Identity Governance

Installation and Configuration Guide

24.3 (v4.3.1)

Legal Notice

The only warranties for products and services of Open Text and its affiliates and licensors (“Open Text”) are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Open Text shall not be liable for technical or editorial errors or omissions contained herein. The information contained herein is subject to change without notice.

About this Book and the Library

The *Installation Guide* provides installation and initial configuration information for the Identity Governance product. This book also provides upgrade information for current product installations.

Intended Audience

This book provides information for Identity Governance administrators responsible for installing and configuring the product in their environment.

Other Information in the Library

The library provides the following information resources in addition to this guide. Visit the Identity Governance Documentation Web site to access all the documents in this library.

Release Notes

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

User and Administration Guide

The User and Administration Guide provides a step-by-step guidance for Identity Governance user-oriented and administration tasks. Specifically, it provides instructions for the following Identity Governance users:

- Access requesters
- Access Request approvers
- Reviewers
- Review owners
- Fulfillers
- Application owners
- Separation of Duties Policy owners
- Business Role managers
- All administrator authorizations

Reporting Guide

Provides information about Identity Reporting for Identity Governance and how you can use the features it offers.

Identity Manager Driver for Identity Governance

Provides information about how to install and configure the Identity Manager Driver for 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.

Technical References

Provide specific details about narrow topics relevant to few use cases.

Contents

1 Identity Governance Overview

Identity Governance is a solution that 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.

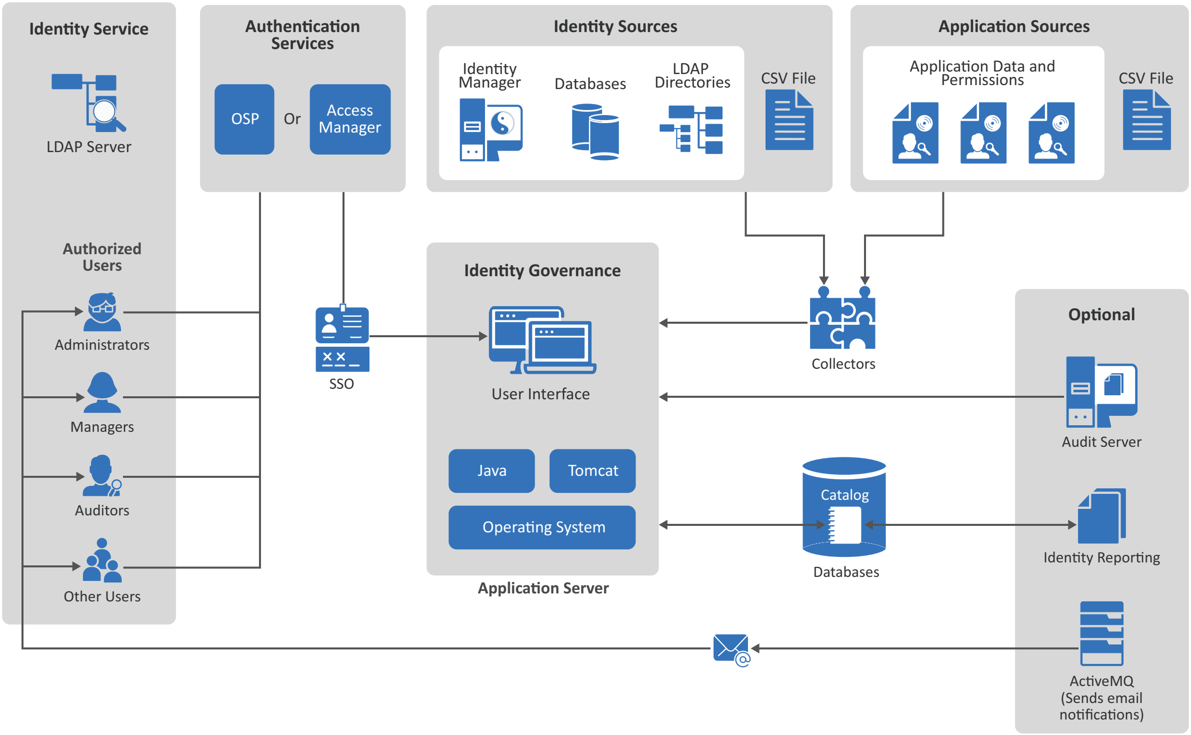
With Identity Governance, administrators and business managers can ensure that your employees, either individually or as a group, have the appropriate set of permissions. Identity Governance collects information from various identity and application data sources and manages the entire review and certification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

- Section 1.1, “Understanding the Identity Governance Components,” on page 12
- Section 1.2, “Understanding the Installation Methods,” on page 18
- Section 1.3, “Understanding the Uninstallation Methods,” on page 22
- Section 1.4, “Understanding the Identity Governance Configuration Utilities,” on page 24
- Section 1.5, “Understanding REST Services for Identity Governance,” on page 25

1.1 Understanding the Identity Governance Components

Identity Governance is a web application that consists of several components. Out of these, you must install and configure some components before installing Identity Governance and some, which are optional, after installation. These optional components provide additional functionality during deployment. The following graphic is an overview of the Identity Manager components.

Figure 1-1 *Overview of the Identity Governance Components*



This guide explains the different components that are part of Identity Governance. The User and Administration Guide contains information about how Identity Governance works and the features it provides. For more information, see "Introduction" in the *Identity Governance User and Administration Guide*.

The following information is useful for people who deploys Identity Governance and configures it to obtain the identity data and application data in the IT environment.

- Section 1.1.1, "Understanding the Required Components for Identity Governance," on page 13
- Section 1.1.2, "Understanding Authorized Users for Identity Governance," on page 14
- Section 1.1.3, "Understanding the Data Sources," on page 15
- Section 1.1.4, "Understanding the Optional Components," on page 16

1.1.1 Understanding the Required Components for Identity Governance

Identity Governance requires that you install several components and have these components running and configured before you can start the Identity Governance installation. Before you start installing the components, you should read the following sections:

- Section 1.1.1.1, "Understanding How Identity Governance Uses Java," on page 13
- Section 1.1.1.2, "Understanding the Application Server," on page 13
- Section 1.1.1.3, "Understanding the Catalog," on page 13

1.1.1.1 Understanding How Identity Governance Uses Java

Identity Governance uses Java to perform all the data processing in your environment to create reports and reviews and perform other actions. You must have the open Java version from Zulu installed and running on the same server where you install Apache Tomcat and Identity Governance. Zulu provides the Java Developer Kit (JDK). The Zulu Java Runtime Environment (JRE) comes with the Zulu OpenJDK.

WARNING: Identity Governance must have a supported Java instance installed and running to function. You cannot assume the Java version installed with the operating system also works with Identity Governance. The Zulu OpenJDK is the only supported Java version for Identity Governance.

For more information, see Section 3.4, "Installing Zulu OpenJDK," on page 48.

1.1.1.2 Understanding the Application Server

Identity Governance is a web application that requires a web application server to run the user interface. For this release, Identity Governance supports Apache Tomcat as the web server that runs the Identity Governance user interface application.

Because the user interface is a web application, people that are inside or outside the firewall can access and use Identity Governance as long as they are authorized users and have the proper credentials. For more information, see Section 3.5, "Installing the Apache Tomcat Application Server," on page 49.

1.1.1.3 Understanding the Catalog

Identity Governance collects account data, permissions, and access information for all users in your IT environment. Identity Governance stores the collected data in a catalog. Identity Governance stores the catalog in an external databases and it uses that data to generate reviews and reports to help ensure that you comply with any applicable regulations. Identity Governance requires that you install a database server or use a database instance in the cloud before you start to install Identity Governance. The database installation and configuration are not part of the Identity Governance installation process.

For a production environment, we recommend that you have the databases installed on a dedicated server that runs only the databases. Having any other Identity Governance components or any Identity Manager components installed on the database server slows down the performance of Identity Governance.

Identity Governance contains multiple databases. There are the main databases that make Identity Governance work and there is an additional separate database for Identity Reporting. The installer creates and populates the database for you. If your policies do not allow external programs to modify the database server, the installer generates a SQL script file that you can use to create the required databases and populate them correctly for Identity Governance, Identity Reporting and Workflow Engine to use. For more information about the databases, see Chapter 5, “Creating Databases for Identity Governance and Components,” on page 95.

1.1.2 Understanding Authorized Users for Identity Governance

Identity Governance requires that any administrator, manager, auditor, or any other user that accesses and uses Identity Governance have an account for an identity service and an authentication service to log in and access Identity Governance.

- Section 1.1.2.1, “Understanding the Bootstrap Administrator for Identity Governance,” on page 14
- Section 1.1.2.2, “Understanding the Identity Service,” on page 14
- Section 1.1.2.3, “Understanding the Authentication Services,” on page 15

1.1.2.1 Understanding the Bootstrap Administrator for Identity Governance

The bootstrap administrator account is an account that you define during the Identity Governance installation that can immediately log in and configure Identity Governance before importing any identity data from the systems in your environment. You can have an LDAP-based or file-based bootstrap administrator account. The file-based bootstrap account is useful if you do not have an authentication server installed that contains your administrator accounts before installing Identity Governance. For more information, see Section 4.1.1, “Using the Bootstrap Administrator,” on page 58.

1.1.2.2 Understanding the Identity Service

The identity service is an LDAP server that contains the user accounts that access and use the features in Identity Governance. This service allows Identity Governance to control which accounts in the IT environment can access the features in Identity Governance. To grant users access to Identity Governance and its features, you must add the users to the identity service (LDAP server) and import their account information into Identity Governance using an identity source. For more information, see Section 3.7, “Preparing or Installing an Identity Service,” on page 50.

1.1.2.3 Understanding the Authentication Services

Identity Governance uses an authentication service to provide authentication methods for authorized user accounts stored in the identity service. By default, Identity Governance uses the LDAP account name and password as the authentication method for the authorized users. However, this means that users must remember a separate user name and password to access Identity Governance.

Identity Governance provides additional authentication methods through the two supported authentication services: One SSO Provider (OSP) and NetIQ Access Manager. Both of these authentication services allow you to create a single sign-on (SSO) experience for your users and they provide advanced authentication options like two-factor authentication or biometric authentication for the authorized users. OSP or Access Manager can be a shared service providing SSO across Identity Governance, Identity Manager, and Identity Reporting services. You must select one of the authentication services for your Identity Governance deployment. For more information, see Chapter 4, “Installing an Authentication Service,” on page 57.

1.1.3 Understanding the Data Sources

The purpose of Identity Governance is to gather identity data, application accounts, and application permissions information from your IT environment so you can analyze the information and ensure that the correct people have the correct access to the correct applications at the correct time. This ensures that you can comply with the regulations that your industry must follow. Identity Governance allows you to import identity data from many different data sources and many different applications. You can also use a CSV file that contains this information to populate Identity Governance.

- Section 1.1.3.1, “Understanding Collectors,” on page 15
- Section 1.1.3.2, “Understanding Identity Sources,” on page 15
- Section 1.1.3.3, “Understanding the Application Sources,” on page 16

1.1.3.1 Understanding Collectors

Collectors are templates that you add to Identity Governance for each data source to map the identity data and application data to a minimum standard schema that Identity Governance uses. The standard schema allows Identity Governance to understand and translate the data to match the definitions in the Identity Governance schema. Identity Governance requires that you add the connection-specific information, such as accounts and passwords or API keys and access tokens, in the collector templates to be able to save the templates and collect the data from the sources. For more information, see “Understanding Collector Templates for Identity Sources” in the *Identity Governance User and Administration Guide*.

1.1.3.2 Understanding Identity Sources

Identity Governance imports identities from many identity sources, such as NetIQ Identity Manager, databases, LDAP directories, and CSV files. You use the collectors in Identity Governance to define the same namespace for these identity sources that Identity Governance uses. This allows Identity Governance to perform the required analysis to ensure that you comply with your industry regulations. For more information, see “Creating Identity Sources ” in the *Identity Governance User and Administration Guide*.

1.1.3.3 Understanding the Application Sources

Identity Governance imports application data, application account information, and application permissions to ensure that the users have the correct access to the correct applications and the data stored in those applications. You use the collectors in Identity Governance to define the same name space for these application sources as Identity Governance uses. This allows Identity Governance to perform the required analysis to ensure that you comply with your industry regulations. For more information, see "Creating an Application Source " in the *Identity Governance User and Administration Guide*.

1.1.4 Understanding the Optional Components

Identity Governance allows you to install additional components to increase the capabilities of Identity Governance. These components are not installed and enabled by default. You must install the component separately from the Identity Governance installation and then configure these components to work with your Identity Governance deployment.

- Section 1.1.4.1, "Understanding Auditing," on page 16
- Section 1.1.4.2, "Understanding How to Send Email Notifications," on page 17
- Section 1.1.4.3, "Understanding Identity Reporting," on page 17
- Section 1.1.4.4, "Understanding Workflow Engine," on page 17

1.1.4.1 Understanding Auditing

Identity Governance generates common event format (CEF) events that you can forward to an audit server to analyze the events and to create reports. Identity Governance events contain an authentication tracking identifier to correlate audit events from multiple systems. Identity Governance also generates audit events for Identity Governance, Identity Reporting, and OSP, and Workflow Engine.

If you have the audit server details when you install Identity Governance, you can configure them during the installation. If your audit server uses TLS, you can retrieve the certificate during installation. You can also add or change your audit server details after you install Identity Governance. For more information, see Section 12.4, "Configuring Auditing after the Installation," on page 256.

Identity Governance supports the following audit servers:

- ArcSight Enterprise Security Manager Suite
- NetIQ Sentinel
- NetIQ Sentinel Log Manager
- Splunk

For more information about supported versions, see Section 2.4.6, "Audit Server System Requirements," on page 43.

1.1.4.2 Understanding How to Send Email Notifications

Identity Governance can send email notifications to people who must take action in Identity Governance or it can send email notifications to administrators if something is wrong with the system. Identity Governance requires that you install ActiveMQ to be able to send these notifications. After you install ActiveMQ, you must configure Identity Governance to send email notifications through the ActiveMQ server. For more information, see Section 12.5, “Enabling Email Notifications after the Installation,” on page 261.

1.1.4.3 Understanding Identity Reporting

Identity Reporting generates reports that show critical business information about various aspects of your Identity Reporting and Identity Manager configuration, including information collected from the identity services and managed systems such as Active Directory or SAP. Identity Reporting provides a set of predefined report definitions that you can use to generate reports. It also gives you the option to import custom reports.

Identity Reporting generates a snapshot of the catalog and the state of permissions or reviews. You can use the reports to comply with applicable 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. For more information, see Chapter 7, “Installing Identity Reporting,” on page 163.

1.1.4.4 Understanding Workflow Engine

The Workflow Engine is responsible for managing and executing steps in an administrator-defined workflow. It also keeps track of the different states of a workflow and persists them in a database. The Workflow Engine provides additional functionality to Identity Governance such as starting a workflow process, logging, generating reminders, escalation notifications, and retrying failed processes. Additionally, the Workflow Engine sends email messages to notify users of changes in the state of the workflow during workflow execution. For more information, see Chapter 8, “Installing Workflow Engine,” on page 183.

1.2 Understanding the Installation Methods

Identity Governance and OSP provide multiple installation methods.The following information applies to both the OSP installer and the Identity Governance installer. Select which method you want to use, depending on your environment. The different installation methods are the guided installation, the console installation, and the silent installation. You must provide the same information no matter which installation method you use.

For example, if you do not have X server installed on the server that hosts Identity Governance, you would use console mode. If you have multiple installations to perform, we recommend that you use guided mode for the first server and silent mode for the remaining servers.

The installers for the Identity Governance components install the components in the following default directories no matter which installation method you choose to use. You can change these directories during the different installation methods. The default installation paths are:

- **OSP:** Default installation directory
  - **Linux:** `/opt/netiq/idm/apps/osp`
  - **Windows:** `C:\netiq\idm\apps\osp`
- **Identity Governance:** Default installation directory
  - **Linux:** `/opt/netiq/idm/apps/idgov`
  - **Windows:** `C:\netiq\idm\apps\idgov`
- **Identity Reporting:** Default installation directory
  - **Linux:** `/opt/netiq/idm/apps/idrpt`
  - **Windows:** `C:\netiq\idm\apps\idrpt`
- **Workflow Engine:** Default installation directory
  - **Linux:** `/opt/netiq/idm/apps/wfe`
  - **Windows:** `C:\netiq\idm\apps\wfe`

Use the following information to determine which method works best for your environment.

- Section 1.2.1, “Understanding the Sample Installation Scripts,” on page 18
- Section 1.2.2, “Understanding the Guided Installation,” on page 19
- Section 1.2.3, “Understanding the Console Installation,” on page 20
- Section 1.2.4, “Understanding the Silent Installation,” on page 20

1.2.1 Understanding the Sample Installation Scripts

Identity Governance requires multiple products to be installed, configured, and running before you start the Identity Governance installation. OpenText provides some sample installation scripts that you can download, edit, and then use to install some of the required components before starting the Identity Governance installation.

The sample scripts install the following components:

- Apache ActiveMQ

- Apache Tomcat
- Zulu OpenJDK

The Linux sample script does not install the PostgreSQL database. You must have a database installed before starting the Identity Governance installation. For more information, see Chapter 5, “Creating Databases for Identity Governance and Components,” on page 95.

The sample installation scripts are located on the Identity Governance documentation page under the **References** heading. You must download the scripts, extract the ZIP file, and then read the `Readme.txt` file. The file contains the instructions on how to use the sample scripts.

The sample scripts place all of the files for the installations in the following default directory:

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

The OSP, Identity Governance, Identity Reporting, and Workflow Engine installers use this as a default location as well. This guide lists these default directories to help you know where to access the different products, configuration files, and tools to manage Identity Governance. You can choose to change this default path by editing the installation scripts or changing the path when you run the installers.

1.2.2 Understanding the Guided Installation

The default installer utility for OSP, Identity Governance, Identity Reporting, and Workflow Engine is an interactive installation with a guided interface. This installer guides you through the installation by asking questions you must answer. To use the guided installation utility on a Linux server you must have X server enabled to display the guided installation. You must interact with the guided installation utility to have the installation finished successfully.

To run the guided installation, you launch the installer from the command line with no additional parameters. For example:

- **OSP:** Use the following command for your platform.
  - **Linux:** `./osp-install-linux.bin`
  - **Windows:** `osp-install-win.exe`
- **Identity Governance, Identity Reporting, and Workflow Engine:** Use the following command for your platform.
  - **Linux:** `./identity-governance-install-linux.bin`
  - **Windows:** `identity-governance-install-win.exe`

The information you must provide to complete the installation is the same whether you use the guided installation, the console installation, or the silent installation. For more information, see the following sections:

- Section 4.2, “Installing OSP for Identity Governance,” on page 61
- Chapter 6, “Installing Identity Governance,” on page 131
- Chapter 7, “Installing Identity Reporting,” on page 163
- Chapter 8, “Installing Workflow Engine,” on page 183

1.2.3 Understanding the Console Installation

Identity Governance provides an interactive, console installation for OSP, Identity Governance, and Identity Reporting without requiring graphics to be enabled on the servers that run these products. This allows you to complete the installation without enabling X server on the Linux servers.

To run the installation in console mode, you launch the installer from the command line with the `-i console` parameter. For example:

- **OSP:** Use the following command for your platform.
  - **Linux:** `./osp-install-linux.bin -i console`
  - **Windows:** `osp-install-win.exe -i console`
- **Identity Governance and Identity Reporting:** Use the following command for your platform.
  - **Linux:** `./identity-governance-install-linux.bin -i console`
  - **Windows:** `identity-governance-install-win.exe -i console`

The information you must provide to complete the installation is the same whether you use the guided installation, the console installation, or the silent installation. For more information, see:

- Section 4.2.3, “OSP Installation Worksheet,” on page 63
- Section 6.4, “Identity Governance Installation Worksheet,” on page 134
- Section 7.4, “Identity Reporting Installation Worksheet,” on page 167
- Section 8.4, “Workflow Engine Installation Worksheet,” on page 185

1.2.4 Understanding the Silent Installation

Identity Governance provides two files that allow you to install Identity Governance, OSP, and Identity Reporting without any interaction. The files are included in the ZIP files that you download for Identity Governance and OSP. You install Identity Reporting using the Identity Governance file. The two files are:

- **Identity Governance, Identity Reporting, and Workflow Engine:** `identity-governance-install-silent.properties`
- **OSP:** `osp-install-silent.properties`

You can use these files if you have multiple installations to perform or you do not want to interact with the installation utility. You can also use the silent installation to install additional nodes when you cluster the components. For more information, see Section 2.3.4, “Ensuring High Availability or Load Balancing for Identity Governance,” on page 35.

To use the file, you open the file in a text editor and define the different parameters for your environment. You can use the default paths listed in the sample installation scripts for the required components or you can define different paths. The default paths are:

- **OSP:** Default installation directory
  - **Linux:** `/opt/netiq/idm/apps/osp`
  - **Windows:** `C:\netiq\idm\apps\osp`
- **Identity Governance:** Default installation directory
  - **Linux:** `/opt/netiq/idm/apps/idgov`

    - **Windows:** `C:\netiq\idm\apps\idgov`
- **Identity Reporting:** Default installation directory
    - **Linux:** `/opt/netiq/idm/apps/idrpt`
    - **Windows:** `C:\netiq\idm\apps\idrpt`
- **Workflow Engine:** Default installation directory
    - **Linux:** `/opt/netiq/idm/apps/wfe`
    - **Windows:** `C:\netiq\idm\apps\wfe`

We recommend that you perform a guided installation with the `-r` *`path-to-filename`* option to create a response file containing the correctly formatted values for your environment. For OSP, you must add the values to the silent properties file.

- **OSP:** Use the following command for your platform.
    - **Linux:** `./osp-install-linux.bin -r` *`path_to_response_file`*
    - **Windows:** `osp-install-win.exe -r path_to_response_file`
- **Identity Governance and Identity Reporting:** Use the following command for your platform.
    - **Linux:** `./identity-governance-install-linux.bin -r` *`path_to_silent_properties_file`*
    - **Windows:** `identity-governance-install-win.exe -r` *`path_to_silent_properties_file`*

For OSP, open the response file and the silent properties file in a text editor. Copy the properly formatted values for your environment from the response file to the silent properties file.

For Identity Governance and Identity Reporting, open the path_to_silent_properties_file and provide the appropriate passwords where needed.

After you have created the silent properties files and updated them with the proper values, you use the files in conjunction with the installer utility. The installer uses the information in the silent properties file to complete the installation. For example, from the directory containing the installation files, enter the following:

- **OSP:** Use the following command for your platform.
    - **Linux:** `./osp-install-linux.bin -i silent -f` *`path_to_silent_properties_file`*
    - **Windows:** `osp-install-win.exe -i silent -f` *`path_to_silent_properties_file`*
- **Identity Governance and Identity Reporting:** Use the following command for your platform.
    - **Linux:** `./identity-governance-install-linux.bin -i silent -f` *`path_to_silent_properties_file`*
    - **Windows:** `identity-governance-install-win.exe -i silent -f` *`path_to_silent_properties_file`*

For more information, see the following sections:

- Section 4.2.5, “Silently Installing One SSO Provider,” on page 73
- Section 6.6, “Silently Installing Identity Governance and its Components,” on page 155

- Section 7.6, “Silently Installing Identity Reporting,” on page 181
- Section 8.6, “Silently Installing Workflow Engine,” on page 198

1.3 Understanding the Uninstallation Methods

The uninstall utilities support the same methods that the installation utilities support. By default, the uninstall utility uses the same method as what you used during the installation of the component. For example, if you performed a silent installation for the installation of OSP, when you run the uninstall utility for OSP it runs using the silent installation method by default. The following information applies to the OSP uninstaller and the Identity Governance uninstaller.

There is no separate uninstall utility for all features just as there is no separate installation utility. You can choose to install Identity Governance, Identity Reporting, and Workflow Engine on the same server or a separate server. The uninstall utility appears in the directory depending on the order the first feature is installed, that is, Identity Governance followed by Identity Reporting, and then Workflow Engine. Features installed together are removed together. If you install only Identity Governance, the uninstall utility will uninstall only Identity Governance.

IMPORTANT: The uninstall utilities do not contain Java. You edit the uninstall utility and add the path to the `jre bin` directory. The uninstall utility adds it as an environment variable to your server. If you do not do this, the uninstall utility will not run.

The default name of the uninstall utilities are `LaunchUninstall.sh` (Linux) or `LaunchUninstall.bat` (Windows) for all of the Identity Governance components. The utilities are located in the following default directories:

- **OSP:** Default directory for the uninstall utility:
  - **Linux:** `/opt/netiq/idm/apps/osp/Uninstall_osp`
  - **Windows:** `C:\netiq\idm\apps\osp\Uninstall_osp`
- **Identity Governance:** Default directory for the uninstall utility:
  - **Linux:** `/opt/netiq/idm/apps/idgov/Uninstall_IdentityGovernance`
  - **Windows:** `C:\netiq\idm\apps\idgov\Uninstall_IdentityGovernance`
- **Identity Reporting:** (Conditional) Only if you installed Identity Reporting on a separate server
  - **Linux:** `/opt/netiq/idm/apps/idrpt/Uninstall_IdentityGovernance`
  - **Windows:** `C:\netiq\idm\apps\idrpt\Uninstall_IdentityGovernance`
- **Workflow Engine:** (Conditional) Only if you installed Workflow Engine on a separate server
  - **Linux:** `/opt/netiq/idm/apps/idrpt/Uninstall_IdentityGovernance`
  - **Windows:** `C:\netiq\idm\apps\idrpt\Uninstall_IdentityGovernance`

You can change the uninstall methods by passing the appropriate parameter for the different uninstall method you want to use. For more information about how to change uninstall methods, see the following topics:

- Section 1.3.1, “Understanding the Guided Uninstallation,” on page 23
- Section 1.3.2, “Understanding the Console Uninstallation,” on page 23
- Section 1.3.3, “Understanding the Silent Uninstallation,” on page 24

1.3.1 Understanding the Guided Uninstallation

The guided uninstall method runs automatically if you used the guided installation method for OSP, Identity Governance, Identity Reporting, and Workflow Engine. For more information, see Section 1.2.2, "Understanding the Guided Installation," on page 19.

The guided uninstall method is an interactive utility that walks you through the uninstall process and asks you questions as you proceed through the uninstallation of the components. The default name of the uninstall utilities are `LaunchUninstall.sh` (Linux) or `LaunchUninstall.bat` (Windows) for all of the Identity Governance components. If you run the installer using a different method and you want to use the guided method to uninstall the Identity Governance components, you must enter the following from a command prompt in the directory where the uninstall utility resides:

- **Linux:** `./LaunchUninstall.sh -i swing`
- **Windows:** `LaunchUninstall.bat -i swing`

For more information, see Chapter 14, "Uninstalling the Identity Governance Components," on page 279.

1.3.2 Understanding the Console Uninstallation

Identity Governance provides an interactive, console uninstall utility for OSP, Identity Governance, Identity Reporting, and Workflow Engine without requiring graphics to be enabled on the servers that run these products. This allows you to complete the uninstallation without enabling X server on the Linux servers. This uninstall method requires interaction to complete.

The console uninstall method runs automatically if you used the console installation method for OSP, Identity Governance, Identity Reporting, and Workflow Engine. For more information, see Section 1.2.3, "Understanding the Console Installation," on page 20.

The console uninstall method provides an interactive uninstall process that walks you through the uninstallation and asks you questions as you proceed with uninstalling the components. To run the uninstall utilities using the console method, enter the following at a command prompt in the directory where the uninstall utility resides:

- **Linux:** `./LaunchUninstall.sh -i console`
- **Windows:** `LaunchUninstall.bat -i console`

For more information, see Chapter 14, "Uninstalling the Identity Governance Components," on page 279.

1.3.3 Understanding the Silent Uninstallation

The silent uninstall method uninstalls the components without any prompts or interaction from you. Unlike the silent installation, it does not require the silent properties file. You would use the silent uninstall method if you had multiple instances of the Identity Governance components to uninstall. By default, the uninstall utility runs using the silent method if you installed the component using the silent installation.

To uninstall the components, enter the following at a command prompt from the directory where the uninstall utility resides:

- **Linux:** `./LaunchUninstall.sh -i silent`
- **Windows:** `LaunchUninstall.bat -i silent`

For more information, see Chapter 14, "Uninstalling the Identity Governance Components," on page 279.

1.4 Understanding the Identity Governance Configuration Utilities

Identity Governance contains two configuration utilities. You can use the two utilities to change the configuration or enable features after you have completed the installation. The utilities perform different tasks and you must use the proper utility for the proper task. The utilities are:

- **Identity Governance Configuration Update Utility (ConfigUpdate):** You use this utility to modify Identity Reporting, OSP, and Auditing. These features are also part of other NetIQ products and you use this utility on these common products across different products. Some properties require that you use the Identity Governance Configuration Update utility to update them. For more information, see Section 15.1.5, "Using the Identity Governance Configuration Update Utility," on page 293.
- **Identity Governance Configuration Utility (ConfigUtil):** You use this utility to modify any of the Identity Governance settings you defined during the installation. For more information, see Section 15.1.4, "Using the Identity Governance Configuration Utility," on page 290.

Identity Governance contains multiple components, and you can install the components on the same server or different servers. Identity Governance uses databases and `.properties` files to store the configuration information. If you have Identity Governance and either Identity Reporting or OSP installed on the same server, the GLOBAL configuration databases and the `ism-configuration.properties` file might contain duplicate settings.

NOTE: For each property located in both the GLOBAL configuration database, and the `ism.configuration.properties` file, Identity Governance uses the property in the `ism.configuration.properties` file.

When updating the values associated with the duplicate settings, the different installation utilities place the information in different locations. If you are updating a duplicate setting using the Identity Governance Configuration Update utility, the value ends up in the `ism-configuration.properties` file. If you are updating a duplicate setting using the Identity Governance Configuration utility, the value ends up in the GLOBAL database.

Any component of Identity Governance, Identity Reporting, or OSP that retrieves the value of the duplicate property, retrieves the value from the `ism-configuration.properties` file rather than the value found in the GLOBAL database. This can cause issues in a clustered environment.

If you are running Identity Governance, Identity Reporting, and OSP in a clustered environment, ensure that you run the Identity Governance Configuration Update utility on each server in the cluster to get the information populated on each server.

1.5 Understanding REST Services for Identity Governance

Identity Governance supports REST API functionality. The REST APIs use the OAuth2 protocol for authentication. The installation program deploys a special API WAR file, `doc.war`, which contains the documentation of REST services needed for Identity Governance. On Tomcat the `apidoc.war` file is automatically deployed when Identity Governance is installed.

The REST API documentation can be found at *protocol*://*server*:*port*/apidoc. For example, `http://myserver.netiq.com:8080/apidoc`.

NOTE: You should manually move or delete the WAR files and folders from the Tomcat webapps directory in your production environment.

2 Planning to Install Identity Governance

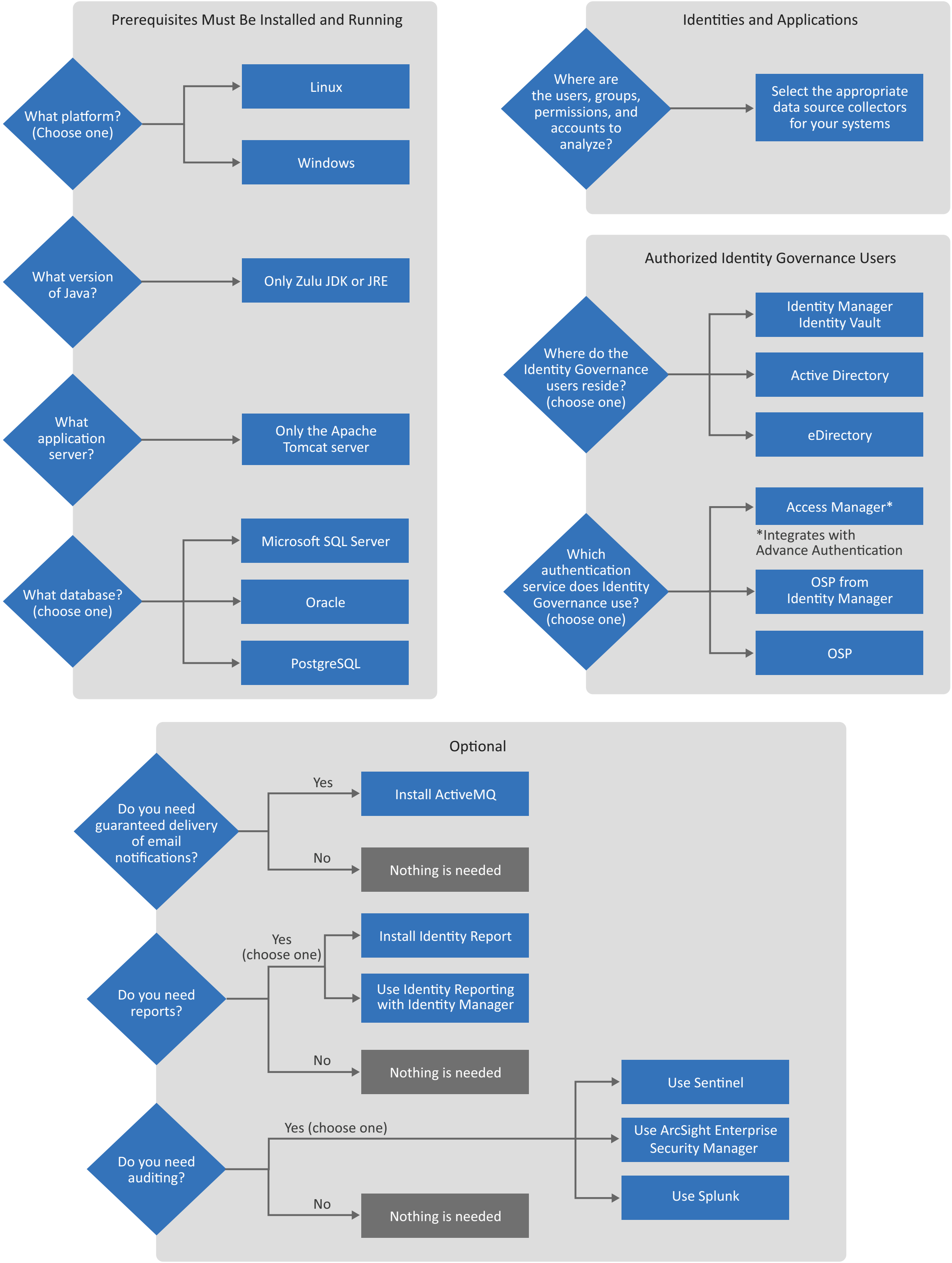
Identity Governance requires that you install and configure additional components for the product to work. Identity Governance allows many different configuration deployments of the product. You must make several decisions before installing Identity Governance. Use the following information to create a plan and gather the required information before starting the Identity Governance installation.

- Section 2.1, “Making Decisions on How to Install Identity Governance,” on page 28
- Section 2.2, “Obtaining Identity Governance, Identity Reporting, Workflow Engine, and OSP,” on page 31
- Section 2.3, “Recommended Production Environment Installation Scenarios,” on page 32
- Section 2.4, “Hardware and Software Requirements,” on page 39

2.1 Making Decisions on How to Install Identity Governance

There are many decisions that you must make before you can start the installation of Identity Governance. Identity Governance has many options to allow you to add it to your IT environment. There are some main high-level choices you must make to properly install and configure Identity Governance. Use the following Figure 2-1 to make the decisions that are appropriate for your environment and then use the worksheet in Table 2-1 to capture those choices.

Figure 2-1 *Identity Governance Decision Flow*


Prerequisites Must Be Installed and Running
What platform? (Choose one)
Linux
Windows
What version of Java?
Only Zulu JDK or JRE
What application server?
Only the Apache Tomcat server
What database? (choose one)
Microsoft SQL Server
Oracle
PostgreSQL
Identities and Applications
Where are the users, groups, permissions, and accounts to analyze?
Select the appropriate data source collectors for your systems
Authorized Identity Governance Users
Where do the Identity Governance users reside? (choose one)
Identity Manager Identity Vault
Active Directory
eDirectory
Which authentication service does Identity Governance use? (choose one)
Access Manager*
*Integrates with Advance Authentication
OSP from Identity Manager
OSP
Optional
Do you need guaranteed delivery of email notifications?
Yes
Install ActiveMQ
No
Nothing is needed
Do you need reports?
Yes (choose one)
Install Identity Report
Use Identity Reporting with Identity Manager
No
Nothing is needed
Do you need auditing?
Yes (choose one)
Use Sentinel
Use ArcSight Enterprise Security Manager
Use Splunk
No
Nothing is needed

This worksheet is a place to record the decisions you make about deploying Identity Governance and the additional components. To complete the installations successfully, use this worksheet in conjunction with the installation worksheets for the different components so that you will have all of the information required before starting the installations. For more information, see:

- Section 3.1, "Checklist for Installing Required Components," on page 46
- Section 4.2.3, "OSP Installation Worksheet," on page 63
- Section 6.4, "Identity Governance Installation Worksheet," on page 134

This worksheet does not list the specific supported versions of the different components. To see that information, see Section 2.4, "Hardware and Software Requirements," on page 39.

Table 2-1 *Identity Governance Planning Worksheet*

Item	Options	Choice
Platform	Select one of the following options: ◆ Linux ◆ Windows ◆ Virtual (As long as the virtual environment supports the Linux or Windows version, we support Identity Governance running on those platforms in virtual environments.)	
Java version	Zulu OpenJDK	
Application server	Apache Tomcat	
Database	Select one of the following options: ◆ Microsoft SQL Server ◆ Oracle ◆ PostgreSQL	
Location of users, groups, and permissions	Select the appropriate connector to use during the configuration of Identity Governance. For more information, see "Creating and Monitoring Scheduled Collections" in the *Identity Governance User and Administration Guide*.	
Identity Service	Select one of the following LDAP server options: ◆ Microsoft Active Directory ◆ Microsoft Active Directory Federation Service (AD FS) ◆ eDirectory ◆ Identity Vault from Identity Manager	

Item	Options	Choice
Authentication Service	Select one of the following options: ◆ OSP ◆ Access Manager ◆ OSP from Identity Manager	
Guarantee email delivery	If you want to guarantee email delivery to the users for Identity Governance notifications, you must install ActiveMQ.	
Detailed reports	If you want detailed reports, you must install and configure the version of Identity Reporting that comes with Identity Governance.	
Auditing	If you want auditing capabilities for OSP, Identity Governance, Identity Reporting, and Workflow Engine, you must enable auditing on these components and forward the `syslog` events to one of the supported audit servers: ◆ ArcSight Enterprise Security Manager ◆ Sentinel ◆ Sentinel Log Manager ◆ Splunk	

You can install the components for Identity Governance in many different configurations depending on your IT environment. We recommend that you install the components in a distributed environment for production deployments. Several of the components can also run in a high-availability cluster. For more information about where you should install these components, see Section 2.3, “Recommended Production Environment Installation Scenarios,” on page 32.

2.2 Obtaining Identity Governance, Identity Reporting, Workflow Engine, and OSP

You must have purchased Identity Governance to access the product in the Customer Center. The activation code for Identity Governance is in the Customer Center where you download the software. If you have issues finding or accessing the activation code, see Customer Center Frequently Asked Questions (https://support.microfocus.com/help/). For more information about Identity Governance, see Identity Governance website (https://www.opentext.com/products/netiq-identity-governance).

Identity Governance only works for 90 days without the license key. After that time, the product stops working until you enter the license key. For more information, see Section 15.7, “Updating the License Key,” on page 308.

The ZIP file that you download contains installers for Identity Governance and OSP. The Identity Reporting installer is part of the Identity Governance installer, so it is not included with the installation files. The ZIP file contains installers for Linux, Windows, and a `silent.properties` file. These files provide different installation methods for Identity Governance, Identity Reporting, Workflow Engine, and OSP.

To obtain Identity Governance:

1. Log in to the Customer Center.
2. Click **Software**.
3. On the **Entitled Software** tab, click the appropriate version of Identity Governance to download the product.
4. Download the ZIP file that contains the installers for Identity Governance.

2.3 Recommended Production Environment Installation Scenarios

You can install Identity Governance and the required components in many different configurations, depending on network topology and the identity management products with which it integrates. This section presents a few common installation scenarios and recommendations to inform your installation choices:

- Section 2.3.1, “Identity Governance in a New Environment,” on page 32
- Section 2.3.2, “Identity Governance and Existing Components,” on page 33
- Section 2.3.3, “Installing Identity Governance to Integrate with Identity Manager,” on page 34
- Section 2.3.4, “Ensuring High Availability or Load Balancing for Identity Governance,” on page 35
- Section 2.3.5, “Recommended Deployment Scenarios,” on page 37

2.3.1 Identity Governance in a New Environment

You must prepare a new environment with the required components for Identity Governance. If you do not have all of the required components in your environment, you must install them before starting the Identity Governance installation. The Identity Governance installer includes an installer for Identity Reporting and Workflow Engine. In addition to the Identity Governance installer, the software download page provides the installer for OSP. You must download the other required components from the manufacturer’s website. For more information, see Chapter 3, “Installing Required Components,” on page 45.

For best performance, do not install Identity Governance on the same server as the databases, but ensure that the databases and Identity Governance run in the same subnetwork. You must determine where you will install the required components and the Identity Governance components. For more information, see Section 2.3.5, “Recommended Deployment Scenarios,” on page 37.

You must install the Identity Governance components in a specific order, which depends on whether you plan to integrate Identity Governance with Identity Manager. If you are integrating with Identity Manager, the order is different. For more information, see Section 2.3.3, “Installing Identity Governance to Integrate with Identity Manager,” on page 34.

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

1. (Conditional) LDAP identity service with admin and user containers

   To use an identity service for the data source, ensure that you have Active Directory or eDirectory already installed.
2. (Optional) Audit server if enabling auditing during installation.
3. Zulu OpenJDK on the server that runs Identity Governance.
4. Apache Tomcat on the server that runs Identity Governance.
5. One of the supported databases in the same subnetwork as Identity Governance.
6. OSP or Access Manager.
7. Identity Governance, Identity Reporting, and Workflow Engine.
8. (Optional) Identity Reporting, if not installed at the same time as Identity Governance.
9. (Optional) Workflow Engine, if not installed at the same time as Identity Governance, is installed on a server specific to workflow.
10. (Optional) Audit server if enabling auditing after the installation.

2.3.2 Identity Governance and Existing Components

If you are installing Identity Governance into an environment that already has a supported version of the following components, you can use these components for the Identity Governance installation. Those components are:

- Zulu OpenJDK must run on the server where you will install Identity Governance
- Apache Tomcat that runs against the Zulu OpenJDK on the server where you will install Identity Governance
- Identity service of the Identity Manager Identity Vault (eDirectory); the identity service in Identity Manager is always eDirectory
- Authentication service of OSP or Access Manager
- A supported database server on the same subnetwork as Identity Governance
- ActiveMQ

NOTE: The version of Identity Reporting that comes with Identity Manager contains different reports than the version that comes with Identity Governance. If you want the Identity Governance reports, you must install the version of Identity Reporting that comes with Identity Governance. If you have a prior version of Identity Reporting that came with Identity Governance, you must upgrade that version of Identity Reporting to match what comes with the version of Identity Governance that you install.

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 Apache Tomcat environment at https://www.owasp.org/index.php/Securing_tomcat.

2.3.3 Installing Identity Governance to Integrate with 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 and Identity Reporting. The Identity Governance installation program needs 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 of Identity Reporting that comes with Identity Manager. Identity Reporting that comes with Identity Manager uses the Identity Manager security module to determine who has access to the reports.

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

1. Identity Manager Advanced Edition
2. (Optional) Audit server if enabling auditing during Identity Governance installation
3. Use the Identity Manager Identity Vault as the identity service, or use a supported LDAP directory
4. Zulu OpenJDK on the server that runs Identity Governance
5. Apache Tomcat on the server that runs Identity Governance
6. One of the supported databases in the same subnetwork as Identity Governance
7. Ensure that you use an LDAP-based bootstrap administrator during the Identity Governance installation for security reasons. For more information, see Section 4.1.1, “Using the Bootstrap Administrator,” on page 58.
8. Identity Governance
9. (Conditional) If you are using OSP as the authentication service and the identity service is an eDirectory server or an Active Directory server that is separate from Identity Manager, you must manually extend the schema on that server or the OSP authentications do not work. For more information, seeSection 9.2.3, “Extending the Schema for OSP in the Identity Service not Part of Identity Manager,” on page 206.
10. (Optional) If you want the Identity Governance reports, install the version of Identity Reporting that comes with Identity Governance. If you want the Identity Manager reports, you must install the version of Identity Reporting on a separate server that comes with Identity Manager.
11. (Optional) Audit server if enabling auditing after the installation

For more information about these activities, see "Integrating Single Sign-on Access with Identity Manager Using OSP" on page 232.

You must 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:

- Section 6.3, "Prerequisites for Identity Governance," on page 134
- Section 5.2, "Prerequisites for the Databases," on page 97
- Section 2.4.1, "Identity Governance Server System Requirements," on page 39
- Section 2.4.2, "Database Requirements," on page 41
- Chapter 6, "Installing Identity Governance," on page 131

2.3.4 Ensuring High Availability or Load Balancing for Identity Governance

High availability ensures efficient manageability of critical network resources including data, applications, and services. **Load balancing** allows you to divide the workload on a component across multiple instances of that component. Identity Governance supports high availability and load balancing through stateless clustering or Hypervisor clustering, such as VMware Vmotion. When planning a high-availability or load balancing environment, the following considerations apply:

- ❒ To manage the availability of your network resources for Identity Governance, use the High Availability tools provided with your operating system. Always have the latest patches installed for your operating system.
- ❒ To provide load balancing for Identity Governance, 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 host name and port for the Apache Tomcat server.
- ❒ Each node in the cluster must have a persistent unique runtime identifier. For example, `node1` or `ProdNode1`. For more information, see Section 9.6.1, "Configuring the Nodes in the Apache Tomcat Cluster," on page 218.

  Each Identity Governance runtime instance uses this identifier to claim and identify tasks that it processes. Some of these tasks are long-running, so the identifier must remain unique after a restart of the environment, where an IP address or another identifier might not remain the same.
- ❒ The configuration settings and keystore passwords for OSP and Identity Governance must be identical for all nodes in the cluster.
- ❒ When you are running Identity Governance, Identity Reporting, and OSP in a clustered environment, ensure that you run the Identity Governance Configuration Update utility on each server in the cluster to get the information populated on each server and also use the same keystore files.
- ❒ When installing an identity service, consider the following requirements:
  - ❒ Configure a load balancer with a DNS host name and port for the identity service.

    The identity service can use the same load balancer specified for Identity Governance, a dedicated load balancer, or a single Apache Tomcat instance.

    - ❒ Specify the values for the appropriate load balancer instead of the connection settings to the Apache Tomcat instance. For more information, see **Application address** in Step 6 on page 73.
    - ❒ The configuration files must be on each identity service deployment in the environment. For example, if using OSP, the `osp.war` file must be on each deployment of OSP in the environment.
    - ❒ After the first installation, copy and use the same Identity Service keystore and Database Encryption keystore files on all nodes for all deployments. For more information, see Chapter 4, “Installing an Authentication Service,” on page 57.
- ❒ 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 for the identity service.
    - ❒ Specify the values for the load balancer instead of the host and port for the Apache Tomcat connection. For more information, see **Application address** in Step 8 on page 154.
    - ❒ On the primary (or master) node, perform the steps for configuring the databases. For more information, see **Database details** in Step 8 on page 154.
    - ❒ 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 8 on page 154.
- ❒ To silently install OSP, Identity Governance, Identity Reporting, or Workflow Engine on the secondary nodes in the cluster, create a response file the first time you install a component using the guided installer. A **response file** contains the correctly formatted values for your environment that you must add to the `install-silent.properties` file. To create a response file, you must run the installer with the `-r` *`path-to-response-file`* option. For example:
    - **OSP:** Use the following command for your platform.
        - **Linux:** `./osp-install-linux.bin -r` *`path_to_silent_properties_file`*
        - **Windows:** `osp-install-win.exe -r` *`path_to_silent_properties_file`*
    - **Identity Governance and Identity Reporting:** Use the following command for your platform.
        - **Linux:** `./identity-governance-install-linux.bin -r` *`path_to_silent_properties_file`*
        - **Windows:** `identity-governance-install-win.exe -r` *`path_to_silent_properties_file`*

  After you have the response file, you open the response file and the `silent.properties` file in a text editor. You copy and paste the values from the response file 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=node1`

For more information, see the following:

- Section 4.2.4, "Installing One SSO Provider (OSP)," on page 72
- Section 6.6, "Silently Installing Identity Governance and its Components," on page 155
- Section 7.6, "Silently Installing Identity Reporting," on page 181

2.3.5 Recommended Deployment Scenarios

In a typical production environment, you might install Identity Governance components on three or more servers. The reason to have different components on different servers is due to the workload of the component. If one of the components has a heavy load and you have other components installed on the same server, the heavy workload impacts the performance of the other components.

The following information contains deployment recommendations for the components. Each component has different reasons why you would install it with other components or not. Use this information and the information in Table 2-2, "Different Identity Governance Component Deployment Scenarios in a Production Environment," on page 38 to determine how you deploy the Identity Governance components in your production environment.

- **OSP:** OSP does not require a lot of processing power to function unless you have hundreds of thousands of authentications occurring at the same time. In most of the production environments, you can install OSP on the Identity Governance server. In larger environments, having OSP with a clustered load on its server balances the authentications through each clustered OSP node.
- **Database:** We recommend that you always install the databases for Identity Governance and Identity Reporting on a database server. Databases require a lot of processing power. If you install the database on a server with another Identity Governance component, this causes performance issues for the component.
- **ActiveMQ:** ActiveMQ is an optional component that you can install to guarantee delivery of the emails that Identity Governance sends. ActiveMQ does not require a lot of processing power. You can install ActiveMQ on the Identity Governance server.
- **Identity Governance:** Is a web application that the authorized users access to perform all of the tasks. We recommend that you cluster the Identity Governance component for fail-over scenarios. If one node goes down, the authorized users can still log in and use Identity Governance. You can run OSP on the same server as Identity Governance except for very large production environments. You can even run Workflow Engine on the same server with Identity Governance. You would only run Identity Reporting on the Identity Governance service if you do not generate a lot of reports. If you generate a lot of reports, we recommend that you install Identity Reporting on its own server.
- **Identity Service:** The identity service is an existing, supported LDAP server in your IT environment. In most scenarios, the LDAP server already exists and contains the user accounts. Installing other components on the LDAP server can impact the performance of the users' authentications. It is best practice to have the LDAP directory installed on its server.
- **Identity Reporting:** We recommend that you install Identity Reporting on its own server if you generate a lot of reports daily. Generating reports requires a lot of processing power for Identity Reporting. If you have Identity Reporting installed on the server with other components and

you see the performance of the other components being impacted, you must move Identity Reporting to its own server. You can also cluster Identity Reporting for load balancing and fail-over scenarios.

- **Workflow Engine:** The Workflow Engine runs the workflow at runtime and manages approval tasks for approvers. If you have the Workflow Engine installed on the server with other components and you see the performance of the other components being impacted, you must move the Workflow Engine on a separate server. You can also cluster the Workflow Engine for load balancing and fail-over scenarios.

- **Audit Server:** Identity Governance forwards the audit events to the audit server. We recommend you have the audit server installed and configured before you install Identity Governance. In a production environment, you should always install the audit server on its own server for performance reasons.

Table 2-2 Different Identity Governance Component Deployment Scenarios in a Production Environment

	Case 1	Case 2	Case 3	Case 4
Server 1	OSP Identity Governance ActiveMQ	(can be clustered) OSP Identity Governance Identity Reporting Workflow Engine ActiveMQ	(can be clustered) OSP Identity Governance ActiveMQ	(can be clustered) OSP or Access Manager
Server 2	Database server	Database server	(can be clustered) Identity Reporting Workflow Engine	(can be clustered) Identity Governance ActiveMQ
Server 3	Identity service	Identity service	Database server	(can be clustered) Identity Governance
Server 4		Audit server	Identity service	Identity Reporting
Server 5			Audit server	Database server
Server 6				Identity service
Server 7				Audit server
Server 8				Workflow Engine (Will be supported in a future release)

2.4 Hardware and Software Requirements

The following section describes the verified components. However, customers running on any component not provided in this list or with untested configurations will be supported until the point it is determined that the root cause is the untested component or configuration. Issues that can be reproduced on the verified component will be prioritized and fixed according to standard defect-handling policies. For more information about support polices, see Support Policies.

Ensure that the systems you install and use with Identity Governance meet the hardware and software requirements listed here.

- Section 2.4.1, “Identity Governance Server System Requirements,” on page 39
- Section 2.4.2, “Database Requirements,” on page 41
- Section 2.4.3, “Identity Reporting Server System Requirements,” on page 43
- Section 2.4.4, “Workflow Engine Server System Requirements,” on page 43
- Section 2.4.5, “Browser Requirements for Identity Governance and its Components,” on page 43
- Section 2.4.6, “Audit Server System Requirements,” on page 44
- Section 2.4.7, “Email Notification Server System Requirements,” on page 44

2.4.1 Identity Governance Server System Requirements

This section provides the minimum requirements for the servers where you want to install Identity Governance. You can install Identity Governance and the required components in different configurations. For more information, see Section 2.3, “Recommended Production Environment Installation Scenarios,” on page 32.

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.

Category	**Minimum Requirement**
Processor	◆ 4.0 GHz, single processor (small catalog) ◆ 4 physical cores of 2.0 GHz or higher per processor
Disk Space	50 GB
Memory	◆ 16 GB (small catalog) ◆ 32 GB
Utilities	Identity Governance Configuration Update utility (ConfigUpdate) 5.0
Operating System	◆ Red Hat Enterprise Linux 8.8 (64-bit) or later patched versions of 8.*x* ◆ SUSE Linux Enterprise Server 15.4 or later patched version of 15.*x* ◆ Microsoft Windows Server 2022 or later patched versions of Windows Server 2022 **IMPORTANT:** Before installing Identity Governance, apply the latest operating system patches.

Category	Minimum Requirement
Virtual Systems	We support Identity Governance on enterprise-class virtual systems that provide official support for the operating systems where our products are running. As long as the vendors of the virtual systems officially support these operating systems, we support Identity Governance running on them. **IMPORTANT:** Ensure to configure the virtual machines running Identity Governance as Thick Provisioned.
Java	Azul JDK 11.0.24 or later respective patched versions of 11.0.*xx*
Application Server	Apache Tomcat 9.0.91 and later patched versions of 9.0.*xx* **NOTE:** (Conditional) For guaranteed delivery of email notifications, your application server must include support for Apache ActiveMQ Java Message Service (JMS) and clustering.
LDAP Identity Service	◆ Microsoft Active Directory that comes with Windows Server 2022 ◆ eDirectory 9.2.8 or later patched versions of 9.2.*x* ◆ Identity Manager 4.8.7 or 4.9 or later patched versions of 4.8.*x* or 4.9.*x*
Authentication Service	◆ OSP 6.7.6 or later versions of 6.7.x when deployed with Identity Governance 4.3.1 or Identity Manager 4.9 ◆ Access Manager 5.0.4, or later patched versions of 5.0.*x*
Secure Communication	TLS 1.2 or later for secure communication
Third-Party Connector Libraries	(Optional) The Identity Governance JDBC Collectors and SAP User Management Collector use third-party client connector software that is not distributed with the product. Find and download the appropriate JDBC driver file for your database from the database vendor. ◆ DB2: `com.ibm.db2.jcc.DB2Driver` ◆ Generic jTDS: `net.sourceforge.jtds.jdbc.Driver` ◆ Microsoft SQL Server: `com.microsoft.sqlserver.jdbc.SQLServerDriver` ◆ MySQL: `com.mysql.jdbc.Driver` ◆ Oracle Thin Client: `oracle.jdbc.driver.OracleDriver` ◆ PostgreSQL: `org.postgresql.Driver` ◆ SAP: `sapjco3.jar` **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. ◆ Sybase: `com.sybase.jdbc3.jdbc.SybDriver` To gather identity and application data from one of these sources, put one or more of the these client `.jar` files into the Apache Tomcat `/lib` folder, then restart the Apache Tomcat server. The default installation location is: ◆ **Linux:** `/opt/netiq/idm/apps/tomcat/lib` ◆ **Windows:** `c:\netiq\idm\apps\tomcat\lib`

2.4.2 Database Requirements

This section provides the minimum requirements for the server where you want to install the databases for Identity Governance and the supported versions of the databases. The databases for Identity Governance are required for the product to work.

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	◆ 4.0 GHz, single processor (small catalog) ◆ 4 physical cores of 2.0 GHz or higher per processor
Disk Space	◆ 60 GB (small catalog) ◆ 100 GB
Memory	◆ 16 GB (small catalog) ◆ 32 GB
Operating System	◆ Red Hat Enterprise Linux 8.8 (64-bit) or later patched versions of 8.*x* ◆ SUSE Linux Enterprise Server 15.4 or later patched version of 15.*x* ◆ Microsoft Windows Server 2022 or later patched versions of Windows Server 2022 **IMPORTANT:** Before installing Identity Governance, apply the latest operating system patches.
Virtual Systems	We support the databases for Identity Governance on enterprise-class virtual systems that provide official support for the operating systems where our products are running. As long as the vendors of the virtual systems officially support these operating systems, we support Identity Governance running on them. **IMPORTANT:** Ensure to configure the virtual machines running Identity Governance as Thick Provisioned.

Category	Minimum Requirement
Database	One of the following: ◆ Microsoft SQL Server ◆ Microsoft SQL Server 2019 or later patched versions of the SQL Server 2019 ◆ Microsoft SQL JDBC driver 10.2 or later patched versions of the Microsoft SQL JDBC driver ◆ Oracle ◆ Oracle 19c, or later patched versions of 19*x* ◆ Oracle JDBC driver `ojdbc8.jar` ◆ PostgreSQL ◆ PostgreSQL 14.13, or later patched versions of 14.*x* ◆ PostgreSQL JDBC driver 42.6.0 or later patched versions of the PostgreSQL JDBC driver ◆ Vertica **NOTE:** Identity Governance supports Vertica as an Identity Governance custom metrics data store and as an external archive. You cannot use Vertica as a runtime database for Identity Governance, Identity Reporting, or Workflow Service. ◆ Vertica 12.0 or later patched versions of 12.0.*x* ◆ Vertica JDBC driver 12.0.*x*
Secure Communication	TLS 1.2 or later for secure communication

For information about the different options on how to create and populate the different Identity Governance databases, see Chapter 5, “Creating Databases for Identity Governance and Components,” on page 95.

2.4.3 Identity Reporting Server System Requirements

Servers that host Identity Reporting when installing only for Identity Governance have the same minimum requirements as for the Identity Governance server and support the same databases.

Identity Reporting is a separate product that comes with Identity Governance that provides detailed reports about your business-critical processes and systems. It is optional to install Identity Reporting. If you determine that you will install Identity Reporting, you install it after you have completed the Identity Governance installation.

This section lists the requirements for the server that hosts Identity Reporting when installing only for Identity Governance. For more information about whether to install the components on the same server, see Section 2.3, “Recommended Production Environment Installation Scenarios,” on page 32.

Identity Reporting comes with Identity Manager and Identity Governance, however, the reports provided are different if you install the version that comes with Identity Manager than the version of Identity Reporting that comes with Identity Governance. There are different requirements if you want to install Identity Reporting in an Identity Manager environment. For more information about the system requirements for installing in an Identity Manager environment that includes Identity Governance, see *System Requirements for Identity Manager (https://www.netiq.com/documentation/identity-manager-49/system-requirements-identity-manager-49x/data/system-requirements-identity-manager-49x.html)*.

To see how to install Identity Reporting that comes with Identity Governance, see Chapter 7, “Installing Identity Reporting,” on page 163.

2.4.4 Workflow Engine Server System Requirements

The Workflow Engine runs the workflows at runtime and manages the approval tasks for approvers. It comes with Identity Governance but it is optional to install the Workflow Engine. To see how to install the Workflow Engine see Chapter 8, “Installing Workflow Engine,” on page 183.

IMPORTANT: Installing Workflow Engine on a remote server will be supported in a future release. If installing Workflow Engine, install it on the same Tomcat Server as Identity Governance.

2.4.5 Browser Requirements for Identity Governance and its Components

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 17.6
- Google Chrome 128.0.6613.119
- Microsoft Edge Browser 128.0.2739.42
- Mozilla Firefox 129.0.2

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

2.4.6 Audit Server System Requirements

Identity Governance generates the common event format (CEF) events which you can forward to an audit server to generate audit logs that can help prove compliance with regulations. Enabling auditing in Identity Governance is optional.

If you decide to use auditing, you must have your audit server installed and running. Identity Governance does not install the third-party audit servers for you. This section provides the minimum version of the audit servers where you want to send audit events from Identity Governance. We support the following audit servers using `syslogger` for use with Identity Governance:

- ArcSight Enterprise Security Manager Suite 7.6 (Including ArcSight Enterprise SmartConnector 8.4)
- Sentinel 8.5

- Sentinel Log Manager 8.5
- Splunk 9.0.80

To determine where you should install the audit server, see Section 2.3, “Recommended Production Environment Installation Scenarios,” on page 32. You can enable auditing during the installation of the components or you can enable auditing after you have installed the components. It depends on your environment and your needs.

2.4.7 Email Notification Server System Requirements

Identity Governance can send email notifications to managers, reviewers, administrators, or other people who must receive notifications about events or processes occurring. To be able to send emails and ensure that there are not any lapses in communication, you can install Apache ActiveMQ to guarantee that Identity Governance sends notifications using SMTP. Enabling email notifications is optional. If you choose to enable email notifications, Identity Governance supports the following:

- Apache ActiveMQ 5.17.6

You can enable email notification during the installation of Identity Governance, Identity Reporting, and Workflow Engine or you can enable email notifications after the installation. It depends on your environment and your needs.

3 Installing Required Components

Several software components must be present in your environment before you install Identity Governance. Apache Tomcat, a database server, and Zulu OpenJDK JRE must be available in your environment when you install Identity Governance. Optionally, you can have the authentication service available for Identity Governance to reference during the installation. You must use a file-based bootstrap administrator until you have the LDAP server available. For more information, see Section 4.1.1, "Using the Bootstrap Administrator," on page 58.

Additionally, you can install ActiveMQ and your audit server before installing Identity Governance to allow the Identity Governance installer to configure these additional features for you. You can perform this configuration after you have installed Identity Governance as well. For more information, see Section 3.10, "Installing Optional Components," on page 53.

IMPORTANT: You must install Identity Reporting either when you install Identity Governance, or after you complete the Identity Governance installation.

This guide contains information on how to install and configure the Identity Reporting version that comes with Identity Governance. If you want to integrate and use the version of Identity Reporting that comes with Identity Manager, you must refer to and use the Identity Manager documentation. For more information, see the *Administrator Guide to NetIQ Identity Reporting*.

To prepare for the installation of the required components, review "Planning to Install Identity Governance" on page 27 to ensure that you prepared your environment for Identity Governance. It is also important to review the latest release notes before beginning. For more information, see *Identity Governance Release Notes (https://www.microfocus.com/documentation/identity-governance/4.3/releasenotes/releasenotes.html)*. For more detailed information, see:

- Section 3.1, "Checklist for Installing Required Components," on page 46
- Section 3.2, "Understanding the Keystore for the Identity Service," on page 47
- Section 3.3, "Understanding the Encryption Keystore," on page 48
- Section 3.4, "Installing Zulu OpenJDK," on page 48
- Section 3.5, "Installing the Apache Tomcat Application Server," on page 49
- Section 3.6, "Installing or Preparing a Database Server," on page 50
- Section 3.7, "Preparing or Installing an Identity Service," on page 50
- Section 3.8, "Installing an Authentication Service," on page 51
- Section 3.9, "Securing Connections with TLS/SSL," on page 51
- Section 3.10, "Installing Optional Components," on page 53

3.1 Checklist for Installing Required Components

You must complete the steps in the following checklist before starting the Identity Governance installation.

	Checklist Items
□	1. Decide which servers you want to use for your Identity Governance components. For more information, see the following sections: ◆ Section 2.3.5, “Recommended Deployment Scenarios,” on page 37 ◆ Section 2.4.1, “Identity Governance Server System Requirements,” on page 39 ◆ Section 2.4.2, “Database Requirements,” on page 41
□	2. Review the minimum required versions for the components. For more information, see Section 2.4, “Hardware and Software Requirements,” on page 39.
□	3. Install the supported versions of Zulu OpenJDK, Apache Tomcat, a database platform, an identity service, and an authentication service before installing Identity Governance. For the installation steps, see: ◆ Section 3.4, “Installing Zulu OpenJDK,” on page 48 ◆ Section 3.5, “Installing the Apache Tomcat Application Server,” on page 49 ◆ Section 3.6, “Installing or Preparing a Database Server,” on page 50 ◆ Section 3.7, “Preparing or Installing an Identity Service,” on page 50 ◆ Section 3.8, “Installing an Authentication Service,” on page 51 For sample installation scripts, go to the product documentation site (https://www.microfocus.com/documentation/identity-governance/) and look under the References section.
□	4. Installation directories cannot contain any spaces. If you install Zulu Java OpenJDK, Apache Tomcat, or ActiveMQ in a directory with spaces, the OSP and Identity Governance installers fail.
□	5. Ensure that you have a supported identity service installed and configured. For more information, see Section 3.7, “Preparing or Installing an Identity Service,” on page 50.
□	6. Determine if you will use TLS/SSL to secure communication between the required components and OSP, Identity Governance, or Identity Reporting. If you do want to secure communication between these components, ensure that you configure the application server, identity service, and the databases for secure communication before starting the OSP, Identity Governance, or Identity Reporting installations. For more information, see Section 3.9, “Securing Connections with TLS/SSL,” on page 51.
□	7. Determine if you will install any of the optional features that require additional components to be installed. For more information, see Section 3.10, “Installing Optional Components,” on page 53.

3.2 Understanding the Keystore for the Identity Service

During installation, you must provide a password that the Identity Governance service uses for authorized interactions with the identity service. The installation process assumes that you want to use OSP or Access Manager with an LDAP server. By default, if you select **SSL** for LDAP protocol or **TLS** for audit protocol, the OSP installation program places the TLS/SSL trust certificates in the following location:

- **Linux:** `/opt/netiq/idm/apps/osp/osp-truststore.pkcs12`
- **Windows:** `c:\netiq\idm\apps\osp\osp-truststore.pkcs12`

The OSP installer provides a keystore that houses several symmetric keys and key pairs for signing, encryption, and, when necessary, TLS. The OSP keystore is located at:

- **Linux:** `/opt/netiq/idm/apps/osp/osp.pkcs12`
- **Windows:** `c:\netiq\idm\apps\osp\osp.pkcs12`

By default, the Identity Governance and the Identity Reporting installation programs place TLS/SSL trust certificates in the following locations:

- **Linux:** `/opt/netiq/idm/apps/tomcat/conf/apps-truststore.pkcs12`
- **Windows:** `c:\netiq\idm\apps\tomcat\conf\apps-truststore.pkcs12`

This file stores certificates from the following secured servers:

- Identity service when you specify https for OSP or when you use Access Manager for authentication and when the identity service is on a different server than Identity Governance or Identity Reporting
- Identity Governance server when installing only Identity Reporting, specifying https, and the server or port differs from the Identity Reporting server or port
- SMTP server when specifying SSL for use and the port is valid
- Audit server when specifying TLS
- Application server when specifying https

Both the guided and console installation modes display the certificate details and ask for confirmation of each certificate retrieved. The silent installation mode imports certificate files specified in the silent properties file.

To use SAML 2.0 authentication, you must manually install the SAML identity provider's TLS/SSL certificate in the trust store that you want to use. When using a Certificate Authority (CA) to issue certificates for the LDAP server, SAML IDP, or Advanced Identity Services, you can install the trusted root certificate of the certificate authority into the trust store and remove any server-specific certificates. For more information, see Section 4.2.2, "Considerations for Installing One SSO Provider," on page 62.

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:** `/opt/netiq/idm/apps/configupdate/configupdate.sh`
- **Windows:** `C:\netiq\idm\apps\configupdate\configupdate.bat`

Next, modify the keystore settings in the Configuration Update utility. For more information, see Section 15.1.5, "Using the Identity Governance Configuration Update Utility," on page 293.

3.3 Understanding the Encryption Keystore

Identity Governance enables you to create and store encryption keys that will be used for handling sensitive data.

During installation, you must provide a password that the Identity Governance service uses for encrypting and decrypting the Identity Governance sensitive data. By default, the installation program places the encryption keystore file in the following location:

- **Linux:** `/opt/netiq/idm/apps/tomcat/conf/encrypt-keys.pkcs12`
- **Windows:** `c:\netiq\idm\apps\tomcat\conf\encrypt-keys.pkcs12`

During installation, the installer stores the encryption keystore password file in the following locations:

- **Linux**: `/opt/netiq/idm/apps/tomcat/conf/ism-sensitive.properties`
- **Windows**: `c:\opt\netiq\idm\apps\tomcat\conf\ism-sensitive.properties`

The installer also installs the following scripts to help you with encryption key related tasks:

- `configutil` utility which includes support for encryption keystores
- `encode-password` utility to obfuscate a value that is stored in the password supplier properties file
- `encrypt-password` utility to encrypt database passwords that are stored in the `server.xml`
- `masterkey-gen` utility to either generate a new encryption key keystore, or rotate a master key within an existing encryption key keystore

IMPORTANT: After installation, copy the keystore file:

- For consistent use across other nodes and servers in a clustered and distributed environment.
- To back up the file in case of VM or server crashes. When you back up the encryption keystore file, also back up the password file.

3.4 Installing Zulu OpenJDK

Identity Governance uses Java to perform all of the processing of the data in your environment to create reports, reviews, and many other actions. You must have the Zulu OpenJDK installed and running on the same server where you install Apache Tomcat and Identity Governance. The JRE comes with the JDK.

WARNING: Identity Governance must have a supported JRE to work. Zulu OpenJDK JRE is the only version of Java that works with Identity Governance.

To install Zulu OpenJDK:

1. Ensure that you know what version of Zulu OpenJDK Identity Governance requires. For more information, see Section 2.4.1, "Identity Governance Server System Requirements," on page 39.
2. Access the Azul website and download the supported version of Zulu OpenJDK from the Zulu Community Download (https://www.azul.com/downloads/zulu-community/) web page.
3. Use the documentation for Zulu OpenJDK to install the product. For more information, see the *Zulu Installation Guide* (https://docs.azul.com/zulu/zuludocs/index.htm).
4. (Optional) Create and use a common directory for the Zulu OpenJDK installation such as:
    - **Linux:** `/opt/netiq/idm/apps/java`
    - **Windows:** `C:\netiq\idm\apps\java`
5. Record the installation path to use when installing Identity Governance and OSP.

3.5 Installing the Apache Tomcat Application Server

Identity Governance uses Apache Tomcat to host and run the user interface, which allows users to access and use Identity Governance without having to install a client. You must install Apache Tomcat on the same server where you install Zulu OpenJDK and Identity Governance. Use the following information to help you install Apache Tomcat.

- Section 3.5.1, "Prerequisites for the Apache Tomcat Application Server," on page 49
- Section 3.5.2, "Installing Apache Tomcat," on page 49
- Section 3.5.3, "Starting and Stopping Apache Tomcat," on page 50

3.5.1 Prerequisites for the Apache Tomcat Application Server

Review the following considerations before installing Apache Tomcat:

- We highly recommend that you configure Apache Tomcat to use https with either TLSv1.2 or TLS1.1. Any prior version of TLS should not be used. For more information, see "SSL/TLS Configuration How-To".
- (Conditional) If you use Linux, do not run Apache Tomcat as `root`. Best practice for security on Linux is to not install programs as `root` and use an administrator account with privileges to install products instead.

3.5.2 Installing Apache Tomcat

You must install Apache Tomcat on the same server that has Zulu OpenJDK installed and where you will install Identity Governance.

1. Ensure that you install the version of Apache Tomcat that Identity Governance requires. For more information, see Section 2.4.1, "Identity Governance Server System Requirements," on page 39.
2. Access the Apache Tomcat website (http://tomcat.apache.org/) and download the supported version.

3 Use the documentation for the supported version of Apache Tomcat (https://tomcat.apache.org/) to complete the installation.

4 (Optional) Create and use a common directory for the Apache Tomcat installation such as:

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

5 Ensure that you configure TLSv1.2 or TLSv1.1 for https communication. For more information, see “SSL/TLS Configuration How-To”.

6 Record the installation path for Apache Tomcat to use when installing Identity Governance, OSP, and Identity Reporting.

3.5.3 Starting and Stopping Apache Tomcat

When you make configuration changes for Identity Governance, you must either restart, or stop and start Apache Tomcat to have the changes take effect. If you used the installation scripts we provided to install Apache Tomcat, you use different commands to restart Apache Tomcat. For more information, see Section B.1, “Stopping, Starting, and Restarting the Apache Tomcat Service,” on page 315.

3.6 Installing or Preparing a Database Server

Identity Governance requires that you have a database server or a database instance running the specific version of the supported database platform before starting the Identity Governance installation. If you are installing Identity Governance with Identity Reporting or Workflow Engine, then you must have specific databases with specific names for each product. You can use an existing database server or instance, but have the option to create the required databases. For more information, see Chapter 5, “Creating Databases for Identity Governance and Components,” on page 95

Ensure that you have a supported database installed and running that meets the system requirements. For the supported databases, see Section 2.4.2, “Database Requirements,” on page 41.

3.7 Preparing or Installing an Identity Service

Identity Governance requires that you have an identity service that stores the authorized users that log in to and use Identity Governance. Identity Governance supports:

- Active Directory
- eDirectory
- Identity Manager Identity Vault
- Active Directory Federation Server (AD FS) back by eDirectory or Active Directory

You can install Identity Governance without an LDAP directory installed, configured, and populated with user accounts if you use a file-based bootstrap administrator account to perform the installation and basic configuration. For more information, see “Understanding the Bootstrap Administrator for Identity Governance” on page 14.

We recommend that you configure the LDAP directory to communicate over LDAP over SSL (LDAPS) to ensure that the authorized users' credentials are kept secure. The Identity Governance installer can configure Identity Governance to communicate over LDAPS with the LDAP directory when you provide the DNS host name, port, and administrator credentials for the LDAP directory during the installation. The LDAP directory must be populated with user accounts that have passwords and must be configured to use LDAPS so that the installer can get the proper information to establish the secure connection.

Ensure that you either use the bootstrap administrator account for the installation of Identity Governance or have the LDAP directory installed, configured to use LDAPS, and populated with the user accounts and passwords of the authorized users for Identity Governance.

Using AD FS with OSP requires additional configuration steps that must performed after you install OSP. For more information, see Section 9.2.3, "Configuring OSP to Work with AD FS," on page 205.

3.8 Installing an Authentication Service

Identity Governance requires that you configure an authentication service for the users that access and use consoles for Identity Governance. The authentication service allows you to configure how the users authenticate to provide single sign-on (SSO) access and to increase security. Identity Governance supports OSP and Access Manager as authentication services. For more information, see Chapter 4, "Installing an Authentication Service," on page 57.

3.9 Securing Connections with TLS/SSL

Identity Governance handles user account information, permissions, and other sensitive data. You want to ensure that all communication channels between Identity Governance and the other components are secure using the Transport Layer Security/Secure Sockets Layer (TLS/SSL) protocol. This ensures that any data that Identity Governance gathers for reviews, reports, or any other activity is secure from eavesdropping or tampering from external sources.

Use the following information to understand the different communication paths and how to secure them for secure communication with Identity Governance.

- Section 3.9.1, "Understanding Secure Communication with Identity Governance," on page 51
- Section 3.9.2, "Securing Communications with Apache Tomcat," on page 52
- Section 3.9.3, "Securing Connections to the Identity Service," on page 52
- Section 3.9.4, "Securing Communications to the Database Server," on page 53
- Section 3.9.5, "Securing Communications with the SMTP Server," on page 53
- Section 3.9.6, "Securing Communications with the Audit Server," on page 53

3.9.1 Understanding Secure Communication with Identity Governance

Use the TLS/SSL protocol to secure the following types of network connections:

- **HTTPS:** Provides secure end-user access to and from Identity Governance. You would configure the application server (Apache Tomcat) to communicate over https instead of http.

- **LDAPS:** Ensures that the communication between the authentication provider and the identity service is secure. You would configure OSP or Access Manager to use the certificates from the LDAP directory to communicate securely with the LDAP directory for the authorized users.
- **JDBC:** Ensures that the communication between Identity Governance and the database server is secure.
- **SMTP:** Ensures that the email notifications Identity Governance, Identity Reporting, and Workflow Engine sends are secure.

By default, the Identity Governance installer does not enable secure communications. You must enable it during the installation or after the installation. You enable the secure communications by selecting **https** when you define the application server and the identity service.

If you have configured the components for secure communication using TLS/SSL, the Identity Governance installer imports the correct certificates from these locations to the trust store for Identity Governance when you select to communicate over TLS/SSL. We highly recommend that you configure these components to communicate over TLS/SSL in a production environment. Use the following information to enable TLS/SSL communication for these products before starting the OSP, Identity Governance, or the Identity Reporting installations.

If you do install OSP, Identity Governance, Identity Reporting, or Workflow Engine without configuring these components to communicate securely using TLS/SSL, you can configure secure communication at a later time using the configuration utilities. For more information, see Section 12.1, “Configuring SSL/TLS Communication after the Installation,” on page 253.

3.9.2 Securing Communications with Apache Tomcat

Each server that has OSP, Identity Governance, Identity Reporting, and Workflow Engine installed must have Apache Tomcat configured for https communication to provide secure communication between all of the separate Identity Governance components.

If you use Access Manager instead of OSP as the authentication service, the Identity Governance installer assumes Access Manager is configured to communicate over its default “https”. The Identity Governance installer prompts you for the ports for the Access Manager Identity Server and the Access Manager administration console. The Identity Governance installer automatically retrieves the certificates from Access Manager before prompting you to accept them into the Identity Governance keystore.

To configure the application server to use TLS/SSL, you configure Apache Tomcat to use TLS/SSL. We highly recommend that you configure Apache 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.”

3.9.3 Securing Connections to the Identity Service

To configure the identity service to use TLS/SSL, you configure the LDAP server that contains the authorized Identity Governance users to use LDAPS. For more information, see:

- **Active Directory:** Step by Step Guide to Setup LDAPS on Windows Server (https://blogs.msdn.microsoft.com/microsoftrservertigerteam/2017/04/10/step-by-step-guide-to-setup-ldaps-on-windows-server/)
- **eDirectory:** “Authentication and Security” in the *eDirectory Administration Guide*

3.9.4 Securing Communications to the Database Server

To configure the database for your environment to communicate securely, you must configure the database to communicate over JDBC using TLS/SSL. For more information, see:

- **Microsoft SQL:** "Enabling Encrypted Connections to the Database Engine (https://docs.microsoft.com/en-us/sql/database-engine/configure-windows/enable-encrypted-connections-to-the-database-engine?view=sql-server-2017)"
- **Oracle:** "Keeping Your Oracle Database Secure (https://docs.oracle.com/en/database/oracle/oracle-database/19/dbseg/keeping-your-oracle-database-secure.html#GUID-ED169179-BB00-4C1E-9C2D-C7C30CC4E6CA)"
- **PostgreSQL:** "Secure TCP/IP Connections with SSL (https://www.postgresql.org/docs/10/ssl-tcp.html)"
- **Vertica:** "TLS Protocol (https://www.vertica.com/docs/9.2.x/HTML/Content/Authoring/Security/SSL/ImplementingSSL.htm)"

3.9.5 Securing Communications with the SMTP Server

To provide secure emails for email notifications you must configure the SMTP server for secure communications. Follow the documentation for your specific SMTP server to enable secure communications before starting the installation.

3.9.6 Securing Communications with the Audit Server

To provide secure communications between OSP, Identity Governance, Identity Reporting and Workflow Engine with the audit server, you must configure the audit server to communicate over TLS/SSL. The OSP, Identity Governance, and the Identity Reporting installers can import the trusted certificate from the audit server during the installation. See the documentation for your audit server on how to enable secure communications with external applications.

3.10 Installing Optional Components

Identity Governance provides additional features that increase the capabilities of Identity Governance. These features are Identity Reporting, Workflow Engine, Auditing, and email notifications. If you want this additional functionality, use the following information to prepare the server or servers to enable these features.

- Section 3.10.1, "Understanding the Identity Reporting Installation," on page 54
- Section 3.10.2, "Understanding the Workflow Engine Installation," on page 54
- Section 3.10.3, "Understanding the Auditing Installation," on page 55
- Section 3.10.4, "Understanding Enabling Email Notifications," on page 56

3.10.1 Understanding the Identity Reporting Installation

Identity Reporting is an optional feature for Identity Governance. The Identity Reporting installer is part of the Identity Governance installer. Depending on your environment, you can install Identity Reporting on the Identity Governance server or on a separate server. If you choose to install Identity Reporting on a separate server, run the Identity Governance installation and be sure that you select only the option to install Identity Reporting.

One of the first options the Identity Governance presents is whether you want to install Identity Governance, Identity Governance and Identity Reporting, or only Identity Reporting. You must choose if you want to install Identity Reporting and how you want to install Identity Reporting before starting the Identity Governance installation. For more information, see Section 2.3, "Recommended Production Environment Installation Scenarios," on page 32.

- ❒ Install Zulu OpenJDK. For more information, see Section 3.4, "Installing Zulu OpenJDK," on page 48.
- ❒ Install Apache Tomcat. For more information, see Section 3.5, "Installing the Apache Tomcat Application Server," on page 49.
- ❒ (Conditional) Configure Apache Tomcat for TLS/SSL communication if you choose to have secure communication between Identity Governance and Identity Reporting. For more information, see Section 3.9, "Securing Connections with TLS/SSL," on page 51.

The Identity Reporting installer prompts for the URL access information for the Identity Reporting server. You are asked for this information before you install Identity Reporting on the separate server. This is why you must have Zulu OpenJDK and Apache Tomcat installed on the separate server.

There are additional tasks you must perform on the separate server before starting the Identity Reporting installation. For more information, see Chapter 7, "Installing Identity Reporting," on page 163.

3.10.2 Understanding the Workflow Engine Installation

The Workflow Engine is an optional feature for Identity Governance. The Workflow Engine installer is part of the Identity Governance installer. Depending on your environment, you can install the Workflow Engine on the Identity Governance server or a separate server. If you choose to install the Workflow Engine on a separate server, run the Identity Governance installation and be sure that you select only the option to install Workflow Engine.

The Identity Governance installer presents the following options for installation:

- Identity Governance only
- Identity Governance and Identity Reporting
- Identity Reporting only
- Workflow Engine only
- Identity Reporting and Workflow Engine
- Identity Governance and Workflow Engine
- Identity Governance, Identity Reporting, and Workflow Engine

You must determine whether to install the Workflow Engine and how you want to install it before starting the Identity Governance installation. For more information, seeSection 2.3.1, “Identity Governance in a New Environment,” on page 32.

- ❐ Install Zulu OpenJDK. For more information, see Section 3.4, “Installing Zulu OpenJDK,” on page 48.
- ❐ Install Apache Tomcat. For more information, see Section 3.5, “Installing the Apache Tomcat Application Server,” on page 49.
- ❐ (Conditional) Configure Apache Tomcat for TLS/SSL communication if you choose to have secure communication between Identity Governance and Identity Reporting. For more information, see Section 3.9, “Securing Connections with TLS/SSL,” on page 51.
- ❐ Install ActiveMQ. For more information, see Chapter 3, “Installing Required Components,” on page 45.

There are additional tasks you must perform on the separate server that will host the Workflow Engine before starting the Workflow Engine installation. For more information, see Chapter 8, “Installing Workflow Engine,” on page 183.

3.10.3 Understanding the Auditing Installation

OSP, Identity Governance, Identity Reporting, and Workflow Engine provide CEF auditing files you can send to an audit server through `syslog`. The installers for OSP, Identity Governance, Identity Reporting, and Workflow Engine prompt you if you want to enable auditing. If you select to enable auditing, you must provide the DNS name and port to the audit server. The installers also prompt if you want to communicate securely.

You can enable auditing after the installation of OSP, Identity Governance, Identity Reporting, and Workflow Engine. If you have the audit server installed and configured for TLS/SSL communication before starting the installations, the installers prompt you for the connection information to the audit server and the installers can also import the certificates from the audit server to enable TLS/SSL. To enable auditing during the installations:

- ❐ Install a supported audit server. For more information, see Section 2.4.6, “Audit Server System Requirements,” on page 43.
- ❐ (Conditional) Configure the audit server to communicate securely by enabling TLS/SSL on the audit server. For more information, see Section 3.9, “Securing Connections with TLS/SSL,” on page 51.

To enable auditing after the installations complete, see Section 12.4, “Configuring Auditing after the Installation,” on page 256.

3.10.4 Understanding Enabling Email Notifications

Identity Governance sends email notifications to authorized users who can take action through those notifications. To enable email notifications you must have an SMTP server installed and configured. The Identity Governance installer allows you to configure the SMTP server while installing Identity Governance, Identity Reporting or the Workflow Engine. To guarantee the delivery of the emails, you must install ActiveMQ on the server that runs Identity Governance.

You can enable email notification after the installation of the products. However, if you do not provide configuration details during installation, the Identity Governance installer adds default values that you can change through the Identity Governance Configuration Update utility. To configure the email notifications during the installation:

- ❒ Install and configure an SMTP server.
- ❒ (Conditional) Configure the SMTP server for secure communications over TLS/SSL. For more information, see Section 3.9, “Securing Connections with TLS/SSL,” on page 51.
- ❒ If you are installing Identity Governance, Identity Reporting, and Workflow Engine together the installer prompts you for the SMTP server information only once.

To enable email notification after the installation is complete, see Section 12.5, “Enabling Email Notifications after the Installation,” on page 261.

4 Installing an Authentication Service

This section provides information about installing an authentication service, such as One SSO Provider (OSP) or Access Manager, which Identity Governance uses for login authentication and allows you to configure Identity Governance for single sign-on (SSO) access.

Identity Governance requires one of the following scenarios for the authentication service:

- OSP
- Access Manager
- Access Manager configured to connect to OSP

Ensure that the version of OSP and Identity Governance you use is supported. For more information, see Section 2.4, "Hardware and Software Requirements," on page 39.

IMPORTANT: Identity Governance always uses an authentication service as the login mechanism, even in a non-SSO environment. You must have OSP or Access Manager installed before installing Identity Governance.

You must understand the Identity Governance authentication process before you start any installation or integration. Next, you must select whether to use OSP, Access Manager, or Access Manager with OSP as your authentication service for Identity Governance.

Use the following information to determine which authentication service works best for your environment, and then use the appropriate section to either install OSP or integrate Access Manager with Identity Governance.

- Section 4.1, "Understanding Authentication for Identity Governance," on page 57
- Section 4.2, "Installing OSP for Identity Governance," on page 61
- Section 4.3, "Integrating Access Manager with Identity Governance," on page 78

4.1 Understanding Authentication for Identity Governance

To verify the identity of users who log in to Identity Governance, you need an LDAP identity service and an authentication service. These two items allow Identity Governance to control who has access to the Identity Governance resource. The authentication service allows you to enable SSO for the Identity Governance users or provide additional authentication methods such as two-factor authentication.

Identity Governance supports Active Directory and eDirectory as identity services and One SSO Provider (OSP) and Access Manager as authentication services. For example, you can use the Identity Vault for Identity Manager as an identity service. Users can log in to Identity Governance immediately after installation if the users in the specified containers of the identity service have passwords for the users' accounts. However, the accounts cannot do much until the bootstrap administrator account assigns access rights to the features in Identity Governance.

The bootstrap administrator is the only account that can log in immediately after the installation and make configuration changes.

- Section 4.1.1, “Using the Bootstrap Administrator,” on page 58
- Section 4.1.2, “Understanding Authentication with SSO,” on page 59
- Section 4.1.3, “Using OSP for Authentication,” on page 61
- Section 4.1.4, “Using Access Manager for Authentication,” on page 61
- Section 4.1.5, “Using Access Manager with OSP for Authentication,” on page 61

4.1.1 Using the Bootstrap Administrator

During installation, you can create a **bootstrap administrator** account that can immediately log in and configure Identity Governance. This account is useful if you do not have an identity service populated with user accounts before installing Identity Governance.

NOTE: The name for the bootstrap administrator account must be unique. Do not duplicate the name of any accounts, the root container, or subtrees that you use for authentication. The default file-based bootstrap administrator account name is `igadmin`. You can specify an alternative name for this account through the bootstrap administrator script. Do not use “admin” or “administrator” for the account name.

During the installation, you select one of two methods to create a bootstrap administrator account. You must select one of the options. The options are:

- **File:** If the bootstrap administrator account is file-based, this account does not link to any account in the LDAP directory. This account exists in a file that the installer for OSP creates for you. The default name of the file that contains the bootstrap administrator account is `adminusers.txt`. The default bootstrap administrator account name is `igadmin`.The file-based bootstrap administrator account can access all items in the administration console except for **Reviews** and **Access Request**.

  If you selected to use the LDAP-based bootstrap administrator and want to move back to file-base, you must use a script included in the Identity Governance product to make this change. For more information, see “Creating a Bootstrap Administrator Using a Script” on page 294.

  You should not continue using the file-based bootstrap administrator account after you have Identity Governance running in a production environment. As soon as you have collected user accounts in Identity Governance, assign one of the collected LDAP accounts as a global administrator. For more information about assigning authentications, see “Global Authorizations ” in *Identity Governance User and Administration Guide*.
- **LDAP:** If you have not performed a data collection on the LDAP directory where the LDAP-based bootstrap administrator resides or mapped this account to an identity in Identity Governance, the LDAP-based bootstrap administrator account has limited rights. When you have performed a data collection on the LDAP directory or mapped this account to an identity in Identity Governance, Identity Governance adds the Identity Governance Global Administrator role to this LDAP-based bootstrap administrator account and it has unrestricted access.

  The restricted LDAP-based bootstrap administrator account can access all items in the administration console except for **Reviews** and **Access Request**. After you collect and publish the data from a data source and you map the LDAP-based bootstrap administrator account to an identity in Identity Governance, Identity Governance changes the restricted LDAP-based bootstrap administrator account into a full global administrator account. For more information, see “Global Authorizations ” in the *Identity Governance User and Administration Guide*.

IMPORTANT: Due to access to the file system and security updates for Identity Governance 3.6 or later you cannot always use the file-based bootstrap administrator account.

If your environment matches any of the following conditions, you must always use the LDAP-based bootstrap administrator account.

- Integrated with Identity Manager
- Using SAML authentication method
- Using Access Manager as the authentication service
- Not using OSP as the authentication service

The silent installation, guided installation, and the console installation can create the bootstrap administrator account for you or you can use a script to create the account. For more information, see Section 15.2.1, “Creating a Bootstrap Administrator Using a Script,” on page 294.

4.1.2 Understanding Authentication with SSO

Identity Governance allows the following authentication service configurations to achieve SSO in your environment:

- OSP
- Access Manager
- Access Manager connecting to OSP with SAML

The OSP authentication service supports the OAuth2 specification and requires an LDAP identity service. Identity Governance works with eDirectory, Identity Manager Identity Vault, and Microsoft Active Directory. You must deploy the identity service before you install Identity Governance. For more information, see Section 3.7, “Preparing or Installing an Identity Service,” on page 50.

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.

Access Manager supports several authentication methods, such as name/password, RADIUS token-based authentication, X.509 digital certificates, Kerberos, risk-based authentication, Time-Based One-Time Password (TOTP), social authentication, and OpenID Connect. Plus, Access Manager can integrate with Advanced Authentication to provide many more authentication methods.

How do OSP, Access Manager, and SSO work?

If you use Identity Manager Identity Vault as your identity service, users with the names (CN) 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 it requires authentication and temporarily redirects the browser to the OSP or to the Access Manager authentication service. The OSP service or the Access Manager service authenticates the user by asking the configured authentication method for the user. The authentication service 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 the authentication service work with Kerberos?

The authentication service 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, authentication occurs automatically and without the user’s intervening.

Identity Governance allows you to configure the users’ logout experiences to be the same. If the option **Use Logout Landing page** is set to **True**, the users in a Kerberos environment can log out and the authentication service does not reauthorize the users. Identity Governance presents the users 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 users to the login window and the authentication service reauthorizes the users’ sessions.

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 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 results in the browser displaying the "logged out" page for the IDP. For more information, see Section 10.3, “Using SAML Authentications from Access Manager to Provide Single Sign-On to Identity Governance through the OSP,” on page 226.

How do I set up authentication and SSO access for OSP or Access Manager?

For OSP or Access Manager and SSO to function, you must install OSP or install and configure Access Manager. Next, specify the URLs for client access to each component, the URL that redirects validation requests to OSP or Access Manager, and the settings for the Identity Vault. 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. For more information, see Chapter 10, “Configuring Authentication Options for Identity Governance,” on page 221.

4.1.3 Using OSP for Authentication

Identity Governance can use the OSP authentication service, which supports the OAuth2 specification. With OSP, you can provide SSO 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.

IMPORTANT: Identity Governance always uses an authentication service as the login mechanism, even in a non-SSO environment.

4.1.4 Using Access Manager for Authentication

Identity Governance can use the Access Manager authentication service, which supports several authentication methods. For a list of the authentication methods, see the Access Manager documentation. With Access Manager, you can provide SSO access among Identity Governance and other applications, such as Identity Manager Home and Provisioning Dashboard. All requests to Access Manager use the HTTP or HTTPS protocols.

IMPORTANT: Identity Governance always uses an authentication service as the login mechanism, even in a non-SSO environment.

4.1.5 Using Access Manager with OSP for Authentication

Identity Governance can use Access Manager to connect with OSP as the authentication service. With Access Manager, you can provide SSO access among Identity Governance and other applications in your environment that use Access Manager for authentication. For more information, see "Configuring Single Sign-On to Specific Applications" in the *NetIQ Access Manager 5.0 Administration Guide*.

IMPORTANT: Identity Governance always uses an authentication service as the login mechanism, even in a non-SSO environment.

4.2 Installing OSP for Identity Governance

Use the following information to install One SSO Provider (OSP) for Identity Governance. If you are going to use Access Manager as the authentication services, skip the following sections and proceed to Section 4.3, "Integrating Access Manager with Identity Governance," on page 78.

- Section 4.2.1, "Checklist for Installing One SSO Provider," on page 62
- Section 4.2.2, "Considerations for Installing One SSO Provider," on page 62
- Section 4.2.3, "OSP Installation Worksheet," on page 63
- Section 4.2.4, "Installing One SSO Provider (OSP)," on page 72
- Section 4.2.5, "Silently Installing One SSO Provider," on page 73

4.2.1 Checklist for Installing One SSO Provider

You must complete the steps in the following checklist to complete the OSP installation:

	Checklist Items
❑	1. Decide where to deploy OSP and the required components in relation to your Identity Governance components. For more information, see Section 2.3, “Recommended Production Environment Installation Scenarios,” on page 32.
❑	2. Decide whether you want to install Identity Governance and the authentication service in a clustered environment. For more information about the requirements, see Section 2.3.4, “Ensuring High Availability or Load Balancing for Identity Governance,” on page 35.
❑	3. Review the considerations for before installing OSP. For more information, see “Considerations for Installing One SSO Provider” on page 62
❑	4. Ensure that Apache Tomcat has been installed on the server where you install OSP. For more information, see Chapter 3, “Installing Required Components,” on page 45.
❑	5. Ensure that you have an identity service installed and configured. If you are in a production environment ensure that you have configured the identity service for SSL/TLS communication. For more information, see Section 3.9, “Securing Connections with TLS/SSL,” on page 51.
❑	6. Decide which installation method to use. For more information, see Section 1.2, “Understanding the Installation Methods,” on page 18.
❑	7. The installation directory for OSP cannot contain any spaces in the name. If it does contain spaces, the installation fails.
❑	8. Ensure that you fill out the OSP Installation Worksheet before starting the installation. The worksheet helps you gather the required information to complete the installation. You use the information you gather for the guided, console, and silent installation method. For more information, see Section 4.2.3, “OSP Installation Worksheet,” on page 63.
❑	9. You must manually extend the schema for eDirectory or Active Directory to allow OSP authentications to work. If you integrate with Identity Manager you can skip this step. For more information, see Section 9.2.2, “Extending the Schema for OSP in the Identity Service not Part of Identity Manager,” on page 205.

4.2.2 Considerations for Installing One SSO Provider

Before installing OSP, review the following considerations:

- ❑ (Conditional) If you intend to utilize the OSP installed with Identity Manager, confirm that the version of OSP provided by Identity Manager is supported with this version of Identity Governance. For more information, see Section 2.4, “Hardware and Software Requirements,” on page 39.
- ❑ (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 identity service, a SAML provider, or one or more Advanced Authentication servers. For more information, see Section 3.2, “Understanding the Keystore for the Identity Service,” on page 47.

❒ OSP requires several generated symmetric keys along with public/private key pairs for signing, encryption, and TLS for use during normal operations to generate other key material. The installation program automatically creates the symmetric keys and key pairs and places them in the `osp.pkcs12` file.

❒ OSP also requires encryption keys for sensitive data encryption. The installation program creates these keys and places them in the `encrypt-keys.pkcs12` file.

❒ (Conditional) If you set up multiple instances of OSP for use in a high availability cluster, copy the `osp.pkcs12` and encrypt-keys.pkcs12 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 keys on each member server in the cluster.

❒ (Optional) If you want to enable auditing for OSP, you must configure the audit server to use TLS before beginning the OSP installation so that the OSP installer can connect to the audit server and retrieve the audit server's certificate to add to the local keystore.

4.2.3 OSP Installation Worksheet

Use the following worksheet to gather the required information to successfully complete the OSP installation. You use the information that you gather with the guided installation, the console installation, and the silent installation. Select one of the installation methods to install OSP and use the worksheet so that you do not have to pause during the installation to find the required information.

Table 4-1 *OSP Installation Worksheet*

Item	Description	Value
Installation Location	Specify the installation path for OSP. **WARNING:** Spaces in the names of the directories in the path are not supported. The default location is: ◆ **Linux:** `/opt/netiq/idm/apps/osp` ◆ **Windows:** `C:\netiq\idm\apps\osp`	
Apache Tomcat Details		
Apache Tomcat Home Directory	Specify the path to the Apache Tomcat home directory. **WARNING:** Spaces in the names of the directories in the path are not supported. The installation process adds some files for OSP to this folder. The default location is: ◆ **Linux:** `/opt/netiq/idm/apps/tomcat` ◆ **Windows:** `c:\netiq\idm\apps\tomcat`	

Item	Description	Value
Java Home Directory for Apache Tomcat	Specify the path to the Zulu JRE home directory. The Zulu JRE is installed when you install the Zulu OpenJDK. The installation process uses Java for several processes, such as to run commands and create security stores. **WARNING:** Spaces in the names of the directories in the path are not supported. The default location is: ◆ **Linux:** `/opt/netiq/idm/apps/jre` ◆ **Windows:** `c:\netiq\idm\apps\jre`	
Application Address for OSP	Specify the address of the application that represents the settings of the URL that users need to connect to OSP. For example, `https://myserver.mycompany.com:8443`. The installation program creates several symmetric keys and key pairs for signing, encryption, and TLS, which it places in the `osp.pkcs12` file. The TLS key pair also specifies the host name as part of its distinguished name.	
Application Address for OSP > Protocol	Select if you want the users to access a secure OSP URL for authentication to Identity Governance or not. Select `http` for an unsecure URL or select `https` for a secure URL. If you select `https`, ensure that you have configured Apache Tomcat to use TLS/SSL on the server that runs OSP before starting the OSP installation. For more information, see Section 3.9, “Securing Connections with TLS/SSL,” on page 51.	

Item	Description	Value
Application Address for OSP > Host Name	**WARNING:** Use the fully qualified domain name (FQDN) name rather than localhost or an IP address. In a non-clustered environment, specify the DNS name of the Apache Tomcat server for OSP. In a clustered environment, specify the DNS name of the server that hosts the load balancer for OSP. For more information about installing in a clustered environment, see Section 2.3.4, “Ensuring High Availability or Load Balancing for Identity Governance,” on page 35.	
Application Address for OSP > Port	Specify the port that you want OSP to use for communication with the Identity Governance clients. When installing in a clustered environment, specify the port for the load balancer.	
Encryption Keystore	Specify if you want to create a new encryption keystore file or use an existing file. Create a new file when you are installing OSP for the first time. The installation process creates a `pkcs12` file used for encryption. The file is saved in the `opt/netiq/idm/apps/tomcat/conf` folder by default. Note that the same encryption keys must be used for all subsequent product installations regardless of a same server or distributed server deployment scenarios. Use the existing keystore when you have multiple instances of OSP installed in a clustered environment. In such scenario, copy the `pkcs12` encrypt file from the installed location of the first server to the other servers, then during installation, navigate to the location where you had copied the keystore file so that the sensitive data generated by each server installation is encrypted with the same encryption keys.	

Item	Description	Value
Encryption Keystore Password	Specify the password for the keystore. Note that the same encryption password must be used for all subsequent product installations regardless of a same server or distributed server deployment scenarios.	
Customize the Login Screen	(Optional) Specify a name that represents the organization name that users see on the login screen. 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 to pseudo-tags `[apos]` and `[nbsp]`, respectively ◆ To insert a copyright symbol, type `(R)`, which is converted to the pseudo-tag `[reg]`. ◆ To insert a trademark symbol, type `(TM)`, which is converted to the pseudo-tag `[tm]`. ◆ An ampersand is converted to the pseudo-tag `[amp]`. ◆ To insert a line break, type \\r\\n, which is converted to the pseudo-tag `[br]`. ◆ The plus sign is converted to the pseudo-tag `[plus]`.	
Expected Setup	Select where Identity Governance, Identity Reporting, and Workflow Engine reside in regard to the OSP installation. The options are **external**, **local**, and **none**. If you select external for Identity Governance or Identity Reporting or Workflow Engine you must gather the following information that allows OSP to communicate with these products.	

Item	Description	Value
(Conditional) External Identity Governance Details > Protocol	Select whether you want OSP to communicate to Identity Governance securely or not. Select `http` for unsecure communications or select `https` for secure communications. If you select `https`, ensure that you have configured Apache Tomcat to use TLS/SSL on the server that runs Identity Governance before starting the OSP installation. For more information, see Section 3.9, “Securing Connections with TLS/SSL,” on page 51.	
(Conditional) External Identity Governance Details > Host Name	**IMPORTANT:** Do not use `localhost` or the IP address. In a non-clustered environment, specify the DNS name of the Apache Tomcat server for Identity Governance. In a clustered environment, specify the DNS name of the server that hosts the load balancer for Identity Governance. For more information about installing in a clustered environment, see Section 2.3.4, “Ensuring High Availability or Load Balancing for Identity Governance,” on page 35.	
(Conditional) External Identity Governance Details > Port	Specify the port that you want OSP to use for communication with Identity Governance. When installing in a clustered environment, specify the port for the load balancer.	
(Conditional) External Identity Governance Details > Client Password	Specify a client password. The **Client Password** is the OAuth 2.0 password Identity Reporting uses for the various SSO clients. After the installation, you can change this password for each client through the Identity Governance Configuration Update utility.	
(Conditional) External Identity Governance Details > Database Host Name	Specify the DNS name of the database server. **WARNING:** If you use the IP address of the database server, rather than the DNS name, the installation may not succeed.	
(Conditional) External Identity Governance Details > Database Port	Specify the port the database server uses to communicate. The default port is: ◆ Microsoft SQL: 1433 ◆ Oracle: 1521 ◆ PostgreSQL: 5432	

Item	Description	Value
(Conditional) External Identity Reporting Details > Protocol	Specify the details for the URL and client password to connect OSP to the Identity Reporting server. These are the Apache Tomcat details that host Identity Reporting.	
(Conditional) External Identity Reporting Details > Host Name	**IMPORTANT:** Do not use `localhost` or the IP address. In a non-clustered environment, specify the DNS name of the Apache Tomcat server for Identity Reporting. In a clustered environment, specify the DNS name of the server that hosts the load balancer for Identity Reporting. For more information about installing in a clustered environment, see Section 2.3.4, "Ensuring High Availability or Load Balancing for Identity Governance," on page 35.	
(Conditional) External Identity Reporting Details > Port	Specify the port that you want OSP to use for communication with Identity Reporting. When installing in a clustered environment, specify the port for the load balancer.	
(Conditional) External Identity Reporting Details > Client Password	Specify a client password. The **Client Password** is the OAuth 2.0 password Identity Governance uses for the various SSO clients. After the installation, you can change this password for each client through the Identity Governance Configuration Update utility.	
(Conditional) External Workflow Engine Details > Protocol	Specify the details for the URL and client password to connect OSP to the Workflow Engine server. These are the Apache Tomcat details that host Workflow Engine.	
(Conditional) External Workflow Engine Details > Host Name	**IMPORTANT:** Do not use `localhost` or the IP address. In a non-clustered environment, specify the DNS name of the Apache Tomcat server for Workflow Engine. In a clustered environment, specify the DNS name of the server that hosts the load balancer for Workflow Engine. For more information about installing in a clustered environment, see Section 2.3.4, "Ensuring High Availability or Load Balancing for Identity Governance," on page 35.	

Item	Description	Value
(Conditional) External Workflow Engine Details > Port	Specify the port that you want OSP to use for communication with Workflow Engine. When installing in a clustered environment, specify the port for the load balancer.	
(Conditional) External Workflow Engine Details > Client Password	Specify a client password. The **Client Password** is the OAuth 2.0 password Identity Governance uses for the various SSO clients. After the installation, you can change this password for each client through the Identity Governance Configuration Update utility.	
Bootstrap Administrator Details	Select whether you want to use the file-based bootstrap administrator or the LDAP-based bootstrap administrator. For more information, see Section 4.1.1, “Using the Bootstrap Administrator,” on page 58	
(Conditional) File-Based Bootstrap Administrator	If you select **File-Based Bootstrap Administrator**, you must provide a name and a password for the bootstrap administrator. The default name is `igadmin`. **IMPORTANT:** If you are using SAML authentication for your users or Access Manager, you must select the **LDAP-Based Bootstrap Administrator** option. The file-based bootstrap administrator does not work in those scenarios.	
(Conditional) LDAP-Based Bootstrap Administrator	If you select **LDAP-Based Bootstrap Administrator**, you must then provide details about the LDAP identity service so that Identity Governance can access and communicate with this server to authenticate the authorized users. **IMPORTANT:** If you are using SAML authentication for your users or Access Manager, you must select the **LDAP-Based Bootstrap Administrator** option. The file-based bootstrap administrator does not work in those scenarios.	
Identity Service Details	Specify the information for the Identity Vault (LDAP server). For more information, see “Understanding the Identity Service” on page 14.	

Item	Description	Value
LDAP Host	Specify the DNS name of the LDAP identity service that contains the distinguished names of your user accounts. **IMPORTANT:** Do not use `localhost` unless you want to specify a CSV file instead of an identity service. (Test environments only)	
LDAP Port	Specify the port that you want the LDAP identity service to use for communication with Identity Governance. For example, specify 389 for a non-secure port or 636 for TLS/SSL connections.	
Use SSL	Select this option if the LDAP server communicates over TLS/SSL. You must have configured the LDAP server to use TLS/SSL before starting the OSP installation. For more information, see Section 3.9, “Securing Connections with TLS/SSL,” on page 51.	
Trust Store Secret	Specify the password for the trust store. The trust store is empty unless you select to use SSL for LDAP or audit.	
Admin DN	*Applies only when installing a new identity service.* Specify the distinguished name of the LDAP administrator account that Identity Governance uses to access the LDAP identity service. For example, `cn=admin,ou=sa,o=system`.	
Admin Password	*Applies only when installing a new identity service.* Specify the password of the LDAP administrator account.	
User Container	*Applies only when installing a new identity service.* Specify the distinguished name of the LDAP container where the user accounts reside. These are the authorized users that can access and use Identity Governance. Identity Governance uses this as the top container when it searches for users. For example, `ou=users,o=system`.	

Item	Description	Value
Admin Container	*Applies only when installing a new identity service.* Specify the distinguished name of the container where the administrator account resides. If it is the same container where all user accounts resides, specify that name. For example, `ou=sa,o=system`.	
(Conditional) Identity Service	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 or eDirectory. If this test is unsuccessful, then the installer prompts you to select the LDAP server type. The options are **Active Directory** or **eDirectory**.	
(Optional) Enable Auditing	Select this option and gather the following information if you want to enable auditing for OSP.	
Enable Auditing > Audit Server	**IMPORTANT:** Do not use `localhost` or the IP address. Specify the host name of the audit server.	
Enabling Auditing > Audit Port	Specify the port to use for communications to the audit server. The default port is 6514.	
Enabling Auditing > Audit Cache Location	Specify a local directory on the OSP server for caching of audit events before they are sent to the audit server. The default directory is: ◆ **Linux:** `/opt/netiq/idm/apps/audit` ◆ **Windows:** `c:\netiq\idm\apps\audit`	
Enable Auditing > Secure Layer	Select this option if you want to communicate securely to the audit server. The OSP installer can test the certificate on the audit server to ensure that secure communication works. For more information, see Section 3.9, “Securing Connections with TLS/SSL,” on page 51.	

Item	Description	Value
ConfigUpdate Details	Specify the directory where the OSP installer places the files for the Identity Governance Configuration Update utility. The default path is: ◆ **Linux:** `/opt/netiq/idm/apps/configupdate` ◆ **Windows:** `c:\netiq\idm\apps\configudate`	

4.2.4 Installing One SSO Provider (OSP)

The following procedure describes how to install OSP using the guided installation or the console installation. For information about how to perform a silent installation, see Section 4.2.5, “Silently Installing One SSO Provider,” on page 73. Ensure that you meet the prerequisites for OSP before starting the appropriate installation for your environment. For more information, see Section 4.2.2, “Considerations for Installing One SSO Provider,” on page 62.

If you are in a clustered environment, all of the nodes of the cluster must contain the same keystore and use the same certificates for secure communication. The OSP installer can do this work for you if you wait to stop Apache Tomcat at the **Installation Summary** screen of the OSP installer. You must do this for each node in the cluster. If you are not clustering OSP, you must stop Apache Tomcat before the installation starts.

To install OSP:

1. Ensure that you have completed the OSP Installation Worksheet before starting the installation. For more information, see Section 4.2.3, “OSP Installation Worksheet,” on page 63.
2. Log in as `root` on a Linux server or as an administrator on a Windows server where you want to install OSP.
3. Download and extract the OSP installation file. For more information, see Section 2.2, “Obtaining Identity Governance, Identity Reporting, Workflow Engine, and OSP,” on page 31.
4. If you are in a clustered environment, proceed to Step 5, otherwise, stop Apache Tomcat. For more information, see Section 3.5.3, “Starting and Stopping Apache Tomcat,” on page 50.
5. From the directory that contains the installation files, complete one of the following actions:
   - **Linux**: Enter the following at a command prompt:
     - **Guided:** `./osp-install-linux.bin`
     - **Console:** `./osp-install-linux.bin -i console`
   - **Windows**: Enter the following from a command prompt:
     - **Guided:** `osp-install-win.exe`
     - **Console:** `osp-install-win.exe -i console`

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

6 Complete the installation, using the information you gathered in the OSP Installation Worksheet. For more information, see Section 4.2.3, “OSP Installation Worksheet,” on page 63.

7 Review the pre-installation summary.

8 (Conditional) If you are in a clustered environment, stop Apache Tomcat at this time. For more information, see Section 3.5.3, “Starting and Stopping Apache Tomcat,” on page 50.

9 Start the installation process.

10 (Conditional) At the end of the installation, if prompted, accept or reject any certificates, and acknowledge any errors.

The installer checks to see if you specified SSL for LDAP or audit. If so, the installer creates the trust store and attempts to retrieve the certificates. Untrusted certificates result in a prompt to accept or reject each certificate chain, with tabs showing extra certificates in the chain. The installer adds accepted certificates to the trust store.

The installer displays errors in the following conditions:

- A single warning about potential future failures for all rejected certificates
- A single warning for any errors when connecting to the secured servers

11 When the installation process completes, review the `OSP_Install.log` file to see what the installer did. The default location of the `OSP_Install.log` file is here:

- **Linux:** `/opt/netiq/idm/apps/osp/logs`
- **Windows:** `c:\netiq\idm\apps\osp\logs`

12 Before starting Apache Tomcat again, delete the contents of the following two directories from Apache Tomcat that contain cached files. The directories are:

- **Linux:** Default installation location:
  - `/opt/netiq/idm/apps/tomcat/temp`
  - `/opt/netiq/idm/apps/tomcat/work/Catalina/localhost`
- **Windows:** Default installation location:
  - `c:\netiq\idm\apps\tomcat\temp`
  - `c:\netiq\idm\apps\tomcat\work\Catalina\localhost`

13 Start Apache Tomcat. For more information, see Section 3.5.3, “Starting and Stopping Apache Tomcat,” on page 50.

4.2.5 Silently Installing One SSO Provider

A silent (non-interactive) installation does not display a user interface or ask you any questions. The installation files that you download from the Customer Center contain the `osp-install-silent.properties`. You must edit the `osp-install-silent.properties` file and add the correct parameters for your environment. Ensure that you have met the prerequisites before starting the silent installation. For more information, see Section 4.2.2, “Considerations for Installing One SSO Provider,” on page 62.

Use the following information to properly populate the `osp-install-silent.properties` file with values from your environment and how to use the `osp-install-silent.properties` file to silently install OSP.

- Section 4.2.5.1, “Creating a Silent Properties File for One SSO Provider,” on page 74
- Section 4.2.5.2, “Creating a Silent Properties File for Installing an Additional Node to Cluster OSP,” on page 75
- Section 4.2.5.3, “Running a Silent Installation for One SSO Provider,” on page 77

4.2.5.1 Creating a Silent Properties File for One SSO Provider

The silent properties file for OSP allows you to perform an installation without any interaction. The `osp-install-silent.properties` file is in the ZIP file that you download from the Customer Center. You must edit the file to add the appropriate values for your environment. The different properties in the file relate to the questions that you answer during a guided installation or console installation.

You would use the silent installation if you had several instances of OSP to install. We recommend that you install the first instance of OSP using the guided installation or the console installation with the `-r` parameter and a path where the installer creates a response file for you.

IMPORTANT: To ensure the installation runs correctly, create an empty file in the installation location before starting the installation.

A **response file** contains the correctly formated properties and values that you must add to the `osp-install-silent.properties` file for your environment. You can open the response file and copy the values from the response file to the `osp-install-silent.properties` file to simplify the process of creating the `osp-install-silent.properties` file.

You can also use the OSP Installation Worksheet to add the proper values to the `osp-install-silent.properties` file. You open the `osp-install-silent.properties` file in a text editor and then use the information you gathered in the OSP Installation Worksheet to add the correct values for your environment. For more information, see Section 4.2.3, “OSP Installation Worksheet,” on page 63.

To create the osp-install-silent.properties file using the response file:

1. Download and extract the OSP installation files. For more information, see Section 2.2, “Obtaining Identity Governance, Identity Reporting, Workflow Engine, and OSP,” on page 31.
2. Ensure that you have completed the OSP Installation Worksheet to have the information required to complete the installation. For more information, see Section 4.2.3, “OSP Installation Worksheet,” on page 63

3 Create the response file.

3a From the directory that contains the installation files, complete one of the following actions:

- **Linux**: Enter the following at a command prompt:
  - **Guided:** `./osp-install-linux.bin -r` *`path-to-response-file`*
  - **Console:** `./osp-install-linux.bin -i console -r` *`path-to-response-file`*
- **Windows**: Enter the following at a command prompt:
  - **Guided:**`osp-install-win.exe -r` *`path-to-response-file`*
  - **Console:** `osp-install-win.exe -i console -r` *`path-to-response-file`*

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

3b Use the OSP Installation Worksheet to complete the first guided or console installation of OSP to create the response file. For more information, see Section 4.2.3, “OSP Installation Worksheet,” on page 63.

3c Review the `OSP_Install.log` file to ensure that no errors occurred.

- **Linux:** `/opt/netiq/idm/apps/osp/logs`
- **Windows:** `c:\netiq\idm\apps\osp\logs`

4 Find and open the response file in a text editor.

5 Find and open the `osp-install-silent.properties` in a text editor.

6 Copy the values from the response file to the `osp-install-silent.properties` file.

NOTE: If you are deploying on Windows, ensure that you escape the backslashes `'\'` or the silent properties files does not work.

7 Close the response file and save the `osp-install-silent.properties` file.

8 (Conditional) When installing on a secondary node in a cluster, you can modify the silent properties file using the steps in Section 4.2.5.2, “Creating a Silent Properties File for Installing an Additional Node to Cluster OSP,” on page 75.

9 Proceed to “Running a Silent Installation for One SSO Provider” on page 77 to see how to run the silent installation using the `osp-install-silent.properties` file for the next installation of OSP.

4.2.5.2 Creating a Silent Properties File for Installing an Additional Node to Cluster OSP

In a clustered environment, you can use the same silent properties file for each node. However, you might choose to run the guided installation or the console installation on the primary node with the `-r` parameter to create the response file. You can then silently install on the secondary nodes. You can quickly create a silent properties file from the response file that the guided installation or console installation creates. For more information, see "Creating a Silent Properties File for One SSO Provider" on page 74.

There are additional parameters that you must add to the `osp-install-silent.properties` file if you are installing secondary nodes in a cluster. Use the following procedure to modify the `osp-install-silent.properties` file for any secondary nodes in the OSP cluster.

To create an `osp-install-silent.properties` file for secondary cluster nodes:

1. After installing OSP on the primary node, locate the response file in the directory you specified. For more information, see "Creating a Silent Properties File for One SSO Provider" on page 74.
2. Locate the sample `osp-install-silent.properties` file, by default in the same directory as the installer program for OSP.
3. Open the files in a text editor.
4. Copy the parameter values from the response file to their corresponding parameters in the silent properties 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. (Optional) Specify any number of certificate files and corresponding aliases to accept into the trust store. For example:

```
NETIQ_CERT_1_FILE=/home/username/Downloads/ldap_cert
NETIQ_CERT_1_ALIAS=osp-ldap
```

NOTE: You can specify the files in any order, and they must exist on the same machine as the OSP installer. The installer starts trusting with `1` and stops with the first missing consecutive number. So if you list files 1, 2, and 4, the installer only trusts certificates 1 and 2.

8. Save and close the files.
9. ***Copy the `encrypt-keys.pkcs12` from the primary server to the server that becomes a new node in the cluster.***
10. Copy the updated `osp-install-silent.properties` file from the primary server to the new node.
11. Open the `osp-install-silent.properties` file, then change the encryption keystore related properties to use the same encryption keystore file on the new node. Specifically set:

    ```
    install_enc_create_file=false
    install_enc_source_file=PATH
    ```

    where *PATH* is the location the copied `encrypt-keys.pkcs12` file.
12. Save your changes.
13. Perform the silent installation on the new node using this modified file. For more information, see "Running a Silent Installation for One SSO Provider" on page 77.

4.2.5.3 Running a Silent Installation for One SSO Provider

A silent (non-interactive) installation does not display a user interface or ask any questions. Instead, the system uses information from the `osp-install-silent.properties` file to complete the installation. You would perform this type of installation if you have multiple installations to perform or you are deploying a clustered environment. This file is included with the OSP installation files. You must have the `osp-install-silent.properties` file populated with the correct values for your environment before you start the silent installation.

To perform a silent installation of OSP:

1. Ensure that you have created the `osp-install-silent.properties` file for your environment. For more information, see "Creating a Silent Properties File for One SSO Provider" on page 74.
2. (Conditional) If this server is an additional node to cluster OSP, ensure that you properly modify the `osp-install-silent.properties` file for the additional nodes in a cluster. For more information, see "Creating a Silent Properties File for Installing an Additional Node to Cluster OSP" on page 75.
3. Ensure that this server meets the prerequisites for OSP before starting the installation. For more information, see Section 4.2.2, "Considerations for Installing One SSO Provider," on page 62
4. Ensure that the OSP installation files are on this server. For more information, see Section 2.2, "Obtaining Identity Governance, Identity Reporting, Workflow Engine, and OSP," on page 31.
5. Log in as `root` on Linux server or an administrator on Windows server where you want to install OSP.
6. Stop Apache Tomcat. For more information, see Section 3.5.3, "Starting and Stopping Apache Tomcat," on page 50.

7 Copy the populated `osp-install-silent.properties` file to this server.

8 To run the silent installation, from a command prompt issue the following command:

- **Linux:** `./osp-install-linux.bin -i silent -f` *`path_to_silent_properties_file`*
- **Windows:** `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.

9 When the console prompt returns, review the log file to ensure that the installation completed successfully. The silent installation does not display any messages on the console.

The log file is located in the following default directory:

- **Linux:** `/opt/netiq/idm/apps/osp/logs`/
- **Windows:** `c:\netiq\idm\apps\osp\logs`\

10 When the installation process completes, continue to Chapter 6, "Installing Identity Governance," on page 131.

4.3 Integrating Access Manager with Identity Governance

To use Access Manager as the authentication service for Identity Governance, you must configure Access Manager to use the OAuth 2.0 protocol, and you must define or add an attribute in the identity store for Access Manager to use to store authentication information. You can perform these steps before installing Identity Governance. If you use OSP as the authentication service and you want to move to Access Manager, you must perform these steps at that time.

- Section 4.3.1, "Access Manager and the Identity Service Integration Checklist for OAuth 2.0," on page 79
- Section 4.3.2, "Integrating Identity Governance and Access Manager During the Installation of Identity Governance," on page 80
- Section 4.3.3, "Integrating Identity Governance and Access Manager After the Identity Governance Installation (Single Server)," on page 81
- Section 4.3.4, "Integrating Identity Governance and Access Manager After the Identity Governance Installation in a Distributed Environment," on page 84

4.3.1 Access Manager and the Identity Service Integration Checklist for OAuth 2.0

Access Manager integrates with Identity Governance through the use of the OAuth 2.0 protocol to allow for secure communication between the two products. OAuth 2.0 allows you to use different authentication methods beyond the name/password method. For more information, see “ OAuth and OpenID Connect” in the *NetIQ Access Manager 5.0 Administration Guide*.

You must configure Access Manager to use OAuth 2.0 before starting the Identity Governance installation. You must also use an LDAP-based bootstrap administrator and add a special attribute to the identity store to store authentication information from Access Manager.

Use the following checklist to complete the configuration tasks in the identity store and Access Manager before starting the Identity Governance installation or if you want to stop using OSP as your authentication service.

	Checklist Items
□	1. Create an LDAP-based bootstrap administrator for Identity Governance. Identity Governance does not have access to the Access Manager file system to be able to use a file-based administrator. **WARNING:** Do not use the name admin and ensure that the name is unique. Create a user account in your identity service that has administrative rights to the identity service. Ensure that this account is only used as the bootstrap administrator for Identity Governance. For more information, see Section 4.1.1, “Using the Bootstrap Administrator,” on page 58
□	2. Create an attribute in the identity service to store the authorization grant information from Access Manager. Identity Governance uses the term **identity service** to refer to the LDAP server that holds the authorized users. The LDAP directory can either be Active Directory, Identity Manager Identity Vault, or eDirectory. Access Manager uses the term **User Store** to refer to the LDAP directory that stores the Access Manager users and configuration information. Access Manager stores the OAuth 2,0 authorization grant information for each user in an attribute in the identity service. You can use an unused attribute in your identity service or you can create a new attribute. This attribute must exist to enable OAuth 2.0 in Access Manager. The Access Manager contains the instructions on how to create a new attribute for Active Directory and eDirectory. For more information, see “Extending a User Store for OAuth 2.0 Authorization Grant Information” in the *NetIQ Access Manager 5.0 Administration Guide*.
□	3. Enable the OAuth protocol in Access Manager. For more information, see “Enabling OAuth in Access Gateway” in the *NetIQ Access Manager 5.0 Administration Guide*.
□	4. Add your identity service as the local User Store in Access Manager. Access Manager must be able to access the authorized user accounts to be able to authenticate the users to Identity Governance. For more information, see “Configuring Identity User Stores” in the *NetIQ Access Manager 5.0 Administration Guide*.

	Checklist Items
❑	5. Configure an Access Manager authentication contract to define how the Identity Governance authorized users authenticate. You can define one or more authentication contracts for the authorized users to use depending on the needs of the users. For more information, see "Configuring Authentication Contracts" in the *NetIQ Access Manager 5.0 Administration Guide*.
❑	6. Configure Access Manager to use the authentication contract for Identity Governance. You can define the Identity Governance authentication contract as the default authentication contract for Access Manager or you can define the Identity Governance application as a protected resource in Access Manager to enable SSO for the authorized users. ◆ To make the Identity Governance authentication contract the default contract for the Access Manager Identity Server, see "Specifying Authentication Defaults" in the *NetIQ Access Manager 5.0 Administration Guide*. ◆ To make the Identity Governance application a protected resource, see "Protecting Web Resources Through Access Gateway" in the *NetIQ Access Manager 5.0 Administration Guide*.
❑	7. Register Identity Governance as an OAuth application in Access Manager. You must create an Access Manager role with the exact name of `NAM_OAUTH2_ADMIN` to register Identity Governance. For more information, see "Registering OAuth Client Applications" in the *NetIQ Access Manager 5.0 Administration Guide*.

4.3.2 Integrating Identity Governance and Access Manager During the Installation of Identity Governance

You can integrate Identity Governance and Access Manager during the installation of Identity Governance. You must select to use an LDAP-based bootstrap administrator and you provide connection information to Access Manager during the install. Installing Identity Governance contains the details for the configuration. For more information, see Section 6.4, "Identity Governance Installation Worksheet," on page 134.

After you have completed the Identity Governance installation and if you are using Active Directory as the identity service, you must change the Access Manager Mapping Table to point to the Active Directory attribute of `distinguishedName` instead of `entryDN`. For more information, see Editing Attribute Sets in the *NetIQ Access Manager 5.0 Administration Guide*.

1 Log in to the Access Manager administration console as an administrator.

2 Click **Devices > Identity Server**.

3 Click the **Shared Settings** tab, then click the **Attributes Sets** tab.

4 Click the Identity Governance object.

- **Identity Governance:** If you used the default values during the Identity Governance Configuration Update utility conversion, the name is `Micro Focus ISM`.
- **Access Manager:** If during the Access Manager OAuth Configuration you used the advanced option of **ISM Application Instance ID** the name is `Micro Focus ISM_`*`specified_name`*.

5 Click **Mapping**.

6 Click **Ldap Attribute:entryDN [LDAP Attribute Profile]**.

7 Select **Local attribute**.

8 Select **Ldap Attribute:distinguishedName [LDAP Attribute Profile]**.

9 Click **OK**.

10 Click **Apply**, then click **OK**.

11 Click **Servers**, then click **Update All**.

12 On the OSP server, restart Apache Tomcat. For more information, see Section 3.5.3, “Starting and Stopping Apache Tomcat,” on page 50.

4.3.3 Integrating Identity Governance and Access Manager After the Identity Governance Installation (Single Server)

If you installed Identity Governance using OSP as the authentication service and now you want to use Access Manager, Identity Governance allows you to do that without having to uninstall Identity Governance. To make the change it is a process that does require multiple steps.

The process is different if you have Access Manager, Identity Governance, Identity Reporting, and Workflow Engine installed on separate server. For more information, see Section 4.3.4, “Integrating Identity Governance and Access Manager After the Identity Governance Installation in a Distributed Environment,” on page 84. Use the following information to switch from OSP to Access Manager if you have OSP and Identity Governance installed on the same server.

1 Ensure that you have completed all of the Access Manager integration steps before proceeding. For more information, see Section 4.3.1, “Access Manager and the Identity Service Integration Checklist for OAuth 2.0,” on page 79.

2 Stop Apache Tomcat. For more information, see Section 3.5.3, “Starting and Stopping Apache Tomcat,” on page 50.

3 Verify that the single sign-on settings are populated.

3a Launch the Identity Governance Configuration Update utility. For more information, see Section 15.1.5, “Using the Identity Governance Configuration Update Utility,” on page 293.

3b Click the **IG SSO Clients** tab.

3c Click **Show Advanced Options**.

3d Ensure that all of the fields except for **Identity Governance Client > Additional mapped LDAP attributes** are populated. If any fields are missing information, add the information for your environment.

3e Click **OK** even if you didn’t make any changes to save the configuration and the Identity Governance Configuration Update utility automatically closes.

4 Verify that the `ism-configuration.properties` contains four `response-types = client_credentials`.

4a Open the `ism-configuration.properties` file in a text editor. The default location is:

- **Linux:** `/opt/netiq/idm/apps/tomcat/conf`
- **Windows:** `c:\netiq\idm\apps\tomcat\conf`

4b Search for `response-types = client_credentials`. There should be four.

4c If there are not four entries, repeat Step 3.

5 Change the authentication settings to use Access Manager.

5a Launch the Identity Governance Configuration Update utility. For more information, see Section 15.1.5, “Using the Identity Governance Configuration Update Utility,” on page 293.

5b Click the **Authentications** tab.

5c (Conditional) Select **OAuth server uses TLS**.

5d Select **Access Manager is the OAuth provider**.

5e Populate the following fields with the Access Manager information.

OAuth server host name

Specify the fully qualified DNS name of your Access Manager server.

OAuth server TCP port

Specify the port for Access Manager. By default is 443.

Identity Governance bootstrap admin

Browse to and select the LDAP bootstrap administrator you created in Step 1.

5f Click **Configure Access Manager now**.

5g Use the following information to configure Identity Governance to work with Access Manager:

Administrative Console > Console host

Specify the fully qualified DNS name of the Access Manager administration console.

Administrative Console > Console port

Specify the port for the Access Manager administration console.

Administrative Console > Administrator DN

Specify the fully qualified DN of an Access Manager administrator user.

Administrative Console > Administrator Password

Specify the password for the Access Manager administrator.

Administrative Console > Update IDP

Ensure that this option is selected to automatically update the Access Manager Identity Server with the Identity Governance information.

OAuth 2.0 Administrator > Administrator DN

Browse to and select the bootstrap administrator that you created with the `NAM_OAUTH2_ADMIN` Access Manager role in Step 7.

OAuth 2.0 Administrator > Administrator Password

Specify the password for the bootstrap administrator.

5h Click **OK** to save the changes.

5i Review and accept the certificate presented.

5j After the configuration work is completed, click **OK** on the Notification message.

5k Select the **IG SSO Client** tab and notice that the Client IDs and Secrets have been updated.

5l Click **OK** to save the changes and the Identity Governance Configuration Update utility automatically closes.

6 (Conditional) If you are using Active Directory as the identity service, change the Access Manager Mapping Table to point to the Active Directory attribute of `distinguishedName` instead of `entryDN`. For more information, see Editing Attribute Sets in the *NetIQ Access Manager 5.0 Administration Guide*.

6a Log in to the Access Manager administration console as an administrator.

6b Click **Devices > Identity Server**.

6c Click the **Shared Settings** tab, then click the **Attributes Sets** tab.

6d Click the Identity Governance object.

- **Identity Governance:** If you used the default values during the Identity Governance Configuration Update utility conversion, the name is `Micro Focus ISM`.
- **Access Manager:** If during the Access Manager OAuth Configuration you used the advanced option of **ISM Application Instance ID** the name is `Micro Focus ISM_`*`specified_name`*.

6e Click **Mapping**.

6f Click **Ldap Attribute:entryDN [LDAP Attribute Profile]**.

6g Select **Local attribute**.

6h Select **Ldap Attribute:distinguishedName [LDAP Attribute Profile]**.

6i Click **OK**.

6j Click **Apply**, then click **OK**.

6k Click **Servers**, then click **Update All**.

7 Ensure that the `ism-configuration.properties` file lists the protocol as secure.

7a Open the `ism-configuration.properties` file in a text editor. The default location is:

- **Linux:** `/opt/netiq/idm/apps/tomcat/conf`
- **Windows:** `c:\netiq\idm\apps\tomcat\conf`

7b Search for `com.netiq.idm.osp.url.host`.

7c If it is not set to `https` change it from `http` to `https`.

7d Save and close the file.

8 (Conditional) If the `ism-configuration.properties` file was incorrect the Identity Governance Configuration Update utility must receive a valid certificate.

8a Launch the Identity Governance Configuration Update utility. For more information, see Section 15.1.5, "Using the Identity Governance Configuration Update Utility," on page 293.

8b When it displays the fields, click **OK**.

8c Review and accept the new certificate, then click **OK** to save and the Identity Governance Configuration Update utility automatically closes.

9 Change additional settings in the Identity Governance Configuration utility.

9a Launch the Identity Governance Configuration utility using the database password. For more information, see Section 15.1.4, "Using the Identity Governance Configuration Utility," on page 290.

9b Click the **Authentication** tab.

9c In the **OAuth Server** section, make the following changes:

Same as IG Server

Deselect this option.

Protocol

(Conditional) Change the protocol from **http** to **https** if it is not already at **https**.

Host Name

Specify the fully qualified DNS name of the Access Manager server.

Port

Specify the port for the Access Manager server. The default value is 443.

9d Click **Save** to save the changes, then close the utility.

10 Update the `ism-configuration.properties` file.

10a Open the `ism-configuration.properties` file in a text editor. The default location is:

- **Linux:** `/opt/netiq/idm/apps/tomcat/conf`
- **Windows:** `c:\netiq\idm\apps\tomcat\conf`

10b Add the following entry:

```
com.netiq.iac.authserver.url.logout =
${com.netiq.idm.osp.url.host}/nidp/app/logout
```

10c Save and close the file.

11 Clean up Apache Tomcat.

11a Delete the following cache directory. This is the default location.

- **Linux:** `/opt/netiq/idm/apps/tomcat/work/Catalina/localhost`
- **Windows:** `c:\netiq\idm\apps\tomcat\work\Catalina\localhost`

11b Delete all of the files and sub-folders in the `temp` directory. This is the default location.

- **Linux:** `/opt/netiq/idm/apps/tomcat/temp`
- **Windows:** `c:\netiq\idm\apps\tomcat\temp`

11c Delete or move any Apache Tomcat log files. This is the default location.

- **Linux:** `/opt/netiq/idm/apps/tomcat/logs`
- **Windows:** `c:\netiq\idm\apps\tomcat\logs`

12 Start Apache Tomcat. For more information, see Section 3.5.3, “Starting and Stopping Apache Tomcat,” on page 50.

13 Log in to Identity Governance to test if the authentication is now going through Access Manager.

4.3.4 Integrating Identity Governance and Access Manager After the Identity Governance Installation in a Distributed Environment

Identity Governance allows you to switch your authentication service from OSP to Access Manager without having to reinstall Identity Governance. If you have OSP, Identity Governance, Identity Reporting, and Workflow Engine installed on separate servers, you must use the following procedure to make the change. The steps are different than if you have all of the components installed on one server. If you have all of the components installed on one server, see Section 4.3.2, “Integrating Identity Governance and Access Manager During the Installation of Identity Governance,” on page 80.

1 Ensure that you have completed all of the Access Manager integration steps before proceeding. For more information, see Section 4.3.1, “Access Manager and the Identity Service Integration Checklist for OAuth 2.0,” on page 79.

2 On the OSP server, change the authentication service to Access Manager.

2a Stop Apache Tomcat on the OSP, Identity Governance, Identity Reporting, and Workflow Engine servers. For more information, see Section 3.5.3, “Starting and Stopping Apache Tomcat,” on page 50.

2a1 Verify that the single sign-on settings are populated.

2a1a Launch the Identity Governance Configuration Update utility. For more information, see Section 15.1.5, “Using the Identity Governance Configuration Update Utility,” on page 293.

2a1b Click the **IG SSO Clients** tab.

2a1c Click **Show Advanced Options**.

2a1d Ensure that all of the fields except for **Identity Governance Client > Additional mapped LDAP attributes** are populated. If any fields are missing information, add the information for your environment.

2a1e Click the **External Workflow** tab.

2a1f (Conditional) Ensure that all the above fields are populated. If any fields are missing information, add the information for your environment.

2a1g Click **OK** even if you didn’t make any changes to save the configuration and the Identity Governance Configuration Update utility automatically closes.

2b Verify that the database contains four or six `response-types = client_credentials`.

2b1 On the Identity Governance server, create the following script using the path and file name of your choice:

- `set-backup-dir <`*`path`*`>`
- `set-backup-file-name <`*`filename`*`>`
- `backup`

2b2 Execute the script:

```
/opt/netiq/idm/apps/idgov/bin/configutil.sh -password <password>
-script <script>
```

2b3 Open the backup file and look for the instances of `client_credentials`.

Search for the following entries once you open the backup file for Identity Governance:

- `com.netiq.iac.dc_server.response-types`
- `com.netiq.iac.dtp_server.response-types`
- `com.netiq.iac.general-service.response-types`
- `com.netiq.iac.wf_server.response-types`

(Conditional) Search for the following entries once you open the backup file for the Workflow Engine:

- `com.netiq.iac.standaloneworkflow.response-types`
- `com.netiq.workflow.response-types`

2c Change the authentication settings to use Access Manager.

2c1 Launch the Identity Governance Configuration Update utility. For more information, see Section 15.1.5, "Using the Identity Governance Configuration Update Utility," on page 293.

2c2 Click the **Authentication** tab.

2c3 (Conditional) Select **OAuth server uses TLS**.

2c4 Select **Access Manager is the OAuth provider**.

2c5 OAuth server host identifier.

OAuth server host name

Specify the fully qualified DNS name of your Access Manager server.

OAuth server TCP port

Specify the port for Access Manager. By default is 443.

Identity Governance Bootstrap Admin

Browse to and select the LDAP bootstrap administrator you created in Step 1.

2c6 Click **Configure Access Manager now**.

2c7 Click **Show Advanced Options** button.

2c8 Use the following information to configure Identity Governance to work with Access Manager:

Administrative Console > Console host

Specify the fully qualified DNS name of the Access Manager administration console.

Administrative Console > Console port

Specify the port for the Access Manager administration console.

Administrative Console > Administrator DN

Specify the fully qualified DN of an Access Manager administrator user.

Administrative Console > Administrator Password

Specify the password for the Access Manager administrator.

Administrative Console > Update IDP

Ensure that this option is selected to automatically update the Access Manager Identity Server with the Identity Governance information.

OAuth 2.0 Administrator > Administrator DN

Browse to and select the bootstrap administrator that you created with the `NAM_OAUTH2_ADMIN` Access Manager role in Step 7.

OAuth 2.0 Administrator > Administrator Password

Specify the password for the bootstrap administrator.

2c9 Click **OK** to save the changes.

2c10 Review and accept the certificate presented.

2c11 After the configuration work is completed, click **OK** on the Notification message.

2c12 (Conditional) Select the **External Workflow** tab and notice that the Client IDs and Secrets have been updated.

2c13 Select the **IG SSO Client** tab and notice that the Client IDs and Secrets have been updated.

2c14 Click **OK** to save the changes and the Identity Governance Configuration Update utility automatically closes.

2d Ensure the com.netiq.idm.osp.url.host property is set correctly with a secure protocol.

2d1 On the Identity Governance server, create a script with the following content:

display-configs com.netiq.idm.osp.url.host

2d2 Execute the script.

```
/opt/netiq/idm/apps/idgov/bin/configutil.sh -password <password>
-script <script>
```

2d3 (Conditional) If you need to update the value, create and execute the following script with your expected protocol, server, and host. The script prints the final value after the change.

```
set-property com.netiq.idm.osp.url.host https://<Access Manager
DNS name>

display-configs com.netiq.idm.osp.url.host

set-property com.netiq.iac.authserver.host https://<Access
Manager DNS name>

display-configs: com.netiq.iac.authserver.host

set-property com.netiq.client.authserver.url.logout https://
<Access Manager DNS name>/nidp/app/logout

display-configs com.netiq.client.authserver.url.logout
```

2d4 Save and close the file.

2e (Conditional) If you are using Active Directory as the identity service, change the Access Manager Mapping Table to point to the Active Directory attribute of `distinguishedName` instead of `entryDN`. For more information, see Editing Attribute Sets in the *NetIQ Access Manager 5.0 Administration Guide*.

2e1 Log in to the Access Manager administration console as an administrator.

2e2 Click **Devices > Identity Server**.

2e3 Click the **Shared Settings** tab, then click the **Attributes Sets** tab.

2e4 Click the Identity Governance object.

- **Identity Governance:** If you used the default values during the Identity Governance Configuration Update utility conversion, the name is `Micro Focus ISM`.
- **Access Manager:** If during the Access Manager OAuth Configuration you used the advanced option of **ISM Application Instance ID** the name is `Micro Focus ISM_`*`specified_name`*.

2e5 Click **Mapping**.

2e6 Click **Ldap Attribute:entryDN [LDAP Attribute Profile]**.

2e7 Select **Local attribute**.

2e8 Select **Ldap Attribute:distinguishedName [LDAP Attribute Profile]**.

2e9 Click **OK**.

2e10 Click **Apply**, then click **OK**.

2e11 Click **Servers**, then click **Update All**.

2f (Conditional) If the `ism-configuration.properties` file was incorrect the Identity Governance Configuration Update utility must receive a valid certificate.

2f1 Launch the Identity Governance Configuration Update utility. For more information, see Section 15.1.5, "Using the Identity Governance Configuration Update Utility," on page 293.

2f2 When it displays the fields, click **OK**.

2f3 Review and accept the new certificate, then click **OK** to save and the Identity Governance Configuration Update utility automatically closes.

3 On the Identity Governance server change the authentication service to be Access Manager.

3a At the Access Manager URL, access the OAuth Client IDs and Secrets.

3a1 On the Identity Governance server launch a browser and access the Access Manager administration console.

3a2 On the Dashboard under **Identity Servers**, select **IDPCluster**.

3a3 Click the **OAuth & OpenID Connect** tab, then click the **Client Applications** tab.

3a4 Leave the **Client Applications** tab open because it contains the client IDs and secrets for the Identity Governance applications that you created in Step 7. Add this information to the Identity Governance configuration.

3b Verify that the client IDs and secrets from Access Manager have made it to the Identity Governance configuration. Because the properties are stored in the OSP database, and Configupdate on both OSP and IG servers have connection information for connecting to that database, the entries should already be populated.

3b1 Launch the Identity Governance Configuration Update utility. For more information, see Section 15.1.5, "Using the Identity Governance Configuration Update Utility," on page 293.

3b2 Click the **IG SSO Clients** tab.

3b3 Copy the **Client ID** and **Secret** for each Identity Governance application listed in Access Manager. Use the following table to correlate the names in Identity Governance to the names in Access Manager.

IMPORTANT: Ensure that you copy the **Client ID** not the **Client Application Name**.

Identity Governance Application Name	Access Manager Application Name
Identity Governance	iac
Request Client	cx_client
Data Connectivity Service	iac_dc_server
General Service	iac_general_service
Data Transformation and Processing Service	iac_dtp_server
Workflow Service	iac_wf_server
Form Builder Client	form_builder
Identity Governance Client	iac_ig_web

3c In the Identity Governance Configuration Update utility ensure that the authentication settings are set to Access Manager values.

3c1 Click the **Authentication** tab.

3c2 (Conditional) Select **OAuth server uses TLS**.

3c3 Select **Access Manager is the OAuth provider**.

3c4 Populate the following fields with the Access Manager information.

OAuth server host name

Specify the fully qualified DNS name of your Access Manager server.

OAuth server TCP port

Specify the port for Access Manager. By default is 443.

Identity Governance bootstrap admin

Browse to and select the LDAP bootstrap administrator you created in Step 1.

3c5 Click **OK** to save the changes and the Identity Governance Configuration Update utility automatically closes.

3d Ensure that the `ism-configuration.properties` file lists the protocol as secure.

3d1 Open the `ism-configuration.properties` file in a text editor. The default location is:

- **Linux:** `/opt/netiq/idm/apps/tomcat/conf`
- **Windows:** `c:\netiq\idm\apps\tomcat\conf`

3d2 Search for `com.netiq.idm.osp.url.host`.

3d3 If it is not set to `https` change it from `http` to `https`.

3d4 Save and close the file.

3e (Conditional) If the `ism-configuration.properties` file was incorrect the Identity Governance Configuration Update utility must receive a valid certificate.

3e1 Launch the Identity Governance Configuration Update utility. For more information, see Section 15.1.5, "Using the Identity Governance Configuration Update Utility," on page 293.

3e2 When it displays the fields, click **OK**.

3e3 Review and accept the new certificate, then click **OK** to save and the Identity Governance Configuration Update utility automatically closes.

4 On the Identity Governance server change additional settings in the Identity Governance Configuration utility.

4a Launch the Identity Governance Configuration utility using the database password. For more information, see Section 15.1.4, "Using the Identity Governance Configuration Utility," on page 290.

4b Click the **Authentication** tab.

4c In the **OAuth Server** section, make the following changes:

Protocol

(Conditional) Change the protocol from **http** to **https** if it is not already at **https**.

Host Name

Specify the fully qualified DNS name of the Access Manager server.

Port

Specify the port for the Access Manager server. The default value is 443.

4d In the **Bootstrap Admin** section, update the **Name** field to contain the fully qualified DN name of the bootstrap administrator you created in Step 1.

4e Click **Save** to save the changes, then close the utility.

5 On the Identity Governance server clean up Apache Tomcat.

5a Delete the following cache directory. This is the default location.

- **Linux:** `/opt/netiq/idm/apps/tomcat/work/Catalina/localhost`
- **Windows:** `c:\netiq\idm\apps\tomcat\work\Catalina\localhost`

5b Delete all of the files and sub-folders in the `temp` directory. This is the default location.

- **Linux:** `/opt/netiq/idm/apps/tomcat/temp`
- **Windows:** `c:\netiq\idm\apps\tomcat\temp`

5c Delete or move any Apache Tomcat log files. This is the default location.

- **Linux:** `/opt/netiq/idm/apps/tomcat/logs`
- **Windows:** `c:\netiq\idm\apps\tomcat\logs`

6 On the Identity Governance server only, start Apache Tomcat. For more information, see Section 3.5.3, "Starting and Stopping Apache Tomcat," on page 50.

7 Test authentication to Identity Governance to ensure that the changes worked.

8 Make the following changes to the Identity Reporting server to use Access Manager instead of OSP.

8a On the Identity Reporting server change the authentication service to be Access Manager.

8a1 On the Access Manager server, access the OAuth Client IDs and Secrets.

8a1a On the Identity Reporting server launch a browser and access the Access Manager administration console.

8a1b On the Dashboard under **Identity Servers**, select **IDPCluster**.

8a1c Click the **OAuth & OpenID Connect** tab, then click the **Client Applications** tab.

8a1d Leave the **Client Applications** tab open, because it contains the client IDs and secrets for the Identity Governance applications that you created in Step 7. You will add this information to the Identity Governance configuration.

8a2 Add the client IDs and secrets from Access Manager to the Identity Reporting server configuration.

8a2a Launch the Identity Governance Configuration Update utility. For more information, see Section 15.1.5, "Using the Identity Governance Configuration Update Utility," on page 293.

8a2b Click the **OAuth SSO Client** tab.

8a2c Copy the **Client ID** and **Secret** for the Identity Reporting application listed in Access Manager as **rpt** to the **Reporting** application.

IMPORTANT: Ensure that you copy the **Client ID** not the **Client Application Name**.

Identity Governance Application Name	Access Manager Application Name
Reporting Utility Client	**rpt**
Reporting Client	**rpt_rpt_web**

8a3 In the Identity Governance Configuration Update utility ensure that the authentication settings are set to Access Manager values.

8a3a Click the **Authentications** tab.

8a3b (Conditional) Select **OAuth server uses TLS**.

8a3c Select **Access Manager is the OAuth provider**.

8a3d Populate the following fields with the Access Manager information.

OAuth server host name

Specify the fully qualified DNS name of your Access Manager server.

OAuth server TCP port

Specify the port for Access Manager. By default is 443.

8a3e Click **OK** to save the changes and the Identity Governance Configuration Update utility automatically closes.

8b Ensure the `com.netiq.idm.osp.url.host` property is set correctly with a secure protocol.

8b1 On the Identity Governance server, create a script with the following content:

display-configs `com.netiq.idm.osp.url.host`

8b2 Execute the script.

/opt/netiq/idm/apps/idgov/bin/configutil.sh -password <password> -script <script>

8b3 (Conditional) If you need to update the value, create and execute the following script with your expected protocol, server, and host. The script prints the final value after the change.

set-property com.netiq.idm.osp.url.host https://<server>

display-configs com.netiq.idm.osp.url.host

8b4 Save and close the file.

8c (Conditional) If the `ism-configuration.properties` file was incorrect the Identity Governance Configuration Update utility must receive a valid certificate.

8c1 On the Identity Reporting server, launch the Identity Governance Configuration Update utility. For more information, see Section 15.1.5, "Using the Identity Governance Configuration Update Utility," on page 293.

8c2 When it displays the fields, click **OK**.

8c3 Review and accept the new certificate, then click **OK** to save and the Identity Governance Configuration Update utility automatically closes.

8d On the Identity Reporting server clean up Apache Tomcat.

8d1 Delete the following cache directory. This is the default location.

- **Linux:** `/opt/netiq/idm/apps/tomcat/work/Catalina/localhost`
- **Windows:** `c:\netiq\idm\apps\tomcat\work\Catalina\localhost`

8d2 Delete all of the files and sub-folders in the `temp` directory. This is the default location.

- **Linux:** `/opt/netiq/idm/apps/tomcat/temp`
- **Windows:** `c:\netiq\idm\apps\tomcat\temp`

8d3 Delete or move any Apache Tomcat log files. This is the default location.

- **Linux:** `/opt/netiq/idm/apps/tomcat/logs`
- **Windows:** `c:\netiq\idm\apps\tomcat\logs`

8e On the Identity Reporting server only, start Apache Tomcat. For more information, see Section 3.5.3, "Starting and Stopping Apache Tomcat," on page 50.

8f Test authentication to Identity Governance to ensure that the changes worked.

9 On the Workflow Engine server change the authentication service to be Access Manager.

9a At the Access Manager URL, access the OAuth Client IDs and Secrets.

9a1 On the Identity Governance server launch a browser and access the Access Manager administration console.

9a2 On the Dashboard under **Identity Servers**, select **IDPCluster**

9a3 Click the **OAuth & OpenID Connect** tab, then click the **Client Applications** tab.

9a4 Leave the **Client Applications** tab open because it contains the client IDs and secrets for the Identity Governance applications that you created in Step 7. Add this information to the Identity Governance configuration.

9b Verify that the client IDs and secrets from Access Manager have made it to the Identity Governance configuration. Because the properties are stored in the OSP database, and Configupdate on both OSP and IG servers have connection information for connecting to that database, the entries should already be populated.

9b1 Launch the Identity Governance Configuration Update utility. For more information, see Section 15.1.5, "Using the Identity Governance Configuration Update Utility," on page 293.

9b2 Click the **IG SSO Clients** tab.

9b3 Copy the **Client ID** and **Secret** for each Identity Governance application listed in Access Manager. Use the following table to correlate the names in Identity Governance to the names in Access Manager.

9c Add the client IDs and secrets from Access Manager to the Workflow Engine configuration.

9c1 Launch the Identity Governance Configuration Update utility. For more information, see Section 15.1.5, "Using the Identity Governance Configuration Update Utility," on page 293.

9c2 Click the **External Workflow** tab.

9c3 Copy the **Client ID** and **Secret** for each Identity Governance application listed in Access Manager. Use the following table correlate the names in Workflow Engine to the names in Access Manager.

Identity Governance Application Name	Access Manager Application Name
Web Client	**wfconsole**
Workflow Consumer	**workflow**

9c4 Make sure all fields have valid entries.

10 Update the `ism-configuration.properties` file on the Workflow Engine server with information from the Access Manager server.

10a On the Identity Governance server, export the properties similar to steps Step 2b1 - 2.b.2 using a different backup filename.

10b On the Workflow Engine server, copy the following property values from those exported in step 4.a into the `ism-configuration.properties` file.

- `com.microfocus.wfe.consumer.password`
- `com.microfocus.wfe.consumer.password._attr_obscurity`
- `com.microfocus.wfe.consumer.userId`

Repeat Step 5, Step 6, and Step 7 for the Workflow Engine server.

5 Creating Databases for Identity Governance and Components

Identity Governance, Identity Reporting, and the Workflow Engine require databases to function. You can allow the Identity Governance installer to create and populate these required databases or you can manually create and populate these databases. The Identity Governance installer also installs Identity Reporting and the Workflow Engine and it can create and populate the databases required for both.

Identity Governance requires multiple databases to function and Identity Reporting and the Workflow Engine requires a single database to function. You can have the Identity Governance installation program do most of the work of building these databases, adding the schema for each database, and creating tables and views or you can have a database administrator manually do this work. Your IT policies that specify who can modify and create databases should determine whether you allow the Identity Governance installer to create the databases, or whether your database administrator creates the databases.

Use the following information to understand how you can install the databases required for Identity Governance, Identity Reporting, and the Workflow Engine and what is required to get the databases installed properly.

5.1 Understanding the Databases

Identity Governance requires five different databases to function and one database for Identity Reporting. You can allow the Identity Governance installer to create and populate these databases for you, or you can have your database administrator create and populate the databases for you using a SQL file that the installer generates. It depends on your IT policies of who can modify databases and as to whether you allow the Identity Governance installer to create and populate the databases or whether your database administrator creates and populates the databases.

Whether you allow the installer to create the databases or if you have your database administrator create the databases, you must have the databases installed and running before starting Identity Governance, Identity Reporting, and the Workflow Engine.

If you are allowing the installer to create the databases, the databases must either be absent or not contain data for the installer to be able to properly create the databases. For more information, see Section 5.4, "Using the Identity Governance Installer to Create and Populate the Databases," on page 98.

If you are manually creating the databases, you must have all of the databases created with the proper names before starting the installation. For more information, see Section 5.6, "Manually Creating and Populating the Databases," on page 100.

The installer creates databases with default names. If you are manually creating the database, you must use these default names, which are listed in the following table.

Table 5-1 *The Identity Governance Databases*

Database Function	Default Database Name
operations	`igops`
archive	`igarc`
data collection	`igdcs`
workflow	`igwf`
analytics	`igara`
Identity Reporting database	`igrpt`
workflow engine	`igaworkflowdb`

For production environments, you must install one database server that hosts multiple Identity Governance databases. You can install the Identity Governance databases, the Identity Reporting database, and the Workflow Engine database on the same database server. For more information about Identity Reporting, see Chapter 7, "Installing Identity Reporting," on page 163.

Each database performs a specific function. For example, the data collection database stores the catalog information for your identity sources and application sources. The administration console for Identity Governance displays these database names with the associated functions you must perform.

5.2 Prerequisites for the Databases

You can install Identity Governance and Identity Reporting on the same server, on separate servers, or not install Identity Reporting. The following considerations apply to all of the scenarios. Review the following considerations for the database that you use with Identity Governance and Identity Reporting:

Requirements

- ❒ The database server, the Identity Governance server, the Identity Reporting server, and the Workflow Engine server must run in the same subnetwork.
- ❒ Install a database server or use an existing database server that Identity Governance supports. For more information about the specific database versions, see Section 2.4.2, “Database Requirements,” on page 41.
- ❒ (Conditional) If you do not use PostgreSQL, ensure that the JDBC driver for the supported database is on the server where you install Identity Governance and its components. For more information, see Section 5.7, “Adding the JDBC File to the Application Server,” on page 101.
- ❒ (Conditional) You can install the version of PostgreSQL that Identity Governance requires 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 new files.

Recommendations

- ❒ For production environments, we recommend that you never install Identity Governance or Identity Manager components on the same server where the databases run. If you do install these components on the same server where the databases run, it significantly impacts the performance of Identity Governance. For more information, see Section 2.3, “Recommended Production Environment Installation Scenarios,” on page 32.
- ❒ For production environments, we recommend that you cluster the database server to provide fault tolerance for the information stored in the database. The Identity Governance installer does not cluster the database server for you. For more information on how to cluster the database server, Section 2.3.4, “Ensuring High Availability or Load Balancing for Identity Governance,” on page 35.
- ❒ For production environments, if you use Identity Reporting often, we recommend that you install Identity Reporting on a separate server from Identity Governance. For more information, see Section 2.3, “Recommended Production Environment Installation Scenarios,” on page 32.
- ❒ For production environments, if you are installing both Identity Governance and Identity Reporting on the same server, and you plan to move one of the features to a different server, we recommend that you install both features separately to facilitate the future move.

5.3 Clustering the Database

We recommends that you cluster the database in a production environment to provide fault tolerance for the information Identity Governance stores on the database. Database clustering is a feature of each respective database server. We do not officially test with any clustered database configuration since clustering is independent of the functionality of Identity Governance. In our code, we use a combination of Hibernate and Liquibase; as a result, the database server and its configuration are transparent to us.

In summary, we support clustered database servers within the following constraints:

- Our installers are not designed to install the products into a database cluster. We require database administrators to install into a specific instance of the database and then modify the JDBC URL information accordingly. You might need to adjust other utilities as well.
- We have not performed any official tests with any clustered database servers.
- You might have to disable some features or aspects of the clustered database server. For example, Transactional Replication must be disabled on certain tables due to a constraint violation when trying to insert a duplicate key.
- We do not provide assistance with the installation, configuration, or optimization of the clustered database server, and we do not assist in installing our products into a clustered database server.
- You must reproduce issues or analyze the behavior of the components in a non-clustered environment to help isolate potential cluster setup issues from issues within our products.
- We exert best effort to resolve any issues that might arise with the use of our products in a clustered database environment. Troubleshooting methods in a complex environment often require cooperative work to resolve issues. We provide expertise to analyze, plan, and troubleshoot our products. You must provide the expertise to analyze, plan, and troubleshoot any 3rd party products such as the database server, database clustering, and so forth.

5.4 Using the Identity Governance Installer to Create and Populate the Databases

There are two ways you can create and populate the databases for Identity Governance, Identity Reporting, and the Workflow Engine. You can have the Identity Governance installer create and populate the databases for you or you can have a database administrator manually create the databases and use the SQL scripts to populate the databases. It depends on your IT policies of who can modify and create databases as to whether you allow the Identity Governance installer to create and populate the databases or whether your database administrator creates and populates the databases.

This section explains the steps required to have the Identity Governance installer to create and populate the required databases for Identity Governance and its components while you install Identity Governance and its components on the same server. The installer creates the databases with the correct names, populates the schema and adds the correct tables and views for each database, and it adds any additional required artifacts.

The reason you would not use this option is if your business policies do not allow installers for programs or other people than the database administrator to install and configure databases. If this is the case for you, you must manually create and populate the databases. For more information, see Section 5.6, "Manually Creating and Populating the Databases," on page 100.

If you are installing Identity Reporting or Workflow Engine on a separate server, there are additional steps you must perform to have the Identity Governance installer create and populate the database for Identity Reporting or Workflow Engine. For more information, see Section 5.5, "Using the Identity Governance Installer to Create and Populate the Component Databases," on page 99.

There are some required steps you must perform before you start the Identity Governance installation. These required steps allow the installer to properly create, configure, and populate the Identity Governance databases for you.

To have the Identity Governance installer create and populate the database:

1. Ensure that Identity Governance supports the database version you are using. For more information, see Section 2.4, "Hardware and Software Requirements," on page 39.
2. Ensure that the database server and the Identity Governance server run on the same subnetwork in your IT environment.
3. (Conditional) If you are not using PostgreSQL, download the appropriate JDBC driver for your database and copy it to the server where you will install Identity Governance. For more information, see Section 5.7, "Adding the JDBC File to the Application Server," on page 101.
4. Ensure that you meet the prerequisites for the Identity Governance installation and then you can start the installation. For more information, see Section 6.3, "Prerequisites for Identity Governance," on page 134.
5. Use the information that you gather in the Table 6-1, "Identity Governance Installation Worksheet," on page 135 to install Identity Governance.
6. During the installation of Identity Governance, select **Configure database now** to have the installer create and populate the databases.
7. When the installation process completes, review the `Identity_Governance_InstallLog.log` file. The default location of the `Identity_Governance_InstallLog.log` file is here:
   - **Linux:** `/opt/netiq/idm/apps/idgov/logs`
   - **Windows:** `c:\netiq\idm\apps\idgov\logs`

5.5 Using the Identity Governance Installer to Create and Populate the Component Databases

If you are installing Identity Reporting on a separate server from Identity Governance, there are additional steps you must perform to have the Identity Governance installer create and populate the Identity Reporting database. The following steps assume that you are using the same database server for Identity Governance, Identity Reporting, and the Workflow Engine.

To have the Identity Governance installer create and populate the database:

1. Ensure that Identity Governance supports the database version you are using. For more information, see Section 2.4, "Hardware and Software Requirements," on page 39.
2. Ensure that all database servers run on the same subnetwork in your IT environment.
3. (Conditional) If you are not using PostgreSQL, download the appropriate JDBC driver for your database and copy it to the server where you will install the components. For more information, see Section 5.7, "Adding the JDBC File to the Application Server," on page 101.
4. During the installation of Identity Reporting or the Workflow Engine, select **Configure database now** to have the installer create and populate the databases.

5.6 Manually Creating and Populating the Databases

A Database Administrator can manually create the databases and use the SQL scripts to populate the databases. Your business policies that specify who can modify databases should determine whether you allow the Identity Governance installer to create and populate the databases, or whether your database administrator creates and populates the databases.

This section explains the steps required to have a database administrator manually create and populate the databases. The Identity Governance installer generates SQL scripts that can be run after the Identity Governance installation completes.

The database must exist before you install Identity Governance. The database administrator can populate the databases after you complete the Identity Governance installation. This option allows your database administrator to see what changes the Identity Governance installer makes to the database server before making the changes.

To use the SQL script to populate the databases:

1. Ensure that Identity Governance supports the database version you are using. For more information, see Section 2.4, “Hardware and Software Requirements,” on page 39.
2. Ensure that the database server and the Identity Governance server run on the same subnetwork in your IT environment.
3. (Conditional) If you are not using PostgreSQL, download the appropriate JDBC driver for your database and copy it to the application server. For more information, see Section 5.7, “Adding the JDBC File to the Application Server,” on page 101.
4. Create the appropriate database for your IT environment. For more information, see Section 5.8, “Creating the Databases before Installing Identity Governance,” on page 101.
5. Create a temporary database administrator account that the Identity Governance installer uses to populate the databases. For more information, see Section 5.9, “Creating a Temporary Database Administrator,” on page 113.
6. Start the Identity Governance Installer, then select **Generate SQL for later** in the **Database details** section of the installation program.
7. (Conditional) If you install Identity Reporting on a separate server from Identity Governance, install Identity Reporting after you install Identity Governance, and select **Generate SQL for later** in the **Database details** section of the installation program.
8. After the installation completes, have the database administrator review the SQL scripts to see what changes they make to the database.
9. Use the SQL scripts to populate the databases. For more information, see Section 5.11, “Configuring the Databases Using the SQL Scripts,” on page 117.

IMPORTANT: If you start Identity Governance or Identity Reporting before using the SQL scripts, Identity Governance automatically populates the databases for you. If you do not want to have the Identity Governance installer modify the databases, you must run the SQL scripts before starting Identity Governance or Identity Reporting.

5.7 Adding the JDBC File to the Application Server

To have Identity Governance run queries against the database, the application server must have access to the Java Database Connectivity (JDBC) driver file. If you are using PostgreSQL, the installer provides the JDBC driver file and copies it to the correct locations. If you are not using PostgreSQL, you must download the JDBC file from the website of the database you are using, and have it ready during the installation.

IMPORTANT: If you are not using PostgreSQL, you must perform these steps regardless of whether the Identity Governance installer is creating the databases. You must have a copy of the appropriate JDBC driver file located on the server where the Apache Tomcat instance is running for Identity Governance.

To add the JDBC file to the application server:

1. (Conditional) Ensure that you do not have an older version of the JDBC file or the installation fails. The directory is located:
   - **Linux:** `/opt/netiq/idm/apps/tomcat/lib` directory
   - **Windows:** `c:\netiq\idm\apps\tomcat\lib` directory
2. (Conditional) If you are not using PostgreSQL, download the appropriate JDBC file for your database. For more information, see Section 2.4.2, “Database Requirements,” on page 41.
3. (Conditional) If you are allowing the installer to create the databases, copy the JDBC driver file to a temporary directory on the server where the Apache Tomcat server is running. The Identity Governance installer copies the JDBC driver to the correct location.
4. (Conditional) If you are manually creating the databases, ensure that you copy the JDBC driver file to the Apache Tomcat `lib` directory of the Apache Tomcat instance Identity Governance uses.

5.8 Creating the Databases before Installing Identity Governance

You must first create the required databases if you use the SQL scripts. If you use the Identity Governance installer to create the databases, you can skip this section.

You can install the database server and create the databases for Identity Governance if you do not want the installation program to create the databases for you. If you do manually create the databases, you must add the schema for the different databases and create a temporary administrator. The installation program uses this information to 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.

IMPORTANT: The databases must not contain anything but the schema, or the installation of Identity Governance fails.

The Identity Governance installer needs the name of the databases to represent the operations, archive, data collection, provisioning workflow, and analytics databases for Identity Governance. For more information, see Section 5.1, “Understanding the Databases,” on page 95.

However, your database administrator might prefer to create the schema for the databases, as well as the database artifacts, rather than allowing the installation process to do so. If that is the case, then you would use the SQL scripts to create the schema and populate the databases. Use the steps for the appropriate database version to manually create the databases before starting the Identity Governance installation.

- Section 5.8.1, “Creating the Microsoft SQL Server Databases before Installing,” on page 102
- Section 5.8.2, “Creating the Oracle Schema Before Installing Identity Governance,” on page 105
- Section 5.8.3, “Creating the PostgreSQL Databases Before Installing,” on page 110
- Section 5.8.4, “Using Vertica,” on page 113

5.8.1 Creating the Microsoft SQL Server Databases before Installing

If your database administrator uses the SQL scripts to create and populate the databases for Identity Governance, Identity Reporting, and Workflow Engine, you must manually create the databases. Use the following information to create the databases for Identity Governance, Identity Reporting, and Workflow Engine.

- Section 5.8.1.1, “Creating the Microsoft SQL Server Databases before the Identity Governance Installation,” on page 102
- Section 5.8.1.2, “Creating the Microsoft SQL Server Database before Installing Identity Reporting,” on page 104
- Section 5.8.1.3, “Creating the Microsoft SQL Server Database before Installing the Workflow Engine,” on page 105

5.8.1.1 Creating the Microsoft SQL Server Databases before the Identity Governance Installation

Use the following procedure to create databases for Identity Governance on a Microsoft SQL Server. The database administrator would perform these steps if you did not want the Identity Governance installer to create the databases for you.

1. Install a supported version of SQL Server. For more information, see “Database Requirements” on page 41.
2. Ensure that the database server and the Identity Governance server run on the same subnetwork in your IT environment.
3. Create the databases, logins, users, and roles using the following commands:

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

ALTER DATABASE [igops] SET READ_COMMITTED_SNAPSHOT ON WITH NO_WAIT;
ALTER DATABASE [igarc] 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 [igarc] 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 [master];
GRANT VIEW SERVER STATE TO igops;
GO

USE [igarc];
CREATE USER [igarc] FOR LOGIN [igarc];
ALTER ROLE [db_owner] ADD MEMBER [igarc];
CREATE ROLE [IG_REPORT_ROLE];
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
```

4 Specify the same password for all databases.

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

5 (Conditional) To run Database Statistics for Identity Governance report, grant the reporting user additional privilege.

```
GRANT VIEW ANY DEFINITION TO igrptuser;
```

6 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 the previous release of Identity Governance
- **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

For more information about using SQL scripts, see Section 5.6, “Manually Creating and Populating the Databases,” on page 100.

5.8.1.2 Creating the Microsoft SQL Server Database before Installing Identity Reporting

As a system administrator, create a database, such as igrpt. 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 Microsoft SQL Server Database Administrator for the installation process” on page 114.

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

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

USE [igrpt];
CREATE USER [idm_rpt_cfg] FOR LOGIN [idm_rpt_cfg] WITH DEFAULT_SCHEMA =
[idm_rpt_cfg];
CREATE SCHEMA [IDM_RPT_CFG] AUTHORIZATION [idm_rpt_cfg];
ALTER AUTHORIZATION ON SCHEMA::[IDM_RPT_CFG] TO [idm_rpt_cfg];
ALTER ROLE [db_owner] ADD MEMBER [idm_rpt_cfg];
GO
```

2 When installing Identity Reporting, 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 the previous release of Identity Governance

- **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

For more information about using SQL scripts, see Section 5.6, “Manually Creating and Populating the Databases,” on page 100.

5.8.1.3 Creating the Microsoft SQL Server Database before Installing the Workflow Engine

The Identity Governance installer creates the databases for you. However, you have the option to create the database for the Workflow Engine. Use the following procedure to create the databases on an Microsoft SQL Server.

1. Install a supported version of the SQL Server. For more information, see Section 2.4.2, “Database Requirements,” on page 41.
2. Ensure that the database server and the Identity Governance server run on the same subnetwork in your IT environment.
3. Create the database, login, user, and role using the following commands:

```
USE [master];
CREATE DATABASE [igaworkflowdb];
ALTER DATABASE [igaworkflowdb] SET READ_COMMITTED_SNAPSHOT ON WITH
NO_WAIT;
CREATE LOGIN [igawfadmin] WITH PASSWORD = 'password';

USE [igaworkflowdb];
CREATE USER [igawfadmin] FOR LOGIN [igawfadmin];
ALTER ROLE [db_owner] ADD MEMBER [igawfadmin];
```

4. When installing Workflow Engine, 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
   - **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

   For more information about using SQL scripts, see Section 5.6, “Manually Creating and Populating the Databases,” on page 100.

5.8.2 Creating the Oracle Schema Before Installing Identity Governance

Oracle has you create schemas instead of separate databases like the other supported database types. Use the following procedure to create the schema for Identity Governance, Identity Reporting, and Workflow Engine on an Oracle database server. The database administrator would perform these steps if you did not want the Identity Governance installer to create the schema for you. 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), the temporary tablespace (`TEMP` by default), and the user schemas to represent the operations, archive, data collection, provisioning workflow, and analytics tables for Identity Governance and Identity Reporting.

- Section 5.8.2.1, “Creating the Oracle Schemas before Installing Identity Governance,” on page 106
- Section 5.8.2.2, “Creating the Oracle Schema before Installing Identity Reporting,” on page 108
- Section 5.8.2.3, “Creating the Oracle Schema before Installing the Workflow Engine,” on page 109

5.8.2.1 Creating the Oracle Schemas before Installing Identity Governance

This procedure assumes that you will use the default names for the schemas. For more information, see Section 5.1, “Understanding the Databases,” on page 95.

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

To create the Oracle schema for the Identity Governance databases:

1. Install a supported version of Oracle. For more information, see Section 2.4.2, “Database Requirements,” on page 41.
2. Ensure that the database server and the Identity Governance server run on the same subnetwork in your IT environment.
3. Create or identify the database that you want Identity Governance to use.
4. In the database, create the schemas for `igops`, `igarc`, `igdcs`, `igwf`, and `igara` with the following privileges:
    - select_catalog_role
    - Create session
    - Create table
    - Create view
    - Create sequence
    - Create procedure
    - Create trigger
    - Create type (`igops` and `igarc` only)
    - Create materialized view (`igops` only)
    - Analyze any (`igops` and `igarc` only)
    - Create public synonym (`igops` and `igarc` only)
    - Drop public synonym (`igops` and `igarc` only)

5 Specify the same password for all schemas.

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

6 Issue the following commands:

NOTE: If you use the default values of `users` and `temp`, skip these 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 igarc DEFAULT TABLESPACE USERS;
ALTER USER igarc TEMPORARY TABLESPACE TEMP;
ALTER USER igarc 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 igrptuser IDENTIFIED BY "igrptuser_password";
GRANT CREATE SESSION TO igrptuser;
ALTER USER igrptuser DEFAULT TABLESPACE USERS;
ALTER USER igrptuser TEMPORARY TABLESPACE TEMP;
CREATE ROLE IG_REPORT_ROLE NOT IDENTIFIED;
GRANT IG_REPORT_ROLE TO igrptuser;
```

7 Create the Identity Governance user, igrptuser, that has access to reporting information.

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

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

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

9 (Conditional) To run Database Statistics for Identity Governance report, grant the reporting user additional privilege.

```
GRANT SELECT_CATALOG_ROLE TO igrptuser;
```

10 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 the previous release of Identity Governance
- **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

For more information about using SQL statements after installation, see Section 5.11, "Configuring the Databases Using the SQL Scripts," on page 117.

5.8.2.2 Creating the Oracle Schema before Installing Identity Reporting

This procedure assumes that you will use the default name for the schema. For more information, see Section 5.1, "Understanding the Databases," on page 95.

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

1 Install a supported version of Oracle.

For more information, see Section 2.4.2, "Database Requirements," on page 41.

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

2 Ensure that the database server, Identity Governance, and Identity Reporting run in the same subnetwork.

3 Use the following commands to create the database:

```
CREATE USER idm_rpt_cfg IDENTIFIED BY idm_rpt_cfg_password;
GRANT CREATE SESSION, CREATE TABLE, CREATE VIEW, CREATE PROCEDURE,
CREATE SEQUENCE, CREATE TRIGGER, UNLIMITED TABLESPACE TO idm_rpt_cfg
```

4 To prepare the database, complete the following steps:

4a Create or identify the database that you want Identity Reporting to use, such as `igrpt`.

4b 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.

4c Specify a password for the schema.

5 When installing Identity Reporting, 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 the previous release of Identity Governance

- **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

For more information about using SQL statements after installation, see Section 5.11, "Configuring the Databases Using the SQL Scripts," on page 117.

5.8.2.3 Creating the Oracle Schema before Installing the Workflow Engine

This procedure assumes that you will use the default names for the schemas. For more information, see Section 5.1, "Understanding the Databases," on page 95.

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

1. Install a supported version of Oracle. For more information, see Section 2.4.2, "Database Requirements," on page 41.
2. Ensure that the database server and the Identity Governance server run on the same subnetwork in your IT environment.
3. Create or identify the database that you want the Workflow Engine to use.
4. In the database, create the user for igworkflowdb with the following privileges:
   - select_catalog_role
   - Create procedure
   - Create sequence
   - Create session
   - Create table
   - Create trigger
   - Create view
5. Create user igawfadmin identified by *password* and assign the following privileges:
   - grant connect, resource to igawfadmin
   - grant create table to igawfadmin
   - grant create view to igawfadmin
   - grant create sequence to igawfadmin
   - grant create procedure to igawfadmin
   - grant create trigger to igawfadmin
   - grant SELECT_CATALOG_ROLE to igawfadmin
   - grant ANALYZE ANY to igawfadmin
6. Issue the following commands:

   NOTE: If you use the default values of users and temp, skip these commands:
   - alter user *dbname* default tablespace users;
   - alter user *dbname* temporary tablespace temp;

```
ALTER USER igawfadmin DEFAULT TABLESPACE USERS;
ALTER USER igawfadmin TEMPORARY TABLESPACE TEMP;
ALTER USER igawfadmin QUOTA UNLIMITED ON USERS;
```

7 When installing Workflow Engine, 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
- **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

5.8.3 Creating the PostgreSQL Databases Before Installing

Use the following procedures to create the databases for Identity Governance, Identity Reporting, and Workflow Engine on a PostgreSQL database server. The database administrator performs these steps if you did not want the Identity Governance installer to create the databases for you. The installation program creates 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.

- Section 5.8.3.1, “Creating the PostgreSQL Databases before Installing Identity Governance,” on page 110
- Section 5.8.3.2, “Creating the PostgreSQL Database before Installing Identity Reporting,” on page 112
- Section 5.8.3.3, “Creating the PostgreSQL Database before Installing the Workflow Engine,” on page 112

5.8.3.1 Creating the PostgreSQL Databases before Installing Identity Governance

Use the following procedure to create the PostgreSQL databases for Identity Governance. You would use these if you do not want the Identity Governance installer to create the databases for you.

1 Install a supported version of PostgreSQL. For more information, see Section 2.4.2, “Database Requirements,” on page 41.

2 Ensure that the database server and the Identity Governance server run on the same subnetwork in your IT environment.

3. 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 archive_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;
   --(Optional if installing the cloud (AWS or Azure)
   GRANT "igops" TO current_user;
   GRANT "igarc" TO current_user;
   GRANT "igdcs" TO current_user;
   GRANT "igwf" TO current_user;
   GRANT "igara" TO current_user;
   --(End of optional)
   CREATE DATABASE igops WITH OWNER = operations_db_name ENCODING =
   'UTF8';
   CREATE DATABASE igarc WITH OWNER = archive_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';
   ```

4. Create the reporting user `igrptuser`.

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

5. Grant database connection privileges to the reporting user.

   ```
   GRANT CONNECT ON DATABASE "igops" TO "igrptuser";
   ```

6. Grant the reporting role to the reporting user.

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

7. 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.

8. When you install Identity Governance, specify one of the following settings:

   - **Configure database now** > **Update**, if you want the installation program to either create missing or update existing schemas, tables, and views, as when you migrate from the previous release of Identity Governance
   - **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

   For more information about using SQL statements after installation, see Section 5.11, "Configuring the Databases Using the SQL Scripts," on page 117.

5.8.3.2 Creating the PostgreSQL Database before Installing Identity Reporting

Use the following procedure to create the PostgreSQL database for Identity Reporting. You would use these if you do not want the Identity Governance installer to create the database for you.

1. Use the following commands to create the database for Identity Reporting:

   ```
   CREATE DATABASE "igrpt" WITH OWNER "pg_admin_user" TEMPLATE = template0
   ENCODING = 'UTF8';
   CREATE ROLE idm_rpt_cfg WITH LOGIN PASSWORD 'idm_rpt_cfg_password';
   \connect igrpt;
   CREATE SCHEMA idm_rpt_cfg AUTHORIZATION idm_rpt_cfg;
   GRANT CREATE ON SCHEMA public TO idm_rpt_cfg;
   GRANT CREATE ON SCHEMA idm_rpt_cfg TO idm_rpt_cfg;
   ```

2. Specify the same password for the Identity Reporting database as the Identity Governance 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.

3. When you install Identity Reporting or during the Identity Governance installation if you install Identity Reporting on the Identity Governance server, specify one of the following settings:

   - **Configure database now** > **Update**, if you want the installation program to either create missing or update existing schemas, tables, and views, as when you migrate from the previous release of Identity Reporting
   - **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 create the schemas, tables, and views

   For more information about using SQL statements after installation, see Section 5.11, “Configuring the Databases Using the SQL Scripts,” on page 117.

5.8.3.3 Creating the PostgreSQL Database before Installing the Workflow Engine

Use the following procedure to create the PostgreSQL database for the Workflow Engine. You can follow these steps if you do not want the Identity Governance installer to create the database for you.

1. Install a supported version of PostgreSQL. For more information, see Section 2.4.2, “Database Requirements,” on page 41.
2. Ensure that the database server and the Identity Governance server run on the same subnetwork in your IT environment.
3. Use the following commands to create the database for Workflow Engine:

```
CREATE ROLE igawfadmin PASSWORD 'password' LOGIN;
(if cloud) GRANT "igawfadmin" TO current_user;
CREATE DATABASE "igaworkflowdb" WITH OWNER "igawfadmin" TEMPLATE =
template0 ENCODING = 'UTF8';
GRANT ALL PRIVILEGES ON DATABASE "igaworkflowdb" TO "igawfadmin";
GRANT TEMPORARY, CONNECT ON DATABASE "igaworkflowdb" TO PUBLIC;
```

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

4. When installing Workflow Engine, 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
   - **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

5.8.4 Using Vertica

You can send the information in the SQL databases to Vertica for further analysis. You can configure Vertica to obtain the information from the supported database that you choose to use in Identity Governance. Use the Vertica documentation for the procedure to integrate Vertica with the specific database type. For more information, see the Vertica Documentation (https://www.vertica.com/documentation/vertica/9-2-x-documentation/).

5.9 Creating a Temporary Database Administrator

The installation process requires the password for a database administrator account that can create tables, views, and other artifacts in the databases. You can avoid using your database administrator account password by creating a temporary administrator for the installation process to use.

You would need a temporary database administrator account if the installer is creating the databases for you, or if you manually create the databases and allow the installer to populate the databases for you. Use the appropriate steps for your database type to create a temporary database administrator.

- Section 5.9.1, “Creating a Temporary Oracle Database Administrator for the Installation Process,” on page 114
- Section 5.9.2, “Creating a Temporary Microsoft SQL Server Database Administrator for the installation process,” on page 114
- Section 5.9.3, “Creating a Temporary PostgreSQL Database Administrator for the Installation Process,” on page 115

5.9.1 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.

IMPORTANT: If you create the Oracle database administrator in a database hosted in the cloud, ensure that you follow the documentation for the cloud platform you are using to have the proper rights for the database administrator. The following steps are for databases installed on-premises and might not be correct if you are installing in the cloud.

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 Section 5.11, “Configuring the Databases Using the SQL Scripts,” on page 117.

5.9.2 Creating a Temporary Microsoft SQL Server Database Administrator for the installation process

The installation process requires the password for an administrator account in Microsoft 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.

IMPORTANT: If you create the Microsoft SQL database administrator in a database hosted in the cloud, ensure that you follow the documentation for the cloud platform you are using to have the proper rights for the database administrator. The following steps are for databases installed on premise and might not be correct if you are installing in the cloud.

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 databases. Instead, the program generates a SQL file for each database, which your database administrator can run to update the database. For more information about using the SQL files, see "Configuring the Databases Using the SQL Scripts" on page 117.

5.9.3 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.

IMPORTANT: If you create the PostgreSQL database administrator in a database hosted in the cloud, ensure that you follow the documentation for the cloud platform you are using to have the proper rights for the database administrator. The following steps are for databases installed on premise and might not be correct if you are installing in the cloud.

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 Section 5.11, "Configuring the Databases Using the SQL Scripts," on page 117.

5.10 Creating the Schema for Each Database

If you choose to manually create the database or use the SQL scripts to allow your database administrator to create the database, you must manually add the schema to each Identity Governance database. If you allow the Identity Governance installer to create the databases, you can skip this section.

You can add the schema before the Identity Governance installation starts or after the installation completes. Perform the following steps to add the schema before the installation.

To create the schema for your specific database type:

1 Initialize or reset the database with the following Liquibase commands:

- **Linux:** Default location in `/opt/netiq/idm/apps/idgov/bin`

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

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

  ```
  db-init.bat -password database-password
  ```

2 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/ig-configutil.jar":"/opt/
  netiq/idm/apps/idgov/lib/postgresql-42.2.6.0.jar"
  com.netiq.iac.config.util.IacConfigUtil -dbDriver
  org.postgresql.Driver -dbUser igops -dbPassword password -dbUrl
  "jdbc:postgresql://postgresql-server:port/igops" -keystore "/opt/
  netiq/idm/apps/tomcat/conf/encrypt-keys.pkcs12" -storepass
  encryption-keystore-password -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/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" -keystore "/opt/
  netiq/idm/apps/tomcat/conf/encrypt-keys.pkcs12" -storepass
  encryption-keystore-password -script "/opt/netiq/idm/apps/idgov/
  scripts/all-import-configs.script"
  ```

- **Microsoft SQL:** Use 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/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" -keystore "/opt/netiq/idm/apps/
  tomcat/conf/encrypt-keys.pkcs12" -storepass encryption-keystore-
  password -script "/opt/netiq/idm/apps/idgov/scripts/all-import-
  configs.script"
  ```

NOTE: The commands in these examples contain the default installation path of `/opt/netiq/idm/apps`.

5.11 Configuring the Databases Using the SQL Scripts

During the installation process, you might have specified **Generate SQL for later** to configure the databases or schema after the 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 Microsoft SQL, the administrator also needs to create the logins, users, and roles for the Identity Governance databases. If you select **Configure Database Now** during the installation, you can skip this section.

Identity Governance, Identity Reporting, and Workflow Engine need the following SQL scripts, located by default in:

- **Linux:** `/opt/netiq/idm/apps/idgov/sql`, `/opt/netiq/idm/apps/idrpt/sql`, and `/opt/netiq/idm/apps/wfe/sql`
- **Windows:** `c:\netiq\idm\apps\idgov\sql`, `c:\netiq\idm\apps\idrpt\sql`, and `c:\netiq\idm\apps\wfe\sql`

These are files for the specific database or schema:

- `ops-init.sql` for the `igops` database or schema
- `arc-init.sql` for the `igarc` 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
- `rpt-init-01-idm_rpt_cfg.sql` for the `igrpt` database or schema
- wfe-00-workflow.sql for the `wfe` database or schema

The installation program uses an additional file in the reporting SQL directory, `create_rpt_roles_and_schemas.sql`, to initialize the reporting database. It remains so the database administrator can see how the installer would modify the reporting database.

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

- Section 5.11.1, “Configuring the PostgreSQL Databases for Identity Governance,” on page 118
- Section 5.11.2, “Configuring the Oracle Database for Identity Governance,” on page 120
- Section 5.11.3, “Configuring the Microsoft SQL Databases for Identity Governance,” on page 121
- Section 5.11.4, “Configuring the Identity Reporting Database,” on page 122
- Section 5.11.5, “Configuring the Workflow Engine Database,” on page 124

5.11.1 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, igara, and igarc database passwords rather than the database administrator password.

Ensure that the scripts are located on the database server. If you cannot access the SQL scripts, see Section 12.2, “Manually Generating the Database Schema after the Installation,” on page 253.

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

```
CREATE ROLE operations_db_name LOGIN password 'password';
CREATE ROLE archive_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 igarc WITH OWNER = archive_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 igarc 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 igarc WITH OWNER = igarc 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 directories:

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

3 Have the database administrator run the scripts in the order listed. For example, if you have the PostgreSQL utility and psql installed at `/usr/lib/postgresql/bin/psql` use the following commands:

```
/usr/lib/postgresql/bin/psql -h localhost -p 5432 -U igops igops -f /
tmp/sql/ops-init.sql
/usr/lib/postgresql/bin/psql -h localhost -p 5432 -U igarc igarc -f /
tmp/sql/arc-init.sql
/usr/lib/postgresql/bin/psql -h localhost -p 5432 -U igdcs igdcs -f /
tmp/sql/dcs-init.sql
/usr/lib/postgresql/bin/psql -h localhost -p 5432 -U igwf  igwf  -f /
tmp/sql/wf-init.sql
/usr/lib/postgresql/bin/psql -h localhost -p 5432 -U igara igara -f /
tmp/sql/ara-init.sql
```

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/
postgresql-42.2.6.0.jar" com.netiq.iac.config.util.IacConfigUtil -
dbDriver org.postgresql.Driver -dbUser igops -dbPassword password -
dbUrl "jdbc:postgresql://postgresql-server:port/igops-db" -keystore "/
opt/netiq/idm/apps/tomcat/conf/encrypt-keys.pkcs12" -storepass
encryption-keystore-password -script "/opt/netiq/idm/apps/idgov/
scripts/all-import-configs.script"
```

5.11.2 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.

Ensure that the scripts are located on the database server. If you cannot access the SQL scripts, see Section 12.2, “Manually Generating the Database Schema after the Installation,” on page 253.

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 Have the database administrator run the scripts in the order listed. For example, if you have the Oracle `sqlplus` is on the `$PATH` at `/home/oracle/app/oracle/product/12.1.0/db_rpt_1/bin/sqlplus` use the following commands:

   ```
   sqlplus -L igops/"password"@<server>:1521/pdborcl @ /tmp/sql/ops-init.sql
   sqlplus -L igarc/"password"@<server>:1521/pdborcl @ /tmp/sql/arc-init.sql
   sqlplus -L igdcs/"password"@<server>:1521/pdborcl @ /tmp/sql/dcs-init.sql
   sqlplus -L igwf/"password"@<server>:1521/pdborcl @ /tmp/sql/wf-init.sql
   sqlplus -L igara/"password"@<server>:1521/pdborcl @ /tmp/sql/ara-init.sql
   ```

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" -keystore "/opt/netiq/idm/apps/tomcat/conf/encrypt-keys.pkcs12" -storepass encryption-keystore-password -script "/opt/netiq/idm/apps/idgov/scripts/all-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 1g0p5Pa55 -dbUrl
"jdbc:oracle:thin:@myoracle.mycompany.com:1521/mysid" -keystore "/opt/
netiq/idm/apps/tomcat/conf/encrypt-keys.pkcs12" -storepass K3yPa55 -
script "/opt/netiq/idm/apps/idgov/scripts/all-import-configs.script"
```

5.11.3 Configuring the Microsoft SQL Databases 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.

Ensure that the scripts are located on the database server. If you cannot access the SQL scripts, see Section 12.2, “Manually Generating the Database Schema after the Installation,” on page 253.

NOTE: You must create the roles with the `igops`, `igarc`, `igdcs`, `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 directories:

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

3 Have the database administrator run the scripts in the order listed. For example, if `sqlcmd` is on the *PATH* use the following commands:

```
sqlcmd -S <server IP or DNS>,1433 -U igops -d igops -P "password" -i
TEMP\sql\ops-init.sql
sqlcmd -S <server IP or DNS>,1433 -U igarc -d igarc -P "password" -i
TEMP\sql\arc-init.sql
sqlcmd -S <server IP or DNS>,1433 -U igdcs -d igdcs -P "password" -i
TEMP\sql\dcs-init.sql
sqlcmd -S <server IP or DNS>,1433 -U igwf -d igwf -P "password" -i
TEMP\sql\wf-init.sql
sqlcmd -S <server IP or DNS>,1433 -U igara -d igara -P "password" -i
TEMP\sql\ara-init.sql
```

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"  -
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;encrypt=false;databaseName=igops" -keystore "/opt/netiq/
idm/apps/tomcat/conf/encrypt-keys.pkcs12" -storepass encryption-
keystore-password -script "/opt/netiq/idm/apps/idgov/scripts/all-
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/msjdbc.jar"
com.netiq.iac.config.util.IacConfigUtil -dbDriver
com.microsoft.sqlserver.jdbc.SQLServerDriver -dbUser igops -dbPassword
1g0p5Pa55 -dbUrl "jdbc:sqlserver://
mysever.netiq.com:1433;encrypt=false;databaseName=igops" -keystore "/
opt/netiq/idm/apps/tomcat/conf/encrypt-keys.pkcs12" -storepass K3y_Pa55
-script "/opt/netiq/idm/apps/idgov/scripts/all-import-configs.script"
```

5.11.4 Configuring the Identity Reporting Database

If you select **Generate SQL for later** during installation, have the database administrator run the SQL script to configure the Identity Reporting database, then configure global configuration values. 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 Section 12.2, “Manually Generating the Database Schema after the Installation,” on page 253. Ensure that the script is located on the database server.

1 Generate the Identity Reporting database. The following is a list of example commands to run on the different databases to generate the Identity Reporting database.

PostgreSQL

For example, if you have the PostgreSQL utility and `psql` installed at `/usr/lib/postgresql/bin/psql` use the following command:

```
/usr/lib/postgresql/bin/psql -h localhost -p 5432 -U idm_rpt_cfg igrpt
-f /tmp/sql/rpt-init-01-idm_rpt_cfg.sql
```

Oracle

```
sqlplus -L idm_rpt_cfg/"password"@<server>:1521/pdborcl @ /tmp/sql/rpt-
init-01-idm_rpt_cfg.sql
```

Microsoft SQL Server For example, if `sqlcmd` is on the *`PATH`* use the following command:

```
sqlcmd -S <server IP or DNS>,1433 -U idm_rpt_cfg -d igrpt -P "password"
-i TEMP\sql\rpt-init-01-idm_rpt_cfg.sql
```

2 (Conditional) When Identity Reporting is installed on a separate server than Identity Governance, enter the following command to populate the global configuration values in the database:

PostgreSQL

```
"/opt/netiq/idm/apps/jre/bin/java" -Djava.util.logging.config.file="/
opt/netiq/idm/apps/idrpt/conf/logging.properties" -
Djava.security.egd=file:///dev/urandom -Dcom.netiq.ism.config="/opt/
netiq/idm/apps/idrpt/conf/unused.props" -classpath "/opt/netiq/idm/
apps/idrpt/lib/ig-configutil.jar":"/opt/netiq/idm/apps/idrpt/lib/
postgresql-42.6.0.jar" com.netiq.iac.config.util.IacConfigUtil -
dbDriver org.postgresql.Driver -dbUser igops-user -dbPassword password
-dbUrl "jdbc:postgresql://postgresql-server:port/igops-db" -keystore "/
opt/netiq/idm/apps/tomcat/conf/encrypt-keys.pkcs12" -storepass
encryption-keystore-password -script "/opt/netiq/idm/apps/idrpt/
scripts/all-import-configs.script"
```

For example:

```
"/opt/netiq/idm/apps/jre/bin/java" -Djava.util.logging.config.file="/
opt/netiq/idm/apps/idrpt/conf/logging.properties" -
Djava.security.egd=file:///dev/urandom -Dcom.netiq.ism.config="/opt/
netiq/idm/apps/idrpt/conf/unused.props" -classpath "/opt/netiq/idm/
apps/idrpt/lib/ig-configutil.jar":"/opt/netiq/idm/apps/idrpt/lib/
postgresql-42.6.0.jar" com.netiq.iac.config.util.IacConfigUtil -
dbDriver org.postgresql.Driver -dbUser igops -dbPassword 1g0p5Pa55 -
dbUrl "jdbc:postgresql://myserver.netiq.com:5432/igops" -keystore "/
opt/netiq/idm/apps/tomcat/conf/encrypt-keys.pkcs12" -storepass K3y_Pa55
-script "/opt/netiq/idm/apps/idrpt/scripts/all-import-configs.script"
```

Oracle

```
"/opt/netiq/idm/apps/jre/bin/java" -Djava.util.logging.config.file="/
opt/netiq/idm/apps/idrpt/conf/logging.properties" -
Djava.security.egd=file:///dev/urandom -Dcom.netiq.ism.config="/opt/
netiq/idm/apps/idrpt/conf/unused.props" -classpath "/opt/netiq/idm/
apps/idrpt/lib/ig-configutil.jar":"/opt/netiq/idm/apps/idrpt/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" -keystore "/opt/netiq/idm/
apps/tomcat/conf/encrypt-keys.pkcs12" -storepass encryption-keystore-
password -script "/opt/netiq/idm/apps/idrpt/scripts/all-import-
configs.script"
```

For example:

```
"/opt/netiq/idm/apps/jre/bin/java" -Djava.util.logging.config.file="/
opt/netiq/idm/apps/idrpt/conf/logging.properties" -
Djava.security.egd=file:///dev/urandom -Dcom.netiq.ism.config="/opt/
netiq/idm/apps/idrpt/conf/unused.props" -classpath "/opt/netiq/idm/
apps/idrpt/lib/ig-configutil.jar":"/opt/netiq/idm/apps/idrpt/lib/
ojdbc.jar" com.netiq.iac.config.util.IacConfigUtil -dbDriver
oracle.jdbc.OracleDriver -dbUser igops -dbPassword 1g0p5Pa55 -dbUrl
"jdbc:oracle:thin:@myoracle.mycompany.com:1521/mysid" -keystore "/opt/
netiq/idm/apps/tomcat/conf/encrypt-keys.pkcs12" -storepass K3y_Pa55 -
script "/opt/netiq/idm/apps/idrpt/scripts/all-import-configs.script"
```

Microsoft SQL Server

```
"/opt/netiq/idm/apps/jre/bin/java" -Djava.util.logging.config.file="/
opt/netiq/idm/apps/idrpt/conf/logging.properties"  -
Dcom.netiq.ism.config="/opt/netiq/idm/apps/idrpt/conf/unused.props" -
classpath "/opt/netiq/idm/apps/idrpt/lib/ig-configutil.jar":"/opt/
netiq/idm/apps/idrpt/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;encrypt=false;databaseName=igops" -keystore "/opt/netiq/
idm/apps/tomcat/conf/encrypt-keys.pkcs12" -storepass encryption-
keystore-password -script "/opt/netiq/idm/apps/idrpt/scripts/all-
import-configs.script"
```

For example:

```
"/opt/netiq/idm/apps/jre/bin/java" -Djava.util.logging.config.file="/
opt/netiq/idm/apps/idrpt/conf/logging.properties"  -
Dcom.netiq.ism.config="/opt/netiq/idm/apps/idrpt/conf/unused.props" -
classpath "/opt/netiq/idm/apps/idrpt/lib/ig-configutil.jar":"/opt/
netiq/idm/apps/idrpt/lib/msjdbc.jar"
com.netiq.iac.config.util.IacConfigUtil -dbDriver
com.microsoft.sqlserver.jdbc.SQLServerDriver -dbUser igops -dbPassword
1g0p5Pa55 -dbUrl "jdbc:sqlserver://
myserver.netiq.com:1433;encrypt=false;databaseName=igops" -keystore "/
opt/netiq/idm/apps/tomcat/conf/encrypt-keys.pkcs12" -storepass K3y_Pa55
-script "/opt/netiq/idm/apps/idrpt/scripts/all-import-configs.script"
```

5.11.5 Configuring the Workflow Engine Database

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

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

If you cannot access the SQL scripts, see Section 12.2, “Manually Generating the Database Schema after the Installation,” on page 253.

Ensure that the script is located in the database server. The examples listed below are the commands that the Database Administrator can run on specific databases to generate the Workflow Engine database.

PostgreSQL

For example, if you have the PostgreSQL utility and `psql` installed at `/usr/lib/postgresql/bin/psql` use the following command:

```
/usr/lib/postgresql/bin/psql -h localhost -p 5432 -U igawfadmin
igaworkflowdb -f /tmp/sql/wfe-00-workflow.sql
```

Oracle

For example, if you have the Oracle `sqlplus` on the `$PATH` at `/home/oracle/app/oracle/product/12.1.0/db_wfe_1/bin/sqlplus` use the following command:

```
sqlplus -L igawfadmin /"password"@<server>:1521/pdborcl @ /tmp/sql/wfe-
00-workflow.sql
```

Microsoft SQL Server

For example, if `sqlcmd` is on the `%PATH%` use the following command:

```
sqlcmd -S <server IP or DNS>,1433 -U igawfadmin -d igaworkflowdb -P
"password" -f 65001 -i %TEMP%\sql\wfe-00-workflow.sql
```

5.12 How to Change the Configuration Options for the Databases

Identity Governance allows you to change some of the configuration options for the databases that you define during the installation. The options that you can change are:

- JDBC driver for the database
- URL of the database
- Database names
- Password for the databases

Identity Governance stores this information in multiple locations. You must update this information in all of the locations to have Identity Governance see the changes. Use the following information to update the database configuration information in Identity Governance.

- Section 5.12.1, “Updating the Identity Governance Configuration Update Utility for the Database Changes,” on page 126
- Section 5.12.2, “Updating the Identity Governance Configuration Utility for the Database Changes,” on page 127
- Section 5.12.3, “Updating the Identity Governance Database Initialization File for the Database Changes,” on page 127
- Section 5.12.4, “Updating the Apache Tomcat sever.xml File,” on page 129

5.12.1 Updating the Identity Governance Configuration Update Utility for the Database Changes

The database changes must be updated in the properties file of the Identity Governance Configuration Update utility. You must edit the properties file to update the database changes.

1. Make the appropriate corresponding changes in the main database (`igops`) on the database server for the:
   - JDBC driver for the database
   - URL of the database
   - Database name
   - Password for the database
2. Log in to the server running Identity Governance as an administrative user.
3. Stop Apache Tomcat. For more information, see Section 3.5.3, "Starting and Stopping Apache Tomcat," on page 50.
4. Open the properties file for the Identity Governance Configuration Update utility in a text editor. The default location is:
   - **Linux:** `/opt/netiq/idm/apps/configupdate/configupdate.sh.properties`
   - **Windows:** `c:\netiq\idm\apps\configupdate\configupdate.bat.properties`
5. Make the appropriate changes to the following parameters:

   dbDriver

   Specify the name of the new JDBC driver. You would change this if you were adding a patched driver.

   dbURL

   Specify the updated URL and port to access the database.

   dbUser

   Specify the new name for the database.

   dbPassword

   Specify the new password for the database.
6. (Conditional) If you do not want to have the password set in clear text.

   6a Encrypt the password by running the following script:
   - **Linux:** `/opt/netiq/idm/apps/idgov/bin/encrypt-password.sh` *`password`*
   - **Windows:** `c:\netiq\idm\apps\idgov\bin\encrypt-password.sh` *`password`*

   6b Copy the new value and replace the value in the `dbPassword` property.
7. Save and close the file.
8. Restart Apache Tomcat on the Identity Governance server. For more information, see Section 3.5.3, "Starting and Stopping Apache Tomcat," on page 50.

5.12.2 Updating the Identity Governance Configuration Utility for the Database Changes

You must edit the Identity Governance Configuration utility to update the database changes.

1. Make the appropriate corresponding changes in the main database (`igops`) on the database server for the:
   - JDCB driver for the database
   - URL of the database
   - Database name
2. Log in to the server running Identity Governance as an administrative user.
3. Open the Identity Governance Configuration utility in a text editor. The default location is:
   - **Linux:** `/opt/netiq/idm/apps/idgov/bin/configutil.sh`
   - **Windows:** `c:\netiq\idm\apps\idgov\bin\configutil.bat`
4. Make the appropriate changes to the following parameters:

   _db_driver

   Specify the name of the new JDBC driver. You would change this if you had a patched version of the driver.

   _db_url

   Specify the updated URL and port to access the database.

   _db_user

   Specify the new name for the database or encode the password.

   _db_jdbc_jar

   Specify the path to the JDBC driver JAR file.

   NOTE: Make changes here only if your database version required an updated JDBC driver JAR.
5. Save and close the file.

5.12.3 Updating the Identity Governance Database Initialization File for the Database Changes

You must edit the Identity Governance database initialization file to make Identity Governance aware of what changes you made to the database in case you ever have to reinitialize the schema. For more information, see Section 12.2, “Manually Generating the Database Schema after the Installation,” on page 253.

To change the database information in the database initialization file:

1. Make the appropriate corresponding changes in the main database (`igops`) on the database server for the:
   - JDCB driver for the database

- URL of the database
- Database name

2 Edit the Identity Governance database initialization file to change the database names or the URL and port for the database server.

2a Access the database initialization files. The default locations are:

- **Linux:** `/opt/netiq/idm/apps/idgov/bin/db-init.sh`
- **Windows:** `c:\netiq\idm\apps\idgov\bin\db-init.bat`

2b Open the database initialization file in a text editor.

2c Change the following entries in the file for your database:

Database name

Change each entry that lists a database name. Change the following entries:

- `_db_name_ops=`
- `_db_name_arc=`
- `_db_name_dcs=`
- `_db_name_wf=`
- `_db_name_ara=`

Database URL

Specify the URL and port for your database for each of the following lines:

- `_db_url_ops=`
- `_db_url_arc=`
- `_db_url_dcs=`
- `_db_url_wf=`
- `_db_url_ara=`

Database Driver

Specify the new JDBC JAR file in the following entry: `_dc_jdbc_jar=`

3 Edit the Identity Reporting database initialization file to change the database names or the URL and port for the database server.

3a Access the database initialization files. The default locations are:

- **Linux:** `/opt/netiq/idm/apps/idrpt/bin/db-init.sh`
- **Windows:** `c:\netiq\idm\apps\idrpt\bin\db-init.bat`

3b Open the database initialization file in a text editor.

3c Change the following entries in the file for your database:

Database URL

Specify the URL and port for your database in the following line: `_db_url_rpt=`

Database Driver

Specify the new JDBC JAR file in the following entry: `_dc_jdbc_jar=`

4 Edit the Workflow Engine database initialization file to change the database names or the URL and port for the database server.

  4a Access the database initialization files. The default locations are:

  - **Linux:** `/opt/netiq/idm/apps/wfe/bin/db-init.sh`
  - **Windows:** `c:\netiq\idm\apps\wfe\bin\db-init.bat`

  4b Open the database initialization file in a text editor.

  4c Change the following entries in the file for your database:

  Database name

  Change each entry that lists a database name. Change the following entry: `_db_role_name=`

  Database URL

  Specify the URL and port for your database for each of the following lines:

  - `_db_url_wfe=`
  - `_db_url_wfe_consumer=`

  Database Driver

  - Specify the name of the JDBC driver in the following entry: `_db_driver=`
  - Specify the new JDBC JAR file in the following entry: `_dc_jdbc_jar=`

5 Save and close the file.

5.12.4 Updating the Apache Tomcat sever.xml File

You must update the `server.xml` file for the Apache Tomcat instance that you use for Identity Governance.

1 Make the appropriate corresponding changes in the database for the:

  - JDCB driver for the database
  - URL of the database
  - Database names
  - Password for the databases

2 Log in to the server running Identity Governance as an administrative user.

3 Stop Apache Tomcat. For more information, see Section 3.5.3, “Starting and Stopping Apache Tomcat,” on page 50.

4 Open the Apache Tomcat `server.xml` file for Identity Governance in a text editor. The default location is:

  - **Linux:** `/opt/netiq/idm/apps/tomcat/conf/server.xml`
  - **Windows:** `c:\netiq\idm\apps\tomcat\conf\server.xml`

5 Make the appropriate changes to the following parameters:

  username

  Specify the name of the database names in the `username=` entries.

  url

  Specify the updated URL and port to access the database for the `url=` entries.

6 (Conditional) You do not want to have the password set in clear text.

   6a Encrypt the password by running the following script:

   - **Linux:** `/opt/netiq/idm/apps/idgov/bin/encrypt-password.sh` *`password`*
   - **Windows:** `c:\netiq\idm\apps\idgov\bin\encrypt-password.sh` *`password`*

   6b Copy the new value and replace the value in the **password** field.

7 Save and close the file.

8 Start Apache Tomcat. For more information, see Section 3.5.3, "Starting and Stopping Apache Tomcat," on page 50.

6 Installing Identity Governance

This section provides information about installing and configuring Identity Governance. You must review the installation process, including the prerequisites and requirements, before beginning:

- Section 6.1, “Checklist for Installing Identity Governance,” on page 131
- Section 6.2, “Installing the Optional Components for Identity Governance,” on page 132
- Section 6.3, “Prerequisites for Identity Governance,” on page 134
- Section 6.4, “Identity Governance Installation Worksheet,” on page 134
- Section 6.5, “Installing Identity Governance,” on page 153
- Section 6.6, “Silently Installing Identity Governance and its Components,” on page 155

6.1 Checklist for Installing Identity Governance

Before beginning the installation process, you must review the following steps:

	Checklist Items
□	1. Ensure that your environment meets the prerequisites and requirements for hosting Identity Governance. For more information, see Section 6.3, “Prerequisites for Identity Governance,” on page 134 and Section 2.4, “Hardware and Software Requirements,” on page 39.
□	2. Decide whether you want to install Identity Governance in a clustered environment. For more information about the requirements, see Section 2.3.4, “Ensuring High Availability or Load Balancing for Identity Governance,” on page 35.
	3. Determine if you need Identity Reporting or Workflow Engine. For more information, see “Understanding Identity Reporting” on page 17 and “Understanding Workflow Engine” on page 17.
□	4. Determine how many servers to use with your Identity Governance deployment. For more information, see Section 2.3, “Recommended Production Environment Installation Scenarios,” on page 32.
□	5. Determine which installation method you will use. For more information, see Section 1.2, “Understanding the Installation Methods,” on page 18.
□	6. Ensure that your environment has the required components installed and configured. For more information, see Chapter 3, “Installing Required Components,” on page 45.

	Checklist Items
□	7. Ensure that you installed one of the following supported databases on a separate server for a production environment. □ (Conditional) Microsoft SQL Server □ (Conditional) Oracle □ (Conditional) PostgreSQL For more information about supported databases and versions, see Section 2.4.2, “Database Requirements,” on page 41.
□	8. Ensure that your environment has a supported version of OSP or Access Manager installed. For more information, see Chapter 4, “Installing an Authentication Service,” on page 57.
□	9. The installation directory for Identity Governance cannot contain spaces in the path. If the path contains spaces, the installation fails.
□	10. Complete the Identity Governance Installation Worksheet before starting the installation. For more information, see Section 6.4, “Identity Governance Installation Worksheet,” on page 134.
□	11. (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 trust store. For more information, see Section 3.9, “Securing Connections with TLS/SSL,” on page 51.
□	12. Install Identity Governance and Identity Reporting (optional): ◆ For a guided installation, see Section 6.5, “Installing Identity Governance,” on page 153. ◆ For silent installation, see Section 6.6, “Silently Installing Identity Governance and its Components,” on page 155.

6.2 Installing the Optional Components for Identity Governance

Identity Governance allows you to install other components that provide additional functionality to your deployment. These other components are optional to install. Whether you choose to install these components or not depends if you need the additional functionality these components provide.

You can choose to install and configure these components when you install Identity Governance or you can add these components after the installation. If you want to have these optional components, it is best to have the auditing and email components installed before starting the Identity Governance installation. You can install Identity Reporting or Workflow Engine on the same server as Identity Governance, or you can install them on a separate server, depending on your environment. For more information, see Section 2.3, “Recommended Production Environment Installation Scenarios,” on page 32.

The optional components are:

- **Auditing:** Identity Governance generates common event format (CEF) events that you can forward to an audit server to analyze the events and to create reports. These reports allow you to prove that you comply with regulations.

  If you want auditing capabilities, we recommend that you install a supported audit server before starting the Identity Governance installation. For more information, see Section 2.4.6, “Audit Server System Requirements,” on page 43.
- **Email Notifications:** Identity Governance can send emails to people who must take action in Identity Governance or it can send emails to administrators if something is wrong with the system.

  If you want to enable email notifications, we recommend that you have an SMTP server installed and running before starting the installation. If you want to guarantee the delivery of the emails, ensure that you have ActiveMQ installed on the Identity Governance server before starting the installation. For more information, see Section 3.10, “Installing Optional Components,” on page 53.
- **Identity Reporting:** Identity Reporting generates reports that show critical business information about various aspects of your Identity Manager configuration, including information collected from the identity services and managed systems such as Active Directory or SAP. Identity Reporting provides a set of predefined reports definitions you can use to generate reports. It also gives you the option to import custom reports.

  If you are installing Identity Reporting on the same server as Identity Governance, continue with this section and gather the appropriate information in Table 6-1, “Identity Governance Installation Worksheet,” on page 135.

  If you are installing Identity Reporting on a separate server, you must install Identity Governance first and then install Identity Reporting on a separate server. For more information, see Chapter 7, “Installing Identity Reporting,” on page 163.

  If you are installing Identity Governance after you install Identity Governance, and if Identity Governance is installed on another server and its Tomcat uses SSL, you can have Identity Reporting retrieve the Identity Governance certificate even if it is running on a different server.
- **Workflow Engine:** The Workflow Engine runs the workflow at runtime and manages the approval tasks for approvers. The Workflow Engine persists the different workflow states in the `igaworkflowdb` database and uses a REST service to obtain the tasks and workflow history from the Workflow Engine service.

  If you are installing the Workflow Engine on the same server as Identity Governance, continue with this section and gather the appropriate information in Table 6-1, “Identity Governance Installation Worksheet,” on page 135.

  If you are installing the Workflow Engine on a separate server, you must install Identity Governance first and then install the Workflow Engine on a separate server. For more information, see Chapter 8, “Installing Workflow Engine,” on page 183.

6.3 Prerequisites for Identity Governance

Identity Governance includes prerequisites for installation and for authentication.

Identity Governance Installation Prerequisites

Review the following items that affect the installation of Identity Governance:

- ❒ You can install Identity Governance and OSP in a stateless cluster. For more information about the installation requirements, see Section 2.3.4, “Ensuring High Availability or Load Balancing for Identity Governance,” on page 35.
- ❒ The Identity Governance server must include the supported versions of Zulu OpenJDK and Apache Tomcat application server.
- ❒ For best performance, do not install Identity Governance on the same server as the databases; however, the database server and the Identity Governance server must run in the same subnetwork.
- ❒ 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.
- ❒ (Optional) If you want to enable auditing for Identity Governance using TLS, and if you want the Identity Governance installation to automatically retrieve the audit server certificate into the Identity Governance trust-store, you must ensure the following before you begin the Identity Governance installation:
  - Configure the auditing server to use TLS
  - Ensure the auditing server is running

Authentication Prerequisites

Review the following prerequisites for authentication to Identity Governance:

- ❒ Do not use mixed case domains. Identity Governance utilizes OAuth2 for authentication. OAuth2 does not support mixed case domains. For more information, see “RCF 3986 Section 6.2.1 Simple String Comparison”.
- ❒ To use an identity service 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” in *Identity Governance User and Administration Guide*.
- ❒ To integrate Identity Governance with Identity Manager, the Identity Manager component must already be installed and configured with OSP.
- ❒ Ensure that the communication ports that you want to use are open in the firewall. For more information, see Appendix A, “Ports Used in Identity Governance,” on page 313.

6.4 Identity Governance Installation Worksheet

Use the following worksheet to gather the information that you need to complete the Identity Governance installation successfully. You can use this information for the guided installation, the console installation, or the silent installation.

Table 6-1 Identity Governance Installation Worksheet

Item	Description	Value
Components to Install		
Identity Governance, and or Identity Reporting, Workflow Engine	The Identity Governance installer installs Identity Governance, Identity Reporting, and the Workflow Engine. You must decide if you want to install Identity Reporting and the Workflow Engine and if you want to run them on the same server as Identity Governance. If you want to install and run Identity Reporting and the Workflow Engine on servers separate from Identity Governance, you must run the Identity Governance installer on those separate servers by clearing the Identity Governance option, and selecting only the components you want for that server.	
Identity Governance Installation Location	Specify the installation path for Identity Governance. **WARNING:** Spaces in the path are not supported. The default directory is: ◆ **Linux:** `/opt/netiq/idm/apps/idgov` ◆ **Windows:** `C:\netiq\idm\apps\idgov`	

Item	Description	Value
(Conditional) Identity Reporting Installation Location	If you are installing Identity Reporting on the same server as Identity Governance, specify the installation path for Identity Reporting. **WARNING:** Spaces in the path are not supported. The default default directory is: ◆ **Linux:** `/opt/netiq/idm/apps/idrpt` ◆ **Windows:** `C:\netiq\idm\apps\idrpt`	
(Conditional) Workflow Engine Installation Location	If you are installing the Workflow Engine on the same server as Identity Governance, specify the installation path. **WARNING:** Spaces in the path are not supported. The default directory is: ◆ **Linux:** `/opt/netiq/idm/apps/wfe` ◆ **Windows:** `C:\netiq\idm\apps\wfe`	
Apache Tomcat Installation	Specify the address of the application that represents the settings of the URL that users need to connect to Identity Governance. For example: `https://myserver.mycompany.com:8443`	

Item	Description	Value
Tomcat Installation Location	Specify the installation path for Apache Tomcat. **WARNING:** Spaces in the path are not supported. The default directory is: ◆ **Linux:** `/opt/netiq/idm/apps/tomcat` ◆ **Windows:** `C:\netiq\idm\apps\tomcat`	
Runtime host name	**WARNING:** Use the fully qualified domain name (FQDN) rather than localhost or an IP address. Specify the runtime host name for the local instances of Apache Tomcat that Identity Governance uses. If you have installed OSP on this same server, OSP uses this same instance of Apache Tomcat. If you are installing Identity Reporting and/or Workflow Engine, Identity Reporting and Workflow Engine use this same instance of Apache Tomcat. The Identity Governance installer creates a trust store for the certificates to allow for SSL/TLS communication. Certificates use the fully qualified domain name (FQDN) of the servers, which is why you must use the DNS name of the server instead of an IP address.	
Runtime port	Specify the runtime port that the local instance of Apache Tomcat uses. For http, the default port is 8080. For https, the default port is 8443.	
Runtime identifier	In a non-clustered environment, specify the local server name. In a clustered environment, specify the unique name for the current node. For example, node1.	

Item	Description	Value
Apache Tomcat Java Home > JRE home folder	Specify the path to the Zulu JRE home directory. The Zulu JRE is installed when you install Zulu OpenJDK. The installation process uses Java for several processes, such as to run commands and create security stores. **WARNING:** Spaces in the path are not supported. The default location is: ◆ **Linux:** `/opt/netiq/idm/apps/jre` ◆ **Windows:** `C:\netiq\idm\apps\jre`	
Encryption Keystore	Specify the keystore file. You must always select the **Use existing option** so that you can select the `encrypt-keys.pkcs12` file that was created while installing OSP. If OSP is on a separate server, copy the `encrypt-keys.pkcs12` file from the installed location of the first server to the second server. Then during installation, navigate to the location where you had copied the file and then select the file. If OSP is on the same server, navigate to the `/opt/netiq/idm/apps/tomcat/conf` folder and select the `encrypt-keys.pkcs12` file. Select the **Create new** option if: ◆ OSP is deployed with Identity Manager and an encryption key was not created OR ◆ Your authentication method is Access Manager.	
Encryption Keystore Password	Enter the encryption keystore password that you created while installing OSP or a new password when using Access Manager as your authentication method.	

Item	Description	Value
Trust store password	The Identity Governance installer creates a trust store to store the certificates for SSL/TLS communication. The installer creates the trust store in the following default file: ◆ **Linux:** `/opt/netiq/idm/apps/tomcat/conf/apps-truststore.pkcs12` ◆ **Windows:** `C:\netiq\idm\apps\tomcat\conf\apps-truststore.pkcs12` If this trust store already exists, specify the password for it. If this is a new installation, specify a new password for this new trust store and the installer creates the trust store for you. The password must be six characters or longer and contain no spaces.	
Authentication Service	Use the following sections to gather information about your OSP deployment or your Access Manager deployment. You must use one of these services to deploy Identity Governance.	
Access Manager or OSP	Select the appropriate authentication service for your environment. Depending on your choices, there are different options presented that you must populate with the information for the specific authentication service. The options are **OSP** or **Access Manager**.	

Item	Description	Value
(Conditional) OSP > Application Address	If you selected Access Manager, skip this section and proceed to the Access Manager sections here **(Conditional) Access Manager > Application Address**. If you plan to install OSP and Identity Governance on the same server, this information is for that server. If you install OSP and Identity Governance on separate server, this information is for Identity Governance and the external OSP. The application address represents the URL that users need to connect to Identity Governance, Identity Reporting or the Workflow Engine if installed on the same server. For example, https://myserver.mycompany.com:8443 and for Reporting https://myserver.mycompany.com:8443/IDMRPT.	
Identity Governance protocol	Select if you want to use **http** or **https** for Identity Governance. If you select **https**, you must have configured Apache Tomcat for TLS/SSL communication on the Identity Governance server. For more information, see Section 3.9, "Securing Connections with TLS/SSL," on page 51.	

Item	Description	Value
Identity Governance host name	**WARNING:** Use the fully qualified domain name (FQDN) rather than localhost or an IP address for the Identity Governance server. If you have installed OSP and Identity Governance on the same server, this information is for that server. If you install OSP and Identity Governance on separate server, this information is for Identity Governance. In a non-clustered environment, specify the DNS name of the server hosting Identity Governance. In a clustered environment, specify the DNS name of the server that hosts the load balancer or reverse proxy that you want to use. For more information, see Section 2.3.4, “Ensuring High Availability or Load Balancing for Identity Governance,” on page 35.	
Identity Governance port	If you have installed OSP and Identity Governance on the same server, this information is for that server. If you install OSP and Identity Governance on separate server, this information is for Identity Governance. Specify the port you want the server to use for communication with client computers. The default is 8080. To use TLS/SSL, the default is 8443. When installing in a clustered environment or when using a reverse proxy, specify the port of the load balancer or of the reverse proxy.	
(Conditional) OSP > Connect to an external OSP server	You define how the clients connect to the external authentication service (OSP), if OSP is on a separate server from Identity Governance select this option, otherwise do not select this option and proceed with the installation.	

Item	Description	Value
OSP authentication server protocol	If OSP is on a separate server, select whether the clients that connect to OSP use **http** or **https**. To use https, ensure that you have configured the Apache Tomcat instance on the OSP and Identity Governance servers to use SSL/TLS. For more information, see Section 3.9, “Securing Connections with TLS/SSL,” on page 51.	
OSP authentication host name	In a non-clustered environment, specifies the DNS name of the OSP server. In a clustered environment, specifies the DNS name of the server that hosts the load balancer or the reverse proxy.	
OSP authentication server port	Specify the port that the clients use to access OSP. For http, the default port is 8080. For https, the default port is 8443.	
(Conditional) OSP > Bootstrap Administrator Details	Specify whether you are using a file-based or an LDAP-based bootstrap administrator. If you are using an LDAP-based bootstrap administrator, you must specify the distinguished name for the administrator account that is the bootstrap administrator. For example, `cn=admin,ou=sa,o=company`. **NOTE:** If you are enabling hosted SaaS, you will need to provide the SaaS bootstrap administrator name and authentication source details, as well as the analytics bootstrap administrator name and authentication source details, if applicable. If you are installing Identity Governance on-premises, you need not provide this information.	

Item	Description	Value
(Conditional) Access Manager > Application Address	If you selected **OSP**, skip the following sections about Access Manager and proceed to **(Conditional) Identity Reporting Settings** if you have installed Identity Reporting on this server. If you do not have Identity Reporting on this server, proceed to **ConfigUpdate details**.	
Identity Governance protocol	Select if you want to use **http** or **https** for Identity Governance. If you select **https**, you must have configured Apache Tomcat for TLS/SSL communication on the Identity Governance server. For more information, see Section 3.9, "Securing Connections with TLS/SSL," on page 51.	
Identity Governance host name	**WARNING:** Use the fully qualified domain name (FQDN) rather than localhost or an IP address. Specify the DNS name of the Identity Governance server.	
Identity Governance port	Specify the port that Identity Governance uses. For http, the default port is 8080. For https, the default port is 8443.	
Access Manager IDP host name	Specify the DNS name of the Access Manager Identity Server.	
Access Manager IDP port	Specify the port the Access Manager Identity Server uses.	
Access Manager Console host name	Specify the DNS name of the Access Manager administration console.	
Access Manager Console port	Specify the port the Access Manager administration console uses.	
Service Password	This is an OAuth 2.0 password that allows users to single sign-on to Identity Governance. Specify this password and remember it for later use. You can change this password after the installation completes through the configuration utilities.	

Item	Description	Value
(Conditional) Access Manager > Bootstrap Administrator Details		
Bootstrap admin DN	Specify the DN of the LDAP bootstrap administrator for Identity Governance. You must have an LDAP bootstrap administrator to integrate with Access Manager. For more information, see Section 4.1.1, “Using the Bootstrap Administrator,” on page 58.	
Bootstrap admin password	Specify the password of the LDAP bootstrap administrator account for Identity Governance.	
Access Manager admin DN	Specify the DN of an Access Manager administrator account.	
Access Manager admin password	Specify the password for the Access Manager administrator account.	
(Conditional) Identity Reporting Settings	If you plan to install Identity Reporting on another server or you are not using Identity Reporting, skip to Workflow Engine Settings. If you plan to install Identity Reporting on the same server as Identity Governance, gather the following information to configure Identity Reporting. You are defining the URL settings that the clients access to use Identity Reporting on this server.	
Identity Reporting > Protocol	Select whether the clients that connect to Identity Reporting use **http** or **https**. To use https, ensure that you have configured the Apache Tomcat instance on this server to use SSL/TLS. For more information, see Section 3.9, “Securing Connections with TLS/SSL,” on page 51.	

Item	Description	Value
Identity Reporting > Host name	**WARNING:** Use the fully qualified domain name (FQDN) rather than localhost or an IP address. In a non-clustered environment, specify the DNS name of the server hosting Identity Reporting. In a clustered environment, specify the DNS name of the server that hosts the load balancer or reverse proxy that you want to use. For more information, see Section 2.3.4, “Ensuring High Availability or Load Balancing for Identity Governance,” on page 35.	
Identity Reporting > Port	Specify the port that the clients use to access Identity Reporting. For http, the default port is 8080. For https, the default port is 8443.	
(Conditional) Workflow Engine Settings	If you plan to install Workflow Engine on another server or you are not using Workflow Engine, skip to **ConfigUpdate details**. If you plan to install Workflow Engine on the same server as Identity Governance, gather the following information to configure Workflow Engine.	
Workflow Engine > Protocol	Select whether the clients that connect to Workflow Engine use **http** or **https**. To use https, ensure that you have configured the Apache Tomcat instance on this server to use SSL/TLS. For more information, see Section 3.9, “Securing Connections with TLS/SSL,” on page 51.	

Item	Description	Value
Workflow Engine > Host name	**WARNING:** Use the fully qualified domain name (FQDN) rather than localhost or an IP address. In a non-clustered environment, specify the DNS name of the server hosting Workflow Engine. In a clustered environment, specify the DNS name of the server that hosts the load balancer or reverse proxy that you want to use. For more information, see Section 2.3.4, “Ensuring High Availability or Load Balancing for Identity Governance,” on page 35.	
Workflow Engine > Port	Specify the port that the clients use to access Workflow Engine. For http, the default port is 8080. For https, the default port is 8443.	
ConfigUpdate details	Specify the directory where the Identity Governance installer installs the Configuration Update utility.	
(Conditional) ActiveMQ Details		
Use ActiveMQ or Do not use ActiveMQ	Select whether you want to use ActiveMQ to guarantee email delivery.	
ActiveMQ host name	Specify the DNS name of the server where you have installed ActiveMQ.	
ActiveMQ port	Specify the port that ActiveMQ uses to communicate. The default port is 61616.	
Database Details	Collect the following information for the database type that you have selected to use. Ensure that you install the database before starting the Identity Governance installation. For more information, see Section 5.8, “Creating the Databases before Installing Identity Governance,” on page 101.	

Item	Description	Value
Database type	Select the type of database you are using. The supported databases are: - Microsoft SQL Server - Oracle - PostgreSQL For a list of the supported database versions, see Section 2.4.2, "Database Requirements," on page 41.	
Database Configuration Details	Select one of the following three options: - Database details > Configure database now - Database details > Generate SQL for later - Database details > No database configuration	
Database details > **Configure database now**	Select this option to have the Identity Governance installer to create and populate the databases. You select this option if you are performing an upgrade or a new installation. For more information, see Section 5.4, "Using the Identity Governance Installer to Create and Populate the Databases," on page 98.	

Item	Description	Value
Database details > **Generate SQL for later**	Select this option to have your database administrator create and populate the databases using the SQL scripts generated and stored by the installer in the following default directory for Identity Governance: ◆ **Linux:** `/opt/netiq/idm/apps/idgov/sql` ◆ **Windows:** `C:\netiq\idm\apps\idgov\sql` If you installed Identity Reporting at the same time, the Identity Reporting files are located in the following default directory: ◆ **Linux:** `/opt/netiq/idm/apps/idrpt/sql` ◆ **Windows:** `C:\netiq\idm\apps\idrpt\sql` If you installed the Workflow Engine at the same time, the Workflow Engine files are located in the following default directory: ◆ **Linux:** `/opt/netiq/idm/apps/wfe/sql` ◆ **Windows:** `C:\netiq\idm\apps\wfe\sql` For more information about using the SQL files, see Section 5.11, "Configuring the Databases Using the SQL Scripts," on page 117.	
Database details > **No database configuration**	Select this option to do nothing. You would select this option if you were installing the second node in a cluster. For more information, see Section 2.3.4, "Ensuring High Availability or Load Balancing for Identity Governance," on page 35.	
Host	Specify the DNS name of the database server.	

Item	Description	Value
Port	Specify the port the database server uses to communicate. The default port is: ◆ **Microsoft SQL:** 1433 ◆ **Oracle:** 1521 ◆ **PostgreSQL:** 5432	
(Conditional) Microsoft SQL Server JDBC JAR	If you are using Microsoft SQL Server, specify the path to the Microsoft SQL Server JDBC JAR file. For more information, see Section 5.7, "Adding the JDBC File to the Application Server," on page 101.	
(Conditional) Oracle Database Details	If you are using an Oracle database, gather the following information to complete the Identity Governance installation.	
Oracle JDBC JAR	Specify the path to the Oracle JDBC JAR file. For more information, see Section 5.7, "Adding the JDBC File to the Application Server," on page 101	
Oracle Database name	Specify the name of the Oracle database where the installer will add the schema for Identity Governance, Identity Reporting, Workflow Engine, or for all three. For example, `oracleidgov`	
Oracle User tablespace	Specify the name of the database storage unit for storing the schema for the Identity Governance databases. The default is `USERS`.	
Oracle Temporary tablespace	Specify the name of the temporary database storage unit for storing the schema. The default name is `TEMP`.	
Database credentials	Specify the credentials for accessing the various Identity Governance databases.	

Item	Description	Value
(Conditional) Database Administrator user and password	Specify the credentials of a database account that can access and modify data in the databases. This account must be able to create databases, tables, views, and other artifacts. You can test the connection to the database.	
Database names	Specify the names of the required databases for Identity Governance. This is a list of the default names of the databases and what they do. ◆ **Operations:** `igops` ◆ **Archive:** `igarc` ◆ **Data collection:** `igdcs` ◆ **Workflow:** `igwf` ◆ **Analytics:** `igara`	
Database password	Specify a single password the Identity Governance installer uses to create the databases. The installer sets the same password for each database. You can change the password at a later time if you want to have a separate password for each database. For more information, see Section 5.12, "How to Change the Configuration Options for the Databases," on page 125.	
Reporting user and password	Specify a name and password of a database user that Identity Governance uses to generate reports for Identity Governance. The default name is `igrptuser`. Identity Governance uses this user if you have Identity Reporting installed or not.	
(Conditional) Identity Reporting database users password	If you install Identity Reporting with Identity Governance, specify the name and password of the required database for Identity Reporting. The default database name is `igrpt`. **NOTE:** The database password is requested only for Microsoft SQL Server and PostgreSQL.	

Item	Description	Value
(Conditional) Workflow Engine database name	If you install Workflow Engine with Identity Governance, specify the name of the required database for the Workflow Engine. The default name is `igaworkflowdb`.	
Workflow Engine user name and password	Specify the name and password of the database user for the Workflow Engine. The default name is `igwfadmin`.	
Update or Only use existing	Applies only when you choose to configure the database during the installation. Select whether the Identity Governance installer creates the database names, creates the schema, creates users, creates roles, assigns permissions to roles, and populates the databases with this information. Select this option for new installations or upgrades. Or select to use existing databases with your database names and users.	
(Conditional) Additional Identity Reporting Options Identity Reporting > Target Locale	If you install Identity Reporting with Identity Governance, you must select the language Identity Reporting uses to generate the reports. The default is English.	
Email Delivery	Gather the information for the SMTP server that delivers report notifications.	
Default email address	Specify the email address that you want to use as the origin of email notifications.	
SMTP Server	**WARNING:** Use the fully qualified domain name (FQDN) rather than localhost or an IP address. Specify the DNS name of the SMTP email host that is used for email notifications.	
SMTP Server Port	Specify the port number for the SMTP server. The default value is 465.	

Item	Description	Value
(Conditional) Use SSL for SMTP	Select whether you want to use secure communication with the SMTP server. If you select this option, you must configure your SMTP server for TLS/SSL communication. For more information, see Section 3.9, “Securing Connections with TLS/SSL,” on page 51.	
(Conditional) Require server authentication	Select whether you want to use authentication for communication with the SMTP server. If you select this option, you must provide the SMTP server credentials.	
SMTP user name and password	Specify the credentials for a login account to the SMTP server.	
(Conditional) Identity Reporting > Keep finished reports for	If you install Identity Reporting with Identity Governance, then specify the report retention time and location. For example, to specify retention time of six months, enter 6, then select **Month**. Identity Reporting retains completed reports for the specified time then deletes them.	
(Conditional) Identity Reporting > Location of report definitions	Specify a path where you want to store the report definitions. The default directory is: - **Linux:** `/opt/netiq/idm/apps/idrpt` - **Windows:** `C:\netiq\idm\apps\idrpt`	
(Conditional) Auditing Details	Gather the following information if you want to enable auditing capabilities for Identity Governance.	
Enable auditing	Select whether you want to enable auditing.	
Audit server	Specify the DNS name of the audit server.	
Audit port	Specify the port the audit server uses to communicate. The default port is 6514.	

Item	Description	Value
Audit cache location	Specify a local directory on the Identity Governance server for caching of audit events before they are sent to the audit server. The default directory is: ◆ **Linux:** `/opt/netiq/idm/apps/audit` ◆ **Windows:** `C:\netiq\idm\apps\audit`	
Secure layer	Select if you are using TLS communication to the audit server. If you are, you can test the connection before you proceed. For more information, see Section 3.9, “Securing Connections with TLS/SSL,” on page 51.	

6.5 Installing Identity Governance

The following procedure describes how to install Identity Governance or Identity Governance and Identity Reporting or Identity Governance and the Workflow Engine on the same server using the guided installation or the console installation methods. To perform a silent, unattended installation, see Section 6.6, “Silently Installing Identity Governance and its Components,” on page 155.

Ensure that you meet the prerequisites and requirements before starting the installation. For more information, see Section 6.3, “Prerequisites for Identity Governance,” on page 134 and Section 2.4.1, “Identity Governance Server System Requirements,” on page 39.

To install Identity Governance or to install Identity Governance with Identity Reporting or Workflow Engine:

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. Download and extract the Identity Governance installation files. For more information, see Section 2.2, “Obtaining Identity Governance, Identity Reporting, Workflow Engine, and OSP,” on page 31.
3. If you are in a clustered environment, proceed to Step 4. If you are not using HTTPS for this installation, stop Apache Tomcat. For more information, see Section 3.5.3, “Starting and Stopping Apache Tomcat,” on page 50.
4. From the directory that contains the installation files, complete one of the following actions:
   - **Linux:** Enter the following from a command prompt.
     - **Guided**:`./identity-governance-install-linux.bin`
     - **Console**:`./identity-governance-install-linux.bin -i console`

- **Windows:** Enter the following from a command prompt.
  - **Guided:** `identity-governance-install-win.exe`
  - **Console**: `identity-governance-install-win.exe -i console`

NOTE: To execute the file, you might need to use the `chmod +x` or `sh` command for Linux or use **Run as administrator** if you did not log in to your Windows server as an administrator.

---

5 Read and accept the license agreement.

6 Select whether to install Identity Governance, Identity Reporting, Workflow Engine, or all.

7 Specify an installation path for each installed feature.

8 Complete the installation following the prompts and using the information you gathered in the Table 6-1, "Identity Governance Installation Worksheet," on page 135.

9 Review the pre-installation summary.

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

---

10 Click **Install**.

11 (Conditional) If prompted, accept the certificates you trust, reject any certificates you do not trust, and acknowledge any errors.

The installer checks to see if you selected SSL/TLS or HTTPS for communication to the connected systems. The installer attempts to retrieve those certificates and add them to the trust store. If you used a self-signed certificate for any of the connected systems, the installer prompts you to accept or reject the certificates, because self-signed certificates are untrusted certificates. The installer adds the accepted certificates to the trust store. For more information, see Section 3.9, "Securing Connections with TLS/SSL," on page 51.

The installer displays errors in the following conditions:

- A single warning about potential future failures for all rejected certificates
- A single warning for any errors when connecting to the secured servers

---

NOTE: If you are in a distributed environment, and if you are using a later version of Java Zulu OpenJDK (such as 8u312), the installer could present each certificate for acceptance only once. The installer compares certificates in a specific order. If the certificates you accepted are from a certificate authority (CA), then any subsequent certificates signed by the same CA are automatically trusted.

---

12 (Conditional) If you are in a clustered environment, or if you are using HTTPS, stop Apache Tomcat if it is still running. For more information, see Section 3.5.3, "Starting and Stopping Apache Tomcat," on page 50.

13 After the installation process completes, close the installer and review the `Identity_Governance_InstallLog.log` file. The default location of the `Identity_Governance_InstallLog.log` file is here:

- **Linux:** `/opt/netiq/idm/apps/idgov/logs`
- **Windows:** `C:\netiq\idm\apps\idgov\logs`

NOTE: The `Identity_Governance_InstallLog.log` file is not available until you close the Identity Governance installer.

---

14 Proceed to Section 9.3, “Starting and Initializing Identity Governance,” on page 209

or

If you are installing Identity Reporting on a separate server, proceed to Chapter 7, “Installing Identity Reporting,” on page 163.

or

If you are installing the Workflow Engine on a separate server, proceed to Chapter 8, “Installing Workflow Engine,” on page 183.

6.6 Silently Installing Identity Governance and its Components

A silent (non-interactive) installation does not display a user interface or ask any questions. Instead, the system uses information from the `identity-governance-install-silent.properties` file to complete the installation. The installation files that you download from the Customer Center contain the `identity-governance-install-silent.properties` file. You must edit the file and add the correct values for your environment in the properties. Ensure that you have met the prerequisites before starting the silent installation. For more information, see Section 6.3, “Prerequisites for Identity Governance,” on page 134.

You can use the `identity-governance-install-silent.properties` to install the different combinations of Identity Governance, Identity Reporting, and Workflow Engine. Identity Reporting or Workflow Engine does not have a separate silent properties file. The different configurations of Identity Governance with its components are:

- Identity Governance only
- Identity Governance and Identity Reporting
- Identity Reporting only
- Workflow Engine only
- Identity Reporting and Workflow Engine
- Identity Governance and Workflow Engine
- Identity Governance, Identity Reporting, and Workflow Engine

Use the following information to populate the `identity-governance-install-silent.properties` file with values from your environment and how to use the `identity-governance-install-silent.properties` file to silently install your selected features from Identity Governance, Identity Reporting, and Workflow Engine.

- Section 6.6.1, “Understanding the Passwords that Identity Governance Reads from Environment Variables During the Installation Process,” on page 156
- Section 6.6.2, “Creating a Silent Properties File for Identity Governance and its Components,” on page 156
- Section 6.6.3, “Creating a Silent Properties File for Installing an Additional Node to Cluster Identity Governance and its Components,” on page 158
- Section 6.6.4, “Performing the Silent Installation of Identity Governance and its Components,” on page 161

6.6.1 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 and guided installation processes. Identity Governance must have access to these passwords to be properly configured and installed. These passwords are for Identity Governance, Identity Reporting, and Workflow Engine.

- `install_authserver_client_secret`: It is the password for the SSO clients used with OSP. This password is also gathered for Access Manager, but is ignored after the Access Manager configuration succeeds.
- `install_bootstrap_secret`: It is the password for the bootstrap administrator. When using Access Manager, the user must exist in an LDAP server connected to the Access Manager IDP.
- `install_db_admin_secret`: It is the password for the database administrator.
- `install_db_secret`: It is the password for `igops`, `igarc`, `igdcs`, `igwf`, and `igara` users.
- `install_db_rpt_secret`: It is the password for `igrptuser`.
- `install_db_reporting_secret`: It is the password for `idm_rpt_cfg` (used only in Identity Reporting installations).
- `install_truststore_secret`: It is the password for the application trust store.
- `install_smtp_secret_auth_user`: It is the password for the SMTP authentication user (used only in Identity Reporting installations).
- `install_nam_admin_secret`: It is the password for the Access Manager console administrator.
- `install_db_workflow_secret`: It is the password for the Workflow Engine database.
- `install_enc_keystore_secret`: It is the password for the encryption key keystore.

For the silent installation to succeed, you must either set these passwords in the silent properties file or set them as environment variables. If you do not want to set the passwords in a file because of security concerns, it is best to set the passwords as environment variables. 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.

6.6.2 Creating a Silent Properties File for Identity Governance and its Components

The silent properties file for Identity Governance allows you to perform an installation without any interaction. The `identity-governance-install-silent.properties` file is in the ZIP file that you download from the Customer Center. This file does not contain many values, and you must edit the file to add some values for your environment. The different parameters in the file relate to the questions that you answer during a guided installation or console installation.

You would use the silent installation if you want to install several instances of Identity Governance. We recommend that you install the first instance of Identity Governance using the guided installation or the console installation with the `-r` parameter and a path where the installer creates a response file for you.

A **response file** contains the values that you must add to the `identity-governance-install-silent.properties` file for your environment. You can open the response file and copy the parameters from the response file to `identity-governance-install-silent.properties` file to simplify the process of creating the `identity-governance-install-silent.properties` file.

You can also use the Identity Governance Installation Worksheet to add the proper values to the `identity-governance-install-silent.properties` file. You open the `identity-governance-install-silent.properties` file in a text editor and then use the information you gathered in the Identity Governance Installation Worksheet to add the correct values for your environment. For more information, see Table 6-1, "Identity Governance Installation Worksheet," on page 135.

To create the identity-governance-install-silent.properties file using the response file:

1 Download and extract the Identity Governance installation files. For more information, see Section 2.2, "Obtaining Identity Governance, Identity Reporting, Workflow Engine, and OSP," on page 31.

2 Ensure that you have completed the Identity Governance Installation Worksheet to have the information required to complete the installation. For more information, see Table 6-1, "Identity Governance Installation Worksheet," on page 135.

3 Create the response file.

3a From the directory that contains the installation files, complete one of the following actions:

- **Linux**: Enter the following at a command prompt:
  - **Guided:** `./identity-governance-install-linux.bin -r` *`path-to-response-file`*
  - **Console:** `./identity-governance-install-linux.bin -i console -r` *`path-to-response-file`*
- **Windows**: Enter the following at a command prompt:
  - **Guided**: `identity-governance-install-win.exe -r` *`path-to-response-file`*
  - **Console:** `identity-governance-install-win.exe -i console -r` *`path-to-response-file`*

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

NOTE: The `path-to-response-file` is either the name of the response file to be created within the same directory as the installation file, or an existing absolute path, and the name of the response file to be created.

3b Use the Identity Governance Installation Worksheet to complete the first guided or console installation of Identity Governance to create the response file. For more information, see Table 6-1, "Identity Governance Installation Worksheet," on page 135.

3c Review the `Identity_Governance_InstallLog.log` file to ensure that no errors occurred.

- **Linux:** `/opt/netiq/idm/apps/idgov/logs`
- **Windows:** `C:\netiq\idm\apps\idgov\logs`

4 Find and open the response file in a text editor.

5 Find and open the `identity-governance-install-silent.properties` in a text editor.

6 Copy the values from the response file to the `identity-governance-install-silent.properties` file.

NOTE: If you are deploying on Windows, ensure that you escape the backslashes `'\'` or the silent properties file does not work.

7 Close the response file and save the `identity-governance-install-silent.properties` file.

8 (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
```

For more information, see Section 6.6.1, “Understanding the Passwords that Identity Governance Reads from Environment Variables During the Installation Process,” on page 156.

9 (Conditional) When installing on a secondary node in a cluster, you can modify the silent properties file using the steps in Section 6.6.3, “Creating a Silent Properties File for Installing an Additional Node to Cluster Identity Governance and its Components,” on page 158.

10 Proceed to “Running a Silent Installation for One SSO Provider” on page 77 to run the silent installation using the `osp-install-silent.properties` file for the next installation of OSP.

6.6.3 Creating a Silent Properties File for Installing an Additional Node to Cluster Identity Governance and its Components

In a clustered environment, you can use the same silent properties file for each node. However, you might choose to run the guided installation or the console installation on the primary node with the `-r` parameter to create the response file. You can then silently install on the secondary nodes. You can quickly create a silent properties file from the response file that the guided installation or console installation creates. For more information, see Section 6.6.2, “Creating a Silent Properties File for Identity Governance and its Components,” on page 156.

There are additional parameters that you must add to the `identity-governance-install-silent.properties` file if you are installing secondary nodes in a cluster. Use the following procedure to modify the `identity-governance-install-silent.properties` file for any secondary nodes in the Identity Governance, Identity Reporting, or Workflow Engine clusters.

1 Locate the Identity Governance response file.

2 Locate the sample `identity-governance-install-silent.properties` file, by default in the same directory as the installation files for Identity Governance.

3 Open the files in a text editor.

4 Copy the parameter values from the response file or installation log 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 that are appropriate to your environment. In the response file, they are represented as 0 or 1 and in the silent properties file they are represented as false and true:

Response file	Silent.properties file
0	false
1	true

6 Change the values as specified in the following table:

Response 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 (Conditional) If you are not installing Identity Governance, change the values as specified in the following table:

Log file	Silent.properties file

install_govern_protocol_http=1
install_govern_protocol_https=0
	install_govern_protocol=http

install_govern_protocol_http=0
install_govern_protocol_https=1
	install_govern_protocol=https

The default value in the silent properties file uses the values set for the servlet:

- `install_govern_protocol=$install_servlet_protocol$`
- `install_govern_hostname=$install_servlet_hostname$`
- `install_govern_port=$install_servlet_port$`

8 (Optional) Specify any number of certificate files and corresponding aliases to accept into the trust store (`/opt/netiq/idm/apps/tomcat/conf/apps-truststore.pkcs12`). For example:

```
install_cert_1_file=/home/username/Downloads/tomcat_cert
install_cert_1_alias=ig-tomcat
install_cert_2_file=/home/username/Downloads/audit_cert
install_cert_2_alias=ig-audit
```

NOTE: You can specify the files in any order, and they must exist on the same machine as the Identity Governance installer. The installer will start trusting with 1 and stop with the first missing consecutive number. So if you list files 1, 2, and 4, the installer only trusts certificates 1 and 2.

9 (Optional) 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`.

10 Save and close the file.

11 ***Copy the `encrypt-keys.pkcs12` from the primary server to the server that becomes a new node in the cluster.***

12 Copy the updated `identity-governance-install-silent.properties` file from the primary server to the new node.

13 Open the `identity-governance-install-silent.properties` file, then change the encryption keystore related properties to use the same encryption keystore file on the new node. Specifically set:

```
install_enc_create_file=false
install_enc_source_file=PATH
```

where *PATH* is the location the copied `encrypt-keys.pkcs12` file.

14 Save your changes.

15 Run the silent installation using this updated file. For more information, see Section 6.6.4, "Performing the Silent Installation of Identity Governance and its Components," on page 161

6.6.4 Performing the Silent Installation of Identity Governance and its Components

After you have populated the `identity-governance-install-silent.properties` file with the correct values for your environment, you must run the Identity Governance installer in the silent installation mode and pass this file to the installer. These steps are the same whether you are only installing Identity Governance, installing Identity Governance and Identity Reporting, or only installing Identity Reporting or Workflow Engine.

To perform a silent installation:

1. Ensure that you have created the `identity-governance-install-silent.properties` file for your environment. For more information, see Section 6.6.2, "Creating a Silent Properties File for Identity Governance and its Components," on page 156.
2. (Conditional) If this server is an additional node to cluster Identity Governance, ensure that you have properly modified the `identity-governance-install-silent.properties` file for the additional nodes in a cluster. For more information, see Section 6.6.3, "Creating a Silent Properties File for Installing an Additional Node to Cluster Identity Governance and its Components," on page 158.
3. Ensure that this server meets the prerequisites for the feature or features you are installing, such as, Identity Governance, Identity Reporting, or Workflow Engine.
4. Ensure that the Identity Governance installation files are on the server. For more information, see Section 2.2, "Obtaining Identity Governance, Identity Reporting, Workflow Engine, and OSP," on page 31.
5. Log in as `root` on the Linux server or an administrator on the Windows server where you want to install Identity Governance.
6. Stop Apache Tomcat. For more information, see Section 3.5.3, "Starting and Stopping Apache Tomcat," on page 50.
7. Copy the populated `identity-governance-install-silent.properties` file to this server.
8. To run the silent installation, enter the following at a command prompt:
   - **Linux:** `./identity-governance-install-linux.bin -i silent -f` *`path_to_silent_properties_file`*
   - **Windows:** `cmd /c "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 file, 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.

9. When the console prompt returns, review the log file to ensure that the installation completed successfully. The silent installation does not display any messages on the console.

   The log file is located in the following default directory:
   - **Linux:** `/opt/netiq/idm/apps/idgov/logs`/
   - **Windows:** `C:\netiq\idm\apps\idgov\logs`\

When the installation completes, there are additional configuration steps to perform before you can use Identity Governance and Identity Reporting. For more information, see Chapter 9, “Completing the Installation Process,” on page 201.

7 Installing Identity Reporting

There are two different versions of Identity Reporting you can install. You can install the version that comes with Identity Governance and is configured to run only 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 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 that 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 where you store the data.

You can also install a version of Identity Reporting in the Identity Governance and Identity Manager environments so that each system has its separate reporting environment. However, installing Identity Reporting this way requires that you deploy, configure, and run reports on two different servers. For more information about Identity Reporting, see the *Identity Governance Reporting Guide* and *Administrator Guide to NetIQ Identity Reporting*.

Before you install Identity Reporting, you must decide if you want to install the Identity Reporting that comes with Identity Governance or the Identity Reporting that comes with Identity Manager. In addition, if your Identity Reporting server does not have internet access, you must have a proxy server that can access and download the most current reports for Identity Governance from the Reporting Content Delivery Network (CDN), and can access and send updated reports to the Identity Reporting server. For more information, see Section 9.4.4, "Configuring a Proxy Server for the Identity Reporting Server," on page 214.

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 Identity Reporting 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:** *NetIQ Identity Manager Setup Guide for Linux*
- **Windows:** *NetIQ Identity Manager Setup Guide for Windows*

The Identity Governance installer installs Identity Reporting. You can install Identity Reporting on the same server as Identity Governance or a separate server. The following information explains how to install Identity Reporting on a different server from Identity Governance. For information about installing Identity Reporting with Identity Governance, see Chapter 6, "Installing Identity Governance," on page 131.

Use the following information to install Identity Reporting that comes with Identity Governance on a separate server from Identity Governance:

- Section 7.3, “Understanding the Installation Process for the Identity Reporting Components,” on page 166
- Section 7.4, “Identity Reporting Installation Worksheet,” on page 167
- Section 7.5, “Installing Identity Reporting,” on page 179
- Section 7.6, “Silently Installing Identity Reporting,” on page 181

7.1 Checklist for Installing Identity Reporting

You must complete the steps in the following checklist to install Identity Reporting on a separate server from Identity Governance:

	Checklist Items
❑	1. Learn about the interaction among Identity Reporting components. For more information, see “Understanding Identity Reporting” on page 17.
❑	2. Decide which server you want to use for your Identity Reporting components. For more information, see Section 2.3, “Recommended Production Environment Installation Scenarios,” on page 32.
❑	3. Review the considerations for installing Identity Reporting. For more information, see Section 7.2, “Prerequisites for Identity Reporting,” on page 165.
❑	4. Review the hardware and software requirements for the computer that will host Identity Reporting. For more information, see Section 2.4.3, “Identity Reporting Server System Requirements,” on page 42.
❑	5. Ensure that the server where you want to install Identity Reporting has Zulu OpenJDK and Apache Tomcat installed. For more information, see Chapter 3, “Installing Required Components,” on page 45.
❑	6. Ensure that you have a database to which the installation process can connect. For more information, see Chapter 5, “Creating Databases for Identity Governance and Components,” on page 95. (Conditional) Add the schema for the reporting user. For more information, see Section 5.8.2, “Creating the Oracle Schema Before Installing Identity Governance,” on page 105 and Section 7.3.2, “Understanding the Users that the Installation Process Creates,” on page 166.
❑	7. Determine the installation method you want to use. For more information, see Section 1.2, “Understanding the Installation Methods,” on page 18.
❑	8. The installation directory for Identity Reporting cannot contain any spaces in the name. If it does contain spaces, the installation fails.
❑	9. (Conditional) If you want email notifications for reports, you must have an SMTP server installed and running. If you want to guarantee the delivery of emails, you must install ActiveMQ on the Identity Governance server. For more information, see Chapter 3, “Installing Required Components,” on page 45.

	Checklist Items
❑	10. Install Identity Reporting: ◆ For a guided installation, see Section 7.5, “Installing Identity Reporting,” on page 179. ◆ To install Identity Reporting silently, see Section 7.6, “Silently Installing Identity Reporting,” on page 181.
❑	11. Complete the installation and configuration for Identity Reporting. For more information, see Section 9.4, “Configuring Identity Reporting,” on page 211.

7.2 Prerequisites for Identity Reporting

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, you might not need to install it again for Identity Governance. Ensure that you have the appropriate version of Identity Reporting. For more information about installing with Identity Manager, see:

- **Linux:** “Considerations for Installing Identity Reporting Components” in the *NetIQ Identity Manager Setup Guide for Linux*.
- **Windows:** “Identity Reporting 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 Apache Tomcat instance, or you can install it on a separate server running a separate instance of Apache Tomcat.

❑ Assign the Report Administrator authorization to any users that you want to be able to access the reporting functionality.

❑ Install Zulu OpenJDK and Apache Tomcat on the server that runs Identity Reporting. For more information, see Chapter 3, “Installing Required Components,” on page 45.

❑ Ensure that you have a supported database to which the installation process can connect. You can use the same database you deployed for Identity Governance. For more information, see Chapter 5, “Creating Databases for Identity Governance and Components,” on page 95.

  ❑ Ensure that the JDBC driver for the supported database is on the server where you install Identity Reporting. For more information, see Section 2.4.2, “Database Requirements,” on page 41.

  ❑ Ensure that the database runs in the same subnetwork as Identity Reporting.

  ❑ If you use an Oracle database, you must create the database (SID) in AL32UTF-8 (Unicode UTF-8 Universal character set) before installing Identity Reporting.

❑ 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.

- ❒ (Conditional) If you want to enable email notifications for reports, you must have an SMTP server installed and configured. If you want to guarantee email delivery, you must install ActiveMQ on the server where you install Identity Governance.
- ❒ (Conditional) If you want to enable secured auditing for Identity Reporting, it is recommended that you configure the audit server to use TLS before beginning the Identity Reporting installation so that the Identity Reporting installer can connect to the audit server and retrieve the audit server certificate to add to the local keystore. For more information, see Section 3.9, "Securing Connections with TLS/SSL," on page 51.

7.3 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 Section 2.3, "Recommended Production Environment Installation Scenarios," on page 32.

- Section 7.3.1, "Understanding the Installation Process for Identity Reporting," on page 166
- Section 7.3.2, "Understanding the Users that the Installation Process Creates," on page 166

7.3.1 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

7.3.2 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

User name	Description
igrptuser	Created by Identity Governance and granted access to run and view reports for Identity Governance
idm_rpt_cfg	Owns the reporting configuration data and the Identity Manager reporting views

If you do not want the installer to create the database for you, you must manually create the database and use the SQL files to populate the databases. For more information, see Chapter 5, “Creating Databases for Identity Governance and Components,” on page 95.

7.4 Identity Reporting Installation Worksheet

Gather the information listed in the following worksheet before starting the Identity Reporting installation. Use the information in the worksheet when you install Identity Reporting on a separate server from Identity Governance. If you are installing Identity Governance and Identity Reporting on the same server, follow the Identity Governance installation procedure. For more information, see Chapter 6, “Installing Identity Governance,” on page 131.

Table 7-1 *Identity Reporting Installation Worksheet*

Item	Description	Value
Installation location	Specify the installation path for Identity Reporting. **WARNING:** Spaces in the path are not supported. The default directory is: ◆ **Linux:** `/opt/netiq/idm/apps/idrpt` ◆ **Windows:** `C:\netiq\idm\apps\idrpt`	
(Conditional) Workflow Engine Installation Location	If you are installing the Workflow Engine on the same server as Identity Reporting, specify the installation path. **WARNING:** Spaces in the path are not supported. The default directory is: ◆ **Linux:** `/opt/netiq/idm/apps/wfe` ◆ **Windows:** `C:\netiq\idm\apps\wfe`	

Item	Description	Value
Tomcat installation location	Specify the path to the Apache Tomcat home directory. The installation process adds some files for Identity Reporting to this folder. **WARNING:** Spaces in the path are not supported. The default location is: - **Linux:** `/opt/netiq/idm/apps/tomcat` - **Windows:** `C:\netiq\idm\apps\tomcat`	
JRE home folder	Specify the path to the Zulu JRE directory. The Zulu JRE is installed when you install the Zulu OpenJDK. The installation process uses Java for several processes, such as running commands and creating security stores. **WARNING:** Spaces in the path are not supported. The default location is: - **Linux:** `/opt/netiq/idm/apps/jre` - **Windows:** `C:\netiq\idm\apps\jre`	

Item	Description	Value
(Conditional) Encryption Keystore	If Identity Reporting is not installed at the same time as Identity Governance, then you must specify the encryption keystore file. You must always select the **Use existing option** so that you can select the `encrypt-keys.pkcs12` file that was created while installing OSP. If OSP is on a separate server, copy the `encrypt-keys.pkcs12` file from the installed location of the first server to the second server. Then during installation, navigate to the location where you had copied the file and then select the file. If OSP is on the same server, navigate to the `/opt/netiq/idm/apps/tomcat/conf` folder and select the `encrypt-keys.pkcs12` file. Select the **Create new** option if: ◆ You do not have an existing encryption key from a previous OSP or Identity Governance installation ◆ Your authentication method is Access Manager	
Encryption Keystore Password	Enter the encryption keystore password that you have created while installing OSP or enter a new password when using Access Manager as your authentication method.	
Trust store password	If you have a trust store that contains the certificates for TLS communication, specify that password, otherwise, specify a password that is six characters or longer and has no spaces. The installer creates the trust store for you using this password. For more information, see Section 3.9, “Securing Connections with TLS/SSL,” on page 51.	
Authentication Service	Use the following sections to gather information about your OSP deployment or your Access Manager deployment. You must use one of these services to deploy Identity Reporting.	

Item	Description	Value
Access Manager or OSP	Select the appropriate authentication service for your environment. Depending on your choices, there are different options presented that you must populate with the information for the specific authentication service. The options are **OSP** or **Access Manager**.	
(Conditional) OSP > Application address	If you selected Access Manager, skip the sections about OSP. Specify the URL connection information the clients use to access Identity Reporting.	
OSP > Identity Reporting Protocol	Select if you want to use **http** or **https** for Identity Reporting. If you select **https**, you must have configured Apache Tomcat for TLS/SSL communication on the Identity Reporting server. For more information, see Section 3.9, "Securing Connections with TLS/SSL," on page 51.	
OSP > Identity Reporting Host name	**WARNING:** Use the fully qualified domain name (FQDN) rather than localhost or an IP address. In a non-clustered environment, specifies the DNS name of the Identity Reporting server. In a clustered environment, specifies the DNS name of the server that hosts the load balancer or the reverse proxy.	
OSP > Identity Reporting Port	Specify the port you want the Identity Reporting server to use for communication with client computers. The default is 8080. To use TLS/SSL, the default is 8443. When installing in a clustered environment or when using a reverse proxy, specify the port of the load balancer or of the reverse proxy.	
(Conditional) OSP > Connect to an external OSP server	If you have OSP installed on a separate server from Identity Reporting, select this option and the define the protocol, host name, and port for the external OSP server.	

Item	Description	Value
OSP > OSP authentication server protocol	If OSP is on a separate server from Identity Reporting, select whether the clients that connect to OSP use **http** or **https**. To use **https**, ensure that you have configured the Apache Tomcat instance on the OSP server to use SSL/TLS. For more information, see Section 3.9, "Securing Connections with TLS/SSL," on page 51.	
OSP > OSP authentication server host name	**WARNING:** Use the fully qualified domain name (FQDN) rather than localhost or an IP address of the external OSP server. In a non-clustered environment, specifies the DNS name of the OSP server. In a clustered environment, specifies the DNS name of the server that hosts the load balancer or the reverse proxy for OSP.	
OSP > OSP authentication server port	Specify the port that the clients use to access OSP. For http, the default port 8080. For https, the default port is 8443.	
(Conditional) Access Manager > Application address	If you selected **OSP**, skip the following sections about Access Manager.	
Identity Reporting protocol	Select if you want to use **http** or **https** for Identity Reporting.	
Identity Reporting host name	**WARNING:** Use the fully qualified domain name (FQDN) rather than localhost or an IP address of the Apache Tomcat instance for Identity Reporting.	
Identity Reporting port	Specify the port that Identity Reporting uses. The default port for http is 8080. The default port for https is 8443.	
Access Manager IDP Host name	**WARNING:** Use the fully qualified domain name (FQDN) rather than localhost or an IP address. Specify the DNS name of the Access Manager identity provider server.	
Access Manager IDP Port	Specify the port the Access Manager identity provider uses. The default port is 443.	

Item	Description	Value
Access Manager Console host name	Specify the DNS name of the Access Manager administration console.	
Access Manager Console port	**WARNING:** Use the fully qualified domain name (FQDN) rather than localhost or an IP address. Specify the port of the Access Manager administration console. The default port is 443.	
Identity Governance details	If you are installing Identity Reporting after you have installed Identity Governance, you must provide information about the protocol, server, and port.	
Identity Governance protocol	Provide information about the communication protocol.	
Identity Governance server information	Provide the Identity Governance host name.	
Identity Governance port number	Provide the Identity Governance port information.	
Service Password	This is an OAuth 2.0 password that allows users to single sign-on to Identity Reporting. Specify this password and remember it for later use. You can change this password after the installation completes through the configuration utilities.	
(Conditional) Access Manager > Bootstrap Administrator Details		
Bootstrap admin DN	Specify the DN of the LDAP bootstrap administrator for Identity Governance. You must have an LDAP bootstrap administrator to integrate with Access Manager. For more information, see Section 4.1.1, “Using the Bootstrap Administrator,” on page 58.	
Bootstrap admin password	Specify the password of the LDAP bootstrap administrator account for Identity Governance.	
Access Manager admin DN	Specify the DN of an Access Manager administrator account.	
Access Manager admin password	Specify the password for the Access Manager administrator account.	

Item	Description	Value
Database Details	Collect the following information for the database type that you have selected to use. Ensure that you install the database before starting the Identity Reporting installation. For more information, see Section 5.8, “Creating the Databases before Installing Identity Governance,” on page 101.	
Database type:	Select the type of database that you are using. - Microsoft SQL Server - Oracle - PostgreSQL For a list of the supported database versions, see Section 2.4.2, “Database Requirements,” on page 41.	
Database Configuration Details	Select one of the following three options: - “Database details > Configure database now” on page 173 - “Database details > Generate SQL for later” on page 174 - “Database details > No database configuration” on page 174	
Database details > **Configure database now**	Select this option to have the installer create and populate the database. You select this option if you are performing an upgrade or a new installation. For more information, see Section 5.4, “Using the Identity Governance Installer to Create and Populate the Databases,” on page 98.	

Item	Description	Value
Database details > **Generate SQL for later**	Select this option to have your database administrator create and populate the database for Identity Reporting using the SQL scripts generated and stored by the installer in the following default directory for Identity Reporting: - **Linux:** `/opt/netiq/idm/apps/idrpt/sql` - **Windows:** `C:\netiq\idm\apps\idrpt\sql` If you install the Workflow Engine at the same time, the Workflow Engine files are located in the following default directory: - **Linux:** opt/netiq/idm/apps/wfe/sql - **Windows:** C:\netiq\idm\apps\wfe\sql For more information about using the SQL files, see Section 5.11, “Configuring the Databases Using the SQL Scripts,” on page 117.	
Database details > **No database configuration**	Select this option to do nothing. You would select this option if you were installing the second node in a cluster. For more information, see Section 2.3.4, “Ensuring High Availability or Load Balancing for Identity Governance,” on page 35.	
Host	**WARNING:** Use the fully qualified domain name (FQDN) rather than localhost or an IP address. Specify the DNS name of the database server.	
Port	Specify the port the database server uses to communicate. The default port is: - **Microsoft SQL:** 1433 - **Oracle:** 1521 - **PostgreSQL:** 5432	

Item	Description	Value
(Conditional) Microsoft SQL Server JDBC JAR	If you are using the Microsoft SQL Server, specify the path to the Microsoft SQL Server JDBC JAR file. For more information, see Section 5.7, “Adding the JDBC File to the Application Server,” on page 101.	
(Conditional) Oracle Database Details	If you are using an Oracle database, gather the following information to complete the Identity Reporting installation.	
Oracle JDBC JAR	Specify the path to the Oracle JDBC JAR file. For more information, see Section 5.7, “Adding the JDBC File to the Application Server,” on page 101.	
Oracle Database name	Specify the name of the Oracle database where the installer will add the schema for Identity Reporting. For example, `oracleidgov`.	
Oracle User tablespace	Specify the name of the database storage unit for storing the schema for the Identity Reporting databases. The default is `USERS`.	
Oracle Temporary tablespace	Specify the name of the temporary database storage unit for storing the schema. The default name is `TEMP`.	
Database credentials	Specify the credentials for accessing the various databases.	
(Conditional) Database Administrator user and password	Specify the credentials of a database account that can access and modify data in the databases. This account must be able to create databases, tables, views, and other artifacts. You can test the connection to the database.	
Reporting database user’s password	Specify the password for the reporting database user that you created during the Identity Governance installation. The default user name is `igrptuser`.	
(Conditional) Reporting database name	Specify the name of the required database for Identity Reporting. The default name is `igrpt`.	
(Conditional) Workflow Engine database name	If you are installing the Workflow Engine with Identity Reporting, then specify the name of the database for the Workflow Engine. The default name is `igaworkflowdb`.	

Item	Description	Value
(Conditional) Workflow Engine database user name	Specify the user name of the Workflow Engine database. The default name is `igawfadmin`.	
(Conditional) Workflow Engine database user's password	Specify the password of the Workflow Engine database.	
Update or Only use existing	Applies only when you choose to configure the database during the installation. Select whether the installer creates the database name, creates the schema, creates users, creates roles, assigns permissions to roles, and populates the database with this information. Select this option for new installations or upgrades. Or select to use existing databases with your database name and user.	
Operation user database and password	Specify the name of the operations database and the password for the operations database. The default name is `igops`.	
(Conditional) Different database vendor than Identity Governance	Select this option if you have a different database type for the Identity Reporting database than what you used for Identity Governance. You can use the same database type for the two components or you can use separate, supported database types.	
Database host	Specify the DNS name of the separate database from the database Identity Governance uses.	
Database port	Specify the port the separate database server uses to communicate. The default port is: ◆ **Microsoft SQL Server:** 1433 ◆ **Oracle:** 1521 ◆ **PostgreSQL:** 5432	

Item	Description	Value
Database type:	Select the type of database that you are using: ◆ Microsoft SQL Server ◆ Oracle ◆ PostgreSQL For a list of the supported database versions, see Section 2.4.2, “Database Requirements,” on page 41.	
(Conditional) Microsoft SQL Server JDBC JAR	If you are using Microsoft SQL Server, specify the path to the Microsoft SQL Server JDBC JAR file. For more information, see Section 5.7, “Adding the JDBC File to the Application Server,” on page 101.	
(Conditional) Oracle Database Details	If you are using an Oracle database, gather the following information to complete the Identity Reporting installation.	
Oracle JDBC JAR	Specify the path to the Oracle JDBC JAR file. For more information, see Section 5.7, “Adding the JDBC File to the Application Server,” on page 101	
Oracle Database name	Specify the name of the Oracle database where you will add the Oracle schema for Identity Reporting. For example, `oracleidrpt`.	
Identity Reporting Settings	Gather the information to define the settings for Identity Reporting.	
Target Locale	Select the language Identity Reporting uses to generate the reports. The default is English.	
Email Delivery	Gather the following information for the SMTP server that delivers the email notifications about the Identity Reporting reports.	
Default email address	Specify the email address that you want Identity Reporting to use as the origin of email notifications.	
SMTP Server	Specify the DNS name of the SMTP server that Identity Reporting uses.	
SMTP Server Port	Specify the port number for the SMTP server. The default value is 465.	

Item	Description	Value
(Conditional) Use SSL for SMTP	Select whether you want to use secure communications with the SMTP server. If you select this option, you must configure your SMTP server for TLS/SSL communication. For more information, see Section 3.9, “Securing Connections with TLS/SSL,” on page 51.	
(Conditional) Require server authentication	Select whether you want to use authentication for communication with the SMTP server. If you select this option, you must provide the SMTP server credentials.	
SMTP user name and password	Specify the credentials for a login account to the SMTP server.	
Keep finished reports for	Specify the amount of time that Identity Reporting retains completed reports before deleting them. For example, to specify six months, enter 6, then select **Month**.	
Location of report definitions	Specify a path where you want to store the report definitions. The default directory is: ◆ **Linux:** `/opt/netiq/idm/apps/idrpt` ◆ **Windows:** `C:\netiq\idm\apps\idrpt`	
(Conditional) Auditing Details	Gather the following information if you want to enable auditing for Identity Reporting.	
Enable auditing	Select whether you want to enable auditing.	
Audit server	Specify the DNS name of the audit server.	
Audit port	Specify the port the audit server uses to communicate. The default port is 6514.	
Audit cache location	Specify a local directory on the Identity Reporting server for caching of audit events before they are sent to the audit server. The default directory is: ◆ **Linux:** `/opt/netiq/idm/apps/audit` ◆ **Windows:** `C:\netiq\idm\apps\audit`	

Item	Description	Value
Secure layer	Select if you are using TLS communication to the audit server. If you are, you can test the connection before you proceed. For more information, see Section 3.9, “Securing Connections with TLS/SSL,” on page 51.	
ConfigUpdate details	Specify the directory where the installer installs the Identity Governance Configuration Update utility, if it is not already installed.	

7.5 Installing Identity Reporting

This procedure describes how to install Identity Reporting for Identity Governance on a server without Identity Governance using the guided method or the console method. To perform a silent, unattended installation, see Section 7.6, “Silently Installing Identity Reporting,” on page 181.

To prepare for the installation, review the prerequisites and system requirements listed in Section 2.4.3, “Identity Reporting Server System Requirements,” on page 42. Also see the Release Notes accompanying the release.

1 Ensure that you review the prerequisites and system requirements as well as the current Release Notes for this release. For more information, see Section 2.4.3, “Identity Reporting Server System Requirements,” on page 42.

2 Ensure that you have completed the Identity Reporting Installation Worksheet and have all of the information to complete the installation. For more information, see Table 7-1, “Identity Reporting Installation Worksheet,” on page 167.

3 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 the Linux server or an administrator on the Windows server to complete the installation successfully.

4 Ensure that you have a copy of the installer on this server. For more information, see Section 2.2, “Obtaining Identity Governance, Identity Reporting, Workflow Engine, and OSP,” on page 31.

5 If you are in a clustered environment, proceed to Step 6, otherwise, stop Apache Tomcat. For more information, see Section 3.5.3, “Starting and Stopping Apache Tomcat,” on page 50.

6 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 use **Run as administrator** if you did not log in to your Windows server as an administrator.

   - **Linux:** Enter one of the following commands from a command prompt:
     - **Console:** `./identity-governance-install-linux.bin -i console`
     - **Guided:** `./identity-governance-install-linux.bin`

- **Windows:** Enter the following from a command prompt:
    - **Console:** `identity-governance-install-win.exe -i console`
    - **Guided:** `identity-governance-install-win.exe`

7 Read and accept the License Agreement.

8 Select **Identity Reporting** for the install set.

9 Use the information you gathered in Table 7-1, “Identity Reporting Installation Worksheet,” on page 167 to complete the installation.

10 Review the pre-installation summary.

11 (Conditional) If prompted, accept the certificates you trust, reject any certificates you do not trust, and acknowledge any errors.

The installer checks to see if you selected SSL/TLS or https for communication to the connected systems. The installer attempts to retrieve those certificates and add them to the trust store. If you used a self-signed certificate for any of the connected systems, the installer prompts you to accept or reject the certificates because self-signed certificates are untrusted certificates. The installer adds the accepted certificates to the trust store. For more information, see Section 3.9, “Securing Connections with TLS/SSL,” on page 51.

NOTE: If you are in a distributed environment, and if you are using a later version of Java Zulu OpenJDK (such as 8u312), the installer could present each certificate for acceptance only once. The installer compares certificates in a specific order. If the certificates you accepted are from a certificate authority (CA), then any subsequent certificates signed by the same CA are automatically trusted.

12 (Conditional) In a clustered environment, stop Apache Tomcat. For more information, see Section 3.5.3, “Starting and Stopping Apache Tomcat,” on page 50.

13 Start the installation process.

14 When the installation process completes, review the Identity Reporting installation logs. The default location of the logs is here:

- **Linux:** `/opt/netiq/idm/apps/idrpt/logs`
- **Windows:** `C:\netiq\idm\apps\idrpt\logs`

15 Before starting Apache Tomcat again, delete the contents of the following two directories from Apache Tomcat that contain cached files. The directories are:

- **Linux:** Default installation location:
    - `/opt/netiq/idm/apps/tomcat/temp`
    - `/opt/netiq/idm/apps/tomcat/work/Catalina/localhost`
- **Windows:** Default installation location:
    - `C:\netiq\idm\apps\tomcat\temp`
    - `C:\netiq\idm\apps\tomcat\work\Catalina\localhost`

16 Proceed to Chapter 9, “Completing the Installation Process,” on page 201.

NOTE: If you installed Identity Reporting on a server that does note have Internet access, see Section 9.4.4, “Configuring a Proxy Server for the Identity Reporting Server,” on page 214

7.6 Silently Installing Identity Reporting

A silent (non-interactive) installation does not display a user interface or any questions. Instead, the system uses information from a silent properties file. Identity Reporting and Identity Governance use the same installer to install these separate components. To silently install Identity Reporting you use the `identity-governance-install-silent.properties` file.

If you are installing Identity Reporting on a server without Identity Governance installed on it, we recommend that you perform a guided installation or console install of Identity Reporting and generate a response file. The response file contains the properties with values for your environment that you add to the `identity-governance-install-silent.properties` file.

WARNING: If you are deploying on Windows, ensure that you escape the backslashes `'\'` or the silent properties file do not work.

The steps to populate the `identity-governance-install-silent.properties` file and run it are the same whether you are installing Identity Reporting on a separate server or with Identity Governance. Follow the steps for silently installing Identity Governance to silently install Identity Reporting. For more information, see Section 6.6, "Silently Installing Identity Governance and its Components," on page 155.

When installing Identity Reporting on a separate server:

1. Copy the `encrypt-keys.pkcs` file.
2. Open the `identity-governance-install-silent.properties` file, then change the encryption keystore related properties to use the same encryption keystore file on the new node. Specifically set:

   ```
   install_enc_create_file=false
   install_enc_source_file=PATH
   ```

   where *PATH* is the location of the copied `encrypt-keys.pkcs12` file.

NOTE: If you installed Identity Reporting on a server that does note have Internet access, see Section 9.4.4, "Configuring a Proxy Server for the Identity Reporting Server," on page 214

8 Installing Workflow Engine

The Workflow Engine is a set of Java executables responsible for managing and executing steps in a workflow. Identity Governance contains the Workflow Engine, which you can install using the Identity Governance Installer. For information about installing Identity Governance, see Chapter 6, "Installing Identity Governance," on page 131.

When installing the Workflow Engine you can:

- Install the Workflow Engine on a separate server than identity Governance.

  IMPORTANT: Installing Workflow Engine on a remote server will be supported in a future release. If installing Workflow Engine, install it on the same Tomcat Server as Identity Governance.

- Install the Workflow Engine on the same server as Identity Governance. For more information on how to install the Workflow Engine with Identity Governance, see Chapter 6, "Installing Identity Governance," on page 129.
- Install the Workflow Engine on the same server as Identity Reporting. For more information on how to install the Workflow Engine with Identity Reporting, see Chapter 7, "Installing Identity Reporting," on page 163.

This chapter provides information about installing the Workflow Engine on a separate server from Identity Governance. Use the following information for the installation:

8.1 Prerequisites to Install the Workflow Engine

When installing the Workflow Engine you must meet the following prerequisites:

- ❒ Ensure that you have the appropriate version of Identity Governance installed on a different server. For more information, see "Identity Governance Installation Prerequisites" on page 134.
- ❒ Ensure that you meet hardware and software requirements for the computer that will host the Workflow Engine. For more information, see Section 2.4, "Hardware and Software Requirements," on page 39.
- ❒ Install Zulu OpenJDK and Apache Tomcat on the server that will host the Workflow Engine. For more information, see Chapter 3, "Installing Required Components," on page 45.

❒ Ensure that you have a supported database to which the installation process can connect. You can use the same database you deployed for Identity Governance. For more information, see Chapter 5, “Creating Databases for Identity Governance and Components,” on page 95.

  ❒ Ensure that the JDBC driver for the supported database is on the server where you install the Workflow Engine.

  ❒ Ensure that the database runs in the same subnetwork as the Workflow Engine.

  ❒ If you use an Oracle database, you must create the database (SID) in AL32UTF-8 (Unicode UTF-8 Universal character set) before installing the Workflow Engine.

❒ Ensure that all servers are set to the same time, particularly the servers for the database and events auditing components.

❒ (Conditional) If you want to enable email notifications, you must have an SMTP server installed and configured. If you want to guarantee email delivery, you must install ActiveMQ on the server where you install the Workflow Engine.

❒ (Conditional) If you want to enable secured auditing for the Workflow Engine, it is recommended that you configure the audit server to use TLS before beginning the installation so that the Workflow Engine installer can connect to the audit server and retrieve the audit server certificate to add to the local keystore. For more information, see Section 3.9, “Securing Connections with TLS/SSL,” on page 51.

8.2 Understanding the Installation Process for the Workflow Engine

The installation program for the Workflow Engine performs the following functions:

- Deploys the `wfconsole WAR` file, which contains the user interface components for workflows to the application server
- Deploys the `workflow WAR` file, which contains the core REST services needed for workflows
- Deploys the `wfdocs WAR` file, which contains the documentation for online help
- Installs, updates, or positions the JDBC driver that connects to the workflow database
- Configures the authentication services for the Workflow Engine
- (Optional) Creates the Bootstrap Administrator for the Workflow Engine

8.3 Understanding the Users that the Installation Process Creates

The Workflow Engine requires a specific user and schema for the 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.
igawfadmin	Created by Identity Governance and granted access to the Workflow Engine database.

If you do not want the installer to create the database for you, you must manually create the database and use the SQL files to populate the databases.

8.4 Workflow Engine Installation Worksheet

Gather the information listed in the following worksheet before starting the Workflow Engine installation. Use the information in the worksheet when you install Workflow Engine on a separate server from Identity Governance.

***Table 8-1** Workflow Engine Installation Worksheet*

Item	Description	Value
Installation location	Specify the installation path for Workflow Engine. **WARNING:** Spaces in the path are not supported. The default directory is: ◆ **Linux:** `/opt/netiq/idm/apps/wfe` ◆ **Windows:** `C:\netiq\idm\apps\wfe`	

Item	Description	Value
(Conditional) Identity Reporting Installation Location	If you are installing Identity Reporting on the same server as Workflow Engine, specify the installation path for Identity Reporting. **WARNING:** Spaces in the path are not supported. The default directory is: - **Linux:** `/opt/netiq/idm/apps/idrpt` - **Windows:** `C:\netiq\idm\apps\idrpt`	
Tomcat installation location	Specify the path to the Apache Tomcat home directory. **WARNING:** Spaces in the path are not supported. The default location is: - **Linux:** `/opt/netiq/idm/apps/tomcat` - **Windows:** `C:\netiq\idm\apps\tomcat`	
JRE home folder	Specify the path to the Zulu JRE directory. The Zulu JRE is installed when you install the Zulu OpenJDK. The installation process uses Java for several processes, such as to run commands and create security stores. **WARNING:** Spaces in the path are not supported. The default location is: - **Linux:** `/opt/netiq/idm/apps/jre` - **Windows:** `C:\netiq\idm\apps\jre`	

Item	Description	Value
(Conditional) Encryption Keystore	If Workflow Engine is not installed at the same time as Identity Governance, then you must specify the encryption keystore file. You must always select the **Use existing option** so that you can select the `encrypt-keys.pkcs12` file that was created while installing OSP. If OSP is on a separate server, copy the `encrypt-keys.pkcs12` file from the installed location of the first server to the second server. Then during installation, navigate to the location where you had copied the file and then select the file. If OSP is on the same server, navigate to the `/opt/netiq/idm/apps/tomcat/conf` folder and select the `encrypt-keys.pkcs12` file. Select the **Create new** option if: ◆ You do not have an existing encryption key from a previous OSP or Identity Governance installation ◆ Your authentication method is Access Manager	
Encryption Keystore Password	Enter the encryption keystore password that you have created while installing OSP or enter a new password when using Access Manager as your authentication method.	
Trust store password	If you have a trust store that contains the certificates for TLS communication, specify that password, otherwise, specify a password that is six characters or longer and has no spaces. The installer creates the trust store for you using this password.	
Authentication Service	Use the following sections to gather information about your OSP deployment or your Access Manager deployment. You must use one of these services to deploy the Workflow Engine.	

Item	Description	Value
Access Manager or OSP	Select the appropriate authentication service for your environment. Depending on your choices, there are different options presented that you must populate with the information for the specific authentication service. The options are **OSP** or **Access Manager**.	
(Conditional) OSP > Application address	If you selected Access Manager, skip the sections about OSP. Specify the URL connection information the clients use to access the Workflow Engine.	
OSP > Workflow Engine protocol	Select if you want to use **http** or **https** for the Workflow Engine. If you select **https**, you must have configured Apache Tomcat for TLS/SSL communication.	
OSP > Workflow Engine host name	**WARNING:** Use the fully qualified domain name (FQDN) rather than localhost or an IP address. In a non-clustered environment, specifies the DNS name of the Workflow Engine server. In a clustered environment, specifies the DNS name of the server that hosts the load balancer or the reverse proxy.	
OSP > Workflow Engine port	Specify the port you want the Workflow Engine server to use for communication with client computers. The default is 8080. To use TLS/SSL, the default is 8443. When installing in a clustered environment or when using a reverse proxy, specify the port of the load balancer or the reverse proxy.	
(Conditional) OSP > Connect to an external OSP server	If you have OSP installed on a separate server from the Workflow Engine, select this option and then define the protocol, host name, and port for the external OSP server.	

Item	Description	Value
OSP > OSP authentication server protocol	If OSP is on a separate server from the Workflow Engine select whether the clients that connect to OSP use **http** or **https**. To use **https**, ensure that you have configured the Apache Tomcat instance on the OSP server to use SSL/TLS.	
OSP > OSP authentication server host name	**WARNING:** Use the fully qualified domain name (FQDN) rather than localhost or an IP address of the external OSP server. In a non-clustered environment, specifies the DNS name of the OSP server. In a clustered environment, specifies the DNS name of the server that hosts the load balancer or the reverse proxy for OSP.	
OSP > OSP authentication server port	Specify the port that the clients use to access OSP. For http, the default port is 8080. For https, the default port is 8443.	
(Conditional) Access Manager > Application address	If you selected **OSP**, skip the following sections about Access Manager.	
Workflow Engine protocol	Select if you want to use **http** or **https** for the Workflow Engine.	
Workflow Engine host name	**WARNING:** Use the fully qualified domain name (FQDN) rather than localhost or an IP address of the Apache Tomcat instance for the Workflow Engine.	
Workflow Engine port	Specify the port that the Workflow Engine uses. The default port for http is 8080. The default port for https is 8443.	
Access Manager IDP host name	**WARNING:** Use the fully qualified domain name (FQDN) rather than localhost or an IP address. Specify the DNS name of the Access Manager identity provider server.	
Access Manager IDP port	Specify the port the Access Manager identity provider uses. The default port is 443.	
Access Manager Console host name	Specify the DNS name of the Access Manager administration console.	

Item	Description	Value
Access Manager Console port	**WARNING:** Use the fully qualified domain name (FQDN) rather than localhost or an IP address. Specify the port of the Access Manager administration console. The default port is 443.	
Identity Governance details	If you are installing the Workflow Engine after you have installed Identity Governance, you must provide information about the protocol, server, and port for Identity Governance.	
Identity Governance protocol	Provide information about the communication protocol.	
Identity Governance server information	Provide the Identity Governance host name.	
Identity Governance port number	Provide the Identity Governance port information.	
Service Password	This is an OAuth 2.0 password that allows users to single sign-on to the Workflow Engine. Specify this password and remember it for later use. You can change this password after the installation completes through the configuration utilities.	
(Conditional) ActiveMQ Details		
Use ActiveMQ or Do not use ActiveMQ	Select whether you want to use ActiveMQ to guarantee email delivery. If you select Use ActiveMQ, you must install ActiveMQ on the server where you are installing the Workflow Engine.	
ActiveMQ host name	Specify the DNS name of the server where you have installed ActiveMQ.	
ActiveMQ port	Specify the port that ActiveMQ uses to communicate. The default port is 61616.	
(Conditional) Access Manager > Bootstrap Administrator Details		

Item	Description	Value
Bootstrap admin DN	Specify the DN of the LDAP bootstrap administrator for Identity Governance. You must have an LDAP bootstrap administrator to integrate with Access Manager. For more information, see Section 4.1.1, “Using the Bootstrap Administrator,” on page 58.	
Bootstrap admin password	Specify the password of the LDAP bootstrap administrator account for Identity Governance.	
Access Manager admin DN	Specify the DN of an Access Manager administrator account.	
Access Manager admin password	Specify the password for the Access Manager administrator account.	
Database Details	Collect the following information for the database type that you have selected to use. Ensure that you install the database before starting the Workflow Engine installation. For more information, see Section 5.8, “Creating the Databases before Installing Identity Governance,” on page 101.	
Database type:	Select the type of database that you are using. ◆ Microsoft SQL Server ◆ Oracle ◆ PostgreSQL For a list of the supported database versions, see Section 2.4.2, “Database Requirements,” on page 41.	
Database Configuration Details	Select one of the following three options: ◆ “Database details > Configure database now” on page 173 ◆ “Database details > Generate SQL for later” on page 174 ◆ “Database details > No database configuration” on page 174	

Item	Description	Value
Database details > **Configure database now**	Select this option to have the installer create and populate the database. You select this option if you are performing an upgrade or a new installation. For more information, see Section 5.4, "Using the Identity Governance Installer to Create and Populate the Databases," on page 98.	
Database details > **Generate SQL for later**	Select this option to have your database administrator create and populate the database for the Workflow Engine using the SQL scripts generated and stored by the installer in the following default directory for the Workflow Engine: - **Linux:** `/opt/netiq/idm/apps/wfe/sql` - **Windows:** `C:\netiq\idm\apps\wfe\sql`	
Database details > **No database configuration**	Select this option to do nothing. You would select this option if you were installing the second node in a cluster. For more information, see Section 2.3.4, "Ensuring High Availability or Load Balancing for Identity Governance," on page 35.	
Host	**WARNING:** Use the fully qualified domain name (FQDN) rather than localhost or an IP address. Specify the DNS name of the database server.	
Port	Specify the port the database server uses to communicate. The default port is: - **Microsoft SQL:** 1433 - **Oracle:** 1521 - **PostgreSQL:** 5432	
(Conditional) Microsoft SQL Server JDBC JAR	If you are using the Microsoft SQL Server, specify the path to the Microsoft SQL Server JDBC JAR file. For more information, see Section 5.7, "Adding the JDBC File to the Application Server," on page 101.	

Item	Description	Value
(Conditional) Oracle Database Details	If you are using an Oracle database, gather the following information to complete the Workflow Engine installation.	
Oracle JDBC JAR	Specify the path to the Oracle JDBC JAR file. For more information, see Section 5.7, “Adding the JDBC File to the Application Server,” on page 101	
Oracle Database name	Specify the name of the Oracle database where the installer will add the schema for the Workflow Engine. For example, `oracleidgov`	
Oracle User tablespace	Specify the name of the database storage unit for storing the schema for the Workflow Engine databases. The default is `USERS`.	
Oracle Temporary tablespace	Specify the name of the temporary database storage unit for storing the schema. The default name is `TEMP`.	
Database credentials	Specify the credentials for accessing the various databases.	
(Conditional) Database Administrator user and password	Specify the credentials of a database account that can access and modify data in the databases. This account must be able to create databases, tables, views, and other artifacts. You can test the connection to the database.	
(Conditional) Identity Reporting database users password	If you install Identity Reporting with Workflow Engine, specify the name and password of the required database for Identity Reporting. The default database name is `igrpt`. **NOTE:** The database password is requested only for Microsoft SQL Server and PostgreSQL.	
Workflow Engine database name	Specify the name of the required database for the Workflow Engine. The default name is `igaworkflowdb`.	
Workflow Engine database user name	Specify the user name of the Workflow Engine database. The default name is `igawfadmin`.	
Workflow Engine database user’s password	Specify the password of the Workflow Engine database.	

Item	Description	Value
Update or Only use existing	Applies only when you choose to configure the database during the installation. Select whether the installer creates the database name, creates the schema, creates users, creates roles, assigns permissions to roles, and populates the database with this information. Select this option for new installations or upgrades. Or select to use existing databases with your database name and user.	
Operation user database and password	Specify the name of the operations database and the password for the operations database. The default name is `igops`.	
(Conditional) Different database vendor than Identity Governance	Select this option if you have a different database type for the Workflow Engine database than what you used for Identity Governance. You can use the same database type for the two components or you can use separate, supported database types.	
Database host	Specify the DNS name of the separate database from the database Identity Governance uses.	
Database port	Specify the port the separate database server uses to communicate. The default port is: ◆ **Microsoft SQL Server:** 1433 ◆ **Oracle:** 1521 ◆ **PostgreSQL:** 5432	
Database type:	Select the type of database that you are using: ◆ Microsoft SQL Server ◆ Oracle ◆ PostgreSQL For a list of the supported database versions, see Section 2.4.2, "Database Requirements," on page 41.	

Item	Description	Value
(Conditional) Microsoft SQL Server JDBC JAR	If you are using Microsoft SQL Server, specify the path to the Microsoft SQL Server JDBC JAR file. For more information, see Section 5.7, "Adding the JDBC File to the Application Server," on page 101.	
(Conditional) Oracle Database Details	If you are using an Oracle database, gather the following information to complete the Workflow Engine installation.	
Oracle JDBC JAR	Specify the path to the Oracle JDBC JAR file. For more information, see Section 5.7, "Adding the JDBC File to the Application Server," on page 101	
Oracle Database name	Specify the name of the Oracle database where you will add the Oracle schema for the Workflow Engine.	
(Conditional) Additional Identity Reporting Options Identity Reporting > Target Locale	If you install Identity Reporting with Workflow Engine, you must select the language Identity Reporting uses to generate the reports. The default is English.	
Email Delivery	Gather the information for the SMTP server that delivers report notifications.	
Default email address	Specify the email address that you want to use as the origin of email notifications.	
SMTP Server	**WARNING:** Use the fully qualified domain name (FQDN) rather than localhost or an IP address. Specify the DNS name of the SMTP email host that is used for email notifications.	
SMTP Server Port	Specify the port number for the SMTP server. The default value is 465.	
(Conditional) Use SSL for SMTP	Select whether you want to use secure communication with the SMTP server. If you select this option, you must configure your SMTP server for TLS/SSL communication. For more information, see Section 3.9, "Securing Connections with TLS/SSL," on page 51.	

Item	Description	Value
(Conditional) Require server authentication	Select whether you want to use authentication for communication with the SMTP server. If you select this option, you must provide the SMTP server credentials.	
SMTP user name and password	Specify the credentials for a login account to the SMTP server.	
(Conditional) Identity Reporting > Keep finished reports for	If you install Identity Reporting with Workflow Engine, then specify the report retention time and location. For example, to specify retention time of six months, enter 6, then select **Month**. Identity Reporting retains completed reports for the specified time then deletes them.	
(Conditional) Identity Reporting > Location of report definitions	Specify a path where you want to store the report definitions. The default directory is: ◆ **Linux:** `/opt/netiq/idm/apps/idrpt` ◆ **Windows:** `C:\netiq\idm\apps\idrpt`	
(Conditional) Auditing Details	Gather the following information if you want to enable auditing for the Workflow Engine.	
Enable auditing	Select whether you want to enable auditing.	
Audit server	Specify the DNS name of the audit server.	
Audit port	Specify the port the audit server uses to communicate. The default port is 6514.	
Audit cache location	Specify a local directory for caching of audit events before they are sent to the audit server. The default directory is: ◆ **Linux:** `/opt/netiq/idm/apps/audit` ◆ **Windows:** `C:\netiq\idm\apps\audit`	

Item	Description	Value
Secure layer	Select if you are using TLS communication to the audit server. If you are, you can test the connection before you proceed. For more information, see Section 3.9, “Securing Connections with TLS/SSL,” on page 51.	

8.5 Installing Workflow Engine on a Separate Server

This procedure describes how to install Workflow Engine for Identity Governance using the guided method or the console method. You can also perform a silent installation by using the silent properties file.

To prepare for the installation, review the prerequisites and system requirements.

1 Log in as an administrator on the server where you want to install the Workflow Engine.

> **NOTE:** The Workflow Engine requires you to log in as `root` on the Linux server or an administrator on the Windows server to complete the installation successfully.

2 Ensure that you have a copy of the installer on this server. For more information, see Section 2.2, “Obtaining Identity Governance, Identity Reporting, Workflow Engine, and OSP,” on page 31.

3 If you are using an unsecured environment, stop Apache Tomcat. Otherwise you need Apache Tomcat running so the certificates can be retrieved during Step 9.

4 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 use **Run as administrator** if you did not log in to your Windows server as an administrator.

- **Linux:** Enter one of the following commands from a command prompt:
  - **Console:** `./identity-governance-install-linux.bin -i console`
  - **Guided:** `./identity-governance-install-linux.bin`
- **Windows:** Enter the following from a command prompt:
  - **Console:** `identity-governance-install-win.exe -i console`
  - **Guided:** `identity-governance-install-win.exe`

5 Read and accept the License Agreement.

6 Select **Workflow Engine** for the install set.

7 Use the information you gathered in Section 8.4, “Workflow Engine Installation Worksheet,” on page 185 to complete the installation.

8 Review the pre-installation summary.

9 (Conditional) If prompted, accept the certificates you trust, reject any certificates you do not trust, and acknowledge any errors.

The installer checks to see if you selected SSL/TLS or https for communication to the connected systems. The installer attempts to retrieve those certificates and add them to the trust store. If you used a self-signed certificate for any of the connected systems, the installer prompts you to accept or reject the certificates because self-signed certificates are untrusted certificates. The installer adds the accepted certificates to the trust store. For more information, see Section 3.9, “Securing Connections with TLS/SSL,” on page 51.

NOTE: If you are in a distributed environment, and if you are using a later version of Java 11, such as 11.0.22, the installer could present each certificate for acceptance only once. The installer compares certificates in a specific order. If the certificates you accepted are from a certificate authority (CA), then any subsequent certificates signed by the same CA are automatically trusted.

10. (Conditional) In a secured (TLS) environment, stop Apache Tomcat. For more information, see Section 3.5.3, “Starting and Stopping Apache Tomcat,” on page 50.
11. Start the installation process.
12. When the installation process completes, review the Workflow Engine logs. The default location of the logs is here:
    - **Linux:** `/opt/netiq/idm/apps/wfe/logs`
    - **Windows:** `C:\netiq\idm\apps\wfe\logs`
13. Before starting Apache Tomcat again, delete the contents of the following two directories from Apache Tomcat that contain cached files. The directories are:
    - **Linux:** Default installation location:
        - `/opt/netiq/idm/apps/tomcat/temp`
        - `/opt/netiq/idm/apps/tomcat/work/Catalina/localhost`
    - **Windows:** Default installation location:
        - `C:\netiq\idm\apps\tomcat\temp`
        - `C:\netiq\idm\apps\tomcat\work\Catalina\localhost`
14. Proceed to Chapter 9, “Completing the Installation Process,” on page 201.

8.6 Silently Installing Workflow Engine

A silent (non-interactive) installation does not display a user interface or any questions. Instead, the system uses information from a silent properties file. The Workflow Engine and Identity Governance use the same installer to install these separate components. To silently install the Workflow Engine you use the `identity-governance-install-silent.properties` file.

If you are installing the Workflow Engine on a server without Identity Governance installed on it, we recommend that you perform a guided installation or console installation of Workflow Engine and generate a response file. The response file contains the properties with values for your environment that you add to the `identity-governance-install-silent.properties` file.

WARNING: If you are deploying on Windows, ensure that you escape the backslashes `'\'` or the silent properties file do not work.

The steps to populate the `identity-governance-install-silent.properties` file and run it are the same whether you are installing the Workflow Engine on a separate server or with Identity Governance. Follow the steps for silently installing Identity Governance to silently install the Workflow Engine. For more information, see Section 6.6, “Silently Installing Identity Governance and its Components,” on page 155.

When installing Workflow Engine on a separate server:

1. Copy the `encrypt-keys.pkcs` file.
2. Open the `identity-governance-install-silent.properties` file, then change the encryption keystore related properties to use the same encryption keystore file on the new node. Specifically set:

   ```
   install_enc_create_file=false
   install_enc_source_file=PATH
   ```

   where *PATH* is the location the copied `encrypt-keys.pkcs12` file.

9 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 Apache Tomcat configuration file on each node specifies a unique runtime identifier.

9.1 Checklist for Configuring Identity Governance

After you complete the installation of the required components, the database, OSP or Access Manager, Identity Governance, Identity Reporting, and Workflow Engine (optional) you must perform some configuration tasks with the bootstrap administrator account before you can use Identity Governance. Use the following checklist to ensure that you complete all of the required configuration tasks for Identity Governance to work.

	Checklist Item
□	1. 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 Section 2.4.1, “Identity Governance Server System Requirements,” on page 39.
□	2. Complete the setup for Identity Governance and its database. For more information, see Section 9, “Completing the Installation Process,” on page 201.
□	3. (Conditional) For OSP authentications to work you must manually extend the schema in the identity service if it is not part of Identity Manager. For more information, see Section 9.2.2, “Extending the Schema for OSP in the Identity Service not Part of Identity Manager,” on page 205.
□	4. (Optional) Modify the SSL settings for communication with the identity service. For more information, see Section 3.9, “Securing Connections with TLS/SSL,” on page 51.
□	5. (Optional) Modify the configuration settings for Identity Governance. For more information, see Chapter 11, “Customizing Your Installation,” on page 239.
□	6. (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” in the *Identity Governance User and Administration Guide*.
□	7. (Optional) Customize the user interface. For more information, see Section 11.3.1, “Customizing the Labels in the Identity Governance Interface,” on page 241.

	Checklist Item
□	8. (Optional) Customize the templates for email notifications and collectors. For more information, see “Customizing Email Notification Templates” and “Customizing the Collector Templates for Data Sources” in the *Identity Governance User and Administration Guide*.
□	9. (Optional) Create a single sign-on experience for users between Identity Governance and Identity Manager Home and Provisioning Dashboard. For more information, see Section 10.5.1, “Checklist for Integrating Identity Governance with Identity Manager,” on page 232.

9.2 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 identity service require some additional steps.

- Section 9.2.1, “Ensuring the Identity Governance Configuration Update Utility Can Run OSP,” on page 202
- Section 9.2.2, “Extending the Schema for OSP in the Identity Service not Part of Identity Manager,” on page 205
- Section 9.2.3, “Configuring OSP to Work with AD FS,” on page 205
- Section 9.2.4, “Configuring OSP to Use Google reCAPTCHA,” on page 208

9.2.1 Ensuring the Identity Governance Configuration Update Utility Can Run OSP

When you run OSP on a different Apache Tomcat server than Identity Governance, and you do not have Identity Manager in your environment, you must ensure that the Identity Governance Configuration Update utility has the appropriate values to run OSP. The Identity Governance Configuration Update utility (`configupdate.sh` or `configupdate.bat`) contains the settings that allow OSP to function and settings for Identity Governance.

The installation programs for Identity Governance, OSP, and Identity Reporting modify the following properties in the Identity Governance Configuration Update utility during the following conditions:

Table 9-1 *Identity Governance Configuration Update Utility Properties*

Properties	Conditions
`use_ssl=true` if LDAP is secured	Only the OSP installer sets this option. The Identity Governance and Identity Reporting installers preserve the existing value.
`use_ssl=false` if LDAP is not secured	Only the OSP installer sets this option. The Identity Governance and Identity Reporting installers preserve the existing value.
`edition=none`	Limits the pages that the Identity Governance Configuration Update utility displays. The alternative values are `standard` and `advanced`.

Properties	Conditions
`sso_apps=' '`	Property is usually missing entirely. Identity Governance and Reporting are on this server. If the property value is empty, it removes the **SSO Clients** tab from the Identity Governance Configuration Update utility.
`sso_apps='ig'`	Identity Governance is on a different server. Reporting exists on this server or no server. The tab title displays as **IG SSO Clients**.
`sso_apps='ig,rpt'`	Identity Governance and Reporting are on different servers. The tab title displays as **IG SSO Clients**.
`sso_apps='rpt'`	Reporting is on a different server. The tab title displays as **Reporting SSO Clients**.
`force_no_osp=true`	OSP is not on this server. This property removes the **Identity Vault** tab from the Identity Governance Configuration Update utility.
`force_no_osp=false`	OSP is on this server. The Identity Governance Configuration Update utility displays the **Identity Vault** tab.
`reporting_admins_app=`	Reporting is not on this server.
`reporting_admins_app=ig`	Reporting is on this server.

For more information, see "SSO Clients Parameters" in the *NetIQ Identity Manager Setup Guide for Linux*.

To update properties in the Identity Governance Configuration Update utility:

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:\netiq\idm\apps\tomcat\conf`

2 In a text editor, open the `configupdate.sh.properties` or `configupdate.bat.properties` to update the values.

- **Linux:** Default location in `/opt/netiq/idm/apps/configupdate/configupdate.sh.properties`
- **Windows:** Default location in `C:\netiq\idm\apps\configupdate\configupdate.bat.properties`

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 the Identity Governance Configuration Update utility in guided mode

2b Save and close the file.

3 Update settings in the Identity Governance Configuration Update utility.

3a Launch the Identity Governance Configuration Update utility.

- **Linux:** Default location in the `/opt/netiq/idm/apps/configupdate`

  ```
  ./configupdate.sh
  ```

- **Windows:** Default location in `C:\netiq\idm\apps\configupdate`

  ```
  configupdate.bat
  ```

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, `dcsdriver`.

- **OAuth client secret**

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

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

3g (Conditional) If this is the first time you run the Identity Governance Configuration Update utility, under **Authentication**, go to Advanced Settings and enter the bootstrap administrator password. By doing this, the `adminusers.txt` file is not overwritten or deleted. If you do not do this, you will not be able to login as bootstrap administrator when you restart Apache Tomcat.

9.2.2 Extending the Schema for OSP in the Identity Service not Part of Identity Manager

If you have integrated with Identity Manager you can skip this section. To have OSP authentications work, you must manually extend the schema in the identity service that is not part of the Identity Manager deployment.

WARNING: Work with your directory administrator to properly extend the schema on the server or data corruption can occur.

The OSP installation places the files required to extend the schema in the following default directory:

- **Linux**
  - **Active Directory:** `/opt/netiq/idm/apps/osp/osp-extras/schema/ad/osp_ext.ldif`
  - **eDirectory:** `/opt/netiq/idm/apps/osp/osp-extras/schema/edir/osp.sch`
- **Windows**
  - **Active Directory:** `c:\netiq\idm\apps\osp\osp-extras\schema\ad\osp_ext.ldif`
  - **eDirectory:** `c:\netiq\idm\apps\osp\osp-extras\schema\edir\osp.sch`

To manually extend the schema on the eDirectory server, see “Manually Extending the Schema”. To manually extend the schema on the Active Directory server, see “How to Extend the Schema”.

9.2.3 Configuring OSP to Work with AD FS

Identity Governance supports AD FS as an identity service as long as AD FS is pointing to eDirectory or Active Directory. You must perform additional configuration steps for OSP and AD FS for this integration to work. There are requirements that you must meet before starting the configuration process.

- Section 9.2.3.1, “Requirements for Configuring OSP to Work with AD FS,” on page 205
- Section 9.2.3.2, “Configuring OSP to Provide SAML Authentications to AD FS,” on page 206

9.2.3.1 Requirements for Configuring OSP to Work with AD FS

Ensure that you meet the following requirements that you must meet before you can configure OSP to work with AD FS.

- ❒ Ensure that AD FS uses the same TLS version that the Apache Tomcat instance for Identity Governance uses for both incoming and outgoing communication. By default, Identity Governance uses TLS 1.2 and by default AD FS uses TLS 1.0. If AD FS uses a lower version than what Identity Governance uses it can cause issues with the integration. For more information, see “Managing SSL/TLS Protocol and Cipher Suites for AD FS ”.
- ❒ Ensure that Identity Governance is using https because AD FS requires it. For more information, see Section 3.9, “Securing Connections with TLS/SSL,” on page 51.
- ❒ Ensure that you are using Identity Governance 3.6 or later.

9.2.3.2 Configuring OSP to Provide SAML Authentications to AD FS

To configure OSP to provide authentications to AD FS you must perform configuration steps for OSP and AD FS. The following procedure contains information to match the users on the email attribute from Active Directory using a local Active directory server. You must change the custom rule examples for your environment.

1 Ensure that you meet the requirements for this integration before proceeding. For more information, see “Requirements for Configuring OSP to Work with AD FS” on page 205.

2 Configure the OSP server to provide SAML authentications to AD FS.

2a Ensure that Apache Tomcat is running on the OSP server.

2b Launch the Identity Governance Configuration Update utility on the OSP server. For more information, see Section 15.1.5, “Using the Identity Governance Configuration Update Utility,” on page 293.

2c Click the **Authentication** tab.

2d Click **Show Advanced Options** at the end of the page.

2e Under **Authentication Method > Method** select **SAML 2.0**.

2f Use the following information to configure OSP to use SAML 2.0:

Mapping Attribute

Specify the attribute listed is the one you want to use to map the user accounts to Access Manager. The default value is `mail`.

Landing Page

Select where the landing page for your users is internal, external, or if there is not one. The default value is **None**.

Metadata source

Select **URL** to use the Access Manager metadata.

Metadata URL

Specify the AD FS metadata URL in this field.

```
https://adfs-server/FederationMetadata/2007-06/
FederationMetadata.xml
```

Load on save

Select this option to load the metadata.

2g Under the **Identity Governance Bootstrap Administrator** heading, ensure that you are using an LDAP-based bootstrap administrator account. For more information, see Section 4.1.1, “Using the Bootstrap Administrator,” on page 58.

2h Click **OK**.

2i Click **Yes** to accept the certificate.

2j Restart Apache Tomcat on the OSP server. For more information, see Section 3.5.3, “Starting and Stopping Apache Tomcat,” on page 50.

2k Ensure that Apache Tomcat is running on the OSP server before proceeding.

3 Create a relying party trust in AD FS to the OSP server using the OPS metadata.

3a Create the relying party trust in AD FS following the Microsoft documentation. For more information, see "Creating a Relying Party Trust (https://docs.microsoft.com/en-us/windows-server/identity/ad-fs/operations/create-a-relying-party-trust)".

3b Use OSP metadata URL to finish the configuration. The default location of the URL is:

```
https://osp-server:port/osp/a/idm/auth/saml2/spmetadata
```

3c At the end of the configuration, ensure that you select **Configure claims assurance policy for this application**.

3d (Conditional) If the **Configure claims assurance policy configuration** does not automatically load, right click on the **Relaying Party Trust** you created in Step 3a, then select **Edit Claims Insurance Policy**.

3e Add two custom rules to have AD FS send the email attribute and a local Active Directory server information to the OSP server. For more information, see AD FS 2.0 Claim Rule LanguagePrimer(https://blogs.technet.microsoft.com/askds/2011/10/07/ad-fs-2-0-claims-rule-language-primer/).

Sending the email attribute

Use the following information to create the first custom rule to send the email attribute:

Name

Specify a name for the rule.

Provide the Custom Rule

The following is a sample rule that you might need to edit for your environment.

```
c:[Type == "http://schemas.microsoft.com/ws/2008/06/
identity/claims/windowsaccountname", Issuer == "AD
AUTHORITY"]
 => issue(store = "Active Directory", types = ("mail",
"http://schemas.xmlsoap.org/ws/2005/05/identity/claims/
upn"), query = ";mail,userPrincipalName;{0}", param =
c.Value);
```

Sending Via SAML

Use the following information to create the second rule to send the attribute to the OSP server via SAML:

Name

Specify a name for the custom rule.

Provide the Custom Rule

The following is a sample rule that you must edit for your environment.

```
c:[Type == "http://schemas.xmlsoap.org/ws/2005/05/identity/
claims/upn"]
 => issue(Type = "http://schemas.xmlsoap.org/ws/2005/05/
identity/claims/nameidentifier", Issuer = c.Issuer,
OriginalIssuer = c.OriginalIssuer, Value = c.Value,
ValueType = c.ValueType, Properties["http://
schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/
format"] = "urn:oasis:names:tc:SAML:2.0:nameid-
format:transient", Properties["http://schemas.xmlsoap.org/
ws/2005/05/identity/claimproperties/namequalifier"] =
"http://adfs-server/adfs/services/trust", Properties["http:/
/schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/
spnamequalifier"] = "https://osp-server:osp-port/osp/a/idm/
auth/saml2/metadata", Properties["http://
schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/
spprovidedid"] = c.Value);
```

9.2.4 Configuring OSP to Use Google reCAPTCHA

To configure OSP to use Google reCAPTCHA, you need a Google account to sign in to Google, and then sign up for an API key pair. For more information about reCAPTCHA, and how to create the API key pair, see the *Google reCAPTCHA Developer's Guide.* After you create the API key pair, you can configure OSP to work with Google reCAPTCHA.

NOTE: The API key pair includes a site key and a secret key, which are required to perform this configuration procedure.

1 Launch the Identity Governance Configuration Update utility on the OSP server. For more information, see Section 15.1.5, "Using the Identity Governance Configuration Update Utility," on page 293.

2 Click the **Authentication** tab.

3 Click **Show Advanced Options**.

4 In the Authentication Method section, perform the following steps:

4a Select **Name and Password** from the Method list, if it is not already selected.

4b Select **Enable reCAPTCHA**, and then enter the appropriate values in the following fields:

Number of attempts before required

Type the number of access attempts required before reCAPTCHA is required for access. The default value is 0.

Site key

Copy and paste the site key created when you created the API key pair.

Private key

Copy and paste the secret key created when you created the API key pair.

5. Click **OK**, then accept the Google certificate chain.
6. Restart Apache Tomcat on the OSP server. For more information, see Section 3.5.3, “Starting and Stopping Apache Tomcat,” on page 50.

To verify you correctly configured OSP to work with reCAPTCHA, open a browser and access either Identity Governance or Identity Reporting. If you retained the default 0 attempts in this procedure, reCAPTCHA appears immediately. Otherwise, reCAPTCHA appears after the number of access attempts you defined in this procedure.

9.3 Starting and Initializing Identity Governance

To verify installation and to initialize the Identity Governance databases, you must start Apache Tomcat. In a clustered environment, start the primary node first to ensure that the initial database load occurs before the other nodes start.

1. Before starting Apache Tomcat, delete the contents of the following two directories from Apache Tomcat that contain cached files. The directories are:
   - **Linux:** Default installation location:
     - `/opt/netiq/idm/apps/tomcat/temp`
     - `/opt/netiq/idm/apps/tomcat/work/Catalina/localhost`
   - **Windows:** Default installation location:
     - `C:\netiq\idm\apps\tomcat\temp`
     - `C:\netiq\idm\apps\tomcat\work\Catalina\localhost`
2. (Optional) Verify that the schemas (Oracle) or databases (Microsoft SQL or PostgreSQL) exist in your database platform.
3. To initialize Identity Governance and its databases, start Apache Tomcat. For more information, see Section 3.5.3, “Starting and Stopping Apache Tomcat,” on page 50.

   NOTE: In a clustered environment, start Apache Tomcat only on the primary (or master) node.
4. (Conditional) To observe the initialization process in Apache 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
   ```
5. 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.

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

6a Log in as an administrator to the server where you installed Identity Governance.

6b In a terminal, navigate to the following directory:

- **Linux:** `/opt/netiq/idm/apps/idgov/logs`
- **Windows:** `C:\netiq\idm\apps\idgov\logs`

6c Enter the following command:

```
tail -n 1 *
```

6d 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 commands and multiple iterations of `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.

7 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 “Creating Identity Sources ” in the *Identity Governance User and Administration Guide*.

8 (Conditional) If you can verify installation but cannot get Identity Governance to load in a web browser, complete the following steps:

8a Stop Identity Governance (and Apache Tomcat). For more information, see Section 3.5.3, “Starting and Stopping Apache Tomcat,” on page 50.

8b Navigate to the following directory:

- **Linux:** `/opt/netiq/idm/apps/tomcat/bin`
- **Windows:** `C:\netiq\idm\apps\tomcat\bin`

8c In a text editor, open `setenv.sh` or `setenv.bat`.

This file defines global variables and export paths needed to host Identity Governance under Apache Tomcat.

8d Verify that the file lists the correct host name for the Identity Vault and paths to Apache Tomcat.

8e Save and close the file.

8f Start Identity Governance (and Apache Tomcat). For more information, see Section 3.5.3, “Starting and Stopping Apache Tomcat,” on page 50.

9 (Conditional) In a clustered environment, start Apache Tomcat on the secondary nodes.

10 (Conditional) To configure Identity Reporting, continue to “Configuring Identity Reporting” on page 211.

11 (Conditional) To integrate Identity Governance with Identity Manager, continue to “Integrating Single Sign-on Access with Identity Manager Using OSP” on page 232.

12 Add users who can log in to Identity Governance, and assign authorizations to those users. For more information, see “Adding Identity Governance Users and Assigning Authorizations” in the *Identity Governance User and Administration Guide*.

13 (Optional) Configure Identity Governance, such as customizing the email templates and displayed labels. For more information, see Chapter 11, “Customizing Your Installation,” on page 239.

9.4 Configuring Identity Reporting

After installing Identity Reporting, you can modify many of the installation properties. To make changes, run the Identity Governance Configuration Update utility. For more information, see Section 15.1.5, “Using the Identity Governance Configuration Update Utility,” on page 293.

If you change any setting for Identity Reporting with the Identity Governance Configuration Update 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.

You should also update to the latest version of the Identity Governance reports. For more information, see “Using the Download Page” in the *Identity Governance Reporting Guide*.

- Section 9.4.1, “Assigning the Report Administrator Authorization,” on page 211
- Section 9.4.2, “Starting Identity Reporting,” on page 212
- Section 9.4.3, “Testing the Integration with Identity Governance,” on page 212
- Section 9.4.4, “Configuring a Proxy Server for the Identity Reporting Server,” on page 214
- Section 9.4.5, “Adding Data Sources to Identity Reporting,” on page 215

9.4.1 Assigning the Report Administrator Authorization

To access Identity Reporting you must assign the Report Administrator authorization and identify at least one data source. You assign the administrator authorization in Identity Governance. Use the following steps to assign the Report Administrator authorization to a user or group.

To assign the Report Administrator authorization:

1 Log in to Identity Governance as the Global Administrator.

2 Select **Configuration > 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.

You must now add a data source for Identity Reporting to be able to generate reports. For more information, see Section 9.4.5, “Adding Data Sources to Identity Reporting,” on page 215.

9.4.2 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 cache directory, located by default in `/opt/netiq/idm/apps/tomcat/work/Catalina/localhost`
  - **Windows:** Temporary directory, located by default in:
    - `C:\netiq\idm\apps\tomcat\temp`
    - Catalina cache directory, located by default in: `C:\netiq\idm\apps\tomcat\work\Catalina\localhost`

  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 Apache Tomcat. For more information, see Section 3.5.3, “Starting and Stopping Apache Tomcat,” on page 50.

4 (Optional) To observe the Apache Tomcat initialization process in Linux, 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 Section 9.4.1, “Assigning the Report Administrator Authorization,” on page 211.

9.4.3 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 application through a URL. Only accounts with the Report Administrator authorization can 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 as a Report Administrator.

```
https://myserver.mydomain.com:8443/IDMRPT
```

  1b Select **Home** in the upper right corner.

- **1c** Select the **Reporting** module icon near your user name.
- **1d** Verify that you are redirected to Identity Reporting.

2 To verify that Identity Governance denies other authorizations to Identity Reporting, complete the following steps:

- **2a** Log in to Identity Governance, as a Global Administrator or Security Officer.

  `https://`*`myserver.mydomain.com`*`:`*`8443`*

- **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, and log in to Identity Governance and access the reporting features.
  - **Identity Governance:** `https://`*`myserver.mydomain.com`*`:`*`8443`*
  - **Identity Reporting:** `https://`*`myserver.mydomain.com`*`:`*`8443`*`/IDMRPT`
- **2d** Verify you cannot access Identity Reporting.

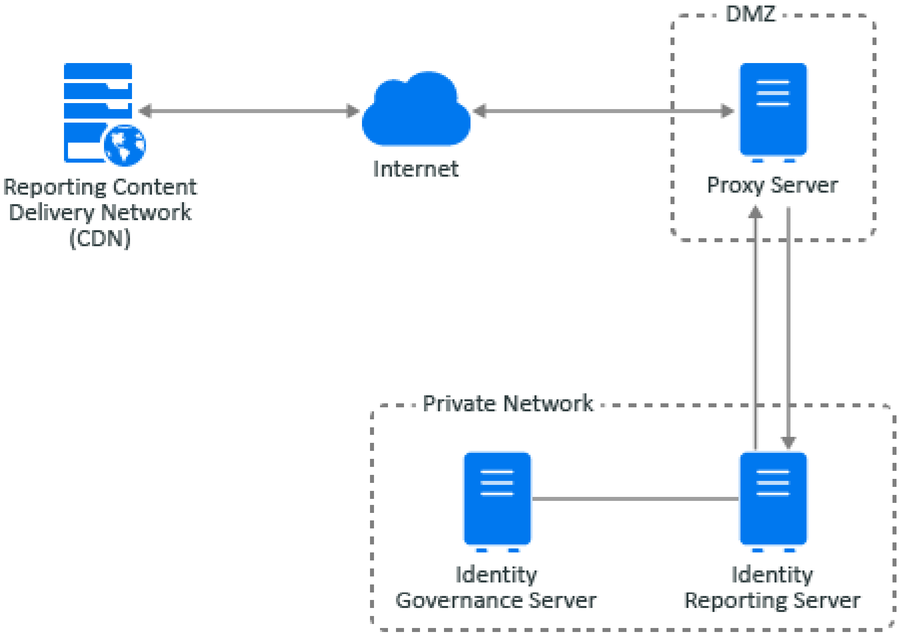
You can also attempt to log in to Identity Reporting by using a Global Administrator or Security Officer account to verify that accounts with high-level privileges cannot access Identity Reporting without the Report Administrator authorization.

9.4.4 Configuring a Proxy Server for the Identity Reporting Server

The server that runs Identity Reporting must have internet access to be able to access and download the most current reports for Identity Governance from the Reporting Content Delivery Network (CDN). For more information, see "Using the Download Page" in the *Identity Governance Reporting Guide*.

If your Identity Reporting server does not have internet access, you must configure a proxy server that can access and download the most current reports for Identity Governance from the Reporting content delivery network (CDN), and is also configured to access and send updated reports to the Identity Reporting server. This configuration allows you to isolate the Identity Reporting server from the internet while ensuring reports are up to date.

***Figure 9-1** Identity Reporting Server Using a Proxy Server*


DMZ
Reporting Content Delivery Network (CDN)
Internet
Proxy Server
Private Network
Identity Governance Server
Identity Reporting Server

You must use the Identity Governance Configuration Update utility to enable the Identity Reporting server to send the request for the Reporting CDN through the proxy server.

To configure the Identity Reporting server to use a proxy server for the updated reports requests:

1 Log in to the Identity Reporting server as an administrator user on a Windows server or as a user with `root` access on a Linux server.

2 From a command prompt, access the Identity Governance Configuration Update utility directory.

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

3 Launch the Identity Governance Configuration Update utility.

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

4 Click the **Reporting** tab.

5 In the lower left corner, click **Show Advanced Options**.

6 Scroll towards the bottom of the page and find the **Outbound Proxy** section.

7 Specify the hostname or IP address, the port, and if you are using SSL or not of the proxy server.

8 Click **OK** to save the changes and the Identity Governance Configuration Update utility automatically closes.

9 Restart Apache Tomcat. For more information, see Section 3.5.3, “Starting and Stopping Apache Tomcat,” on page 50.

9.4.5 Adding Data Sources to Identity Reporting

Identity Reporting runs reports against your connected data sources. Before you can run reports, you need to add one or more data sources.

IMPORTANT: You must add the Identity Governance operations (`igops)` database as a data source in Identity Reporting. The `igops` name is the default name of the operations database.

1 Log in to Identity Reporting as the Report Administrator.

```
https://myserver.mydomain.com:8443/IDMRPT
```

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 Apache Tomcat folders as described in Step 2 on page 212.

You might need to restart Apache Tomcat.

9 Run a test report to verify functionality in Identity Reporting.

For more information about running reports, see “Using the Reports Page” in the *Identity Reporting Guide*.

9.5 Configuring Workflow Engine

You can modify the installation properties after installing the Workflow Engine by running the Identity Governance Configuration Update utility. However, you must restart the application server that hosts the Workflow Engine for the changes to take effect. For more information, see Section 15.1.5, “Using the Identity Governance Configuration Update Utility,” on page 293.

9.5.1 Starting Workflow Engine

To verify installation and to initialize the Workflow Engine database, you must start the application server.

1 Log in to the application server that hosts the Workflow Engine.

2 (Conditional) If this is the first time you are starting the Workflow Engine, 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 cache directory, located by default in `/opt/netiq/idm/apps/tomcat/work/Catalina/localhost`
  - **Windows:** Temporary directory, located by default in:
    - `C:\netiq\idm\apps\tomcat\temp`
    - Catalina cache directory, located by default in: `C:\netiq\idm\apps\tomcat\work\Catalina\localhost`

  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 Apache Tomcat. For more information, see Section 3.5.3, “Starting and Stopping Apache Tomcat,” on page 50.

4 (Optional) To observe the Apache Tomcat initialization process in Linux, 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
```

9.6 Completing the Cluster Configuration for Identity Governance

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

- Section 9.6.1, "Configuring the Nodes in the Apache Tomcat Cluster," on page 217
- Section 9.6.2, "Configuring ActiveMQ Failover in the Apache Tomcat Cluster," on page 218
- Section 9.6.3, "Cleaning Up Unfinished Data Production Jobs," on page 219

9.6.1 Configuring the Nodes in the Apache Tomcat Cluster

To run Identity Governance in an Apache Tomcat cluster, each node in the cluster must have a unique runtime identifier. Also, the Apache 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 Section 2.3.4, "Ensuring High Availability or Load Balancing for Identity Governance," on page 35.

1 Stop Apache Tomcat, if the application server is running. For more information, see Section 3.5.3, "Starting and Stopping Apache Tomcat," on page 50.

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 Apache Tomcat port for the local node.

3d Save and close the file.

4 When you have completed all configuration changes for the cluster, start Apache Tomcat. For more information, Section 3.5.3, "Starting and Stopping Apache Tomcat," on page 50.

9.6.2 Configuring ActiveMQ Failover in the Apache 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.

- **Linux:** Default location in `/opt/netiq/idm/apps/idgov/bin/`
  - **Console mode:** `./configutil.sh -password` *`db_password`* `-storepass` *`encryption_keystore_password`* `-console`
  - **Guided mode:** `./configutil.sh -password` *`db_password`* `-storepass` *`encryption_keystore_password`*
- **Windows:** Default location in `C:\netiq\idm\apps\idgov\bin\`
  - **Console mode:** `configutil.bat -password` *`db_password`* `-console`
  - **Guided mode:** `configutil.bat -password` *`db_password`*

For more information, see Section 15.1.4, "Using the Identity Governance Configuration Utility," on page 290.

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.

9.6.3 Cleaning Up Unfinished Data Production Jobs

When running Identity Governance 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 the health and performance of your system.

Data production jobs are tied to specific runtime instances, identified by their runtime_identitifer. Do not use a host name 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 `igops` 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 perform the following steps:

   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.

10 Configuring Authentication Options for Identity Governance

By default, Identity Governance uses the user name and password as the authentication method for both OSP or Access Manager. You can use any available authentication method provided by OSP, or Access Manager. You can deploy Identity Governance in many different configurations and you can use the different authentication methods that work best for your environment.

The following are use cases for some authentication methods that you can use with Identity Governance. We assume that you have an administrative level of understanding of common authentication methods such as SAML, OAuth2, and so forth. This guide is not a primer for these authentication methods. You must also have administrative level knowledge of the different products that you can integrate with Identity Governance to provide the different authentication methods.

- Section 10.1, “Configuring Identity Governance for Two-Factor Authentication,” on page 221
- Section 10.2, “Configuring Single Sign-on Access with Access Manager,” on page 225
- Section 10.3, “Using SAML Authentications from Access Manager to Provide Single Sign-On to Identity Governance through the OSP,” on page 226
- Section 10.4, “Configuring OSP to Use Kerberos for Single Sign-On,” on page 227
- Section 10.5, “Integrating Single Sign-on Access with Identity Manager Using OSP,” on page 232
- Section 10.6, “Ensuring Rapid Response to Authentication Requests,” on page 237

10.1 Configuring Identity Governance for Two-Factor Authentication

OSP and Access Manager can provide two-factor authentication for the Identity Governance authorized users. Two-factor authentication for OSP requires that you have NetIQ Advanced Authentication. Access Manager can provide two-factor authentication using time-based one-time password (TOTP). Use the following information to configure either OSP or Access Manager for two-factor authentication for the Identity Governance authorized users.

- Section 10.1.1, “Configuring OSP for Two-Factor Authentication,” on page 222
- Section 10.1.2, “Configuring Access Manager for Two-Factor Authentication,” on page 225

10.1.1 Configuring OSP for Two-Factor Authentication

To configure OSP to use two-factor authentication for the Identity Governance authorized users, you must have Advanced Authentication installed and configured in your IT environment. Use the following information to configure OSP for two-factor authentication.

- Section 10.1.1.1, "Prerequisites for Configuring Two-Factor Authentication," on page 222
- Section 10.1.1.2, "Configure the Advanced Authentication Server for Two-Factor Authentication," on page 222
- Section 10.1.1.3, "Using the Identity Governance Configuration Update Utility to Configure OSP for Two-Factor Authentication," on page 223
- Section 10.1.1.4, "Testing the Enrolled Methods," on page 225

10.1.1.1 Prerequisites for Configuring Two-Factor Authentication

Before configuring any servers for two-factor authentication, ensure the following conditions exist:

- ❒ Advanced Authentication is installed and configured
- ❒ The server time where you installed OSP is in synchronization with the Identity Governance servers and the Advanced Authentication servers
- ❒ Each server can correctly resolve the DNS name of the other servers

10.1.1.2 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 OSP 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 (https://www.netiq.com/documentation/advanced-authentication) documentation.

To configure Advanced Authentication for two-factor authentication:

1. Log in to the Advanced Authentication Administration portal using administrator credentials. For more information, see "Logging In to the Advanced Authentication Administration Portal".
2. Create a repository for the LDAP identity service for OSP. For more information, see "Adding an LDAP Repository".
3. (Optional) To change default attributes or collect a new attribute, change the **Advanced Settings**. For more information, see "Advanced Settings".
4. Find the new repository that you just created, then click **Edit > Full synchronization** to synchronize the users and groups from the LDAP server.
5. Define the method for two-factor authentication of **EMail OTP** and **LDAP Password**. For more information, see:
   - "Email OTP"
   - "LDAP Password"

6 Configure the policy for the mail sender for the **Email OTP** method. For more information, see “Mail Sender”.

7 Create a chain to make the authentication methods available for OSP. For more information, see “Creating a Chain”.

8 Create an event to define the type of authentication event you use. You can use an existing event or create a custom event. For more information, see “Configuring Events”.

10.1.1.3 Using the Identity Governance Configuration Update Utility to Configure OSP for Two-Factor Authentication

Ensure that you have created the methods, chain, and events in Advanced Authentication before proceeding. For more information, see Section 10.1.1.2, “Configure the Advanced Authentication Server for Two-Factor Authentication,” on page 222.

To complete the two-factor authentication configuration, you must configure OSP to accept the authentications from Advanced Authentication.

1 Run the Identity Governance Configuration Update utility. For more information, see Section 15.1.5, “Using the Identity Governance Configuration Update Utility,” on page 293.

2 Click the **Authentication** tab, and 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\admin 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 222. This repository corresponds to the LDAP identity service for Identity Governance.

Advanced Authentication Servers

Click **Enter host name or address**, 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**, and specify each DNS name or IP address for each server in the cluster with the corresponding port.

Advanced Authentication Endpoint

An Advanced Authentication endpoint is an identifier and secret that ensures that it is an authorized entity performing authentication with the Advanced Authentication server.

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 Identity Governance Configuration Update utility selects **Create new endpoint**.

You must specify a name and description for the new endpoint for Advanced Authentication. The name and description appear in the **Endpoints** section of the Advanced Authentication Administration portal.

If you have already created an endpoint, and the endpoint information is in the configuration, and Identity Governance can resolve the endpoint data with the Advanced Authentication server, then the Identity Governance Configuration Update utility does not select the **Create new endpoint** option 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 select **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, 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 the Identity Governance Configuration Update utility automatically closes.

10.1.1.4 Testing the Enrolled Methods

After you 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.

10.1.2 Configuring Access Manager for Two-Factor Authentication

Access Manager provides two-factor authentication through the use of time-based one-time password (TOTP) or it provides multi-factor authentication if you have integrated Access Manager with Advanced Authentication. If Access Manager provides the OAuth 2 authentication for the authorized users instead of OSP, there are no additional configuration steps required for two-factor authentication. You would configure Access Manager to provide two-factor or multi-factor authentication for the authorized users. For more information see:

- "Two-Factor Authentication Using Time-Based One-Time Password" in the *NetIQ Access Manager 5.0 Administration Guide*
- *Multi-Factor Authentication Using Advanced Authentication*

10.2 Configuring Single Sign-on Access with Access Manager

If you are using Access Manager as the authentication service for Identity Governance, you can use Access Manager to configure the products in your IT environment to provide a single sign-on experience for the users using Identity Governance or any other product you have installed. One of the features of Access Manager is that it contains a single sign-on solution.

To provide single sign-on to Identity Governance you must configure Identity Governance as a trusted provider in Access Manager. If you are running Identity Governance and Identity Manager, you can configure both products to be trusted providers in Access Manager and any time an authorized user accesses Identity Governance, Identity Reporting, Workflow Engine or any identity applications, they have a single sign-on experience. For more information, see "Configuring Trusted Providers for Single Sign-On" in the *NetIQ Access Manager 5.0 Administration Guide*.

10.3 Using SAML Authentications from Access Manager to Provide Single Sign-On to Identity Governance through the OSP

If you are using OSP with Identity Governance and you have Access Manager installed and configured to provide SAML authentications to other applications, you can allow the SAML authentications from Access Manager to provide single sign-on through OSP to Identity Governance.

1 Obtain the SAML 2.0 metadata from the Access Manager server by accessing the following default URL:

```
https://identity-server-dns-name:port/nidp/saml2/metadata
```

2 Configure the SAML 2.0 settings on the OSP server.

2a Ensure that Apache Tomcat is running on the OSP server.

2b Launch the Identity Governance Configuration Update utility from the OSP server. For more information, see Section 15.1.5, "Using the Identity Governance Configuration Update Utility," on page 293.

2c Click the **Authentication** tab.

2d Click **Show Advanced Options**.

2e Under **Authentication Method > Method** select **SAML 2.0**.

2f Use the following information to configure OSP to use SAML 2.0:

Mapping Attribute

Specify the attribute listed is the one you want to use to map the user accounts to Access Manager. The default value is `mail`.

Landing Page

Select where the landing page for your users is internal, external, or if there is not one. The default value is **None**.

Metadata source

Select **URL** to use the Access Manager metadata.

Metadata URL:

Specify the Access Manager metadata URL in this field.

```
https://identity-server-dns-name:port/nidp/saml2/metadata
```

Load on save

Select this option to load the metadata.

Configure Access Manager on exit

Select this option to automatically configure Access Manager when you exit the Identity Governance Configuration Update utility.

2g Under the Identity Governance Bootstrap Administrator heading, ensure that you are using an LDAP-based bootstrap administrator account. For more information, see Section 4.1.1, "Using the Bootstrap Administrator," on page 58.

2h Click **OK** to save the changes.

2i Click **Yes** to accept the certificate.

2j When the Access Manager Auto-Configuration appears, restart Apache Tomcat on the OSP server. For more information, see Section 3.5.3, "Starting and Stopping Apache Tomcat," on page 50.

3 Automatically configure the SAML 2.0 settings in Access Manager for OSP.

3a Access the Administration Console for Access Manager using the full DNS name. For example:

```
https://mybusiness.com:8443
```

3b In **Access Manager Administrator Credentials**, specify the user name and password of the Access Manager administrator in LDAP format. For example, `cn=admin,o=mybusiness`.

3c Ensure that the **Unique Display Name** is automatically created as `IDM-NAM Trust`.

3d In **Authentication Server Administrator Credentials**, specify the user name and password of the Identity Governance configuration administrator.

3e Click **OK** to save the configuration information.

3f In the pop-up window, click **Yes** to update the Access Manager configuration.

3g Read the Access Manager SAML 2 configuration summary when it appears, then click **OK**.

4 Restart Apache Tomcat on the OSP server. For more information, see Section 3.5.3, "Starting and Stopping Apache Tomcat," on page 50.

5 (Conditional) If you configured OSP to utilize multiple keypairs, you might have to import the OSP encryption certificate into the NIPD Trust Store in Access Manager.

5a Obtain a copy of the OSP encryption certificate from:

```
https://osp-server:port/osp/s/idm/encryptionCertificate
```

5b Add the encryption certificate to the NIDP Trust Store in Access Manager. For more information, see "Managing Trusted Roots and Trust Stores" in the *NetIQ Access Manager 5.0 Administration Guide*.

10.4 Configuring OSP to Use Kerberos for Single Sign-On

You can use Kerberos as an authentication method for the identity applications that allow SSO. This also allows users to use Integrated Windows Authentication to log in to the applications. This section provides instructions for configuring Active Directory to use Kerberos for connecting to the identity applications:

- Section 10.4.1, "Configuring the Kerberos User Account in Active Directory," on page 227
- Section 10.4.2, "Configuring the Servers for Identity Governance and its Components," on page 229
- Section 10.4.3, "Configure Browsers to Use Integrated Windows Authentication," on page 231

10.4.1 Configuring the Kerberos User Account in Active Directory

Use the Active Directory administration tools to configure Active Directory for Kerberos authentication. You need to create a new Active Directory user account for Identity Governance, Identity Reporting, and Workflow Engine. If Identity Governance, Identity Reporting or Workflow

Engine are not on the same server, you must create three accounts. The user account name must use the DNS name of the server that hosts Identity Governance or Identity Reporting or Workflow Engine.

NOTE: For domain or realm references, use uppercase format. For example `@MYCOMPANY.COM`.

1 As an Active Directory administrator, use the Microsoft Management Console (MMC) to create a new user account with the DNS name of the server that hosts Identity Governance or Identity Reporting.

For example, if the DNS name of the server is `idgov.mycompany.com`, use the following information to create the user:

First name: idgov

User login name: HTTP/idgov.mycompany.com

Pre-windows logon name: idgov

Set password: Specify the appropriate password. For example: `Passw0rd`.

Password never expires: Select this option.

User must change password at next logon: Do not select this option.

2 Associate the new user with the Service Principal Name (SPN).

2a In the Active Directory server, open a cmd shell.

2b At the command prompt, enter the following:

```
setspn -A HTTP/DNS_Identity_Governance_server@WINDOWS-DOMAIN userID
```

For example:

```
setspn -A HTTP/idgov.mycompany.com@MYCOMPANY.COM idgov
```

2c Verify setspn by entering `setspn -L` *`userID`*.

3 To generate the `keytab` file, use the `ktpass` utility:

3a At the command line prompt, enter the following:

```
ktpass /out filename.keytab /princ servicePrincipalName /mapuser
userPrincipalName /mapop set /pass password /crypto ALL /ptype
KRB5_NT_PRINCIPAL
```

For example:

```
ktpass /out idgov.keytab /princ HTTP/identity-
governance.mycompany.com@MYCOMPANY.COM /mapuser idgov  /mapop set /pass
Passw0rd /crypto All /ptype KRB5_NT_PRINCIPAL
```

IMPORTANT: For domain or realm references, use uppercase format. For example, `@MYCOMPANY.COM`.

3b Copy the `rbpm.keytab` file to your Identity Governance server.

4 An an Administrator in Active Directory, create an end user account with the MCC to prepare for SSO.

The end user account name must match some attribute value of an eDirectory user to support single sign-on. Create the user with some name such as cnano, remember the password, and ensure that **User must change password at next logon** is not selected.

5 (Optional) Repeat these steps for Identity Reporting if you installed the reporting component on a separate server.

6 (Optional) Repeat these steps for Workflow Engine if you installed it on a separate server.

7 Configure the server for Identity Governance, Identity Reporting, or the server for Workflow Engine to accept the Kerberos configuration by proceeding to Section 10.4.2, "Configuring the Servers for Identity Governance and its Components," on page 229.

10.4.2 Configuring the Servers for Identity Governance and its Components

You must configure your Identity Governance, Identity Reporting, and the Workflow Engine servers to use the Kerberos keytab file and the user account that you created in Active Directory. Ensure that you complete Section 10.4.1, "Configuring the Kerberos User Account in Active Directory," on page 227 before proceeding.

NOTE: For domain or realm references, use uppercase format. For example @MYCOMPANY.COM.

IMPORTANT: JDK 11.0.21 is the minimum required version for Identity Governance. With JDK 11, Oracle has made changes to Kerberos encryption types. Adjust your configuration as needed based on "Deprecate 3DES and RC4 in Kerberos (JDK-8139348) (https://www.oracle.com/java/technologies/javase/11-0-17-relnotes.html)" section in the *JDK 11.0.17 Release Notes*.

1 To define your operating system settings for the Kerberos configuration, complete the following steps:

1a Open the krb5 file in a text editor on the Identity Governance server.

Linux: /etc/krb5.conf

Windows: C:\Windows\krb5.ini

1b Add the following information to the krb5 file:

```
[libdefaults]
    default_realm = WINDOWS-DOMAIN
    kdc_timesync = 0
    forwardable = true
    proxiable = false
[realms]
    WINDOWS-DOMAIN = {
         kdc = FQDN Active Directory Server
         admin_server = FQDN Active Directory Server
    }
[domain_realm]
    .your.domain = WINDOWS-DOMAIN
    your.domain = WINDOWS-DOMAIN
```

For example:

```
[libdefaults]
    default_realm = MYCOMPANY.COM
    kdc_timesync = 0
    forwardable = true
    proxiable = false
[realms]
    MYCOMPANY.COM = {
         kdc = myadserver.mycompany.com
         admin_server = myadserver.mycompany.com
    }
[domain_realm]
    .mycompany.com = MYCOMPANY.COM
    mycompany.com = MYCOMPANY.COM
```

1c Save the changes and close the `krb5` file.

2 To define the Kerberos configuration information for Apache Tomcat, complete the following steps:

2a Create a sample `Kerberos_login.config` file on the Identity Governance server where the Apache Tomcat instance is running with the following content:

NOTE: The novlua user needs permissions to create the `Kerberos_login.config` file.

```
com.sun.security.jgss.krb5.accept {
        com.sun.security.auth.module.Krb5LoginModule required
    debug="true"
        refreshKrb5Config="true"
    useTicketCache="true"
        ticketCache="/opt/netiq/idm/apps/tomcat/kerberos/
spnegoTicket.cache"
    doNotPrompt="true"
        principal="HTTP/DNS_Identity_Governance_server@WINDOWS-
DOMAIN"
    useKeyTab="true"
        keyTab="/absolute_path/filename.keytab"
    storeKey="true";
    };
```

An example on a Windows server is as follows:

```
keyTab="c:\\NetIQ\\IdentityGoverance\\apps\\tomcat\\kerberos\\rbpm.
keytab"
```

2b In the file, specify values for `principal` and `keyTab`. For example:

```
principal="HTTP/idgov.mycompany.com@MYCOMPANY.COM"
keyTab="/home/usr/rbpm.keytab"
```

- The value for `principal` must match the same value that you specified for Kerberos. For more information, see Step 3 on page 228.
- Provide the absolute path of the `keytab` file on your Identity Governance server. The file does not have to reside in the default directory for Identity Governance.

2c Refer to the `Kerberos_login.config` file in JVM `java.security` file with the following line:

```
login.config.url.1=file:/opt/netiq/idm/apps/tomcat/kerberos/
Kerberos_login.config
```

The path listed is the default installation location for a Linux server.

An example of the `java.security` file on a Windows server is as follows:

```
login.config.url.1=file:c:/NetIQ/IdentityManager/apps/tomcat/
kerberos/Kerberos_login.config
```

3 To specify the authentication method in the Identity Governance Configuration utility, complete the following steps:

3a Launch the Identity Governance Configuration Update utility on the Identity Governance server. For more information, see Section 15.1.5, “Using the Identity Governance Configuration Update Utility,” on page 293.

3b Click the **Authentication** tab.

3c At the end of the page, click **Show Advanced Options**.

3d Under **Authentication Method > Method** select **Kerberos**.

3e In the **Mapping attribute name** field, specify `cn`.

3f Select any of the following options that apply to your environment:

- **Enable fallback reCAPTCHA** and provided the additional required information. For more information, see Section 9.2.4, “Configuring OSP to Use Google reCAPTCHA,” on page 208.
- **Enable fallback two-factor authentication**
- **Use logout landing page**

3g Click **OK** to save the changes.

3h Restart Apache Tomcat. For more information, see Section 3.5.3, “Starting and Stopping Apache Tomcat,” on page 50.

4 (Optional) Repeat these steps for Identity Reporting if you installed it on a separate server.

5 (Optional) Repeat these steps for Workflow Engine if you installed it on a separate server.

6 Configure the browsers that end-users use to access the identity applications. For more information, see Section 10.4.3, “Configure Browsers to Use Integrated Windows Authentication,” on page 231.

10.4.3 Configure Browsers to Use Integrated Windows Authentication

The browsers used to access Identity Governance, Identity Reporting, and Workflow Engine also need to be configured for Integrated Windows Authentication. This section provides instructions for configuring an end-user computer to support single sign-on access using Integrated Windows Authentication.

NOTE: You must perform this procedure for each end-user computer where you want to provide single sign-on access to Identity Governance, Identity Reporting and Workflow Engine.

1 Log in to the computer where users need single sign-on access.

2 Open the Internet options control panel.

3. Click **Security**.
4. Click **Trusted Sites** > **Sites**.
5. Add the DNS name of the Identity Governance, Identity Reporting, and Workflow Engine server.

   For example: `idgov.mycompany.com`
6. Click **Add**, then click **Close**.
7. Click **Custom level...**.
8. Under **User Authentication**, select **Automatic logon with current user name and password**.
9. Click **OK**.
10. In Internet Options, click **Advanced**.
11. Under Security, select **Enable Integrated Windows Authentication**.
12. Repeat this procedure for each end-user computer where you want to provide single sign-on access to Identity Governance, Identity Reporting., and Workflow Engine.

10.5 Integrating Single Sign-on Access with Identity Manager Using OSP

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. These products use 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 identity service that the identity applications use.

- Section 10.5.1, “Checklist for Integrating Identity Governance with Identity Manager,” on page 232
- Section 10.5.2, “Configuring Identity Governance for Integration with Identity Manager,” on page 233
- Section 10.5.3, “Configuring Identity Manager for Integration with Identity Governance,” on page 235

10.5.1 Checklist for Integrating Identity Governance with Identity Manager

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

	Checklist Items
❑	1. To ensure that you have the correct software versions for integration, review the 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/).

	Checklist Items
❑	2. (Conditional) Create an index in eDirectory for the login attribute if you do not use a standard login attribute. For more information, see Section 10.6, “Ensuring Rapid Response to Authentication Requests,” on page 237.
❑	3. Ensure that users can link to Identity Manager Home from Identity Governance. For more information, see Section 10.5.2.1, “Adding a Link to Identity Manager Home in the Identity Governance Menu,” on page 234.
❑	4. Ensure that Identity Governance connects to the Identity Vault for Identity Manager. For more information, see Section 10.5.2.2, “Changing Identity Governance to Use the Identity Manager Identity Vault as the Identity Service,” on page 234.
❑	5. (Conditional) If your identity service is a separate eDirectory or Active Directory from the Identity Manager Identity Vault, you must manually extend the schema for the OSP authentications to work. For more information, see Section 9.2.2, “Extending the Schema for OSP in the Identity Service not Part of Identity Manager,” on page 205.
❑	6. (Conditional) If you are using the OSP that comes with Identity Manager, ensure that you are using the LDAP-based instead of the file-based bootstrap administrator account. For more information, see Section 4.1.1, “Using the Bootstrap Administrator,” on page 58.
❑	7. Update Identity Manager Home to connect to Identity Governance. For more information, see Section 10.5.3, “Configuring Identity Manager for Integration with Identity Governance,” on page 235.
❑	8. (Optional) Integrate Identity Governance with the workflows used in Identity Manager. For more information, see “Workflows to Fulfill the Changesets (https://www.microfocus.com/documentation/identity-governance/4.3/user-guide/fulfill-changesets.html#fulfill-changeset-workflow)” and “Configuring Fulfillment (https://www.microfocus.com/documentation/identity-governance/4.3/user-guide/configure-fulfillment.html)” in the *Identity Governance User and Administration Guide*.

For more information about Identity Manager, see the *NetIQ Identity Manager Overview and Planning Guide*.

10.5.2 Configuring Identity Governance for Integration with Identity Manager

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 identity service that the identity applications use to verify login attempts. This process includes the following activities:

- Section 10.5.2.1, “Adding a Link to Identity Manager Home in the Identity Governance Menu,” on page 234
- Section 10.5.2.2, “Changing Identity Governance to Use the Identity Manager Identity Vault as the Identity Service,” on page 234

10.5.2.1 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 **Configuration > 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.

10.5.2.2 Changing Identity Governance to Use the Identity Manager Identity Vault as the Identity Service

This section describes how to configure Identity Governance to use the Identity Manager Identity Vault as the Identity Governance identity service for verifying users who log in to Identity Governance. This section assumes that, when you installed Identity Governance, you did not specify the Identity Manager Identity Vault and that you specified a different identity service. For example, you might have installed Identity Governance before adding Identity Manager to your environment.

NOTE: Identity Applications use `https` communication by default. You create a wildcard certificate on one of the servers and copy the certificate on all the servers. For example, you create the wildcard certificate `*.example.com` on the OSP server.

1. Add this certificate to the `keystoreFile` on all the servers.
2. Restart Apache Tomcat on all the servers.
3. Ensure that `keystoreFile` is updated in the `server.xml`.

```
 <Connector port="8543"
protocol="org.apache.coyote.http11.Http11NioProtocol" maxThreads="150"
SSLEnabled="true" scheme="https" secure="true" clientAuth="false"
sslProtocol="TLSv1.2" keystoreFile="conf/tomcat.ks"
keystorePass="novell" sslEnabledProtocols="TLSv1.2" />
```

1. Stop Identity Governance and Apache Tomcat. For more information, see Section 3.5.3, “Starting and Stopping Apache Tomcat,” on page 50.
2. Launch the Identity Governance Configuration utility. For more information, see Section 15.1.4, “Using the Identity Governance Configuration Utility,” on page 290.
3. Click the **Authentication Server Details** tab.
4. Deselect **Same as IG Server**.

5 Specify the protocol, DNS host name or IP address, and port that represent the Identity Vault for Identity Manager identity applications.

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

6 Click **Save**.

7 Make a note of the settings for the Identity Vault.

The values for these settings must match the settings that you specify for Identity Governance in the RBPM Configuration utility. For more information, see Section 10.5.3, "Configuring Identity Manager for Integration with Identity Governance," on page 235.

8 Click the **Security Settings** tab, then 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 Section 10.5.3, "Configuring Identity Manager for Integration with Identity Governance," on page 235.

9 Close the utility.

10 Start Apache Tomcat to start Identity Governance. For more information, see Section 3.5.3, "Starting and Stopping Apache Tomcat," on page 50.

10.5.3 Configuring Identity Manager for Integration with Identity Governance

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.

1 Ensure that you have configured single sign-on for the Identity Manager identity applications. For more information, see "Preparing for Single Sign-on Access" in the *NetIQ Identity Manager - Administrator's Guide to the Identity Applications*.

2 (Conditional) If you are using the OSP that comes with Identity Manager, ensure that you are using the LDAP-based instead of the file-based bootstrap administrator account. For more information, see Section 4.1.1, "Using the Bootstrap Administrator," on page 58.

3 (Conditional) If you are running Identity Manager 4.8 or 4.9, ensure that the **IG SSO** tab appears in the Configuration Update utility for the identity applications.

3a Ensure that the Configuration Update utility is not running.

3b Find the properties file for the Configuration Update utility for the identity applications. The default location is:

- **Linux:** `/opt/netiq/idm/apps/UserApplication/configupdate.sh.properties`
- **Windows:**

  `c:\netiq\idm\apps\UserApplication\configudate.bat.properties`

3c Open the properties file in a text editor.

3d If the line `sso_apps=` exists, ensure that it lists the User Application, Identity Reporting, and Identity Governance. For example:

```
sso_apps=ua,rpt,ig
```

3e If the `sso_apps=` line does not exist, add it to file listing the User Application, Identity Reporting, and Identity Governance. For example:

```
sso_apps=ua,rpt,ig
```

3f Save and close the file.

4 Configure the single sign-on settings in the Configuration Update utility for the identity applications server.

4a Launch the Configuration Update utility for the identity applications server.

4b In the Configuration Update utility, click the **IG SSO Client** tab.

4c Specify the values based on the **OAuth SSO Client** and **Security Settings > General Service** settings that you observed in Step 7 through Step 8 in Section 10.5.2.2, “Changing Identity Governance to Use the Identity Manager Identity Vault as the Identity Service,” on page 234.

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.

4d Save your changes and close the Configuration Update utility for the identity applications server.

5 Before restarting Apache Tomcat, delete the contents of the following two directories from Apache Tomcat that contain cached files. The directories are:

- **Linux:** Default installation location:
  - `/opt/netiq/idm/apps/tomcat/temp`
  - `/opt/netiq/idm/apps/tomcat/work/Catalina/localhost`
- **Windows:** Default installation location:
  - `c:\netiq\idm\apps\tomcat\temp`
  - `c:\netiq\idm\apps\tomcat\work\Catalina\localhost`

6 Restart Tomcat on the Identity Manager application server.

- Linux:

  From the Linux command line, type: `systemctl restart netiq-tomcat.service`.
- Windows:
  1. Open the Services window (`C:\Windows\system32\services.msc`).
  2. Select **IDM Apps Tomcat Service**.
  3. Click **Restart**.

7 Add a link to Identity Governance on the Identity Manager Home page. For more information, see “Setting Up the Dashboard for Identity Applications” in the *NetIQ Identity Manager - Administrator’s Guide to the Identity Applications*.

8 On the Identity Governance server, start Identity Governance (and Apache Tomcat). For more information, see Section 3.5.3, “Starting and Stopping Apache Tomcat,” on page 50.

10.6 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 identity service. 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 identity service 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 “Configuring Identity Applications” in the *NetIQ Identity Manager Setup Guide for Linux*.

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

For more information, see “Authentication Parameters” 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.

11 Customizing Your Installation

Identity Governance allows you to customize the Identity Governance web application to provide the appropriate experience for authorized users. You can change the preferred language for your users, you can customize the web application, and translate content for Identity Governance and OSP.

Similarly, you can customize the appearance of the Workflow Administration Console by modifying the cascading style sheet. Use the default NetIQ template while customizing.

If you use Access Manager as your authentication service, the users access and log in through the Access Manager log in pages, not the Identity Governance application. None of the following information applies if you use Access Manager as your authentication service. Access Manager allows you to customize their pages. For more information, see “Identity Server Advanced Configuration” in the *NetIQ Access Manager 5.0 Administration Guide*.

Use the following information to customize your environment.

- Section 11.1, “Customizing the Name in the Identity Governance Application,” on page 239
- Section 11.2, “Localizing the Preferred Language of the User,” on page 240
- Section 11.3, “Customizing the User Interface,” on page 241
- Section 11.4, “Translation Content for Identity Governance and One SSO Provider,” on page 245
- Section 11.5, “Customizing the Identity Governance Style Sheet,” on page 250
- Section 11.6, “Customizing the Workflow Administration Console,” on page 251

11.1 Customizing the Name in the Identity Governance Application

You can change the name that the authorized users see when they access the Identity Governance application through a web browser. You can change the name during the installation of Identity Governance or you can change it after the installation using the Identity Governance Configuration utility.

You can also change the product name in the user interface. For more information about customizing the product name and header using the user interface, see “Customizing and Configuring Identity Governance for Your Enterprise” in the *NetIQ Identity Governance Administration and User Guide*.

To customize the name in the application using the Configuration Utility:

1 Access the installation directory for the utility from a command prompt as a user with `root` access on a Linux server or administrative privileges on a Windows server. The default installation directory is:

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

2 From the command line, enter:

   - **Linux:** `./configutil.sh -password` *`db_password`* `-storepass` *`encryption_keystore_password`*
   - **Windows:** `configutil.bat -password` *`database_password`*

3 Click the **IG Server Details** tab.

4 In the **Product Name** field, add the name you want to appear.

5 Click **Save** to save the changes.

11.2 Localizing the Preferred Language of the User

Identity Governance displays content in the user interface based on the browser language setting but localizes emails according to the collected preferred language of the user. For example, when the preferred language is set to Spanish (es), a Spanish email template is available, and the browser language is set to English, the user interface of Identity Governance is rendered in English and all emails are in Spanish.

If the preferred language value is not collected or if the preferred language is not supported, then the email is delivered in the default language of Identity Governance.

Be aware that Identity Governance cannot always reconcile the differences in language that occur when different users collect data and run reports on the 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.

The following is a list of the languages Identity Governance localizes:

- Chinese Simplified
- Chinese Traditional
- Czech
- Danish
- Dutch
- English
- French
- German
- Hebrew
- Italian
- Japanese
- Norwegian
- Polish
- Portuguese
- Russian

- Spanish
- Swedish

You can customize the content in the provided languages. Alternatively, you can apply a new language to Identity Governance and OSP.

11.3 Customizing the User Interface

Identity Governance and OSP automatically display content in the user interface according to your browser 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.

- Section 11.3.1, "Customizing the Labels in the Identity Governance Interface," on page 241
- Section 11.3.2, "Customizing Strings in the Properties Files," on page 242

For more information about translating the content to a new language instead of customizing it, see Section 11.4.1, "Preparing Files for Translation," on page 246.

11.3.1 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 **Configuration > 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 could need to sign out of Identity Governance, clear the cache in the browser, and then log in again.

11.3.2 Customizing Strings in the 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.

11.3.2.1 Customizing Strings for the Configuration Utility

If you want to use different terminology in the Identity Governance Configuration utility, you can do so by editing `.properties` files.

To customize strings for the Configuration utility:

1 Log in to the server where you installed Identity Governance.

2 Navigate to the `/opt/netiq/idm/apps/idgov/localization` directory.

3 Copy the `iac-configutil-strings.jar` to a temporary directory.

For example: `opt/netiq/idm/apps/work`

4 Extract the `iac-configutil-strings.jar`, making sure to maintain folder structure.

For example: `/opt/netiq/idm/apps/work/com/netiq/iac/config/util/`

5 Navigate to the `com/netiq/iac/config/util` directory.

6 Perform the following steps to create a new `.properties` file:

6a Rename the existing `IacConfigUIstringsRsrc_en.properties` file to `org-IacConfigUIstringsRsrc_en.properties`.

6b Create a new, empty `IacConfigUIstringsRsrc_en.properties` file.

7 Perform the following steps to modify specific strings:

7a Use a text editor to open the `org-IacConfigUIstringsRsrc_en.properties` file.

7b Find the properties that you want to modify.

For example, the labels **Bootstrap Admin** and **Bootstrap File Details**, which appear on the **Authentication Server Details** tab in the Configuration utility:

```
FILE_DETAILS_TITLE=Bootstrap File Details
```

```
BOOTSTRAP_ADMIN_TITLE=Bootstrap Admin
```

7c Copy the properties into the empty `IacConfigUIstringsRsrc_en.properties` file.

7d Modify the string values, which appear after the equal sign.

For example:

```
FILE_DETAILS_TITLE=Default Admin File Details
BOOTSTRAP_ADMIN_TITLE=Default Admin
```

7e Save and close the file.

8 (Optional) Repeat Step 6 through Step 7 for each language you want to modify.

9 Navigate to the folder from which you extracted the `iac-configutil-strings.jar` file.

For example: `/opt/netiq/idm/apps/work`

10 Create a custom `.jar` file that contains only the `.properties` files you modified.

For example: `jar -cMf my-configutil-strings.jar com/netiq/iac/config/util/IacConfigUIstringsRsrc_en.properties`

11 Copy the custom `.jar` file to the `/opt/netiq/idm/apps/idgov/lib` directory.

NOTE: Be sure to set the correct permissions and ownership of the `.jar` file.

12 Navigate to the `/opt/netiq/idm/apps/idgov/bin` directory, and perform the following steps:

12a Use a text editor to open the `configutil.sh` file.

12b Scroll to the bottom of the file, then add the custom `.jar` file you created in Step 10 to the `-cp` section.

For example: `-cp "${app_home}/lib/ig-configutil.jar":"${app_home}/lib/${_db_jdbc_jar}":"${app_home}/lib/my-configutil-strings.jar"`

12c Save and close the file.

13 Launch the Configuration utility in GUI mode to view the changes.

11.3.2.2 Customizing Strings for Identity Governance

If you want to use different terminology in Identity Governance and Access Request, you can do so by editing `.properties` files.

To customize strings for Identity Governance and Access Request:

1 Log in to the server where you installed Identity Governance.

2 Navigate to the `/opt/netiq/idm/apps/idgov/localization` directory.

3 Copy the `client-strings.jar` file and the `cx-client-strings.jar` file to a temporary directory.

For example: `/opt/netiq/idm/apps/work`

4 Extract the `client-strings.jar` file and the `cx-client-strings.jar` file, making sure to maintain folder structure.

For example:

`/opt/netiq/idm/apps/work/com/netiq/iac/client` and

`/opt/netiq/idm/apps/work/com/netiq/cx/client/`

5 Navigate to the `/com/netiq/iac/client` directory.

6 Perform the following steps to create a new `.properties` file for Identity Governance:

6a Rename the `ArRsrc_en.properties` file to `org-ArRsrc_en.properties`.

6b Create a new, empty file named `ArRsrc_en.properties`.

7 Perform the following steps to modify specific strings:

7a Use a text editor to open the `org-ArRsrc_en.properties` file.

7b Find the properties that you want to modify.

For example, the **Legend** and **About** labels that appear when you click your user name in the title bar:

```
legend=Legend
```

```
about=About
```

7c Copy the properties you want to modify into the empty `ArRsrc_en.properties` file.

7d Modify the string values, which appear after the equal sign.

For example:

```
legend=Key
```

```
about=Info
```

7e Save and close the file.

8 (Optional) Repeat Step 6 through Step 7 for each language you want to modify.

9 Navigate to the `/com/netiq/cx/client` directory.

10 Perform the following steps to create a new `.properties` file for Access Request:

10a Rename the `CxRsrc_en.properties` file to `org-CxRsrc_en.properties`.

10b Create a new, empty `CxRsrc_en.properties` file.

11 Perform the following steps to modify specific strings:

11a Use a text editor to open the `org-CxRsrc_en.properties` file.

11b Find the properties that you want to modify.

For example, the **Legend** and **About** labels that appear when you click your user name in the title bar:

```
legend=Legend
```

```
about=About
```

11c Copy the properties into the empty `CxRsrc_en.properties` file.

11d Modify the string values, which appear after the equal sign.

For example:

```
legend=Key
```

```
about=Info
```

11e Save and close the file.

12 (Optional) Repeat Step 10 through Step 11 for each language for which you want to modify strings.

13 Navigate to the folder from which you extracted the `.jar` files.

For example: `/opt/netiq/idm/apps/work`

14 Create a custom `.jar` file that contains only the `.properties` files you modified.

For example: `jar -cMf my-ui-strings.jar com/netiq/iac/client/ArRsrc_en.properties com/netiq/cx/client/CxRsrc_en.properties`

15 Copy the custom `.jar` file to the `tomcat/lib` directory.

For example: `/opt/netiq/idm/apps/tomcat/lib`

NOTE: Be sure to set the correct permissions and ownership of the `.jar` file.

16 Stop Apache Tomcat. For more information, see Section 3.5.3, “Starting and Stopping Apache Tomcat,” on page 50.

17 Delete all files and folders in the following temporary directories:

```
/opt/netiq/idm/apps/tomcat/temp
/opt/netiq/idm/apps/tomcat/work/Catalina/localhost
```

18 Delete all log files from the logs directory for Apache Tomcat.

```
/opt/netiq/idm/apps/tomcat/logs
```

19 Start Apache Tomcat. For more information, see Section 3.5.3, “Starting and Stopping Apache Tomcat,” on page 50.

If you want to verify your changes, clear your browser cache, then log in to Identity Governance and view the pages that should contain your changes.

For example, to verify changes for the examples used in the procedure:

1. Log in to Identity Governance as a user who can access both Identity Governance and Access Request.
2. Within Governance Administration, select your name in the Navigation to view the changes.
3. Within Access Request, select your name in the Navigation to view the changes.

11.4 Translation Content for Identity Governance and One SSO Provider

If the default languages for Identity Governance and OSP do not meet the needs of your organization, 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.

- Section 11.4.1, “Preparing Files for Translation,” on page 246
- Section 11.4.2, “Ensuring that Identity Governance Recognizes the New Language,” on page 247
- Section 11.4.3, “Adding the Translated Labels to the Identity Governance Interface,” on page 248
- Section 11.4.4, “Adding Translated Content to Identity Governance and OSP,” on page 248
- Section 11.4.5, “Verifying the New Translations,” on page 249

For more information about customizing the content for a current new language instead of adding a language, see Section 11.3.1, “Customizing the Labels in the Identity Governance Interface,” on page 241.

11.4.1 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 Section 11.3.1, "Customizing the Labels in the Identity Governance Interface," on page 241.

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.

11.4.2 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:** `./configutil.sh -password` *`db_password`* `-storepass` *`encryption_keystore_password`* `-console`
     - **Guided mode:** `./configutil.sh -password` *`db_password`* `-storepass` *`encryption_keystore_password`*
   - **Windows:** Enter the following command:
     - **Console mode:** `configutil.bat -password` *`db_password`* `-storepass` *`encryption_keystore_password`* `-console`

- **Guided mode:** `configutil.bat -password` *`db_password`* `-storepass` *`encryption_keystore_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 and `it|ru` for Italian or Russian.
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.

11.4.3 Adding the Translated Labels to the Identity Governance Interface

1. Complete the steps in Section 11.4.2, "Ensuring that Identity Governance Recognizes the New Language," on page 247.
2. Log in to Identity Governance as a Global Administrator.
3. Select **Configuration > 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.

11.4.4 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 Apache 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 Section 11.4.2, "Ensuring that Identity Governance Recognizes the New Language," on page 247 before starting this procedure.

1. Navigate to the temporary directory where you had copied the original `.jar` files in Step 2b on page 246.
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 Apache Tomcat.

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

7 Stop Apache Tomcat. For more information, see Section 3.5.3, "Starting and Stopping Apache Tomcat," on page 50.

8 Delete all files and folders in the following Apache 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 Apache Tomcat `logs` directory.

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

10 Start Apache Tomcat. For more information, see Section 3.5.3, "Starting and Stopping Apache Tomcat," on page 50.

11 Before logging in to Identity Governance, clear the browser cache to ensure that the browser displays your new language.

11.4.5 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.

11.5 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 Apache Tomcat server administrator to the Apache Tomcat server that hosts Identity Governance.

2 In the home directory of the Apache Tomcat server administrator, create a directory named `netiq_custom_css`. For example:

   - **Linux:** `/opt/netiq/idm/apps/novlua/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) 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 `QueryOpen`
   - 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 Restart Tomcat.

6 Edit the `custom.css` file to include your branding and other custom style settings that you want Identity Governance to use.

7 (Conditional) To use custom images, add the images to the `netiq_custom_css` directory.

8 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 Apache Tomcat server to see the changes added to the `custom.css` file. Changes to the `custom.css` file are reflected without a restart. Restart is required only after creating the directory, creating the `custom.css` file, or adding images to the directory.

11.6 Customizing the Workflow Administration Console

The customization is done through a file called `custom.css` which is located in the directory `netiq_custom_css`, within the home directory of the user who started the Tomcat on the server. By default, this user is novlua.

1 Log in as the Apache Tomcat server administrator to the Apache Tomcat server that hosts the Workflow Engine.

2 In the home directory of the Apache Tomcat server administrator, create a directory named `netiq_custom_css`:

- **Linux:** `/opt/netiq/idm/apps/novlua/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) 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 `QueryOpen`
- 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 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 the Workflow Administration Console.

You might need to refresh the page in the browser. You do not need to restart the Apache Tomcat server.

12 Adding Features after the Installation

After you install Identity Governance, you may find you need features you did not enable during the installation. Identity Governance allows you to add these features without reinstalling Identity Governance or running the installers again.

12.1 Configuring SSL/TLS Communication after the Installation

If you did not configure OSP, Identity Governance, Identity Reporting, or the Workflow Engine to communicate over TLS/SSL to the external components, you can do so using the Identity Governance Configuration utility.

To configure secure communication after the installation:

1. Stop Identity Governance (and Apache Tomcat). For more information, see Section 3.5.3, “Starting and Stopping Apache Tomcat,” on page 50.
2. Run the Identity Governance Configuration utility. For more information, see Section 15.1.4, “Using the Identity Governance Configuration Utility,” on page 290.
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 identity service support TLS/SSL communication.
6. Start Identity Governance (and Apache Tomcat). For more information, see Section 3.5.3, “Starting and Stopping Apache Tomcat,” on page 50.

12.2 Manually Generating the Database Schema after the Installation

You can recreate the databases after installation without having to reinstall. The following steps apply to Identity Governance, Identity Reporting, and Workflow. Identity Governance and Identity Reporting provide a database initialization script that clears the checksums before initializing the databases for Identity Governance and Identity Reporting. Each script contains variables for the JRE path and the installation path for either Identity Governance or Identity Reporting, depending on the feature. Workflow has its own intitialization script with variables for the JRE path and the installation path.

If you have changed your database information, you must ensure that the database initialization file contains the proper information for your database. For more information, see Section 5.12.3, "Updating the Identity Governance Database Initialization File for the Database Changes," on page 127.

To manually generate the database schema:

1. Stop the application server, such as Apache Tomcat. For more information, see Section 3.5.3, "Starting and Stopping Apache Tomcat," on page 50.
2. Record the names of the databases.
3. (Conditional) Perform the following steps to recreate the existing database.
   - **3a** Back up the data in the database.
   - **3b** Drop the existing database.
   - **3c** Create a new database with the same name as the one that you deleted in the prior step.
4. Open the database initialization script in a text editor and ensure that the installation paths for Java and Identity Governance, Identity Reporting, or Workflow match what is in your environment.
   - **4a** Access the directory where the database installation script resides. This is the default installation location:
     - **Identity Governance**
       - **Linux:** `/opt/netiq/idm/apps/idgov/bin`
       - **Windows:** `c:\netiq\idm\apps\idgov\bin`
     - **Identity Reporting**
       - **Linux:** `/opt/netiq/idm/apps/idrpt/bin`
       - **Windows:** `c:\netiq\idm\apps\idrpt\bin`
     - **Workflow Engine [4.2]**
       - **Linux:** `/opt/netiq/idm/apps/wfe/bin`
       - **Windows:** `c:\netiq\idm\apps\wfe\bin`
   - **4b** Open the database script in a text editor.
     - **Linux:** `db-init.sh`
     - **Windows:** `db-init.bat`
   - **4c** Ensure that the following items have the correct paths for your environment.
     - **install_path:** Installation path for Identity Governance.
     - **java_home:** Installation path for the JRE that was installed with Zulu OpenJDK.
     - **reporting_path:** Installation path for Identity Reporting.
   - **4d** Save and close the file.
   - **4e** Open the Workflow database script in a text editor.
     - **Linux:** `db-init-wfe.sh`

- **Windows:** `db-init-wfe.bat`

4f Ensure that you have the correct JRE and Workflow installation paths for your environment.

4g Save and close the file.

5 (Conditional) If you do not want to generate SQL to re-initialize the databases, you can initialize the databases using the database scripts by entering the following at a command prompt in the directory where the database script resides.

- **Linux:** `./db-init.sh -password` *`database-password`*`[4.2]./db-init-wfe.sh -dbpwd database-password -consumerpwd aa-clientpassword`

```
-encrypt-storepass encryption-keystore-password -storepwd truststore-

password
```

- **Windows:** `db-init.bat -password` *`database-password`*`[4.2]db-init-wfe.bat -dbpwd database-password -consumerpwd aa-clientpassword`

```
-encrypt-storepass encryption-keystore-password -storepwd truststore-

password
```

6 (Conditional) If you want to generate a single SQL file for re-initializing the databases, perform the following steps:

6a Enter the following at a command prompt in the directory where the database script resides.

- **Linux:** `./db-init.sh -password` *`database-password`* `-sql >` *`/opt/netiq/idm/apps/idrpt/sql/output.sql`*`[4.2]./db-init-wfe.sh -dbpwd database-password -consumerpwd aa-clientpassword`

```
-encrypt-storepass encryption-keystore-password -storepwd truststore-

password -sql > /opt/netiq/ idm/apps/wfe/sql/output.sql
```

- **Windows:** `db-init.bat -password` *`database-password`* `-sql > c:\netiq\idm\apps\idrpt\sql\output.sql[4.2]db-init-wfe.bat -dbpwd database-password -consumerpwd aa-clientpassword`

```
-encrypt-storepass encryption-keystore-password -storepwd truststore-

password -sql > c:\netiq\idm\apps\wfe\sql\output.sql
```

6b Have your database administrator open the `output.sql` file in a text editor and create a SQL file for each section in the file for each database listed. You must re-initialize each database one by one.

6c Have the database administrator run each SQL script that they create in the prior step to re-initialize the databases.

7 Start the application server such as Apache Tomcat. For more information, see Section 3.5.3, "Starting and Stopping Apache Tomcat," on page 50.

12.3 Creating or Changing Database Encryption Keys after the Installation

You can generate a new primary encryption key and rotate the existing primary keys within the encryption keystore. The new primary key will be used when encrypting any sensitive data. The old, rotated keys will be used to decrypt existing sensitive data.

To list the current encryption keys:

1 Run the Java Key Tool utility:

- **Linux:** `$JAVA_HOME/bin/keytool -list -keystore /opt/netiq/idm/apps/tomcat/conf/encrypt-keys.pkcs12 -storepass encryption-keystore-password -v`
- **Windows:** `$JAVA_HOME\bin\keytool -list -keystore c:\opt\netiq\idm\apps\tomcat\conf\encrypt-keys.pkcs12 -storepass encryption-keystore-password -v`

To rotate the primary encryption key:

1 Stop the application server, such as Apache Tomcat. For more information, see Section 3.5.3, “Starting and Stopping Apache Tomcat,” on page 50.

2 Take a backup of the current encryption keystore:

- **Linux:** `/opt/netiq/idm/apps/tomcat/conf/encrypt-keys.pkcs12`
- **Windows:** `c:\opt\netiq\idm\apps\tomcat\conf\encrypt-keys.pkcs12`

3 Run the Master Key Generation utility.

- **Linux:** `/opt/netiq/idm/apps/idgov/bin/masterkey-gen.sh -keystore`

`/opt/netiq/idm/apps/tomcat/conf/encrypt-keys.pkcs12 -storepass`*`encryption-keystore-password`*

- **Windows:** `c:\opt\netiq\idm\apps\idgov\bin\masterkey-gen.cmd -keystore`

`c:\opt\netiq\idm\apps\tomcat\conf\encrypt-keys.pkcs12 -storepass`*`encryption-keystore-password`*

4 Start the application server such as Apache Tomcat. For more information, see Section 3.5.3, “Starting and Stopping Apache Tomcat,” on page 50.

12.4 Configuring Auditing after the Installation

Identity Governance generates common event format (CEF) events that you can forward to an audit server to analyze the events and to create reports. These reports allow you to provide that you are in compliance with regulations.

Identity Governance provides auditing for the following components:

- OSP
- Identity Governance
- Identity Reporting

You can choose to enable auditing during the installation of these components, or you can enable it through configuration any time after you have installed the components. To enable auditing events for Identity Governance or Identity Reporting after installation, you must log into Identity Governance as a Global Administrator and use the Configuration menu. To do so for OSP, use the Identity Governance Configuration Update utility, which also allows you to change the server details, and TLS settings.

Identity Governance also allows you to enable a more granular view of the audit events by enabling loggers. For more information, see Section 15.6, “Increasing Logging Levels for Identity Governance and the Identity Governance Clients,” on page 308.

- Section 12.4.1, “Enabling Auditing for OSP,” on page 257
- Section 12.4.2, “Enabling Auditing for Identity Governance,” on page 258
- Section 12.4.3, “Enabling Auditing for Identity Reporting,” on page 258
- Section 12.4.4, “Enabling Auditing for the Workflow Engine,” on page 259

12.4.1 Enabling Auditing for OSP

If you have the components installed on separate servers, you must perform the following steps for each OSP server that you have installed.

To configure auditing after the installation:

1 Stop the application server. For more information, see Section 3.5.3, “Starting and Stopping Apache Tomcat,” on page 50.

2 Launch the Identity Governance Configuration Update utility:

  2a Navigate to one of the following directories:

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

  2b Launch the Identity Governance Configuration Update utility:

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

3 Click the **CEF Auditing** tab, then use the following information to enable auditing: click **Auditing Settings**, then click **Send audit events**.

Send audit events

Select this option to enable auditing for this server.

Destination host

Specify the DNS name of the audit server. If it is this server, you can use localhost.

Destination port

Specify the port the audit server uses to communicate. The default port is 6514.

Network protocol

Select if the audit server communicates over **TCP** or **UDP**.

Use TLS

This option only appears if you select **TCP.** Select this option if you have configured the audit server to communicate over TLS. For more information, see Section 3.9, "Securing Connections with TLS/SSL," on page 51.

Intermediate event store directory

Specify a path to a directory on this server where Identity Governance stores the audit cache files until the information is sent to the audit server.

4. Click **OK**.
5. Start the application server. For more information, see Section 3.5.3, "Starting and Stopping Apache Tomcat," on page 50.

We provide a list of the events that the server sends to the audit server. To see the list of events, see OSP Audit Events (https://www.microfocus.com/documentation/identity-governance/4.3/tech-refs/AuditEventTable.pdf).

12.4.2 Enabling Auditing for Identity Governance

If you want to enable auditing for Identity Governance after installation, you must do so through the Identity Governance Configuration feature.

To enable auditing for Identity Governance after installation:

1. Log in to Identity Governance as a Global Administrator.
2. Select **Configuration** > **Advanced**.
3. Click **+** to add, enable, or configure each of the following properties:
   - `ig.audit.server.enabled`
   - `ig.audit.server.httpAuditData`
   - `ig.audit.server.check-tls-cert-exp`
   - `ig.audit.server.syslog.enabled`
   - `ig.audit.server.syslog.protocol`
   - `ig.audit.server.syslog.host`
   - `ig.audit.server.syslog.port`
   - `ig.audit.server.syslog.cache-dir`
   - `ig.audit.server.syslog.cache-file`
   - `ig.audit.server.syslog.keystore-file`
   - `ig.audit.server.syslog.keystore-password`
   - `ig.audit.server.syslog.keystore-type`

12.4.3 Enabling Auditing for Identity Reporting

If you want to enable auditing for Identity Reporting after installation, you must do so through the Identity Governance Configuration feature.

To enable auditing for Identity Reporting after installation:

1. Log in to Identity Governance as a Global Administrator.
2. Select **Configuration** > **Advanced**.
3. Click **+** to add, enable, or configure each of the following properties:
   - `ig.audit.rpt.check-tls-cert-exp`
   - `ig.audit.rpt.enabled`
   - `ig.audit.rpt.httpAuditData`
   - `ig.audit.rpt.syslog.cache-dir`
   - `ig.audit.rpt.syslog.cache-file`
   - `ig.audit.rpt.syslog.enabled`
   - `ig.audit.rpt.syslog.host`
   - `ig.audit.rpt.syslog.keystore-file`
   - `ig.audit.rpt.syslog.keystore-password`
   - `ig.audit.rpt.syslog.keystore-type`
   - `ig.audit.rpt.syslog.port`
   - `ig.audit.rpt.syslog.protocol`

12.4.4 Enabling Auditing for the Workflow Engine

The auditing events provides a record of what the Workflow Engine has done.

To configure auditing you must access the Workflow Administration Console:

1. Log in to the Workflow Administration Console as a Global Administrator.
2. Select **Configuration** > **Audit Configuration**.

   NOTE: Depending on your requirement, you can enable one or all the audit configurations.

3. (Optional) Select **Tomcat** to add, enable, or configure the following properties:
   - `workflow.audit.wfs.server-log.enabled`
   - `workflow.audit.wfs.server-log.httpAuditData`
   - `workflow.audit.wfs.server-log.truncate-to-cef`
4. (Optional) Select **Syslog** to add, enable, or configure the following properties:
   - `workflow.audit.wfs.syslog.cache-dir`
   - `workflow.audit.wfs.syslog.cache-file`
   - `workflow.audit.wfs.syslog.check-tls-cert-exp`
   - `workflow.audit.wfs.syslog.enabled`
   - `workflow.audit.wfs.syslog.host`
   - `workflow.audit.wfs.syslog.httpAuditData`
   - `workflow.audit.wfs.syslog.keystore-file`
   - `workflow.audit.wfs.syslog.keystore-password`

- `workflow.audit.wfs.syslog.keystore-type`
- `workflow.audit.wfs.syslog.port`
- `workflow.audit.wfs.syslog.protocol`
- `workflow.audit.wfs.syslog.truncate-to-cef`

5 (Optional) Select **File** to add, enable, or configure the following properties:

- `workflow.audit.wfs.cef-to-file.directory`
- `workflow.audit.wfs.cef-to-file.enabled`
- `workflow.audit.wfs.cef-to-file.filename-prefix`
- `workflow.audit.wfs.cef-to-file.filename-suffix`
- `workflow.audit.wfs.cef-to-file.httpAuditData`
- `workflow.audit.wfs.cef-to-file.truncate-to-cef`

6 (Optional) Select **JDBC** to add, enable, or configure the following properties:

- `workflow.audit.wfs.jdbc.driver`
- `workflow.audit.wfs.jdbc.enabled`
- `workflow.audit.wfs.jdbc.fallback-datasource`
- `workflow.audit.wfs.jdbc.httpAuditData`
- `workflow.audit.wfs.jdbc.jdbc-password`
- `workflow.audit.wfs.jdbc.jdbcURL`
- `workflow.audit.wfs.jdbc.jdbc-username`
- `workflow.audit.wfs.jdbc.keystore-file`
- `workflow.audit.wfs.jdbc.keystore-password`
- `workflow.audit.wfs.jdbc.keystore-type`
- `workflow.audit.wfs.jdbc.schema`
- `workflow.audit.wfs.jdbc.ssl-type`
- `workflow.audit.wfs.jdbc.tablename`
- `workflow.audit.wfs.jdbc.truncate-to-cef`
- `workflow.audit.wfs.jdbc.truststore-file`
- `workflow.audit.wfs.jdbc.truststore-password`
- `workflow.audit.wfs.jdbc.truststore-type`
- `workflow.audit.wfs.jdbc.use-ssl`

12.5 Enabling Email Notifications after the Installation

Identity Governance, Identity Reporting, and Workflow Services can notify users of tasks to perform via email. You can use an SMTP mail server to deliver the emails but it does not guarantee that the users will receive the email. To guarantee delivery of email notifications, you must install 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 "Creating and Modifying Review Definitions " in the *Identity Governance User and Administration Guide*.

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 email uses the default language for the system. You can customize the content in the emails. For more information, see "Customizing Email Notification Templates" in the *Identity Governance User and Administration Guide*.

- Section 12.5.1, "Prerequisites for Email Notifications," on page 261
- Section 12.5.2, "Enabling Email Notifications for Identity Governance," on page 261
- Section 12.5.3, "Enabling Email Notifications with a Load Balancer or a Reverse Proxy," on page 262

12.5.1 Prerequisites for Email Notifications

Ensure that you have an SMTP mail server running and configured for SSL/TLS communications before enabling email notifications. This ensures that the email communication between Identity Governance and the users is secure.

NOTE: If you are using the Gmail SMTP server, Gmail ignores the SMTP server value and uses the actual Gmail address as the origination for email notifications.

12.5.2 Enabling Email Notifications for Identity Governance

Ensure that you have an SMTP server configured and that you have the connection information for the SMTP server to enter in to the Identity Governance Configuration utility. Also, ensure that you have ActiveMQ installed using the same Apache Tomcat instance that Identity Governance uses.

To enable the mail server for notifications:

1. Launch the Identity Governance Configuration utility. For more information, see Section 15.1.4, "Using the Identity Governance Configuration Utility," on page 290.
2. Select **Workflow Settings**.
3. Under **Notification System**, specify the settings for the mail server.
4. Select **Save**.

5 (Conditional) To ensure guaranteed delivery of the notifications by using ActiveMQ, complete the following steps:

5a Select **Enable persistent notification message queue**.

5b Enter the settings for the JMS broker.

5c (Optional) To use TLS/SSL protocol for messaging, select **SSL** and then specify the keystore settings.

5d Select **Save**.

5e Navigate to the installation directory for ActiveMQ. For example,

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

5f Copy the `activemq-all-x.x.x.jar` file.

5g Navigate to the installation directory for the Apache Tomcat server supporting Identity Governance. For example,

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

5h In the `lib` directory of the Apache Tomcat installation, paste the `activemq-all-x.x.x.jar` file.

5i Restart Apache Tomcat after copying the `activemq-all-x.x.x.jar` file. For more information, see Section 3.5.3, “Starting and Stopping Apache Tomcat,” on page 50.

6 (Optional) To change the text in the email notifications, see “Customizing Email Notification Templates” in the *Identity Governance User and Administration Guide*.

12.5.3 Enabling Email Notifications with a Load Balancer or a Reverse Proxy

Identity Governance supports load balancers and a reverse proxy. If you are using either option, you must perform some additional steps. The load balancer and reverse proxy contain multiple IP addresses or DNS names. You must configure additional fields either during the Identity Governance installation or after you have completed the installation.

1 Obtain the protocol, DNS value, and port of the load balancer or the reverse proxy.

2 Launch the Identity Governance Configuration utility. For more information, see Section 15.1.4, “Using the Identity Governance Configuration Utility,” on page 290.

3 Click the **Authentication Server** tab.

4 Enter the protocol, DNS value, and port of the load balancer or the reverse proxy in the following fields:

- **IG Redirect URL**
- **IG Request Redirect URL**
- **OSP URL** (This depends upon where you deployed OSP)

5 Click the **Network Topology** tab, then click **Protocol**.

6 In the **Host** and **Port** fields, specify the local host information for the load balancer or reverse proxy, then save the changes.

7 Exit the Identity Governance Configuration utility.

8 Restart Apache Tomcat. For more information, see Section 3.5.3, “Starting and Stopping Apache Tomcat,” on page 50.

13 Upgrading Identity Governance

You can upgrade to Identity Governance 4.3.1 from Identity Governance 3.7, 3.7.3, or 4.2.0. The Identity Governance components run against Apache Tomcat and Zulu OpenJDK. To ensure that the Identity Governance components run against the supported versions of Apache Tomcat and Zulu OpenJDK, you must uninstall the old Identity Governance components, upgrade Apache Tomcat and Zulu OpenJDK, and then reinstall the current version of the Identity Governance components to complete the upgrade. As part of the upgrade process, you must also migrate data because some of the collector templates and database tables and views change between the releases of Identity Governance.

Upgrading to the latest Identity Governance version is a process of multiple tasks that you must follow. You must back up your current data, uninstall the version of the Identity Governance components you currently have installed, upgrade the required hardware and software, and then reinstall the current version of the Identity Governance components.

If you installed Identity Governance and Identity Reporting on the same server, but you need to have Identity Reporting run on a separate server, an upgrade is the best time to move Identity Reporting to its own server to increase the performance of Identity Governance.

Use the following information to plan and perform the upgrade of the Identity Governance components.

13.1 Planning to Upgrade Identity Governance

As you plan your upgrade, keep in mind the following considerations:

- ❒ You might need to upgrade the hardware and software required to install the latest version of Identity Governance. For more information, see Section 2.4, “Hardware and Software Requirements,” on page 39.
- ❒ Open fulfillment requests are available after the upgrade.
- ❒ In Identity Governance, only review owners and administrators can view the review runs that were completed in a previous version. If you have reporting installed, run reports before you upgrade to capture these details and make them available to other users after the upgrade.
- ❒ Ensure you have the DNS names to identify server hosts before beginning the upgrade procedure. Because of new standards-based authentication, using IP addresses might not work correctly in all circumstances. The side effect is that the OSP integration with Identity Governance and Identity Reporting will not work correctly in these circumstances.

❒ Upgrading Identity Governance does not update data collectors. New data collection options added in the new release only appear if you create a new collector from the new template.

❒ If you are upgrading from Identity Governance 4.2.0 or later, make sure to back up the encryption keystore file before proceeding with the upgrade.

❒ Before you upgrade, record the values for the following settings. The installation process fails to restore or adversely modifies these settings:

Location of settings	Affected Settings
Workflow Setting > Notification System in the Identity Governance Configuration utility	◆ Mail Server ◆ From Address

❒ Upgrade the Identity Governance components:

1. Verify you have the correct operating system for this upgrade. For more information, see Section 2.4, “Hardware and Software Requirements,” on page 39.
2. Upgrade the framework components to supported versions. You can download scripts from the Identity Governance documentation page under the **Reference** heading to help you upgrade these components.

   ❒ Zulu OpenJDK

   ❒ Apache Tomcat

   ❒ Identity Vault (LDAP server)

   ❒ Access Manager if it is your authentication service

   ❒ Database

   IMPORTANT: 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.

   ❒ (Conditional) To upgrade your Identity Governance Oracle database, you must grant the `CREATE PUBLIC SYNONYM` and `DROP PUBLIC SYNONYM` privileges to the `igops` schema.
3. Back up your trust store files, and then run the OSP installer.

   NOTE: Specify the same password that was used for sensitive data encryption and decryption during the installation of previous versions of Identity Governance, when upgrading from Identity Governance 4.2.0 or later.
4. Run the Identity Governance and Identity Reporting installers.
5. Restore trust store files.
6. If you installed the Identity Governance components on the same server and you want to install the components separately, prepare the proper amount of new servers to run the components.

NOTE: If you have additional conditions or questions, work with your support representative or consultants to upgrade in your environment.

13.2 Securing Passwords for a Silent Install

To allow the silent installation of Identity Governance to work, Identity Governance reads passwords stored in environment variables or entered into silent properties files. For more information, see "Understanding the Passwords that Identity Governance Reads from Environment Variables During the Installation Process" on page 156.

Specify each password either as an environment variable, or in the silent properties file before you run the silent installer.

If you are performing a silent installation for the Identity Governance components, ensure that you use the current silent properties file for the proper component, and then update these properties with the values in your old silent properties files.

If you specified passwords as environment variables for the silent installation, you can remove these variables after the installation completes by following the appropriate procedure for your operating system.

13.3 Upgrading Procedure for Identity Governance

The following upgrade procedures contain steps on how to upgrade Identity Governance and the components you have installed. Some of the steps are conditional depending on your deployment and the configuration of the different components.

- Section 13.3.1, "Upgrading Identity Governance Framework Components," on page 267
- Section 13.3.2, "Upgrading Identity Governance and Its Core Components," on page 273

13.3.1 Upgrading Identity Governance Framework Components

We provide scripts to help you upgrade the required components you installed for Identity Governance. One script scans your installations of Tomcat, ActiveMQ, Java, and PostgreSQL to determine which of those components require updates for the Identity Governance upgrade. The second script helps you upgrade those components, if needed, and leave your existing files intact and disabled.

If you run Identity Governance in a clustered environment, and if you installed components on multiple nodes, you must run the scripts on each of those nodes.

NOTE: These scripts help you upgrade only the framework components installed for Identity Governance. After you upgrade the components, you must then upgrade Identity Governance and Identity Reporting (if applicable).

Download one of the following appropriate component upgrade scripts for your operating system from the Identity Governance documentation page under the **References** heading:

- Identity Governance Component Upgrade Scripts - Linux
- Identity Governance Component Upgrade Scripts - Windows

NOTE: The upgrade component script for Linux does not upgrade PostgreSQL, so you must do so manually. For more information, see "Upgrading PostgreSQL for Linux" on page 270.

13.3.1.1 Running the Version Compare Script

The version compare script scans your installations of Tomcat, ActiveMQ, Java, and PostgreSQL to determine which of those components require updates for the Identity Governance upgrade.

To run the version compare script:

1. From a Linux command line or a Windows PowerShell command line, execute the script.
   - Linux: `versions.sh`
   - Windows: `versions.ps1`
2. Provide the path of the component, if different from the default path. The script then:
   - Verifies the component path provided contains files and directories expected for that component.
   - Retrieves the component version for your setup.
   - Compares the installed component version with the required version.
   - Provides feedback for whether you should upgrade the component.
   - Repeats the process for the next component.

13.3.1.2 Downloading the Identity Governance Components

After you run the version compare script, create a `compressed` directory in the directory where you stored and unzipped the component upgrade scripts, and then copy the component updates that the script identified as needed.

- For a Linux installation, download `*tar.gz` files to `/Downloads/idgov-core-upgrader-master/linux/compressed`.
- For a Windows installation, download `*.zip` files to `\Downloads\idgov-core-upgrader-master\windows\compressed`.

NOTE: For PostgreSQL, you have to download the `*.exe` file to `\Downloads\idgov-core-upgrader-master\windows\compressed`.

13.3.1.3 Running the Upgrade Component Script

The upgrade component script upgrades Tomcat, ActiveMQ, and Java on Linux, and upgrades Tomcat, ActiveMQ, Java, and PostgreSQL on Windows.

NOTE: The upgrade component script does not upgrade your database if:

- You use Oracle or Microsoft SQL Server as your database
- You use PostgreSQL on Linux

If you need to upgrade your database in these cases, you must do so manually.

The upgrade component script renames the existing component folders to a name that includes a time stamp matching the time you launched the upgrade component script (all components on Windows; but only Tomcat, ActiveMQ, and Java on Linux). The script creates a new directory with the original directory name, and then places the updated components in that directory.

In addition, the script copies specified files from the old setup, and provides you with the option to see file structure differences. Doing so allows you to manually copy additional files the script did not copy. In theory, you should be able to swap the new and old component folders again if you change your mind.

To run the upgrade component script:

1. From a Linux command line or a Windows PowerShell command line, execute the script.
   - Linux: `upgrade.sh`
   - Windows: `upgrade.ps1`
2. Provide the requested input when prompted.

   NOTE: For Windows, the prompt to upgrade PostgreSQL defaults to “No.” If you use PostgreSQL as a database, and want to upgrade it using the script, press “Y” or “y” when prompted to upgrade PostgreSQL.

Specifically, the script:

- Checks whether the replacement file for the component is in the `/compressed` directory.
  - If not, the script displays the file it was expecting to find, and then proceeds to the next component.
  - If so, the script continues.
- Offers you the choice of upgrading the current component.
- Asks for the existing component path.
- Checks the validity of the provided component path and, if invalid, prompts you for a valid path.
- Instructs you to terminate the following corresponding services:
  - Tomcat service for Tomcat
  - ActiveMQ service for ActiveMQ
  - Tomcat and ActiveMQ services for Java
  - PostgreSQL (Windows script only)

  NOTE: The Windows script provides the option to terminate services for you, including some applications if files (such as Tomcat logs) are open and locked.
- (Linux only) Saves component ownership for applying later.

- Renames the existing component folder with a time stamp indicating the time you launched the upgrade component script.
- Unpacks the contents of the downloaded component into the same path you provided.

NOTE: The Java upgrade places a symbolic link in its place, regardless of whether it was originally symbolic.

- Deletes certain `webapps` folders from the unpacked content (Tomcat only).
- Copies known files from the old file structure to the new.

NOTE: If the script copies an unpacked file, it backs up the file with `*-backup.*` in its name.

- (Linux only) Applies the ownership retrieved above, and recursively applies it to the new folder.

NOTE: Depending on your setup, you could need to apply a different sub-ownership.

- Gives you the option of viewing file differences, with the following caveats:
  - (Windows only) Tomcat and PostgreSQL can take a significant amount of time generating these differences.
  - File and directory comparison for Linux is more efficient than that for Windows.

13.3.1.4 Upgrading PostgreSQL for Linux

If you need to upgrade your Linux installation of PostgreSQL, you need to perform preliminary steps before you upgrade. Extra preparation is not needed for Windows installations, unless your PostgreSQL database contains more than just Identity Governance and Identity Reporting. In that case, you should back up and restore your personal databases.

In Linux, the PostgreSQL upgrade process is through a repository.

To upgrade to the required version of PostgreSQL:

1. Add the PostgreSQL repository.
   - SLES 15 SP4: https://mirrorcache-us.opensuse.org/repositories/server:/database:/postgresql/15.4/server:database:postgresql.repo (https://mirrorcache-us.opensuse.org/repositories/server:/database:/postgresql/15.4/server:database:postgresql.repo)
   - RHEL 8.8: https://download.postgresql.org/pub/repos/yum/reporpms/EL-8-x86_64/pgdg-redhat-repo-latest.noarch.rpm
2. For SLES, install the updated library: `libpq5`.
3. For either SLES or RHEL, install postgresql14-server through the package manager.
4. At the command line, type the following to back up the Identity Governance and Identity Reporting databases:

   NOTE: Perform these commands as a PostgreSQL user.

   - `"${PATH_TO_POSTGRESQL}/bin/pg_dump" -h "localhost" -p "5432" -U "postgres" -Fc "igops" > "igops.dump"`
   - `"${PATH_TO_POSTGRESQL}/bin/pg_dump" -h "localhost" -p "5432" -U "postgres" -Fc "igdcs" > "igdcs.dump"`

- "${PATH_TO_POSTGRESQL}/bin/pg_dump" -h "localhost" -p "5432" -U "postgres" -Fc "igwf" > "igwf.dump"
- "${PATH_TO_POSTGRESQL}/bin/pg_dump" -h "localhost" -p "5432" -U "postgres" -Fc "igara" > "igara.dump"
- "${PATH_TO_POSTGRESQL}/bin/pg_dump" -h "localhost" -p "5432" -U "postgres" -Fc "igrpt" > "igrpt.dump"
- (Conditional) When using JDBC auditing: # "${PATH_TO_POSTGRESQL}/bin/pg_dump" -h "localhost" -p "5432" -U "postgres" -Fc "iacaud" > "iacaud.dump"
- (Conditional) When using the external Workflow Service: # "${PATH_TO_POSTGRESQL}/bin/pg_dump" -h "localhost" -p "5432" -U "postgres" -Fc "igaworkflowdb" > "igaworkflowdb.dump"
- "${PATH_TO_POSTGRESQL}/bin/pg_dumpall" -h "localhost" -p "5432" -U "postgres" --roles-only > "roles.sql"

5. Stop the PostgreSQL service.
6. Rename the PostgreSQL data folder, and then create a new /data folder.
7. (Optional) Rename the PostgreSQL /bin folder, and then create a new /bin folder.
8. Place your PostgreSQL password as the only line in a file as follows:

   ```
   vi /tmp/pg_secret_to_remove
   ```

9. Use a package manager to install the new version of PostgreSQL.
10. Configure PostgreSQL 14 as follows:
    - export FILE_CONTAINING_PG_PASSWORD="/tmp/pg_secret_to_remove"
    - export PATH_TO_POSTGRESQL_DATA="/opt/netiq/idm/apps/postgres/data"
    - export ADMIN_POSTGRESQL="postgres"
    - For SLES: runuser -l postgres -c "/usr/lib/postgresql14/bin/initdb --auth='md5' --pwfile='${FILE_CONTAINING_PG_PASSWORD}' --username='${ADMIN_POSTGRESQL}' --pgdata='${PATH_TO_POSTGRESQL_DATA}'"
    - For RHEL: runuser -l postgres -c "/usr/pgsql-14/bin/initdb --auth='md5' --pwfile='${FILE_CONTAINING_PG_PASSWORD}' --username='${ADMIN_POSTGRESQL}' --pgdata='${PATH_TO_POSTGRESQL_DATA}'"
    - unset FILE_CONTAINING_PG_PASSWORD
    - unset PATH_TO_POSTGRESQL_DATA
    - unset ADMIN_POSTGRESQL
11. Remove the file in which you placed your PostgreSQL password.

    ```
    rm /tmp/pg_secret_to_remove
    ```

12. Copy the following older files to the new directory.
    - pg_hba.conf
    - postgresql.conf
13. Open postgresql.conf, uncomment the setting: password_encryption = md5, then save postgresql.conf.

14 Type the appropriate command to enable and restart the PostgreSQL service.

- SLES: `postgresql.service`
- RHEL: `postgresql-14.service`

15 At the command line, type the following to restore the Identity Governance and Identity Reporting databases:

- `"${PATH_TO_NEW_POSTGRESQL}/bin/psql" -h "localhost" -p "5432" -U "postgres" -d "postgres" -f "roles.sql"`
- `"${PATH_TO_NEW_POSTGRESQL}/bin/createdb" -h "localhost" -p "5432" -U "postgres" -T template0 "igops"`
- `"${PATH_TO_NEW_POSTGRESQL}/bin/pg_restore" -h "localhost" -p "5432" -U "postgres" -d "igops" -Fc "igops.dump"`
- `"${PATH_TO_NEW_POSTGRESQL}/bin/createdb" -h "localhost" -p "5432" -U "postgres" -T template0 "igdcs"`
- `"${PATH_TO_NEW_POSTGRESQL}/bin/pg_restore" -h "localhost" -p "5432" -U "postgres" -d "igdcs" -Fc "igdcs.dump"`
- `"${PATH_TO_NEW_POSTGRESQL}/bin/createdb" -h "localhost" -p "5432" -U "postgres" -T template0 "igwf"`
- `"${PATH_TO_NEW_POSTGRESQL}/bin/pg_restore" -h "localhost" -p "5432" -U "postgres" -d "igwf" -Fc "igwf.dump"`
- `"${PATH_TO_NEW_POSTGRESQL}/bin/createdb" -h "localhost" -p "5432" -U "postgres" -T template0 "igara"`
- `"${PATH_TO_NEW_POSTGRESQL}/bin/pg_restore" -h "localhost" -p "5432" -U "postgres" -d "igara" -Fc "igara.dump"`
- `"${PATH_TO_NEW_POSTGRESQL}/bin/createdb" -h "localhost" -p "5432" -U "postgres" -T template0 "igrpt"`
- `"${PATH_TO_NEW_POSTGRESQL}/bin/pg_restore" -h "localhost" -p "5432" -U "postgres" -d "igrpt" -Fc "igrpt.dump"`
- (Conditional) When using external JDBC auditing:`"${PATH_TO_NEW_POSTGRESQL}/bin/createdb" -h "localhost" -p "5432" -U "postgres" -T template0 "iacaud"`
- (Conditional) When using JDBC auditing:`"${PATH_TO_NEW_POSTGRESQL}/bin/pg_restore" -h "localhost" -p "5432" -U "postgres" -d "iacaud" -Fc "iacaud.dump"`
- (Conditional) When using external Workflow Service: `"${PATH_TO_NEW_POSTGRESQL}/bin/createdb" -h "localhost" -p "5432" -U "postgres" -T template0 "igaworkflowdb"`
- (Conditional) When using external Workflow Service:`"${PATH_TO_NEW_POSTGRESQL}/bin/pg_restore" -h "localhost" -p "5432" -U "postgres" -d "igaworkflowdb" -Fc "igaworkflowdb.dump"`

NOTE: Perform these commands as a PostgreSQL user only.

13.3.2 Upgrading Identity Governance and Its Core Components

Before you start the upgrade procedure, ensure that you review the considerations in "Planning to Upgrade Identity Governance" on page 265.

To upgrade Identity Governance and its core components:

1. Purge any unwanted data from the database before upgrading. For more information, see "Identifying Purgeable Data" in the *Identity Governance User and Administration Guide*.
2. (Optional) Run reports for any review run details you want to make available after the upgrade.
3. Launch the Identity Governance Configuration Utility in console mode, then issue the `export-sql` (or `es`) command to generate a SQL file that contains your current environment system properties. Move the file to another location, so you can compare it with a similar file you create after upgrading. For more information, see Section 15.1.4, "Using the Identity Governance Configuration Utility," on page 290.
4. Stop Identity Governance (and Apache Tomcat). For more information, see Section 3.5.3, "Starting and Stopping Apache Tomcat," on page 50.
5. (Conditional) If you are using PostgreSQL, back up and export your full Identity Governance data and confirm that you can restore it with no problems.

   Include all of the Identity Governance databases (default names). If you installed Identity Reporting, back up the Identity Reporting database (default name) as well.

   - `igops`
   - `igarc`
   - `igdcs`
   - `igwf`
   - `igara`
   - `igrpt`

   For more information, see the *PostgreSQL Documentation (https://www.postgresql.org/docs/)* for your version of PostgreSQL.
6. (Conditional) If you are using Oracle, perform the following steps:

   6a Back up the following schemas:

   - `igops`
   - `igarc`
   - `igdcs`
   - `igwf`
   - `igara`
   - `igrpt`

   6b (Conditional) If your Oracle database has virtual columns, run the following command to identify virtual columns:

```
select distinct 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';
```

6c (Conditional) If your Oracle database has virtual columns, run the following script, modified for your specific environment details, to drop extended statistics and virtual columns:

```
declare
  v_owner varchar2(255);
  v_table varchar2(255);
  v_extension varchar2(32000);
begin
  select SYS_CONTEXT('USERENV', 'SESSION_USER') into v_owner from
DUAL;
  for rec in (
    select distinct c.table_name, dbms_lob.substr(e.extension,
32000, 1) as extension,
    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_table := rec.table_name;
    v_extension := rec.extension    execute immediate 'call
dbms_stats.drop_extended_stats(:v_owner, ;
:v_table, :v_extension)' using v_owner, v_table, v_extension;
  end loop;
end;
```

For more information, see the Oracle documentation (https://docs.oracle.com/en/) for the version of Oracle you have.

7 (Conditional) If you are using MS SQL, back up the following databases:

- `igops`
- `igarc`
- `igdcs`
- `igwf`
- `igara`
- `igrpt`

For more information, see the Microsoft SQL documentation (https://docs.microsoft.com/en-us/sql/?view=sql-server-ver15).

8 Move your generated reports (`pdf` and `csv` files) from the Reporting home folder to a backup directory.

9 Perform the following steps to upgrade OSP:

9a Back up the following trust store files:

- Linux:
  - `/opt/netiq/idm/apps/osp/osp.pkcs12`
  - `/opt/netiq/idm/apps/osp/osp-truststore.pkcs12`
  - `/opt/netiq/idm/apps/tomcat/conf/apps-truststore.pkcs12`
- Windows:
  - `\opt\netiq\idm\apps\osp\osp.pkcs12`

- `\opt\netiq\idm\apps\osp\osp-truststore.pkcs12`
- `\opt\netiq\idm\apps\tomcat\conf\apps-truststore.pkcs12`

9b Run the OSP upgrade installer.

> **NOTE:** If you are upgrading from Identity Governance 4.2.0 or later while installing OSP, you must specify the same password used during the installation of the previous version of Identity Governance for encrypting and decrypting sensitive data, which has been backed up.

10 Run the Identity Governance installer.

11 (Optional) Install the current version of Identity Reporting on the same server or a different server if needed. For more information, see Chapter 7, "Installing Identity Reporting," on page 163.

12 (Conditional) If you are upgrading in a Windows environment, reboot the Windows server.

13 Remove the `localhost` folder located in the `/opt/netiq/idm/apps/tomcat/work/Catalina` folder in Linux, or the `C:\netiq\idm\apps\tomcat\work\Catalina` folder in Windows.

14 (Conditional) Add the virtual columns back into the Oracle database. For more information, see Oracle documentation.

15 Delete all files and folders from the `/opt/netiq/idm/apps/tomcat/temp` folder in Linux, or from the `C:\netiq\idm\apps\tomcat\temp` folder in Windows.

16 Move existing logs to a backup location.

17 (Conditional) If you are integrated with an IDP (for example Access Manager), you can either:

- Move the newly created trust store files (`osp.pkcs12` and `osp-truststore.pkcs12)` to a different location, and then move the original trust store files (`osp.pkcs12` and `osp-truststore.pkcs12)` back to the OSP installation folder, or
- Update the IDP with the newly-created certificates.

18 Clear your internet browser cache and remove cookies.

19 Copy the generated `pdf` and `csv` report files to the location you specified during the installation.

20 Start Tomcat. For more information, see Section 3.5.3, "Starting and Stopping Apache Tomcat," on page 50.

21 (Conditional) Log in to Identity Governance to review any customized settings you have made to the user interface. Because of changed or additional element IDs and the different navigation settings, customizations you made to your previous environment might not work as expected. Adjust your customizations as needed.

22 (Conditional) If you are collecting identities from a source that supports change events, run the Identity Source Migration and Upgrade utility to convert your existing source to use change event processing. If you are already using a change event collector, you can also use the utility to upgrade the configuration. For more information, see "Converting an Identity Collector to a Change Event Identity Collector (https://www.microfocus.com/documentation/identity-governance/4.3/user-guide/t4ndywshnp9q.html#t44iequ5otlm)" in the *Identity Governance User and Administration Guide*.

23 Publish the collected data again to populate the business roles and other items. For more information, see *Publishing the Collected Data* (https://www.microfocus.com/documentation/identity-governance/4.3/user-guide/publishing-collected-data.html) in the.

24 If needed, run the Identity Governance Configuration Utility to restore your values for **Workflow Settings > Notification System**. For more information, see Section 15.1.4, "Using the Identity Governance Configuration Utility," on page 290.

25 If needed, run the Identity Governance Configuration Utility in console mode with the `export-sql (-es)` command to get a list of system settings for your upgraded environment. Compare it to the list you generated before upgrading and restore any additional custom settings for your environment. For more information, see Section 15.1.4, "Using the Identity Governance Configuration Utility," on page 290.

26 If you used the Identity Governance Configuration Utility to make changes in Step 23 or Step 24, restart Tomcat for these changes to take effect.

13.4 Applying the Latest Patches

After upgrading to the latest version of Identity Governance, apply any available patches by following the procedure included with the patch. You can download the patches by logging in to Software Licenses and Downloads (https://sld.microfocus.com/mysoftware/index).

NOTE: The Software Licenses and Downloads page requires you be granted access. Follow the prompts on screen to request access.

13.5 Moving Identity Reporting to a Separate Server

You can move Identity Reporting to a separate server from Identity Governance. This could occur if you realize that Identity Reporting impacts the performance of Identity Governance. The steps to move Identity Reporting to a separate server are similar to those for upgrading Identity Reporting. The difference is where you reinstall Identity Reporting.

Before you move Identity Reporting to a separate server, you must uninstall Identity Reporting. The uninstaller program restores files, including the Apache Tomcat files to how they were before installing Identity Governance and Identity Reporting.

Use the following steps to move Identity Reporting to a separate server from Identity Governance:

1. Back up the files in following directories:
   - **Linux:** The default location on a Linux server.
     - `/opt/netiq/idm/apps/tomcat`
     - `/opt/netiq/idm/apps/idgov`
     - `/opt/netiq/idm/apps/idrpt`
   - **Windows:** The default location on a Windows server.
     - `c:\netiq\idm\apps\tomcat`
     - `c:\netiq\idm\apps\idgov`
     - `c:\netiq\idm\apps\idrpt`

2. Uninstall Identity Governance and Identity Reporting. For more information, see Section 14.2, “Uninstalling Components Installed with the Identity Governance Installer,” on page 281.
3. Install Identity Governance again on the same server. For more information, see Chapter 6, “Installing Identity Governance,” on page 131.
4. Ensure that the new server meets the Identity Reporting requirements. For more information, see Section 7.2, “Prerequisites for Identity Reporting,” on page 165.
5. Install Identity Reporting on the new server and select **Not to configure** the database during the install. For more information, see Section 7.5, “Installing Identity Reporting,” on page 179.
6. Start Apache Tomcat on the Identity Reporting server. For more information, see Section 3.5.3, “Starting and Stopping Apache Tomcat,” on page 50.

13.6 Moving Workflow Engine to a Separate Server

You can move the Workflow Engine to a separate server from other components, such as Identity Governance and Identity Reporting. This could occur if you realize that Workflow Engine impacts the performance of the other components. The steps to move to a separate server are similar to upgrading. The difference is where you reinstall the Workflow Engine.

To move the Workflow Engine to a separate server you must uninstall the Workflow Engine. The uninstaller program restores files, including the Apache Tomcat files to how they were before installing the Workflow Engine.

Use the following steps to move the Workflow Engine to a separate server from Identity Governance.

1. Back up the files in the following directories depending on what you installed with the Workflow Engine:
   - **Linux:** The default location on a Linux server:
     - `/opt/netiq/idm/apps/tomcat`
     - `/opt/netiq/idm/apps/idgov`
     - `/opt/netiq/idm/apps/idrpt`
     - `/opt/netiq/idm/apps/wfe`
   - **Windows:** The default location on a Windows server:
     - `c:\netiq\idm\apps\tomcat`
     - `c:\netiq\idm\apps\idgov`
     - `c:\netiq\idm\apps\idrpt`
     - c:\netiq\idm\apps\wfe
2. If you installed the Workflow Engine with Identity Governance and Identity Reporting, then uninstall Identity Governance, Identity Reporting and the Workflow Engine. For more information, see Section 14.2, “Uninstalling Components Installed with the Identity Governance Installer,” on page 281.
3. Install Identity Governance and Identity Reporting again on the same server. For more information, see Chapter 6, “Installing Identity Governance,” on page 131 and Chapter 7, “Installing Identity Reporting,” on page 163.

4. Ensure that the new server meets the Workflow Engine requirements. For more information, see Section 8.1, “Prerequisites to Install the Workflow Engine,” on page 183.
5. Install the Workflow Engine on the new server and select **Not to configure** the database during the install. For more information, see Chapter 8, “Installing Workflow Engine,” on page 183.
6. Start Apache Tomcat on the Workflow Engine server. For more information, see Section 3.5.3, “Starting and Stopping Apache Tomcat,” on page 50.

14 Uninstalling the Identity Governance Components

There are times when you are required to uninstall Identity Governance. You would uninstall Identity Governance in a lab environment or during an upgrade procedure. The Identity Governance components run against Apache Tomcat and Zulu OpenJDK, to perform an upgrade you must uninstall the Identity Governance components, upgrade Zulu OpenJDK and Apache Tomcat, and then reinstall the Identity Governance components. For more information about upgrading, see Chapter 13, "Upgrading Identity Governance," on page 265.

Identity Governance does come with an uninstall utility that you use to uninstall the product. OSP contains a separate uninstall utility. The uninstall utility for Identity Reporting is the Identity Governance uninstall utility. If you have installed Identity Reporting and Identity Governance together on the same server, the uninstall utility removes Identity Governance and Identity Reporting at the same time. If you have installed Identity Reporting on a separate server without Identity Governance, the uninstall utility only removes Identity Reporting.

IMPORTANT: 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 for the upgrade procedure.

You can also uninstall the components using the guided method, console method, and silent method in the same way that you install these components. The silent uninstall method does not require a silent properties file. It does not require any interaction to complete the uninstallation. For more information, see Section 1.3, "Understanding the Uninstallation Methods," on page 22.

IMPORTANT: If you installed Identity Governance and OSP on the same server, you must uninstall them in the reverse order in which you installed them. For example, if you installed Identity Governance, then installed OSP, you must uninstall OSP, then uninstall Identity Governance.

Use the following information to uninstall the Identity Governance components.

14.1 Uninstalling OSP

The installation utility for OSP places an uninstall utility on the server. You must run this utility to uninstall OSP. If you installed OSP on the same server as Identity Governance or if you have installed it on a separate server, you must use the OSP uninstall utility to uninstall OSP. The Identity

Governance uninstall utility does not uninstall OSP. You would uninstall OSP if you wanted to install OSP on a separate server from Identity Governance or if you were upgrading to the current version of Identity Governance.

IMPORTANT: You must always use the version of OSP that comes with the version of Identity Governance that you are using. Trying to use different versions of OSP causes unexpected behavior and is not supported.

The default mode of the uninstall utility is the mode that you used to install OSP. If you want to uninstall using a different method you must pass the appropriate parameter to perform that type of uninstall. For more information, see Section 1.3, "Understanding the Uninstallation Methods," on page 22.

To uninstall OSP:

1 Log in to the server running OSP as `root` on a Linux server, or as a user with administrative privileges on a Windows server.

2 Define the Java path to the `jre bin` directory as an environment variable in the uninstall script file that launches the uninstall utility.

IMPORTANT: If you do not define the path to the `jre bin` directory, the uninstall utility does not work. The utility does not come with Java. You must point to the Java you use with OSP.

2a Open the uninstall script file in a text editor. The default location of the script is:

- **Linux:** `/opt/netiq/idm/apps/osp/Uninstall_osp/LaunchUninstall.sh`
- **Windows:** `c:\netiq\idm\apps\osp\Uninstall_osp\LaunchUninstall.bat`

2b Change or ensure that the path listed for the `JRE_HOME` variable is the path to the `jre bin` directory that is installed with the Zulu OpenJDK. The default path is:

- **Linux:** `/opt/netiq/idm/apps/jre/bin`
- **Windows:** `c:\netiq\idm\apps\jre\bin`

2c Save and close the file.

3 Stop Apache Tomcat. For more information, see Section 3.5.3, "Starting and Stopping Apache Tomcat," on page 50.

4 Uninstall OSP.

4a (Conditional) Uninstall OSP from a Linux server.

4a1 Access the uninstall directory located here: `/opt/netiq/idm/apps/osp/Uninstall_osp`

4a2 Execute the script as `root` from a command line enter the following:

```
./LaunchUninstall.sh
```

4b (Conditional) Uninstall OSP on a Windows server.

4b1 Access the **Control Panel** as an administrator.

4b2 Search for and select OSP.

4b3 Select **Uninstall** and follow the prompts to complete the uninstall.

5 When the uninstall completes, delete the following files and folders:

- **Linux:** The default installation path is /opt/netiq/idm/apps/osp.
    - Delete the contents of the following folders including any subdirectories.
        - /opt/netiq/idm/apps/tomcat/work/Catalina/localhost
        - /opt/netiq/idm/apps/tomcat/temp
- **Windows:** The default installation path is C:\netiq\idm\apps\osp.
    - Delete the contents of the following folders including any subdirectories.
        - C:\netiq\idm\apps\tomcat\work\Catalina\localhost
        - C:\netiq\idm\apps\tomcat\temp

6 Restart Apache Tomcat, if needed. For more information, see Section 3.5.3, "Starting and Stopping Apache Tomcat," on page 50.

14.2 Uninstalling Components Installed with the Identity Governance Installer

The installation utility for Identity Governance, Identity Reporting, and Workflow Engine places an uninstall utility on the server. The uninstall utility uninstalls Identity Governance, Identity Reporting, and Workflow Engine, or Identity Governance and its components if you install the components at the same time. The uninstall utility provides the guided uninstall, the console uninstall, and the silent uninstall just like the installer utility does.

If you install Identity Governance and its components at separate times, the uninstall utility uninstalls the component that you installed last. For example, if you only installed Identity Governance and ran the system for a while and then installed Identity Reporting or Workflow Engine on the same server, the uninstall utility uninstalls Identity Reporting or Workflow Engine when you run it. You must run the utility a second time to uninstall Identity Governance.

The default mode of the uninstall utility is the method that you used to install Identity Governance or Identity Governance and Identity Reporting. If you want to uninstall using a different method you must pass the appropriate parameter to perform that type of uninstallation. For more information, see Section 1.3, "Understanding the Uninstallation Methods," on page 22.

To uninstall Identity Governance:

1 Log in to the server running Identity Governance as root on a Linux server or as a user with administrative privileges on a Windows server.

2 Define the Java path to the jre bin directory as an environment variable in the uninstall script file that launches the uninstall utility.

IMPORTANT: If you do not define the path to the jre bin directory, the uninstall utility does not work. The utility does not come with Java. You must point to the Java you use with Identity Governance.

2a Open the uninstall script file in a text editor. The default location of the script is:

- **Linux:** /opt/netiq/idm/apps/idgov/Uninstall_IdentityGovernance/LaunchUninstall.sh

- **Windows:**

  `c:\netiq\idm\apps\idgov\Uninstall_IdentityGovernance\LaunchUninstall.bat`

2b Change or ensure that the path listed for the `JRE_HOME` variable is the path to the `jre bin` directory installed with the Zulu OpenJDK. The default path is:

- **Linux:** `/opt/netiq/idm/apps/jre/bin`
- **Windows:** `c:\netiq\idm\apps\jre\bin`

2c Save and close the file.

3 Stop Apache Tomcat. For more information, see Section 3.5.3, “Starting and Stopping Apache Tomcat,” on page 50.

4 (Conditional) If you are running any version of Identity Governance prior to 3.0, you must uninstall Identity Reporting separately from Identity Governance.

4a (Conditional) Uninstall Identity Reporting on a Linux server.

4a1 Access the uninstall directory. The default location is: `/opt/netiq/idm/apps/idrpt/Uninstall_IdentityGovernance`

4a2 To execute the script, enter:

```
./LaunchUninstall.sh
```

4b (Conditional) Uninstall Identity Reporting on a Windows server.

4b1 Access the **Control Panel** as an administrator.

4b2 Search for Identity Reporting.

4b3 Click **Uninstall** and follow the prompts to uninstall Identity Reporting.

5 (Conditional) Uninstall Identity Governance or uninstall Identity Governance and Identity Reporting or Workflow Engine if your version of Identity Governance is 3.0 or later.

5a (Conditional) Uninstall Identity Governance or Identity Governance and Identity Reporting or Workflow Engine from a Linux server.

5a1 Access the uninstall directory located here: `/opt/netiq/idm/apps/idgov/Uninstall_IdentityGovernance`

5a2 Execute the script as `root` from a command line enter the following:

```
./LaunchUninstall.sh
```

5b (Conditional) Uninstall Identity Governance or uninstall Identity Governance and Identity Reporting or Workflow Engine on a Windows server.

5b1 Access the **Control Panel** as an administrator.

5b2 Search for and select Identity Governance.

5b3 Select **Uninstall** and follow the prompts to complete the uninstallation.

6 (Conditional) If you installed Identity Governance and Identity Reporting or Workflow Engine at different times on the same server, run the uninstall utility a second time to delete the component you installed first.

7 When the uninstallation completes, delete the following folders. The uninstall utility restores the `*.war` files that were in this directory before you installed Identity Governance.

- **Linux:** The default path is `/opt/netiq/idm/apps`.
    - `/opt/netiq/idm/apps/idgov`
    - `/opt/netiq/idm/apps/tomcat/webapps/api`
    - `/opt/netiq/idm/apps/tomcat/webapps/apidoc`
    - `/opt/netiq/idm/apps/tomcat/webapps/cx`
    - `/opt/netiq/idm/apps/tomcat/webapps/daas`
    - `/opt/netiq/idm/apps/tomcat/webapps/dtp`
    - `/opt/netiq/idm/apps/tomcat/webapps/formbuilder`
    - `/opt/netiq/idm/apps/tomcat/webapps/ROOT`
    - `/opt/netiq/idm/apps/tomcat/webapps/doc`
    - `/opt/netiq/idm/apps/tomcat/webapps/workflow-api`
    - (Conditional) If you installed Identity Reporting on the same server as Identity Governance, you must delete the following files and folders that Identity Reporting installed.
        - `/opt/netiq/idm/apps/idrpt`
        - `/opt/netiq/idm/apps/tomcat/webapps/IDMRPT`
        - `/opt/netiq/idm/apps/tomcat/webapps/IDMRPT-CORE`
        - `/opt/netiq/idm/apps/tomcat/webapps/rptdoc`
    - (Conditional) If you installed Workflow Engine on the same server as Identity Governance, you must delete the following files and folders that Workflow Engine installed.
        - `/opt/netiq/idm/apps/wfe`
        - `/opt/netiq/idm/apps/tomcat/webapps/wfconsole`
        - `/opt/netiq/idm/apps/tomcat/webapps/wfdocs`
        - `/opt/netiq/idm/apps/tomcat/webapps/workflow`
    - Delete the contents of the following folders including any subdirectories.
        - `/opt/netiq/idm/apps/tomcat/work/Catalina/localhost`
        - `/opt/netiq/idm/apps/tomcat/temp`
- **Windows:** The default path is `C:\netiq\idm\apps`.
    - `C:\netiq\idm\apps\idgov`
    - `C:\netiq\idm\apps\tomcat\webapps\api`
    - `C:\netiq\idm\apps\tomcat\webapps\apidoc`
    - `C:\netiq\idm\apps\tomcat\webapps\cx`
    - `C:\netiq\idm\apps\tomcat\webapps\daas`
    - `C:\netiq\idm\apps\tomcat\webapps\dtp`
    - `C:\netiq\idm\apps\tomcat\webapps\formbuilder`
    - `C:\netiq\idm\apps\tomcat\webapps\ROOT`

- `C:\netiq\idm\apps\tomcat\webapps\doc`
- `C:\netiq\idm\apps\tomcat\webapps\workflow-api`
- (Conditional) If you installed Identity Reporting on the same server as Identity Governance, you must delete the following files and folders that Identity Reporting installed.
    - `C:\netiq\idm\apps\idrpt`
    - `C:\netiq\idm\apps\tomcat\webapps\IDMRPT`
    - `C:\netiq\idm\apps\tomcat\webapps\IDMRPT-CORE`
    - `C:\netiq\idm\apps\tomcat\webapps\rptdoc`
- (Conditional) If you installed Workflow Engine on the same server as Identity Governance, you must delete the following files and folders that Workflow Engine installed.
    - `C:\netiq\idm\apps\wfe`
    - `C:\netiq\idm\apps\tomcat\webapps\wfconsole`
    - `C:\netiq\idm\apps\tomcat\webapps\wfdocs`
    - `C:\netiq\idm\apps\tomcat\webapps\workflow`
- Delete the contents of the following folders including any subdirectories.
    - `C:\netiq\idm\apps\tomcat\work\Catalina\localhost`
    - `C:\netiq\idm\apps\tomcat\temp`

8 Restart Apache Tomcat, if needed. For more information, see Section 3.5.3, “Starting and Stopping Apache Tomcat,” on page 50.

14.3 Uninstalling Identity Reporting

The installation utility for Identity Governance and Identity Reporting places an uninstall utility on the server for Identity Reporting if you installed Identity Reporting on a separate server from Identity Governance. If you installed Identity Reporting on the same server as Identity Governance you must use the Identity Governance uninstall utility to uninstall Identity Reporting and Identity Governance. For more information, see Section 14.2, “Uninstalling Components Installed with the Identity Governance Installer,” on page 281.

You would uninstall Identity Reporting if you want to move to new hardware, you want to run Identity Reporting on a separate server, or if you are upgrading to the latest version of Identity Governance. If you install Identity Reporting on a separate server, use the uninstall utility that was installed when you installed Identity Reporting to uninstall it.

If you installed Identity Reporting on the same server as Identity Governance and Identity Reporting impacts the performance of Identity Governance, you can move Identity Reporting to a separate server but it is a process. For more information, see Section 13.5, “Moving Identity Reporting to a Separate Server,” on page 276.

The Identity Reporting uninstall utility provides the guided uninstall, the console uninstall, and the silent uninstall just like the installer utility does. The default mode of the uninstall utility is the method that you used to install Identity Reporting. If you want to uninstall using a different method you must pass the appropriate parameter to perform that type of uninstallation. For more information, see Section 1.3, “Understanding the Uninstallation Methods,” on page 22.

Use the following procedure to uninstall Identity Reporting if you installed on a separate server from Identity Governance.

To uninstall Identity Reporting when it is installed on a separate server from Identity Governance:

1 Log in to the server running Identity Reporting as `root` on a Linux server or as a user with administrative privileges on a Windows server.

2 Define the Java path to the `jre bin` directory as an environment variable in the uninstall script file that launches the uninstall utility.

IMPORTANT: If you do not define the path to the `jre bin` directory, the uninstall utility does not work. The utility does not come with Java. You must point to the Java you use with Identity Governance.

2a Open the uninstall script file in a text editor. The default location is:

- **Linux:** `/opt/netiq/idm/apps/idrpt/Uninstall_IdentityGovernance/LaunchUninstall.sh`
- **Windows:**

  `c:\netiq\idm\apps\idrpt\Uninstall_IdentityGovernance\LaunchUninstall.bat`

2b Change or ensure that the path listed for the `JRE_HOME` variable is the path to the `jre bin` directory for the Zulu JRE that is installed with the Zulu OpenJDK. The default path is:

- **Linux:** `/opt/netiq/idm/apps/jre/bin`
- **Windows:** `c:\netiq\idm\apps\jre\bin`

2c Save and close the file.

3 Stop Apache Tomcat. For more information, see Section 3.5.3, “Starting and Stopping Apache Tomcat,” on page 50.

4 (Conditional) If you are running any version of Identity Governance prior to 3.0, you must use a different uninstall utility for Identity Reporting.

4a (Conditional) Uninstall Identity Reporting on a Linux server.

4a1 Access the uninstall directory. The default location is: `/opt/netiq/idm/apps/idrpt/Uninstall_IdentityGovernance`.

4a2 To execute the script, enter:

```
./LaunchUninstall.sh
```

4b (Conditional) Uninstall Identity Reporting on a Windows server.

4b1 Access the **Control Panel** as an administrator.

4b2 Search for Identity Reporting.

4b3 Click **Uninstall** and follow the prompts to uninstall Identity Reporting.

5 (Conditional) Uninstall Identity Reporting if your version of Identity Governance is 3.0 or later.

- **5a** (Conditional) Uninstall Identity Reporting from a Linux server.
  - **5a1** Access the uninstall directory located here: `/opt/netiq/idm/apps/idrpt/Uninstall_IdentityGovernance`
  - **5a2** Execute the script as `root` from a command line enter the following:

    ```
    ./LaunchUninstall.sh
    ```

- **5b** (Conditional) Uninstall Identity Reporting on a Windows server.
  - **5b1** Access the **Control Panel** as an administrator.
  - **5b2** Search for and select Identity Governance.
  - **5b3** Select **Uninstall** and follow the prompts to complete the uninstallation.

6 When the uninstallation completes, delete the following folders. The uninstall utility restores the `*.war` files that were in this directory before you installed Identity Reporting.

- **Linux:** The default path is `/opt/netiq/idm/apps`.
  - `/opt/netiq/idm/apps/idrpt`
  - `/opt/netiq/idm/apps/tomcat/webapps/IDMRPT`
  - `/opt/netiq/idm/apps/tomcat/webapps/IDMRPT-CORE`
  - `/opt/netiq/idm/apps/tomcat/webapps/rptdoc`
  - Delete the contents of the following folders including any subdirectories.
    - `/opt/netiq/idm/apps/tomcat/work/Catalina/localhost`
    - `/opt/netiq/idm/apps/tomcat/temp`
- **Windows:** The default path is `C:\netiq\idm\apps`.
  - `C:\netiq\idm\apps\idrpt`
  - `C:\netiq\idm\apps\tomcat\webapps\IDMRPT`
  - `C:\netiq\idm\apps\tomcat\webapps\IDMRPT-CORE`
  - `C:\netiq\idm\apps\tomcat\webapps\rptdoc`
  - Delete the contents of the following folders including any subdirectories.
    - `C:\netiq\idm\apps\tomcat\work\Catalina\localhost`
    - `C:\netiq\idm\apps\tomcat\temp`

7 Restart Apache Tomcat, if needed. For more information, see Section 3.5.3, “Starting and Stopping Apache Tomcat,” on page 50.

14.4 Uninstalling the Workflow Engine

The installation utility for Identity Governance and the Workflow Engine places an uninstall utility on the server for the Workflow Engine. If you have installed the Workflow Engine on a separate server, use the uninstall utility that was installed when you install the Workflow Engine.

If you installed the Workflow Engine on the same server as Identity Governance you must use the Identity Governance uninstall utility to uninstall the Workflow Engine and Identity Governance. For more information, see Section 14.2, "Uninstalling Components Installed with the Identity Governance Installer," on page 281.

While uninstalling, you must uninstall the features in the reverse order in which you installed them. For example, if you installed Identity Governance, then Workflow Engine, you must uninstall Workflow Engine, then Identity Governance.

The Workflow Engine uninstall utility provides the guided uninstall, the console uninstall, and the silent uninstall just like the installer utility does. The default mode of the uninstall utility is the method that you used to install. If you want to uninstall using a different method you must pass the appropriate parameter to perform that type of uninstallation. For more information, see Section 1.3, "Understanding the Uninstallation Methods," on page 22.

If the Workflow Engine is on the same server as Identity Governance and the Workflow Engine impacts the performance of Identity Governance, you can move the Workflow Engine to a separate server. For more information, see Section 13.6, "Moving Workflow Engine to a Separate Server," on page 277.

Use the following procedure to uninstall the Workflow Engine if you installed on a separate server from Identity Governance.

To uninstall the Workflow Engine when it is installed on a separate server from Identity Governance

1 Log in as an administrator on the server from where you want to uninstall the Workflow Engine.

2 Define the Java path to the `jre/bin` directory as an environment variable in the uninstall script file that launches the uninstall utility.

2a Open the uninstall script file in a text editor. The default location is:

- **Linux:** `/opt/netiq/idm/apps/wfe/Uninstall_IdentityGovernance/LaunchUninstall.sh`
- **Windows:**

  `c:\netiq\idm\apps\wfe\Uninstall_IdentityGovernance\LaunchUninstall.bat`

2b Change or ensure that the path listed for the `JRE_HOME` variable is the path to the `jre/bin` directory for the Zulu JRE that is installed with the Zulu OpenJDK. The default path is:

- **Linux:** `/opt/netiq/idm/apps/jre/bin`
- **Windows:** `c:\netiq\idm\apps\jre\bin`

2c Save and close the file.

3 Stop Apache Tomcat. For more information, see Section 3.5.3, "Starting and Stopping Apache Tomcat," on page 50.

4 Uninstall Workflow Engine if your version of Identity Governance is 3.0 or later.

4a (Conditional) Uninstall Workflow Engine from a Linux server.

4a1 Access the uninstall directory located here: `/opt/netiq/idm/apps/wfe/Uninstall_IdentityGovernance`.

4a2 Execute the script as `root` from a command line enter the following:

```
./LaunchUninstall.sh
```

4b (Conditional) Uninstall Workflow Engine on a Windows server.

4b1 Access the **Control Panel** as an administrator.

4b2 Search for Workflow Engine.

4b3 Select **Uninstall** and follow the prompts to complete the uninstallation.

5 When the uninstallation completes, delete the following folders.

NOTE: The uninstall utility restores the `*.war` files that were in this directory before you installed the Workflow Engine.

- **Linux:** The default path is `/opt/netiq/idm/apps`:
  - `/opt/netiq/idm/apps/wfe`
  - `/opt/netiq/idm/apps/tomcat/webapps/wfconsole`
  - `/opt/netiq/idm/apps/tomcat/webapps/wfdocs`
  - `/opt/netiq/idm/apps/tomcat/webapps/workflow`

    Delete the contents of the following folders including any subdirectories:
    - `/opt/netiq/idm/apps/tomcat/work/Catalina/localhost`
    - `/opt/netiq/idm/apps/tomcat/temp`
- **Windows:** The default path is C:\netiq\idm\apps:
  - `C:\netiq\idm\apps\wfe`
  - `C:\netiq\idm\apps\tomcat\webapps\wfconsole`
  - `C:\netiq\idm\apps\tomcat\webapps\wfdoc`
  - `C:\netiq\idm\apps\tomcat\webapps\workflow`

  Delete the contents of the following folders including any subdirectories:
  - `C:\netiq\idm\apps\tomcat\work\Catalina\localhost`
  - `C:\netiq\idm\apps\tomcat\temp`

6 Restart Apache Tomcat, if needed. For more information, see Section 3.5.3, “Starting and Stopping Apache Tomcat,” on page 50.

15 Managing Identity Governance

After you have installed and configured Identity Governance, you must perform some configuration tasks using the administration utilities. There are additional management tasks that you might have to perform. Use the following information to help perform these tasks.

15.1 Accessing the Application and Administration Utilities

After you have installed the authentication service, Identity Governance, and optionally Identity Reporting, there are additional configuration tasks you must perform to allow your authorized users to start using Identity Governance. Plus, there are additional administration tasks to perform to complete the installation of these components.

Identity Governance provides different administration utilities: Identity Governance Configuration utility, Identity Governance Configuration Update utility, and the Identity Governance application and the Identity Reporting application, if you installed Identity Reporting. Use the following information to access the different administration utilities.

15.1.1 How to Log in to Identity Governance

Identity Governance is a web application that you access through a web browser. You access the URL you defined during the installation. The default URL for Identity Governance is:

- **Non-secure:** `http://`*`dns-name-Identity-Governance-server`*`:`*`8080`*
- **Secure:** `https://`*`dns-name-Identity-Governance-server`*`:`*`8443`*

If you are logged in and your access token times out, you see a popup message that requires you to re-authenticate or log out of the application. If you re-authenticate, Identity Governance displays the login screen in a separate window or browser tab. You must log in again to continue working in the Identity Governance application.

15.1.2 How to Log in to Identity Reporting

Identity Reporting is a web application that you access through a web browser. The default Identity Reporting URL is `https://`*`mycompany.mydomain.com`*`:`*`8443`*`/IDMRPT`.

To be able to log in to Identity Reporting, you must have the Reporting Administrator authorization, and you must assign a data source to Identity Reporting to use its features. For more information, see Section 9.4.1, “Assigning the Report Administrator Authorization,” on page 211.

15.1.3 How to Log in to the Workflow Administration Console

The Workflow Administration Console is a web application that you access through a web browser. The default URL is `https://`*`mycompany.mydomain.com`*`:`*`8443`*`/wfconsole.`

You can log into the Workflow Administration console using any login account, but to access all its features, you must have the Workflow Administrator authorization automatically granted to Bootstrap and Global administrators. For more information, see Understanding Authorizations in Workflow Service.

15.1.4 Using the Identity Governance Configuration Utility

The Identity Governance Configuration utility allows you to modify settings specifically for Identity Governance, such as the URL for Identity Governance.

The Identity Governance Configuration utility also allows to perform the following administration tasks:

- Specify an external provisioning system for workflows. For more information, see “Using Workflows to Fulfill the Changeset (https://www.microfocus.com/documentation/identity-governance/4.3/user-guide/fulfill-changesets.html#fulfill-changeset-workflow)” in the *Identity Governance User and Administration Guide*.
- Configure the settings for data collection and publication. For more information, see “Collecting Identities (https://www.microfocus.com/documentation/identity-governance/4.3/user-guide/collecting-identities.html)” and “Publishing the Collected Data (https://www.microfocus.com/documentation/identity-governance/4.3/user-guide/publishing-collected-data.html)” in the *Identity Governance User and Administration Guide*.
- Configure the settings to perform a bulk update of data. For more information, see “Understanding Bulk Data Update (https://www.microfocus.com/documentation/identity-governance/4.3/user-guide/b19xy91k.html#t4dma7zut07f)” in the *Identity Governance User and Administration Guide*.

You can run the Identity Governance Configuration utility in two different modes. The default mode provides a user interface with menu options to configure the different features and components of Identity Governance. The console mode is a command line option used only under the direction of Technical Support.

Use the following information to run the Identity Governance Configuration utility.

- Section 15.1.4.1, “Using the Default Mode of the Identity Governance Configuration Utility,” on page 291
- Section 15.1.4.2, “Understanding the Console Mode of the Identity Governance Configuration Utility,” on page 291
- Section 15.1.4.3, “Using the Identity Governance Configuration Utility in Console Mode,” on page 293

15.1.4.1 Using the Default Mode of the Identity Governance Configuration Utility

The default mode of the Identity Governance Configuration utility provides an interface which requires graphics to be enabled on the server running the utility. The utility provides menus that allow you to change the configuration setting you defined during the installation and to perform some administration tasks as well.

The Identity Governance Configuration utility default installation location is:

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

To run the Identity Governance Configuration utility you must access the utility from a command prompt as root on a Linux server or as a user with administrative privileges on a Windows server. Enter the following from the Identity Governance Configuration utility installation directory:

- **Linux:** `./configutil.sh -password` *`db_password`* `-storepass` *`encryption_keystore_password`*
- **Windows:** `configutil.bat -password` *`database_password`*

15.1.4.2 Understanding the Console Mode of the Identity Governance Configuration Utility

The Identity Governance Configuration utility console mode enables you to make uncommon, specific, or extensive changes to the application configuration that can potentially damage the application data.

Identity Governance uses configuration properties to define new features and to control what Identity Governance does with the application data. There are two different configuration types:

- **Node:** Node configuration properties reside in properties files Identity Governance places on the local file system of the Identity Governance server.
- **Global:** Global configuration properties reside in database tables that Identity Governance places in the database so that the information is the same for each Identity Governance node in a cluster.

When you run the utility in console mode, you are presented with a cursor and you must know the commands you want to use, the correct format of the commands, the correct property name, and the parameter to make any changes in console mode.

IMPORTANT: The proper format of the commands is to have the commands, parameters, and values separated by a space. The console mode only recognizes spaces. It does not recognize parentheses or commas.

Table 15-1 contains the list of commands that are currently used in the documentation.

WARNING: Identity Governance utility console mode enables you to make uncommon, specific, or extensive changes to the application configuration that can potentially damage the application data. Run the utility in console mode only under the guidance of Technical Support.

Table 15-1 *Identity Governance Configuration Utility Console Mode Commands*

Command	Parameter Name	Parameter Value	Description
`display-configs`	`prefix-filter`		Displays all the known configuration keys and values. If you use the `prefix-filter` parameter, you can filter the configuration keys and values by a known prefix. For example: `display-configs ism` Displays all of the properties that start with ism.

`add-property`	`configuration-type` (optional)
	`property-key`
	`property-value`
		`NODE` or `GLOBAL`
		`some.key`
		`some value`
			Adds a property with the node or global configuration type and adds the value you specify. For example:
			`add-property com.netiq.iac.access.request.enabled false`
			Disables the Access Request service for Identity Governance.

`set-property`	`property-key`
	`property-value`
		`some.key`
		`some value`
			Updates the value of an existing property that is identified with the property-key. For example:
			`set-property com.netiq.iac.analytics.roles.technical.MaxPermSize 10000`
			Sets the maximum permission size as 10000.

`exit`			Exits from the console mode and from the Identity Governance Configuration utility.

15.1.4.3 Using the Identity Governance Configuration Utility in Console Mode

The Identity Governance Configuration utility console mode does not require graphics on the server to run. The utility allows you to add and modify properties that reside in properties files stored on the local file system or in the database to add a new feature or change the behavior of Identity Governance. The console mode allows you to make uncommon, specific, or extensive changes to the application configuration that can potentially damage the application data.

WARNING: The Identity Governance Configuration utility console mode enables you to make uncommon, specific, or extensive changes to the application configuration that can potentially damage the application data. Run the utility in console mode only under the guidance of Technical Support.

To use the Identity Governance Configuration utility in console mode:

1. Access the installation directory for the utility from a command prompt as user with `root` access on a Linux server or administrative privileges on a Windows server. The default installation directory is:
   - **Linux:** `/opt/netiq/idm/apps/idgov/bin`
   - **Windows:** `c:\netiq\idm\apps\idgov/bin`
2. From the command line, enter:
   - **Linux:** `./configutil.sh -password` *`db_password`* `-storepass` *`encryption_keystore_password`* `-console`
   - **Windows:** `configutil.bat -password` *`database_password`* `-console`
3. Use the information in Table 15-1, "Identity Governance Configuration Utility Console Mode Commands," on page 292 to issue the commands properly.
4. When you have performed the required changes, type `exit` to exit console mode and the Identity Governance Configuration utility.

15.1.5 Using the Identity Governance Configuration Update Utility

Three of the Identity Governance components use the Identity Governance Configuration Update utility to change settings instead of using the Identity Governance Configuration utility. There is a separate utility because the Identity Governance Configuration utility allows more granular and scripted functionality for manipulating properties than the Identity Governance Configuration Update utility can currently offer. The three components that use the Identity Governance Configuration Update utility are:

- One SSO Provider (OSP)
- Identity Reporting
- Auditing

If the path to the Identity Governance Configuration Update utility is unknown to the current installer, then the installer will prompt you to specify its location during the installation of Identity Governance. The default location is:

- **Linux:** `/opt/netiq/idm/apps/configupdate/configupdate.sh`
- **Windows:** `C:\netiq\idm\apps\configupdate\configupdate.bat`

You can run the Identity Governance Configuration Update utility in console mode or guided mode. The console mode provides menu-based options to walk through to update the settings. You would use the Identity Governance Configuration Update utility in console mode if your Linux server did not have graphical capabilities (X server).

To run the Identity Governance Configuration Update utility access the `configupdate` directory from a command prompt.

- **Linux:** Enter the following at the command prompt:
  - **Guided:** `./configupdate.sh --use-console false`
  - **Console:** `./configupdate.sh --use-console true`
- **Windows:** Enter the following at the command prompt:
  - **Guided:** `configupdate.bat --use-console false`
  - **Console:** `configupdate.bat --use-console true`

The Identity Governance Configuration Update utility console mode is different from the Identity Governance Configuration utility console mode. The Identity Governance Configuration Update utility provides menu-based options to update the settings in the three products. The Identity Governance Configuration Update utility does not have command options like the Identity Governance Configuration utility does.

15.2 Managing the Bootstrap Administrator

You define the bootstrap administrator during the installation process. Identity Governance allows you to create a new bootstrap administrator in certain scenarios, change the password, and change the details of the bootstrap administrator after you have completed the installation. Use the following information to perform those actions.

- Section 15.2.1, “Creating a Bootstrap Administrator Using a Script,” on page 294
- Section 15.2.2, “Changing the Password for the Bootstrap Administrator,” on page 295
- Section 15.2.3, “Changing the Details of the Bootstrap Administrator,” on page 296

15.2.1 Creating a Bootstrap Administrator Using a Script

You would use the bootstrap administrator script to create a new bootstrap administrator account in the following scenarios:

- If you are using the Identity Manager OSP instead of the OSP that comes with Identity Governance.
- If you specify LDAP for the bootstrap administrator during the installation and want to change to using a file-based bootstrap administrator.

If you are going to use the bootstrap administrator script, you must use it after the OSP and Identity Governance installations complete. The Identity Governance installer places the script on the Identity Governance server. The bootstrap administrator script contains links that the installer configures relative to the JARs that the installer creates during the Identity Governance installation.

The default location of the bootstrap administrator script is:

- **Linux:** `/opt/netiq/idm/apps/idgov/bin/bootstrap-file-gen.sh`

- **Windows:** `C:\netiq\idm\apps\idgov\bin\bootstrap-file-gen.bat`

You use the bootstrap administrator script with parameters that define an alternate name for the administrator account, the password for the administrator account, and the location of the bootstrap administrator file. The following table lists the parameters, the default values, and a description of the parameter. If you run the script but do not use the parameters, the script uses the default values.

Table 15-2 *Bootstrap Administrator Script Parameters*

Parameter	Default Value	Description
-p	None	You must use this option with a password to set the password for the bootstrap administrator account.
-u	igadmin	Defines an alternate user name for the bootstrap administrator account.
-f	File name with the relative or absolute path	Defines the file location to redirect the bootstrap credentials.

To run the bootstrap administrator script:

1 Access the command line utility on the Identity Governance server.

2 Access the directory where the installer placed the bootstrap administrator script.

- **Linux:** `/opt/netiq/idm/apps/idgov/bin/`
- **Windows:** `C:\netiq\idm\apps\idgov\bin\`

3 Execute the script with the appropriate parameters for your environment. For example:

- **Linux:** ./bootstrap-file-gen.sh -p *password* -u *bootstrap administrator name* -f *`/opt/netiq/idm/apps/idgov/`*`adminusers.txt`
- **Windows:** bootstrap-file-gen -p *password* -u *bootstrap administrator name* -f *`C:\netiq\idm\apps\idgov\`*`adminusers.txt`

4 Restart Apache Tomcat to have the change take effect. For an example, see Section 3.5.3, "Starting and Stopping Apache Tomcat," on page 50.

15.2.2 Changing the Password for the Bootstrap Administrator

If you have the bootstrap administrator coming from the file system, you can change the password using the bootstrap administrator script. If you use an LDAP-based bootstrap, you must update the password stored within the LDAP server. Use the following steps to change the password if you use OSP as the authentication service and file-based bootstrap administrator where the system stores the credentials within a file.

1 Run the bootstrap administrator script from a command line as follows:

- **Linux:** ./bootstrap-file-gen.sh -p *password*
- **Windows:** bootstrap-file-gen -p *password*

2 (Conditional) If OSP runs on a separate server than Identity Governance, copy the `adminusers.txt` file to the OSP server and place it in the following directory:

- **Linux:** `/opt/netiq/idm/apps/osp/osp-extras/adminusers.txt`

- **Windows:** `c:\netiq\idm\apps\osp\osp-extras\adminusers.txt`

  The Identity Governance Configuration Update utility displays the path to this directory under **Advanced Options**. To see the path, click the **Authentication** tab, then **Identity Governance Bootstrap Administrator**.

3 Restart Apache Tomcat on the server running OSP. For more information, see Section 3.5.3, “Starting and Stopping Apache Tomcat,” on page 50.

15.2.3 Changing the Details of the Bootstrap Administrator

Identity Governance allows to you change if the bootstrap administrator is file-based or LDAP-based after the installation without having to run the installation a second time. You use the Identity Governance Configuration utility to make these changes.

1 From a command prompt, launch the Identity Governance Configuration utility with the database password. For more information, see Section 15.1.4, “Using the Identity Governance Configuration Utility,” on page 290.

2 Click the **Authentication Server Details** tab.

3 (Conditional) Change the bootstrap administrator to be file-based.

3a Select **Bootstrap Admin > Authentication Source > File**.

3b In **Bootstrap Admin > Name**, specify the name for the bootstrap administrator. The default name is `igadmin`.

3c In **Bootstrap Admin > Directory**, specify the directory where the file is located that stores your bootstrap administrator information. The default location is:

- **Linux:** `/opt/netiq/idm/apps/idgov/osp/adminusers.txt`
- **Windows:** `c:\netiq\idm\apps\idgov\osp\adminusers.txt`

3d In **Bootstrap Admin > Filename**, specify the file name for the bootstrap administrator. The default name is `adminusers.txt`.

3e Click **Save** to save the changes.

4 (Conditional) Change the bootstrap administrator to be LDAP-Based.

4a Select **Bootstrap Admin > Authentication Source > Identity Vault**.

4b In **Bootstrap Admin > Name**, specify the fully qualified domain name of a unique administrator user in LDAP. 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.

4c Click **Save**.

15.3 Changing the Values for Authentication Matching and Identity Governance Services

Identity Governance allows you to define the values it uses for authentication matching and the values for the services it runs.

1. From a command prompt launch the Identity Governance Configuration utility with the database password. For more information, see Section 15.1.4, “Using the Identity Governance Configuration Utility,” on page 290.
2. Click the **Security Settings** tab.
3. Use the information from the security settings table to define the values for authentication matching.
4. Click **Save**.

15.3.1 Understanding the Security Setting Values Used for Authentication

Identity Governance allows you to define the values for authentication method in the Identity Governance Configuration utility. Use the following table to understand the values while setting the authentication method:

Table 15-3 Security Settings Values for Authentication

Values	Description
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 the authentication service. 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 "Extending the Identity Governance Schema" in the *Identity Governance User and Administration Guide*.
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.

Values	Description
SSO Client	Defines the values for the Identity Governance SSO client. You must define the values of the SSO client service for the following items: **IG Client ID**: Specifies the name that you want to use to identify the Identity Governance SSO client ID. The default value is `iac`. **IG Client Secret**: Specifies the password for the data transformation service. **Response types**: Defines what the data transformation service uses for a response. The default response type is `client_credentials`.
General Service	Defines the values for the Identity Governance general service. You must define the values of the general service for the following items: **IG Client ID**: Specifies the name that you want to use to identify the Identity Governance general service. The default value is `iac-service`. **IG Client Secret**: Specifies the password for the Identity Governance general service ID. **Response types**: Defines what the general service uses for a response. The default response type is `client_credentials`.
Data Collection Service	Define the values for the data collection service. You must define the values of the data collection service for the following items: **IG Client ID**: Specifies the name that you want to use to identify the data collection service. The default value is `iac-daas`. **IG Client Secret**: Specifies the password for the data collection service. **Response types**: Defines what the data collection service uses for a response. The default response type is `client_credentials`.

Values	Description
Data Transformation Service	Define the values for the data transformation service. You must define the values of the data transformation service for the following items: **IG Client ID**: Specifies the name that you want to use to identify the data transformation service. The default value is `iac-dtp`. **IG Client Secret**: Specifies the password for the data transformation service. **Response types**: Defines what the data transformation service uses for a response. The default response type is `client_credentials`.
Workflow Service	Define the values for the workflow server. You must define the values of the workflow service for the following items: **IG Client ID**: Specifies the name that you want to use to identify the workflow service. The default value is `wf`. **IG Client Secret**: Specifies the password for the worflow service. **Response types**: Defines what the data transformation service uses for a response. The default response type is `client_credentials`.
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.

15.4 Managing Connected Systems Information

Identity Governance allows you to use the Identity Governance Configuration utility to change the information for the Identity Vault if you integrated with Identity Manager.

If you need to change the network settings for your identity service, you must change the information in the Identity Governance Configuration Update utility.

To change the identity service information:

1. Launch the Identity Governance Configuration Update utility. For more information, see Section 15.1.5, "Using the Identity Governance Configuration Update Utility," on page 293.
2. Click the **Reporting** tab.
3. Use the following information to change the LDAP Identity Vault configuration information:

   Identity Vault Server

      Specify the fully qualified DNS name of the identity service server.

LDAP Port

Specify the LDAP port you identity service server uses to communicate.

Identity Vault Administrator

Specify the fully qualified DN of the administrator account in your identity service.

Identity Vault Password

Specify the password for your identity service administrator account.

Secure Administrator Connection

Select this option to communicate securely with the identity service.

4 Change where Identity Governance searches for the users in the identity service under the **Identity Vault User Identity** heading using the following information:

User Container DN

Specify the fully qualified DN of the user container in the identity service where Identity Governance starts searching for users.

Login Attribute

Specify the name of the login attribute Identity Governance uses to search for unique user accounts.

User Search Scope

Select the type of search Identity Governance performs of the identity service for the user accounts.

5 Click **Save**.

15.5 Changing Network Settings for Identity Governance Components

Identity Governance allows you to change your network setting or the runtime instance settings after you have completed the installation. You change the network setting for the different Identity Governance components in different utilities, and there are multiple places that you must ensure that you change the network setting to have it take effect.

You must change your network setting on the servers running the different Identity Governance components. You must then perform the following additional steps to change the network settings for the Identity Governance components.

You must perform the following steps for each component, even if the components reside on the same server. The different components contain different settings that store networking information. Use the following information to change the Identity Governance network settings for the different Identity Governance components.

- Section 15.5.1, “Changing the Network Settings for Identity Governance,” on page 302
- Section 15.5.2, “Changing the Network Settings for the Authentication Service,” on page 303
- Section 15.5.3, “Changing the Networking Settings for Identity Reporting,” on page 306
- Section 15.5.4, “Changing the Network Settings for the Workflow Engine,” on page 307

15.5.1 Changing the Network Settings for Identity Governance

You change the network settings for Identity Governance through the Identity Governance Configuration utility. You must change the settings in multiple locations to ensure that Identity Governance uses the new network settings.

To change the network settings:

1. Update the IP address and DNS name of the server and Apache Tomcat using the server and Apache Tomcat documentation.
2. Stop Apache Tomcat. For more information, see Section 3.5.3, "Starting and Stopping Apache Tomcat," on page 50.
3. (Conditional) If you clustered Identity Governance stop Apache Tomcat on each node in the cluster.
4. Update the DNS names in the `setenv` script that sets the environment variables for Apache Tomcat.

   4a Open the `setenv` file in a text editor. The default location of the file is:

   - **Linux:** `/opt/netiq/idm/apps/tomcat/bin/setenv.sh`
   - **Windows:** `C:\netiq\idm\apps\tomcat\bin\setenv.bat`

   4b Change the IP address or DNS name associated with `com.netiq.idm.osp.client.host` to the new fully-qualified DNS name.

   4c Save and close the file.
5. (Conditional) If you clustered Identity Governance repeat Step 4 on each node of the cluster.
6. Update the DNS names in the `ism-configuration.properties` file.

   6a Open the `ism-configuration.properties` file in a text editor.

   - **Linux:** `/opt/netiq/idm/apps/tomcat/conf/ism-configuration.properties`
   - **Windows:** `C:\netiq\idm\apps\tomcat\conf\ism-configuration.properties`

   6b Change the IP address or DNS name associated with the following attributes to the new fully-qualified DNS name:

   - `com.netiq.idm.osp.url.host`
   - `com.netiq.iac.url.local.host`
   - `com.netiq.rpt.authserver.url`
   - `com.netiq.rpt.access.review.url`
   - `com.netiq.rpt.landing.url`
   - `com.netiq.rpt.rpt-web.redirect.url`

   6c Save and close the file.
7. (Conditional) If you clustered Identity Governance repeat Step 6 on each node in the cluster.

8 Update the DNS names in the Identity Governance Configuration utility.

8a Ensure that the Identity Governance database is running.

8b Start the Identity Governance Configuration utility with the database password. The default location is:

- **Linux:** `/opt/netiq/idm/apps/idgov/bin/configutil.sh`
- **Windows:** `C:\netiq\idm\apps\idgov\bin\configutil.bat`

For example, use the following command in Linux environments:

```
./configutil.sh -password db_password -storepass
encryption_keystore_password
```

8c Change the IP address or DNS name associated with the following attributes on the specified tabs to the new fully-qualified DNS name:

Tab	Setting
Authentication Server Details	◆ IG Redirect URL ◆ IG Request Redirect URL
Network Topology	Nodes Host Name
Workflow Settings	JMS broker URI

8d Exit the utility.

9 (Conditional) If you have clustered Identity Governance repeat Step 8 on each node in the cluster.

IMPORTANT: Do not restart Apache Tomcat until the networking settings have been changed for each node in the cluster.

10 Start Apache Tomcat.

11 (Conditional) If you clustered Identity Governance start Apache Tomcat on each node in the cluster.

15.5.2 Changing the Network Settings for the Authentication Service

The steps to change the network settings for the authentication service depend on which authentication service you are using. Use the following information to change the network settings for your authentication service:

- Section 15.5.2.1, “Changing the Network Settings for OSP,” on page 304
- Section 15.5.2.2, “Changing the Network Settings for Access Manager,” on page 305

15.5.2.1 Changing the Network Settings for OSP

To change the network setting for OSP requires that you change the network settings for the server or servers running OSP and change the network setting in Apache Tomcat.

To change the network settings for OSP:

1. Update the IP address and DNS name of the server and Apache Tomcat using the server and Apache Tomcat documentation.
2. Stop Apache Tomcat on the OSP server. For more information, see Section 3.5.3, "Starting and Stopping Apache Tomcat," on page 50.
3. (Conditional) If you have clustered OSP stop Apache Tomcat on each node in the cluster.
4. Update the DNS names in the `setenv` script that sets the environment variables for Apache Tomcat.

   4a Open the `setenv` file in a text editor. The default location of the file is:

   - **Linux:** `/opt/netiq/idm/apps/tomcat/bin/setenv.sh`
   - **Windows:** `C:\netiq\idm\apps\tomcat\bin\setenv.bat`

   4b Change the IP address or DNS name associated with `com.netiq.idm.osp.client.host` to the new fully-qualified DNS name.

   4c Save and close the file.
5. (Conditional) If you clustered OSP repeat Step 4 on each node in the cluster.
6. Update the DNS names in the `ism-configuration.properties` file.

   6a Open the `ism-configuration.properties` file in a text editor.

   - **Linux:** `/opt/netiq/idm/apps/tomcat/conf/ism-configuration.properties`
   - **Windows:** `C:\netiq\idm\apps\tomcat\conf\ism-configuration.properties`

   6b Change the IP address or DNS name associated with the following attributes to the new fully-qualified DNS name:

   - `com.netiq.idm.osp.url.host`
   - `com.netiq.iac.url.local.host`
   - `com.netiq.rpt.authserver.url`
   - `com.netiq.rpt.access.review.url`
   - `com.netiq.rpt.landing.url`
   - `com.netiq.rpt.rpt-web.redirect.url`

   6c Save and close the file.
7. (Conditional) If you clustered OSP repeat Step 6 on each node in the cluster.
8. Update the DNS name in the Identity Governance Configuration Update utility.

   8a Launch the Identity Governance Configuration Update utility on the Identity Governance server. For more information, see Section 15.1.5, "Using the Identity Governance Configuration Update Utility," on page 293.

   8b Click the **Authentication** tab.

- **8c** Click **Show Advanced Options** at the end of the page.
- **8d** Update the OAuth server host and OAuth ports with the new fully qualified DNS name and port.
- **8e** Update the truststore file path and password for the new certificate.
- **8f** Click **OK** to save the changes and the Identity Governance Configuration Update utility automatically closes.

9 (Conditional) If you clustered OSP repeat Step 8 on each node in the cluster.

IMPORTANT: Do not restart Apache Tomcat until the networking settings have been changed for each node in the cluster.

---

10 Start Apache Tomcat.

11 (Conditional) If you clustered OSP start Apache Tomcat on each node in the cluster.

15.5.2.2 Changing the Network Settings for Access Manager

To change the network setting for Access Manager requires that you change the networking setting in Access Manager first and then make the changes in Identity Governance.

To change the network settings for Access Manager:

1. Update the IP address and DNS name of the server and Apache Tomcat using the server and Apache Tomcat documentation.
2. Change the IP address and DNS name in Access Manager. For more information, see "Configuring Access Manager "in the *NetIQ Access Manager 5.0 Administration Guide*.
3. Stop Apache Tomcat on the Identity Governance server. For more information, see Section 3.5.3, "Starting and Stopping Apache Tomcat," on page 50.
4. (Conditional) If you have clustered Identity Governance stop Apache Tomcat on each node in the cluster.
5. Update the DNS name in the Identity Governance Configuration Update utility.
   - **5a** Launch the Identity Governance Configuration Update utility on the Identity Governance server. For more information, see Section 15.1.5, "Using the Identity Governance Configuration Update Utility," on page 293.
   - **5b** Click the **Authentication** tab.
   - **5c** Click **Show Advanced Options** at the end of the page.
   - **5d** Update the OAuth server host and OAuth ports with the new Access Manager fully qualified DNS name and port.
   - **5e** Update the truststore file path and password for the new certificate.
   - **5f** Click **OK** to save the changes and the Identity Governance Configuration Update utility automatically closes.
6. (Conditional) If you have clustered Identity Governance repeat Step 5 on each node in the cluster.

IMPORTANT: Do not restart Apache Tomcat until the networking settings have been changed for each node in the cluster.

---

7 Start Apache Tomcat.

8 (Conditional) If you clustered Identity Governance start Apache Tomcat on each node in the cluster.

15.5.3 Changing the Networking Settings for Identity Reporting

You can change the networking settings for Identity Reporting. You must perform the following steps if you have Identity Reporting installed on the same server as Identity Governance or if it is installed on a separate server.

To change the network settings for Identity Reporting:

1 Update the IP address and DNS name of the server and Apache Tomcat using the server and Apache Tomcat documentation.

2 (Conditional) If you clustered Identity Reporting ensure that you change the IP address and DNS name of each node in the cluster and each instance of Apache Tomcat using the server and Apache Tomcat documentation.

3 Stop Apache Tomcat. For more information, see Section 3.5.3, “Starting and Stopping Apache Tomcat,” on page 50.

4 (Conditional) If you clustered Identity Reporting, stop Apache Tomcat on each node in the cluster.

5 Update the DNS names in the `ism-configuration.properties` file.

5a Open the `ism-configuration.properties` file in a text editor.

- **Linux:** `/opt/netiq/idm/apps/tomcat/conf/ism-configuration.properties`
- **Windows:** `C:\netiq\idm\apps\tomcat\conf\ism-configuration.properties`

5b Change the IP address or DNS name associated with the following attributes to the new fully-qualified DNS name:

- `com.netiq.idm.osp.url.host`
- `com.netiq.rpt.access.review.url`
- `com.netiq.rpt.landing.url`
- `com.netiq.rpt.rpt-web.redirect.url`

5c Save and close the file.

6 (Conditional) If you clustered Identity Reporting repeat Step 5 on each node in the cluster.

7 Update the DNS Name in the Identity Governance Configuration Update utility.

7a Launch the Identity Governance Configuration Update utility. For more information, see Section 15.1.5, “Using the Identity Governance Configuration Update Utility,” on page 293.

7b Click the **Reporting** tab.

7c Scroll down, in **Landing Page > URL link to landing page** specify the new fully qualified hostname of the Apache Tomcat instances that runs Identity Reporting including the port.

7d Ensure that **Reporting Administrators > URL link to Identity Governance** contains the proper URL to access Identity Governance.

7e (Conditional) If you use a reverse proxy server for Identity Reporting in the **Outbound Proxy > Use proxy** field, ensure that the connection information to the reverse proxy server is correct.

7f Click **OK** to save the changes and the Identity Governance Configuration Update utility automatically closes.

8 (Conditional) If you have clustered Identity Reporting repeat Step 7.

IMPORTANT: Do not restart Apache Tomcat until the networking settings have been changed for each Identity Reporting node in the cluster.

---

9 Start Apache Tomcat.

10 (Conditional) If you have clustered Identity Reporting start Apache Tomcat on each node in the cluster.

15.5.4 Changing the Network Settings for the Workflow Engine

If the Workflow Engine is installed on the same server as Identity Governance or if it is installed on a separate server, you can change the networking settings. You must perform the following steps for each server where you installed the Workflow Engine.

To change the network settings for Workflow Engine:

1 Update the IP address, DNS name of the server, and Apache Tomcat using the server and Apache Tomcat documentation.

2 (Conditional) If you clustered the Workflow Engine ensure that you change the IP address and DNS name of each node in the cluster and each instance of Apache Tomcat using the server and Apache Tomcat documentation.

3 Stop Apache Tomcat.

4 (Conditional) If you clustered Workflow Engine, stop Apache Tomcat on each node in the cluster. For more information, see Section 3.5.3, “Starting and Stopping Apache Tomcat,” on page 50.

5 Update the DNS names in the `ism-configuration.properties` file.

5a Open the `ism-configuration.properties` file in a text editor.

- **Linux:** `/opt/netiq/idm/apps/tomcat/conf/ism-configuration.properties`
- **Windows:** `C:\netiq\idm\apps\tomcat\conf\ism-configuration.properties`

5b Change the IP address or DNS name associated with the following attributes to the new fully-qualified DNS name:

- `com.netiq.idm.osp.url.host`
- `com.microfocus.idm.application.url`
- `com.microfocus.wfe.consumer.url`
- `com.netiq.idm.forms.url.host`
- `com.netiq.idm.wfconsole.url.host`

- `com.netiq.wfconsole.redirect.url`
- `com.netiq.client.authserver.url.logout`

5c Save and close the file.

6 (Conditional) If you have clustered the Workflow Engine, repeat Step 5 on each node in the cluster.

7 Start Apache Tomcat.

8 (Conditional) If you have clustered the Workflow Engine, start Apache Tomcat on each node in the cluster.

15.6 Increasing Logging Levels for Identity Governance and the Identity Governance Clients

You can increase the logging levels for Identity Governance and the Identity Governance clients to have a more granular view of the events occurring. OSP and Identity Reporting do not provide the granular view that Identity Governance provides.

Identity Governance allows you to set the following logging levels:

- Info
- Warning
- Error
- Fatal
- Debug
- Trace
- None

You can use the following information to enable or increase the logging levels for Identity Governance and Identity Governance clients, or you can use the Identity Governance Configuration menu to set logging levels. For more information, see “Managing Logging Levels (https://www.microfocus.com/documentation/identity-governance/4.3/user-guide/manage-logging.html)” in the *Identity Governance User and Administration Guide*.

- Section 15.6.1, “Increasing the Logging Levels for Identity Governance,” on page 309
- Section 15.6.2, “Increasing the Logging Levels for Identity Governance Client and Other Modules,” on page 310

15.6.1 Increasing the Logging Levels for Identity Governance

In prior releases of Identity Governance, you had to edit the `ig-server-logging.xml` file to add your audit server details, the TLS information, and to enable the auditing service. Now, you can use the Identity Governance Configuration Update utility to enable auditing. You can still edit part of the `ig-server-logging.xml` file to set the level of logging details provided by the auditing service in Identity Governance.

WARNING: Use the Identity Governance Configuration Update utility to change the server details, TLS settings, and to enable auditing. If you make changes for these options in the `ig-server-logging.xml` file, it can cause the Identity Governance Configuration Update utility to no longer affect the audit settings.

The `ig-server-logging.xml` file is an XML file. It contains three parts. You must understand what each part does and which part to edit and not to edit. The parts are listed by XML parent-child relationships.

- **audit/syslog:** This section contains the global auditing setting.

  WARNING: Use the Identity Governance Configuration Update utility to change the settings for the server details, TLS settings, and to enable auditing. If you make changes for these options in the `ig-server-logging.xml` file, it can cause the Configuration Update utility to no longer affect the audit settings.

- **audit/httpAuditData:** This section is a filter that indicates whether the audit event includes a copy of the HTTP request data, the HTTP response data, both, or only the ID. The options are:
  - **ALL:** The auditing log includes a copy of the HTTP request data, the HTTP response data, and the ID of the REST call.
  - **REQUEST:** The auditing log includes a copy of the HTTP request data.
  - **RESPONSE:** The auditing log includes a copy of the HTTP response data.
  - **ID_ONLY:** The auditing log includes only the ID of the REST call.
- **loggers:** This section contains all of the Identity Governance auditing and logging service. You edit this section to customize auditing and logging levels for your environment. There are four types of loggers. They are:
  - **Logger names not prefixed with "audit":** These loggers are regular and not auditing loggers. These loggers control standard logging output to the logging files such as INFO, DEBUG, ERROR, and so forth. You can add or remove this type of logger and adjust the logging level of each logger to what is appropriate for your environment or situation.
  - **Logger names prefixed with "audit" and ending in a class name:** These are the audit loggers that control specific REST services.

    The INFO level enables auditing for the services listed in the class name. Any other level turns off auditing for the service in Identity Governance.
  - **Logger names prefixed with "audit" and ending in an HTTP method (GET, PUT, POST, or DELETE):** These audit loggers enable auditing only for a specified HTTP method for the named class. You would use these loggers to show data modifications rather than only seeing the queries in the auditing logs.

For example, if you add three lines for the class `audit.com.netiq.iac.server.rest.CollectionService` appended with PUT, POST, and DELETE, the auditing log shows the data modification carried out by that service but the auditing logs would not contain any queries.

- **Logger names prefixed with “audit” and ending in an integer even ID:** These are a specific type of loggers that target only one method of a service class, as each method has a unique event ID. You can see a list of all of the events in the Audit Event Table (https://www.microfocus.com/documentation/identity-governance/4.3/tech-refs/AuditEventTable.pdf).

After you understand the loggers in the `ig-server-logging.xml` file, you can change the loggers that are appropriate for your environment.

To edit the `ig-server-logging.xml` file:

1. Open the `ig-server-logging.xml` file in a text editor. The default location is:
   - **Linux:** `/opt/netiq/idm/apps/tomcat/conf`
   - **Windows:** `C:\netiq\idm\apps\tomcat\conf`
2. Change the appropriate settings for the loggers for your environment.
3. Save and close the file.
4. Restart Apache Tomcat. For more information, see Section 3.5.3, “Starting and Stopping Apache Tomcat,” on page 50.

15.6.2 Increasing the Logging Levels for Identity Governance Client and Other Modules

Identity Governance contains application-specific logging configuration files to help obtain debugging information from the Identity Governance clients and other modules. In the past, you would have to add client-specific logging configuration information in the general Apache Tomcat `logging.properties` file. However, now you can edit the respective xml files.

The logging configuration files that you can edit and enable the loggers per the request of technical support are:

- `ig-client-logging.xml`
- `cx-client-logging.xml`
- `idm-rptclient-logging.xml`
- `ig-health-logging.xml`

Restart Apache Tomcat after editing these files.

15.7 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 to the Identity Governance application 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.

15.8 Adjusting Timeout Values to Increase Performance

Identity Governance allows you to adjust 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 work for the majority of installations.

1 From a command prompt launch the Identity Governance Configuration utility with the database password. For more information, see Section 15.1.4, “Using the Identity Governance Configuration Utility,” on page 290.

2 Click the **Miscellaneous Setting** tab.

3 In the **Data Production Timeouts** section, adjust the following settings as needed for your environment:

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.

4 Click **Save**.

A Ports Used in Identity Governance

Identity Governance uses the following ports by default:

Transport Protocol	TCP Port	Secure Channel
HTTP	8080	TLS
HTTPS	8443	TLS
LDAP(S)	389, 636 (OSP)	TLS
JDBC	1433 (Microsoft SQL Server) 1521 (Oracle) 5432 (PostgreSQL)	TLS
SMTP	25, 465, 587	TLS
AJP	8009	TLS
AMQP	61616 (IG)	TLS
Audit	6514 (default)	TLS
Shutdown Port	8005	TLS

If, in your environment, you use different ports, ensure that you change the ports during the installation to match your environment.

B Managing the Services the Installation Scripts Create

OpenText provides sample installation scripts that you can use to install the required components, the optional components, and Identity Governance. You can download the sample scripts from the Identity Governance documentation page under the **Reference** heading. The sample scripts install some of the components as services. If a product is a service, then starting and stopping the service is different from starting and stopping the regular product. Use the following information to manage the components that the sample scripts install as services.

- Section B.1, "Stopping, Starting, and Restarting the Apache Tomcat Service," on page 315
- Section B.2, "Stopping, Starting, and Restarting the ActiveMQ Service," on page 316

B.1 Stopping, Starting, and Restarting the Apache Tomcat Service

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

- Section B.1.1, "Linux Examples for the Apache Tomcat Service," on page 315
- Section B.1.2, "Windows Examples for the Apache Tomcat Service," on page 315

B.1.1 Linux Examples for the Apache Tomcat Service

To stop Apache Tomcat:

```
systemctl stop identity_tomcat.service
```

To start Apache Tomcat:

```
systemctl start identity_tomcat.service
```

To restart Apache Tomcat:

```
systemctl restart identity_tomcat.service
```

To show the status of Apache Tomcat.service:

```
systemctl status identity_tomcat.service
```

B.1.2 Windows Examples for the Apache Tomcat Service

To stop, start, or restart Apache 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 and select **IDM Apps Tomcat Service** and right-click, then 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.

B.2 Stopping, Starting, and Restarting the ActiveMQ Service

If you have installed ActiveMQ, Identity Governance starts it from within the Apache Tomcat service. Some installation and configuration tasks require stopping ActiveMQ before completing the steps and then starting it afterwards. The following examples guide these processes.

- Section B.2.1, "Linux Examples for the ActiveMQ Service," on page 316
- Section B.2.2, "Windows Examples for the ActiveMQ Service," on page 317

B.2.1 Linux Examples for the ActiveMQ Service

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
```

B.2.2 Windows Examples for the ActiveMQ Service

On Windows, you start, stop, and restart ActiveMQ by starting, stopping, and restarting Apache Tomcat. For more information, see “Stopping, Starting, and Restarting the Apache Tomcat Service” on page 315.