Server or Oracle to the latest supported version by following the database platform instructions.
- 14 (Conditional) Add the invisible columns back into the Oracle database. For more information, see [“Tips and Tricks Invisible Columns in Oracle Database 12c”](#).
- 15 (Conditional) Install the most recent version of Postgres. For more information, see [Chapter 3, “Installing Tomcat, PostgreSQL, and ActiveMQ for Identity Governance,”](#) on page 47
- 16 (Conditional) If using PostgreSQL, add the following users:
 - ♦ `idm_rpt-cfg`
 - ♦ `igara`
 - ♦ `igdc`
 - ♦ `igops`
 - ♦ `igrptuser`
 - ♦ `igwf`
 - ♦ `ig_rpt_role`
- 17 (Conditional) If you have exported the PostgreSQL data, import your data to the new database.
- 18 Install Tomcat. For more information, see [Chapter 3, “Installing Tomcat, PostgreSQL, and ActiveMQ for Identity Governance,”](#) on page 47.
- 19 Install the current version of OSP. For more information, see [Chapter 4, “Installing One SSO Provider,”](#) on page 55.
- 20 Install the current version of Identity Governance. For more information, see [Chapter 5, “Installing Identity Governance,”](#) on page 63.
- 21 Install the current version of Identity Reporting. For more information, see [Chapter 6, “Installing Identity Reporting,”](#) on page 83.
- 22 After the installation completes, copy the generated `pdf` and `csv` report files to the location specified during the installation.
- 23 Start Identity Governance (and Tomcat). For more information, see [“Stopping, Starting, and Restarting Tomcat”](#) on page 52.
- 24 Review changes to existing collectors and adjust mappings as necessary.
- 25 Publish the collected data again to populate the business roles and other items. For more information, see [Chapter 18, “Publishing the Collected Data,”](#) on page 221.
- 26 Activate schedules or create new schedules, if needed.
- 27 To restore your **Administration** settings, complete the following steps:
 - 27a Log in to Identity Governance as a Global Administrator.
 - 27b Select **Administration**.
 - 27c Restore your values in the following **Administration** sections, as needed:
 - ♦ **Risk Level Configuration**
 - ♦ **General Settings**
 - ♦ **Identity Manager System Connection Information**
 - 27d Save your changes.
- 28 Restore your values for **Escalation timeout** and **Reminder notification** in your review definitions.
- 29 Run the Configuration utility to restore your values for **Workflow Settings > Notification System**. For more information, see [“Running the Identity Governance Configuration Utility”](#) on page 129.

9 Uninstalling Identity Governance

There are times where you are required to uninstall Identity Governance. You would uninstall Identity Governance in a lab environment or during an upgrade procedure. For more information about upgrading, see [Chapter 8, “Upgrading Identity Governance,” on page 119](#).

Identity Governance does come with an uninstall utility that you use to uninstall the product, however, you must ensure that all of the files are removed from the server before reinstalling the same version of Identity Governance or a new version of Identity Governance.

To uninstall Identity Governance:

- 1 Define the Java path to the `jre bin` directory as an environment variable.
- 2 Stop Tomcat. For more information, see [“Stopping, Starting, and Restarting Tomcat” on page 52](#).
- 3 (Conditional) If you are running any version of Identity Governance prior to 3.0, you must uninstall Identity Reporting separately from Identity Governance.
 - 3a Access and run the uninstall utility for Identity Reporting.
 - 3b If you are running Linux, access the uninstall directory located here: `/opt/netiq/idm/apps/IdentityReporting/Uninstall_IdentityReporting`.
To execute the script, enter:

```
./LaunchUninstall.sh
```
 - 3c If you are running Windows, access the **Control Panel**, then search for Identity Reporting and click **Uninstall**.
- 4 Access and run the uninstall utility for Identity Governance.
 - 4a If you are running Linux, access the uninstall directory located here: `/opt/netiq/idm/apps/idgov/Uninstall_IdentityGovernance`.
To execute the script, enter:

```
./LaunchUninstall.sh
```


or
 - 4b If you are running Windows, access the **Control Panel**, then search for Identity Governance and click **Uninstall**.
- 5 When the uninstall completes, delete the following files and folders:
 - ♦ **Linux:** The default installation path is `/opt/netiq/idm/apps`.
 - ♦ `/opt/netiq/idm/apps/IdentityReporting`
 - ♦ `/opt/netiq/idm/apps/idgov`
 - ♦ `/opt/netiq/idm/apps/tomcat/webapps/api`
 - ♦ `/opt/netiq/idm/apps/tomcat/webapps/cx`
 - ♦ `/opt/netiq/idm/apps/tomcat/webapps/daas`
 - ♦ `/opt/netiq/idm/apps/tomcat/webapps/doc`
 - ♦ `/opt/netiq/idm/apps/tomcat/webapps/dtp`
 - ♦ `/opt/netiq/idm/apps/tomcat/webapps/IDMRPT`

- ♦ /opt/netiq/idm/apps/tomcat/webapps/IDMRPT-CORE
- ♦ /opt/netiq/idm/apps/tomcat/webapps/ROOT
- ♦ /opt/netiq/idm/apps/tomcat/webapps/rptdoc
- ♦ /opt/netiq/idm/apps/tomcat/webapps/workflow-api
- ♦ /opt/netiq/idm/apps/tomcat/work/Catalina/localhost
- ♦ /opt/netiq/idm/apps/tomcat/temp

♦ **Windows:** The default installation path is C:\netiq\idm\apps.

- ♦ C:\netiq\idm\apps\IdentityReporting
- ♦ C:\netiq\idm\apps\idgov
- ♦ C:\netiq\idm\apps\tomcat\webapps\api
- ♦ C:\netiq\idm\apps\tomcat\webapps\cx
- ♦ C:\netiq\idm\apps\tomcat\webapps\daas
- ♦ C:\netiq\idm\apps\tomcat\webapps\doc
- ♦ C:\netiq\idm\apps\tomcat\webapps\ntp
- ♦ C:\netiq\idm\apps\tomcat\webapps\IDMRPT
- ♦ C:\netiq\idm\apps\tomcat\webapps\IDMRPT-CORE
- ♦ C:\netiq\idm\apps\tomcat\webapps\ROOT
- ♦ C:\netiq\idm\apps\tomcat\webapps\rptdoc
- ♦ C:\netiq\idm\apps\tomcat\webapps\workflow-api
- ♦ C:\netiq\idm\apps\tomcat\work\Catalina\localhost
- ♦ C:\netiq\idm\apps\tomcat\temp\

6 Restart Tomcat, if needed. For more information, see [“Stopping, Starting, and Restarting Tomcat”](#) on page 52.

Configuring and Managing Identity Governance

This section helps you configure, manage, and customize Identity Governance. For example, you can configure Identity Governance to use secure network communications, customize the content and style sheet used in the user interface, and integrate single sign-on with NetIQ Identity Manager. Also, for users to log in to Identity Governance, you must first collect their account information from your environment and then configure authorization assignments to grant appropriate access.

- ♦ [Chapter 10, “Configuring Identity Governance Settings,” on page 129](#)
- ♦ [Chapter 11, “Customizing Identity Governance for Your Enterprise,” on page 153](#)
- ♦ [Chapter 12, “Changing Passwords for Administrative Users,” on page 177](#)
- ♦ [Chapter 13, “Adding Identity Governance Users and Assigning Authorizations,” on page 179](#)
- ♦ [Chapter 14, “Integrating Single Sign-on Access with Identity Manager,” on page 187](#)

10 Configuring Identity Governance Settings

To configure Identity Governance, you use the Identity Governance Configuration Utility, which allows you to modify the settings for the product.

- ♦ [“Running the Identity Governance Configuration Utility” on page 129](#)
- ♦ [“Using the TLS/SSL Protocol for Secure Connections” on page 136](#)
- ♦ [“Configuring the Mail Server for Notifications” on page 137](#)
- ♦ [“Configuring Fulfillment” on page 138](#)
- ♦ [“Configuring Analytics and Role Mining Settings” on page 148](#)

Running the Identity Governance Configuration Utility

The Identity Governance Configuration Utility allows you to modify settings for Identity Governance, such as the URL for Identity Governance, 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 from the Identity Governance installation location. To script changes to the configuration of Identity Governance, use the console mode option.

In the command line, navigate to the installation directory for Identity Governance. by default . Enter one of the following commands:

- ♦ **Linux:** Default location of `/opt/netiq/idm/apps/idgov`, then enter one of the following commands:
 - ♦ **Console mode:** `./bin/configutil.sh -password db_password -console`
 - ♦ **GUI mode:** `./bin/configutil.sh -password db_password`
- ♦ **Windows:** Default location of `c:\netiq\idm\apps\idgov`, then enter one of the following from a command prompt:
 - ♦ **Console mode:** `configutil.bat -password db_password -console`
 - ♦ **GUI mode:** `configutil.bat -password db_password`

The utility provides settings under the following tabs:

- ♦ [“Identity Governance Server Details” on page 130](#)
- ♦ [“Authentication Server Details” on page 130](#)
- ♦ [“Security Settings” on page 131](#)
- ♦ [“Network Topology Settings” on page 132](#)
- ♦ [“Miscellaneous Settings” on page 132](#)
- ♦ [“Bulk Data Update Settings” on page 134](#)
- ♦ [“Workflow Settings” on page 134](#)

Identity Governance Server Details

This tab allows you to display your organization's branding instead of the default branding displayed when your users run Identity Governance.

NOTE: In early versions of Identity Governance (formerly named Access Review), this tab included values for the login page, such as protocol, host name, and port. Starting with Access Review 1.5, those values are on the [Authentication Server Details](#) tab.

Authentication Server Details

This tab defines the values for the LDAP authentication server, OSP authentication service, and bootstrap administrator. This tab provides the following groups of settings:

- ♦ [“OAuth Server” on page 130](#)
- ♦ [“OAuth SSO Client” on page 130](#)
- ♦ [“Bootstrap Admin” on page 131](#)

For more information, see [“Understanding Authentication for Identity Governance” on page 27](#).

OAuth Server

This section represents the values for the LDAP authentication server.

Same as IG Server

Specifies whether the authentication server runs on the same computer as Identity Governance.

Protocol

Applies only when the authentication server and the Identity Governance server run on different computers.

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

Host Name

Applies only when the authentication server and the Identity Governance server run on different computers.

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

Port

Applies only when the authentication server and the Identity Governance server run on different computers.

Specifies the port that you want the server to use for communication with client computers. The default is 8080. To use SSL, the default is 8443.

OAuth SSO Client

This section represents the values for OAuth authentication services to Identity Governance.

IG Client ID

Specifies the client ID of Identity Governance with which it is registered to OSP.

IG Client Secret

Specifies the client password of Identity Governance with OSP.

IG Redirect URL

Specifies the URL used by OSP to redirect to the Identity Governance login page if authentication token is valid.

IG Request Client ID

Specifies the client ID of Identity Governance Access Request with which it is registered to OSP.

IG Request Client Secret

Specifies the client password of Identity Governance Access Request with OSP.

IG Request Redirect URL

Specifies the URL used by OSP to redirect to the Identity Governance Access Request page if authentication token is valid.

Bootstrap Admin

This section represents the values for the bootstrap administrator. For more information, see [“Understanding the Bootstrap Administrator for Identity Governance” on page 29](#).

Bootstrap Admin

Specifies the name of the bootstrap administrator account. The default value is `igadmin`.

(Conditional) When connecting to an existing Identity Manager authentication server, specify the full DN of a unique identity that already exists and can access Identity Manager Home as a bootstrap administrator. For example, `cn=uaadmin,ou=sa,o=data`.

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.

Authentication Source

Specifies whether the credentials for the bootstrap admin reside in an Identity Vault (LDAP authentication server) or a text file.

(Conditional) If you specify **File**, you must also specify values for **Directory** and **Filename** that correspond to the file that stores your bootstrap admin information. The default location is .

- ♦ **Linux:** Default location of `/opt/netiq/idm/apps/idgov/osp`
- ♦ **Windows:** Default location of `c:\netiq\idm\apps\idgov\osp`

Security Settings

This tab defines the values for authentication matching and Identity Governance services.

Auth Matching Rules

Specifies how Identity Governance authenticates login requests and grants the appropriate permissions to users. Enter one or more rules that Identity Governance uses to compare attributes in the `SUSER` table, such as `dn`, with attributes retrieved from OSP. Specify the matching rules using properties named `iac.auth.matching.rule.N.attrs` where *N* specifies the order that Identity Governance uses the rule to match users, such as 1, 2, 3, and so on.

Keep in mind the following points:

- ♦ For best results, add an index for the matching rule attributes.
- ♦ Identity Governance evaluates only collected attribute values for the matching rules, not edited values.
- ♦ When an attribute value is a string, Identity Governance performs an exact case match by default.

IMPORTANT: Set all matching rule attributes with the following list and search options in the Identity Governance User (identity) schema:

- ♦ Display in lists and detail views
- ♦ Available in catalog searches. Changes take effect after publication.

For more information, see [“Adding or Editing Attributes to Extend the Schema” on page 173](#).

Auth Attribute Map

Specifies the mapping of SUSER attributes to OSP attributes using a comma-separated list of attribute name pairs. Use the format `SUSER attribute:OSP attribute`. For example, `dn:name,lastName:last_name,firstName:first_name,emails:email` maps the SUSER attributes of `dn`, `lastName`, `firstName`, and `emails` to the OSP attributes of `name`, `last_name`, `first_name`, and `email`.

IG Client ID

Specifies the name that you want to use to identify Identity Governance to each service listed.

IG Client Secret

Specifies the password for the corresponding client ID.

Enable test client for utilities

Specifies that you want to use test IDs to run utilities that interact with Identity Governance without creating client IDs for each utility.

Network Topology Settings

This tab defines network connection settings that Identity Governance uses to connect to the single Tomcat instance or to the load balancer if you are running Identity Governance in a cluster. If you select [https](#) for the protocol, the [Keystore File](#) and [Keystore Password](#) fields become active.

This tab also defines runtime instance settings.

Miscellaneous Settings

This tab defines additional settings for your configuration. Some fields are self explanatory and some should not be changed. This tab provides the following groups of settings:

Miscellaneous

Do not change the settings in this section except for the [Default Locale](#), if needed.

Collection and Publication Batch Sizes

These settings allow an administrator to tune the size of the record chunks that Identity Governance uses for the data collection and publication operations to achieve optimal performance in each environment.

Collection and Publication Settings

Do not clear **Clean DAAS Configuration post collection**. The **Max supported Depth of permission relations** field prevents loops of relationship mappings in deeply nested permissions environments. The default setting should be best for most environments.

Identity Manager Integration

If you also have Identity Manager installed, these settings help you integrate Identity Governance with Identity Manager.

Enable integration using Identity Manager Driver for Identity Governance

Requires the Identity Manager Driver for Access Review (Access Review driver)

Specifies whether you want to integrate the permissions and permission assignment tasks in the Identity Governance catalog with the role and resource catalog in Identity Manager.

For more information, see [“Understanding Synchronization and Reflection” on page 215](#).

Exclude Identity Manager permissions from review when they provision any native permissions in the same review

Specifies whether you want to review Identity Manager permissions that duplicate native permissions along with the native permissions in a review.

Data Production Timeouts

These settings allow an administrator to tune the timeout values for various data production operations to achieve optimal performance in each environment. The timeout values are expressed in milliseconds. The default values should suffice for the majority of installations.

Heartbeat interval (com.netiq.iac.dataProduction.heartbeat.interval)

The interval between heartbeat updates for data production jobs. The default is 2 minutes (120000 ms).

Job idle cutoff timeout (com.netiq.iac.dataProduction.cutoff.timeout)

The amount of time, after the last heartbeat update, that a running job is deemed to be in an idle state where the data production processing has halted. The default is 6 hours (21600000 ms).

Orphaned job idle add-on timeout (com.netiq.iac.dataProduction.orphan.addon.timeout)

The additional amount of time, combined with the **Job idle cutoff timeout**, that will pass before a runtime instance can detect and clean up data production jobs with a different runtime identifier that have an idle state. The default is 1 hour (3600000 ms), which combined with the default cutoff timeout sets up an overall 7 hour default.

Bulk Data Update Settings

This tab defines settings that you use to submit multiple attribute updates to objects in the catalog by using a CSV file. For more information about performing bulk data updates, see [“Editing Attribute Values in Bulk” on page 229](#).

Base Folder

Create a folder on your Identity Governance server for update files. Specify that full path name of that folder in this field. You must also create sub-folders named `input` and `output`. The Identity Governance service must have read/write access permission on both of these folders. Identity Governance creates the CSV data template files in the output folder, and you submit edits by copying the updated template in the input folder.

Batch Size

(Optional) Specifies the maximum number of CSV data rows processed at one time. This option is useful for tuning the memory usage of the Bulk Update process. The default value is 1000.

When you place the `csv` file in the `input` directory, Identity Governance changes the extension name of the file as it process the file. Here are the different extensions and process the file goes through during the bulk process:

File Extension Name	Process
<code>.csv</code>	Identity Governance start the bulk process. It is the name on the file when you add it into the <code>input</code> directory.
<code>.ph1</code>	Phase 1 of the bulk process.
<code>.fail</code>	If the bulk process fails, the file name becomes <code>.fail</code> .
<code>.done</code>	If the bulk process completed, the name becomes <code>.done</code> .

Workflow Settings

This tab defines settings that you use to automate external provisioning and notifications. This tab provides the following groups of settings:

- ♦ [“External Provisioning System” on page 134](#)
- ♦ [“Notification System” on page 135](#)
- ♦ [“Message Queue” on page 135](#)

External Provisioning System

To use an external provisioning system, specify the **URL**, **User ID**, and **Password** that Identity Governance needs to connect to the system. For example:

URL

```
http://$test:8180/IDMProv
```

User ID

```
globaladmin
```

Password

`adminpassword`

For more information, see [“Using Workflows to Fulfill the Changeset” on page 261](#).

Notification System

This section represents the values that Identity Governance uses to send email notifications.

Mail Server

Specifies the IP address or DNS name and port for the mail server. For example, `12.345.675.90:25`.

From Address

Specifies the email address that you want Identity Governance to use as the origination for email notifications.

NOTE: If you are using a Gmail SMTP server for your mail server, Gmail ignores this value and uses the actual Gmail address as the origination for email notifications.

Enable SMTP TLS

Specifies to use secure email delivery.

User ID

Specifies the email address that you want to use for authenticating Identity Governance to the mail server.

Password

Specifies the password associated with the specified **User ID**.

Enable persistent notification message queue

Specifies whether you want to use message queuing functionality.

Message Queue

This section represents the values for the message queue for email notifications. The queue can use TLS/SSL protocol for secure communication.

JMS broker URI

Specifies the Uniform Resource Identifier (URI) for the Java Message Service (JMS) that the mail server uses. For example, `tcp://12.345.675.90:61616`.

(Conditional) In a clustered environment, add `failover:` to the prefix, then specify the host name or IP address and port for each ActiveMQ server. Use commas to separate the server values. For example, `failover:tcp://amq1.mycompany.com:61616,tcp://amq2.mycompany.com:61616`.

SSL

Specifies whether you want to use TLS/SSL protocol for secure communication when sending notifications.

Queue Keystore

Applies when you want to use the SSL protocol.

Specifies the path and filename of the keystore file that contains the authentication server trust certificate for the mail server.

Queue Keystore Password

Applies when you want to use the SSL protocol.

Specifies the password used to load the keystore file.

Queue Trust Store

Applies when you want to use the SSL protocol.

Specifies the path to the Trusted Key Store that contains all trusted signers' certificates.

Queue Trust Store Password

Applies when you want to use the SSL protocol.

Specifies the password for the Trusted Key Store.

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 Identity Governance:

- ♦ HTTP, which provides end-user access to and from Identity Governance
- ♦ LDAP, which ensures secure communication between Identity Governance and the authentication server
- ♦ JDBC, which ensures secure communication between Identity Governance 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 Identity Governance database stores the certificate and password. After installation, you can configure Identity Governance to use the TLS/SSL protocol before putting the system into production.

We highly recommend that you configure Tomcat to use https with either TLSv1.2 or TLS1.1. Any prior version of TLS should not be used. For more information, see [“Securing Tomcat”](#).

For more information about the Identity Governance Configuration Utility, see [“Running the Identity Governance Configuration Utility” on page 129](#).

To configure secure communication with the authentication server:

- 1 Stop Identity Governance (and Tomcat). For examples, see [“Stopping, Starting, and Restarting Tomcat” on page 52](#).
- 2 Run the Identity Governance Configuration Utility.
- 3 For **Authentication Server Details** and **Network Topology**, verify that the connection protocol for the servers is set to *https*.
- 4 Select **Save**, and then close the utility.

- 5 Ensure that the specified host and port for the authentication server support TLS/SSL communication.
- 6 Start Identity Governance (and Tomcat). For examples, see [“Stopping, Starting, and Restarting Tomcat” on page 52](#).

Configuring the Mail Server for Notifications

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

You can also configure Identity Governance to send reminders of tasks, based on the escalation timeout setting. For more information, see [“Escalating Review Items” on page 249](#).

When Identity Governance sends an email, the application queries the preferred language of the target user. If Identity Governance 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 [“Customizing the Email Notification Templates” on page 160](#).

To configure the mail server for notifications:

- 1 In the Identity Governance Configuration Utility, select **Workflow Settings**.
- 2 Under **Notification System**, specify the settings for the mail server.
- 3 Select **Save**.
- 4 (Conditional) To ensure guaranteed delivery of the notifications by using ActiveMQ, complete the following steps:
 - 4a Select **Enable persistent notification message queue**.
 - 4b Enter the settings for the JMS broker.
 - 4c (Optional) To use TLS/SSL protocol for messaging, select **SSL** and then specify the keystore settings.
 - 4d Select **Save**.
 - 4e Navigate to the installation directory for ActiveMQ. For example, .
 - ♦ **Linux:** /opt/netiq/idmapps/apache-activemq-x.x.x
 - ♦ **Windows:** c:\netiq\idmapps\apache-activemq-x.x.x
 - 4f Copy the `activemq-all-x.x.x.jar` file.
 - 4g Navigate to the installation directory for the Tomcat server supporting Identity Governance. For example, .
 - ♦ **Linux:** /opt/apache-tomcat-x.x.xx
 - ♦ **Windows:** c:\ProgramFiles\apache-tomcat\x.x.xx
 - 4h In the `lib` directory of the Tomcat installation, paste the `activemq-all-x.x.x.jar` file.
 - 4i Restart Tomcat after copying the `activemq-all-x.x.x.jar` file. For examples, see [“Stopping, Starting, and Restarting Tomcat” on page 52](#).
- 5 (Optional) To change the text in the email notifications, continue to [“Customizing the Email Notification Templates” on page 160](#).

Configuring Fulfillment

The review process results in Identity Governance building a list of changes, or **changesets**, that are then submitted for **fulfillment**. The Identity Governance fulfillment system evaluates the individual permission change items, determines which applications use these permissions, and then sends the changesets to the appropriate fulfillment target for each application. Identity Governance users with global, provisioning, or bootstrap administrator authorization assignments can configure fulfillment options.

- ♦ [“Configuring Multiple Fulfillment Targets for an Application” on page 139](#)
- ♦ [“Transforming Data from Fulfillment Targets” on page 140](#)
- ♦ [“Configuring Identity Manager and Manual Fulfillment Methods” on page 140](#)
- ♦ [“Configuring Service Desk Fulfillment” on page 141](#)
- ♦ [“Understanding Fulfillment Status” on page 146](#)

Identity Governance provides three default options for fulfillment targets for provisioning the changeset items from a review: Identity Manager automated, Identity Manager workflow, and manual (a user or group). You can also integrate and automate Identity Governance fulfillment with your service desk system by adding and configuring a connector to your service desk system in Identity Governance **Fulfillment Configuration**. Identity Governance supports the following fulfillment targets:

- ♦ Active Directory LDAP
- ♦ BMC Remedy Incident
- ♦ CSV
- ♦ eDirectory LDAP
- ♦ Generic HTTP
- ♦ Identity Manager Dxcmd Fulfillment for Active Directory
- ♦ REST Service
- ♦ ServiceNow Generic
- ♦ ServiceNow Incident
- ♦ ServiceNow Request
- ♦ SOAP Service

To configure fulfillment methods:

- 1 Log in to Identity Governance as a user with global, fulfillment, or bootstrap administrator authorization assignment.
- 2 Select **Fulfillment > Configuration**.
- 3 (Conditional) Select a fulfillment target.

or

If you want to add a fulfillment target, select **+** and complete the required fields in the template. When adding fulfillment targets, you must configure service parameters to connect Identity Governance to your fulfillment service, and then configure mappings to create an appropriate fulfillment request. When viewing the list of mapped attributes for a field, you could see some items not available to select and marked with a strike-through line across the text. An Identity Governance administrator must enable these attributes in **Administration > Context Fulfillment Attributes**.

NOTE: You can download the fulfillment target templates, edit them, and upload them to Identity Governance instead of configuring the service parameters and mappings in the application. For more information, see [“Customizing Fulfillment Target Templates” on page 165](#).

- 4 Make any additional updates for the selected fulfillment target, such as fulfillment response mapping and specifying change request types, and select **Save**.
- 5 Select **Fulfillment > Configuration** and select the **Application setup** tab.
- 6 (Optional) If you want to use the same fulfillment method for multiple applications, you can select and configure them using the **Fulfillment Target** selector at the top of the page.
- 7 For each application, select the fulfillment method in the **Fulfillment Target** column. The **Change Request Type** column updates to show whether the fulfillment target handles all change request types or some types for this application.
- 8 (Optional) Select **customize** to change the default configuration for any fulfillment method you want to customize for a given application. Identity Governance adds an icon to each application row showing that you have customized the fulfillment configuration and providing an easy way to restore default values.
- 9 Select **Save Fulfillment Configuration** using the icon at the top of the tab when you have made changes.

Configuring Multiple Fulfillment Targets for an Application

You can configure each application to use multiple fulfillment targets. For example, you might have one system that processes all requests to add access and a different system that processes all requests to remove access.

- 1 Log in to Identity Governance as a user with global, fulfillment, or bootstrap administrator authorization assignment.
- 2 Select **Fulfillment > Configuration** and select the **Application setup** tab.
- 3 Select the green plus sign (+) next to the fulfillment target where you want to specify multiple targets.
- 4 Select the target you want to process change requests in each row for the application. You can use the same fulfillment target and customize each row to process different requests, or you can use a different target for certain requests.

NOTE: To assist the Fulfillment Administrator in making sure that the configured fulfillment targets handle all change request types, Identity Governance shows which change request types are configured next to each fulfillment target. If a target does not support any of the change request types, those unsupported types display in red text.

- 5 After making changes, select the save icon at the top of the tab to save your settings.

Transforming Data from Fulfillment Targets

You can transform the incoming data from fulfillment targets to have Identity Governance display more meaningful information. For example, instead of displaying only the incident number from your fulfillment system, you could display additional text, such as “Incident number 123456 was created in ServiceNow” in Identity Governance.

The transforms are done through Nashorn-compatible Javascript in the **Fulfillment Response mapping** section of the fulfillment target configuration. Within the Javascript, you can access the incoming value by creating a variable name `inputValue`. After manipulating the incoming value, you can return the value to Identity Governance by assigning the value to a variable name `outputValue`.

The following example transforms the incoming value, which is a tracking number from the connected system to `Incident number 123456 created in ServiceNow` in the Identity Governance displays.

```
outputValue = 'Incident number ' + inputValue + ' created in ServiceNow'
```

To change fulfillment target response mapping:

- 1 Log in to Identity Governance as a user with global, fulfillment, or bootstrap administrator authorization assignment.
- 2 Under **Fulfillment > Configuration**, select an existing fulfillment target or create a new one.
- 3 Expand the Fulfillment Response mapping section and select the braces (`{ }`) next to the attribute you want to transform.

NOTE: Two dots between the braces (`{..}`) denotes that a transform script exists for an attribute.

- 4 Enter or edit the existing transform script in one of the following ways:
 - ♦ Paste a script in the text field
 - ♦ Select **Advanced Edit** to open a script editor
 - ♦ Select **Browse** to upload a script file
- 5 Save the fulfillment target.

Configuring Identity Manager and Manual Fulfillment Methods

For Identity Manager automated, Identity Manager workflow, and manual fulfillment methods, Identity Governance evaluates and fulfills the change items without the need for extensive configuration. When specifying one of the default methods of fulfillment, observe the following considerations:

Identity Manager Automated

Applies only when you integrate Identity Governance with Identity Manager.

Specify whether you want to use automated provisioning with manual fulfillment or a workflow as the fallback method. Then specify the values associated with the fallback method. For more information, see [“Automatically Fulfilling the Changeset” on page 261](#).

Identity Manager Workflow

Applies only when you integrate Identity Governance with Identity Manager.

Specify the name of a workflow that already exists in Identity Manager. The workflow needs to have inputs for the following fields:

- ◆ String: `changesetId`
- ◆ String: `appId`

To connect to the external provisioning system, specify the workflow settings in the Identity Governance Configuration Utility. For more information, see [“External Provisioning System” on page 134](#).

For more information about the workflow process, see [“Using Workflows to Fulfill the Changeset” on page 261](#).

Manual

Specify an individual or group of individuals to serve as the fulfiller. For more information about manual fulfillment, see [“Manually Fulfilling the Changeset” on page 260](#).

To have Identity Governance email reminders to the fulfillers, ensure that you configure email notifications. For more information about configuring notifications, see [“Notification System” on page 135](#). For more information about customizing emails, see [“Customizing the Email Notification Templates” on page 160](#).

Configuring Service Desk Fulfillment

Identity Governance includes connectors to various service desk products to enable fulfillment integration with your incident management applications. When you connect to an application for fulfillment, you must configure the connector to map the data fields in the change item to the input fields of the application. In a typical service desk environment, all systems and applications that the service desk manages are input as configuration management items.

The Identity Governance Fulfillment target configuration allows you to customize your incidents for these various systems. When you create a service desk fulfillment target in Identity Governance, you provide the connection information and credentials for the target system as well as a default configuration specifying the fields you want Identity Governance to populate in your incidents. After you assign a target fulfillment system to an application, you can then customize that default configuration to appropriately map the application configuration item, assignment group, severity, and other fields for that specific application.

Identity Governance exposes the following data fields from each changeset item to the fulfillment target connectors:

changeItemId

A long value containing the internal change item number

changeSetId (optional)

A long value containing the internal changeset number

changeRequestType

A string value containing one of the following values:

- ◆ `REMOVE_ACCOUNT_PERMISSION`
- ◆ `ADD_USER_TO_ACCOUNT`
- ◆ `REMOVE_PERMISSION_ASSIGNMENT`
- ◆ `REMOVE_ACCOUNT_ASSIGNMENT`
- ◆ `REMOVE_ACCOUNT`
- ◆ `ADD_PERMISSION_TO_USER`

- ◆ ADD_APPLICATION_TO_USER
- ◆ ADD_TECH_ROLE_TO_USER
- ◆ MODIFY_PERMISSION_ASSIGNMENT
- ◆ MODIFY_ACCOUNT_ASSIGNMENT
- ◆ MODIFY_ACCOUNT
- ◆ REMOVE_APPLICATION_FROM_USER

fulfillmentInstructions (optional)

Instructions the reviewer provided for the fulfiller

userName

Display name of the user that is the target of the change item

account (optional)

Identifier of the account

accountLogicalId (optional)

Logical system identifier of the account. This only applies to Identity Manager SAP User Management driver accounts.

accountProvid (optional)

The collected identifier that indicates the unique ID of the account

appName

Name of the application to which the permission being provisioned belongs

fulfillerName (optional)

Name of the fallback fulfillment user

reason

Generated description of the action being requested by the change item

requesterName

Display name of the reviewer who requested the change

permName

Name of the permission being provisioned

permProvAttr

Name of the target permission attribute being modified

permProvLogicalId (optional)

Logical system identifier of the permission being provisioned. This only applies to the Identity Manager SAP User Management driver permissions.

permProvid (optional)

The collected unique provisioning identifier of the permission

reviewReasonId (optional)

The internal long value for the reason

reviewReason (optional)

The reason text

userProfile (optional)

Attribute to provide context to the fulfiller on the recipient of the fulfillment item

requesterProfile (optional)

Attribute to provide context to the fulfiller on the requester of the fulfillment item

accountProfile (optional)

Attribute to provide context to the fulfiller on the account if the fulfillment item is an account

permissionProfile (optional)

Attribute to provide context to the fulfiller on the permission if the fulfillment item is a permission

The following shows a sample change item payload:

```
{
  "accountProvId": "d2a293ff-71c5-492f-9415-e08830b635b2",
  "changeItemId": 8300,
  "changeRequestType": "REMOVE_PERMISSION_ASSIGNMENT",
  "userName": "Abby Spencer",
  "accountName": "aspencer",
  "account": "CN=Abby Spencer,OU=Users,OU=MyServer,DC=mydc,DC=mycompany,DC=com",
  "appName": "Money Honey Financials",
  "reason": "REMOVE_PERMISSION_ASSIGNMENT remove permission Marketing Portal
requested by Aaron Corry while certifying Money Honey Financials",
  "requesterName": "Andrew Astin",
  "permName": "Marketing Portal",
  "permProvAttr": "member",
  "permProvId": "e07db779-5c30-44d2-bc0c-6dfa30cfa6af"
}
```

Mapping Identity Governance change item data to target application data fields is similar to configuring data source collectors. This includes support for static-value mapping and per-field data transformation. For more information, see [“Customizing the Collector Templates for Data Sources” on page 164](#).

Since the implementation of any particular service desk application varies widely for each customer, it may be useful to manually create sample incidents using the application user interfaces to validate the desired inputs for each fulfillment method.

BMC Remedy Incident Management Integration

The Identity Governance fulfillment connector for BMC Remedy uses the HPD_IncidentInterface_Create SOAP service Helpdesk_Submit_Service method for creating incidents in the Remedy application. For example, `http://your-service-host/arsys/WSDL/public/your_server/HPD_IncidentInterface_Create_WS`.

The connector uses a pre-configured template that maps the Identity Governance change item data and application-specific static values into various attributes in the SOAP XML payload. The WSDL from your incident management application indicates any value constraints for input fields. The fulfillment target service can populate all valid fields in the service desk interface, so if you want to extend the set of fields that the Identity Governance template populates or modify the default mappings of the template, contact your Micro Focus technical support representative for details.

IMPORTANT: The Remedy application requires several fields to create an incident. The template identifies fields that *must* be properly configured to ensure the ability to create incidents.

Use the following table to understand the Identity Governance mappings to the Remedy incident fields. Quotation marks surround static values. You can modify the static values provided in the template to conform with the options available in the target service desk application.

BMC Remedy Incident Field	Identity Governance Mapping
Service_Type	"User Service Request" (required)
Reported_Source	"Direct Input" (required)
Status	"New" (required)
Action	"CREATE" (required)
Urgency	"3-Medium" (required)
Impact	"3-Moderate/Limited" (required)
First_Name	(required)
Last_Name	(required)
Notes	Reason, appName, username, account (ecmascript transformation provided)
Summary	changeRequestType
HPD_CI_ReconID	

ServiceNow Incident Management Integration

The Identity Governance fulfillment connector for ServiceNow Incident Management uses the Incident SOAP service `insert` method for creating incidents in the Incident Management application. For example, <https://your-service-url/incident.do?WSDL>.

The connector uses a pre-configured template that maps the Identity Governance change item data and application-specific static values into various attributes in the SOAP XML payload. The WSDL from your incident management application indicates any value constraints for input fields. The fulfillment target service can populate all valid fields in the service desk interface, so if you want to extend the set of fields that the Identity Governance template populates or modify the default mappings of the template, contact your Micro Focus technical support representative for details.

Use the following table to understand the Identity Governance mappings to the Incident Management incident fields. Quotation marks surround static values. You can modify the static values provided in the template to conform with the options available in the target service desk application.

ServiceNow Incident Field	Identity Governance Mapping
cmdb_ci	appName
assignment_group	
category	"request"
subcategory	
description	reason, appName, userName, account (ecmascript transformation provided)
contact_type	"automated"

ServiceNow Incident Field	Identity Governance Mapping
short_description	
correlation_id	changeItemId
correlation_display	"Access review or request fulfillment item"
caller_id	requesterName
opened_by	requesterName
severity	"2"
urgency	"2"
impact	"2"

ServiceNow Service Catalog Request Management Integration

The Identity Governance fulfillment connector for ServiceNow Service Catalog Request Management uses the Service Catalog Request SOAP service `insert` method for creating requests in the Service Catalog application. For example, `https://your-service-url/sc_request.do?WSDL`.

The connector uses a pre-configured template that maps the Identity Governance change item data and application-specific static values into various attributes in the SOAP XML payload. The WSDL from your service catalog request management application indicates any value constraints for input fields. The fulfillment target service can populate all valid fields in the service desk interface, so if you want to extend the set of fields that the Identity Governance template populates or modify the default mappings of the template, contact your Micro Focus technical support representative for details.

Use the following table to understand the Identity Governance mappings to the Service Catalog Request Management incident fields. Quotation marks surround static values. You can modify the static values provided in the template to conform with the options available in the target service desk application.

ServiceNow Incident Field	Identity Governance Mapping
fulfillment_type	"request"
cmdb_ci	appName
assignment_group	
description	reason, appName, userName, account, fulfillmentInstructions (ecmascript transformation provided)
contact_type	"automated"
request_state	"requested"
short_description	
correlation_id	changeItemId
correlation_display	"Access review or request fulfillment item"
requested_for	userName
opened_by	requesterName

ServiceNow Incident Field	Identity Governance Mapping
priority	"2"
urgency	"2"
impact	"2"

Understanding Fulfillment Status

The following details on fulfillment status conditions can help with troubleshooting fulfillment in your environment. A change item has 11 possible status conditions, listed below in the associated status column. The general status column shows the broad status categories that Identity Governance displays to users. The table includes details on each status and what actions, if any, you can take to move an item to a different status. No user action is required for some status conditions, either because they are intermediate states or terminal states.

General Status	Summary	Associated Status	Entry Conditions	Exit Conditions
Error or timeout	Provisioning was marked as complete, but the status after a collect and publish cycle shows the item as not fulfilled.	Not fulfilled, verification error (NOT_VERIFIED)	Change item marked as fulfilled but updated catalog shows that status to be incorrect. This can be valid when fulfillment target is an asynchronous process, such as Service Now. When Service Now opens a ticket, Identity Governance marks the change request item complete. However, the help desk might not have completed the update to the associated application.	Examine the change item and take one of the following actions: <ul style="list-style-type: none"> ♦ If the fulfillment target is an asynchronous task, such as Service Now, ensure the help desk has fulfilled the item and then run another collect and publish cycle. ♦ If possible, fulfill the item and then run a collect and publish cycle. ♦ If not possible to fulfill the item, mark the item as Ignore.
	Fulfiller has marked item as Declined.	Declined by (REFUSED)	Manual fulfiller has marked and submitted item as Declined.	Mark the item as Ignore .

General Status	Summary	Associated Status	Entry Conditions	Exit Conditions
	Change item was marked as being in error.	Not fulfilled, verification error (ERROR)	This status will not be reached by normal operation of the system. It is a transitory state on the way to automatic retry in case there was an error detected during fulfillment. However, an API endpoint can set the status to ERROR, so an external system might have caused the item to have this status.	Intermediate status; no action needed.
	Change item has not been successfully verified at the end of verification expiration timeout.	Not fulfilled, verification timed out (VERIFICATION_TIMEOUT)	If Identity Governance is set up to monitor verification timeouts and the change item has not been verified within that time, it moves to this status. By default, this value is set to 365 days.	Mark the item as Ignore .
Fulfilled	Fulfillment is reported as complete.	Fulfilled, pending verification (COMPLETED)	Identity Governance has received communication that fulfillment has completed. This status might not mean the item is fulfilled. If the fulfillment target is an asynchronous process, such as Service Now, the status changes to completed when the asynchronous process opens a ticket, not when the tasks in the ticket have been fulfilled.	After the next collect and publish cycle, Identity Governance verifies the item target matches the change item. If so, the item status changes to Verified. If not, the item status changes to Error.
Pending fulfillment	Fulfillment is in progress.	Initializing (INITIALIZED, IN_PROGRESS)	Change request item has been created.	Intermediate status; no action needed.

General Status	Summary	Associated Status	Entry Conditions	Exit Conditions
	Fulfillment has been initiated.	Pending fulfillment by, Sending for fulfillment by external workflow (PENDING)	Identity Governance successfully communicates with provisioning workflow or adds change items to manual fulfiller queue.	Change item is acted on by either an automated fulfillment system or a manual fulfiller. If fulfiller marks item as fulfilled, the item status changes to Fulfilled (COMPLETED). If the fulfiller marks the item as refused, the item status changes to Error (REFUSED).
Verified	Catalog shows item has been fulfilled.	Verified (VERIFIED)	Identity Governance verifies changes in catalog.	Terminal status; no action needed.
Ignored	Fulfiller or review owner has ignored closed-loop verification.	Verification ignored (VERIFICATION_IGNORED)	Fulfiller or review owner has selected Ignore for a change item that was in error or timeout status.	Terminal status; no action needed.
Retry	The change item has had an error during fulfillment and is waiting for administrator action.	Retry	An error is detected during fulfillment.	Global Administrator or Fulfillment Administrator selects Retry or Terminate for the item on the Fulfillment Requests page.

Configuring Analytics and Role Mining Settings

Identity Governance tracks key risk indicators so that you can monitor these risk factors in your environment and make improvements based on the collected metrics. In addition to the preset metrics, you can also create custom metrics based on your business needs. Additionally, you can also choose to include or exclude specific decision support information, and configure role mining settings.

- ♦ [“Understanding Role Mining Settings” on page 150](#)
- ♦ [“Creating Custom Metrics” on page 150](#)
- ♦ [“Viewing Entitlement Assignments Statistics to Leverage Roles” on page 151](#)
- ♦ [“Viewing Account Statistics and Details” on page 151](#)

To configure analytics and role mining settings:

- 1 Log in as a Global, Data, or Business Administrator.

NOTE: Business Administrator does not have the same access permissions as a Global or Data Administrator and can only configure **Role Mining** settings and collect **Business Role Mining metrics**.

- 2 Select **Administration > Analytics and Role Mining Settings**.
- 3 (Optional) Under **Decision Support**, specify if business role authorization status, similarity statistics in reviews and access requests, and login statistics for review item users and accounts are included in the guidance provided to reviewers, review owners, review administrators, and access approvers.
 - 3a Deselect option **Show business role authorization status** either if business roles are not used or if the reviewer of user reviews or access request approver does not need guidance about whether the review or request item was authorized by business role.
 - 3b Deselect option **Show similarity statistics in reviews and access requests** if the reviewer of user reviews or access request approver does not need guidance about how many users have similar permissions.
 - 3c Deselect option **Show login statistics for review item users and accounts** if Last Login and Number of Logins attributes are not configured/collected/logged for the users and accounts.
- 4 (Optional) Under **Similarity Profile**, select additional attributes to use in the similarity profile so that Identity Governance can provide decision support.

TIP: Use wildcard * to search for attributes.

5 Under **Role Mining**:

- 5a Enter the **Maximum** number of results that should be returned when mining business roles using the directed role mining approach.
 - 5b Specify which additional user **Attributes** should be used for both directed and visual business role mining. For more information about which attributes to select, see [“Understanding Role Mining Settings” on page 150](#).
- 6 Select **Save** to save all the settings.
- 7 Under **Metric Collection**, select one or more items, and then specify **Actions > Set collection interval** to change the default setting of 24 hours between metrics collections or disable collection.

TIP: Click on an item name to view detailed information about the metric, including list of metric columns' aliases and corresponding data types.

NOTE: In addition to the default metrics, you can create custom metric. For more information, see [“Creating Custom Metrics” on page 150](#).

- 8 Enter **Hours** or **Disable collection**.
- 9 Click **Save** to set the new interval.
- 10 (Optional) Select one or more times and then select **Actions > Collect metrics** to initiate a metrics collection on demand.

TIP: Always collect metrics after a collection and publication to refresh charts on the **Overview** page.

- 11 (Optional) Select one or more items and then select **Actions > Download** to download metrics in CSV format.
- 12 (Optional) When a collection is running and you want to cancel it, select the item or items, and then select **Cancel Collection**.
- 13 Click **Cancel Collection** to confirm the cancellation.

Understanding Role Mining Settings

Identity Governance uses attributes specified in **Administration > Analytics and Role Mining Settings** to provide business role recommendations. If the specifications do not meet certain conditions you may not see any recommendations.

When specifying attributes make sure that:

- ♦ Specified attributes have values. User attributes with zero strength will not be displayed in the directed mining recommended attribute bar graph or visual attribute map.

In addition, in order for visual role mining to render recommendations make sure that:

- ♦ At least two attributes are selected. For example, "Title" and "Department".
- ♦ Selected attributes share commonality. For example, Department A, B, and C have users with same titles like Administrative Assistant and Department Lead.

NOTE: After customizing attributes select **Collect Metrics > Business Role Mining metrics** to refresh data. For more information about role mining, see ["Understanding Business Role Mining" on page 275](#).

Creating Custom Metrics

In addition to default metrics, Identity Governance provides the ability to create SQL statement to query your operations database for additional statistics. The product also displays an * in front of the names of the custom metrics to distinguish them from other metrics. You can click the metric name to view the details of the metric.

After creating custom metrics, you can **Collect Metrics**, and **Download** metrics using the same procedures as for default metrics. In addition, you can also select **Actions > Delete Custom** to delete custom metrics.

To create a custom metric:

- 1 Log in as a Global, or Data Administrator.
- 2 Select **Administration > Analytics and Role Mining Settings**.
- 3 Next to **Metrics Collection**, select **+**.
- 4 Enter **Name** for the new metric.
- 5 Optionally, select an existing category or **Add Custom** category; and enter **Description**.
- 6 Select **SQL Statement** and enter a SQL select statement.

NOTE: Identity Governance automatically checks for statement errors and potential SQL injections to prevent invalid or malicious code. However, ensure that you have defined your query correctly, as once created and saved you cannot edit the custom metric. If needed, you will have to delete the custom metric, and then create a new one to change your definition.

- 7 Select **Metrics Columns** and then **Add Column** to specify an alias and type for each column selected in the SQL statement. For example, given the SQL statement: `select count(id) as active from role_policy where state = 'ACTIVE'`, add a metric column `active` with a type of `Long`.
- 8 Select **Save**.

Viewing Entitlement Assignments Statistics to Leverage Roles

To understand how your entitlement assignments conform to your business policies, you can view the **Role Leverage** widget on the **Overview** page. It includes a graphical overview of effectiveness of your roles over a period of time, entitlements assignments using roles versus entitlements assigned directly, and ratio of indirect role-based entitlements versus total entitlement assignments in percentage. To change the default time range, select the calendar icon and select dates. To refresh the graphs, collect metrics for business role mining after publishing new business roles. Based on these metrics, you can then lower risk by using role mining to create more roles. For more information, see [“Defining Business Roles” on page 277](#).

Viewing Account Statistics and Details

On the **Overview** page, you can see an account statistics summary for your environment. To see data, you must collect and publish data sources and then collect metrics on demand or wait the default metrics collection interval of 24 hours.

NOTE: To keep statistics up to date, collect metrics on demand after every publication.

Identity Governance displays available metrics on the summary panel followed by a chart for each metric per risk levels. To change the default settings:

- ♦ Select the calendar icon to change the time range for account statistics.
- ♦ Select the change option icon to show or hide risk level series.

To drill down to see many more specific charts relating to your accounts:

- 1 On **Overview** under **Account Statistics**, select **View statistics details**.
or
Select a data point on any chart to drill down to statistics details for that chart.
- 2 Select the calendar icon to change the date for the statistics.
- 3 Select a chart or table from the drop down menu to change to a different set of statistics. You can modify or delete these.
- 4 Drag and drop available metrics from header to columns or rows.
- 5 (Optional) To create a customized chart or table:
 - 5a Start with a chart or table that contains the basic elements you want.
 - 5b Select the type of table, such as heatmap or line chart.
 - 5c Select the type of statistics, such as count or average.
 - 5d (Optional) Select additional options, if needed. Some selections add more options to customize.
 - 5e Customize the row and column headings.
- 6 Type a name for the customized view and select **Save**.

11

Customizing Identity Governance for Your Enterprise

You can customize the displayed names of attributes and risk levels in the Identity Governance interface. You can also customize the content in the templates for the email notifications.

- ♦ [“Localizing to the User’s Preferred Language” on page 153](#)
- ♦ [“Customizing the User Interface” on page 154](#)
- ♦ [“Translating Content for Identity Governance and One SSO Provider” on page 156](#)
- ♦ [“Customizing the Email Notification Templates” on page 160](#)
- ♦ [“Customizing the Identity Governance Style Sheet” on page 163](#)
- ♦ [“Customizing the Collector Templates for Data Sources” on page 164](#)
- ♦ [“Customizing Fulfillment Target Templates” on page 165](#)
- ♦ [“Specifying Additional Fulfillment Context Attributes” on page 165](#)
- ♦ [“Using Coverage Maps” on page 165](#)
- ♦ [“Customizing Categories” on page 171](#)
- ♦ [“Customizing Review Display” on page 171](#)
- ♦ [“Configuring Reasons for Review Actions” on page 172](#)
- ♦ [“Disabling Review Email Notifications” on page 172](#)
- ♦ [“Extending the Identity Governance Schema” on page 173](#)

Localizing to the User’s Preferred Language

Identity Governance 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
- ♦ Polish
- ♦ Portuguese
- ♦ Russian

- ♦ Spanish
- ♦ Swedish

Identity Governance cannot always reconcile the differences in language that occur when different users collect data and run reports on that collection. For example, a user in Spain runs a collection for a set of data. Then a user in Russia runs a report against that collection. The fields in the report appear in Russian since that is the report user's default language. However, the reported data is in Spanish because the collection occurred on a computer with Spanish as the default language.

You can customize the content in the provided languages. Alternatively, you can apply a new language to Identity Governance and OSP.

Customizing the User Interface

Identity Governance and OSP automatically display content in the user interface according to your preferred language. You can customize content such as attribute names and informational messages using a text editor.

You might customize the content 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.

- ♦ [“Customizing the Labels in the Identity Governance Interface” on page 154](#)
- ♦ [“Customizing Strings in the JAR Properties Files” on page 155](#)

For more information about translating the content to a new language instead of customizing it, see [“Translating Content for Identity Governance and One SSO Provider” on page 156](#).

Customizing the Labels in the Identity Governance Interface

Some organizations might want to customize the default names for the attributes, risk levels, and navigation items in Identity Governance. The `.properties` file for customizing this content is available from the Identity Governance interface, rather than a `.jar` file.

To customize the labels:

- 1 Log in to Identity Governance as a Global Administrator.
- 2 Select **Administration > Localization Import and Export**.
Identity Governance lists the `.properties` files by language.
- 3 For the language that you want to customize, select **Download**.

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

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

- 4 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.userID=User ID from
source
```

Change `User ID from Source` to `Account Name from Source`.

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

- 5 Save and close the file.
- 6 To submit the modified file, select **Upload** for the language that you customized.
- 7 Refresh the browser window to view the changes.

NOTE: Depending on the browser settings, you might need to sign out of Identity Governance, clear the cache in the browser, then log in again.

Customizing Strings in the JAR Properties Files

By editing the various `.properties` files in the Identity Governance and OSP `.jar` files, you can customize the content displayed in the Identity Governance Configuration Utility as well as most of the Identity Governance and OSP interface. For example, you might want to use different terminology in the Identity Governance Configuration utility.

The `.jar` files are located:

- ♦ **Linux:** Default directories:
 - ♦ **Identity Governance:** `/opt/netiq/idm/apps/idgov/localization`
 - ♦ **OSP:** `/opt/netiq/idm/apps/osp/osp-extras/l10n-resources`
- ♦ **Windows:** Default directories:
 - ♦ **Identity Governance:** `c:\netiq\idm\apps\idgov\localization`
 - ♦ **OSP:** `c:\netiq\idm\apps\osp\osp-extras\l10n-resources`

To customize strings for Identity Governance or OSP:

- 1 Log in to the server where you installed Identity Governance or OSP.
- 2 To modify the `.properties` files, complete the following steps:
 - 2a Locate the `.jar` file that you want to update.

For example, the `iac-configutil-strings.jar` file contains all displayed text for the Identity Governance Configuration Utility.
 - 2b Copy the `.jar` files that you want to update to a temporary directory.
 - 2c In the temporary directory, extract the `.jar` that you want to edit.

WARNING: Do not change the file names or directory structure of the `.jar` files.

- 2d Browse the file directory to the `.properties` file that you want to edit.

For example, `iac-ConfigUIstringsRsrc_fr.properties`.
- 2e In a text editor, customize the displayed text for the content that you want to change.

WARNING: Do not modify any text in the code string before the = sign. For example, `ADMIN_PASSWORD=`. Identity Governance might not function appropriately if you change the code string incorrectly.

- 2f Save and close the editor.

- 3 Copy the customized `.properties` files to their appropriate locations in the original `.jar` files in the temporary directory.
For example, replace the `iac-ConfigUIStringsRsrc_fr.properties` file with the modified version of the file in the following location:
 - ♦ **Linux:** Default location of `/opt/netiq/idm/apps/tomcat/lib`
 - ♦ **Windows:** Default location of `c:\netiq\idm\apps\tomcat\lib`
- 4 Copy the `.jar` file(s) with the customized content to the `lib` directory.
 - ♦ **Linux:** Default location of `/opt/netiq/idm/apps/tomcat/lib`
 - ♦ **Windows:** Default location of `c:\netiq\idm\apps\tomcat\lib`
- 5 Stop Tomcat. For examples, see [“Stopping, Starting, and Restarting Tomcat” on page 52](#).
- 6 Delete all files and folders in the following directories:
 - ♦ **Linux:** Default location of the:
 - ♦ Tomcat temporary directory in `/opt/netiq/idm/apps/tomcat/temp`
 - ♦ Catalina directory `/opt/netiq/idm/apps/tomcat/work/Catalina`
 - ♦ **Windows:**
 - ♦ Tomcat temporary directory in `c:\netiq\idm\apps\tomcat\temp`
 - ♦ Catalina directory `c:\netiq\idm\apps\tomcat\work\Catalina`
- 7 Delete all log files from the `logs` directory for Tomcat.
 - ♦ **Linux:** Default location of `/opt/netiq/idm/apps/tomcat/logs`
 - ♦ **Windows:** Default location of `c:\netiq\idm\apps\tomcat\logs`
- 8 Start Tomcat. For examples, see [“Stopping, Starting, and Restarting Tomcat” on page 52](#).
- 9 Before logging in to Identity Governance, clear the browser cache to ensure that the browser displays your changes.

Translating Content for Identity Governance and One SSO Provider

If the default languages for Identity Governance and OSP do not meet your organization’s needs, you can translate the strings and user interface content to a different language. For example, you might want to interact with Identity Governance in Norwegian (language code=`nb`). To use a non-default language, you need to translate the `.properties` files of an existing language.

- ♦ [“Preparing Files for Translation” on page 157](#)
- ♦ [“Ensuring that Identity Governance Recognizes the New Language” on page 158](#)
- ♦ [“Adding the Translated Labels to the Identity Governance Interface” on page 159](#)
- ♦ [“Adding Translated Content to Identity Governance and OSP” on page 159](#)
- ♦ [“Verifying the New Translations” on page 160](#)

For more information about customizing the content for a current new language instead of adding a language, see [“Customizing the User Interface” on page 154](#).

Preparing Files for Translation

This procedure assumes that you will translate English `.properties` files to the new language, rather than starting from another language such as French. Most of the `.properties` files are located in `.jar` files.

- ♦ **Linux:** Default location:
 - ♦ **Identity Governance:** `/opt/netiq/idm/apps/idgov/localization`
 - ♦ **OSP:** `/opt/netiq/idm/apps/osp/osp-extras/l10n-resources`
- ♦ **Windows:** Default location:
 - ♦ **Identity Governance:** `c:\netiq\idm\apps\idgov\localization`
 - ♦ **OSP:** `c:\netiq\idm\apps\osp\osp-extras\l10n-resources`

WARNING: Do not change the directory structure of the `.jar` files or modify any text in the code strings before the `=` sign. Identity Governance might not function if you make inappropriate alterations.

To prepare files for translation:

- 1 To prepare the file that Identity Governance uses for labels in the user interface, complete the following steps:
 - 1a To download a file to use as the template for translation, complete [Step 1](#) through [Step 3](#) in “Customizing the Labels in the Identity Governance Interface” on page 154.
 - 1b Change the locale code in the file name to represent the language that you want to add.
For example, to add Norwegian, change
`localizedLabels_en.properties`
to
`localizedLabels_nb.properties`
- 2 To prepare the content in the `.jar` files, complete the following steps:
 - 2a Create backup copies of the `.jar` files that you want to translate. Store the backups in a safe location.
 - 2b Copy the `.jar` files that you want to translate to a temporary directory.
You will need these files again after the translations are complete.
 - 2c For each `.jar` file in the temporary directory, extract the English `.properties` files that you want to translate.
For example, extract `iac-ConfigUIStringsRsrc_en.properties` from the `iac-configutil-strings.jar` file for Identity Governance.
 - 2d For each extracted `.properties` file, change the locale code in the file name to represent the language that you want to add.
For example, to add Norwegian, change
`iac-ConfigUIStringsRsrc_en.properties`
to
`iac-ConfigUIStringsRsrc_nb.properties`

- 2e** (Conditional) If a string that you want to translate and use in the `.properties` file has a comment, you must un-comment it.

For example, change

```
#OIDPENDUSER.50048=Next
```

to

```
OIDPENDUSER.50048=Next
```

- 2f** Create `.jar` files to contain the `.properties` files that you want to translate.

For example, for the Norwegian translator, you might create `nb-iac-configutil-strings.jar`.

The new `.jar` files must mimic the directory structure of the original files.

- 2g** Add the `.properties` files that are ready for translating to the new language in the new, appropriate `.jar` files.

For example, add the `iac-ConfigUIStringsRsrc_nb.properties` file to the `nb-iac-configutil-strings.jar` file.

- 3** Provide the `.jar` files and the `localizedLabels_xx.properties` file to your translator.

WARNING: Ensure that the translator maintains the file names and directory structure of the `.jar` files. Also, do not modify any text in the code string before the `=` sign. For example, `com.netiq.iac.persistence.ops.AttributeDefinition.USER.guid=`. Identity Governance might not function if you make inappropriate alterations.

Ensuring that Identity Governance Recognizes the New Language

The Identity Governance Configuration Utility controls which languages appear in Identity Governance and sets the default language. When you integrate with Identity Manager, the RBPM Configuration Utility performs this duty.

Perform this procedure when you are ready to add new translations to Identity Governance.

- 1** In a terminal, navigate to the following directory:
 - ♦ **Linux:** Default location of `/opt/netiq/idm/apps/idgov/bin`
 - ♦ **Windows:** Default location of `c:\netiq\idm\apps\idgov\bin`
- 2** Run the Identity Governance Configuration Utility:
 - ♦ **Linux:** Enter the following command:
 - ♦ **Console mode:** `./bin/configutil.sh -password db_password -console`
 - ♦ **GUI mode:** `./bin/configutil.sh -password db_password`
 - ♦ **Windows:** Enter the following command:
 - ♦ **Console mode:** `configutil.bat -password db_password -console`
 - ♦ **GUI mode:** `configutil.bat -password db_password`
- 3** Select **Miscellaneous**.
- 4** For **Supported Locales**, add the locale code that represents the language(s) that you want to include. Use a pipe sign to separate entries.

For example, enter `|nb` for Norwegian.

- 5 For Default Locale, specify the language that you want to use.
For example, enter `nb` for Norwegian.
- 6 Save your changes and close the utility.

Adding the Translated Labels to the Identity Governance Interface

- 1 Complete the steps in [“Ensuring that Identity Governance Recognizes the New Language” on page 158](#).
- 2 Log in to Identity Governance as a Global Administrator.
- 3 Select **Administration > Localization Import and Export**.
Identity Governance lists the `.properties` files by language.
- 4 For the language that you added to Identity Governance, select **Upload**.
For example, if you added the locale code for Norwegian to the Identity Governance Configuration Utility, upload the `localizedLabels_nb.properties` file.
- 5 Refresh the browser window to view the changes.

NOTE: Depending on the browser settings, you might need to sign out of Identity Governance, clear the cache in the browser, then log in again.

Adding Translated Content to Identity Governance and OSP

To add the new content to Identity Governance and OSP, you need to place the translated `.properties` files in their appropriate locations in the `.jar` files in the temporary directory. The updated `.jar` files belong in the `lib` directory for Tomcat.

- ♦ **Linux:** Default directory of `/opt/netiq/idm/apps/tomcat/lib`
- ♦ **Windows:** Default directory of `c:\netiq\idm\apps\tomcat\lib`

Ensure that you Complete the steps in [“Ensuring that Identity Governance Recognizes the New Language” on page 158](#) before starting this procedure.

- 1 Navigate to the temporary directory where you had copied the original `.jar` files in [Step 2b on page 157](#).
- 2 Add the translated `.jar` files to the temporary directory.
- 3 For each translated `.jar` file, extract the translated `.properties` file(s).
- 4 Copy the translated `.properties` file(s) to their appropriate locations in the original `.jar` files in the temporary directory.
 - ♦ **Linux:** For example, place the `iac-ConfigUIStringsRsrc_nb.properties` file in the `/com/netiq/iac/config/util` directory of the `iac-configutil-strings.jar` file.
 - ♦ **Windows:** For example, place the `iac-ConfigUIStringsRsrc_nb.properties` file in the `c:\netiq\com\iac\config\util` directory of the `iac-configutil-strings.jar` file.
- 5 Delete the translated `.jar` file(s) from the temporary directory.
- 6 Copy the `.jar` file(s) with the added translations to the `lib` directory for Tomcat.
 - ♦ **Linux:** Default directory of `/opt/netiq/idm/apps/tomcat/lib`
 - ♦ **Windows:** Default directory of `c:\netiq\idm\apps\tomcat\lib`

- 7 Stop Tomcat. For examples, see [“Stopping, Starting, and Restarting Tomcat” on page 52](#).
- 8 Delete all files and folders in the following Tomcat directories:
 - ♦ **Linux:** Default locations of
 - ♦ /opt/netiq/idm/apps/tomcat/temp
 - ♦ /opt/netiq/idm/apps/tomcat/work/Catalina
 - ♦ **Windows:** Default locations of:
 - ♦ c:\netiq\idm\apps\tomcat\temp
 - ♦ c:\netiq\idm\apps\tomcat\work\Catalina
- 9 Delete all log files from the Tomcat logs directory.
 - ♦ **Linux:** Default location of /opt/netiq/idm/apps/tomcat
 - ♦ **Windows:** Default location of c:\netiq\idm\apps\tomcat
- 10 Start Tomcat. For examples, see [“Stopping, Starting, and Restarting Tomcat” on page 52](#).
- 11 Before logging in to Identity Governance, clear the browser cache to ensure that the browser displays your new language.

Verifying the New Translations

- 1 In a browser, clear the browser cache.
- 2 Change the browser language to the language that you added to Identity Governance.
- 3 Enter the URL for Identity Governance.

If you did not translate the content in the OSP . jar files, the login page continues to appear in the default language.
- 4 Log in to Identity Governance.
- 5 Observe the translated content.

Customizing the Email Notification Templates

Identity Governance notifies users of tasks in their queue, as well as other review events, as specified in review definitions. Depending on your configuration, various events associated with functional areas, such as bulk data update, business role approval, request, review, Separation of Duties (SoD), and fulfillment, might trigger email notifications. For example, the Bulk Data Administrator can be notified when a bulk data template is generated and when a bulk data update occurs; and an SoD Policy Owner can be notified when a new SoD violation has been detected after data source collection and publication. The application supplies default templates with preconfigured tokens for the email notifications and uses the templates as is unless you customize them for your environment.

You can also customize the product name in email notifications to brand it for your organization instead of the default name of NetIQ Identity Governance. To change the product name, run the Identity Governance Configuration Utility, and enter the product name you prefer on the **Identity Governance Server Details** tab. For more information, see [“Running the Identity Governance Configuration Utility” on page 129](#).

For information about configuring Identity Governance to send email notifications, see [“Configuring the Mail Server for Notifications” on page 137](#). For information about Review related notifications, see [“Setting Up Review Notifications” on page 249](#).

- ♦ [“Modifying Email Templates” on page 161](#)
- ♦ [“Adding an Image to the Email Template” on page 163](#)

Modifying Email Templates

Identity Governance allows you to modify an XML file that contains the email text in the languages supported for Identity Governance. You can edit the XML file in one of the following programs to customize it for your organization:

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

To modify an email template content:

- 1 Log in to Identity Governance as a Global Administrator.
- 2 Select **Administration > Notification Emails**.
- 3 (Conditional) To customize all email templates in a single file, under **email templates (all languages)**, select **Download**.

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

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

- 4 (Conditional) To customize email templates for specific functional areas, such as Bulk Data or Business Role Approval, next to **View functional areas by**:

4a Select **Email Name**.

4b Select an email name, such as **Bulk Data Update Performed** from the list of functional areas.

TIP: Click on an email name and then select **Email source preview (en)** to view the template. Enter an email address to **Send notification preview**.

4c Select **Download** to download the email template for the languages for your locale.

- 5 Modify the content in the email templates you have downloaded.

NOTE: Do not modify any text in the code strings in the file. Identity Governance might not function appropriately if you change the code strings incorrectly. For descriptions of the email tokens, see [“Email Tokens” on page 162](#).

- 6 Save and close the files.
- 7 To submit the modified files, select the **Upload** icon next to **email templates (all languages)**.
- 8 Select **Save**.

Email Tokens

When customizing emails be careful in handling the tokens. Some email templates expect only certain processing tokens. Therefore, the product might not be able to replace a token with a value in some situations. In these situations, the template contains blank values when unexpected tokens are present. Notifications sent during review preview mode that enable administrators and review owners to preview notifications, might also not always replace tokens with values, and names seen in the preview might not be the name that is sent in the live mode email.

The email templates use the following processing tokens:

Token	Notes
applicationId	Application ID, unused in the Certification External Provisioning Start Error template
applicationName	Application name
appName	Application name
approverName	Business role approver
certifierFullName	Reviewer's full name
certifyTaskLink	Link to task
changesetId	Unused in the Certification External Provisioning Start Error template
content	Used in the generic email template
curatorFullName	Bulk data feed curator
error	Fulfillment error
errorMessage	Error message text
externalPrdLink	Unused in the Certification External Provisioning Start Error template
feedName	Bulk data update definition
fulfillerName	Full name of the fulfiller
host	The workflow hostname
inputFile	Bulk data CSV file
link	URL link
message	The output message from a system process.
newTaskType	Used in the Certification Auto Provisioning Start Failed template
ownerName	Owner of the SoD policy
permissionsToLose	List of application permissions
prdName	Workflow name used in the external fulfillment template
prevReviewerFullName	User that the task was reassigned from
productName	Configured product name, such as Identity Governance or Access Review
reassignedByFullName	User who reassigned the task
reassignComment	Optional comment entered at reassignment

Token	Notes
retryCount	Number of fulfillment items in a retry state
reviewLink	URL link to review
reviewName	Name of the review
reviewOwner	Review owner's name
reviewOwnerPhone	Review owner's phone number
roles	List of business approval roles
subject	Found in Certification Started and Certification Changed email templates with no reference to the token in the templates.
taskTimeoutDays	Task timeout in days
theTerminator	The user that terminated a review
userFullName	Identity Governance user's full name
violations	Used in the Detected SoD Violation email template.

Adding an Image to the Email Template

In addition to modifying an email template, you can also add an image or logo to the email template.

To add an image to the email template:

- 1 Select the image you want to add to the template and encode it in base64 string format.

TIP: Use base64encode website or similar encoders to encode the image.

- 2 Download email template.
- 3 Add the `tag` where you want the image to appear. For example, `<p>Powered by </p>`.
- 4 Upload the modified file.

Customizing the Identity Governance Style Sheet

You can modify the stylesheet (CSS file) that Identity Governance uses to display enterprise-specific branding. Identity Governance defaults to the NetIQ template.

- 1 Log in as the Tomcat server administrator to the Tomcat server that hosts Identity Governance.
- 2 In the home directory of the Tomcat server administrator, create a directory named `netiq_custom_css`. For example:

```
/home/name_of_Tomcat_admin/netiq_custom_css
```

- ♦ **Linux:** `/home/SmithJ/netiq_custom_css`
- ♦ **Windows:** `C:\Windows\System32\config\systemprofile\netiq_custom_css`

NOTE: For Windows environments, you might need to create the directory in a different location. To determine the correct location, you can use the Process Monitor tool from Microsoft. For more information, see [Process Monitor \(https://technet.microsoft.com/en-us/sysinternals/processmonitor.aspx\)](https://technet.microsoft.com/en-us/sysinternals/processmonitor.aspx) in the Windows Sysinternals documentation.

- 3 (Optional) If you are using Process Monitor, include the following steps:
 - 3a Create a filter including the following:
 - ♦ Process name is `java.exe`
 - ♦ Operation is `CreateFile`
 - ♦ Result contains `PATH NOT FOUND`
 - ♦ PATH contains `custom.css`
 - 3b Log in to Identity Governance.
 - 3c When the product loads in your browser, look back at Process Monitor to see the path for your Windows environment.
- 4 Create a file named `custom.css`.
- 5 Edit the `custom.css` file to include your branding and other custom style settings that you want Identity Governance to use.
- 6 (Conditional) To use custom images, add the images to the `netiq_custom_css` directory.
- 7 To preview your changes, log in to Identity Governance.

You might need to refresh the page in the browser. You do not need to restart the Tomcat server.

Customizing the Collector Templates for Data Sources

Usually, a collector template includes predefined attribute mappings and value transformation policies suitable for the target data source. To create a custom collector template, you can download and edit an existing template. Collector templates use JavaScript Object Notation (JSON) format for specifying the collection behavior. You can use a JSON formatter or text editor to modify the content of the template file.

When you import a new or modified template for an application source, you must specify whether the template is designed for collecting accounts or permissions from the source. If a new or customized template replaces an existing template, you can disable the template that you no longer need.

- 1 Log in to Identity Governance as a Global or Data administrator.
- 2 Select **Administration**.
- 3 Expand the **Identity Source Collector Templates** or **Application Source Collector Templates** section.
- 4 (Conditional) To customize an existing template, complete the following steps:
 - 4a Select the template that you want to customize.
 - 4b Select **Download**.
 - 4c Specify where you want to save the downloaded file.
 - 4d Edit the template and save the JSON file.
- 5 (Conditional) To import a new or modified collector template, select **+** and then specify the template that you want to import.

- 6 (Conditional) To disable a template that you do not use, complete the following steps:
 - 6a Select the template that you want to disable.
 - 6b Select **Disable**.

Customizing Fulfillment Target Templates

A fulfillment target template includes predefined service parameters and attribute mappings suitable for the fulfillment target application. To create a custom fulfillment target template, you can download and edit an existing template. Fulfillment target templates use JavaScript Object Notation (JSON) format for specifying the service parameters and mappings. You can use a JSON formatter or text editor to modify the content of the template file.

If a new or customized template replaces an existing template, you can disable the template that you no longer need.

- 1 Log in to Identity Governance as a Global or Fulfillment administrator.
- 2 Select **Administration > Fulfillment Target Templates**.
- 3 Select a template, and then select **Download** or **Disable**.
- 4 Edit the content.
- 5 Under **Fulfillment Target Templates**, select **+**.
- 6 Enter a template name and description and then browse to the location of the updated file.
- 7 Select **Save**.

Specifying Additional Fulfillment Context Attributes

By default, the system sends basic information on how to perform fulfillment after a review or a request. Optionally one may specify additional attributes which also should be included when sending instructions to an external fulfillment target.

NOTE: Manual fulfillment target attributes are not based on this setting.

- 1 Log in to Identity Governance as a Global or Fulfillment administrator.
- 2 Select **Administration > Fulfillment Context Attributes**.
- 3 Specify **Requester**, **Recipient**, **Account**, and **Permission** attributes.

TIP: Use wildcard * to search for attributes.

- 4 Select **Save**.

Using Coverage Maps

In review definition and approval policy, administrators can select coverage maps to specify:

- ♦ Reviewers of a **User Access** or **Account Review** definition
- ♦ Approvers for requested access in the **Request** application

Coverage maps are CSV files with header and criteria cells. You can use these files to map review or request items to respective reviewers or approvers by specifying:

- ♦ An entity type or attribute based on the item under review.
- ♦ Different entity and attribute criteria in a single column
- ♦ Secondary or related entity or attribute of related entity referenced via entity-entity relationships

It is important to have an understanding of Identity Governance supported coverage map types, keywords, syntax, and entity-entity relationships in order to create and load coverage maps.

- ♦ [“Creating Coverage Map” on page 166](#)
- ♦ [“Loading Coverage Map” on page 170](#)

Creating Coverage Map

To create a coverage map, create a CSV file with header and criteria cells. For greater flexibility use only keywords.

- ♦ [“Supported Coverage Map Types and Keywords” on page 166](#)
- ♦ [“Supported Syntax” on page 167](#)
- ♦ [“Supported Relationships” on page 168](#)
- ♦ [“User Access Review Coverage Map Examples” on page 168](#)
- ♦ [“Account Review Coverage Map Examples” on page 169](#)
- ♦ [“Access Request Coverage Map Example” on page 170](#)

Supported Coverage Map Types and Keywords

Identity Governance supports the following coverage map type attributes and keywords:

Type	Description	Keywords
REVIEW	Maps for user access and account review based reviews	<ul style="list-style-type: none">♦ Reviewer♦ ReviewItem
REQUEST	Maps for request based approver determination	<ul style="list-style-type: none">♦ Approver♦ RequestItem

Supported Syntax

Header and Criteria Cells Syntax

For	Syntax
USER or GROUP based reviewer header cell	<code><Reviewer.user Reviewer.group>[.related user or group attribute key]</code>
Review item header cell	<code><Approver.user Approver.group>[.related user or group attribute key]</code>
USER or GROUP based approver header cell	<code><Application Permission User>[.entity-attribute-key]</code>
Request item header cell	<code>[RequestItem.]<Application Permission ROLE_POLICY User>.<entity-attribute-key></code>
Keyword(s) only header	<code><Reviewer ReviewItem> or <Approver RequestItem></code>
Attribute based criteria cell	<code>[<entity-name>.]<attribute-name> <Op> <value(s)></code>
Attribute and relationship based criteria cell	<code>[<entity-name>.]<attribute-name> <Op> ReviewItem.<entity-name>.[<relationship-name>.]<attribute-name></code>

NOTE: Specifying only keywords in the header column, and specifying other entity and attributes details in the criteria cells provides more flexibility than other formats.

Operator Syntax

Value entries for attributes that have numeric data types support the following list of comparison prefixes: `>`, `>=`, `<`, `<=`, `!=`, `<>`. For example: `"Permission.risk", "< 40"`.

Value entries for attributes that have string data types support multiple values by using the pipe (`|`) symbol. For example `"Reviewer.user.displayName", "Sue Smith|Jerry Jones|Tom Carter"`. Additionally, you can use the following operators:

- ♦ `!IS_EMPTY!` or `!NULL!`
- ♦ `!IN!`
- ♦ `!CONTAINS!`
- ♦ `!MATCHES!`
- ♦ `!ENDS_WITH!`
- ♦ `!STARTS_WITH!`
- ♦ `!NOT!`

Date Type

The system evaluates date types in comparisons using ISO 8601 date and time format. The following are some examples of January 31, 2017:

- ♦ `2017-01-31`
- ♦ `2017-01-31T10:00Z`
- ♦ `2017-01-31T10:00-05:00`

NOTE: Even though the format allows for time to be specified, Identity Governance only stores the date in the catalog for date entity types.

Supported Relationships

Relationships can be nested in coverage maps. However, relationships cannot be referenced in the ReviewItem criteria cell, they can only be accessed from the Reviewer or Approver criteria cell.

Find below the supported predefined relationships:

Coverage Map Type(s)	Entity	Relationship	Related Entity
REVIEW and REQUEST	USER	supervsior	USER
REVIEW and REQUEST	USER	affiliate	USER
REVIEW and REQUEST	APPLICATION	applicationOwners	applicationOwners (table)
REVIEW and REQUEST	applicationOwners	owner	USER
REVIEW and REQUEST	applicationOwners	groupOwner	GROUP
REVIEW and REQUEST	PERMISSION	permissionOwners	resolved_spermission_owner (table)
REVIEW and REQUEST	resolved_spermission_owner	owner	USER
REVIEW only	ACCOUNT	accountHolders	saccount_user (table)
REVIEW only	saccount_user	holder	USER
REVIEW only	ACCOUNT	accountOwners	resolved_saccount_owner (table)
REVIEW only	resolved_saccount_owner	owner	USER
REQUEST only	ROLE_POLICY (technical role)	role_policyOwners	policy_owner (table)
REQUEST only	policy_owner	owner	USER
REQUEST only	policy_owner	groupOwner	GROUP

NOTE: Any of the relationships that resolve to a table would need another segment to resolve to an ENTITY. For example, APPLICATION.applicationOwners is incomplete, since it resolves to a table. The complete expression should be: APPLICATION.applicationOwners.USER.<attributeName> or APPLICATION.applicationOwners.GROUP.<attributeName>

User Access Review Coverage Map Examples

USER based reviewer with risk and location as criteria

```
"Reviewer.user.displayName", "Permission.risk", "User.location"
"Sue Smith", ">90", "Boston"
"Charles Smith", ">70", "New York"
```


The first line is the header row and contains the column headers that identify the entity attributes that Identity Governance will use to determine reviewers.

The example uses the risk attribute from the permission entity and the location attribute from the user entity to match against review items. Once a review item matches, the example uses the `displayName` attribute from the `User` entity to select a reviewer.

All of the review item criteria columns must match for that row to be considered a match to the review item. In this example, the second line only matches a review item where both the permission's risk is greater than 90 and the user's location is Boston.

USER based reviewer with multiple criteria

```
"Reviewer.user.displayName", "User.department"  
"Armando Colaco", "!STARTS_WITH! Opera"  
"Charles Ward", "!NOT! !MATCHES! Finance"  
"Henry Morgan", "!NOT! !NULL!"
```

The reviewer assignment attempts to perform a match on each row of the coverage map until a match has been found. The first row is the header and contains the entity attributes that are being evaluated. The second row assigns Armando Colaco as reviewer if the department of the user under review starts with `Opera`. The third row assigns Charles Ward as reviewer for users that are not members of the Finance department. The fourth row assigns Henry Morgan as reviewer for users that are members of a department.

During coverage map processing, a matching row is searched for in the order they appear in the CSV file. Once a match has been found for a review item, the reviewers are assigned based on that matching row, and no further rows are processed for that review item.

NOTE: Any review items that do not find a match will be assigned to the review exception queue.

Keywords only header with review item referenced in criteria cells

```
"ReviewItem", "Reviewer"  
"user.department !IN! Transportation|Tours", "user.location ==  
ReviewItem.user.supervisor.location"  
"user.department !NULL!", "user.uniqueUserId !IN!  
ReviewItem.application.applicationOwners.owner.uniqueUserId"
```

In this example, the header cells use a simpler format by using only keywords, and the first criteria row uses relationships to assign reviewer. Note that the `ReviewItem` is referenced within the `Reviewer` criteria cells. For users under review that are in the Transportation or Tours department, reviewer is assigned based on the location of the supervisor of the user

The second criteria row, specifies multiple reviewers based on the owners of the application under review if the department attribute is null.

Account Review Coverage Map Examples

Self and account owners as reviewers

```
"ReviewItem.account.relationToUserType", "Reviewer.user.uniqueUserId"  
"==SHARED", "!IN!ReviewItem.account.accountOwners.owner.uniqueUserId"  
"==SINGULAR", "!IN!ReviewItem.account.accountHolders.holder.uniqueUserId"
```

In this example, the headers cells use keywords and the criteria cells use relationships to specify that all shared accounts are reviewed by the account owner, and single assigned accounts are reviewed by the holder of the account (self).

Supervisors as reviewers

```
"ReviewItem.account.relationToUserType", "Reviewer.user.uniqueUserId"  
"==SHARED", "!IN!ReviewItem.account.accountOwners.owner.supervisorUniqueId"  
"==SINGULAR", "!IN!ReviewItem.account.accountHolders.holder.supervisorUniqueId"
```

In this example, supervisor of the account owner is specified as the reviewer for all shared accounts and supervisor of the holder of the account is specified as reviewer for single accounts.

Access Request Coverage Map Example

Policy owners as approvers

```
"Approver.user.uniqueUserId", "Approver.group.uniqueGroupId", "RequestItem"  
"!IN! RequestItem.role_policy.policyOwners.owner.uniqueUserId", "!IN!  
RequestItem.role_policy.policyOwners.groupOwner.uniqueGroupId", "role_policy.risk >  
30"
```

In this example, for access requests to technical roles, if risk is greater than 30, then the policy owner is assigned as the approver.

Loading Coverage Map

To load coverage map:

- 1 Log in to Identity Governance as a Global or Data Administrator.
- 2 Select **Administration**.
- 3 Select **Coverage Maps** to expand the section.
- 4 To add a new coverage map:
 - 4a Select **+**.
 - 4b Select coverage map type: **REVIEW** or **REQUEST**.
 - 4c Enter coverage map name and description.
 - 4d Browse for the coverage map CSV file.
 - 4e Select **Save**.
- 5 Repeat the above steps to upload additional coverage maps.
- 6 To preview the map, select the number of segments.
- 7 To modify a coverage map:
 - 7a Select the coverage map.
 - 7b Browse for a different CSV file.
 - 7c Select **Open** to upload and replace the selected CSV file.
- 8 To delete a coverage map, select **Delete**.

NOTE: Only coverage maps not in use can be deleted.

Customizing Categories

Identity Governance allows you to set up categories to organize applications, permissions, business roles, and technical roles. You can define these categories in Identity Governance and assign them to entities. To customize your categories offline and upload them in bulk, you can export a JSON file, edit it, and import it to modify categories and category assignments.

- 1 Log in to Identity Governance as a Global or Data Administrator.
- 2 Select **Administration > Categories**.
- 3 To add new categories, select **+** and enter a name and description for the category.
- 4 (Optional) Assign the category to entities:
 - 4a Select **+** next to **Assign entities**.
 - 4b Select the entity type and then select specific entities to assign the category to.
 - 4c When you have selected all the entities, select **Add**.
 - 4d Each entity type with that category assigned now has a tab on the **Category** window. From this window you can remove the category assignment, if needed.
- 5 Select **Save** and then close the window.
- 6 To edit categories in bulk, select **Export Categories** and save the json file.
- 7 After you have edited the file, select **Import Categories** to import the file.

Customizing Review Display

Identity Governance allows you to customize the columns displayed in reviews by review type and review definition.

To select user attributes that can be displayed:

- 1 Log in to Identity Governance as a Global or Review Administrator.
- 2 Select **Administration > Review Display Customization**.
- 3 For each review type, drag-and-drop columns to add, rearrange, or remove a column from reviewer display.
- 4 Click **Save**.

NOTE: Review administrators can either use these default per review type settings or further customize default columns for each review using **Reviews > Definitions > + > Default Reviewer Display Preferences**. In addition, they can also select default grouping and sort options. Only attributes selected in **Review Display Customization** will appear as a column in **Default Reviewer Display Preferences**.

NOTE: To show attribute in expanded details, Global or Data Administrator can select the attribute in the attribute type section of the **Data Administration** area, such as the Department attribute in **Data Administration > User**, and then select **Display in Quick Info views** under **Listable Options**.

Configuring Reasons for Review Actions

Identity Governance allows you to configure reasons for review actions for analytical and reporting purposes. Global or Review Administrator can configure reasons for:

- ♦ Changing reviewers
- ♦ Modifying review items by specifying fulfillment instructions

Once the reasons are configured, they are available as drop-down list options when a review owner or a reviewer changes the reviewer for a review item, and when a reviewer selects **Modify** action in an **User Access Review** or selects **Modify with instructions** in an **Account Review**.

- 1 Log in to Identity Governance as a Global or Review Administrator.
- 2 Select **Administration** and **Change Reviewer Reasons** or **Modify Review Item Reasons**.
- 3 To add a new reason, click **+** and enter a reason. For example, you can add Reviewer is on vacation as a reason for changing reviewer or Assign account custodian as a reason for modifying a review item in Account Review.
- 4 (Conditional) If the modify review item reason requires user selection, click the **User selection required** check box.
- 5 Click **Save**.
- 6 To edit the reason, select the reason and edit it.
- 7 To delete a reason, select the reason and click **Delete**.

NOTE: Once a reason has been used in a review, you can see the number of times it has been used in reviews in the respective reason tab. If the reason has been used even once in any review, you can no longer edit or delete it. However, you can **Enable** or **Disable** the reason. Reviewers will not see the disabled reason as an option in the drop-down list.

Disabling Review Email Notifications

Identity Governance enables you to customize and set up various event notifications. Administrators can also disable notifications during access governance life cycle using the Identity Governance Configuration utility.

To disable review email notifications:

- 1 Stop Tomcat. For examples, see [“Stopping, Starting, and Restarting Tomcat” on page 52](#).
- 2 Launch the Identity Governance Configuration utility in console mode. For examples, see [“Running the Identity Governance Configuration Utility” on page 129](#).
- 3 Enter suppress commands for the emails you want to disable as shown in the following examples.

WARNING: Disabling review notifications will be a global change and will be applied to *all* reviews.

- 3a To stop review termination notifications being sent out to the Review Owner and Reviewers when a running Review is terminated follow these steps:
 - 3a1 Enter `dc com.netiq.iac.reviews.suppressReviewTerminationEmail`. No value should be returned.
 - 3a2 Enter `sp com.netiq.iac.reviews.suppressReviewTerminationEmail true`.

- 3a3** Press Up-arrow two times so that the dc command is active.
- 3a4** Press Enter. You should see

```
com.netiq.iac.reviews.suppressReviewTerminationEmail = true.
```
- 3b** To disable losing permission notification from being sent to the employee that is about to have a permission revoked follow these steps:
 - 3b1** Enter dc

```
com.netiq.iac.reviews.fulfillment.suppressLosingPermissionEmail. No
```

 value should be returned.
 - 3b2** Enter sp

```
com.netiq.iac.reviews.fulfillment.suppressLosingPermissionEmail true.
```
 - 3b3** Press Up-arrow two times so that the dc command is active.
 - 3b4** Press Enter. You should see

```
com.netiq.iac.reviews.fulfillment.suppressLosingPermissionEmail = true.
```
- 4** Exit the console mode.
- 5** Delete the `localhost` folder in the `tomcat/work/Catalina` directory.
- 6** Start Tomcat. For examples, see [“Stopping, Starting, and Restarting Tomcat” on page 52.](#)

Extending the Identity Governance Schema

Identity Governance contains a default schema for entities that you collect in the catalog. If the default schema provided does not meet your needs, you can extend the Identity Governance schema. Extending the schema is a simple process.

Extending the schema is adding attributes to the default schema provided. You can view the default schema for Identity Governance in the console. You login as an global administrator or data administrator to view the schema. The schema is listed under the **Data Administration** menu.

- ♦ [“Adding or Editing Attributes to Extend the Schema” on page 173](#)
- ♦ [“Adding Attributes to a Collector” on page 175](#)
- ♦ [“Viewing Available Attributes in Business Roles” on page 176](#)

Adding or Editing Attributes to Extend the Schema

Identity Governance provides a simple way to extend the schema for the different entities. You add additional attributes and define properties. You can also download attributes as `json` files to edit the properties. After editing, you can import the attributes on the page that lists all attributes for a given entity.

- 1** Log in to Identity Governance as a Global or Data Administrator.
- 2** Under **Data Administration**, select the entity where you want to add or edit the attribute.
 - ♦ **User**
 - ♦ **Account**
 - ♦ **Permission**
 - ♦ **Business Roles**

NOTE: You cannot extend the schema for groups. Identity Governance does not allow it.

- 3** Select the plus sign **+** to add a new attribute or select an existing attribute to edit the properties.

4 Add or edit the attribute by configuring the following:

NOTE: Some values might not be editable, depending on the Attribute Behavior settings.

Attribute name and Key

Specify the attribute name and key. It is the same value for both fields. The attribute name must be unique to your Identity Governance environment.

Type

Select the type of attribute you want to create. The types are **String**, **Boolean**, **Double**, **Long**, **Date**, and **Locale**.

Maximum size

Specify the number of characters allowed for the value of this attribute.

Truncate to size

Enable to allow the system to handle values longer than the attribute's maximum size. If this is not enabled, and the value is longer than the maximum size, it will cause an error and the record will not be collected.

Attribute Behavior

Select the behavior of the attribute. The attribute can be required, allowed to change, allowed to have multiple values, or allowed to have a static value.

Listable Options

Select how you want the attribute displayed in the Identity Governance Console.

Display in Quick Info views

Allows anyone with rights to view reviews to see the attribute. This option does not allow the attribute to be changed.

Display in lists and detail views

Allows administrators to view and change the information in the Identity Governance console.

Sortable in table columns

Allows administrators to store the attribute in the table columns.

Searchable Options

Select how you want the new attribute to be searched for in Identity Governance.

- ♦ Available in catalog searches. Changes take effect after publication.
- ♦ Display as refine search option
- ♦ Display in review item selection criteria
- ♦ Display in business role selection criteria
- ♦ Available in typeahead searches

IMPORTANT: For all attributes that you have configured for authentication matching rules, ensure that you enable the following list and search options for these attributes:

- ♦ Display in lists and detail views
- ♦ Available in catalog searches. Changes take effect after publication.

For more information, see ["Security Settings" on page 131](#).

5 Select **Save**.

Adding Attributes to a Collector

If a collector you are using does not contain the schema you need, you can simply extend the schema of the collector by adding additional attributes. You must have already created and configured the collector before performing the following steps. For more information, see [Chapter 15, “Creating and Managing Data Sources,”](#) on page 195.

- 1 Log in to Identity Governance as a Global Administrator.
- 2 Select **Data Sources > Identities > Your Identity Source**.
- 3 Select **Collect Identity > Collect Identity Attributes > Add attribute**.
- 4 Add the attribute by configuring the following:

Attribute name and Key

Specify the attribute name and key. It is the same value for both fields. The attribute name must be unique to your Identity Governance environment.

Type

Select the type of attribute you want to create. The types are **String**, **Boolean**, **Double**, **Long**, **Date**, and **Locale**.

Maximum size

Specify the number of characters allowed for the value of this attribute.

Truncate to size

Enable to allow the system to handle values longer than the attribute's maximum size. If this is not enabled, and the value is longer than the maximum size, it will cause an error and the record will not be collected.

Attribute Behavior

Select the behavior of the attribute. The attribute can be required, allowed to change, allowed to have multiple valued, or allowed to have a static value.

Listable Options

Select how you want the attribute displayed in the Identity Governance Console.

Display in Quick Info views

Allows anyone with rights to view reviews to see the attribute. This option does not allow the attribute to be changed.

Display in lists and detail views

Allows administrators to view and change the information in the Identity Governance console.

Sortable in table columns

Allows administrators to store the attribute in the table columns.

Searchable Options

Select how you want the new attribute to be searched for in Identity Governance.

- ♦ Available in catalog searches.Changes take effect after publication.
- ♦ Display as refine search option
- ♦ Display in review item selection criteria
- ♦ Display in business role selection criteria

- 5 Select **Save**.

Viewing Available Attributes in Business Roles

When you create a business role, you define a membership expression that search for all users that meet a certain criteria to be added to the business role. For more information, see [“Defining Business Roles” on page 277](#).

The **Membership expression** lists all of the available attributes you can match on under the **Title** field. This list matches the list displays under **Data Administration > Business Roles**. If you want to add more items to this list, you must add a new attribute to the business roles schema.

NOTE: Only Bootstrap, Global, Data or Business Role administrator have rights to administer business role schema. For more information, see [“Adding or Editing Attributes to Extend the Schema” on page 173](#).

12 Changing Passwords for Administrative Users

Identity Governance has a number of embedded users to make the product work. For example, there is a bootstrap administrator and database users. You might need to change the passwords for these users to meet security standards at your company. Identity Governance allows to change these administrative passwords, however, it is a manual process.

- ♦ [“How to Change the Password for the Bootstrap Administrator” on page 177](#)
- ♦ [“How to Change the Password for the Database Users” on page 178](#)

How to Change the Password for the Bootstrap Administrator

If you have the bootstrap administrator coming from the file system, use the following steps to change the password.

- 1 Stop Tomcat. For more information, see [“Stopping, Starting, and Restarting Tomcat” on page 52](#).
- 2 Access the following directory in a terminal:
 - ♦ **Linux:** `/opt/netiq/idm/apps/idgov/lib`
 - ♦ **Windows:** `C:\netiq\idm\apps\idgov\lib`
- 3 With Java in your path enter:

```
java -jar ig-pwtool.jar%new-password-value%
```

For example:

```
java -jar ig-pwtool.jar Netiq123
```
- 4 Copy the value that is returned.
- 5 Navigate to the following directory:
 - ♦ **Linux:** `/opt/netiq/idm/apps/idgov/osp`
 - ♦ **Windows:** `C:\netiq\idm\apps\idgov\osp`
- 6 Edit the `adminsusers.txt` file.
 - 6a In a text editor, open the file `adminusers.txt`.
 - 6b Replace the current value (which will be the second entry in the file) with the one you copied from [Step 4](#).
 - 6c Save and close the file.
- 7 Restart Tomcat. For more information, see [“Stopping, Starting, and Restarting Tomcat” on page 52](#).

How to Change the Password for the Database Users

If you must change the password for the database users, use the following steps.

- 1 Stop Tomcat. For more information, see [“Stopping, Starting, and Restarting Tomcat” on page 52](#).
- 2 Log in to the database server with the appropriate administrator tool and update the necessary users passwords. For example, `igops`
- 3 Access the following directory in a terminal:
 - ♦ **Linux:** `/opt/netiq/idm/apps/idgov/bin`
 - ♦ **Windows:** `C:\netiq\idm\apps\idgov\bin`
- 4 Enter the following command:
 - ♦ **Linux:** `./encode-password.sh %password-set-above%`
 - ♦ **Windows:** `encode-password.cmd %password-set-above%`

For example:

```
./encode-password.sh Netiq123
```

- 5 Record the value that is returned.
- 6 Repeat [Step 4](#) and [Step 5](#) for each database user.
- 7 Navigate to the following directory:
 - ♦ **Linux:** `/opt/netiq/idm/apps/tomcat/conf`
 - ♦ **Windows:** `C:\netiq\idm\apps\tomcat\conf`
- 8 Edit the `server.xml` file.
 - 8a Open the `server.xml` file in a text editor.
 - 8b Find the user name that you updated above:
For example: `username="igops"`
 - 8c Find the `password=` entry for that database connection, then replace the current value with the value you recorded in [Step 5](#).
 - 8d Repeat these steps for each database user.
 - 8e Save and close the file.
- 9 Restart Tomcat. For more information, see [“Stopping, Starting, and Restarting Tomcat” on page 52](#).

13 Adding Identity Governance Users and Assigning Authorizations

Individuals who can log in to Identity Governance are **Identity Governance users**. The authentication server for Identity Governance must include login information for all Identity Governance 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 Identity Governance, you can assign them to one of the built-in authorizations.

- ♦ [“Understanding Authorizations in Identity Governance” on page 179](#)
- ♦ [“Adding Identity Governance Users” on page 184](#)
- ♦ [“Assigning Authorizations to Identity Governance Users” on page 184](#)

Understanding Authorizations in Identity Governance

Identity Governance relies on authorizations to define a fixed set of authorizations and permissions. Identity Governance authorizations can be global or runtime:

- ♦ **Global authorizations** are constant within Identity Governance and assigned through the Identity Governance **Administration** settings. Identity Governance maintains the set of privileges granted by the authorization. For more information, see [“Global Authorizations” on page 179](#).
- ♦ **Runtime authorizations** are those that users assume as needed during an access review and validation cycle. For example, you assign a Review Owner as needed during an access review and validation cycle. You can reassign these authorizations with each review run. For more information, see [“Runtime Authorizations” on page 181](#).

NOTE: When you install Identity Governance, use the bootstrap administrator authorization to collect and publish an initial set of identities. You can then use these identities as authorized users for Identity Governance and assign authorizations to them. If a user does not have the required authorization or does not have an assigned task, the user will be redirected to the Access Request interface. For more information about requesting access, see [Chapter 33, “Instructions for Access Requesters and Approvers,” on page 327](#). For more information about the bootstrap administrator, see [“Understanding the Bootstrap Administrator for Identity Governance” on page 29](#).

Global Authorizations

After collecting and publishing an initial set of identities, assign the Global Administrator authorization to one of these identities. Then the Global Administrator can assign the rest of the global authorizations. For more information, see [“Assigning Authorizations to Identity Governance Users” on page 184](#).

Global Administrator

The Global Administrator is the primary authorization and can:

- ♦ Perform all Identity Governance actions
- ♦ Assign all Identity Governance global and runtime authorizations

Access Request Administrator

The Access Request Administrator manages defining who can request access in your enterprise. This authorization can:

- ♦ Create, modify, and delete Access Request Policies
- ♦ Create, modify, and delete Access Request Approval Policies
- ♦ Edit the default Access Request Approval Policy

Auditor

The Auditor has read-only rights to the catalog, reviews, separation of duties policies and violations, fulfillment status, and the **Overview**. However, an account assigned to the Auditor authorization might also be specified as a Review Auditor in a review definition. For more information, see [“Runtime Authorizations” on page 181](#).

Business Roles Administrator

The Business Roles Administrator performs all administrative functions for all business roles. A Business Roles Administrator can delegate administrative privileges. This authorization can:

- ♦ Administer business role schema under **Data Administration**
- ♦ Mine for business roles
- ♦ Create a business role
- ♦ Modify a business role
 - ♦ Add or change role owners, fulfillers, and categories
 - ♦ Add or change the business role approval policy
 - ♦ Add users and groups to the business role
 - ♦ Exclude users and groups from the business role
- ♦ Publish a business role
- ♦ Delete a business role
- ♦ Analyze business roles
- ♦ Configure the business roles default approval policy
- ♦ Create and modify business roles approval policies

Data Administrator

The Data Administrator manages the identity and application data sources. This authorization can:

- ♦ Create, add, modify, and review data sources
- ♦ Create custom metrics
- ♦ Create scheduled collections
- ♦ Execute data collection and publishing
- ♦ Create and map attributes in the catalog
- ♦ Review and edit data in the catalog
- ♦ Delegate responsibility by assigning application administrators, application owners, or manual fulfillers to applications in the catalog
- ♦ Assign delegates for users
- ♦ View data collection, data summary, and system trends in the **Overview**

Fulfillment Administrator

The Fulfillment Administrator manages fulfillment and verification of requests that result from reviews. This authorization can:

- ♦ Access real time and historical data for provisioning activities, including fulfillment status and verification management

Report Administrator

The Report Administrator can access Identity Reporting. This authorization can:

- ♦ Create, view, and run reports for Identity Governance

Review Administrator

The Review Administrator manages the review process but does not have access to data collection or fulfillment settings. This authorization can:

- ♦ Create, schedule, and start reviews in preview or live mode
- ♦ Modify a review schedule
- ♦ Assign delegates for users
- ♦ Assign all the runtime authorizations as part of a review, thereby delegating certain rights pertaining to the review to those authorizations
- ♦ View running reviews
- ♦ View data summary and system trends in the [Overview](#)
- ♦ View the [Catalog](#) but cannot modify it

Technical Roles Administrator

The Technical Roles Administrator mines for technical role candidates, creates and manages technical roles.

Security Officer

The Security Officer has read-only rights to the catalog and can:

- ♦ Assign authorizations for all functions in Identity Governance
- ♦ View data summary in the [Overview](#)
- ♦ View the [Catalog](#) but cannot modify it

NOTE: Ensure that the users assigned to the Security Officer authorization can also be trusted with global privileges in Identity Governance.

Separation of Duties Administrator

The Separation of Duties Administrator creates and manages SoD policies and violation cases.

Runtime Authorizations

Assign runtime authorizations when you need them. For more information, see [“Assigning Authorizations to Identity Governance Users” on page 184](#).

Access Request Approver

Access Request Approvers confirm whether to approve or deny requested access in the Request application. Identity Governance assigns this authorization if an Access Request Approval policy specifies approvers.

Application Owner

The Application Owner manages all assigned applications. This authorization can:

- ♦ View the catalog
- ♦ Perform data editing for assigned applications
- ♦ Review data and access within the assigned applications, depending on selections as a reviewer
- ♦ (Conditional) Review access entitlements or remediate access policy violations within the application if assigned this responsibility by the review definition

Application Administrator

The Application Administrator validates published data and performs data clean-up, or editing, for all assigned applications. This authorization can:

- ♦ Modify the configuration of a data source
- ♦ Execute collections for the data source
- ♦ Edit data within the scope of the data source
- ♦ Review data and access within the data source
- ♦ View the catalog but edit only items related to the assigned data source

Business Role Owner

The Business Role Owner can review a business role and potentially approve a business role depending on whether or not the assigned approval policy specifies **Approved by owners**.

Business role owners cannot edit business roles, they can only view them. For more information, see [Chapter 25, “Creating and Managing Business Roles,” on page 273](#).

Business Role Manager

A Business Role Manager can edit the assigned business roles, create, and delete new draft versions of the role but cannot delete the business role completely.

Escalation Reviewer

The Escalation Reviewer is an optional participant in a review. All tasks not completed on time are forwarded to the Escalation Reviewer for resolution. Otherwise, the tasks are forwarded to the Review Owner. This authorization can:

- ♦ View user, permission, application, and account details in the context of the review
- ♦ Decide whether to keep, modify, or remove access privileges for a user under review
- ♦ Edit review decisions before submitting those items

For more information about assigning an escalation reviewer in a review definition, see [“Specifying Reviewers” on page 256](#).

Fulfiller

The Fulfiller performs manual provisioning for access changes. This authorization can:

- ♦ View the changeset, identity, permission, and application details for each fulfillment request
- ♦ View guidance from collected analytics data about the requested change
- ♦ View the reason for the requested change and the source of the request, such as a review run, business role fulfillment, or SoD policy
- ♦ Fulfill, decline to fulfill, or reassign requests

Review Auditor

The Review Auditor authorization verifies a review campaign. Each review can have its own Review Auditor. This authorization can:

- ♦ Accept or reject the review after the Review Owner marks the review complete
- ♦ View the data related to the review but cannot modify the data

Review Owner

The Review Owner manages all assigned review instances. The Review Owner can view the details of any user, permission, or application entity within the context of the campaign. This authorization does not have general access to the catalog.

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

NOTE: If you assign a new owner to a review, both the previous and new owners can access the review. The previous owner continues to see review instances run before the ownership change. The new owner sees only the instances run after the ownership change.

For an active Review, the Review Owner can:

- ♦ Start and monitor the review progress
- ♦ Resolve access policy violations in the review
- ♦ Reassign certification tasks within the review
- ♦ Run reports against the review
- ♦ Declare the review complete
- ♦ View review status in **Overview**
- ♦ View **Quick Info** details about a catalog item
- ♦ View fulfillment status of a review item
- ♦ View run history

Reviewer

The Reviewer authorization reviews sets of access permissions or memberships as part of a review run. This authorization can:

- ♦ Decide whether to keep, modify, or remove access privileges for a user under review
- ♦ Decide whether to keep or remove business role membership for a user under review
- ♦ Change the reviewer for any assigned review items
- ♦ View user, permission, application, and account details in the context of the review
- ♦ View a history of review decisions in the context of the review
- ♦ Edit review decisions before submitting them

For more information about assigning reviewers, see [“Specifying Reviewers” on page 256](#).

SoD Policy Owner

The SoD Policy Owner is responsible for managing assigned Separation of Duties policies. This authorization can:

- ♦ Manage assigned policies
- ♦ Manage violation cases for assigned policies

Adding Identity Governance Users

Until you collect data for your Identity Governance users, no one can log in to the application without using the bootstrap administrator account. Do not use the bootstrap administrator after you add your Identity Governance users to the Identity Governance attribute catalog and assign global authorizations to the users. For more information about the bootstrap administrator account, see [“Understanding the Bootstrap Administrator for Identity Governance” on page 29](#). For more information about mapping attributes, see [“Configuring the Data Source for Post Authentication Matching” on page 225](#).

NOTE: In a test environment that does not also use Identity Manager, you might not have an LDAP authentication server to use for your data source. Instead, you can use a CSV file that contains login information for Identity Governance users. The CSV file must use UTF-8 encoding.

To add Identity Governance users:

- 1 Log in to Identity Governance with an Identity Governance bootstrap, global or data administrator account.
- 2 In the **Data Sources**, select **Identities**.
- 3 Under **Identity Sources**, select the LDAP authentication server that you specified during installation.

Alternatively, you can specify a CSV file.

NOTE: If Identity Governance does not list the authentication server, select + to add the identity source. For more information, see [“Creating Identity and Application Sources” on page 201](#).

- 4 To collect the identities from the authentication server, select the icon for **Collect Now**. Later, you can set up scheduled collections to update your catalog.

For more information, see [Chapter 16, “Creating and Monitoring Scheduled Collections,” on page 211](#).

- 5 When collection is completed, select the icon for **Publish identities now**.
 - 6 Assign Identity Governance authorizations to the appropriate identities that you collected.
- For more information, see [“Assigning Authorizations to Identity Governance Users” on page 184](#).

Assigning Authorizations to Identity Governance Users

The method for assigning authorizations in Identity Governance depends on the type of authorization.

Authorization	Assignment Method	Assigned By
Access Request Approver	Access Request Approval policy	Access Request Administrator or Global Administrator
All global authorizations	Administration menu	Bootstrap administrator or Global administrator
Application Administrator	Application in the catalog	Application Owner, Data Administrator, Global Administrator, or Security Officer

Authorization	Assignment Method	Assigned By
Application Owner	Application in the catalog or review definition	Data Administrator, Global Administrator, or Security Officer
Business Role Manager	Business role definition	Business Roles Administrator, Global Administrator, or Security Officer
Business Role Owner	Business role definition	Business Roles Administrator, Global Administrator, or Security Officer
Escalation Reviewer	Review definition	Review Administrator or Global Administrator
Fulfiller	Application setup in Fulfillment > Configuration or Business Role definition	Business Roles Administrator, Fulfillment Administrator, Global Administrator, or Security Officer
Permission Owner	Review definition	Global Administrator, Data Administrator, or Security Officer
Review Auditor	Review definition	Review Administrator or Global Administrator
Review Owner	Review definition	Review Administrator, Review Owner, or Global Administrator
Reviewer	Review definition	Review Administrator or Global Administrator
SoD Policy Owner	SoD policy definition	Separation of Duties Administrator or Global Administrator
Technical Role Owner	Technical role definition	Technical Roles Administrator or Global Administrator

14 Integrating Single Sign-on Access with Identity Manager

If you have installed Identity Manager, your users can log in a single time to access the Identity Manager applications, Identity Reporting, and Identity Governance. NetIQ uses the OSP service for OAuth authentication, which provides users single sign-on access from the Identity Manager Home page. To ensure single sign-on access, you must configure both Identity Manager and Identity Governance. Users can easily shift between the two applications without needing to enter their credentials a second time.

Identity Governance must use the same authentication server that the identity applications use.

- ♦ “Checklist for Integrating Identity Governance with Identity Manager” on page 187
- ♦ “Configuring Identity Governance for Integration” on page 188
- ♦ “Configuring Identity Manager for Integration” on page 189
- ♦ “Configuring a File Authentication Source for the Bootstrap Administrator” on page 190

Checklist for Integrating Identity Governance with Identity Manager

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

	Checklist Items
<input type="checkbox"/>	1. To ensure that you have the correct software versions for integration, review the latest release notes for Identity Governance and Identity Manager identity applications. For more information, see the Identity Manager Documentation site (https://www.netiq.com/documentation/identity-manager/) .
<input type="checkbox"/>	2. (Conditional) Create an index in eDirectory for the login attribute if you do not use a standard login attribute. For more information, see “ Ensuring Rapid Response to Authentication Requests ” on page 105.
<input type="checkbox"/>	3. Ensure that users can link to Identity Manager Home from Identity Governance. For more information, see “ Adding a Link to Identity Manager Home in the Identity Governance Menu ” on page 188.
<input type="checkbox"/>	4. Ensure that Identity Governance connects to the authentication server for Identity Manager. For more information, see “ Using the Same Authentication Server as Identity Manager ” on page 188.
<input type="checkbox"/>	5. Update Identity Manager Home to connect to Identity Governance. For more information, see “ Configuring Identity Manager for Integration ” on page 189.
<input type="checkbox"/>	6. (Optional) Integrate Identity Governance with the workflows used in Identity Manager. For more information, see “ Using Workflows to Fulfill the Changeset ” on page 261 and “ Configuring Fulfillment ” on page 138.

For more information about Identity Manager, see the [NetIQ Identity Manager Overview and Planning Guide](#).

Configuring Identity Governance for Integration

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

- ♦ [“Adding a Link to Identity Manager Home in the Identity Governance Menu” on page 188](#)
- ♦ [“Using the Same Authentication Server as Identity Manager” on page 188](#)

Adding a Link to Identity Manager Home in the Identity Governance Menu

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

- 1 Log in to Identity Governance with an account that has the Global Administrator authorization.
- 2 Select **Administration > General Settings**.
- 3 For **Home Page URL**, specify the URL for Identity Manager Home.
- 4 Select **Save**.
- 5 Sign out of Identity Governance.
- 6 (Optional) To verify the integration, complete the following steps:
 - 6a Log in to Identity Governance. Verify that Identity Governance lists **Home** in the navigation pane.
 - 6b Select **Home**, and verify that it takes you to the Identity Manager Home page.

Using the Same Authentication Server as Identity Manager

This section describes how to configure Identity Governance to use the same authentication server as Identity Manager identity applications for verifying users who log in. This section assumes that, when you installed Identity Governance, you did not specify the Identity Manager authentication server. For example, you might have installed Identity Governance before adding Identity Manager to your environment.

- 1 Stop Identity Governance and Tomcat. For examples, see [“Stopping, Starting, and Restarting Tomcat” on page 52](#).
- 2 In the Identity Governance Configuration Utility, select **Authentication Server Details**.
- 3 Clear **Same as IG Server**.
- 4 Specify the protocol, DNS host name or IP address, and port that represent the authentication server for Identity Manager identity applications.

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

- 5 Select **Save**.
- 6 Make a note of the settings for the authentication server.

The values for these settings must match the settings that you specify for Identity Governance in the RBPM Configuration utility. For more information, see [“Configuring Identity Manager for Integration” on page 189](#).

- 7 Select **Security Settings**, and make a note of the settings in the **General Service** section.
The values for these settings must match the settings that you specify for Identity Governance in the RBPM Configuration utility. For more information, see [“Configuring Identity Manager for Integration” on page 189](#).
- 8 Close the utility.
- 9 Start Identity Governance and Tomcat. For examples, see [“Stopping, Starting, and Restarting Tomcat” on page 52](#).

Configuring Identity Manager for Integration

To ensure proper integration, you must update your version of Identity Manager identity applications to recognize Identity Governance. The process includes copying files from the Identity Governance installation to the Identity Manager identity applications installation.

NOTE: Ensure that you have configured single sign-on for the Identity Manager identity applications. For more information, see

- ♦ **Linux:** “Configuring Single Sign-on Access in Identity Manager” in the [NetIQ Identity Manager Setup Guide for Linux](#).
 - ♦ **Windows:** “Configuring Single Sign-on Access in Identity Manager” in the [NetIQ Identity Manager Setup Guide for Windows](#).
-

- 1 On the server where you installed Identity Governance, log in as an administrator.
- 2 Navigate to the `/osp` folder in the installation directory for Identity Governance. For example:
 - ♦ **Linux:** Default location of `/opt/netiq/idm/apps/idgov/osp`
 - ♦ **Windows:** Default location of `C:\netiq\idm\apps\osp`
- 3 Copy the `uaconfig-ig-defs.xml` file to a location or thumb drive that you can access from the server running Identity Manager identity applications.
- 4 Sign out of the server.
- 5 On the server where you installed the identity applications, log in as an administrator.
- 6 Stop the application server. For examples, see [“Stopping, Starting, and Restarting Tomcat” on page 52](#).
- 7 Navigate to the `conf` directory of the application server.
 - ♦ **Linux:** Default location of `/opt/netiq/idm/apps/tomcat/conf`
 - ♦ **Windows:** Default location of `C:\netiq\idm\apps\tomcat\conf`
- 8 Place the `uaconfig-ig-defs.xml` file from the Identity Governance installation in the `/conf` directory.
- 9 In a text editor, open the `configupdate.sh` or `configupdate.bat` file.
 - ♦ **Linux:** Default location of `/opt/netiq/idm/apps/UserApplication/configupdate.sh`
 - ♦ **Windows:** Default location of `C:\netiq\idm\apps\UserApplication\configupdate.bat`
- 10 In the file, add the following line before the `-Duser.language` entry:

```
-Dcom.netiq.uaconfig.impl.custom.clients=path_to_conf_dir/uaconfig-ig-defs.xml
```

For example:

```
-Dcom.netiq.uaconfig.impl.custom.clients=/opt/netiq/idm/apps/tomcat/server/  
IDMProv/conf/uaconfig-ig-defs.xml
```

- 11 Save and close the file.
- 12 Launch the configuration update utility. by running from the command prompt.

- ♦ **Linux:** Enter:

```
./configupdate.sh
```

- ♦ **Windows:** From a command line enter:

```
configupdate.bat
```

- 13 In the utility, select **Identity Governance SSO Client**.

NOTE: If the utility does not display the **Identity Governance SSO Client** tab, ensure that you copied the correct files from the Identity Governance installation to the identity applications installation.

- 14 Specify the values based on the **OAuth SSO Client** and **Security Settings > General Service** settings that you observed in [Step 6](#) through [Step 7](#) in “[Using the Same Authentication Server as Identity Manager](#)” on page 188.

Observe the following considerations for these settings:

- ♦ By default, the **OAuth client ID** is `iac`. You specified the client ID and its password when you specified the client secret during the Identity Governance installation.
- ♦ **OAuth redirect URL** must be an absolute URL and include the specified value for OAuth client ID. For example, `http://myserver.host:8080/oauth.html`. By default, the configuration utility provides some of this URL. However, you must ensure that you add the server and port information.

- 15 Save your changes and close the utility.
- 16 In the directory of the application server, clear out the `/temp` and `/work` directories.
- 17 Start the application server. For examples, see “[Stopping, Starting, and Restarting Tomcat](#)” on [page 52](#).
- 18 Add a link to Identity Governance on the Identity Manager Home page.
For more information, see “[Identity Manager Dashboard](#)” in the *NetIQ Identity Manager - Administrator's Guide to the Identity Applications*.
- 19 On the Identity Governance server, start Identity Governance (and Tomcat). For examples, see “[Stopping, Starting, and Restarting Tomcat](#)” on [page 52](#).

Configuring a File Authentication Source for the Bootstrap Administrator

If you want to use a file as the authentication source for the bootstrap administrator instead of LDAP authentication, complete the following steps. You might need to modify the files Configuration Update utility files (`configupdate.sh.properties` or `configupdate.bat.properties` and `configupdate.sh` or `configupdate.bat`) similar to [Step 9](#) through [Step 12](#) in “[Configuring Identity Manager for Integration](#)” on [page 189](#).

- 1 (Optional) Make a backup copy of both the Configuration Update utility and properties files for the identity applications.
 - ♦ **Linux:** `/opt/netiq/idm/apps/UserApplication` and the files are `configupdate.sh.properties` and `configupdate.sh`.

- ♦ **Windows:** c:\netiq\idm\apps\UserApplication and the files are configupdate.bat.properties and configupdate.bat.
- 2 (Optional) Copy both the Configuration Update utility and the properties files to the /conf directory of the application server.
 - ♦ **Linux:** Default path of /opt/netiq/idm/apps/tomcat/conf
 - ♦ **Windows:** c:\netiq\idm\apps\tomcat\conf
 - 3 In a text editor, open the configupdate.sh or configupdate.bat file.
 - 4 In the file, add the following line before the -Duser.language entry in the JAVA_OPTS shell variable.
For example:
 - ♦ **Linux:** Using the default installation path:


```
-Dcom.netiq.uaconfig.impl.custom.clients=/opt/netiq/idm/apps/tomcat/server/IDMProv/conf/uaconfig-ig-defs.xml
```
 - ♦ **Windows:** Using the default installation path:


```
-Dcom.netiq.uaconfig.impl.custom.clients=c:\netiq\idm\apps\tomcat\server\IDMProv\conf\uaconfig-ig-defs.xml
```
 - 5 Save and close the file.
 - 6 In a text editor, open the configupdate.sh.properties or the configupdate.bat.properties file.
 - 7 Set INSTALL_JAVA_BASE as the path to the Oracle Java instance that Tomcat uses.
For example:
 - ♦ **Linux:** INSTALL_JAVA_BASE="/root/jdk1.x.x_xx"
 - ♦ **Windows:** INSTALL_JAVA_BASE="c:\Program_Files\jdk1.x.x.xx"
 - 8 Set CONFIG_FILENAME as "ism-configuration.properties".
For example:


```
CONFIG_FILENAME="ism-configuration.properties"
```
 - 9 Save and close the file.
 - 10 Launch the Configuration Update utility.
 - ♦ **Linux:** From the command line, enter ./configupdate.sh
 - ♦ **Windows:** From the command line, enter configupdate.bat
 - 11 In the Configuration Update utility, select **Identity Governance SSO Client** and select **Show Advanced Options**.
 - 12 Enter the file location in the **File Authentication Source** field and the file name in the **File Name** field. The default file name is adminusers.txt.
 - 13 Save your changes and close the utility.



Managing the Identity Governance Catalog

The Identity Governance catalog contains all of the identities and permissions in your organization that you choose to collect. You use this information to create a unified identity for each person in your organization so you can review the permissions assigned to them.

- ♦ [Chapter 15, “Creating and Managing Data Sources,” on page 195](#)
- ♦ [Chapter 16, “Creating and Monitoring Scheduled Collections,” on page 211](#)
- ♦ [Chapter 17, “Integrating Collected Data with Identity Manager,” on page 215](#)
- ♦ [Chapter 18, “Publishing the Collected Data,” on page 221](#)
- ♦ [Chapter 19, “Managing Data in the Catalog,” on page 225](#)
- ♦ [Chapter 20, “Grooming the Identity Governance Databases,” on page 237](#)

To manage the Identity Governance catalog, you must have a Data Administrator, Global Administrator, or bootstrap administrator authorization.

15 Creating and Managing Data Sources

To certify that your users have the appropriate levels of access to your resources and applications, you need to populate the Identity Governance catalog with the identities, application accounts, and application permissions that exist in your environment. Identity Governance organizes data according to their type of source: identity or application. When you create a data source, you also configure the settings for data collection.

Identity Governance must collect information about users from identity sources. After Identity Governance collects this information, you must publish the information to populate the catalog. You can then assign these users administrative authorizations in the product. For more information, see [“Adding Identity Governance Users” on page 184](#).

- ♦ [“Understanding Collector Configuration” on page 195](#)
- ♦ [“Transforming Data During Collection” on page 201](#)
- ♦ [“Creating Identity and Application Sources” on page 201](#)
- ♦ [“Managing Identity and Application Sources” on page 205](#)

For more information about data sources, see [“Understanding Data Sources” on page 18](#).

Understanding Collector Configuration

When you create an identity or application source, you will also create the **collectors** that you want to use for gathering specific identity, account, or permission data from that source. A collector is based on a collector template that is populated, when possible, with common data mappings for the selected data source type. Each collector has one or more views that allow you to specify which data you will collect from your identity or application source, and describe how that data will be linked together in the Identity Governance catalog.

When you configure the collector, you designate the incoming attributes that you want to map to the attributes in the Identity Governance catalog. Then you can map the permissions to the accounts. You can map a static value to any attribute in a collector configuration. This has the effect of assigning the same specified value for the selected attribute to all collected objects. The **multivalue** field allows you to collect multiple values for an attribute. If you collect multiple values for the attribute, you can statically map only a single value.

- ♦ [“Understanding the Common Elements in a Collector” on page 196](#)
- ♦ [“Understanding Collector Templates for Identity Sources” on page 197](#)
- ♦ [“Understanding Collector Templates for Application Sources” on page 197](#)
- ♦ [“Understanding the Variations for Data Sources” on page 199](#)

Understanding the Common Elements in a Collector

Every collector has the following configurable elements:

Collector template

Collector templates include predefined attribute mappings and value transformation policies for specific data source types. Select a template that best suits the data source. For example, select **AD Identity** to collect identities from Active Directory. The templates support the following types of data sources:

- ♦ Active Directory
- ♦ Azure Active Directory
- ♦ CSV file
- ♦ eDirectory
- ♦ Google Apps
- ♦ Identity Manager
- ♦ JDBC, such as Oracle or PostgreSQL
- ♦ Resource Access Control Facility (RACF)
- ♦ Salesforce.com
- ♦ SAP User Management
- ♦ ServiceNow
- ♦ SharePoint 2013 Server

NOTE: Template name ending in **with changes** can be enabled for incremental change events processing.

The CSV collector support TSV file. You enter the word `tab`, in uppercase, lowercase, or any combination in the **Column Delimiter** field.

To see all the data source types, select **Collector Template** when you create the data source. To collect data from a JDBC or SAP User Management source, Identity Governance needs the appropriate third-party connector libraries to be installed on the Identity Governance server. For more information, see [“Identity Governance Server System Requirements” on page 41](#).

You can also customize an existing template or create your own. For more information, see [“Customizing the Collector Templates for Data Sources” on page 164](#).

Service Parameters

These are the configurable parameters that allow the collector to connect and, if required, authenticate to the target data source. These typically include file locations, server host and port specifications, or service URLs. This section includes a **Test connection** button to verify the settings.

Select **Test connection** to verify the settings.

Test Collection and Troubleshooting

This option allows you to preview data before running a full collection, preserve the configuration for a data source, or create an emulation package for a data source. You can use generated files to validate and troubleshoot collections, send results to support engineers, and to import data source configurations to a different environment.

Understanding Collector Templates for Identity Sources

Identity sources provide core identity information to Identity Governance. When using multiple identity sources you can:

- ♦ Specify the order of priority between different sources
- ♦ Specify how identities from different sources will be matched and merged
- ♦ Designate which source will be used for different identity attributes

Identity collectors populate the Identity Governance system with users. When using an LDAP-based One SSO Provider (OSP) system, such as eDirectory or Active Directory, ensure that the proper data source is providing the LDAP Distinguished Name attribute to the identities. This is the attribute that Identity Governance uses for single sign-on authentication.

Collector templates for an identity source can have the following elements:

Collect Identity

To ensure that you can create a unique identity from the data that you collect, you tell Identity Governance how to map the data collected from an application to the data that you collect from identity sources. Collect as much information as you need to fulfill your business needs. Also ensure that you collect enough information to allow application account and permission to be joined to your identities. Some common join attributes that are available from most application sources include `email address`, `workforceId`, and `name` attributes.

Collect Group

An identity in the catalog can have attributes for one or more organizational group. For example, you might group employee identities by their department, such as Finance or Human Resources. You can use the collected group attribute to set the scope of a review, such as reviewing employees only in the Finance group. For example, Active Directory, eDirectory, and Identity Manager support this type of collection.

Identity Governance always uses the `userID` attribute for an identity to join to the membership of collected groups. If a data source does not support group collection, Identity Governance does not allow you to configure this option.

Collect Group to User Membership

This view is used to collect the relationship that joins users to groups from identity sources that maintain these relationships separate from the basic group information. For example, the JDBC Identity collector runs a SQL query that parses the table that contains the links between groups and users.

Collect Parent Group to Child Group Relationships

This view is used to collect the relationship that joins groups to subordinate groups from identity sources that maintain these relationships separate from the basic group information. For example, the eDirectory Identity collector uses this view to obtain nested group members of groups.

Understanding Collector Templates for Application Sources

An application source might contain account and permission collectors. Account collectors gather information about the application users, such as their name, account ID, login name, and login time. Permission collectors gather information about the application access rights of the account users. Since there is no universal method for linking accounts and permissions to identities, these collectors

also provide the attributes and optional views necessary to join application accounts to Identity Governance identities and to join application permissions to either Identity Governance identities or to the application accounts as needed.

Depending on the type of data that you want to collect, the collector template might provide the following elements:

Collect Account

Accounts represent entities, such as a system, application, or data source, that an identity might access. For example, your employees might have an account that lets them log in to your company email system. An account in Identity Governance is similar to an association in Identity Manager.

Collect Permission

Permissions can describe any of the following:

- ♦ Actions that you can take within an application, such as running reports
- ♦ Items that you possess, such as an identity badge
- ♦ Things that you can access, such as a building

A permission in Identity Governance is similar to an entitlement in Identity Manager.

NOTE: If you use **Permission-Account** or **User Mapping** to join permissions to accounts or users, you must disable the optional **Permission and Holders Mapping** collections. Failure to do so could result in duplicate permission assignments in the catalog.

Permission and Holders Mapping

(Optional) These views exist to allow you to specify how a permission will be joined to either an Identity Governance identity or to an application account. In most application sources, such as Active Directory, the permissions (groups) are joined to Active Directory users (accounts). In this situation, you will use an Active Directory account and an Active Directory permission collector and join the permissions to the account using the distinguishedName attribute of the account. However, if your identities also came from the same Active Directory source, the account collector is not needed and the group permissions could be joined directly to the identities using the distinguishedName. The collector configuration page presents all available permission join attribute options. Due to differences in the holder/permission relationship management in different application sources, Identity Governance provides two optional views:

- ♦ **Permission to Holder Mapping** where the relationship is best expressed by starting with the permission object and following the relationships to the holders of that permission. For example, the "member" attribute on an eDirectory permission group.

When Mapping permissions to holders in any application where it exists, you must use **Account ID from Source** not **User ID from Source** if you want the permission to be linked to the user (which is the usual expectation).

- ♦ **Holder to Permissions Mapping** where the relationship is best expressed by starting with the user account and following the relationships to the permissions held by that user account. For example, the "groupMembership" attribute on an eDirectory user.

In some applications, the relationship can exist bidirectionally between the holder and permission. In this situation, use only one of the above views.

Collect Provisioning Applications

Applies only to Identity Manager data sources

Collect Connected Accounts

Applies only to Identity Manager data sources

Collect Permissions hierarchy

(Optional) When an application source organizes permissions in parent-child relationships, you can collect the relationship between the permissions. When gathering nested permissions, specify one of the following methods:

- ♦ **Child to parent** where the collected permissions include an attribute that points to child permissions
- ♦ **Parent to child** where the collected permissions include an attribute that points to a parent permission, such as eDirectory user

Understanding the Variations for Data Sources

In Identity Governance, you associate user identities gathered from identity sources to the accounts and permissions assigned in the application sources. Many user identities are categorized by groups and have parent-child relationships with other identities or accounts. However, some application sources might define groups or parent-child relationships in a different way than Identity Governance. Also, some identity sources might be configured to generate incremental change events.

This section explains how to use the collector templates for the following application sources:

- ♦ [“Collecting from Active Directory with Azure Active Directory” on page 199](#)
- ♦ [“Collecting from a CSV File” on page 199](#)
- ♦ [“Collecting from Google Apps” on page 200](#)
- ♦ [“Collecting from Identity Sources with Change Events” on page 200](#)

Collecting from Active Directory with Azure Active Directory

When your environment uses both Active Directory and Azure AD, some user identities might be unique to one of the applications while other identities might exist in both applications. If you use Active Directory and Azure AD with DirSync or AD Connect, you can create a single identity source for both applications by using the **Azure AD User** collector template.

In the collector template, specify an attribute that you want to use for merging duplicate identities and matching identities to accounts and permissions. The attribute for the matching rule should contain a value that is unique to each identity. For example, in AD and Identity Manager, each user tends to have a unique `Distinguished Name`.

Collecting from a CSV File

A CSV file provides a simple method for storing user account or permissions information that cannot be collected from other data sources. You can include group, account, permission, or user data in the file.

If you use a CSV file as an identity source, you might want to instruct Identity Governance to map the collected users to their collected group memberships. The **Group Members (Users and Groups)** setting allows you to specify an attribute in the CSV file that you want to use for mapping users and groups to groups. However, you can use this setting only when a given value for the specified attribute is not used to identify both a user and a group. For example, if you export data from Active Directory to the CSV file, you can use DN as the Group Members attribute. Otherwise, you can use **Collect Group to User Membership** or **Collect Parent Group to Child Group Relationships** to map users or groups to groups. These two settings match the specified attribute in the collected user or group data, respectively.

In preparing a CSV file, ensure that any values written into a column of the file do not contain any carriage returns and line feeds, since these characters define record boundaries in the CSV file.

NOTE: The CSV collector support TSV file. You enter the word `tab`, in uppercase, lowercase, or any combination in the **Column Delimiter** field.

Collecting from Google Apps

Google Apps manage users, groups, and organizational units, including assigned roles and privileges. Collecting identities from Google Apps is similar to other data sources. However, to collect permissions, Identity Governance pulls information from Google Groups, which resembles discussion-based groups similar to those available in Usenet.

To gather information about actual user groups, Identity Governance collects from the Organizations (organizational units) in Google Apps. These organizational units can contain nested units. The top level organization is always called 'root.' During collection, Identity Governance translates the organizational units into Identity Governance-style groups. In Identity Governance, the root group lists all the users in that organizational unit. If you select one of the nested groups under the root group, Identity Governance lists only the individuals assigned to that group.

Collecting from Identity Sources with Change Events

Identity sources with change events provide incremental change events for user and group data from certain identity sources to incrementally update the identity catalog. To periodically pull change events and incrementally make changes to your identity catalog the following conditions must be met:

- An identity source is configured as an identity event source, either by having created an identity source from a suitable template, or by having migrated a non-event-aware identity source by using the Identity Governance Migration Utility and selecting enabling event collection. For more information, see [“Creating Identity and Application Sources” on page 201](#) and [“Migrating an Identity Collector to a Change Event Identity Collector” on page 207](#).
- The identity source is the primary identity source, for example it is either the sole identity source or an unmerged identity source
- The identity event source has been collected and published
- The configuration of the identity source and its collector has not changed since the last publication
- Identity event source collection, identity publication, or application publication is not in progress.
- (Conditional) For eDirectory, the Change-Log module must be installed to support event processing. For more information, see the [NetIQ Driver for Bidirectional eDirectory Implementation Guide](#).
- (Conditional) For Identity Manager, the Identity Gateway Integration Module must be installed to support event processing. For more information, see [NetIQ Identity Manager Driver Administration Guide](#).

Once event collection is enabled, Identity Governance uses the global configuration parameters: `com.netiq.iac.rtc.event.polling.interval` and `com.netiq.iac.rtc.max.polling.timeout` settings to determine the identity context change event polling frequency and time limit for batch event collection. Typically, events are collected in batches of up to one hundred events. However, if the identity source's **Batch Size Limit** as configured in the **Service Parameters** is less than one hundred, then that batch size is the upper limit for event collection also.

IMPORTANT: The identity source with change event collectors are not intended to handle large-scale changes to the source directory, such as changes to the user population resulting from mergers or spin-offs, major changes to group memberships, or major reorganizations of any kind. In such cases, you should disable event processing and enable it after the major change.

During event collection, a user record move in the underlying LDAP tree from outside of to inside of the scope of the configured Search Base is treated as an ADD event, and a user record move to the outside of the Search Base scope is treated as a DELETE event. The number of events of each type that were processed in the most recent event processing period is reported on the [Data Sources > Activity](#) page, as part of the detail of the most recent collection for that collector.

NOTE: For a more efficient event processing, change events are not generated for any dynamic changes in eDirectory or IDM dynamic groups. Also, removing a member from an eDirectory or IDM group will not remove that member from any of the group's super groups if those groups have been configured to report nested members in membership query.

Transforming Data During Collection

Because each application may have its own format for the data that you plan to collect, you might need to transform the data during the Identity Governance collection process. For example, the application might store dates as a string (20151202) which needs to be converted to the Identity Governance date format. Also, an application might use field lengths that do not match the field length in Identity Governance. These variations in collected data affect your ability to use the data or merge it with data collected from other sources.

The transforms are done through Nashorn-compatible Javascript. Within the Javascript, you can access the collected value by creating a variable name `inputValue`. After manipulating the collected value, you can return the value to Identity Governance by assigning the value to a variable name `outputValue`.

The following example translates the values `true` and `false` from the connected system to `active` and `inactive` in the Identity Governance catalog.

```
if (inputValue == 'true') {
    outputValue = 'active';
}
else {
    outputValue = 'inactive';
}
```

Creating Identity and Application Sources

Identity sources provide the information to build a catalog of the people within your organization. The information that you collect from your data sources can add as much personally identifiable information as you need to create the unique identity for each person. If you have upgraded from Identity Governance 2.5, use the Identity Source Migration utility to update your Active Directory data

collector, eDirectory data collector, and Identity Manager data collector to accept change events. For more information, see [“Migrating an Identity Collector to a Change Event Identity Collector” on page 207](#).

Application sources provide the information to build a catalog of the permissions and accounts within your organization. These data sources are configured with one or more collectors to collect the information from that source. Identity Governance provides collector templates to facilitate this configuration, or you can import a JSON file to add identity or application sources.

NOTE

- ♦ If you are using the Identity Manager Identity collector, it must always be first in the list of collectors, or user authorizations fail. For more information, see [“User Authorizations Fail if the Primary Identity Source is not Identity Manager”](#).
- ♦ When collecting identities using the publish and merge setting, matching attributes become mandatory attributes to have Identity Governance include the user when publishing. If a secondary identity source has users that do not have the matching attribute defined in the collector, they will be collected, but they will not be published.
- ♦ If you collect data from two or more identity sources that have duplicate information for the `Primary Supervisor ID from Source` attribute, Identity Governance cannot merge or publish the data. After collecting each identity source, you must define extended attributes, such as `Source1_userID` and `Source2_userID`, for the `Primary Supervisor ID from Source` attribute. Then, to merge the information, specify the extended attributes as the “Join to” attribute for `Primary Supervisor ID from Source`.
- ♦ To collect from a CSV file, specify the full path to the file.
- ♦ You must export data sources from the current version of Identity Governance to be able to correctly import them.
- ♦ You can use the Identity Governance Custom Collector SDK to create collectors. For more information, see the [Release Notes for Identity Governance 3.0.1](#).
- ♦ The CSV collector supports TSV files. To use a TSV file, enter the word `tab`, in uppercase, lowercase, or any combination in the **Column Delimiter** field.

To create a data source:

- 1 Log in to Identity Governance as a Data Administrator.
 - 2 Select **Data Sources**.
 - 3 (Conditional) To create an identity source collector, select **Identities**.
 - 4 (Conditional) To create an application source collector, select **Applications**.
 - 5 Select **+** to create a data source collector from a template.
- or
- Select **Import an Identity | Application Source** to specify a JSON file to import.

IMPORTANT: You must export a data source from the current version of Identity Governance to import an updated version. Data source files exported from earlier versions of Identity Governance do not import correctly to the current version. Hence, the data source must be recreated in the current version of Identity Governance.

- 6 (Conditional) To configure an identity source with change events collector, select a template name ending in **with changes** and observe the conditions listed in [“Collecting from Identity Sources with Change Events” on page 200](#). For more information, see [“Understanding Change Event Collection Status” on page 204](#) and [“Supported Attribute Syntaxes for eDir and IDM Change Events Collection” on page 204](#).

NOTE: Only one event collector is allowed and any change to the collector configuration suspends change event processing, which does not resume until a full batch collection and publication completes.

IMPORTANT: For large scale changes, disable event collection, and enable it only for incremental change events.

- 7 Enter all the mandatory fields for the data source.

For more information, see the following content in [Understanding Collector Configuration](#):

- ♦ [“Understanding the Common Elements in a Collector” on page 196](#)
- ♦ [“Understanding Collector Templates for Identity Sources” on page 197](#)
- ♦ [“Understanding Collector Templates for Application Sources” on page 197](#)
- ♦ [“Understanding the Variations for Data Sources” on page 199](#)

- 8 Save your settings.

- 9 (Optional) If you want to preview all or part of the data, select **Test Collection and Troubleshooting**. For more information, see [“Testing Collections” on page 206](#).

The first time you set up Identity Governance, you must collect and publish data after creating your data sources so that your catalog contains the data.

To populate the catalog:

- 1 Select **Collect Now** for each data source on the **Identities** and **Applications** pages.
You need to collect and publish the data for Identity Governance to add the data to the catalog.
- 2 (Optional) To merge the collected data from an identity source, specify the rules for publishing and merging.
For more information, see [“Setting the Merge Rules for Publication” on page 222](#).
- 3 Select **Publish Now** on the **Identities** page and next to each application data source on the **Applications** page.

NOTE: When you publish any identity source, Identity Governance publishes all identity sources. For more information, see [“Publishing Identity Sources” on page 221](#).

- 4 When you see that publication has completed, go to **Catalog** to view the collected information.

Understanding Change Event Collection Status

The event collection displays the following status:

Change Event Collection Status	Description
DISABLED	Event processing is not enabled for this collector and identity source. If event processing is enabled from this state, the state becomes BLOCKED, and the identity source must be collected and published before it can become READY.
BLOCKED	Event processing is enabled, but cannot proceed because the preconditions for processing change events were not met. For more information, see “Collecting from Identity Sources with Change Events” on page 200 .
READY	Event processing is enabled and not blocked, but awaiting scheduling to proceed.
IN_PROGRESS	Events are being polled for and processed. NOTE: Event processing will be in progress either until a polling request returns no events, or until the configured maximum event processing time is reached.

Supported Attribute Syntaxes for eDir and IDM Change Events Collection

Identity Governance supports the collection of the following attribute syntaxes during eDir and IDM change events collection:

- ♦ Boolean
- ♦ Case Exact String
- ♦ Case Ignore List
- ♦ Case Ignore String
- ♦ Class Name
- ♦ Counter
- ♦ Distinguished Name
- ♦ Integer
- ♦ Integer 64
- ♦ Interval
- ♦ Numeric String
- ♦ Object ACL
- ♦ Octet String
- ♦ Path
- ♦ Postal Address
- ♦ Printable String

- ♦ Telephone Number
- ♦ Time
- ♦ Typed Name
- ♦ Unknown

Managing Identity and Application Sources

Identity Governance offers several ways to help you manage your data sources.

IMPORTANT: If your Identity Governance database environment runs Oracle, you must turn on the SQL Tuning Advisor to optimize queries in the Oracle database.

- ♦ [“Exporting and Importing Collectors” on page 205](#)
- ♦ [“Comparing Collections and Publications” on page 206](#)
- ♦ [“Testing Collections” on page 206](#)
- ♦ [“Creating Emulation Packages” on page 207](#)
- ♦ [“Migrating an Identity Collector to a Change Event Identity Collector” on page 207](#)

Exporting and Importing Collectors

The ability to export and import collectors helps you manage your environment in several ways.

- ♦ Back up a working collector
- ♦ Replicate an environment
- ♦ Update collector details in a text editor
- ♦ Troubleshoot collections

Configuring collectors can take time and go through several iterations of trial and error. When you have configured a collector that achieves the results you want, you should export it and save it with your other backup files. You can also use exported collectors to replicate an environment, either in a test environment or to use in another office location.

You could decide that you need to change the predefined attribute mappings and value transformation policies of a template to meet your specific environment. If you find that you need to customize a collector template, rather than only editing the values in a collector, you can export and import collector templates under Administration in Identity Governance. For more information, see [“Customizing the Collector Templates for Data Sources” on page 164](#).

To export and import collectors:

- 1 Select a data source, and then select **Test Collection and Troubleshooting**.
- 2 Select **Download and Emulation**, and then select **Download Data Source Configuration**.
- 3 Select a location for the file, and then select **OK**.
- 4 If you make changes and want to import a collector, under **Data Sources**, select **Identities** or **Applications**, and then select **Import an identity source** or **Import an application source**.
- 5 Select the file to import.

Comparing Collections and Publications

When you need to show that you have complete and accurate data, you can compare collection and publication details from the same data source at two different collection or publication times. Identity Governance uses the defined data policies to produce the comparison details. For more information, see [Chapter 30, “Creating and Managing Data Policies,” on page 309](#).

To compare collections and publications from the same source:

- 1 Under **Data Sources**, select **Activity**.
- 2 (Optional) Select the calendar icon to focus the list on a specific time period.
- 3 (Optional) Enter a data source name in the search to focus the list on specific data sources.
- 4 (Optional) Change the number of rows per page to show a longer list.
- 5 (Optional) To quickly compare a collection or publication with the previous collection or publication, select the item from the **Date and status** column.
- 6 Select a listed collection or publication using the checkbox.
- 7 Select a collection or publication from the same source to compare to the first selection.

NOTE: You are able to select only one additional item from the same source and type.

- 8 Under **Action**, select **Compare**.
- 9 View changes and select links to view additional information about the changes. For example, if the number of changes is not zero, that number is a link. Selecting that link opens a quick view of the items that changed.
- 10 (Optional) To quickly view or open the applicable data policies, complete the following:
 - 10a Select **Refine comparison options**.
 - 10b Select or clear listed policies to change your comparison results.
 - 10c Select **Edit Policies** to open the **Data Administration > Data Policy** page. For more information see, [“Creating and Editing Data Policies” on page 309](#).

Testing Collections

When creating, updating, or troubleshooting data collectors, you can test all or part of the collections without publishing the results to the catalog. When you test a collection, you either ensure that the collector is correctly configured, or you have the ability to change the collector configuration and quickly test again to check the results.

You can view the collected data as soon as the test collection completes, or you can download the results to view later. Results of test collections remain available in Identity Governance until you delete them.

When you run a test collection, you have some options for the test data:

- ♦ All records
- ♦ Some records
- ♦ Raw data
- ♦ Transformed data

When you select a subset of records to collect, you cannot control which records to collect. You could use this option if you want to quickly spot check a collector configuration rather than waiting for all the data to be collected.

Raw data contains attribute names from the native application. These attributes have not yet been transformed based on the mappings in the collector. Testing the raw data collection lets you verify that you are collecting the data you intend to collect before Identity Governance transforms it.

Transformed data contains attribute names that you have mapped from the native application to the attribute names you are using within Identity Governance. Testing the transformed data collection lets you verify that your mappings within the data collector meet your expectations.

To test a sample collection from a data source:

- 1 Select a configured data source.
- 2 Select **Test Collection and Troubleshooting**.
- 3 Under **Test Collection**, select the collectors, and then select **Run Test Collection**.
- 4 Select the specific entities to collect and type the number of records to collect or leave **All** to collect all records.
- 5 Select the option for the type of collection to run.
- 6 After the test collection shows **Complete**, select **Action** to view, download, or delete test collection results.

Creating Emulation Packages

You can more easily troubleshoot collection configuration outside your production environment by creating emulation packages for data collectors. An emulation package contains CSV files with the raw collected data from the data source and a CSV file containing data source configuration details. Emulation packages remain available in Identity Governance until you delete them.

To create an emulation package:

- 1 Select a configured data source.
- 2 Select **Test Collection and Troubleshooting**.
- 3 Under **Download and Emulation**, select **Create emulation package**.
- 4 When the emulation status shows **Complete**, select **Action** to view, download, or delete the emulation package.

Migrating an Identity Collector to a Change Event Identity Collector

If you have upgraded from Identity Governance 2.5, use the Identity Source Migration utility to update your Active Directory, eDirectory, or Identity Manager data collector to accept change events. The identity collector you are migrating must publish using the **Publish without merging** or the **Do not publish** setting.

NOTE: eDirectory and IDM change event identity collectors are supported only in Identity Governance 3.0.1.

- 1 Upgrade to Identity Governance 3.0 and make sure Identity Governance is up and running.
- 2 Verify that the `idgov/bin/rtc-migration.sh` (Linux) `c:\netiq\idm\apps\idgov\bin\rtc-migration.bat` (Windows) file references the jar file `idgov/lib/ig-migration.jar` (Linux) `c:\netiq\idm\apps\idgov\lib\ig-migration.jar` (Windows).

- 3 Run the command-line utility from the server where Identity Governance is installed.
 - ♦ **Linux:** Default location of `/opt/netiq/idm/apps/idgov/bin/rtc-migration.sh`, then enter `./rtc-migration.sh`
 - ♦ **Windows:** Default location of `c:\netiq\idm\apps\idgov\bin\rtc-migration.bat`, then enter `rtc-migration.bat` from a command line.
- 4 Provide the information needed to connect and authenticate to Identity Governance and the authentication server. When the utility successfully connects, it displays a numbered list of discovered identity sources.
- 5 Enter the number displayed next to the identity source to migrate.
- 6 After the utility runs checks to determine migration suitability, either confirm to proceed with the migration, if the checks succeeded, or review messages for failed checks and either address the problem areas, select a different source, or quit the utility.
- 7 (Conditional) If you confirm to proceed with migration, enter a local file name for the utility to back up the current collector configuration.
- 8 After the utility applies updates and exits with a success message, you can view the following updates to the collector configuration when viewed in Identity Governance:
 - ♦ The template (just under the name of the collector) has been changed to the **with changes** template corresponding to the one prior to the update.
 - ♦ After the **Collector name** is a new **Enable Change Event Collection** option, which is unchecked. To enable event processing, select this option, and then collect and publish the identity source.
 - ♦ No changes are made to the **Service Parameters**.
 - ♦ Under **Collect Identity** (the user view):
 - ♦ The **Base Dn** parameter is no longer required, but the value has not been changed. Omitting a value here will cause the entire LDAP tree to be collected.
 - ♦ (Conditional) For Active Directory identity event source, a new parameter, **LDAP Search Filter for Identity Object Changes**, has been added, with the value `(objectClass=user)`. This parameter identifies events in Active Directory's DirSync or AD Connect that should be delivered in this view to Identity Governance. Only modify this parameter if there are other object classes in the local AD that correspond to users and only by adding other `objectClass` terms to an LDAP expression.
 - ♦ (Conditional) For Active Directory identity event source, a new parameter, **AD Object Categories for Changes**, has been added with the value `user`. You can modify this value if needed by adding other object category names in a comma-separated list.
 - ♦ **User ID from Source** has been set to `OBJ_ID`. Do not change.
 - ♦ The **Object GUID** parameter is now required. Its value is set to `objectGUID`. Do not change.
 - ♦ **LDAP Distinguished Name** has been set to `OBJ_ID`. You can remove this value if there's no need to collect `dn` separately from the `userId`, but you should not assign any other value.
 - ♦ Under **Collect Group** (the group view):
 - ♦ The **Base Dn** parameter is no longer required, but the value has not been changed. Omitting a value here will cause the entire LDAP tree to be collected.
 - ♦ A new parameter **LDAP Search Filter for Identity Object Changes** has been added, with the value `(objectClass=group)`. This parameter identifies events in Active Directory DirSync or AD Connect that should be delivered in this view to Identity

Governance. Only modify this value if there are other object classes in the local AD that correspond to groups and only by adding other `objectClass` terms to an LDAP expression.

- ♦ A new parameter **AD Object Categories for Changes** has been added with value `group`. You can modify if needed by adding other object category names in a comma-separated list.
- ♦ **Group ID from Source** has been set to `OBJ_ID`. Do not change.
- ♦ A new parameter **Object GUID** has been added with value `objectGUID`. Do not change.

16 Creating and Monitoring Scheduled Collections

You can collect data on individual sources at any time. To enhance the collection and publication process, you can schedule collections to run at regular intervals. Each collection can contain one or more identity and application sources. For example, you might want to update identities associated with your human resources application every week. Instead of manually collecting and publishing those identities, you create a scheduled collection.

To see the status of all recent and pending collections, go to **Data Sources > Activity**.

NOTE: After each run of a scheduled collection, Identity Governance automatically publishes the data.

- ♦ [“Creating a Scheduled Collection” on page 211](#)
- ♦ [“Monitoring Scheduled Collections” on page 212](#)
- ♦ [“Understanding the Cron Expression for a Custom Interval of Collection” on page 212](#)

Creating a Scheduled Collection

You can schedule collections to run on at regular intervals. For example, collect data from Workforce and SAP identity sources every week. You specify the start and end dates for the collection and how often it repeats. Alternatively, you can specify a custom string to run the scheduled collection on a specific set of dates.

- 1 Log in as a Global Administrator.
- 2 Under **Data Sources**, select **Schedules**.
- 3 (Conditional) When adding a new scheduled collection, complete the following steps:
 - 3a Select **+** to create a new schedule.
 - 3b Specify a name and description.
 - 3c Specify the identity and application sources for collection.
- 4 (Conditional) To modify an existing scheduled collection, select its name.
- 5 (Optional) To customize the interval for running the collection, complete the following steps:
 - 5a For **Repeat**, select an interval or specify **custom**.

IMPORTANT: If using the hourly interval, do not schedule collections with fewer than 24 hours between collections to avoid errors when a new collection starts before a previous one completes.

- 5b Specify values for the starting and ending dates and the time zone.
- 5c For **Custom**, use the following syntax to indicate the collection time:

second minute hour day_of_month month year

For example, `0 20 10 ? * *`. For more information about specifying the parameter values, see [“Understanding the Cron Expression for a Custom Interval of Collection” on page 212](#).

- 6 (Conditional) To see a list of the first 10 scheduled runs, select **Preview**.
- 7 To ensure that the schedule runs, select **Active**.
- 8 Save the schedule.

Monitoring Scheduled Collections

The **Data Sources > Schedules** page provides an overview of each scheduled collection. You can find the times for the most recent and next activity of the collection. If a scheduled collection is inactive, Identity Governance displays the collection in a gray field.

To observe the details of a scheduled collection, select its name. Identity Governance lists the settings for the collection. You can modify the settings. For example, add and remove sources. Alternatively, you might want to deactivate the scheduled collection. If you modify the settings, ensure that you save the change.

To review the details for a recent run of the specified collection, select the run. Identity Governance indicates the success and time of collection and publication for each data source. If you select a data source, Identity Governance takes you to the details page for that source or an overview if a group of sources. For example, if your schedule collects data from all identity sources, Identity Governance displays the **Identity Sources** overview page.

Understanding the Cron Expression for a Custom Interval of Collection

Identity Governance uses a cron expression to create the custom schedule. The cron expression is a string of parameters in the following syntax:

second minute hour day_of_month month year

For example:

`0 20 10 ? * *`

Use the following values to specify the parameters in the expression:

n

Specifies a numeric value for the parameter. For example `12` for `day_of_month` or `2015` for `year`.

Specifies that the parameter uses all available values. For example, to run at 10:20 AM every day in July 2015, specify `0 20 10 * 7 2015`.

-

Specifies a range of values. For example, to run the collection during consecutive months, specify `0 20 10 ? MAR-OCT *`.

/

Specifies that you want to run the collection at a particular interval. Use the following syntax: `first_instance/increment`. For example, to run the collection on the first day of the month and every third day after, specify `0 20 10 1/3 * *`.

?

Applies only to `day_of_month`

Specifies that `day_of_month` does not have a specific value. For example, to run the schedule at 10:20 AM on any day of May, specify `0 20 10 ? MAY *`.

L

Applies only to `day_of_month`

Specifies that you want to run the collection on the last day of the month. For example, `0 20 10 L * *`.

To specify multiple values for a parameter, use commas. For example, to run the collection every six hours at specific days during specific months, specify `0 0 0/6 5,7,21,24 MAR-JUN,OCT *`. The schedule runs on the 5th, 7th, 21st, and 24th days of March, April, May, June, and October. This example also combines values to specify the month: `MAR-JUN,OCT`.

17 Integrating Collected Data with Identity Manager

This section provides guidance for using the **NetIQ Identity Manager Driver for NetIQ Identity Governance** (Access Review driver). For more information about installing and configuring the driver, see the [NetIQ Identity Manager Driver for Access Review Installation and Configuration Guide](#).

Identity Governance can collect data from identity and application sources that are not connected to Identity Manager. With the Access Review driver, these user identities and application data can become resources in the Identity Vault for Identity Manager users. This gives you the ability to review and certify permission assignments using Identity Governance, as well as to request and provision these permissions using Identity Manager. The driver also can provision users in the Identity Vault for Identity Manager as needed for the customer's use-case.

- ♦ [“Understanding Synchronization and Reflection” on page 215](#)
- ♦ [“Ensuring Best Performance for Identity Matching” on page 217](#)
- ♦ [“Reflecting Permissions and Assignments from Applications Not Connected to Identity Manager” on page 217](#)
- ♦ [“Synchronizing Changes in Identity Governance Data with Objects in the Identity Vault” on page 218](#)
- ♦ [“Migrating User Objects to the Identity Vault” on page 219](#)

Understanding Synchronization and Reflection

The Access Review driver helps synchronize changes to identities and applications in Identity Governance with matching user and resource objects in Identity Manager. The driver provides Global Configuration Values (GCVs) that allow you to delete or disable user objects or delete resource objects in the Identity Vault. Alternatively, you can remove the association between the user object and the identity in Identity Governance.

- ♦ [“Reflecting Application Permissions in Identity Manager” on page 215](#)
- ♦ [“Synchronizing Data Changes between Identity Governance and Identity Manager” on page 216](#)

Reflecting Application Permissions in Identity Manager

For each application source in Identity Governance, you can **reflect** the collected permissions and assignments as resources in Identity Manager, with the exception of Identity Manager applications or child applications. With this setting enabled for an application, the Access Review driver can create resources in Identity Manager that match the permissions and permission assignments in Identity Governance. Identity Manager users can then request access to these resources even when the application is not a connected system in Identity Manager.

If an application source is also a connected system in Identity Manager and the driver uses entitlements, then you do not need reflection for that application source. However, if the driver does not use entitlements, the you might want to enable reflection for the application source.

When you reflect an application's permissions, the Access Review driver creates a new container in the Identity Vault for the permissions and creates a new Resource Category for grouping the permission resources. The driver specifies the same name for the Resource Category that Identity Governance has for the application. For example, if an application source in Identity Governance is named "SAP Permissions," then the driver creates a Resource Category named "SAP Permissions" in Identity Manager.

If you stop reflecting an application's permissions, the application is no longer linked to the resource containers in the Identity Vault. Identity Manager uses Global Configuration Values (GCVs) to determine the course of action after you disable reflection. By default, a GCV instructs Identity Manager to delete the resource containers and the resource category in the Identity Vault. However, you can modify the GCV to keep the containers and category, which allows you to reestablish reflection. For more information about de-linking the application from the Identity Vault, see ["Synchronizing Data Changes between Identity Governance and Identity Manager" on page 216](#).

When integrating application data with Identity Manager, the Access Review driver serves as the proxy for the application sources. The driver needs both a system account and a workflow in the User Application to create resources. For more information about configuring reflection, see ["Reflecting Permissions and Assignments from Applications Not Connected to Identity Manager" on page 217](#).

Synchronizing Data Changes between Identity Governance and Identity Manager

When you stop reflecting an application's permissions or you delete an application from Identity Governance, you can synchronize those changes with Identity Manager. For example, you replace ABC Money, a financial application, with its competitor DEF Accounting. You stop collecting data from ABC Money, and then delete the application from Identity Governance. When you publish the latest snapshot of collected data to Identity Manager, the Access Review driver uses the Publisher Resource Object Unlink GCV to communicate that the ABC Money application no longer exists in Identity Governance. Identity Manager responds according to the GCV's setting.

After you have turned off reflection for an application, it is necessary to collect and publish both the application and the Identity Manager application in order to update Identity Governance with the changes made to Identity Manager when you turned off reflection. It is also necessary to review, and possibly modify, fulfillment settings for the application.

You can also synchronize changes to user identities. For example, in the latest collection of identities from the SAP application, Identity Governance notes that the identity for Joe Smith has been deleted. This generates an event in Identity Governance to delete the Joe Smith identity. The driver uses the setting for the Publisher User Object Deletion GCV to determine how to process deletions.

The Access Review driver creates user objects only for the identities that you add to Identity Governance after you enable synchronization. If you have identities in Identity Governance already, you can migrate those identities to the Identity Vault.

For more information, see the following sections:

- ♦ ["Migrating User Objects to the Identity Vault" on page 219](#)
- ♦ ["Synchronizing New User Objects" on page 218](#)

Ensuring Best Performance for Identity Matching

Review the following recommendations to ensure the best performance among the Access Review driver, Identity Governance, and Identity Manager components:

- ♦ Before enabling reflection for an application, perform the following actions:
 - ♦ Configure the driver to allow User Add operations on the Publisher channel (synchronization)
 - ♦ Migrate identities that do not exist in Identity Manager from Identity Governance to the Identity Vault
- For more information, see [“Migrating User Objects to the Identity Vault” on page 219](#).

If you enable reflection first, the process might generate a large number of synchronization events and assignment operations.

- ♦ Tune the Identity Vault to index the attributes that the Access Review driver uses for matching a large number identities. For example, you should index the attributes in an identity management solution with more than 100,000 users. The driver runs policies to match attributes in the following order:
 1. workforceID
 2. Internet Email Address
 3. Given Name + Surname
 - ♦ Review the migration queries to reduce the amount of data that the driver transfers through the Remote Loader and the Identity Manager engine.
 - ♦ Order your identity sources in Identity Governance such that the source collecting from Identity Manager is the first source to collect data. If you are using the Identity Manager Identities Collector, it must always be first in the list of collectors or user authorizations fail.
- For more information, see [Chapter 16, “Creating and Monitoring Scheduled Collections,” on page 211](#) and [“Setting the Merge Rules for Publication” on page 222](#).

Reflecting Permissions and Assignments from Applications Not Connected to Identity Manager

Identity Governance can collect account and permission data from application sources that do not have role and resource objects in Identity Manager. The Access Review driver serves as the proxy for the application sources. For more information, see [“Reflecting Application Permissions in Identity Manager” on page 215](#).

NOTE: The driver needs both a system account and a workflow in the User Application to create resources. For more information, see the [NetIQ Identity Manager Driver for Access Review Installation and Configuration Guide](#).

- 1 Log in to Identity Governance as a Global Administrator.
- 2 Add the Identity Manager information to Identity Governance.
 - 2a Select **Administration**, then expand the **Identity Manager system connection information** section.
 - 2b Provide the Identity Manager URL. For example: `http://myserver:8180/IDMProv`.

- 2c Add the administrator user name and password for your Identity Manager system. For example, `admin` or `cn=uadmin,ou=sa,o=data`.
- 2d Select **Test Connection**. Ensure that you have a valid connection before proceeding.
- 3 Under **Catalog**, select **Applications**.
- 4 Select an application that you want to integrate with Identity Manager.
- 5 Select the icon for **Edit application**.
- 6 Under **Identity Manager Synchronization**, select **Reflect permissions and assignments as resources in Identity Manager**.
- 7 Specify the provisioning workflow that you want Identity Manager to use.
- 8 For **Identity Manager Resource Owner**, specify the user account in Identity Manager that can grant permissions for the application. For example, the application owner.

In Identity Governance, the name for this user is the concatenation of the account `GivenName` and `Surname` attributes. For more information about this account, see the [NetIQ Identity Manager Driver for Access Review Installation and Configuration Guide](#).
- 9 For each application, repeat [Step 4](#) through [Step 8](#).

Synchronizing Changes in Identity Governance Data with Objects in the Identity Vault

You can synchronize new and modified identities and application permissions in Identity Governance with user and resource objects in Identity Manager. The Access Review driver includes policies that tell Identity Manager how to respond to changes that occur to application and identity data in Identity Governance. You configure these policies in the Global Configuration Values.

- ♦ [“Synchronizing New User Objects” on page 218](#)
- ♦ [“Synchronizing Resource Objects” on page 219](#)

Synchronizing New User Objects

The Access Review driver synchronizes only the identities that are created in Identity Governance after you enable synchronization with Identity Manager. If you already have identities in Identity Governance when you enable synchronization, you need to migrate the existing user objects. For more information, see [“Migrating User Objects to the Identity Vault” on page 219](#).

The following GCVs allow you to configure how the Access Review driver and Identity Manager synchronize user objects.

Publisher User Object Placement

Specifies the container in the Identity Vault that stores the users created by the driver. When attempting to match Identity Governance identities with Identity Manager identities, the Identity Governance driver looks first in this sub-tree to determine whether an identity from Identity Governance already exists in Identity Manager. The driver recognizes a matched identity by its `Distinguished Name` value in Identity Manager. When the driver creates new users in the Identity Vault, this policy writes the GUID of the Identity Governance user object to a value of the `DirXML-Accounts` attribute on the user object.

The default value is `\data\users\arusers`. Specify a different folder than the one that contains identities imported from connected systems. When you use separate folders for identities from systems connected to Identity Manager and identities from Identity Governance, you can efficiently remove users collected from Identity Governance.

Publisher User Object Deletion

Provides options for Identity Manager when responding to an identity deleted from Identity Governance. When the Access Review driver communicates the delete event through the driver, you can configure Identity Manager to perform one of the following actions:

- ♦ **Remove Association:** Removes the `DirXML` association for the identity between Identity Manager and Identity Governance. The user object remains in the Identity Vault.
- ♦ **Disable Users, Remove Association:** (Default setting) Breaks the relationship for the identity between Identity Manager and Identity Governance. Identity Manager disables the user object. This is the only time the driver can set or reset the Login Disabled flag for a user object in Identity Manager.
- ♦ **Delete Users:** Deletes the user object from the Identity Vault.

For more information about configuring GCVs in a driver, see “[When and How to Use Global Configuration Values](#)” in the *NetIQ Identity Manager Driver Administration Guide*.

Synchronizing Resource Objects

The **Publisher Resource Object Unlink** GCV specifies how Identity Manager responds when you remove an application source from Identity Governance. This policy has the following options:

- ♦ **Delete Unlinked Resources:** Deletes the application and its associated permissions and permission resources from Identity Manager.
- ♦ **Keep Unlinked Resources:** (Default setting) Flags the application resources in Identity Manager to indicate that your organization is no longer interested in the application.

This policy also applies when you deselect **Reflect permissions and assignments as resources in Identity Manager** for the application in Identity Governance. For more information about reflecting permissions, see the following sections:

- ♦ “[Reflecting Application Permissions in Identity Manager](#)” on page 215
- ♦ “[Reflecting Permissions and Assignments from Applications Not Connected to Identity Manager](#)” on page 217

Migrating User Objects to the Identity Vault

The Access Review driver has an optional Publisher channel functionality that enables the driver to capture identities added to Identity Governance then synchronize them with the Identity Vault. To ensure that synchronization does not create duplicate identities, the driver adds only the identities that do not have a value for the `Distinguished Name` attribute. It is recommended that you configure synchronization in the driver for matching identities between Identity Governance and Identity Manager.

However, you might have previously configured the driver to prevent identity synchronization and now need to change that decision. For example, you enabled synchronization after you collected a set of identities. Since the Publisher channel is event driven, the driver publishes only the identities added to Identity Governance after you start synchronization. The only way to publish pre-existing identities to the Identity Vault is to **migrate** them using the Subscriber channel.

NOTE

- ♦ You cannot migrate identities if you have not configured synchronization. For more information about synchronizing identities, see [“Synchronizing New User Objects” on page 218](#).
 - ♦ Before starting user migration to the Identity Vault, enable **Adds and Migrate Allowed** in the driver configuration then restart the driver.
-

For more information, see the following sections:

- ♦ [“Targeting Identities that Do Not Exist in Identity Manager” on page 220](#)
- ♦ [“Adding Application Permissions after Migrating Identities” on page 220](#)

Targeting Identities that Do Not Exist in Identity Manager

To support migration, the Access Review driver provides a full set of migration queries. The migration queries allow for wildcards for any of the supported schema attributes. In general, you should migrate only the identities that do not exist in the Identity Vault. For example, you might already have used the Identity Manager Identity Collector to collect identities from the Identity Vault. You would not want to migrate these identities since they already have user objects in the Identity Vault. The Access Review driver recognizes these synchronized identities by the value of their `Distinguished Name` attribute. To avoid duplicating identities, you can add the `DirXML-Accounts` attribute to the migration query. The `DirXML-Accounts` attribute has the following values:

- ♦ **false**: When you set the value to `false`, the query targets only the identities in Identity Governance that do not have the `Distinguished Name` attribute value. Use this setting to identify the user objects that you want to create in the Identity Vault.
- ♦ **true**: When you set the value to `true`, the query targets only the identities in Identity Governance with the `Distinguished Name` attribute value. Use this setting to find identities that have already been collected from Identity Manager.

To target all of the Identity Governance identities, regardless whether they already exist in the Identity Vault, do not use the `DirXML-Accounts` attribute in the migration query.

Adding Application Permissions after Migrating Identities

When you migrate identities to Identity Manager, the Access Review driver does not include any permission assignments associated with those identities. To add the permission assignments, you must enable reflection for the target application. Then the driver uses the Publisher channel to synchronize the permission and assignments. Each time you modify the application or change the published data for the application, the driver reflects the changes to Identity Manager. For more information, see the following sections:

- ♦ [“Ensuring Best Performance for Identity Matching” on page 217](#)
- ♦ [“Reflecting Application Permissions in Identity Manager” on page 215](#)

18 Publishing the Collected Data

Publication makes the most recently collected data, and the relations among that data, available in the Identity Governance catalog. When you publish identity data, you can configure Identity Governance to merge the attributes of a unified identity. Application publication uses the most recent identity publication to resolve permission and account holder relationships. Identity Governance always publishes the current snapshot of the collection. For example, if a collection is in process, Identity Governance publishes the previously collected data.

- ♦ [“Publishing Identity Sources” on page 221](#)
- ♦ [“Publishing Application Sources” on page 223](#)

Publishing Identity Sources

Identity Governance publishes all identity sources concurrently to ensure that each unified identity receives the latest merged information. Identity sources always get published before application sources.

- ♦ [“Understanding Publication Behavior” on page 221](#)
- ♦ [“Setting the Merge Rules for Publication” on page 222](#)
- ♦ [“Publishing the Identity Sources” on page 222](#)

Understanding Publication Behavior

The catalog contains data collected from multiple data sources. To create a unified identity for each person, you need to merge, or unify, the different sets of collected information. Merging occurs during the publication process. For each identity source, you can specify one of the following publication options:

Publish and merge

Use this option when you collect data for the same identity from different data sources. For example, both Active Directory and Salesforce.com have the same `first_name` and `last_name` attributes for Jane Smith. This option allows you to combine the duplicate attributes from the sources into one identity for Jane in the Identity Governance catalog.

You must specify the rules for merging. Only one of your data sources can be an authoritative source for each identity attribute. To help you specify the **attribute authority**, Identity Governance numbers the data sources within each collection. The first source listed becomes the default authoritative source for all attributes in the collection. However, you can reorder the priority of the data sources or override the default setting for specific attributes. For more information, see [“Setting the Merge Rules for Publication” on page 222](#).

Publish without merging

Use this option if you have only one identity source or your data sources do not contain the same identities. Since Identity Governance does not perform any merging activities during publication, you might observe faster performance. However, if your sources do contain the same identity, Identity Governance will treat those identities as separate people.

Do not publish

Use this option when you are configuring the identity source. For example, you might not want to publish any collected data when you are testing the process.

Setting the Merge Rules for Publication

You might want to customize the rules for unifying the information collected from multiple identity sources for the same identity. Merging rules allow you to control which values will be stored when multiple identity sources provide information for the same fields. For example, if two sources provide an email address, data from the selected source will be saved as the primary value. If you don't select priorities using merging rules, Identity Governance uses the first collected value.

IMPORTANT: When collecting identities using the publish and merge setting, matching attributes become mandatory attributes to have Identity Governance include the user when publishing. If a secondary identity source has users that do not have the matching attribute defined in the collector, they will be collected, but they will not be published.

- 1 Log in to Identity Governance as a Data Administrator.
- 2 Select **Data Sources > Identities**.
- 3 (Optional) Arrange the order of the identity sources to set their priority for merging the published attributes.
- 4 (Optional) To use a specific identity source as the attribute authority, complete the following steps:
 - 4a Under **Publish and merge**, expand **Set merging rules**.
 - 4b For the attribute that you want to modify, specify the identity source.

The **None (go by order)** option instructs Identity Governance to use the first identity source as the attribute authority.
- 5 Select the **Save** icon.
- 6 (Optional) Publish your pending changes.
- 7 (Optional) Verify the changes that you published to the catalog.

Publishing the Identity Sources

If you have a scheduled collection, the scheduled run publishes the collected identities at the end of the run. You can also manually publish the identity sources.

Identity Governance uses a red diamond icon to indicate that an identity source has been collected but not published. Identity Governance shows any collection errors or warnings on the **Identities** and **Applications** data source pages.

- 1 Log in to Identity Governance as a Data Administrator.
- 2 Select **Data Sources > Identities**.
- 3 Select the **Publish identities now** icon.

Publishing Application Sources

You can publish an application source independently from other application sources. However, before publishing an application source, you must publish your identity sources.

- 1 Log in to Identity Governance as a Data Administrator.
- 2 Publish your identity sources.
For more information, see [“Publishing the Identity Sources” on page 222](#).
- 3 Select **Data Sources > Applications**.
- 4 For each application source that you want to publish, select **Publish**.

19 Managing Data in the Catalog

Identity Governance helps you create a unified identity for each user that combines all permissions that have been assigned by your identity and application sources. To build the unified identity, Identity Governance must know how to map incoming identity attributes. The catalog needs at least one identity source, such as Active Directory, and at least one application source. Otherwise, you cannot map identity attributes to permissions. When using a CSV file as a data source, the file must use UTF-8 encoding.

- ♦ [“Configuring the Data Source for Post Authentication Matching” on page 225](#)
- ♦ [“Understanding Identity, Application, and Permission Management” on page 226](#)
- ♦ [“Editing Attribute Values on Objects in the Catalog” on page 228](#)
- ♦ [“Searching for Users or Groups” on page 230](#)
- ♦ [“Managing Technical Roles” on page 231](#)

Configuring the Data Source for Post Authentication Matching

A user is a valid Identity Governance user when the user is authenticated by a One SSO provider (OSP) and has been mapped to a published Identity Governance catalog user. The post authentication mapping occurs based on the User Mapping configuration.

IMPORTANT: Identity Governance evaluates only collected attribute values for the authentication matching rules, not edited values. For more information, see [“Auth Matching Rules” on page 131](#).

You can also add your own custom attributes to the catalog. For example, if your data source is eDirectory, you must extend the schema for the catalog because eDirectory contains more attributes than are built into the catalog.

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

- 1 Log in to Identity Governance as a Global Administrator or Data Administrator.
- 2 Select **Data Sources > Identities**.
- 3 Select the authentication server that you specified during installation.
- 4 Ensure that you have collected data from the data source and it is enabled for user view. For more information, see [“Assigning Authorizations to Identity Governance Users” on page 184](#).
- 5 Scroll down to the **Collect User** or the **Collect Identity** section.
- 6 For **LDAP Distinguished Name**, specify the attribute in your identity source that you want to map to the login attribute for Identity Governance 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. Identity Governance 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 catalog.
- 8 (Optional) To add custom attributes, complete the following steps:
 - 8a Select **Add Attribute**.
 - 8b Specify the settings for the new attribute, and then select **Save**.
 - 8c Specify an attribute from your identity source that you want to map to the new custom attribute.
 - 8d Select **Save**.
- 9 (Optional) Add the new login users to authorizations in Identity Governance. For more information, see [“Assigning Authorizations to Identity Governance Users” on page 184](#).

Understanding Identity, Application, and Permission Management

This section discusses changing identity, application, and permission information:

- ♦ [“Managing Identity Information” on page 226](#)
- ♦ [“Managing Application Information” on page 226](#)
- ♦ [“Reviewing Application Fulfillment Settings” on page 227](#)
- ♦ [“Managing Permission Information” on page 227](#)

Managing Identity Information

Identity information includes the attributes and relationships you collect through the identity collectors, status in Identity Governance, such as role assignments and risk factors, and identity source information. Identity source information shows the collector mappings, curated, and effective values for the identity attributes.

To view or edit identity details:

- 1 Navigate to **Catalog > Users** and select a user. For example, Lisa Haagensen.
- 2 View basic information about that user, and select **More** to see more details.
- 3 Select available tabs to view items such as group membership, role assignments, and source for the user information.
- 4 (Optional) Select the **Edit** icon next to user.
- 5 Modify the available attribute values, and then select **Save**.

Managing Application Information

Application information includes the application's photo, name and description, the identities of the application's owner and administrators as well the method for fulfilling changeset items. You can also specify the risk level for the application and whether reviews include the permission hierarchy of the application.

To manage the application information:

- 1 Navigate to **Catalog > Applications**.
- 2 Select the name of an application. For example, MoneyHoney Financials.
- 3 Select the **Edit** icon.

4 Modify the application settings, such as:

Risk

Specifies the importance the application in terms of limited access and security

For example, you might want to review access to applications with a **high** risk more often than applications with a **mild** risk.

Administrators

Specifies users who can access the Catalog and can manage data

Tags

Specifies a string that creates a new tag or shows existing tags from another application that match the string

Owners

Specifies a user who is responsible for reviews where the review definition references the Application Owner

Show permission hierarchy in review

Specifies whether you want to see the permission that was assigned in a permission hierarchy of relationships when this application is included in a review

Show account name in review and fulfillment details

Specifies whether you want to hide account names

You can use this setting in review definitions as criteria for permissions to be included in the review. For example, if the collected accounts names are obscure names, you might not want to use them.

Permission ID for granting accounts

Specifies whether you want to use an autocompleter of permissions published in the system

Reviewing Application Fulfillment Settings

Identity Governance allows you to specify a fulfillment method for each application. In the catalog, you can see the fulfillment settings for each application.

To review current fulfillment settings:

- 1 Log in to Identity Governance.
- 2 Under **Catalog**, click **Applications**, and select an application.
- 3 Under **Fulfillment Information**, view the fulfillment type and details.

For information about configuring fulfillment methods, see [“Configuring Fulfillment” on page 138](#).

Managing Permission Information

Permission information includes the permission’s photo, name and description, identity of the permission’s owners and the risk level for the permission. You can also observe permission relationships if the permission contains other permissions, has holders, or is part of Separation of Duties policies.

When you save changes, Identity Governance displays an icon beside a changed setting. Select the icon to reset the setting to the originally collected value.

To manage permission information:

- 1 Navigate to **Catalog > Permissions**.
- 2 Select a permission.
- 3 Select the **Edit** icon.
- 4 Modify the permissions settings, such as:

Risk

Specifies the importance the permission in terms of limited access and security

For example, you might want to review access to permissions with a **high** risk more often than permissions with a **mild** risk.

Permission Owner

Specifies one or more users responsible for reviews where the review definition references the Permission Owner

Hide Permission from Review

Specifies whether you want to exclude this permission from reviews

Editing Attribute Values on Objects in the Catalog

After 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 object you want to view.

To edit attribute values, select the pencil icon for that item. Identity Governance displays any attributes that the Data Administrator has designated as editable, along with the current attribute value. When you change a value, Identity Governance shows an icon next to the value to indicate the change. You can later reset the value to its original setting. You can also associate tags, or metadata, so you can more easily identify the information when you create and perform a review.

NOTE

- ♦ You can edit only the attributes that are marked as editable.
 - ♦ You can add new external attributes each time you collect data from a data source. However, after you publish the data for that collector, you cannot remove the attributes.
 - ♦ When you specify a string type for a new extended attribute, Identity Governance always truncates the string at 2000 characters.
 - ♦ If you edit any permission records to set the `excludeFromCatalog` attribute to `true`, the only way to ever see these records in the catalog again is to manually change the `spermission` table value back to `false`, or if bulk editing was used to set it to `true`, copy the Bulk Data Update CSV file that made the original edits and change the edited value to `UNDO_CURATION`.
-

For more information, see the following sections:

- ♦ [“Editing Data” on page 229](#)
- ♦ [“Editing Attribute Values in Bulk” on page 229](#)

Editing Data

When you edit the data, you override the originally collected content. Any attribute that you edit will be persisted through subsequent collection and publication, even if the original value for the attribute changes. To replace the edited value with the currently collected value, reset the collected value.

IMPORTANT: Identity Governance evaluates only collected attribute values for the authentication matching rules, not edited values. For more information, see [“Auth Matching Rules” on page 131](#).

Editing Attribute Values in Bulk

You can edit attribute values for multiple objects at the same time by importing the data into Identity Governance using a comma-separated value (CSV) file. For example, you might want to add photos for users in the catalog. When adding multiple values to a single attribute, separate the values with the pipe sign (|).

IMPORTANT: Identity Governance evaluates only collected attribute values for the authentication matching rules, not edited values. For more information, see [“Auth Matching Rules” on page 131](#).

Before you follow this procedure, make sure you have configured the bulk database folder in the Identity Governance Configuration Utility. For more information, see [“Bulk Data Update Settings” on page 134](#).

To edit a number of attribute values:

- 1 Under **Data Sources** select **Identities** or **Applications** depending on the type of data you want to edit.
- 2 Select **Bulk data update** in the upper right.
- 3 Select **+**.
- 4 Enter all the mandatory fields.
- 5 Select **+** next to **Attributes to update** and select the attributes.
- 6 (Optional) Select **+** next to **Decision context attributes** and select the attributes Identity Governance will use to match the updated information with the correct item.
- 7 Save your settings.
- 8 Select the **Export file** icon to generate the template.
- 9 Get the template from the appropriate location on the Identity Governance server. The template location is specified through the Identity Governance Configuration Utility. For more information, see [“Bulk Data Update Settings” on page 134](#).
- 10 Add the update information to the template, and then copy the updated template to the appropriate location on the Identity Governance server. Identity Governance automatically detects updated files and applies the updated information to your data.

NOTE: You can specify multiple users as permission owners. When performing bulk edits of permission owners, the ID name has changed from `uniqueUserId` to `uniqueOwnerId` and `uniqueOwnerId` requires a new flag, `#true`, with each permission owner ID.

You can also undo an edited value or explicitly set a value to null. Identity Governance recognizes certain keywords in cells that perform specific actions:

- ♦ **UNDO_CURATION:** Removes any previously edited values for this attribute.

- ♦ **SET_NULL**: Sets the appropriate null or empty value on this attribute.

Searching for Users or Groups

You can search for specific items in the catalog by selecting the type of item under **Catalog**, such as **Users** or **Groups**. Then type your search criteria in the search box, and select the search icon.

Identity Governance attempts to complete your search entry as you type. To ensure that users can more easily find a group, always include a description of the group that matches what users might use as a search term. For example, "Finance Team" for your financial group.

Some areas of the catalog provide advanced search options. If available, the search box contains a down arrow icon to access advanced search. The advanced search acts differently from the other searches in Identity Governance.

You can add additional criteria to the advanced search by clicking **+** icon. The advanced search ANDs all search criteria. Meaning for an advanced search to return a catalog item, it must meet all of the search criteria. Some attributes, such as applications or owners, support specifying multiple values in a single criteria to perform OR operations. For example searching for permissions from either application A or B.

The application or owner control provides a type-ahead feature to select applications or users in the system. Searching for applications, groups, or users requires selecting the catalog item. Advanced search does not currently support partial names for applications or owners.

The attributes that appear in the refinement list are fixed for Technical Roles, however, they can be configured for User and Permission catalog items.

To add or remove user attributes from the refinement list:

- 1 Select **Data Administration** > **User** or **Permission**.
- 2 Select an attribute to edit the attribute definition.
- 3 Select the desired searchable option for the attribute to have it displayed in the catalog or not:

Available in catalog searches. Change takes effect after publication.

Select this option to enable the attribute for quick searches. If the option is selected, the attribute is available in the catalog list for searches. This means the search is performed against this column even if this column is not shown in the catalog list.

Display as refine search option

Select this option to enable the attribute for advanced searches.

Display in review item selection criteria

Select this option when you want the attribute displayed in review items. For more information, see [Chapter 22, "Running a Review Instance,"](#) on page 259.

Display in business role selection criteria

Select this option when you want the attribute displayed when creating a business role membership expression. The membership expression contains the search criteria for membership in a business role. For more information, see [Chapter 25, "Creating and Managing Business Roles,"](#) on page 273.

- 4 Select **Save**, then publish the changes to the catalog.

Managing Technical Roles

Technical roles allow business owners to simplify the review process by grouping permissions, which provides a higher level of abstraction, and reduces the number of items for business leaders to review. Technical roles allow the business to provide context for the set of items including a business relevant title and description, risk, cost, and ownership.

After you have published application data, you can create technical roles to group permissions that are common to these technical roles. When you have created technical roles, Identity Governance detects users with permissions that match the technical roles you have defined and lists the technical roles a user has in the user catalog. When you have defined technical roles, you can create user access review definitions for technical roles reviews.

- ♦ [“Understanding Technical Role States” on page 231](#)
- ♦ [“Understanding Technical Role Mining” on page 231](#)
- ♦ [“Creating Technical Roles” on page 232](#)
- ♦ [“Activating Technical Roles” on page 234](#)
- ♦ [“Editing and Deleting a Technical Role” on page 234](#)
- ♦ [“Downloading and Importing Technical Roles” on page 234](#)

Understanding Technical Role States

There are several states in the life cycle of a technical role after they are created manually or mined. From beginning to end, the technical role goes through the following states:

Technical Role State	Description
CANDIDATE	Technical role was created by role mining and must be promoted before it can be activated. This state corresponds to the internal state called MINED.
ACTIVE	Valid, meaning all included permissions are available in the catalog, and the role is included in the detection process.
NOT ACTIVE	Valid; however, the role is excluded from the detection process. This state corresponds to the internal state called REJECTED.
INVALID	Invalid and excluded from detection process due to a detected error. Detection errors are usually the result of a deleted permission that is included in the technical role.

Understanding Technical Role Mining

Identity Governance uses advanced analytics to mine business data and identify role candidates. This process of discovering and analyzing business data in order to group multiple users and access rights under one business or technical role candidate is called Role Mining or Role Discovery. Global

or Technical Role administrators can use role mining to create technical roles with common permissions. Identity Governance uses two approaches to technical role mining to identify technical role candidates.

- ♦ **Automatic Suggestions** enables administrators to direct the mining calculations by either saving the defaults, or by specifying minimum number of permissions that specified number of users should have in common, coverage percentage, maximum number of role suggestions, and other role mining options and saving the options.
- ♦ **Visual Role Mining** enables administrators to select role candidates from a visual representation of the distribution of users based on permissions. Administrators can click in the user access map and drag to select an area in the map, and then view technical role candidates.

NOTE: Technical role candidate can also be generated when using mining to create business roles. For more information about business roles, see [Chapter 25, “Creating and Managing Business Roles,” on page 273](#)

NOTE: Mined business or technical roles are created in a candidate state. Role candidates can be edited and saved, but must be promoted before they can be approved or published as a role.

Creating Technical Roles

To create technical roles you must have either the Global Administrator or the Technical Roles Administrator authorization. You can create technical either manually or by using role mining analytics. Additionally, Business Role Administrator can generate technical roles when creating business role candidate.

When using role mining analytics, permissions are automatically grouped together and presented as role candidates. You must promote role candidates as roles, before they can be activated.

When creating technical roles manually, an understanding of what permissions you want to assign to the technical role is helpful. However, you can create the technical role without adding any permissions to it in order to delegate responsibility for assigning the permissions in a technical role to the Technical Role Owner. The designated owner can then log in to Identity Governance and add the appropriate permissions to the technical role. You cannot activate a technical role until you have added permissions to the technical role.

To create a technical role:

- 1 Log in as a Global or Technical Roles Administrator.
- 2 Under **Catalog**, select **Roles**.
- 3 Select the **Mining** tab.

If	Then
You want to direct role mining calculations and create more than one technical roles	<ul style="list-style-type: none"> ♦ Select Automatic Suggestions. ♦ Save default options, or specify options, and save. ♦ Select one or more items from the list and Create Roles. <p>NOTE: Suggestions are sorted by number of users times the number of permissions. For example, if there are five users who match the role mining options and who hold four permissions in common, they will be listed first, followed by a suggestion with four users who hold four permissions in common.</p>
You want to use user access map to create a role candidate	<ul style="list-style-type: none"> ♦ Select Visual Role Mining. ♦ Click in the map and drag to select an area. ♦ Click View Candidate. ♦ (Optional) Click more to add description, risk, cost, or category. ♦ (Optional) Click + to add permissions, or click Remove next to a permission to remove permissions. ♦ Estimate impact. ♦ Click Create candidate.
<ol style="list-style-type: none"> 4 In the Roles page, click on the mined role. 5 (Optional) Edit the role name, description, risk, cost, or category. 6 Estimate impact by viewing list of associated users and analyzing SoD violations if SoD policies had been previously defined. 7 (Optional) Add or remove permissions based on the estimated impact and save the changes. 8 Select Yes to promote the role candidate. 	
<p>NOTE: If a role candidate is not promoted, it cannot be activated and published as a role.</p>	
<ol style="list-style-type: none"> 9 Alternately, in the Roles page, select + to create a role manually. 10 Enter the required information. 11 (Optional) Select + next to Permissions and select the permissions to include in the role, and then select Add. 12 (Conditional) If permissions have been added to the technical role, estimate impact and edit role if needed. 13 Save your settings. 	
<p>NOTE: When you add a permission to a role, the dialog displays all application permissions in Identity Governance. You can quickly sort or filter permissions by name, description, or application. You can also use the advanced search options to limit the displayed permissions further.</p>	

Activating Technical Roles

After you have added permissions to a technical role definition, you can see an estimate of the number of users holding the permissions of the technical role, and you can activate the definition. If you do not activate the definition, Identity Governance does not identify the users that hold the permissions in the technical role.

NOTE: Mined technical roles are created in a candidate state and must be promoted before they can be activated and published.

To activate a technical role:

- 1 Under **Catalog**, select **Roles** as a Global or Technical Roles Administrator.
- 2 Select the role from the list, then select **Edit**.
- 3 In the role definition, select **Active**.

Activating and deactivating a technical role both start a detection process. Identity Governance detects users in the catalog that contain the permissions when you activate a technical role. When you deactivate a technical role, Identity Governance removes the detected technical roles in the catalog. Similarly, if you change the permissions in an active technical role definition, Identity Governance goes through the detection process and updates the catalog.

You can quickly search for a role by name or description. Identity Governance performs a case-insensitive search of all of the technical roles in the catalog and returns any that contain the string in the technical role name, description, or cost. You can also use the advanced search feature to limit the number of roles.

Editing and Deleting a Technical Role

When you edit a technical role, you can change permissions assigned to the technical role and either leave the technical role active or disable the technical role. However, Identity Governance automatically disables a technical role definition if a permission included in the technical role is deleted from the application. The technical role remains in the disabled state until the permission is removed from the technical role definition or restored in the application and then collected and published to the catalog.

To edit or delete a technical role:

- 1 Under **Catalog**, select **Roles** as a Global or Technical Roles Administrator.
- 2 Select the role you want to edit or delete.
Selecting the role displays a quick overview of the role definition including the name, description, owner, risk, state, selected permissions, and any Separation of Duties policies that reference the technical role.
- 3 Select **Edit** at the end of the details panel to edit the technical role.
- 4 (Conditional) Select **Delete** to delete the technical role.
You must edit the technical role to delete the technical role.

Downloading and Importing Technical Roles

You can download technical roles as a `json` file and import them later into another environment.

To download or import technical roles:

- 1 Under **Catalog**, select **Roles** as a Global or Technical Roles Administrator.
- 2 Select a role or all the roles on the **Roles** tab.
- 3 Select **Actions > Download**.
 - 3a (Optional) Include references to technical role owners and download associated applications and assigned categories.
 - 3b Select **Download**.
- 4 If you make changes, or want to want to import previously downloaded technical roles into another environment, select **Import Technical Roles** on the **Roles** tab.
- 5 Navigate to the technical roles `json` file, select the file to import, and click **Open**.
- 6 Identity Governance detects whether you are importing new or updated roles and whether the updates would create any conflicts or have unresolved references.
- 7 Select how to continue based on what information is displayed.

NOTE: You must activate the role for Identity Governance to recognize the users that hold the permissions as members of a technical role. For more information, see [“Activating Technical Roles” on page 234](#).

20 Grooming the Identity Governance Databases

In addition to regularly backing up the Identity Governance databases, you should periodically groom the databases to remove old and unused data. For example, you can run the Data Purge utility included with Identity Governance.

- ♦ [“Understanding the Data Purge Utility” on page 237](#)
- ♦ [“Identifying Purgeable Data” on page 237](#)
- ♦ [“Purging Data from the Operations Database” on page 240](#)
- ♦ [“Creating a Parameters File to Run the Data Purge Utility” on page 241](#)

Understanding the Data Purge Utility

The operations database (by default, `igops`) maintains a history of activities that occur in Identity Governance. For example, as part of the data collection process, the database stores the previous state of that collection to ensure that Identity Governance can return to that state if an error occurs. Over time, however, the size of the database can increase, and the history list in the user interface can become unwieldy. Identity Governance includes the **Data Purge utility**, which allows you to manually remove historical data.

This utility searches the operations database for purgeable items that are older than the retention date and time or retention days. If you do not specify a retention date and time, the utility uses the current date and time. The utility always preserves the current state of the Identity Governance catalog, such as the most recent version of a review definition. Also, it will not purge data that is in an incomplete or unfulfilled state. For example, an identity has pending changes to its permissions list. Until those changes are resolved or cancelled, the utility does not remove older states of that identity as part of a data source purge. For more information about how the utility decides which items can be purged, see [“Identifying Purgeable Data” on page 237](#).

To run the Data Purge utility, you must have an account with the Global Administrator or Data Administrator authorization in Identity Governance. You should always back up the operations database before purging data to retain historical data that might require records retention for a specific period of time, such as Access Requests, Separation of Duties approvals, and review decisions.

Identifying Purgeable Data

The Data Purge utility removes the following types of data from the operations database when certain conditions are met.

Access Request

Can be purged only when the request is completed, which includes one of the following states:

- ♦ Request was denied approval
- ♦ Request was declined fulfillment

- ♦ Request was fulfilled and verified
- ♦ Request was fulfilled and verification failed

Analytical Facts

Can be purged only when retention time is specified and facts are older than the specified retention time

Business Role

Can be purged under all of the following conditions:

- ♦ Business role approval state must be archive
- ♦ Is not referenced from any review definitions or review items
- ♦ Is not referenced from any change request items

Bulk data update definition

Can be purged if it has been deleted from the Identity Governance catalog.

Certification Policy

Can be purged under any of the following conditions:

- ♦ Policy has been deleted
- ♦ Policy is older than the retention time if specified

Collection

Can be purged under any of the following conditions:

- ♦ Has associations that are not in a canceled, failed, completed, or terminated state
- ♦ Is not in a current snapshot

Data source

Can be purged under any of the following conditions:

- ♦ Is not a parent to another application
- ♦ Is not scheduled for collection
- ♦ Has been deleted from the Identity Governance catalog
- ♦ Is not referenced by a role policy

For example, a role policy references `SPermission` in the data source.

- ♦ Is not referenced by a Separation of Duties policy

For example, a Separation of Duties policy references `SPermission` in the data source.

Request approval policy

Can be purged under all of the following conditions:

- ♦ Policy has been deleted
- ♦ All requests associated with the policy have been previously purged

Request policy

Can be purged under all of the following conditions:

- ♦ Policy has been deleted
- ♦ All requests associated with the policy have been previously purged

Review definition

Can be purged under any of the following conditions:

- ♦ Has been deleted from the Identity Governance catalog
- ♦ Is not referenced by a review instance

Review instance

Can be purged under any of the following conditions:

- ♦ Has been canceled or experienced an error (not running)
- ♦ Is not referenced by a change item action that is not in a verified or error state

NOTE: Materialized view, if any, are also purged when review instances are purged.

Risk Score Status

Can be purged under all of the following conditions:

- ♦ Is in the error, canceled, or completed state
- ♦ If in completed state, there must be another completed risk score status of the same entity type that has a later start time

Snapshot

Can be purged under any of the following conditions:

- ♦ Is not the current snapshot of the Identity Governance catalog
- ♦ Is not a precursor to another snapshot
- ♦ Is not referenced by a review instance
- ♦ Is not referenced by a Separation of Duties violation
- ♦ Is not referenced by a `SPermission` used in a Technical Role definition

Separation of Duties case

Can be purged under any of the following conditions:

- ♦ Case is closed
- ♦ Case action is closed
- ♦ Is referenced by a change item action that is in a verified or error state

Separation of Duties policy

Can be purged under any of the following conditions:

- ♦ Has been deleted from the Identity Governance catalog
- ♦ Does not reference a Separation of Duties policy through a `SoDConditionItem`
- ♦ Does not have a running detection

Technical Role

Can be purged only when *all* of the following conditions are met:

- ♦ Has been deleted from the Identity Governance catalog
- ♦ Is not referenced by a Review Instance through a `ReviewItem`
- ♦ Is not referenced by a Separation of Duties policy through a `SoDConditionItem`
- ♦ Is not referenced by a Review Definition
- ♦ Does not have a running detection

Unregistered Facts

Can be purged when fact tables are available in schema even after custom facts are unregistered from fact catalog

Purging Data from the Operations Database

To run the Data Purge utility, you must have an account with the Global Administrator or Data Administrator authorization in Identity Governance. To avoid entering the settings for the Identity Governance server each time you run the Data Purge utility, you can use a parameters file. For more information, see [“Creating a Parameters File to Run the Data Purge Utility” on page 241](#).

NOTE: The utility always refreshes the list of purgeable items after you perform a purge.

By default, Identity Governance installs the Data Purge utility in the `/opt/netiq/idm/apps/idgov/bin` (Linux) `c:\netiq\idm\apps\idgov\bin` (Windows) directory.

- 1 Back up the operations database (by default, `igops`) to preserve historical information before purging the database.
- 2 (Conditional) If you do not have a parameters file, complete the following steps:
 - 2a Enter the following command:
 - ♦ **Linux:** `./data-purge-utility.sh`
 - ♦ **Windows:** `data-purge-utility.bat`
 - 2b At the prompts, specify the settings for the Identity Governance and OSP servers.
For more information about the required settings, see [“Creating a Parameters File to Run the Data Purge Utility” on page 241](#).
- 3 (Conditional) To run the utility from a parameters file, complete the following steps
 - 3a Enter the following command:
 - ♦ **Linux:** `./data-purge-utility.sh datapurge.paramter.file=file_name`
 - ♦ **Windows:** `data-purge-utility.bat datapurge.parameter.file=file_name`
 - 3b At the prompts, specify the passwords for the Identity Governance user and Client ID for the authentication server.
- 4 (Optional) To review a list of commands and the online help, enter `?`.
- 5 (Optional) To change the timeframe in which the utility searches for purgeable data, complete one of the following sets of steps:
 1. `date`
 2. `mm dd yyyy h:mm:ss AM/PM`
For example, to search for purgeable data since a specific date, enter `date` and then enter `Sep 30 2017 11:20:00 AM`.or
 1. `days`
 2. `n`
For example, to search for purgeable data older than a day, enter `days` and then enter `1`.

NOTE: If you are using a parameters file, the utility applies the retention timeframe specified in the file. You can override that setting by entering a new value.

- 6 Specify the type of data that you want to purge.

For example, to purge one or more data sources, enter **7**.

- 7 Review the list of purgeable items, then specify those that you want to purge.

For example, you chose to purge data sources and the utility responded with the following information:

Data Source Name	Collection ID	Type	Status	Collection Time
1. Full-time Employees	1	Identity	Completed	Sep 29, 2016 9:24:21 AM
2. Miami, Inc. Consultants	3	Identity	Completed	Sep 29, 2016 9:36:36 AM
3. Money Stats	4	Application	Completed	Sep 30, 2016 9:07:01 AM
4. Trending Actions	7	Application	Completed	Sep 30, 2016 11:15:44 AM

To purge the data source called Full-Time Employees, enter **1**. To purge all the sources except Money Stats, enter **1-2,4**.

- 8 To quit the utility, enter **q**.

Creating a Parameters File to Run the Data Purge Utility

When you run the Data Purge utility, you must specify the settings that allow the utility to connect to the Identity Governance server. To speed the process, you create a parameters file that contains these settings, then specify that file to initiate the utility.

For more information about using the file to run the Data Purge utility, see [“Purging Data from the Operations Database” on page 240](#).

NOTE: The Data Purge utility always requests the password for the specified Identity Governance Data Administrator User Name and will accept the password for the Identity Governance OAuth (OSP) Client ID. However, for security reasons, you should not include these values in the parameters file.

- 1 In a text editor, create a new parameters file in the following directory.

- ♦ **Linux:** /opt/netiq/idm/apps/idgov/bin/
- ♦ **Windows:** c:\netiq\idm\apps\idgov\bin

- 2 Specify values for the following parameters:

message.locale

Locale for message prompts

purgeall

Purges all purgeable items from all purgeable types, exits when complete

ar.host

Specifies the host name or IP address of the Identity Governance server

ar.port

Specifies the port of the Identity Governance server

ar.protocol

Specifies whether Identity Governance uses `http` or `https` protocol

ar.user.name

Specifies a user account in Identity Governance with a Data Administrator authorization

ar.usr.password

Specifies the password for the Identity Governance user account

auth.host

Specifies the host name or IP address for the authentication server (OSP)

auth.port

Specifies the port of the authentication server (OSP)

auth.protocol

Specifies whether authentication uses `http` or `https` protocol on the authentication server (OSP)

auth.client.id

Specifies the name used to identify Identity Governance to the authentication server (OSP)

For more information about the server settings, see the following sections:

- ♦ [“Identity Governance Server Details” on page 130](#)
- ♦ [“Authentication Server Details” on page 130](#)

auth.client.password

Specify the password of the `auth.client.id`

- 3 (Optional) Specify the timeframe during which the utility searches for purgeable data:

retention.days

Instructs the utility to search for purgeable data with timestamps older than the specified number of days from the current date.

retention.date

Instructs the utility to search for purgeable data with timestamps older than the specified date and time. Use the following format: `mm dd yyyy h:mm:ss AM/PM`. For example,

`Sep 30, 2015 11:20:00 AM`

NOTE: The utility searches for all purgeable data older than the specified time frame with the following conditions:

- ♦ If you specify values for both `Retention days` and `Retention date/time`, the utility uses the value for `Retention days`.
 - ♦ If you do not specify a value for either parameter, the utility uses the date and time when you initiate the search for purgeable data.
-

- 4 Save and close the properties file.

- 5 To run the utility, see [“Purging Data from the Operations Database” on page 240](#).

Here is the content from a sample parameter file:

```
ar.host=10.10.10.10
ar.port=8080
ar.protocol=http
ar.user.name=jdoe
auth.host=10.10.10.10
auth.port=8080
auth.protocol=http
auth.client.id=iac
retention.days=0
```


IV Creating and Running Reviews

Review Administrators can create several types of reviews to focus reviewers on different types of access, such as user access reviews, mapped and unmapped account reviews, and business role membership reviews. For each type of review, administrators select the users, accounts, applications, permissions, or roles to be reviewed, and define the review process and participants. Administrators and review owners can also preview reviews before going live with the reviews which generate tasks for reviewers. Reviewers determine whether to keep, remove or modify access, change user assignments, or whether to retain role membership for each item assigned to them in the review.

Reviews might contain a single stage, with each review item being assigned to a single reviewer or group of reviewers or multistage, with each review item being assigned to multiple reviewers who act on review items only after the previous reviewer completes an action.

- ♦ [Chapter 21, “Creating and Modifying Review Definitions,” on page 247](#)
- ♦ [Chapter 22, “Running a Review Instance,” on page 259](#)

21 Creating and Modifying Review Definitions

After you have data in your catalog, and (optionally) have customized review display column and configured reasons for review actions by accessing the **Administration** menu; you can begin creating reviews. This is where a set of reviewers examine who has access to what in their environment. Administrators can create review definitions for the following types of objects:

- ♦ Access permissions, accounts, or technical roles of a set of users
- ♦ Unmapped accounts
- ♦ Accounts, which includes both mapped and unmapped accounts, and optionally, the permissions assigned to the accounts
- ♦ Membership of a set of business roles

Only users with the Review Administrator or Global Administrator authorization can create and modify review definitions.

- ♦ [“Viewing the Catalog” on page 247](#)
- ♦ [“Understanding the Review Process” on page 248](#)
- ♦ [“Selecting a Review Type” on page 251](#)
- ♦ [“Creating a Review Definition” on page 252](#)
- ♦ [“Modifying a Review Definition” on page 256](#)
- ♦ [“Specifying Reviewers” on page 256](#)
- ♦ [“Downloading and Importing Review Definitions” on page 257](#)
- ♦ [“Improving Performance in Large Scale Reviews” on page 258](#)

Viewing the Catalog

Before creating or editing review definitions, reviewing the data in the catalog will be helpful in determining who needs to be included in the reviews and whether reviews are needed for certain items. Some examples of the information a Review Administrator or Global Administrator can look for are:

- ♦ Attributes of the user that may not be available in **Quick Info** to help determine whether the person should be included in a review or not
- ♦ The last review date of an account

NOTE: This date reflects the date when an account was last reviewed as part of an **Account Review**. Review of an user’s access to an account as part of an **User Access Review** does not impact this date.

- ♦ Risk levels of users or permissions
- ♦ Association with an application
- ♦ Group or role membership

Understanding the Review Process

Reviews provide a way to monitor access to your business systems. Many users take part in the overall review process:

- ♦ Review administrators create review definitions, preview review definitions, and manage reviews.
- ♦ Review owners preview, monitor, complete, and terminate reviews.
- ♦ Reviewers, such as supervisors and application owners, act on review items.
- ♦ Fulfillers manage change requests.
- ♦ Auditors accept or reject completed reviews.

NOTE: The Identity Governance server needs a 30-minute gap between runs of the same review. For example, you terminate a scheduled review that is in progress. To schedule that review to run again, allow at least 30 minutes to lapse after terminating the previous run. Otherwise, the second run fails to start and Identity Governance does not notify you of the failure.

For multistage reviews, if at any stage in the review an exception occurs, Identity Governance moves the items to the exception queue at the start of the review. The exception queue is handled by the escalation reviewer, if any, or if not, the review owner.

Creating a Review Definition

You can run a review once or multiple times either by starting the review manually or by scheduling it to start at the specified time or interval. Each review is based on a **review definition** that defines all parameters for that particular review process. Review Administrators or Global Administrators create review definitions that focus on specific types of access or access to specific systems. Review definitions assign reviewers based on their relationship to the review items. Often, administrators use review definitions to split up responsibility for reviewing items to prevent bottlenecks and overloading reviewers. Review definitions can also be referenced in certification policies to enable a comprehensive view of your organization's compliance with specific certification controls such as Sarbanes-Oxley Act (SOX) or Health Insurance Portability and Accountability Act (HIPAA).

TIP: For information about certification policies, see [Chapter 28, "Creating and Managing Certification Policies," on page 303](#). Once a review definition is referenced in an active certification policy, it cannot be deleted.

Previewing a Review

Administrators can start a review run, or **review instance**, in preview mode or in live mode. In preview mode, administrators can:

- ♦ Preview review definition version, assigned reviewers, review items, and notification emails
- ♦ Change review properties such as review owner, auditor, review options, or duration properties
- ♦ If needed, change reviewers per review item or in bulk
- ♦ Preview recipients of notifications
- ♦ Export review items to CSV
- ♦ Track details of review assignment changes
- ♦ Go live

NOTE: Review property and reviewer changes made in preview mode will only be applicable to the current review instance. Only changes made in the **Reviews > Definitions** itself, will reflect in future review run instances.

Reviewing Items

When a review run, or **review instance**, is live, the server generates **review items** based on the criteria in the review definition. Assigned reviewers decide what action to take on each review item and submit their decisions. If allowed, by the review definition, reviewers might reassign items to a different reviewer instead of making a decision.

In a multistage review, reviewers must act on review items in the order that the stages are defined in the review definition.

In a review with multiple reviewers for each review item, Identity Governance shows decisions made when the first reviewer submits actions for any of the review items. When any reviewer has submitted a decision for a review item, the other reviewers cannot take any action on that item unless the reviewer has authorization as an administrator. Review items with no actions made remain in each reviewer's list until someone submits actions for them.

NOTE: When Identity Governance cannot determine an identity associated with an account or functional assignment, such as supervisor, to assign a review item to a specific person, the review owner becomes the assignee for the review item. All review items assigned in this way show in an exceptions section in the list of reviewers on the review owner view.

For multistage reviews, if at any stage in the review an exception occurs, Identity Governance moves the items to the escalation reviewer, if any, or if not, the review owner exception queue at the start of the review.

Setting Up Review Notifications

Email notifications let reviewers, escalation reviewers, owners, and others know when a review is at various stages of a review run. The **Notifications** area of a review definition allows you to set up several standard notifications to go to whomever you specify during the course of a review. You can click on an email name to view who will receive the email, why they will receive it, and when they will receive it. You can either accept the defaults or customize it. You can also view the name of the email source, preview the email, and email the notification to specified email address. In addition, you can remove a default notification and add new notifications by selecting an email template provided by Identity Governance. For information about customizing the templates, see [“Customizing the Email Notification Templates” on page 160](#). For information about disabling email notifications such as notification when a running review is terminated or notification when permissions are revoked, see [“Disabling Review Email Notifications” on page 172](#).

Escalating Review Items

Identity Governance provides escalation options to help Review Owners and Administrators ensure that the review process proceeds in a timely manner. You can set one or more escalation reviewers and a timeout value to instruct Identity Governance to **escalate the process** and move pending review items to escalation reviewer queues. If a review definition does not set escalation reviewers, the review owner becomes the default escalation reviewer.

NOTE: If a review definition specifies a group as the reviewers and a member of the group is the person being reviewed, Identity Governance sends the review item to the escalation reviewer instead of to the members of group. To prevent this, enable **Allow self review in all stages**, and Identity Governance then sends the review to the members of the group instead of to the escalation reviewer.

Setting Review Expiration Policy

Review definitions contain an expiration policy. Review administrators and owners specify the actions that Identity Governance takes when a review expires without being completed:

- ♦ complete the review with any final decisions that have been made and send these to fulfillment and the auditor, if these are defined, and leave all other items with no decision
- ♦ complete the review with any final decisions that have been made and send these to fulfillment and the auditor, if these are defined, and keep all other items with assigned accounts, permissions, or roles
- ♦ complete the review with any final decisions that have been made, assign remove decision to all other items, and send all to fulfillment and the auditor, if these are defined
- ♦ extend the review for a grace period that will continue to renew each time the review expires without being completed or terminated
- ♦ terminate the review and discard all decisions

For Identity Governance 2.0 and later, review definitions have the default expiration policy set to complete the review. For review definitions migrated from earlier versions of Identity Governance, review definitions have the default expiration policy set to terminate the review and discard any decisions.

Completing or Terminating a Review

Aside from letting the expiration policy complete the review run, a review run concludes in one of several ways:

- ♦ All specified reviewers submit actions for their review items, and the Review Owner approves or terminates the review run.
- ♦ Reviewers do not submit actions for all their review items, and the Review Owner completes the review run.
- ♦ Reviewers do not submit actions for all their review items, and the Review Owner terminates the review run.

After reviewers have made decisions and submitted all review items, the Review Owner approves or terminates the review run and Identity Governance moves the review run details to a list of completed reviews.

A Review Owner has the option to complete an in-progress review even if reviewers have not submitted decisions for all review items. When a Review Owner completes a review, Identity Governance takes the following actions:

- ♦ Forwards any final decisions that reviewers have made to fulfillment (when all multi-stage reviewers of a review item have submitted their decisions, the review item has a final decision made)
- ♦ Marks the remaining review items **Keep**, **Remove**, or as no decision made based on the review definition expiration policy
- ♦ Shows the review status as a percentage of completion in review history

A Review Owner also has the option to terminate an in-progress review. When a Review Owner terminates a review, Identity Governance takes the following actions:

- ♦ Does not forward anything to fulfillment
- ♦ Marks the review run as terminated

Fulfilling Changes and Audit Acceptance

The **fulfillment** process begins when a review run completes or when a review owner approves review items individually. For more information about fulfillment, see [“Fulfilling the Changeset for a Review Instance” on page 260](#).

The Review Auditor, if specified, accepts or rejects the review run after the review owner approves it. Although a **review audit** is a legal stamp, accepting a review has no impact on the fulfillment of the requested changes.

Selecting a Review Type

Identity Governance enables administrators to create four types of review definitions. Each review type can be defined by selecting different types of objects. Use the following table to select the review type based on the object or objects you want to review, and then create review definition using the procedures in [“Creating a Review Definition” on page 252](#).

	User Access Review	Unmapped Accounts	Account Review	Business Role Membership Review
Identities	Y	N	Y	N
Permissions	Y	N	Y	N
			Permissions are grouped by accounts in this type of review. Use User Access Review if you want to review individual permissions.	
Unmapped Accounts	N	Y	Y	N
Mapped Accounts	Y	N	Y	N
	You can only review an user's access to an account in this type of review. Use Account Review for reviewing account in totality.			
Applications	Y	Y	Y	N
Technical Roles	Y	N	N	N
Business Roles	N	N	N	Y

Creating a Review Definition

The review definition contains all of the information required to run a review. You can also modify the definition for subsequent review runs without the need to create additional review definitions. To create a review definition, the catalog must contain published data.

- 1 Log in as a Review Administrator.
- 2 Select **Definitions**.
- 3 Select **+** to create a new review definition.
- 4 Select the review type based on the object or objects you want to review. For more information, see [“Selecting a Review Type” on page 251](#).
- 5 Name and describe the review.
- 6 (Optional) For **Review Instructions**, enter information that explains to reviewers what they need to do. For example, please review these items or reassign to someone else if necessary.
- 7 Specify review items.

NOTE: The options for specifying review items will differ based on the review type. If you select **User Access Review**, go to [Step 8 on page 252](#). If you select **Unmapped Accounts**, go to [Step 9 on page 253](#). If you select **Account Review**, go to [Step 10 on page 254](#). If you select **Business Role Membership Review**, go to [Step 11 on page 254](#).

- 8 (Conditional) For **User Access Review items**, specify the permissions, authorizations, accounts, applications, users, or a combination of these that you want to review for user access reviews.

Use the following options:

All permissions

Specifies that you want to review the selected users regardless of assigned permissions.

Select permissions

Indicates that you want to enter the permissions criteria for reviewing users.

All roles

Specifies that you want to review the selected users only if their permissions are included in a role in Identity Governance.

Select roles

Indicates that you want to enter the roles criteria for reviewing users.

All applications

Specifies that you want to review the selected users for any application. When you select this option, you then select whether to review the users based on permissions or accounts.

Select applications

Indicates that you want to enter the application criteria for reviewing users.

All users

Specifies that you want to review every user in the catalog

Select users

Specifies that you want to enter the criteria for users to review. You can enter specific user names, browse for users, as well as define criteria such as users in a particular group.

Group

*Applies only when you select **Select users**.*

Specifies the names of the user groups that you want to include in the review.

Managed by

*Applies only when you select **Select users**.*

Indicates that you want to review all users who directly report to the specified manager.

Reporting up to

*Applies only when you select **Select users**.*

Indicates that you want to review all users within the reporting structure of the specified manager. For example, you might want to review a large department that includes several managers with direct reports. To do so, specify the individual to whom the managers report.

Risk

*Applies only when you select **Select users**.*

Indicates that you want to review all users with a greater than, less than, or equal to your risk threshold. For example, you might want to review only users with greater than or equal to 50% risk.

Additional Criteria from the catalog

*Applies only when you select **Select users**.*

In the attribute definition editor of the catalog, you can specify whether an attribute can be used as review criteria. For example, Title, Department, and Job Code. Identity Governance adds these items to the select criteria menu.

TIP: When you specify a boolean attribute in your review criteria and there are null attribute/column values in the database these records will be ignored. You will have to either ensure that there are no null values if you intend to use the attribute as review criteria or add transformation code to convert a null to be true or false or use bulk data update settings to change the null values to true or false. For more information see, [“Editing Attribute Values in Bulk” on page 229](#).

NOTE: When you narrow the review items by specifying criteria rather than selecting all users, permissions, or other types of review items, you have the following options for selecting them:

- ♦ Start typing the name and select the item you want
 - ♦ Select the magnifying glass icon to browse the items
 - ♦ Select + to add selection criteria
-

- 9 (Conditional) For **Unmapped Account Review items**, specify the accounts and applications you want to review.

Use the following options:

All unmapped accounts

Specifies to review all unmapped accounts from all applications.

Select unmapped accounts

Specifies that you want to enter the criteria for unmapped accounts to review. You can enter specific account names as well as define criteria such as last login, last unmapped account review, or number of logins.

All applications

Specifies to review all applications for unmapped accounts. When you select this option, you have an additional option to specify all or selected unmapped accounts.

Select applications

Specifies that you want to enter the application criteria for reviewing unmapped accounts.

- 10 (Conditional) For Account Review items, specify the accounts, identities, and applications you want to review.

Use the following options:

Accounts

Specifies the combination of mapped and unmapped accounts to review.

Identities

Specifies to review all users or select users.

Applications

Specifies to review all applications or select applications.

- 11 (Conditional) For **Business Role Membership Review**, specify the business roles you want to review.

Use the following options:

All business roles

Specifies to review all business roles.

Select business roles

Specifies that you want to enter the criteria for business roles to review. You can enter specific business role names as well as define criteria such as owners or risk.

- 12 (Optional) Further expand or restrict **User Access Review items** and **Account Review items** by selecting related check boxes. For more information, see [“Expanding and Restricting Review Items” on page 256](#).

- 13 (Optional) Select **Estimate Impact** to view the number of users, permissions, roles, accounts, and review items affected by the review.

Because the information is a snapshot of the current state of the catalog, Identity Governance reports approximate numbers. Depending on when you run the review, the catalog might have changed.

Based on the number of items to be reviewed, you might need to revise the **Review period**. For example, a review with 15 items might be completed within days, but one with hundreds of items could require weeks to accomplish.

- 14 (Optional) For **Review Options**, select any additional options that apply to this review. For example, you can require comments for certain actions and allow review owners to override decisions.

- 15 (Optional) Specify the reviewers you want to participate in the review.

For more information about types of reviewers, see [“Specifying Reviewers” on page 256](#).

- 16 (Optional) To create a serial, multistage review, select **Add Reviewer**.

This allows you to specify multiple individuals who review the identity's permissions in the order listed in the definition. For more information, see [“Specifying Reviewers” on page 256](#).

- 17 (Optional) For **Monitor Reviews**, specify the review owner and auditor.

If you do not specify the review owner, the person who created the review definition becomes the review owner by default. If you do not specify an auditor, the review will not go through the audit acceptance phase.

(Conditional) If materialized view is enabled, select **Cache review item names** to cache user, account, permission, and role names to improve performance in large scale reviews.

WARNING: If you enable caching, periodically **Refresh** cache review items to synchronize the review with changes to the catalog. For more information, see [“Improving Performance in Large Scale Reviews” on page 258](#).

18 (Optional) For **Escalation**, specify the following options:

18a Specify the Escalation Reviewer. If you do not specify a value, Identity Governance escalates tasks to the Review Owner.

18b For **escalation timeout**, specify the amount of time allowed for the Reviewers to complete their tasks. You must use whole numbers for the value.

19 (Optional) For **Duration**, set or change any of the following options:

19a For **Review period**, specify the length of time allowed for the review run.

19b For **Expiration policy**, specify what happens when a review expires without being completed.

19c For **Partial approval policy**, specify whether partial approvals are allowed and if so, whether or not partial approvals will occur automatically.

19d For **Validity period**, specify the length of time that the reviewed data will be valid. For example, if you intend to run the review twice a year, specify `6 months`.

20 (Optional) For **Notifications**, customize and add recipients or remove default review notifications. Click **Email source preview** to preview email HTML source and specify a recipient and **Send** the rendered version of the email. Click **Add notification** and specify options to add more notifications based on different criteria.

NOTE: You can specify only one recipient in the **To** field and multiple recipients in the **CC** field. The read-only **Review terminated notice** goes to reviewers, review owners, escalation reviewers, and auditors when a review ends. You cannot change the recipients.

21 (Optional) For **Schedule**, if you want the review runs to begin automatically and repeat automatically, select **Active** and select the appropriate schedule. Select **Start scheduled review in Preview mode requiring manual go live** to start a review in preview mode.

NOTE: The Identity Governance server needs a 30-minute gap between runs of the same review. For example, if you schedule a review to run at frequent intervals, allow at least 30 minutes to lapse between the runs. Otherwise, the subsequent runs might fail to start and Identity Governance does not notify you of the failure.

22 (Optional) For **Default Reviewer Display Preferences**, specify the default grouping and default sort for the reviewer display. Specify default reviewer columns by using display columns previously customized for each review type using the **Administration > Review Display Customization** menu, or set default columns for the current review definition.

NOTE: If needed, the reviewer can change the default grouping for the current review instance by using the **Show All** drop-down list, change the sort order by clicking on headings with descending or ascending arrow, and change the column display by using the display options settings menu.

23 Save the review.

Expanding and Restricting Review Items

In addition to specifying review items using different combinations of users, permissions, accounts, and roles selections, administrators can further expand or restrict items being reviewed in an **User Access Review** and an **Account Review**. For example, selecting **Additionally review accounts for the selected users and permissions for User Access Review items** would enable you to review the accounts that grant the specified permission for the selected set of users and make a decision on it, whereas without selecting this option you will see the account name in the detail information, but will not be able to make a decision about it. You can also select options related to roles, such as to show and review permissions that are part of a technical role or limit review items based on whether the items were authorized or not authorized by a business role.

NOTE: In order for an account to be authorized by a business role, the application to which the account belongs to should be added as an authorized resource for the business role. For more information, see [“Adding Authorizations to a Business Role” on page 281](#).

Modifying a Review Definition

Administrators can modify the attributes of a review definition at any time, including the Review Owner. If there is a running review instance at the time, that running review instance is not affected by changes to the definition. Identity Governance creates a new version of the definition with the changes and only future runs started since the modified definition will reflect the change.

If you have a review currently running, modifying the review definition does not change the attributes of the current review. The running review always points to the version of the review definition that you used to start the review.

If you assign a new owner to a running review instance, both the previous and new owners can access that specific instance of the review. The previous owner continues to see review runs from before the ownership change and future review runs. The new owner sees only that review run. You can also change the review end date and time for a running review.

Specifying Reviewers

When defining a review, you assign users and roles to perform the review. Depending on the type of review, you can specify any of the following options:

Reviewing User Access	Reviewing Unmapped Accounts	Reviewing Accounts	Reviewing Business Role Membership
Supervisor of the individual being reviewed	Owner of the application being reviewed	Supervisor of the individual being reviewed	Supervisor of the individual being reviewed
Owners of the applications being reviewed	Selected users or groups	Owner of the application being reviewed	Business role owner
Owners of the permissions being reviewed (not available for roles reviews)	Account custodian	Owner of the account being reviewed	Selected users or groups
Holder of the permission being reviewed, called self review	Business role	Selected users or groups	Business role

Reviewing User Access	Reviewing Unmapped Accounts	Reviewing Accounts	Reviewing Business Role Membership
Selected users or groups		Account custodian	
Coverage map		Coverage map	
Business role		Business role	

For more information about owners of applications and permissions, see [“Understanding Identity, Application, and Permission Management” on page 226](#). For more information about coverage maps, see [“Using Coverage Maps” on page 165](#).

If you specify more than one reviewer stage, the reviewers must complete the review in the assigned order. For example, you might want the permission holders to verify that they continue to need the assigned permission, then the individual’s supervisor can approve that ongoing need. As a final step, the permission owners can review the assigned permission. In this case, you would specify **Self review**, **Supervisor**, then **Permission owners** as the reviewers. Each stage shows as a separate group of review items to the review owner. When you select **Self Review**, users can review their own access for that stage only, unless the Review Options are set to **Allow self review in all stages**.

If you specify more than one reviewer (such as a set of users or groups), each of the reviewers share the responsibility for submitting a decision within a single reviewer stage. For example, you might want the permission holders to verify that they continue to need the assigned permission, then you want a group of users called **Super group** to approve the ongoing need. In this case, you would specify **Self review** then **Review by Selected Users: Super group** as the reviewers.

At any point during a review run, Identity Governance might not be able to resolve a reviewer. For example, if you specify **Permission owners** as one of the reviewers and no permission owner is actually specified in the catalog, Identity Governance cannot resolve the reviewer to an identity. When this happens, the review item is escalated to the Escalation Reviewer, if one exists, or to the Review Owner, and this reviewer must complete the remaining review tasks for the item. In this situation, the review owner sees an Exceptions stage with these review items in that stage.

To ensure a timely review process, you can also specify an **Escalation Reviewer**. This individual resolves all review tasks that are not completed on time. If you do not specify an Escalation Reviewer, the owner of the review must perform these tasks. Escalated review items also appear in the Exceptions stage. If Identity Governance detects any escalations at the start of a review, all of the review items appear in the Exceptions stage.

For more information about review authorizations, see [“Runtime Authorizations” on page 181](#).

Downloading and Importing Review Definitions

You can download review definitions as `json` files and import them later into another environment.

To download or import review definitions:

- 1 Log in to Identity Governance as a Review or Global Administrator.
- 2 Under **Reviews**, select **Definitions**.
- 3 Select a definition or all the definitions.
- 4 Select **Download**.
 - 4a (Optional) Download included business roles, technical roles, and associated applications.
 - 4b Select **Save**.

- 5 If you make changes, or want to want to import previously downloaded review definitions into another environment, select **Import Review Definitions**.
- 6 Navigate to the review definitions `json` file, select the file to import, and click **Open**.
- 7 Identity Governance detects whether you are importing new or updated roles and whether the updates would create any conflicts or have unresolved references.
- 8 Select how to continue based on what information is displayed.

Improving Performance in Large Scale Reviews

Identity Governance supports **materialized view**. Materialized view is a snapshot or an instance of time which is used to optimize performance in large scale reviews. If this view is enabled using the global configuration setting `iac.review.display.materializedViews.enabled`, you can cache user, account, permission, and role names to improve rendering time of review items by selecting **Monitor Reviews > Cache review item names** in a review definition. The search and sort features will use the values at the time the materialized view was either created or last refreshed.

NOTE: For small scale reviews, caching of review item names is NOT recommended.

As by definition, a materialized view is a snapshot, the data can become stale and out of sync with the catalog, and your search might not yield accurate results. You can refresh the snapshot data at any time by viewing the review definition of a review instance, and clicking **Refresh**. In addition, you can **Enable** or **Disable** the caching of review item names for that review instance.

NOTE: If materialized view is not initially enabled using the global configuration utility, **Cache review item names** check box will not be displayed.

22 Running a Review Instance

When you start a review in live mode, Identity Governance initiates a running review instance and notifies any person or role specified in the **Notifications** settings of the review definition. A review instance will always be associated with the version of the review definition used to start it. After a review owner approves the review run or individual review items, Identity Governance notifies fulfillers if they have change items. For more information, see [“Checklist for Managing a Review in Live Mode” on page 340](#).

- ♦ [“Completing Review Tasks” on page 259](#)
- ♦ [“Verifying and Approving a Review Instance” on page 259](#)
- ♦ [“Fulfilling the Changeset for a Review Instance” on page 260](#)
- ♦ [“Confirming the Fulfillment Activities” on page 261](#)

Completing Review Tasks

Identity Governance notifies reviewers by email when they have tasks for a review run. When you log in as a reviewer, you can see the assigned tasks for each review. Then you can evaluate the items in the task list. Usually, you either certify the permissions assigned to users for a particular application or the presence of unmapped accounts in the application.

After the reviewers have completed their tasks, a Review Owner must approve the changes to create a change list to be fulfilled. At this point, fulfillers and the review auditor, if one exists, get email notifications that they have tasks to complete in the review. For more information about these authorizations, see [“Runtime Authorizations” on page 181](#). For automated fulfillment configurations, Identity Governance sends fulfillment changes to configured systems. For more information about automated fulfillment, see [“Configuring Fulfillment” on page 138](#).

For more information about completing review tasks, see [Chapter 34, “Instructions for Reviewers,” on page 333](#).

Verifying and Approving a Review Instance

Review owners can review the decisions at any time during a review run. The owner can override the status of any decision if **Allow review owner to override decision** is enabled in the review definition. For example, if the review owner changes a **Remove** decision to **Keep**, that decision becomes the final decision for that item.

At any point during the review run, the review owner can end the run by selecting **Complete**, or **Terminate**. Any decisions made before completing an in-progress review are retained and forwarded to fulfillment, when selecting **Approve**, if partial approval was allowed in review definition **Duration > Partial approval policy**.

For more information, see [“Approving the Review” on page 343](#).

Fulfilling the Changeset for a Review Instance

An application owner can configure the application source to require manual or automated fulfillment. After a review generates a changeset for fulfillment, Identity Governance determines which applications have change items. Depending on the specified fulfillment type for the application, Identity Governance performs one of the following actions:

- ♦ [“Manually Fulfilling the Changeset” on page 260](#)
- ♦ [“Using Workflows to Fulfill the Changeset” on page 261](#)
- ♦ [“Automatically Fulfilling the Changeset” on page 261](#)
- ♦ [“Using Service Desk Fulfillment” on page 261](#)

Data administrators can configure the fulfillment method for an application, including configuring multiple fulfillment targets for an application based on change request types. For more information, see [“Configuring Fulfillment” on page 138](#).

Manually Fulfilling the Changeset

During the fulfillment stage of the review instance, Identity Governance creates a task for each review item that must be changed. The assigned fulfillers complete the requested changes in a domain-specific manner, based on the actual permission. The process of fulfilling the changes might occur over the span of many days and you might need to remove many permissions. To complete the process in a timely manner, global or fulfillment administrators can specify a group of users to serve as the Fulfiller. Users in the specified group can work concurrently to fulfill the changes.

Identity Governance provides change items, either through a completed review or SoD case review. Following are some examples of the change items:

- ♦ Remove user from account (user access review), fulfilled by either removing the user from the account or removing the account
- ♦ Modify user access with fulfillment instructions, fulfilled by following the reviewer’s instructions
- ♦ Remove account (unmapped and mapped account review) fulfilled by removing the account
- ♦ Remove permission assignment (user access review or SoD case), fulfilled by removing the permission assignment to the user
- ♦ Assign user (unmapped and mapped account review), fulfilled by assigning user to account
- ♦ Modify account with fulfillment instructions, fulfilled by following the reviewer’s instructions

NOTE: Modify user access and modify account changesets might have a reason, and a user selection might also be required. For more information, see [“Configuring Reasons for Review Actions” on page 172](#). For more information about specific change request types, and fulfillment status, see [“Configuring Fulfillment” on page 138](#).

Identity Governance sends emails to the fulfillers to remind them that they have a manual fulfillment task. The email provides a link to the task. Administrators can customize the message in this reminder. For more information about customizing, see [“Customizing the Email Notification Templates” on page 160](#).

For more information about performing fulfillment tasks, see [Chapter 36, “Instructions for Fulfillers,” on page 345](#).

Using Workflows to Fulfill the Changeset

If you integrate Identity Governance with Identity Manager, you can use a custom workflow to remove the permissions. You create the workflow in the identity applications. In Identity Manager, you specify global configuration values (GCVs) to store the connection parameters between the workflow and Identity Governance. The workflow also must have inputs specified in the following fields:

- ♦ String: `changesetId`
- ♦ String: `appId`

Identity Governance sends the `changesetId` and `appId` to the workflow to process the fulfillment tasks for the review's changeset. The workflow parses the information in the changeset and completes the tasks. When the workflow finishes, Identity Manager informs Identity Governance, which then changes the status of the changes to complete.

For more information, see “[Configuring and Managing Provisioning Workflows](#)” in the *NetIQ Identity Manager - Administrator's Guide to the Identity Applications*.

Automatically Fulfilling the Changeset

You can assign automated provisioning to any application source that derives from Identity Manager. After you complete a review, Identity Governance sends the requested changes to the Identity Manager Identity Vault. The permission type determines whether Identity Manager can automatically provision the requested change. In the identity applications for identity Manager, you specify whether a permission is a **resource** or a **role**. Identity Manager can automatically deprovision all resources because they are explicitly set for the user. Similarly, if a role is explicitly set, it can be deprovisioned. For example, the user has an `nrfAssignedRole` attribute pointing to that role. However, Identity Manager cannot deprovision roles that a user receives indirectly. For example, the user is a member of a container or group to which the role has been assigned.

If deprovisioning can be done automatically, Identity Manager propagates those updates to the connected systems. For those roles that cannot be deprovisioned automatically, the fulfillment process includes a **fallback method**. You can specify that Identity Governance can revert to manual fulfillment or to using an Identity Manager workflow.

Using Service Desk Fulfillment

You can integrate and automate Identity Governance fulfillment with your service desk system by adding and configuring a connector to your service desk system in Identity Governance **Fulfillment Configuration**. For more information, see “[Configuring Service Desk Fulfillment](#)” on page 141.

Confirming the Fulfillment Activities

When the Filler confirms the review fulfillment, Identity Governance updates the fulfillment item status under Fulfillment. Bootstrap, global, and fulfillment administrators can access the Fulfillment tab, as well as any individuals with the Filler authorization in Identity Governance. After the administrator collects and publishes application sources again, Identity Governance updates the status of the fulfillment of all changesets except modify changesets.

The Review Auditor, if assigned, must accept or reject the review. Auditors can see the details and history of the review items. When rejecting a review run, the Auditor must add a comment about the rejection. Before the Auditor can verify fulfillment of the requested changes, you must collect and publish all identities and the application sources related to the review. If the review does not have any fulfillment activities, you do not need to perform this action.

For more information, see [“Viewing Fulfillment Status”](#) on page 343.

V Using Policies in Identity Governance

Policies show external auditors that you have structures in place to ensure compliance in your environment. Separation of duties policies work to keep any single user from having too much access. Business roles automate applying appropriate access based on job function. Risk factors and weighting allow Identity Governance to calculate the level of risk based on your criteria. Request automates granting access on user requests by letting you define criteria to automatically grant requested access or route approval requests to the appropriate entity. Certification policies provide compliance status of all access review processes included in a policy definition.

- ♦ [Chapter 23, “Creating and Managing Separation of Duties Policies,” on page 265](#)
- ♦ [Chapter 24, “Managing Separation of Duties Violations,” on page 269](#)
- ♦ [Chapter 25, “Creating and Managing Business Roles,” on page 273](#)
- ♦ [Chapter 26, “Calculating and Customizing Risk,” on page 289](#)
- ♦ [Chapter 27, “Administering Access Request,” on page 297](#)
- ♦ [Chapter 28, “Creating and Managing Certification Policies,” on page 303](#)
- ♦ [Chapter 29, “Creating and Managing Delegation,” on page 307](#)
- ♦ [Chapter 30, “Creating and Managing Data Policies,” on page 309](#)

23 Creating and Managing Separation of Duties Policies

Separation of Duties Administrators can create policies to enable Identity Governance to look for users and accounts holding too much access. Identity Governance creates cases when it finds violations, and policy owners review the cases and approve or resolve the violations.

- ♦ [“Understanding Separation of Duties” on page 265](#)
- ♦ [“Creating and Editing Separation of Duties Policies” on page 265](#)
- ♦ [“Understanding the Separation of Duties Policy Options” on page 266](#)
- ♦ [“Importing Separation of Duties Policies” on page 268](#)
- ♦ [“Downloading Separation of Duties Policies” on page 268](#)

Understanding Separation of Duties

When any one person in your organization has access to too many systems, you could have problems proving that your systems are safe from fraud when it is time for audits.

The SoD Administrator should be a business owner who understands the appropriate access levels for individuals in your company. By creating policies to keep any one person from having too much responsibility, the SoD Administrator enables Identity Governance to identify users with access to company assets that should be reviewed. Having these SoD policies puts access control rules over your business systems to give you the ability to show auditors the automated protection that Identity Governance provides.

When you have active SoD policies, Identity Governance provides the ability to check for current or potential violations and warns of violations when executing actions such as performing reviews, defining roles, requesting access, approving access, or examining manual fulfillment requests. Identity Governance also creates cases for any violations of the policies and lists them on the **Violations** page. The SoD Administrator or policy owners review the cases to determine whether to resolve or approve them.

The SoD cases are similar to the standard review process. Instead of a review definition running on a regular schedule, SoD policies run as long as they are active and continuously create cases for violations. For more information about reviews, see [“Understanding the Review Process” on page 248](#).

Creating and Editing Separation of Duties Policies

After you have published data, you can create separation of duties (SoD) policies that Identity Governance uses to alert you of possible violations. When you have active SoD policy definitions, Identity Governance lists violations and creates cases for you to review and approve or send to fulfillment for correction. Users with the Separation of Duties Administrator or Global Administrator authorization can create and modify SoD policies.

- 1 Under **Policy**, select **SoD**.
- 2 Select **+** to create a separation of duties policy.

- 3 (Optional) Select **Active** to have Identity Governance discover violations of the policy and create SoD violations and cases.
- 4 Enter the required information. For more information, see [“Understanding the Separation of Duties Policy Options” on page 266](#).

NOTE: Policy names must be unique. When Identity Governance checks for uniqueness, case is not considered. Therefore, Identity Governance considers SoD1 and SOD1 to be equivalent.

- 5 (Optional) Specify one or more compensating controls and a maximum control period. Identity Governance displays these compensating controls in SoD cases as a selection for approving a violation to continue for a certain time period. For more information, see [“Deciding what Occurs when the Separation of Duties Policy is Violated” on page 267](#).
- 6 (Optional) Click Estimate Violations to see an estimate of the number of violations of this policy. You must add SoD conditions to make this button active.
- 7 Save your settings.

After a policy has been created and activated, some of the permissions or authorizations listed in the policy's conditions might be deleted. When this happens, the policy is marked as invalid, and all of the policy's currently open SoD cases are put on hold. If the policy is not active, deleting its permissions or authorizations has no effect, since no detection is being done for the policy.

Understanding the Separation of Duties Policy Options

When you create an SoD policy, you must define what conditions make up the policy, what happens when the policy is violated, and how to solve the violation. Use the following information to create the SoD policies that work best in your environment.

- ♦ [“Providing Resolution Instructions for the Separation of Duties Policies” on page 266](#)
- ♦ [“Deciding what Occurs when the Separation of Duties Policy is Violated” on page 267](#)
- ♦ [“Defining Separation of Duties Conditions” on page 267](#)

Providing Resolution Instructions for the Separation of Duties Policies

When a violation of the SoD policy occurs, Identity Governance displays the violations on the **Policy > Violations** tab. Users with the proper access can access and review these violations. When you provide resolution instructions, users can see what to do in Identity Governance without having to wait for further instructions on how to solve the violations. Providing these instructions is optional.

You add the resolution instructions when you create the SoD policy in the **Resolve** field. You can embed HTML links in these instructions to point to additional information or instructions for a user to follow.

Deciding what Occurs when the Separation of Duties Policy is Violated

When users review and manage an SoD case, they can resolve the violation or allow the violation to continue for a certain period of time. A user can specify compensating controls for an SoD policy.

When allowing a violation to continue, if compensating controls have been defined for the policy, the user can select one or more of them to specify what controls should be in place in order to allow the violation to continue.

When users allow a violation to continue, the user can select one or more of the defined compensating controls to enforce during the continuation period of the violation. They can also specify the amount of time that the violation can continue, but the time must be less than or equal to the maximum control period defined in the policy. The maximum time is 32768 days.

You add these compensating controls when you create the SoD policy in the **Compensating Controls** field.

Defining Separation of Duties Conditions

An SoD policy specifies what combinations of permissions and roles are illegal for a user to hold by defining one or more conditions. Each condition specifies some combination of permissions and roles that are illegal. Most of the time, a single condition suffices, but there are scenarios where you must define multiple conditions to cover more complicated combinations.

Identity Governance tests a user's permissions and roles against a condition to see if the user has the combination of permissions and roles specified in the condition. If the user's permissions and roles match the condition, the user violates that condition. If a user's permissions and roles violate **every** condition in the SoD policy, the user is in violation of the policy.

Identity Governance also tests unmapped accounts against the SoD policies. Unmapped accounts or accounts with no associated users may have permissions assigned to them. Identity Governance uses the same procedure for unmapped accounts as it does for users. It tests if the account has the combination of permissions specified in the condition. If the account's permissions match the condition, the account violates that condition. If an account's permissions violate **every** condition in the SoD policy, the account is in violation of the policy.

Many simple policies require only a single condition to specify illegal permission and role combinations. More complex combinations require multiple conditions, but it is probably very rare that you need more than two conditions.

A condition consists of two parts:

- ♦ A list of one or more permissions and roles that Identity Governance tests against a user's permissions and roles. The list can consist of all permissions, all roles, or a mixture of permissions and roles.
- ♦ A condition **type** specifies how Identity Governance evaluates the user's permissions and roles. There are three types of policy conditions:

User has all of the following

A user violates this condition if the user has all of the listed permissions and roles. This is the most commonly used type of condition. You can specify most illegal combinations of permissions and roles using a single condition.

User has one or more of the following

A user violates this condition if the user has any of the specified permissions and roles. The condition must always be used in conjunction with one or more of the other conditions. Identity Governance does not allow an SoD policy with a single condition of this type.

NOTE: Identity Governance does not allow a SoD policy that would make it illegal for a user or account to possess a single permission or role all by itself. For example, a policy with a single **User has all of the following** condition that lists a single permission or role, or a policy that has a single **User has one or more of the following** condition.

To enforce this restriction, Identity Governance tests each permission or role specified in a policy's conditions. For each listed permission and role, it simulates a dummy user that possesses exactly that one permission or role and determines if the dummy user would violate all of the conditions of the policy. If it does, the policy is invalid and Identity Governance does not allow the SoD policy to be saved in that state.

User has more than one of the following

A user violates this condition if the user has two or more of the specified permissions and roles. A condition of this type must list at least two permissions and roles. If the condition lists exactly two permissions and roles, it is equivalent to a **User has all of the following** condition with two permissions and roles.

Importing Separation of Duties Policies

You can import SoD policies by uploading a `json` file.

- 1 Under **Policy**, select **SoD**.
- 2 Click **Import Separation of Duties Policies**.
- 3 Navigate to the file, select the file to import, and click **Open**.
- 4 Identity Governance detects whether you are importing new or updated policies and whether the updates would create any conflicts.
- 5 Select how to continue based on what information is displayed.

Downloading Separation of Duties Policies

You can download SoD policies in `json` format as a backup to edit offline.

- 1 Under **Policy**, select **SoD**.
- 2 Select one or more policies from the list, and click **Actions > Download**.
- 3 Select any options you want to download with each policy, and then click **Download**.
- 4 To import edited policies, see [“Importing Separation of Duties Policies” on page 268](#).

24 Managing Separation of Duties Violations

Identity Governance provides the ability for you to define and activate Separation of Duties (SoD) policies so the system can look for violations of the policies. SoD policies let you identify combinations of permissions and authorizations that no one person should be granted.

When you have active SoD policies, Identity Governance monitors your environment for violations and creates cases when violations are found. SoD administrators and policy owners can either approve the violation for a time period or remove enough access to resolve the violation. When you remove access, Identity Governance creates a **changeset** for fulfillment. For more information, see [“Fulfilling the Changeset for a Review Instance” on page 260](#).

- ♦ [“Understanding SoD Violation versus SoD Case” on page 269](#)
- ♦ [“Listing SoD Violations or SoD Cases” on page 269](#)
- ♦ [“Viewing SoD Case Details” on page 270](#)
- ♦ [“Understanding SoD Case Status” on page 270](#)
- ♦ [“Approving and Resolving an SoD Violation” on page 271](#)
- ♦ [“Closing an SoD Case” on page 272](#)

Understanding SoD Violation versus SoD Case

The terms SoD Violation and SoD Case are sometimes used interchangeably. Both refer to a specific user or account violating a specific SoD policy. However, Identity Governance can detect an SoD violation multiple times because of the variety of events that trigger SoD violation detection. For example, publishing identities and accounts, creating, changing, or deleting roles all trigger SoD violation detection. Identity Governance creates a new SoD violation record for each of those detections and also notifies the SoD Policy Owner of these violations. All represent the same SoD violation, with different detection times.

An SoD case is the entity that tracks all of the information about an SoD violation, including all of the times the violation was detected. It also keeps track of the actions which users have taken with respect to the violation (approve, resolve). An SoD case is closed when Identity Governance no longer detects the violation. In a sense, an SoD case is the history of an SoD violation from the time it is first detected to the time it is no longer detected.

Listing SoD Violations or SoD Cases

There are multiple places where SoD violations may be listed and the associated SoD case managed. Which you use depends on what your needs are.

SoD violations for a particular user or account

1. Under **Catalog**, select **Users** or **Account**.
2. Select the user or account you want to see.

3. Select the **Separation of Duties Policy Violations** tab. Identity Governance only displays this tab for a user or account if there are active violations.

NOTE: This tab shows only the SoD violations whose associated SoD case is currently open.

SoD violations for a particular SoD policy

1. Under **Policy**, select **SoD**.
Ensure that you display the **# Users** and **# Unmapped Accounts** columns.
2. Select the count in the **# Users** column to see the list of users violating the policy.
3. Select the count in the **# Unmapped Accounts** column to see the list of unmapped accounts violating the policy.

NOTE: This tab shows only the SoD violations whose associated SoD case is currently open.

SoD violations for a particular SoD case

1. Under **Policy**, select **Violations**.
2. Filter on SoD case state list by selecting any of the state icons, for example **Total**, **Not Reviewed**, **Approved**. You can also perform advanced searches.

Viewing SoD Case Details

After you have a list of the SoD violations or SoD cases, you can expand them to see the associated SoD case information. The information displayed is:

- ♦ Information about the user or account that is in violation
- ♦ Information about the SoD policy being violated, including the conditions
- ♦ Information about the SoD case including status

You can see the list of actions taken by selecting the count in **# Actions**.

While viewing SoD details, if you have appropriate rights, and the SoD case is still open, you can resolve or approve the violation.

Understanding SoD Case Status

Identity Governance tracks and records all decisions and selections during the life cycle of an SoD case. The following table provides a brief description of the possible status of an SoD case.

SoD Case Status	Description
Not Reviewed	When an SoD violation is first detected, an SoD case is created, and it is put into this state. It indicates that nobody has yet determined what to do about the violation. Users may have looked at it, but they have not determined whether to approve it or whether to request that certain permissions be removed in order to resolve it.

SoD Case Status	Description
Approved	SoD case has been looked at by a user and was approved. Approval means the user determined that the SoD violation could continue for a certain period of time – the control period. There may be one or more compensating controls that were specified. Compensating controls are basically the conditions under which the approval was granted - i.e. it is expected that the compensating controls will be in effect during the approval period.
Approval Expired	SoD case was approved at one time, but the control period has expired.
Resolving	SoD case has been looked at by a user, and the user determined that one or more permissions should be removed in order to resolve the SoD violation. Change requests will have been initiated to remove one or more permissions. The SoD case will be in the resolving state until Identity Governance detects that the permission(s) have actually been removed. The resolving state can also be overridden if a user later on decides to approve the case instead of resolving it.
On Hold - Policy Inactive	SoD case is on hold because the policy has been deactivated.
On Hold - Policy Invalid	SoD case is on hold because the policy has become invalid. A SoD policy would become invalid if any of the permissions or technical roles it specified were deleted from the catalog.
Closed - Policy Deleted	SoD case has been closed because the SoD policy has been deleted. Thus, there is no longer an SoD policy to violate.
Closed - Policy Conditions Changed	SoD case has been closed because the SoD policy's conditions were changed.
Closed - Permissions or Roles Removed	SoD case has been closed because the violating user or account no longer has one or more of the permissions or technical roles that was causing the violation.
Closed - User Deleted	SoD case has been closed because the violating user is no longer found in the catalog.
Closed - Account Deleted	SoD case has been closed because the violating account is no longer found in the catalog.

Approving and Resolving an SoD Violation

Approving an SoD violation records that the violation has been recognized and approval has been given to allow the violation to continue for some time period. A comment is always required when approving a violation. You must also specify a time period (days) that the violation is allowed to

continue. If the SoD policy has defined compensating controls, you can select one or more controls. This allows you to state what controls you want to be enforced while the violation is allowed to continue.

Resolving an SoD violation allows you to specify what permissions or roles you want removed from the user or account. Upon selecting permissions or roles to remove, changesets are generated which then show up in fulfillment. You can visit the fulfillment pages to perform the usual types of fulfillment actions. For more information, see [“Fulfilling the Changeset for a Review Instance” on page 260](#).

IMPORTANT: The closing of an SoD case is not the same thing as the resolve action. It does not occur automatically because a resolve action has been performed. The resolve action simply initiates fulfillment tasks and notifies appropriate users of the need to perform removal actions and what specific removals are being requested. It does not actually remove permissions or roles. It might be that nobody ends up performing the fulfillment tasks, or rejects them and nothing changes, in which case the SoD violation does not go away and the SoD Case remains open.

Closing an SoD Case

Identity Governance automatically closes an SoD case on any of the following conditions:

- ♦ It detects that enough permissions and roles have been removed from the user or account that is in violation so that the SoD violation is no longer detected.
- ♦ Someone deletes the SoD policy. All SoD violations for the SoD policy cease to exist when the policy does not exist.
- ♦ Someone changes the conditions of the SoD policy such that the SoD violation no longer exists.
- ♦ The violating user or account is no longer found in the catalog.

25 Creating and Managing Business Roles

Business roles are roles whose users have common access requirements within your organization. The set of users is defined by each role's membership policy.

- ♦ [“Overview of Roles” on page 273](#)
- ♦ [“Understanding Business Role States” on page 274](#)
- ♦ [“Understanding Business Role Mining” on page 275](#)
- ♦ [“Managing Business Roles” on page 276](#)
- ♦ [“Defining Business Roles” on page 277](#)
- ♦ [“Authorizing User Access Through Business Roles” on page 281](#)
- ♦ [“Adding Authorizations to a Business Role” on page 281](#)
- ♦ [“Adding a Business Role Approval Policy” on page 282](#)
- ♦ [“Publishing or Deactivating Business Roles” on page 283](#)
- ♦ [“Analyzing Business Roles” on page 284](#)
- ♦ [“Editing Business Roles” on page 284](#)
- ♦ [“Approving Business Roles” on page 285](#)
- ♦ [“Downloading and Importing Business Roles and Approval Policies” on page 286](#)
- ♦ [“Automated Access Provisioning and Deprovisioning” on page 287](#)

Overview of Roles

Identity Governance enables you to manage both the technical and business roles in your organization. To enable easier management of these roles, Identity Governance assigns technical role administrators and business role administrators with separate but overlapping responsibilities.

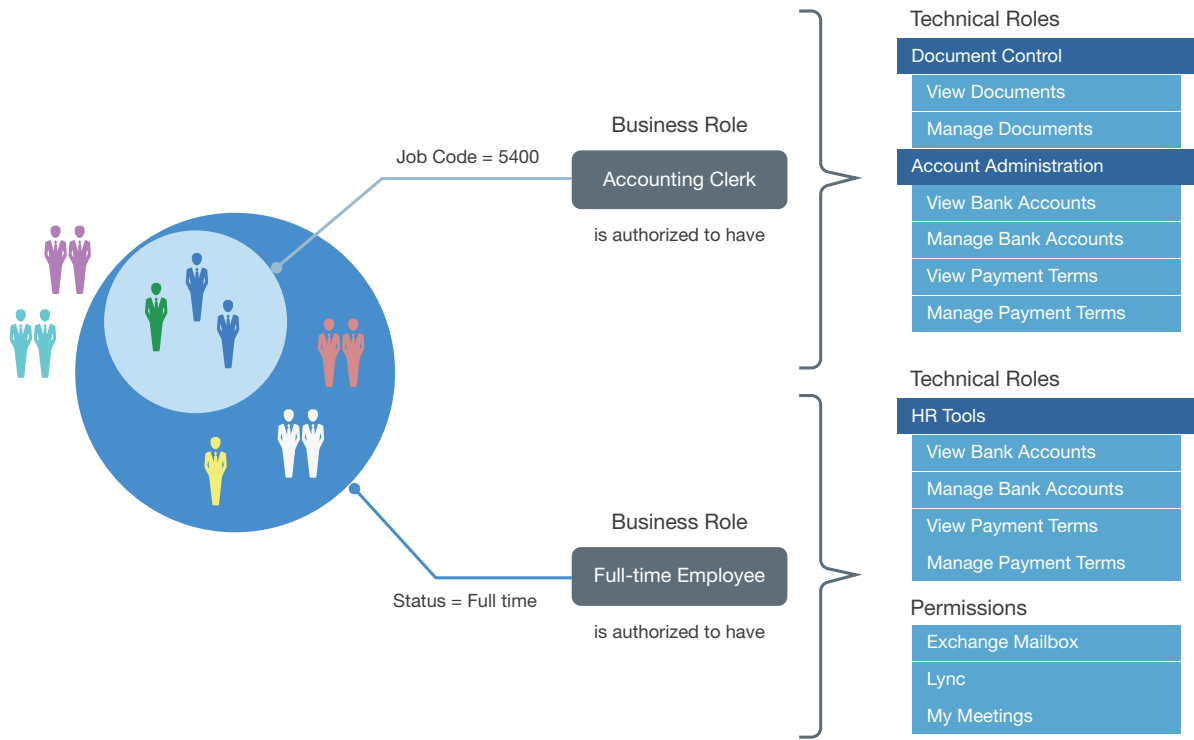
Business roles organize people by their business function and user based attributes to solve questions of what users should have access to because of who they are or what they need or might have an option to request without additional approval.

Technical roles organize lower level permissions into sets of permissions that offer enough business value to be reviewed and assigned as a unit or requested as a unit. Technical roles are designed to limit the number of review items and surface permissions in ways that can be presented to typical non-administrator users.

[Figure 25-1](#) contains an example of how the different types of roles overlap. All full-time employees are authorized to have access to the HR Tools, Exchange Mailboxes, Lync, and My Meeting. Accounting clerks are authorized to have access to Document Control and Account Administration, a technical role that the technical role administrator has created in Identity Governance. When you include a user as a member of a business role of Full-time Employee and Accounting Clerk, Identity Governance authorizes the user to have any of the mandatory or optional technical roles or permissions listed for the given role. Mandatory permissions could potentially be automatically provisioned, while optional permissions could be assigned at a later time without further approval as they have been pre-approved by the policy. This saves you time, effort, and error and enables

controlled access through business roles. To understand how your entitlement assignments confirm to your business policies, you can view the **Role Leverage** widget on the **Overview** page. For more information, see [“Viewing Entitlement Assignments Statistics to Leverage Roles”](#) on page 151.

Figure 25-1 Detailed Example of the Overlap between Business Roles and Technical Roles

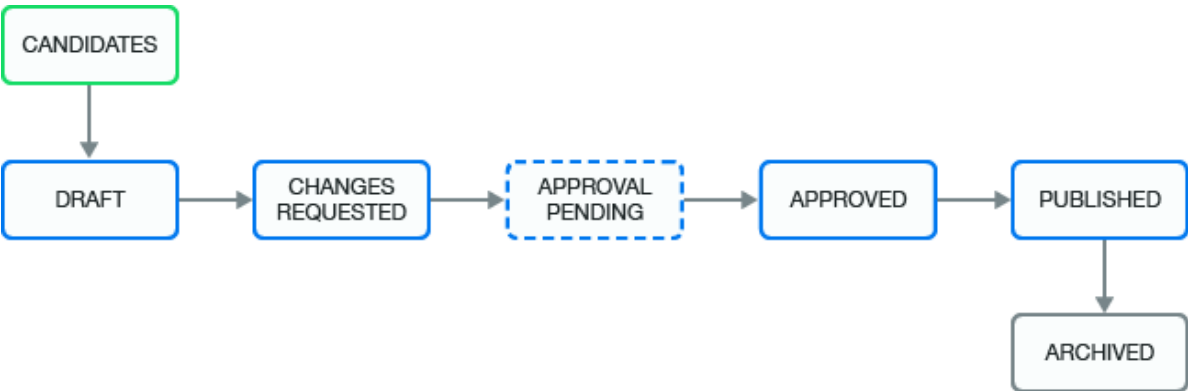


NOTE: This chapter primarily discusses business role policy concepts and procedures. For information about technical roles, see [“Managing Technical Roles”](#) on page 231

Understanding Business Role States

There are several states in the life cycle of a business role after they are created, either manually or mined. From beginning to end, the business role goes through the states in [Figure 25-2 on page 274](#). For detailed description of the states see the following table.

Figure 25-2 Business Role States



Business Role State	Description
CANDIDATES	Business role was created by the mining process and must be promoted before it can be approved or published (depending on the approval policy). This state corresponds to the internal state called MINED.
DRAFT	The assigned approval policy requires approval and changes to the business role have not been submitted for approval.
CHANGES REQUESTED	Approval of a business role was denied. This state corresponds to the internal state called REJECTED.
APPROVAL PENDING	Pending changes are ready for approval by the user specified in the approval policy. This state corresponds to the internal state called PENDING_APPROVAL.
APPROVED	Business role is approved but has not yet been published.
PUBLISHED	Business role is approved and has been published.
ARCHIVED	Policy has been deleted or a new version has been created. It is archived for history and reporting. Archived business roles are never displayed in the application.

Understanding Business Role Mining

Identity Governance uses advanced analytics to mine business data and identify role candidates. This process of discovering and analyzing business data in order to group multiple users and access rights under one business or technical role candidate is called Role Mining or Role Discovery. Global or Business Role administrators can use role mining to reduce complexity in defining roles, and easily select role candidates with authorized users, permissions, technical roles, and applications to create business roles as well as technical roles with common permissions. Identity Governance uses two approaches to business role mining to identify business role candidates.

- ♦ **Directed Role Mining** enables administrators to direct the mining based on user attributes they specify. If administrators are not sure which attribute to select, they can search for recommended attributes, and select an attribute from the recommended bar graph which displays the strength of attributes that have data. Additionally, directed role mining also enables them to specify minimum membership and coverage percentage to identify role candidates. For example, when an administrator selects “Department” as the attribute to group candidates by, the mining results will display list of items consisting of department name with associated users, permissions, roles, and application as role candidates.
- ♦ **Visual Role Mining** enables administrators to select role candidates from a visual representation of the user attributes. The attribute circle’s width displays the recommendation strength, and the width and darkness of the lines indicate the affinity of the attribute to other user attributes. Administrations can customize the mining results by modifying the default maximum number of results, minimum potential members, and number of automatic recommendations.

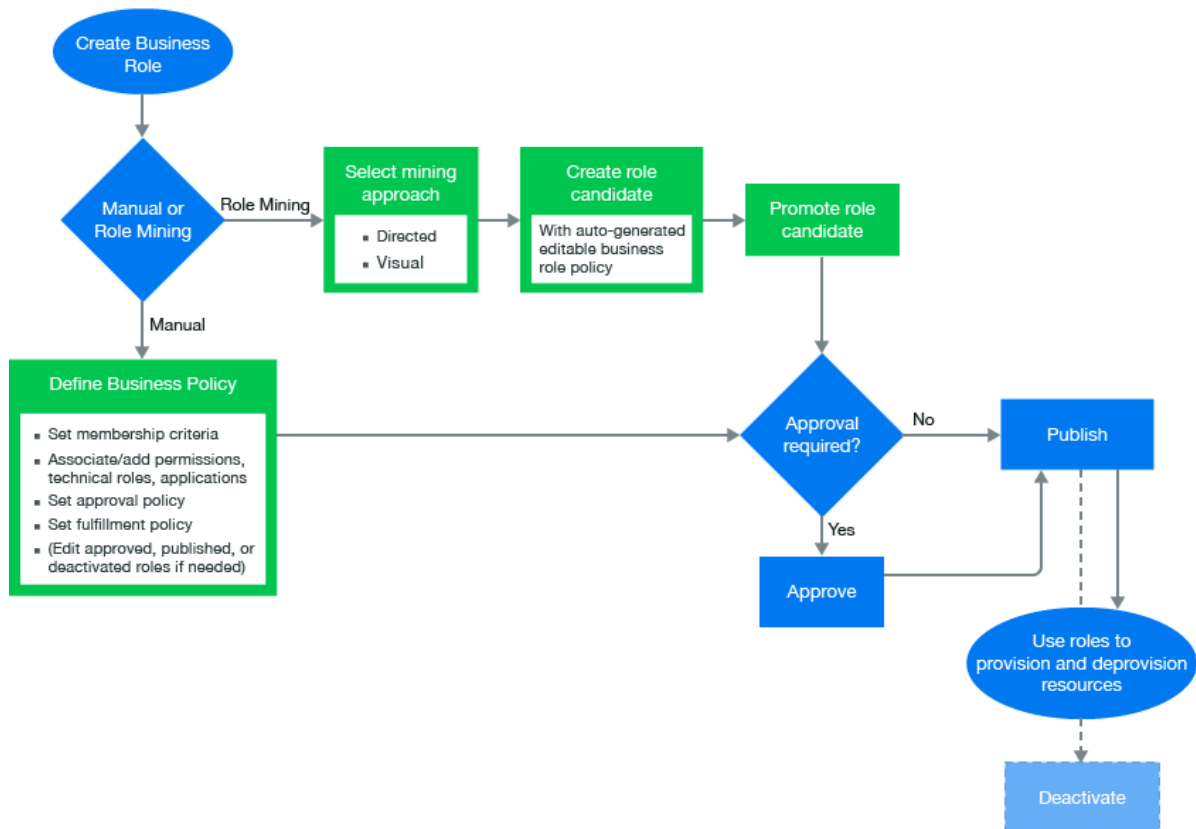
NOTE: Role recommendations are dependent on your data and role mining settings. To optimize search results, administrators can modify default role mining settings in **Administration > Analytics and Role Mining Settings**. For more information see, “[Configuring Analytics and Role Mining Settings](#)” on page 148.

After previewing users and their associated permissions, technical roles, and applications, administrators can select one or more items from the list to either create role candidates for each selected item in the list or a single candidate for all of them. Additionally, common permissions can be grouped under a technical role, and technical role candidate could be generated for each application.

NOTE: Mined business or technical roles are created in a candidate state. Administrators can edit and save role candidates, but candidates must be promoted before they can be approved or published as a role. Administrators can also select multiple role candidates and submit for approval, publish or delete using **Actions** options.

Managing Business Roles

Figure 25-3 Business Role Workflow



Business Role Management is the process of creating, modifying, and defining business roles and managing business role policy.

The primary purpose of business roles is to specify a set of applications, roles, and permissions that each member of a business role is authorized to access. The set of authorized resources is defined by each business role's authorization policy. You add a business role authorization policy when you create or edit the business role.

A business role administrator performs all administrative functions for all business roles. A business role administrator can delegate administrative privileges. For more information, see [“Runtime Authorizations” on page 181](#).

Defining Business Roles

In order to use business roles, you must create a business role and define a membership policy and an authorization policy for the business role based on your business needs. You can create a business role either manually or use role mining analytics.

To define a business role:

- 1 Log in to Identity Governance as a Business Role or Global Administrator.
- 2 Under **Policy**, select **Business Roles**.
- 3 Select the **Mining** tab if you want the system to recommend role candidates and based on your selection auto-create membership expression and authorize associated permissions, technical roles, and applications.

NOTE: If you are confident about your data and want to define membership expression manually, select **+** on the **Business Roles** page to create a new business role and then proceed to Step 12.

If	Then
You are not sure about where to start	<ul style="list-style-type: none">♦ Select Visual Role Mining.♦ (Optionally) Click Settings gear icon to modify the maximum number of results to display for each recommended attributes, and the required minimum number of members for each role candidate.♦ Click on attribute node/circle to select a role candidate. <p>WARNING: You might not see any recommendations if the Settings > Minimum potential members is set too high or when the role mining settings in Administration > Analytics and Role Mining Settings does not meet the required conditions. For more information see, “Configuring Analytics and Role Mining Settings” on page 148.</p>

If	Then
You want to direct the mining by specifying user attribute	<ul style="list-style-type: none"> ♦ Select Directed Role Mining. ♦ Specify user attributes by entering user attribute names or by clicking search and selecting attributes based on the strength of the recommendation. ♦ Specify minimum number of times the attribute value must occur across users, or the percentage of all users who must have the attribute value. ♦ Specify additional coverage criteria. <p>NOTE: The permission, technical role and application coverage fields are used to determine which authorizations are auto-populated in the business role candidate. For example, if permission coverage is at 50% then 50% of the members must hold a permission for it to be added as an authorization in the candidate. If it is 100% then all members must hold the permission for it to be added.</p> ♦ Save the specified values to trigger user catalog analysis. ♦ (Optional) Click Settings gear icon to adjust the settings, and save to refresh the candidate suggestions.
<ol style="list-style-type: none"> Select one or more items from the Directed Role Mining > Mining Results list or Visual Role Mining > Role Candidates list. Click Create Candidates. Create separate candidates for each criteria or Create a single business role candidate. If the latter, enter Name. (Optional) Select Create associated technical for common permissions to generate technical roles with users who have the same permissions. (Optional) Select Group permissions added to technical roles by application to create application-specific technical roles. Click Role tab and click on the newly generated inactive role to view role description. Click Edit. 	
<p>NOTE: Role candidates are created in pending state and must be promoted before they can be approved or published.</p>	
<ol style="list-style-type: none"> Select Yes to promote the role candidate. Specify the following information to create the business role: <p>Name and Description</p> <p>Modify the auto-generated name to a unique name and edit description for the business role.</p> <p>Grace period</p> <p>Specify a grace period. A grace period specifies the number of days a user is still considered to be a member of the role when it is detected that they no longer meet the membership policy requirements.</p> 	

Risk

Specify the importance of the business role in terms of limited access and security.

For example, you might want to review access to business roles with a **high** risk more often than business roles with a **mild** risk.

Included Membership

Optionally, specify roles whose membership criteria, users and groups you want to include in the new business role. When combining the included roles, only published roles membership will be included and duplicates will be eliminated. For example, you can include role A and role B in the membership of role C. Role C will then be the union of role A and role B along with any membership criteria specified for role C.

NOTE: Excluded members of the including role take precedence over inclusion of included business role members. For example, When role C includes A, and A has a member User1, but User1 is excluded by role C the user will be excluded.

Membership expressions

Membership expressions are criteria which specify a set of users that are considered members of the business role and are auto-generated when you mine for roles. Each expression can have an authorization period for when it is valid. Optionally, add one or more expressions to search for users.

Include and Exclude Users and Groups

Optionally, define specific users and groups that you want to include in the business role that might not match any membership expression. You can also specify users and groups to exclude from the business role who would otherwise match membership expressions. For example, you can have a membership expression that matches all managers in engineering, but you do not want John Smith or managers in the CTO group even if they match that criteria. You can also define a time period for when these inclusions or exclusions are valid.

NOTE: Excluding a user or group takes precedence over including them. For example, suppose the Sales group is included and the Contractors group is excluded. A user who belongs to both of those groups would be excluded from the business role, because exclusion takes precedence over inclusion.

- 13 Select the **Authorizations** tab, then define the following:

Permissions

Permissions may be preauthorized when you mine for roles or you may need to define them. Select permissions from the entire catalog or from a list of permissions held by the business role members. Specify whether the permission is mandatory or not. Specify whether the permission should be automatically granted and/or revoked, or manually fulfilled. If needed, click on the calendar control to set an authorization period for when these permissions are authorized for users in the business role.

Technical Role

Technical roles may be preauthorized when you mine for roles or you may need to define them. The technical role acts as a grouping for the permissions. If all of the appropriate permissions are included in a technical role, you can add the technical role instead of the individual permissions. If needed, select technical roles from the entire catalog or from a list of technical roles held by the business role members. Determine whether the technical role is mandatory or not. Specify whether the technical role authorization should be

automatically granted and/or revoked, or manually fulfilled. If needed, click on the calendar control to set an authorization period for when the permissions in the technical role are valid for the business role.

Applications

Applications may be preauthorized when you mine for roles or you may need to define them. If needed, define which applications the members of the business role are authorized to hold. This means accounts can be created for the members of the business role in the listed applications. Select applications from the entire catalog or from a list of applications held by the business role members. Specify whether the application authorization should be automatically granted and/or revoked, or manually fulfilled. If needed, click on the calendar control to set an authorization period for when the members of the business role have access to the application using the calendar control.

NOTE: Auto-grant and auto-revoke requests will be automatically fulfilled if automatic fulfillment has been enabled in the **Owners and Administration** tab and when fulfillment targets have been configured. For information about automatic fulfillment, visit [“Automatically Fulfilling the Changeset” on page 261](#).

For more information about authorizing permissions, technical roles, and applications, see [“Adding Authorizations to a Business Role” on page 281](#).

- 14** Select the **Owners and Administration** tab to assign the following:

- ◆ Role owner
- ◆ Role manager
- ◆ Fulfiller
- ◆ Categories
- ◆ Approval Policy
- ◆ Automatic Fulfillment
- ◆ Auto revoke period

Identity Governance makes default assignments for the owner, fulfiller, and assigns a default approval policy to the business role if you do not make selections on this tab.

Select whether you want this role to be automatically fulfilled. When selected, Identity Governance automatically sends fulfillment requests to provision and revoke mandatory resources for users.

Set the number of days to wait after a user loses authorization for a resource before revoking the access.

- 15** (Optional) On the **Membership** tab, select **View Membership** to view list of business role members.

NOTE: During migration or upgrades, you must always run publication to refresh list of business role members. For more information about publishing data sources, see [Chapter 18, “Publishing the Collected Data,” on page 221](#).

- 16** Under **What-if Scenarios**, select **Estimate Publish Impact** and **Analyze SoD Violations** to respectively view types of changes and SoD violations information.
- 17** (Conditional) Resolve SoD violations or edit business role definition to resolve issues if any. For more information about SoD violations, see [“Approving and Resolving an SoD Violation” on page 271](#).
- 18** Select **Save** to save your modifications to the mined business role definition.

NOTE: When editing an existing business role, the **Owners and Administration** tab has a separate **Save** button, which allows you to change these items independent of other items pertaining to the business role.

After you have created the business role and assigned owners and administrators, the business role is ready for approval or it is ready to be published depending on your approval policy. The approval policy allows you to have people review the business role and approve or request changes to the business role. For more information, see [“Adding a Business Role Approval Policy” on page 282](#).

To have the business role used in reviews or used in the catalog to detect users that meet the business role criteria, you must publish the business role. For more information, see [“Publishing or Deactivating Business Roles” on page 283](#).

Authorizing User Access Through Business Roles

Membership policy determines which users are members of a business role. Membership policy can include membership expressions, user or group inclusion lists, and user or group exclusion lists. Regardless of whether a user is a member of role by virtue of matching a membership expression or because they are explicitly included, they are authorized resources of a business role for as long as they are a member of the business role.

Adding Authorizations to a Business Role

A business role authorization policy defines the permissions, technical roles, and applications authorized by the business role. Users are not automatically assigned the permissions of a business role, nor are business role permissions removed if users no longer meet the criteria for a business role. The business role authorization policy defines whether the user is authorized the access.

A business role can authorize technical roles. That means that users and groups that you add to the business role are authorized all of the permissions included in each technical role. For more information, see [“Managing Technical Roles” on page 231](#).

You add an authorization policy to the business role on the **Authorizations** tab when you create or edit the business role.

There are many different components to an authorization policy. The following information explains the different components.

Authorized Permissions

A user in the business role can be authorized to have all the permissions included in the authorization policy.

Authorized Technical Roles

A user in the business role can be authorized for technical roles included in the authorization policy.

Authorized Applications

A user in the business role can be authorized to have an account in all of the applications included in the authorization policy.

Mandatory and Optional Entitlements

Mandatory entitlements include permissions, technical roles, and applications which a user is expected to have if they are assigned the business role. Optional entitlements are permissions, technical roles, or applications which a user is allowed to have but are not required to have.

Automatic Fulfillment Settings

If you selected **Automatic Fulfillment** on the **Owners and Administration** tab, you can select whether to automatically grant and revoke each permission, technical role, and application. Applications must have an account collector to allow you to specify automatic grant or revoke.

Authorization Period

A user in the business role can be authorized for a set period of time defined in the authorization policy. Typically you may need to set authorization period only during transitions like mergers or changes related to compliance. Avoid setting authorization period for business roles to change specific role authorization, as it can be more efficiently handled using periodic business role membership reviews.

Adding a Business Role Approval Policy

The approval policy for the business role governs all business role life cycle events. Identity Governance contains a default approval policy that is assigned to each business role that you create.

The approval policy for the business role specifies all approval requirements for each business role defined, including whether approval is required when creating or modifying that business role.

Micro Focus recommends that your organization's default policy require approval. A default policy that doesn't require approval could result in roles being approved automatically when they are created. When your policy requires approval, you can submit each role for approval or select multiple draft roles and then select **Actions > Submit for Approval** to submit multiple roles for approval.

The default business role approval policy, which does not require approval, is applied to all business roles that you create. To change this you would have to change the default approval policy to require approval by owners or specify a list of approvers.

Two additional policies are provided for your convenience. One requires approval by the business owner (recommended) and another one that does not require approval. A global administrator or business role administrator can change or delete these sample policies.

You can create additional approval policies and apply them to existing business roles after you have created a business role. To change the business role default approval policy, select **Default approval policy** on the **Approval Policies** tab.

To create a new approval policy:

- 1 Log in to Identity Governance as a Business Role or Global Administrator.
- 2 Under **Policy**, select **Business Roles**.
- 3 Select the **Approval Policies** tab.
- 4 Select **Add approval policy (+)**.
- 5 Specify a name and description for the approval policy, then determine whether it is required or not.
- 6 Select **Save** to save the policy.

You can change the approval policy for a group of business roles at one time by using the bulk action on the business role list. You can also download business role approval policies as `json` files using the bulk action menu. After editing, you can import the policies on the page that lists all approval policies.

Publishing or Deactivating Business Roles

Two possible versions of a business role can exist:

- ♦ **Published:** Before you can publish a business role, it must go through the approval process and be approved, if it requires approval. A published business role is available for governance process and in the general catalog.
- ♦ **Deactivated:** You can edit published, approved, and deactivated roles. When you edit a published business role, Identity Governance creates a draft of the business role that appears in the **Draft** tab that you can send for approval if required, publish, or discard. However, deactivated roles are not available for the governance process or in the general catalog.

The edit and approve cycle is a single cycle that is independent of the publication cycle. When you edit the published business role, Identity Governance creates a draft version of the business role.

The approval cycle is not independent of the draft. If no approval is required the draft is automatically approved but not published. If the draft is then published, it replaces the currently published version.

When the business role administrator deactivates a published role, three things can occur:

1. If there is an approved draft, Identity Governance archives the active version and the approved draft replaces it.
2. If there is not an approved draft when the published role is deactivated, Identity Governance prompts the administrator to keep the published version or the unapproved draft version of the business role.
3. If there is no draft, Identity Governance moves the published business role to the approval state.

When a business role is deactivated, the role cannot take part in the review process. The role must be published to be part of the review process. For more information, see [“Understanding the Review Process” on page 20](#).

To Publish or Deactivate a business role:

- 1 Log in to Identity Governance as a Business Role or Global Administrator.
- 2 Under **Policy**, select **Business Roles**.
- 3 Select the business role to change, then select **Edit**.
- 4 If you have one version of the business role, select **Publish** or **Deactivate** the business role.

NOTE: Deactivating disables the role from being a part of the review process but does not automatically revoke all permissions. Permissions are only revoked if an user is no longer a member of the business role.

or

If you have multiple versions of the business role, select the **Draft** or **Published** tab, then select **Publish** or **Deactivate**.

NOTE: You must have two versions of the business role to have the Draft and **Publish** tabs appear.

If you have a number of business roles that need to be published, Identity Governance provides a way to publish all of the roles at the same time. On the Business Roles page, select the business roles to publish, then select **Actions** > **Publish**.

Analyzing Business Roles

Identity Governance allows you to improve role quality and effectiveness by providing you with various analytical tools. To maintain an effective role model, it's important that organizations are able to understand the quality of the roles that have been implemented. For example, a business role might be created that has all or almost all of the members as another role or a Technical Role might have the same permissions as another role. This might indicate that these roles are redundant and aren't actually needed. Using role analysis, you can analyze selected business roles, all business roles, or membership expression to existing roles to find:

- ♦ similarity in memberships and authorizations
- ♦ effectiveness of the selected business roles based on percentage of users that hold the role authorizations
- ♦ members and authorizations in common
- ♦ members without mandatory authorizations
- ♦ members without auto-grant authorizations

To analyze business roles:

- 1 Log in to Identity Governance as a Business Role or Global Administrator.
- 2 Under **Policy**, select **Business Roles**.
- 3 Select **Analysis** tab.
- 4 Select an **Analyze** option and configure related parameters. For example, when selecting similarity analysis, you can modify the default similarity threshold. If you specify 60%, then the results will display business roles that have 60% of similarity for any authorization or membership.

NOTE: **Business role similarity** and **Common authorizations** analysis can be performed on published or unpublished business roles, while **Authorization effectiveness**, **Mandatory authorizations**, and **Auto-grant authorization** analysis are only performed on published business roles. If there are unpublished business roles in the list selected for **Authorization effectiveness**, **Mandatory authorization**, and **Auto-grant authorization** analysis they will be highlighted, and skipped during analysis.

- 5 Select **Start Analysis**.
- 6 Click on the links in the analysis results for additional information such as comparison tables of memberships and authorizations in **Business role similarity** analysis, and list of members in **Mandatory authorization**.
- 7 (Optional) Select **Download as CSV** to download the results as a csv file for further analysis.

Editing Business Roles

Identity Governance allows you to edit business roles. If you edit a business role that has been approved, it is changed to a draft when you save your edits and then it must be re-approved. To edit a published business role, a new draft copy is made for editing so that the published role continues to

be used in governance processes until the new draft is approved and published. You can also download business roles as `json` files using the bulk action menu. After editing, you can import the roles on the page that lists all business roles.

Editing a business role:

- 1 Log in to Identity Governance as a Business Role or Global Administrator.
- 2 Under **Policy**, select **Business Roles**.
- 3 Select the business role you want to edit, then select **Edit**.
- 4 (Conditional) If the business role is published, on the top of the page, select **Edit**.
Identity Governance creates a draft of the business role for you to edit in the **Draft** tab.
- 5 Make the appropriate changes to the business role.
You can change the name, description, grace period, risk level, memberships, authorizations, owners and administrators of the business role.
- 6 Select **Save** to save the draft.
- 7 (Conditional) Select **Compare with published** to compare the draft version with the published version of the business role to ensure the changes are correct.
- 8 If the business role approval policy requires approval, when the draft is ready for approval select **Submit for approval**. If the business role approval policy does not require approval, the draft is automatically approved whenever you save your edits.
- 9 After you approve a draft, select **Publish** to publish it.

When deleting a business role that has been published, the business role is archived for reporting and auditing purposes.

Approving Business Roles

Identity Governance provides an approval process for users, groups, or business role owners to approve the business roles they have been assigned to approve. The business role owner can approve the business role if the role's approval policy specifies **Business role owners**. However, you can specify a list of users or members of a group to be approvers of the business role.

To approve a business role that is pending:

- 1 Log in to Identity Governance as a user assigned to approve the business role.
- 2 Under **Policy**, select **Business Roles**.
- 3 Select the **Pending Your Approval** tab.
- 4 Select on any of the pending approvals, then read and review the content of the business role.
- 5 Enter a comment in the **Comment** field as to whether you approve the business role or if you want changes to the business role.
- 6 Select **Approve** to approve the role.

or

Select **Request changes** if you desire changes to be made.

When you select the **Request changes** option, the creator of the business role receives notification of the change request. After you change the business role, the approval workflow process starts again.

Downloading and Importing Business Roles and Approval Policies

You can download business roles and approval policies as `json` files and import them later into another environment.

To download or import business roles:

- 1 Log in to Identity Governance as a Business Role or Global Administrator.
- 2 Under **Policy**, select **Business Roles**.
- 3 Select a role or all the roles on the **Roles** tab.
- 4 Select **Actions > Download**.
 - 4a (Optional) Include references to business role owners, managers, and fulfillers; and download included business roles, associated applications, technical roles, and assigned categories and approval policies.
 - 4b Select **Download**.
- 5 If you make changes, or want to want to import previously downloaded business roles into another environment, select **Import Business Roles** on the **Roles** tab.
- 6 Navigate to the business roles `json` file, select the file to import, and click **Open**.
- 7 Identity Governance detects whether you are importing new or updated roles and whether the updates would create any conflicts or have unresolved references.
- 8 Select how to continue based on what information is displayed.

NOTE: You must publish the imported role for Identity Governance to recognize the users that hold the permissions as members of a business role. For more information, see [“Publishing or Deactivating Business Roles” on page 283](#).

To download or import business role approval policies:

- 1 Log in to Identity Governance as a Business Role or Global Administrator.
- 2 Under **Policy**, select **Business Roles**.
- 3 Select a policy or all the policies on the **Approval Policies** tab.
- 4 Select **Actions > Download**.
 - 4a (Optional) Include references to approval policy approver.
 - 4b Select **Download**.
- 5 If you make changes, or want to want to import previously downloaded approval policies into another environment, select **Import Approval Policies** on the **Approval Policies** tab.
- 6 Navigate to the approval policy `json` file, select the file to import, and click **Open**.
- 7 Identity Governance detects whether you are importing new or updated policies and whether the updates would create any conflicts or have unresolved references.
- 8 Select how to continue based on what information is displayed.

Automated Access Provisioning and Deprovisioning

You can set up business roles to automatically request provisioning and deprovisioning of authorized resources for users in the business role. The business role must allow automatic fulfillment on the **Owners and Administration** tab. For more information, see [“Defining Business Roles” on page 277](#). In addition, you must configure individual authorized resources to allow automatic granting or revoking of the resource.

Automatic Provisioning Requests

Identity Governance evaluates whether the system needs to request automatic provisioning of an authorized resource when any of the following events occur:

- ♦ A user has become a member of a business role.
- ♦ A business role is modified to authorize a resource and republished.
- ♦ A business role resource enters its validity period.

Identity Governance detects changes in business role membership when you publish identities, applications, and business roles. In addition, it periodically runs a task to check if authorized resources have entered their validity period.

When Identity Governance determines that a user has become authorized to have a resource for any of the above reasons, it issues a provisioning request for the user + resource if:

- ♦ The resource authorization specifies automatic granting.
- ♦ The user does not already have the resource.

NOTE: For applications, this means that the user does not currently have an account in the application.

- ♦ There is no pending automatic change request for the resource to be granted to the user.

NOTE: A change request is considered pending until it is verified or fails verification for some reason.

Automatic Deprovisioning Requests

Identity Governance evaluates whether the system needs to request automatic deprovisioning of a resource when any of the following events occur:

- ♦ A user is no longer a member of a business role.
- ♦ A business role is modified to no longer authorize a resource and is republished.
- ♦ A business role is deactivated.
- ♦ A business role is deleted.
- ♦ A business role resource authorization exits its validity period.

Identity Governance detects changes in business role membership when you publish identities, applications, and business roles. It also periodically runs a task to check if authorized resources have exited their validity period.

The decision whether to issue a deprovisioning request deliberately has more controls than the decision whether to issue a provisioning request. The extra level of control is intended to prevent mistakes that could lead to accidental and unintended deprovisioning of critical resources for users. When the system detects that a business role no longer authorizes a resource for a particular user for any of the above reasons, it will do the following to determine if it should issue a deprovisioning request for the user + resource:

- ♦ Determine if the user currently has the resource. If not, a deprovisioning request is not needed. For applications, a user has the resource if they have an account in the application.
- ♦ Determine if there is a pending automatic deprovisioning request for the user + resource. If so, no new deprovisioning request will be issued. A change request is considered pending until it is verified or fails verification for some reason.
- ♦ Determine if any other business roles currently authorize the resource for the user. If so, no deprovisioning request will be issued. Identity Governance does not issue automatic deprovisioning requests until the user has lost ALL of its authorizations for a resource. Other business roles might authorize the resource for various other users, but if none of the business roles authorize the resource for the user in question, they are not considered.

When Identity Governance determines that the user has lost its last authorization for a resource, it creates a list of business roles to consult to determine if a deprovisioning request should be issued. The system adds a business role to this list if it meets ALL of the following conditions:

- ♦ Must have authorized the resource for the user at one time. There may be business roles that currently authorize or have previously authorized the resource for other users, but if they have never authorized it for the specific user in question, they are not relevant here.
- ♦ Must have authorized the resource for the user in the not too distant past. If the user lost its authorization for the resource from a business role too long ago, we don't want to consider the business role. The auto revoke period that might be specified for the business role defines what period of time is too long ago. For more information, see [“Defining Business Roles” on page 277](#). The auto revoke period is defined on the **Owners and Administration** tab.
- ♦ Must be currently published, not deactivated or deleted. Deactivated or deleted business roles are not relevant here.
- ♦ Must have a current authorization for the resource in question. Business roles that authorized the resource in the past but no longer authorize it are not relevant here.
- ♦ Resource must be in the validity period specified by that authorization. Business roles that may have authorized the resource in the past but no longer do are not relevant here.

To issue a deprovisioning request, one or more business roles that meet ALL of these conditions must exist, and they must ALL currently specify automatic revoking for the resource in question. Otherwise, no deprovisioning request will be issued.

26 Calculating and Customizing Risk

Identity Governance allows custom definition of risk based on your policies and risk tolerance. Customized risk ranges and levels allow Identity Governance to calculate risk scores for your organization, users, applications, business roles, and permissions. Use risk scores to focus reviews and measure impact. Risk scoring supports better context for decision-makers who conduct reviews prioritized by risk scoring based on attribute value, group membership, management relationship, application, permission, cost, risk, and other criteria. For more information about conducting reviews based on risk, see [Chapter 21, “Creating and Modifying Review Definitions,” on page 247](#).

- ♦ [“Understanding Risk Levels and Risk Scoring” on page 289](#)
- ♦ [“Configuring Risk Levels” on page 294](#)
- ♦ [“Configuring Risk Scores” on page 294](#)
- ♦ [“Setting and Viewing Risk Calculation Schedules and Status” on page 295](#)
- ♦ [“Viewing Calculated Risk Scores” on page 295](#)

Understanding Risk Levels and Risk Scoring

Identity Governance provides **risk levels** to help you classify and label risk factors that matter to your organization. You can configure the number of levels, size of levels, and names of levels to make them appropriate for your organization and stakeholders. **Risk scoring** provides a means for manually setting or calculating risk for the entire organization as well as for catalog objects and policies.

Identity Governance administrators can customize the following risk policies:

- ♦ Risk level configuration
- ♦ Governance risk score
- ♦ Application risk score
- ♦ User risk score
- ♦ Risk score schedule

Users with the following authorizations can manage and customize risk settings for your Identity Governance environment:

- ♦ Global Administrator
- ♦ Data Administrator
- ♦ Auditor (read only)

See the following sections for more details about how Identity Governance helps you manage risk in your environment:

- ♦ [“Risk Levels” on page 290](#)
- ♦ [“Risk Scoring” on page 290](#)
- ♦ [“Risk Factors” on page 290](#)

- ♦ [“Risk Score Calculation Details” on page 292](#)
- ♦ [“Visualizing Risk” on page 293](#)

Risk Levels

Identity Governance gives you the flexibility to create a risk scale of your own choosing. If your environment requires a high level of granularity, you can specify up to 10 risk levels. When you set the risk level size, Identity Governance automatically divides the risk levels in even increments and sets the maximum risk value for calculated values to the maximum value specified in your settings. You can further customize the risk levels by providing your own naming system to the levels. A color-code is assigned to each level ranging from blue at the low end to red at the high end.

Risk Scoring

A risk score quantifies the level of risk that an entity, such as a user or account, exposes an organization to. A higher risk score indicates that you have identified that item as riskier to your organization. You can **manually set** risk scores by collecting risk score attributes along with objects you collect or by using Identity Governance to assign risk scores to individual objects.

You can collect risk scores or assign risk scores to the following items:

- ♦ Users
- ♦ Accounts
- ♦ Applications
- ♦ Permissions
- ♦ Technical roles
- ♦ Separation of duties policies
- ♦ Business roles
- ♦ Certification policies

A **calculated** risk score is based on risk factors and the relative weighting of those factors that you define. You can configure Identity Governance to calculate the following risk scores, either on demand or on a regular schedule:

Governance (your overall system score)

Represents the current level of risk related to access and security that your organization is exposed to based on the risk factors and risk weights you have defined.

Application

Represents the current level of risk related to access and security of each application that your organization is exposed to based on the risk factors and risk weights you have defined.

User

Represents the current level of risk related to access and security for each user that your organization is exposed to based on the risk factors and risk weights you have defined.

Risk Factors

Risk factors, metrics that affect a risk score, apply to specific items and can have a positive or negative impact on the item's risk score. The weight of a risk factor is the percentage of an item's risk that the factor comprises. The maximum value for any risk factor component is the maximum risk

score for the item multiplied by the percentage weight of the factor. For example, an organization specifies that user risk score has a maximum value of 1000 and 3 risk factors of equal weight. Each risk factor can only account for one third of the user's risk score.

For some risk factors, Identity Governance uses either the average value or the maximum value for that factor, based on which one you select. Other risk factors use a range of values that you set. When you assign a weight to a risk factor, such as **Number of unmapped accounts**, Identity Governance then looks at the range you have specified. If the value of the risk factor is at or above the high range, Identity Governance applies the full weight for that risk factor to the risk score. If the value is below the high range, Identity Governance applies a percentage of the weight that is appropriate to the percentage of the high range for the value. If a risk factor value is at or below the low range, that factor does not add anything to the risk score.

You can use the following risk factors to control how Identity Governance calculates risk scores in your environment.

Governance Risk Factors	Risk Factor Type
User risk scores	Average or Max
Application risk scores	Average or Max
Account risk scores	Average or Max
Business role risk scores	Average or Max
Technical role risk scores	Average or Max
Permission risk scores	Average or Max
Number of unmapped accounts	Low to high range
Number of unauthorized assignment (permission and technical role)	Low to high range
Number of outstanding SOD violations	Low to high range
Number of expired certification violations	Low to high range
Total number of certification violations	Low to high range
Number of no decision certification violations	Low to high range
Application Risk Factors	Risk Factor Type
Risk of assigned permissions in application	Average or Max
Risk of accounts in application	Average or Max
Number of unmapped accounts	Low to high range
Number of permissions in the application	Low to high range
Number of exceptions (access not authorized by policy)	Low to high range
Number of expired certification violations	Low to high range
Total number of certification violations	Low to high range
Number of no decision certification violations	Low to high range

User Risk Factors	Risk Factor Type
Risk of permissions assigned to user	Average or Max
Risk of accounts assigned to user	Average or Max
Number of outstanding SOD violations	Low to high range
Number of exceptions (access not authorized by policy)	Low to high range
Number of permissions assigned to the user	Low to high range
Number of business roles the user is in	Low to high range
Collected user risk score attribute	Value
Number of expired certification violations	Low to high range
Total number of certification violations	Low to high range
Number of no decision certification violations	Low to high range
Days past expired certification	Impact

Risk Score Calculation Details

Identity Governance performs separate calculations to determine an overall governance risk score and overall risk scores for each application and user. The calculations use the following variables:

- ♦ **RFV**: raw risk factor value
- ♦ **LL**: lower boundary
- ♦ **UL**: upper boundary
- ♦ **URL**: upper risk level value from risk level configuration
- ♦ **FW**: factor weight as a percentage
- ♦ **RRFV**: ranged risk factor value
- ♦ **FRS**: factor risk score
- ♦ **RS**: overall entity risk score

Risk based factor score

$$FRS = RFV * FW/100$$

Count based factor score

$$RRFV = (RFV - LL) > 0 ? ((RFV - UL) >= 0 ? URL : ((RFV * URL / (UL - LL))) : 0$$

$$FRS = RRFV * FW/100$$

Overall entity risk score

$$RS = \text{SUM } FRS[0-N]$$

Keep in mind the following notes about raw score values:

- ♦ For **average or max risk factor types**, the raw score will be set to either the average or maximum value of all values for a specific calculation. For example, if the administrator has configured that the risk of permissions assigned to users be averaged, Identity Governance averages the permission risk values for each user in the catalog and reports this number as the raw score.
- ♦ For **low to high range risk factor types**, the raw score will be the value for a specific measure. For example, for the **Number of outstanding SOD violations** risk factor, the base score will be equal to the total number of outstanding SoD violations.
- ♦ For **value risk factor types**, the raw score will be set to a value. For **Collected user risk score attribute** factor it will be set to the value of the user attribute configured in the risk factor. For the **Risk** attribute it will be set to the collected risk value. For any other attribute, it will be set to the collected or curated value at calculation time.
- ♦ For **impact risk factor types**, the raw score will be set to a number of days.

Keep in mind the following notes about ranged scores:

- ♦ For **low to high range risk factor types**, the ranged score will depend on upper and low boundaries configured for a factor. The upper boundary is the value at which risk is maximal. Risk level has a boundary and factors have a boundary.

The calculation compares the value to the upper bound to scale it. If the value is at or above the bound, it will apply the full weight to the target raw risk score. If the value is below the upper bound, it will determine the percentage of the upper bound (max risk) that the raw score represents and use that to determine the range to apply.

The lower bound indicates that this factor is below threshold and should not have any effect on the risk score.

- ♦ For **impact risk factor types**, the raw score will be evaluated against the configured interval and proper impact will be determined.

Visualizing Risk

Identity Governance provides several ways you can visualize the risk factors in your environment. In most areas, you can also drill down to details that show you more context for how Identity Governance has assessed the risk.

- ♦ As a separate tab on **User** and **Application** details pages
- ♦ As a governance risk score, and trend graph if multiple scores exist, displayed on the **Overview** page
- ♦ As a governance risk score and context information on the **Risk** policy administration page

Identity Governance assigns a color code to each risk level ranging from blue at the low end to red at the high end. These colors display with risk scores to help you further understand how the score fits into your customized risk level ranges.

Configuring Risk Levels

Identity Governance provides five risk levels in 20-point increments by default. You can set risk values for most objects in the catalog and for separation of duties policies and business roles. Identity Governance lets you customize the number, size, and name of each risk level. For example, if you set four risk levels with a size of 25, Identity Governance creates four equally sized risk levels of 0-25, 26-50, 51-75, and 76-100.

- 1 Log in as a Global or Data Administrator.
- 2 Under **Policy**, select **Risk**.
- 3 Expand **Risk Level Configuration**.
- 4 Specify the number of risk levels and the size for each level.
- 5 (Optional) Select a risk level label, such as **Low** or **High**, and type the desired value to customize the label.

When you set risk values on objects and policies, Identity Governance displays these risk level names so you can easily see whether an object has a risk score associated with it and the risk level label as defined in your environment.

Configuring Risk Scores

You can customize the way Identity Governance summarizes the risk in your environment, either through manual or calculated risk scores. Governance risk score measures risk across your entire system, application risk score measures risk for each application, and user risk score measures the risk for each user. You can assign risk scores manually by editing values in the catalog, either individually or through bulk data updates. If you edit extended attribute risk values that had been collected, Identity Governance uses the edited values for extended attributes for risk calculation instead of the collected values. For more information, see [“Editing Attribute Values on Objects in the Catalog” on page 228](#).

To have Identity Governance calculate risk scores for your environment, you select which factors contribute to risk calculation, configure how much weight each risk factor carries in calculations, and then direct Identity Governance to start the calculation process by clicking **Calculate**. Some risk factors that you can select, such as Certification policies, require that you actually have the factor configured for your environment to have Identity Governance use that factor in the risk score calculation. For more information, see [“Creating and Editing Certification Policies” on page 303](#).

To configure risk scoring:

- 1 Log in as a Global or Data Administrator.
- 2 Under **Policy**, select **Risk**.
- 3 Expand a risk score section to customize it.
- 4 For the governance risk score, you must assign weights and risk factor ranges to enable Identity Governance to calculate risk.

NOTE: The governance risk score depends on application and user risk scores.

- 5 For applications and users, in **Risk scoring**, select **Calculated** to show the risk factors and weights.

NOTE: The application risk score depends on user risk score.

- 6 For each risk factor that you want to use, enter the weight for that risk factor and customize the range values you want to use. When setting a range, any value below the low range will have zero risk set. Any value above the high range will have the maximum risk value set. For more information, see [“Risk Factors” on page 290](#).
- 7 Continue assigning weight values to risk factors until your risk factor weights add up to your desired amount.
- 8 Select **Save** and then select **Calculate**.
Identity Governance shows status when calculation is in progress and completed.
- 9 View calculated risk scores in the appropriate catalog section, such as users or applications, or on the **Overview** page for the Governance risk score. In the catalog, individual items have a **Risk Factors** tab, if applicable, that shows the calculated risk score details, such as risk score, last calculated date, and risk factors used in the calculation.

Setting and Viewing Risk Calculation Schedules and Status

You can set a regular schedule for Identity Governance to calculate risk scores in your environment.

- 1 Log in as a Global or Data Administrator.
- 2 Under **Policy**, select **Risk**.
- 3 Expand **Risk Score Schedule**.
- 4 (Optional) View status of recent risk score calculations. Each risk score section also contains the calculation status for that section.
- 5 Select **Active** and then set the details for Identity Governance to calculate risk in your environment, such as start and end date and time details and whether to repeat on a regular schedule.

Viewing Calculated Risk Scores

After you configure Identity Governance to calculate risk scores, you can view risk scores of items in the catalog and your overall governance risk score on the **Overview**.

- 1 Log in as a Global or Data Administrator.
- 2 (Conditional) On **Overview**, view the Governance risk score for your organization if you have configured Identity Governance to calculate the Governance risk score.
- 3 (Optional) Select the score to display the risk factors and other details of how Identity Governance calculated this score.
- 4 (Optional) Select **Edit** to change the factors of this calculation.
- 5 Under **Catalog** select **Users** or **Applications** and select a user or application to see the user's or application's risk score displayed on the right side of the window.
- 6 Select **Risk Factors** to display the configured details for how Identity Governance calculated the risk score, along with the raw and weighted scores calculated for each risk factor.

Raw Score

The score for a risk factor based on the configured type, such as average or specified range. For example, if the administrator has configured that the **Risk of permissions assigned to user** be averaged, Identity Governance averages the permission risk values for each user in the catalog and reports this number as the raw score.

Weighted Score

The calculated score for a risk factor based on the configured weight for that risk factor. For example, if the administrator has configured that the average value of **Risk of permissions assigned to user** be 50% of the total risk score for each user, Identity Governance takes 50% of the raw score and reports this number as the weighted score.

27 Administering Access Request

The Access Request Administrator or Global Administrator must configure policies that govern who can request access and who can approve access requests in your environment.

- ♦ [“Understanding Access Request” on page 297](#)
- ♦ [“Configuring Access Request” on page 297](#)
- ♦ [“Assigning Request to Identity Governance Users” on page 300](#)
- ♦ [“Disabling the Access Request Service” on page 301](#)

For more information about using the Access Request interface, see [Chapter 33, “Instructions for Access Requesters and Approvers,” on page 327](#).

Understanding Access Request

The Access Request interface allows users to monitor and request access for items that are available in their organization. The Identity Governance Access Request interface allows users to:

- ♦ Review their current access or the access for other users
- ♦ Review access that is recommended for them based on business role policies
- ♦ Browse application access that is available to request
- ♦ Browse Access Profiles to request a group of permissions in a single step
- ♦ Retract access request
- ♦ Retry failed request after fixing the cause of the error
- ♦ Compare access of multiple users
- ♦ Approve requests
- ♦ Review a list of access requests, status of each request, and a timeline of all related events including fulfillment

Administrators can configure the Access Request interface to provide access that is pre-approved or can be automatically routed for approval. For example, you can make access to an application available for anyone in your organization to request. Upon request, the access might be automatically granted based on the requester’s business role membership or routed to another person for approval, such as the requester’s supervisor or the application owner.

Configuring Access Request

Setting up Identity Governance for Access Request requires configuring several items:

- ♦ Business roles
- ♦ Technical roles
- ♦ Request policies
- ♦ Request approval policies
- ♦ Request policies assigned to resources and roles

If you are using business roles in your organization, you can configure Access Request to show users recommended access. If you want to show recommended access to users and do not have any business roles, create business roles first. For more information, see [Chapter 25, “Creating and Managing Business Roles,” on page 273](#).

If you are using technical roles in your organization, you can provide groups of permissions, or Access Profiles, that users can request in a single step. To provide Access Profiles in Access Request, create technical roles to group the permissions. For more information, see [“Managing Technical Roles” on page 231](#).

Request policies define what access can be shown and requested in the Access Request interface. Request approval policies define the approvals needed when users request access. For more information, see the following sections:

- ♦ [“Creating Request Policies” on page 298](#)
- ♦ [“Creating Request Approval Policies” on page 299](#)
- ♦ [“Assigning Resources to Request and Approval Policies” on page 299](#)

Creating Request Policies

To allow users to request access, you must create request policies. Request policies define what access can be shown and requested in the Access Request interface. Users with the Access Request Administrator and Global Administrator authorization can create request policies.

- 1 In Identity Governance, select **Policy > Access Request**.
- 2 On the **Request Policies** tab, select **+** to create a new policy.
- 3 Name the policy.
- 4 Select what types of users **All Users** are allowed to make requests for. For example, if you want all users to be able to request access for themselves and their direct reports, select **Self** and **Direct Reports**.

NOTE: Granting ability to request for **All Users** automatically includes the ability to request for **Self**, **Direct Reports**, and **Downline Reports**. Granting the ability to request for **Downline Reports** automatically includes the ability to request for **Direct Reports** as well.

- 5 For more granular control of specific users and groups, use the **Allowed Users** and **Allowed Groups** sections. For example, if you want specific users or groups to be able to request access for all users, specify that here.

NOTE: If **All Users** are granted the ability to request for a certain type of user, you do not need to grant that same ability to specific users or groups. For example, if **All Users** are granted the ability to request for **Self**, you do not need to grant the request for **Self** ability to specific users or groups.

- 6 For exclusions, use the **Disallowed Users** and **Disallowed Group** sections.
- 7 Use **Allowed Business Roles** to add business roles as requestors for self, downline reports, direct reports, or all users.
- 8 Save the policy.
- 9 Add applications, permissions, and technical roles that you want these users to be able to request on the appropriate tabs.

Creating Request Approval Policies

To set appropriate approvals for requested access, you must create request approval policies. Identity Governance provides a default approval policy that you can edit. You can also create new request approval policies to further define your approval policies for various situations.

- 1 In Identity Governance, select **Policy > Access Request**.
- 2 On the Approval Policies tab, select **+** to add an Access Request approval policy.
- 3 Name the policy.
- 4 Add one or more approval steps, depending on how many levels of approval you require. For each approval step:
 - ◆ Specify approvers

NOTE: You can use coverage maps to specify approvers. For information about coverage maps, see [“Using Coverage Maps” on page 165](#).

- ◆ View notification emails, and optionally set reminder email frequency and add recipients
 - ◆ Set escalation period and specify escalation approvers
 - ◆ Set expiration period and assign default action at the end of the expiration period
- 5 Save the policy.

Assigning Resources to Request and Approval Policies

After you have created request or approval policies, you can assign resources to them, such as applications, permissions, and technical roles.

- 1 In Identity Governance, select either the applications, permissions, or roles catalog.
- 2 Select the applications, permissions, or roles you want to apply request policies to.
- 3 In **Actions**, select the option you want. You can:
 - ◆ Assign access request policy
 - ◆ Remove access request policy
 - ◆ Assign approval policy

You can also assign resources to a policy or remove resources from a policy while editing the policy definition.

- 1 Select the **Applications**, **Permissions**, or **Roles** tab.
- 2 Select **+** under the tab to select resources of the specific type to assign to the policy.
- 3 Select the resources to be removed using the check box next to the ones you want to remove.
- 4 Select **Remove** to remove the selected resources.

NOTE: You cannot remove resources from the default approval policy in this way. A resource can only be removed from the default approval policy by assigning it to another approval policy. Also, removing a resource from a policy other than the default approval policy will re-assign the resource to the default approval policy.

Assigning Request to Identity Governance Users

The method for giving Identity Governance users the ability to request and approve access varies.

Access Request Activity	Configuration Method	Configured By
Add items to Browse list	Create an Access Request policy and add items to the policy.	Global Administrator or Request Administrator
Add items to Recommended items list	Add items to a request policy that are covered in a business roles policy.	Global Administrator or Request Administrator
Specify approval rules for request Items	Create a request approval policy and assign permissions, applications, or roles to that policy either while editing the policy definition or in the catalog using bulk select menu.	Global Administrator or Request Administrator
Specify coverage map for request approvals	Create coverage map in CSV format, add/upload it to application (Administration > Coverage Maps), and then specify approvers in a request approval policy as coverage map. For information about creating and loading coverage maps, see "Using Coverage Maps" on page 165 .	
Configure request item text or icons	Edit the permission, application, or technical role in the data source, the catalog, or with the bulk edit feature.	Global Administrator or Request Administrator
Manage how requests are fulfilled	Identity Governance Fulfillment > Configuration . For information about configuring fulfillment targets, see "Configuring Fulfillment" on page 138 .	Global Administrator or Request Administrator
Manage who can request on behalf of others	Requesters tab in appropriate Request Policy.	Global Administrator or Request Administrator
Manage email notifications for request approvals	Notifications section in each approval step of the appropriate Request Approval Policy	Global Administrator or Request Administrator
Create an Access Profile to allow requesting collections of authorizations	Technical role in the catalog added to Request Policy	Global Administrator or Request Administrator

Access Request Activity	Configuration Method	Configured By
Control approval decision support information	<p>Similarity profile settings in Identity Governance Administration > Role Mining and Analytics Settings.</p> <p>For information about configuring similarity profile settings, see “Configuring Analytics and Role Mining Settings” on page 148.</p>	Global Administrator or Request Administrator

Disabling the Access Request Service

You can prevent displaying the Access Request pages in Identity Governance by disabling the Access Request service. When you disable the service:

- ♦ All Access Request options are removed from navigation
- ♦ Users with no rights in Identity Governance will not be redirected to Access Request
- ♦ All REST API calls for access request will return errors
- ♦ Users directly accessing the Access Request interface will see the following error message after login: `Access request services are disabled. Contact your system administrator.`

NOTE: This setting does not affect request and approval policies. Users still will be able to administer and view policies.

To disable the Access Request service:

- 1 Start the Identity Governance Configuration utility in console mode.
 - ♦ **Linux:** Default location of `/opt/netiq/idm/apps/idgov/bin`, then enter `./configutil -console -password database_password`
 - ♦ **Windows:** Default location of `c:\netiq\idm\apps\idgov\bin`, then enter `configutil -connsole -password database_password`
- 2 Check the current status of Access Request:


```
config> dc com.netiq.iac.access.request.enabled
```
- 3 Disable the Access Request service:


```
config> sp com.netiq.iac.access.request.enabled false
```
- 4 Exit the console and restart tomcat.

28 Creating and Managing Certification Policies

Certification policies allow you to produce a comprehensive view of your organization's compliance with specific certification controls, such as Sarbanes-Oxley Act (SOX) or Health Insurance Portability and Accountability Act (HIPAA). A global, review, or data administrator creates certification policies against review definitions and Identity Governance evaluates the review items and other criteria defined in the policy and reports violations. From the **Overview** or **Certification Policies** page, you can drill down to see specific violations to policies when they exist.

- ♦ [“Understanding Certification Policies” on page 303](#)
- ♦ [“Creating and Editing Certification Policies” on page 303](#)
- ♦ [“Scheduling and Calculating Certification Policy Violations” on page 304](#)
- ♦ [“Managing Certification Policy Violations” on page 305](#)

Understanding Certification Policies

Identity Governance enables organizations to easily manage multiple compliance processes as a cohesive certification policy. For example, if you are required to review all access to applications that process data related to SOX, you can create a certification policy which could include all related reviews, set a validity period for the policy, and then periodically view all SOX related violations or search for a specific violation related to user access, account access, or permissions. Specifically, a certification policy, can enable organizations to:

- ♦ Consolidate reporting and audit queries
- ♦ Schedule when certification policy calculation will occur
- ♦ Calculate violations and determine compliance status
- ♦ View the status of all access review processes included in the policy
- ♦ Get a more comprehensive governance risk overview when risk levels have been configured, and weight and range has been set for certification policy violations related risk factors

Creating and Editing Certification Policies

NOTE: Reviews should be defined before creating a certification policy. For information about review definitions, see [Chapter 21, “Creating and Modifying Review Definitions,” on page 247](#).

After creating review definitions, create certification policies that Identity Governance can use to alert you of possible compliance violations. When a review has been completed, you can view the list of violations.

- 1 Log in as a Global Administrator, Review Administrator, or a Data Administrator.
- 2 Under **Policy**, select **Certification**.
- 3 Select **+** to create a certification policy.
- 4 Enter name, validity period in days, months, or year, and single or multiple review definitions.

NOTE: Policy names must be unique. When Identity Governance checks for uniqueness, case is not considered. Therefore, Identity Governance considers Hippa and HIPPA to be equivalent.

TIP: Use wildcard * to search for reviews, or just start typing the review name to view suggestions.

- 5 (Optional) Set risk.
- 6 (Optional) Specify policy administrator.

NOTE: Policy administrator role is not currently functional, but will be functional in the next release of Identity Governance. Currently, global, review, or data administrator can function as a policy administrator.

- 7 Save your settings.
- 8 Under **Policy**, select **Certification** to view the newly created policy listed with number of violations.
- 9 (Optional) Select the policy, then select **Edit** to edit the policy.
- 10 (Optional) Select a specific policy or multiple policies, then select **Actions > Delete** to delete policies.

Scheduling and Calculating Certification Policy Violations

Policy violations are automatically calculated when a certification policy is modified, or identity or data application source is published, or when reviews included in the policy are completed. In addition, you can also schedule when certification policy will occur. However, after the validity period of a policy, you will need to manually calculate policy violations.

NOTE: If configured, certification policy violations related risk factors impact Identity Governance risk scores. Therefore, calculate certification policy violations before calculating risk scores. For information about risk scoring, see [Chapter 26, “Calculating and Customizing Risk,” on page 289](#).

To schedule certification policy calculation:

- 1 Log in as a Global Administrator, Review Administrator, or a Data Administrator.
- 2 Under **Policy**, select **Certification**.
- 3 Select **Schedule** tab, and set the schedule.
- 4 Select **Active** and then select **Save** to activate the schedule.

To manually calculate policy violations:

- 1 Log in as a Global Administrator, Review Administrator, or a Data Administrator.
- 2 Under **Policy**, select **Certification**.
- 3 In the **Policies** tab, select the policy for which you want to calculate policy violations.
- 4 Select **Actions > Calculate Policy Violations**.

NOTE: When a certification policy includes multiple review definitions, and when an entity is included in more than one review definition, then the certification status is defined based on the last review. All calculations can be canceled when in progress by selecting **Cancel** next to the progress status.

Managing Certification Policy Violations

Identity Governance provides the ability for you to define certification policies so that the system can look for violations to the policies. You can view these violations from the [Overview](#) page or the [Certification](#) page.

Selecting the number of violations, opens a panel of violations listed by users, accounts, and permissions. In each tab, you can search for the related entity or for a specific violation type for each user, account, or permissions. Types of violations include review items with no decision (No Decision), review items that are past their scheduled review period (Overdue), and review items that are past their scheduled review period and do not have any decision (Overdue with No Decision).

Resolving Certification Policy Violations

Certification policy violations can be resolved by running the related reviews. Once the review is completed, the number of violations will be recalculated automatically. For more information, about running a review, see [Chapter 22, "Running a Review Instance," on page 259](#).

29 Creating and Managing Delegation

Delegation enables you to assign delegates for users to enable a more consistent workflow for managing the reassignment of user tasks. A global, data or review administrator assigns delegate for a user, and the delegate will then receive tasks and act on them instead of the original assignee. If the original assignee acts in one of the review management roles (i.e. review owner, escalation reviewer or auditor) then the delegate will have the proper access permissions to act in that role.

- ♦ [“Understanding Delegation” on page 307](#)
- ♦ [“Assigning and Managing Delegates” on page 307](#)

Understanding Delegation

Delegation is a one-to-one mapping between two active users in the catalog. A user can have only one delegate at any given time. A user can act as delegate for multiple users. Delegate chains are allowed. For example, User A can have a delegate User B, User B can have a delegate User C. However, a cyclical chain, where User A’s delegate is User B, and User B’s delegate is User A, is not allowed and will cause the review startup to fail.

When a review is started, Identity Governance calculates reviewers by the active delegate mappings that exist at the start of the review. If a delegate exists for an original assignee, the delegate for all intents and purposes, is now considered the reviewer. To prevent cyclical chain related review startup failure, administrators can use the **Validate delegate mapping** bulk action after mapping delegates. The only other times Identity Governance calculates delegates is when review items are escalated, or when a reviewer is reassigned using the **Change Reviewer** option. When using the **Change Reviewer** option during reviews, the option will become inactive when a cyclical chain is detected.

A delegation continues until it is terminated or a different user is assigned. When a delegation is terminated or modified, all future tasks are reassigned to the original assignee or the new delegate. If the delegation is terminated or modified when a review is in progress, all outstanding tasks are not impacted. For purposes of historical audit, reviewer information and task activity in preview or live review tabs indicate that the task was assigned to a delegate in place of the original assignee.

Assigning and Managing Delegates

- 1 Log in as a **Global Administrator**, **Data Administrator**, or **Review Administrator**.
- 2 Under **Policy**, select **Delegation**.
- 3 Select **Add Row** to create a new delegation. Add the user, assign a delegate, add a reason, and set the status.
- 4 Click **Save**.
- 5 Repeat the above steps to add delegates for other users.

NOTE: A user can have only one delegate at any given time.

- 6 (Optional) Select **Edit** to change user, delegate, reason, or status.
- 7 (Optional) Select **Delete** to terminate a delegation.

- 8 (Optional) Select rows and then select **Actions > Enable** or **Actions > Disable** to change the status of multiple delegations.
- 9 Select rows and then select **Actions > Validate delegate mappings** to ensure delegate mappings, if chained, are chained appropriately. Fix invalid mappings, if any.

NOTE: Review owner and review administrator can by-pass delegation for the review management roles (i.e. review owner, escalation reviewer, and auditor) by editing the running review instance. These change are only made for the running review instance. Delegates also can assign another user as a reviewer by using the **Change Reviewer** option in review tabs.

30 Creating and Managing Data Policies

Data policies can help you prove to auditors and internal risk partners that the data collected and published into the Identity Governance catalog is complete and accurate. Having data policies in place can promote confidence in your data collection processes and help you show others that your processes and configuration comply with a set of standards, reducing the need for further proof unless your process or configuration changes.

When you have defined data policies in place, you can compare collection and publication details from the same data source at two different collection or publication times. Identity Governance uses the defined data policies to produce the comparison details. For more information, see [“Comparing Collections and Publications” on page 206](#).

Creating and Editing Data Policies

Identity Governance provides separate tabs for data collection policies and data publication policies. Each set of policies contains separate tabs for identity and application data sources.

- 1 Log in as a Global Administrator or a Data Administrator.
- 2 Under **Data Administration**, select **Data Policy**.
- 3 Navigate to the appropriate tab and select **+** to create a new policy.
- 4 Select the desired elements for the policy and enter criteria.
- 5 Save your settings.
- 6 Under **Data Administration**, select **Data Policy**.
- 7 (Optional) Select the policy, then select **Edit** to edit the policy.
- 8 (Optional) When editing a policy, select the trashcan icon to delete the policy.



Reporting for Identity Governance

Identity Governance integrates with Identity Reporting to generate reports about the status of reviews, collected and published data, and fulfillment. The Report Administrator can create, run, and view reports. You can install Identity Reporting with Identity Governance or run reports from an existing installation of Identity Manager Identity Reporting. You must decide which scenario works best for your environment. For more information, see

This section assumes that you intend to use Identity Reporting with Identity Governance in an environment without Identity Manager. For more information about using Identity Reporting in an Identity Manager environment, see the [Administrator Guide to NetIQ Identity Reporting](#)

- ♦ [Chapter 31, “Setting Up Identity Reporting,” on page 313](#)
- ♦ [Chapter 32, “Managing Identity Governance Reports,” on page 319](#)

31 Setting Up Identity Reporting

After installing Identity Reporting, you can modify many of the installation properties. To make changes, run the configuration update utility.

- ♦ **Linux:** `configupdate.sh`
- ♦ **Windows:** `configupdate.bat`

If you change any setting for Identity Reporting with the configuration utility, you must restart the application server that hosts Identity Reporting for the changes to take effect. However, you do not need to restart the server after making changes in the web user interface for Identity Reporting.

For more information about installing this component, see [Chapter 6, “Installing Identity Reporting,” on page 83](#).

- ♦ [“Manually Generating the Database Schema” on page 313](#)
- ♦ [“Preparing Identity Reporting for Use” on page 314](#)
- ♦ [“Enabling Auditing for Identity Reporting after Installation” on page 317](#)

Manually Generating the Database Schema

You can recreate the database tables after installation without having to reinstall.

- 1 Stop the application server, such as Tomcat. For more information, see [“Stopping, Starting, and Restarting Tomcat” on page 52](#).
- 2 (Conditional) Delete the existing database.
- 3 (Conditional) Create a new database with the same name as the one that you deleted in [Step 2](#).
- 4 (Conditional) Clear the database checksums.
 - 4a Log in to your database as `idm_rpt_cfg`.
 - 4b Execute the following command for PostgreSQL:

```
DO
$do$
BEGIN
  IF EXISTS
    (select table_name from information_schema.tables where table_schema =
'public' and table_name = 'databasechangelog')
  THEN
    update databasechangelog set md5sum = null;
  END IF;
END $do$
```

or

Execute the following command for Oracle:

```

BEGIN
FOR i IN
  (select null from ALL_TABLES where OWNER = user and TABLE_NAME =
'DATABASECHANGELOG')
LOOP
  EXECUTE IMMEDIATE 'update DATABASECHANGELOG set MD5SUM = NULL';
END LOOP;
END;

```

or

Execute the following command for MSSQL:

```

IF EXISTS (SELECT * FROM INFORMATION_SCHEMA.TABLES WHERE TABLE_NAME =
'DATABASECHANGELOG')
UPDATE idm_rpt_cfg.DATABASECHANGELOG
SET MD5SUM = NULL

```

5 Define the `JAVA_HOME` variable. For example:

- ♦ **Linux:** `export JAVA_HOME=/opt/netiq/idm/apps/jre`
- ♦ **Windows:** For instructions, see [“Installing the JDK Software and Setting JAVA_HOME”](#).

6 Re-initialize the database using the installed script:

```

♦/opt/netiq/idm/apps/idrpt/bin/db-init.sh -cfg_password *** -data_password ***

♦/opt/netiq/idm/apps/idrpt/bin/db-init.sh -cfg_password *** -data_password ***
-sql >
/opt/netiq/idm/apps/idrpt/sql/output.sql

```

7 Start the application server such as Tomcat. For more information, see [“Stopping, Starting, and Restarting Tomcat” on page 52](#).

Preparing Identity Reporting for Use

Identity Reporting needs a Report Administrator and at least one data source. You assign the administrator authorization in Identity Governance. In general, your data source is the Identity Governance database.

To prepare Identity Reporting for daily use, you need to complete the following activities:

- ♦ [“Starting Identity Reporting” on page 315](#)
- ♦ [“Assigning the Report Administrator Authorization” on page 315](#)
- ♦ [“Testing the Integration with Identity Governance” on page 316](#)
- ♦ [“Adding Data Sources to Identity Reporting” on page 316](#)

You should also update to the latest version of the Identity Governance reports. For more information, see [Step 3 on page 322](#).

Starting Identity Reporting

To verify installation and to initialize the Identity Reporting database, you must start the application server.

- 1 Log in to the application server that hosts Identity Reporting.
- 2 (Conditional) If this is the first time for starting Identity Reporting, complete the following steps:
 - 2a Delete all files and folders in the following directories for your application server:
 - ♦ **Linux:** Temporary directory, located by default in
 - ♦ /opt/netiq/idm/apps/tomcat/temp
 - ♦ Catalina directory, located by default in /opt/netiq/idm/apps/tomcat/work/Catalina
 - ♦ **Windows:** Temporary directory, located by default in:
 - ♦ C:\netiq\idm\apps\tomcat\temp
 - ♦ Catalina directory, located by default in C:\netiq\idm\apps\tomcat\work\Catalina
 - 2b Delete all log files from the logs directory of your application server, located by default in: .
 - ♦ **Linux:** /opt/netiq/idm/apps/tomcat/logs
 - ♦ **Windows:** C:\netiq\idm\apps\tomcat\logs
- 3 Start Tomcat. For examples, see [“Stopping, Starting, and Restarting Tomcat” on page 52](#).
- 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 contains the following message:

```
Server startup in nnnn ms
```
- 5 To log in to Identity Reporting, you need an account with the Report Administrator authorization. For more information, see [“Assigning the Report Administrator Authorization” on page 315](#).

Assigning the Report Administrator Authorization

To log in to Identity Reporting, your account must have the Report Administrator authorization in Identity Governance.

- 1 Log in to Identity Governance as the Global Administrator.
- 2 Select **Administration > Authorization Assignments**.
- 3 Assign users or groups to the Report Administrator authorization.
- 4 Save the change.
- 5 Select **Identity Manager System Connection Information**.
- 6 For **Identity Manager URL**, specify the URL for Identity Reporting.
For example, `http://myserver.mydomain.com:8080/IDMRPT`.
- 7 Save the change, then refresh the browser to see the change.

Testing the Integration with Identity Governance

As a Report Administrator, you can access Identity Reporting from the Identity Governance interface. You can also log in directly from the Identity Reporting URL. Only accounts with the Report Administrator authorization should be able to log in to Identity Reporting.

- 1 To verify that you can access Identity Reporting from Identity Governance, complete the following steps:
 - 1a Log in to Identity Reporting, select **Home** in the upper right corner.
 - 1b Select the **Reporting** module icon near your user name.
 - 1c Verify that you are redirected to Identity Reporting.
- 2 To verify that other authorizations are denied access to Identity Reporting, complete the following steps:
 - 2a Log in to Identity Governance, as a Global Administrator or Security Officer.
 - 2b Remove the Report Administrator authorization from the account that successfully logged in to Identity Reporting.
 - 2c Log in to Identity Reporting with that account, which no longer has the authorization.
You should attempt the log in from both Identity Governance and the reporting URL.
 - 2d Verify you cannot access Identity Reporting.

You can also attempt to log in to Identity Reporting by using a Global Administrator or Security Officer account to verify that accounts with high-level privileges cannot access Identity Reporting without the Report Administrator authorization.

Adding Data Sources to Identity Reporting

Identity Reporting runs reports against your connected data sources. Before you can run reports, you need to add the data sources.

NOTE: You must add the Identity Governance `igops` database as a data source in Identity Reporting.

- 1 Log in to Identity Reporting as the Report Administrator.
- 2 Select **Data Sources**.
- 3 Select **Add**.
- 4 Specify whether you want to select from the list of data sources or provide the details for the source.
- 5 (Conditional) If you selected **Provide database details**, specify the values for the data source. For example, database platform, the host name or IP address of the database server, and include the following settings:

Database

Specifies the name of the database. For example, to add the Identity Governance database, specify `igops` for PostgreSQL and `orcl` or whatever name you gave the Oracle database.

Username

Specifies an account that can access the tables and views in the database. For example, when adding the Identity Governance database, specify `igrptuser`.

- 6 (Optional) Test the connection to your data source.
- 7 Select **Save**.

- 8 Clean up the Tomcat folders as described in [Step 2 on page 315](#).
You might need to restart Tomcat.
- 9 Run a test report to verify functionality in Identity Reporting.
For more information about running reports, see [“Running Identity Governance Reports” on page 322](#).

Enabling Auditing for Identity Reporting after Installation

If you did not enable auditing for Identity Reporting during the installation, you must perform additional steps to enable auditing for Identity Reporting.

- 1 Stop the application server. For more information, see [“Stopping, Starting, and Restarting Tomcat” on page 52](#).
- 2 Launch the configuration update utility:
 - 2a Navigate to the `bin` directory of the Identity Reporting installation directory. For example:
 - ♦ **Linux:** `/opt/netiq/idm/apps/osp/bin/configupdate.sh`
 - ♦ **Windows:** `C:\netiq\idm\apps\oap\bin\configupdate.bat`
 - 2b Launch the configuration update utility:
 - ♦ **Linux:** `./configupdate.sh`
 - ♦ **Windows:** `configupdate.bat`
 - 2c In GUI mode, click **CEF Auditing > Auditing Settings**, then click **Send audit events**.
 - 2d In Console mode:
 - 2d1 Enter the number for **CEF Auditing**. By default it is #4.
 - 2d2 Enter the number for the Auditing settings. By default it is #1.
 - 2d3 Enter number 1 to enable auditing.
 - 2e Save and close the configuration update utility.
- 3 Edit the corresponding auditing file for Identity Reporting. For more information, see [“Enabling Auditing for Identity Reporting” on page 108](#).
- 4 Start the application server. For more information, see [“Stopping, Starting, and Restarting Tomcat” on page 52](#).

32 Managing Identity Governance Reports

The Report Administrator can create, run, and view reports.

To use Identity Reporting, your login account must have a Report Administrator authorization. Use a browser to log in to Identity Reporting. For example: `http://server1.mycompany.com:8080/IDMRPT`.

- ♦ “Understanding the Provided Reports” on page 319
- ♦ “Running Identity Governance Reports” on page 322

Understanding the Provided Reports

Identity Reporting provides several pre-defined reports for Identity Governance. For most recent changes to reports, see the latest release notes at the [NetIQ Identity Governance Documentation \(http://www.netiq.com/documentation\)](http://www.netiq.com/documentation) website.

NOTE: For reports in CSV format, you must select CSV as the output format. All CSV reports are downloadable CSV files that can be opened with spreadsheet software and enable user manipulation of the data.

Report	Description
Account Ownership	Shows the average number of accounts owned by identities across all applications. Optionally, it shows average numbers broken down by all applications or specified applications. Averaging across all applications supersedes specific application selection.
Accounts in Review - CSV	Lists all account reviews and displays details such as application sources, reviewers, review status, and final decisions for each review in a downloadable CSV file that can be opened with spreadsheet software and enables user manipulation of the data. Select CSV as the output format.
Bulk Data Update Details	Provides details of bulk data update operations for identity and application sources.
Bulk Data Update Overview	Provides an overview of bulk data update operations for identity and application sources.
Catalog Account Details	Displays information about specified applications including associated permissions, accounts, and Identity Manager System information.
Catalog Account Overview	Provides high-level information about accounts in the catalog.
Catalog Applications Details	Displays information about specified applications including associated permissions, accounts, and Identity Manager System information.

Report	Description
Catalog Applications Overview	Displays high-level information about each application in the catalog.
Catalog Curated Data Details	Provides details of attribute data curated for users, accounts, and permissions, comparing effective values with the most recently collected and published values.
Catalog Curated Data Overview	Displays high-level information about each group in the catalog.
Catalog Extended Attributes	Displays high-level information about each extended attribute in the catalog.
Catalog Group Details	Displays information about the specified groups in the catalog, including group membership.
Catalog Permissions Details	Displays information about specified permissions, their associated users, and their affiliated permissions.
Catalog Permissions Overview	Displays high-level information about each permission in the catalog, grouped by application, and which business roles has authorized it.
Catalog Users Ad Hoc	Displays user-defined information pertaining to identities as well as their associated permissions and applications.
Catalog Users by Supervisor	Provides information about each user in the catalog, grouped by supervisor. Optionally, it includes users without a supervisor.
Catalog Users Details	Displays information about specified users in the catalog, including group membership, permissions held, associated accounts, and direct reports.
Catalog Users Overview	Lists all identity sources and applications, and the times they are collected and published in the system.
Collection Details	Provides the status and details for all collection and publication instances of each identity and application source.
Collection Overview	Lists all identity sources and applications, and the times they are collected and published in the system.
Database Statistics for Identity Governance	Displays Identity Governance database statistics for the selected data source. You must have Administrator-level access to the Identity Governance database to retrieve the statistics from the database.
Fulfillment Status and Closed Loop Verification	Lists the status of application provisioning requests, identifying which requests have been verified as fulfilled and which remain open.
Fulfillment Status and Closed Loop Verification - CSV	Lists the status of application provisioning requests, identifying which requests have been verified as fulfilled and which remain open in CSV format.
Permission Assignment Changes by Permission	Displays permission holders at the beginning and end of the specified date range, as well as permission assignment additions and removals between the displayed lists of permission holders.

Report	Description
Permission Delta by Permission	Displays the changes in permissions held by a specified user within a given date range. Permissions are sorted by application.
Permissions Delta by User	Displays the changes in permissions held by a specified user within a given date range. Permissions are sorted by application.
Permissions in Review - CSV	Lists permissions in review in CSV format.
Preview Changes - CSV	Lists changes made to review instances, and reassigned review items while in preview mode in CSV format.
Privileged Account Ownership	Shows the privileged accounts owned by users across all applications along with the users for each account. Output can be grouped by application.
Review Definitions	Lists details for all review definitions including User Access Review and Unmapped Account Review.
Review Details	Lists all reviews and displays details such as application sources, permissions, reviewers, review status, and final decisions for each report.
Review Details - CSV	Lists all reviews and displays details such as application sources, permissions, reviewers, review status, and final decisions for each report in CSV format.
Review Item Exception	Lists all reviews that contain exception items along with their exception reason and time of exception.
Review Overview	Lists a summary of all reviews, their status, and dates.
Reviewer Status	Lists review status information grouped by supervisor.
Role Details	Provides detailed information about roles, including associated permissions and separation of duties policies.
Role Overview	Provides a summary of technical roles and business roles.
Separation of Duties Open Violations Details	Provides detailed information about open separation of duties violations including violators, violations details, and actions taken.
Separation of Duties Open Violations Overview	Displays high-level information about each Separation of Duty open violation.
Separation of Duties Policies Details	Provides detailed conditions and compensating controls for separation of duties policies.
Separation of Duties Policies Overview	Provides a summary of separation of duties policies.
Unmapped Accounts	Lists application accounts and any permissions that they hold that do not have associated users. The accounts are grouped by application. Duplicate account names across multiple applications can also be highlighted.

Report	Description
User Permissions Snapshot	Displays permission information about the specified user on a selected date. Intended for Identity Governance.

Running Identity Governance Reports

You can run the reports at any time. You can also create a schedule to run the report regularly.

NOTE: Scheduled reports should always use the date and time for the server where you installed Identity Reporting. When you use Identity Reporting in an environment distributed across multiple time zones, scheduled reports might run at a time other than the scheduled hour. This occurs because of the discrepancy between the time zones for the server that hosts Identity Reporting compared to the computer from which you scheduled the report. For example, a user in London schedules a report to run at 4 a.m., with the assumption that the report runs according to Greenwich Mean Time. However, the reporting server in New York City runs the job at 4 a.m. Eastern Daylight Time, which is five hours later than the user planned.

- 1 Log in to Identity Reporting as the Report Administrator.

You can enter the reporting URL directly in the browser or select the **Reporting** module icon near your user name in Identity Governance.

- 2 Select **Repository**.

- 3 (Conditional) If the Repository does not contain any Identity Governance reports or you want to add or update reports, complete the following steps:

- 3a Select **Download**.

- 3b (Optional) Change the filter to **Identity Governance Reports**.

- 3c Browse to **Updated reports** or **New reports**.

- 3d Select the Identity Governance reports that you want to use, and in **Bulk Actions**, select **Install report definition archives (RPZ)**.

- 3e Select **Apply**.

- 4 (Conditional) If you want to change any report values, specify the report values with the following considerations:

Criteria

Ensure that you specify a data source that relates to the report type. If Identity Reporting cannot run the report against the specified data source, Identity Reporting displays an **<!>** icon beside **Data source**.

You can specify the language for fields in the report. The data in the report will always be in the language of its data source.

Default Notifications

You can send the report to anyone. Simply specify the values for the notifications.

Schedule

You can add and remove scheduled runs of the report. You can also have several scheduled runs with different names. To ensure that the report includes the most recent data, select **Attempt data collection before scheduled run**.

- 5 Select **Repository**, and then select the reports that you want to run.

Reports for Identity Governance have a tag of "Identity Governance."

- 6 In **Bulk Actions**, select **Run Now**, and then select **Apply**.
- 7 Select **Reports** to view completed reports.



Instructions for Identity Governance Users

This section provides instructions for the following Identity Governance users:

- ♦ Access requesters
- ♦ Access Request approvers
- ♦ Reviewers
- ♦ Review owners
- ♦ Fulfillers

Users with these transient authorizations might not need access to the administrative functions in Identity Governance and do not need to read the entire *Identity Governance User Guide*. Instead, these users can print their particular instructions or access the information on the [Identity Governance Documentation \(https://www.netiq.com/documentation/\)](https://www.netiq.com/documentation/) website.

- ♦ [Chapter 33, “Instructions for Access Requesters and Approvers,” on page 327](#)
- ♦ [Chapter 34, “Instructions for Reviewers,” on page 333](#)
- ♦ [Chapter 35, “Instructions for Review Owners,” on page 337](#)
- ♦ [Chapter 36, “Instructions for Fulfillers,” on page 345](#)

33 Instructions for Access Requesters and Approvers

This section provides information for individuals using the Identity Governance Request interface to request or approve access for themselves or others.

For more information about configuring and administering Access Request, see [Chapter 27, “Administering Access Request,”](#) on page 297.

- ♦ [“Understanding the Access Request Process”](#) on page 327
- ♦ [“Reviewing Current Access”](#) on page 328
- ♦ [“Requesting Access and Viewing Timeline”](#) on page 328
- ♦ [“Approving Access Requests”](#) on page 330
- ♦ [“Comparing Access of Multiple Users”](#) on page 330
- ♦ [“Retracting Access Request”](#) on page 331
- ♦ [“Restarting Failed Access Request”](#) on page 331

Understanding the Access Request Process

The Access Request interface allows you to request application access and permissions for other resources in your environment. These requests might be subject to an approval chain before they are granted, and Access Request also manages these approvals. Additional features include ability to view access request related activity timeline, ability to view SoD violation if any, and the ability to compare granted permission between users, allowing you to standardize their access. Finally, based on your authorization, it allows you to examine your own current access, or the access of another user, revoke a request, retry a failed request, or terminate a failed request.

Access Request allows you to request the following types of items:

- ♦ Application request, which usually gives login privileges to that application
- ♦ Permission request, which usually gives more rights within an application
- ♦ Access profile (technical role), which is a collection of permissions requested as a single request

Identity Governance administrators define the policies that govern who can request access, what they can access for and for whom, and any required approvals. Approvers are notified by email of pending requests according to these Access Request policies, which contain a fine-grained mechanism for controlling the frequency of these notifications. Access Request policies may also designate CC and BCC email recipients, as well as an escalation policy in case the approver does not act in a timely fashion. For more information, see [Chapter 27, “Administering Access Request,”](#) on page 297.

Reviewing Current Access

Current Access lists all the permissions you currently own. If you have permission to view access for others, you can change to another user to see their access. You might also have permission to remove access items for yourself and others.

- 1 In the Request interface, select **Current Access** to review the permissions you hold. Dynamic resources appear as a link that you can select to show additional information.
- 2 Select your name under Current Access to see any other users whose access you have permission to view.
- 3 (Optional) If a permission appears as a link, select it to view more information.
- 4 Select another user to view their current list of access items.

NOTE: The current list of access items is always for the user listed under Current Access.

- 5 (Optional) Select the trash can icon next to any item you want to remove, type a reason, and then select **Add to request**.

NOTE: If there is no trash can next to an item, that item is not removable.

- 6 (Conditional) If you have any items in the shopping cart, select the shopping cart, and then select **Submit**.

NOTE: Selecting a trash can next to a request in the shopping cart immediately removes the request from the cart but does not submit the request.

Requesting Access and Viewing Timeline

Under **Request**, you can:

- View and refresh a list of your requests, their current status, and a timeline showing details of the request, approval, and fulfillment events
- View and request application access, application permission, or access profile recommended for you or a user you are authorized to request permissions for
- Browse and request application access, application permission, or access profile for you or a user you are authorized to request permissions for

NOTE: Dynamic resources, a specific type of permission, might require additional input. For example, if the dynamic resource is a phone, you might have to select a phone model.

To view a list of your requests, their status, and timeline:

- 1 Select **Request > My Requests**.

TIP: Requests which violate SoD policies will have a warning icon next to the request name. Click on the icon to view violated SoD policies.

- 2 Use **Search** to filter the requests and the page control (if shown) to page through them.
- 3 Select a request item status to view and collapse the timeline of underlying events associated with the request, including fulfillment information.

NOTE: Select **Refresh** icon next to **My Requests** to refresh the status. Do not refresh the browser as it might require you to re-login or lead to an error condition.

If the Identity Governance administrators have created and assigned business roles in your environment, you might see recommended items to request. Business role assignments determine these recommended items. You can also browse other items that you can request for yourself or others.

To view and request items:

- 1 Select **Request > Recommended**.
- 2 (Optional) Use **Search** to filter the recommended items and the page control (if shown) to page through them.

NOTE: Business role assignments determine these recommended items. If in your environment, Identity Governance administrators have not created and assigned business roles, you might not see any recommended items to request.

- 3 (Conditional) If there are recommended items, for example applications or access profiles, select an item, enter a reason, and select **Add to request**. Repeat this to add more items.
- 4 (Conditional) If you have rights to request on behalf of others:
 - 4a Select the current user to change who you are requesting for.
 - 4b Select an item, enter a reason, and select **Add to request**. Repeat this to add more items.
 - 4c (Optional) Select a different user to review and request items for that user.
- 5 Select **Request > Browse**.
- 6 On the **Applications** tab, select an application to expand the items to request.
- 7 Select the application to request login access to the application or select individual permissions, review SoD violation if any, enter a reason, and select **Add to request**.
- 8 On the **Access Profiles** tab, select an access profile (technical role) to request multiple permissions in a single step, enter a reason, and select **Add to request**.
- 9 (Optional) Select a different user to review and request items for that user.
- 10 After you have requested items for all users, select the cart to submit your choices.

NOTE: Selecting **X** next to a request in the shopping cart immediately removes the request from the cart but does not submit the request.

When you review permissions available to request, items have the following icons signifying the state of the item:

Shopping cart

Item has been requested and is in the shopping cart, but the request has not been submitted.

Lock

Item needs approval after being requested.

Clock

Item has been requested and is in progress awaiting fulfillment or approval.

Check mark

User already owns item.

Approving Access Requests

You might have to approve requested items if the Access Request policy specifies you as an approver for requests. Your Access Request administrators might have flagged some items as needing further approval someone requests them. Some administrators require business role members, a person's supervisor or an application owner to approve requested items, and some items might require multiple approvers. In these situations, you must approve items before the next designated approver receives them.

To see and act on your approval items:

- 1 In the Request interface, select **Approvals**.
- 2 Select a request item on the left to display the details on the right. A request might contain more than one requested item.
- 3 (Optional) Select a requested item to see details about the request, including decision support information.

NOTE: By default, Identity Governance enables decision support information, including business role authorization status. If you do not use business roles, and if you are also an administrator, you can disable the status display by deselecting **Administration > Analytics and Role Mining Settings > Show business role authorization status** option.

- 4 Select to **Approve** or **Deny** each requested item.
- 5 Select **Confirm approval** to submit your approval tasks.

Comparing Access of Multiple Users

If you have permission to see and request items for others, you can also show multiple users with their permissions listed to compare their access. When you are comparing a user to other users, you can request items for the first user in the list, making it easy to ensure that users in the same job role have the same access.

- 1 In the Request interface, select **Compare**.
- 2 Select the user under User Access Comparison whose access you want to compare with others.
- 3 Select **Compare to** for a list of users to compare with the first user.
- 4 (Optional) Select **Compare to** and choose additional users to continue adding to the table. As you add users to compare with the first user, Identity Governance adds permissions in the first column to reflect all the listed users' permissions, adds check marks in the appropriate columns to show that a user owns a permission, and puts a link to add or remove permissions for the first column for any permissions you are allowed to change for that user.
- 5 (Optional) Select **Add** or **Remove** to change the permissions for the first user in the table, enter a reason, and select **Add to request**.

NOTE: Dynamic resources might require additional input. For example, if the dynamic resource is a phone, you might have to select a phone model.

- 6 (Conditional) If you have added requests to your cart, select the cart and submit the requests.

NOTE: Selecting a trash can next to a request in the shopping cart immediately removes the request from the cart but does not submit the request.

Retracting Access Request

Occasionally, you might need to retract an access request which has not been fulfilled. Instead of creating a help desk ticket to terminate the request, you can now revoke it directly in the application. A retracted request item will move from a tentatively retracted to a completed retracted state.

NOTE: You can revoke request only for a request item that is either in approval pending or failed state. After fulfillment, use procedures in [“Requesting Access and Viewing Timeline” on page 328](#) to remove or add access.

To retract an access request:

- 1 Select **Request > My Requests**.
- 2 If the **Status** of a request item is Approval Pending or Approval Failed, click **Retract**.

Restarting Failed Access Request

Occasionally, access requests may fail. For example, if OSP is configured for HTTPS, but the server where the request workflow is running does not have the proper certificate in the cert store to be able to communicate with it, then the request item will fail. Once you have fixed the issue, instead of requesting access again, you can retry the failed request item.

To restart a failed access request:

- 1 Select **Request > My Requests**.
- 2 Check the error message for information about the request item with Approval Failed status.
- 3 Fix the issue or contact your system administrator to fix the issue.
- 4 Once the issue has been fixed, click **Retry**.

34 Instructions for Reviewers

This section provides information for individuals assigned the Reviewer authorization for a review run in Identity Governance. Reviewers confirm whether permissions or membership granted to a user or account should be kept or removed or, in some cases, modified.

- ♦ [“Understanding Reviews” on page 333](#)
- ♦ [“Performing a Review” on page 335](#)
- ♦ [“Viewing Completed Reviews” on page 336](#)

Understanding Reviews

Identity Governance collects information from a variety of identity and application data sources in your environment. This allows your organization to periodically review and verify that users have only the level of access that they need to do their jobs.

- ♦ [“Understanding the Steps in a Review Run” on page 333](#)
- ♦ [“Understanding the Reviewer’s Authorization” on page 334](#)

Understanding the Steps in a Review Run

In Identity Governance, Review Administrators create **review definitions** for a particular set of users or accounts that need review. A single instance of a review definition is a **review run** or review campaign, which has a Review Owner. The Review Owners can see only the review runs that they own.

Reviews can be started either in a preview or a live mode. Review Administrators can set up a review to automatically start in preview mode or they can set up a regular schedule in a review definition so that the review runs start automatically in live mode, according to the schedule.

Understanding the Steps in Preview Review Run

When the owner initiates a review run in preview mode, or when a review run starts automatically in preview mode, the following activities occur:

1. Identity Governance generates lists of **Reviewers**, **Review items**, and **Notifications**.
2. Review Owner previews the review definition for the current run and optionally, changes review owner or auditor, and modifies review options, and schedule.
3. Review Owner reviews all the review items and assigned reviewers, or searches for specific review items, to decide whether the items should be assigned to another reviewer.
4. Review Owner also verifies that appropriate notifications are being sent to the correct recipients, and if required, emails notification template for preview.

NOTE: The changes made by the Review Owner are applied to the current run only. If permanent changes need to be made to the review definition, or reviewers need to be changed for all subsequent runs, then the changes must be made by editing the review definition itself.

5. Optionally, Review Owners, downloads all or select review items as CSV to review it manually.

Understanding the Steps in Live Review Run

When the owner initiates a review run in live mode, or when a review run starts by the schedule, the following activities occur:

1. Identity Governance generates tasks for the assigned Reviewers and notifies them as specified in the review definition.
2. Reviewers review their assigned set of review items and decide whether the items should be kept, modified, or removed. If a review item is assigned to multiple reviewers, the first reviewer who acts on that item becomes the decision-maker, and the item continues to the next phase of the review. For more information, see [“Performing a Review” on page 335](#).
3. (Conditional) If the review definition specifies that a permission requires multiple stages of approval, Identity Governance forwards the affected review items to the next assigned reviewer. For example, the application owner, permission owner, or Review Owner might be required to review the permissions and confirm decisions before action is taken to remove any permissions. Reviewers must complete the review in the assigned order.
4. (Conditional) If a Reviewer does not complete tasks in the specified timeframe and the review definition specifies an escalation process, Identity Governance forwards the tasks to the assigned Escalation Reviewer or the Review Owner. For multiple serial reviewers the escalation will forward to the next reviewer before it finally ends up in the escalation reviewer or review owner queue.
5. The Review Owner approves the changes.

NOTE: Review Owners can override reviewer decisions, if the review definition specifies it as allowed, at any point during a review run. When a Review Owner overrides a decision, the review item is removed from the reviewer’s task list.

6. Identity Governance initiates the fulfillment process to enable the requested changes.
7. (Conditional) In a manual fulfillment process, Identity Governance generates tasks that the assigned Fulfillers must complete and notifies them by email.
8. (Optional) An Auditor might be required to certify the results of the review run. For more information, see [“Understanding the Review Process” on page 20](#).

Understanding the Reviewer’s Authorization

Reviewers represent individuals who have the information and authority to determine whether account permissions are correct. You might be assigned to review items in multiple active review runs. Depending on how the review is defined, Identity Governance might send you emails to remind you of incomplete tasks and approaching deadlines.

As a Reviewer, you can:

- ♦ Filter the list to show only incomplete review items

- ♦ Sort the review items by many different characteristics, such as by user, permission, account, type, attribute, application, roles (technical and business), or action
- ♦ Process review items individually or in a batch
- ♦ Add a comment to a review item with your decision to keep or remove, individually or in a batch
- ♦ View the details of the review item
- ♦ View guidance on how the permission was assigned, such as through a direct assignment or authorized by a role
- ♦ Choose to keep, modify, or remove the items
- ♦ View activity for a review item
- ♦ Change Reviewer of a review item, individually or in a batch, if you do not have the information you need to confirm the assigned permissions
- ♦ Submit decisions for your tasks in the allotted timeframe

If you are an **Escalation Reviewer**, you must resolve all review items that are not completed on time.

Secondary reviewers in a multi-stage review can confirm the previous decision or they can override the decision.

For more information, see [“Performing a Review” on page 335](#).

Performing a Review

This section provides the steps required for you to complete Reviewer tasks associated with a review run. Usually, Identity Governance sends an email notification when you have tasks in a review run.

For more information about the Reviewer’s authorization and the review process, see [“Understanding Reviews” on page 333](#).

- 1 In Identity Governance, select **Reviews**.
- 2 Select the review run on which you want to act.
- 3 (Optional) Adjust display options to help you manage your review items:
 - 3a Select **Show submitted items** to see all review items in the list.
 - 3b Click **Show all** to see a list of grouping options. This is especially helpful when you have a long list of review items.
 - 3c Click the gear icon to change display options by adding, removing, or rearranging columns.
- 4 For each review item, click the review item link to view system guidance to assist you with making your decision, and then select one of the following:
 - ♦ **Keep** to specify that you believe that the user should have the account or role
 - ♦ (Conditional) **Assign** if there are unmapped accounts to map the account
 - ♦ (Conditional) **Modify** if the review definition allows this option
 - ♦ **Remove** to specify that you believe that the user should not have the account or role
 - ♦ **View Activity** to decide what actions to take or what actions have been taken
 - ♦ **Change Reviewer** to pass the decision to another reviewer

NOTE: If you select User B, who has a delegate User C who has a delegate User B, as the new reviewer, a warning will be issued, and the **Change Reviewer** option will be disabled to prevent cyclical delegation.

- 5 Look over the changes to ensure accuracy.
- 6 Select **Submit** to confirm your actions on the review items.

This action locks your decisions and moves the items out of your queue. Identity Governance then moves the items to the next reviewer's queue if this is a multistage review and you are not the last reviewer. If you are the last reviewer, Identity Governance notifies the Review Owner that the review is ready for certification.

If one of your review items is in the **Multiple Reviewers** queues, then your decision gets locked in when you **Submit** the decision. If you have not yet submitted a decision and another reviewer makes a decision and submits before you, it is the other reviewer's decision that gets locked. You can see the decision in the **View Activity** option.

Viewing Completed Reviews

Reviewers and Review Owners can view the details of review items they had submitted during an active review, as well as when the review instance is complete. Select **Show completed reviews** to view completed review's start and end date, status including certification percentage, and review items which you submitted. Optionally, sort review items by decision, and select **View Activity** to view actions related to the review item, including change reviewer and modify reasons if any.

35 Instructions for Review Owners

Identity Governance enables your organization to review and verify that users have only the level of access that they need to do their jobs. As a Review Owner, you are responsible for managing one or more review runs in progress. You can view the details of any user, permission, roles (technical or business), or application entity within the context of the review run. However, depending on your authorization assignments, you might not have access to the Identity Governance catalog.

- ♦ [“Understanding the Review Process for Review Owners” on page 337](#)
- ♦ [“Managing a Review in Preview Mode” on page 338](#)
- ♦ [“Managing a Review in Live Mode” on page 339](#)

Understanding the Review Process for Review Owners

As a Review Owner, you can see only the review runs that you own. You can start the review run in preview mode or go live. The preview mode enables you to preview review definition, notifications, and review items before going live. The live review process starts with the initiation of a review run and ends when the Review Owner or Auditor, if specified, certifies the review. Between those two events, Reviewers and Fulfillers perform their assigned tasks.

This section provides the following information:

- ♦ [“Understanding the Review Definition” on page 337](#)
- ♦ [“Understanding Reviewers and Escalation” on page 338](#)
- ♦ [“Understanding the Fulfillment Process” on page 338](#)

For an overview of the review process, see [“Understanding the Review Process” on page 20](#). For steps in a review run, see [“Understanding the Steps in a Review Run” on page 333](#)

Understanding the Review Definition

Each review runs according to its **review definition**, which specifies the following items:

- ♦ Review type and name
- ♦ (Optional) Review description and instructions for reviewers
- ♦ Review items, such as user accounts, roles (technical and business), and permissions, to be reviewed by the specified Reviewers
- ♦ Review options, such as whether certain actions require comments, and whether to allow self reviews
- ♦ Individuals who serve as Reviewers, such as supervisors, permission owners, and application owners
- ♦ (Optional) Individuals who monitor reviews, such as owners and auditors
- ♦ (Optional) Escalation process for review items
- ♦ Review timeframe that contains an expiration policy and partial approval policy

- ♦ Notifications to be sent throughout the review
- ♦ (Optional) A schedule for automatically starting the next review and repeating the review on a regular basis
- ♦ (Optional) Default grouping of request items

For more information, see [Chapter 21, “Creating and Modifying Review Definitions,” on page 247](#).

Understanding Reviewers and Escalation

When you initiate a review run, Identity Governance generates tasks for the assigned Reviewers. The Reviewers are responsible for reviewing a set of users and deciding whether the current user access should be maintained or revoked, or, in some cases, modified. Identity Governance can also escalate the process and send reminders until the Reviewer completes the task. The Review Owner can reassign Reviewers, review their actions on review items, and override their review actions.

Reviews that contain reviewers specified by a coverage map, can result in an escalation if no matches could be found from the coverage map. For more information about reviewers, see [“Specifying Reviewers” on page 256](#). For more information about managing Reviewers, see [“Managing the Progress of Reviewers” on page 342](#).

Understanding the Fulfillment Process

The source of the identities and permissions under review drives how requested changes are fulfilled. The fulfillment process can be manual tasks, automated actions in Identity Manager, actions sent to help desk services, or actions initiated by workflows in Identity Manager. In a manual fulfillment process, the applications catalog specifies the individuals responsible for making the requested changes. For example, your Help Desk group might be assigned to fulfill the changeset. If a Reviewer changes a user’s permissions, Identity Governance creates tasks for the specified Fulfillers.

For more information about fulfillment, see [“Fulfilling Changes Requested in the Review” on page 21](#) and [“Viewing Fulfillment Status” on page 343](#).

Managing a Review in Preview Mode

This section provides the steps required to run a review in preview mode.

- ♦ Start review in preview mode.
- ♦ View review definition version, review items, assigned reviewers, and recipients of notifications
- ♦ Change the Review Owner, Escalation Reviewer, or Auditor for the current review run
- ♦ Change the review period, escalation timeout period, expiration policy, partial approval policy, or validity period of the current run
- ♦ Reassign Reviewers within the current review run, including bulk actions
- ♦ Search for email recipients by name
- ♦ Sort notifications by type
- ♦ Send notification preview to a specific recipient

NOTE: Notifications sent during review preview mode, which enable administrators and review owners to preview notifications, might have blanks for values, and names seen in the preview might not be the name that is sent in the real email.

- ♦ Cancel preview if review properties and items were not as expected and the review definition needs to be modified, or go live

Managing a Review in Live Mode

This section provides the steps required for you to run and complete a review. As the owner of an active review, you can:

- ♦ Start in preview mode and go live, or start the review in live mode, and monitor the review progress
- ♦ View review status in **Reviews**
- ♦ View **Quick Info** details about a catalog item
- ♦ Reassign Reviewers within the review, including bulk actions
- ♦ Send a reminder email to a Reviewer using the **Nudge** option
- ♦ Override a Reviewer's decisions
- ♦ Change the Review Owner or add more Review Owners
- ♦ Change the Escalation Reviewer or Auditor
- ♦ Resolve access policy violations in the review
- ♦ Complete a partial review
- ♦ Terminate the review before completion
- ♦ Approve Reviewer decisions
- ♦ Run reports against the review

If you assign a new owner to a review, both the previous and new owners can access the review. The previous owner continues to see instances of a review run before the ownership change. The new owner sees only the instances run after the ownership change.

If you assign a new review owner while a review run is in progress, the review definition does not change, and the new review owner is in effect for only that review run. The next review run that starts from the same review definition assigns the review owner specified in the review definition.

For example, a review definition specifies Mary Smith as the review owner. During an instance of the review, or a review run, the global administrator realizes that Mary is on vacation. To keep the review moving, the administrator changes the review owner to Sam Butler, who approves that review run when reviewers have submitted all their final decisions. Both Mary and Sam can see the details of this review run. The next time a review run starts from this review definition, Mary is assigned as the review owner.

For more information, see the following sections:

- ♦ [“Checklist for Managing a Review in Live Mode” on page 340](#)
- ♦ [“Starting a Review Run” on page 341](#)
- ♦ [“Managing a Review Run” on page 341](#)
- ♦ [“Modifying the Settings of a Review Run” on page 342](#)
- ♦ [“Managing the Progress of Reviewers” on page 342](#)

- ♦ [“Approving the Review” on page 343](#)
- ♦ [“Viewing Fulfillment Status” on page 343](#)
- ♦ [“Managing the Audit Process” on page 344](#)
- ♦ [“Viewing Run History” on page 344](#)

For more information about running reports, see [“Running Identity Governance Reports” on page 322](#).

Checklist for Managing a Review in Live Mode

	Checklist Items
<input type="checkbox"/>	1. Ensure that you understand the review process. For more information, see “Understanding the Review Process for Review Owners” on page 337 .
<input type="checkbox"/>	2. Start the review run. For more information, see “Starting a Review Run” on page 341 .
<input type="checkbox"/>	3. (Optional) Modify the timeframe for the review. For more information, see “Modifying the Settings of a Review Run” on page 342 .
<input type="checkbox"/>	4. Check the progress of each Reviewer. For more information, see “Managing the Progress of Reviewers” on page 342 .
<input type="checkbox"/>	5. Approve the actions taken by the Reviewers. For more information, see “Approving the Review” on page 343 .
<input type="checkbox"/>	6. (Conditional) Check the status of manual fulfillment activities. If the process is automated or uses external workflows, Identity Governance sends the changeset to Identity Manager for processing. For more information, see “Viewing Fulfillment Status” on page 343 .
<input type="checkbox"/>	7. (Conditional) Confirm the completion of all fulfillment tasks, if any occurred.
<input type="checkbox"/>	8. (Conditional) If a review run generated a changeset, collect and publish all identities and the application sources related to the review run. You might not have an authorization in Identity Governance that allows you to collect and publish. Someone with the Global Administrator or Data Administrator authorization can perform this action.
<input type="checkbox"/>	9. (Conditional) Check the status of the review audit. For more information, see “Managing the Audit Process” on page 344 .
	10. (Optional) View run history. For more information, see “Viewing Run History” on page 344

Starting a Review Run

In Identity Governance, you can see all review definitions assigned to you, including the date that the Review Administrator specified the review should be run.

- 1 In Identity Governance, select **Definitions**.
- 2 In the Actions column, select **Start Review** on the row of the definition that you want to run.
- 3 Select **Start and Go Live**.

Managing a Review Run

You can view the status of the review runs in progress, send reminder emails, change the assignments for reviewers and the auditor, override reviewer decisions, complete, approve, or terminate the review run, and approve the completed review.

- 1 In Identity Governance, select **Reviews**.
Identity Governance displays an overview of runs in progress, which indicates progress of completed tasks.
- 2 To manage the run, select the review.
- 3 To see a status of each of the review items, select **Review Items**.
- 4 Act on individual review items either individually or using the bulk selection options. Actions you can take depend on settings in the review definition and may include:
 - ♦ **View activity** to see review item details
 - ♦ (Conditional) **Override** a Reviewer's decision to make a decision final and remove it from all reviewer queues
 - ♦ **Change reviewer** to transfer the review item to another reviewer
 - ♦ **Approve** to move the decision to fulfillment while allowing the review to continue
 - ♦ **View fulfillment status** to view status of review requests such as removing permission, or assigning new user.
- 5 To complete the review as-is, accepting all final decisions and leaving items without final decisions as **No decision**, select **Complete** in the review completion overview at the top of the review.
- 6 To move all final decisions to fulfillment while allowing the review to continue, select **Approve** in the review completion overview at the top of the review.
- 7 To cancel the review, select **Terminate** in the review completion overview at the top of the review.

Why would I override a Reviewer's action?

As the owner of the software application being reviewed, you might disagree with a Reviewer's decision that grants a user access to the application. Alternatively, you might see the need for a user to have access where the Reviewer did not. For example, you know that a manager in Human Resources requires administrative permissions to the application.

Why would I complete or approve an in-progress review?

As the owner of a review, you might want to implement decisions that have been made without waiting for all reviewers to complete their tasks. Approving individual review items or the overall review sends final decisions to fulfillment while keeping the review running. Completing an in-progress review accepts final decisions, ends the review, marks items without decisions as **No decision**, and sends items with decisions to fulfillment.

Modifying the Settings of a Review Run

As the Review Owner, you can edit the review timeframe and escalation timeout; change the Escalation Reviewer, the assigned Auditor, and the Review Owner; and add multiple Review Owners. Depending on your entitlements, you might also be able to modify the full review definition. However, this section explains how to perform the simple modifications.

- 1 In Identity Governance, select **Reviews > Reviews**.
- 2 Select the active review run that you want to modify.
- 3 To determine whether the number of review tasks can be performed in the specified timeframe, complete the following steps:
 - 3a Under the review name, select **more**, and then select the edit icon.
 - 3b Observe the number of review items that still must be completed.
 - 3c Compare the estimated number of review items with the date in **Review end**.
 - 3d Change the end date for the review if needed.
- 4 Change or add review owners if needed.
- 5 Modify the appropriate settings, then select **Save**.

Why would I modify the review's timeframe?

When Review Administrators create a review, they can estimate the number of users, permissions, accounts, and review items affected by the review. Then they set the timeframe of the review. However, that estimation is based on a snapshot of the catalog at the time that they created the review definitions. Depending on when you run the review, the number of accounts might have increased or decreased considerably. The timeframe might no longer match the current state of the catalog.

Why would I change the Review Owner?

In general, the Review Owner is the owner of the software application with user accounts that the review run affects. However, your authorization in the organization might have changed. You can assign ownership of the review run to an individual more suited to the task. You might also want to assign multiple Review Owners.

Why would I change the Auditor?

If the assigned Auditor is not available to perform the tasks for the review run, you can assign a different individual to the authorization.

Managing the Progress of Reviewers

To ensure that the review run stays on schedule, you can view the progress of each Reviewer. You can also reassign tasks to a different Reviewer and override a Reviewer's action for a review item. Reviewers can change the reviewer for any items.

- 1 Select the active review that you want to manage.
- 2 Under **Reviewers**, select the name of the Reviewer that you want to manage.
- 3 Observe the actions taken by the Reviewer.

You can view the items that have not been completed or all review items. You can send reminder emails, using the **Nudge** option, for items not yet reviewed. You can also change the sort of the items in various ways based on the selectable column headers.

- 4 (Optional) To expand a window that allows you to compose an email, click **Nudge** to send a reminder email to the reviewer.

- 5 (Optional) To assign a review item to a different Reviewer, select **Change Reviewer**.

You can also reassign items in a batch.

- 6 (Optional) To review a Reviewer's decision, select **View Activity** for the task.

Why would I reassign a review item?

If the Reviewer is not able to perform one or more tasks for the review run, you can assign a different individual to the authorization. For example, the Reviewer might be sick or on vacation. Also, some Reviewers might complete tasks faster than others. You might want to reassign items from the slower Reviewers. For more information, see [“Reviewing Access and Permissions” on page 21](#).

What if I have multiple reviewers?

If the reviewer is listed as **Multiple Reviewers**, then more than one reviewer shares the responsibility making a decision on the review item. You can see who are members of the shared queue and send a reminder emails all of the members or delegates, if mapping exists. When changing reviewer out of a **Multiple Reviewers** queue, the item is no longer under shared responsibility.

Approving the Review

The approval process allows the Review Owner to confirm the actions taken by all Reviewers.

- 1 Select the active review that you want to manage.
- 2 Observe the actions taken by the Reviewers.
- 3 (Optional) Override actions as needed.
- 4 To approve the decisions made in the review run, select **Approve**.
- 5 (Optional) Add a comment.
- 6 (Conditional) If the review run included changes to user accounts, ensure that the affected data sources are collected and published.

After the administrator collects and publishes the data sources, Identity Governance updates the status of the fulfillment items.

Viewing Fulfillment Status

The source of the identities and permissions under review drives how requested changes are fulfilled. The changes can be fulfilled manually, by a help desk service, or sent to Identity Manager, which automatically makes the changes or initiates external workflows. In a manual fulfillment process, the applications catalog specifies the individuals responsible for making the requested changes. For example, your Help Desk group might be assigned to fulfill the changeset.

As the Review Owner, you can **View fulfillment status** for each review item which was fulfilled manually.

For more information about the fulfillment process, see the following sections:

- ♦ [“Fulfilling Changes Requested in the Review” on page 21](#)
- ♦ [Chapter 36, “Instructions for Fulfillers,” on page 345](#)

Managing the Audit Process

Some review definitions require an Auditor to certify the results of the review run. Auditors can see the details and history of the review items. When rejecting a review run, the Auditor must add a comment about the rejection.

Viewing Run History

Identity Governance tracks all the reviews, and maintains a history of previews and review runs associated with a review definition. The run history is searchable and sortable, and displays the start and end date of the run, status including certification percentage, review owner, and list of review items and associated actions including change reviewer and modify actions, and remove comments if any. The run history also displays fulfillment status of review items.

To view run history:

- 1 Select **Reviews > Definitions**.
- 2 Search for the review definition and click the review name, or directly click the review name.
- 3 Select **View run history**.

NOTE: Except for terminated previews, all other previews and reviews will be listed in the run history.

36 Instructions for Fulfillers

This section provides information for individuals assigned the Fulfiller authorization for a review run in Identity Governance. Periodically, individuals in your organization participate in a review to determine whether permissions granted to user accounts should be kept or removed. For each change, Identity Governance creates tasks for the Fulfiller who has been assigned to manually fulfill the requests.

- ♦ [“Understanding the Fulfillment Process” on page 345](#)
- ♦ [“Performing a Manual Change” on page 346](#)

Understanding the Fulfillment Process

Identity Governance collects information from a variety of identity and application data sources in your environment. This allows your organization to periodically review and verify that users have only the level of access that they need to do their jobs. The review process results in a list of changes, or **changeset** that are then implemented. Additionally, request for access, also results in a list of changes. Identity Governance refers to the implementation process of a changeset as **fulfillment**.

- ♦ [“Managing the Fulfillment Process” on page 345](#)
- ♦ [“Understanding the Fulfiller’s Authorization” on page 346](#)

Managing the Fulfillment Process

The source of the identities and permissions under review drives how requested changes are fulfilled. The changes can be fulfilled manually, by a help desk service, or sent to Identity Manager, which automatically makes the changes or initiates external workflows. In a manual fulfillment process, the applications catalog specifies the individuals responsible for making the requested changes. For example, your Help Desk group might be assigned to fulfill the changeset.

Fulfillment Administrators can configure fulfillment targets, keep track of the fulfillment process, and reassign manual fulfillment items if needed. Identity Governance provides the following status conditions for fulfillment items:

- ♦ Error or time out
- ♦ Fulfilled
- ♦ Pending fulfillment
- ♦ Verified
- ♦ Ignored
- ♦ Retry

When the fulfiller confirms the fulfillment activities, Identity Governance updates the status of the fulfillment item. Global and Fulfillment administrators can access the Fulfillment page, as well as Auditors. After the administrator collects and publishes application sources again, Identity Governance updates the status of these fulfillment items.

For an overview of the fulfillment process, see [“Fulfilling Changes Requested in the Review” on page 21](#) For more information about status conditions, see [“Understanding Fulfillment Status” on page 146](#)

Understanding the Fulfiller's Authorization

As part of the review, managers might change the permissions assigned to individuals in your organization. Business role membership changes can also generate change requests. Only Global Administrators and Fulfillment Administrators can assign Fulfillers to complete a fulfillment.

As a Fulfiller, you can:

- ♦ Sort the items by column, the available columns depend on the tab you are accessing
- ♦ Add a comment to an item, individually or in a batch
- ♦ View the details of the item at the list level, including where the change request originated, and view additional details including potential SoD violations if any, and reason for the request by clicking on the task link.
- ♦ Make the changes to the user account in the affected application
- ♦ Declare your tasks complete in Identity Governance
- ♦ View fulfillment errors

For more information, see [“Performing a Review” on page 335](#).

Performing a Manual Change

This section provides the steps required for you to complete Fulfiller tasks associated with a review run. Usually, Identity Governance sends an email notification when you have tasks in a review run.

For more information about your authorization and the review process, see [“Understanding Reviews” on page 333](#).

- 1 In Identity Governance, select **Requests** to view the fulfillment requests.
- 2 Change between tabs to see requests from different areas or to see fulfillment errors.
- 3 Click the fulfillment task link to expand the task description and determine the changes to be made, reason for the change, and potential SoD violations if any.
- 4 In the application affected by the requested change, modify the permission according to the fulfillment task. This might impact the SoD policies or uncover unmapped users.
- 5 (Conditional) The Fulfillment Administrator can view the status of the fulfillment requests on the **Fulfillment Status** page.
- 6 Return to Identity Governance to specify one of the following outcomes for the fulfillment task:
 - ♦ **Fulfilled**: to indicate that you successfully changed the permission
 - ♦ **Declined**: to indicate you could not or did not remove the permission with a comment
 - ♦ **Reassign**: to assign the fulfillment task to a different user
- 7 (Conditional) If any errors occur during the fulfillment process, access the **Fulfillment Errors** tab to see more details. From this list you can try to resolve the errors:
 - 7a Click **Fix** to go to the **Fulfillment Configuration** page if you have administrator access, otherwise ask your administrator to do the next step.
 - 7b Click **Application Setup**, view the settings for the application producing errors, and adjust the settings.

- 7c** Go back to the **Fulfillment Requests > Fulfillment Errors** tab, and click **Retry** to route the item to the correct fulfiller.
- 7d** If it is not possible to fix the problem, click **Terminate** to remove this change request item from the **Fulfillment Errors** tab.
- 8** To complete your tasks, select **Submit**.

The fulfillment process starts only after the Review Owner completes the review. Any manual fulfillment changes to the fulfillment request do not effect the Review run.

