NetIQ Identity Governance

Installation Guide

February 2020

Legal Notice

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

Copyright © 2020 NetIQ Corporation, a Micro Focus company. All Rights Reserved.

About this Book and the Library

The *Installation Guide* provides installation and initial configuration information for the NetIQ 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:

Release Notes

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

Administrator Guide

Provides conceptual information and step-by-step guidance for administrative tasks in the Identity Governance product. Specifically, it provides instructions for the following Identity Governance users:

- All administrator authorizations
- Business Role managers
- Review owners
- Separation of Duties Policy owners
- Application owners

User Guide

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

- Access requesters
- Access Request approvers
- Reviewers
- Review owners
- Fulfillers

Reporting Guide

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

NetIQ Identity Manager Driver for Identity Governance

Provides information about how to install and configure the Identity Manager Driver for NetIQ Identity Governance. The Identity Governance driver allows you to provision application-specific permission catalog data from Identity Governance to Identity Manager, giving you the ability to review and certify permission assignments using Identity Governance, as well as to request and provision these permissions using Identity Manager. The driver also can provision users in the Identity Vault for Identity Manager. For more information, see *NetIQ Identity Manager Driver for Access Review Installation and Configuration Guide*.

Technical References

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

Videos

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

Contents

1 Planning to Install Identity Governance

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

- ❒ Databases for Identity Governance and Identity Reporting
- ❒ An application server
- ❒ An authentication service, such as One SSO Provider (OSP) or NetIQ Access Manager (Access Manager)
- ❒ LDAP authentication server
- ❒ Java Runtime Environment
- ❒ (Optional) ActiveMQ
- ❒ (Optional) Identity Reporting
- ❒ (Optional) Audit Server

For a list of the appropriate versions to use with Identity Governance, see Section 1.9, “Hardware and Software Requirements,” on page 25.

You can get the product components from the NetIQ Downloads site. Use the following sections to plan your deployment, prepare your environment, and gather values needed during the installation process.

1.1 Checklist for Installing Identity Governance

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

	Checklist Items
❑	1. Learn about the relationship between the LDAP authentication server and the OSP and Access Manager authentication services. For more information, see Section 1.2, “Understanding Authentication for Identity Governance,” on page 11.

	Checklist Items
❑	2. Learn about the databases for Identity Governance and the options for installing the product with your database platform. For more information, see "Understanding the Identity Governance Databases" on page 15.
❑	3. Decide which servers to use for your Identity Governance components. For more information, see the following sections: ◆ Section 1.7, "Recommended Installation Scenarios and Server Setup," on page 19 ◆ Section 1.9, "Hardware and Software Requirements," on page 25
❑	4. (Conditional) To add Identity Governance to an existing Identity Manager environment, review the scenarios. For more information, see Section 1.7.4, "Identity Governance and Identity Manager," on page 20.
❑	5. Decide whether you want to run the authentication service, ActiveMQ, or Identity Governance in a clustered environment. For more information, see Section 1.7.5, "Ensuring High Availability for Identity Governance," on page 21.
❑	6. Review the sample installation scripts and decide whether you want to use them. For more information, see the sample scripts posted on the Identity Governance documentation page.
❑	7. Install the Tomcat application server: ◆ To review the prerequisites for Tomcat, see Section 2.2, "Prerequisites for the Tomcat Application Server," on page 32. ◆ The Tomcat server has the same server requirements as the Identity Governance server. For more information, see Section 1.9.1, "Identity Governance Server System Requirements," on page 26.
❑	8. Install an authentication service: ◆ To review the prerequisites, see Section 1.8.1, "General Prerequisites for Identity Governance," on page 23. ◆ To install the OSP server, see Chapter 3, "Installing an Authentication Service," on page 35. The OSP server has the same requirements as the Identity Governance server. For more information, see Section 1.9.1, "Identity Governance Server System Requirements," on page 26. ◆ To install Access Manager, see the Access Manager documentation.
❑	9. Install or configure the Identity Governance databases: ◆ To learn about the databases, see Section 1.3, "Understanding the Identity Governance Databases," on page 15. ◆ To review the prerequisites for the databases, see Section 2.3, "Prerequisites for the Identity Governance Databases," on page 32. ◆ To review the server requirements for the databases, see Section 1.9.2, "Database Server System Requirements," on page 27. Select one of the following databases as the database platform: ◆ Microsoft SQL Server. For more information, see Section 4.2, "Preparing an MS SQL Server Database for Identity Governance," on page 44. ◆ Oracle. For more information, see Section 4.3, "Preparing an Oracle Database for Identity Governance," on page 47. ◆ PostgreSQL. For more information, see Section 4.4, "Preparing a PostgreSQL Database for Identity Governance," on page 50.

	Checklist Items
❑	10. Decide whether to use an auditing server with Identity Governance. For more information, see “Understanding Auditing” on page 18.
❑	11. Install Identity Governance: ◆ To review the prerequisites, see Section 1.8.1, “General Prerequisites for Identity Governance,” on page 23. ◆ To review the server requirements, see Section 1.9.1, “Identity Governance Server System Requirements,” on page 26. ◆ To install the Identity Governance server, see Chapter 4, “Installing Identity Governance,” on page 43.
❑	12. (Conditional) Complete the database configuration if you chose **Generate SQL for later** during installation. For more information, see Section 6.1, “Configuring the Databases after Installation,” on page 81.
❑	13. (Conditional) Complete the configuration of the Tomcat cluster: ◆ Section 6.3.1, “Configuring the Nodes in the Tomcat Cluster,” on page 88 ◆ Section 6.3.2, “Configuring ActiveMQ Failover in the Tomcat Cluster,” on page 89
❑	14. (Optional) Install Identity Reporting if you did not install it as part of the Identity Governance installation: ◆ To learn about reporting, see Section 1.4, “Understanding Identity Reporting,” on page 17. ◆ To review the prerequisites, see Section 1.8.2, “Prerequisites for Identity Reporting,” on page 25. ◆ To review the server requirements, see Section 1.9.3, “Identity Reporting Server System Requirements,” on page 28. ◆ To install Identity Reporting, see Chapter 5, “Installing Identity Reporting,” on page 67.
❑	15. (Optional) Configure auditing if you did not configure it as part of the Identity Governance installation. For more information, see “Enabling Auditing” on page 91.
❑	16. If you did not add the license during the installation, add a valid license key to continue using Identity Governance after the 90-day trial period. For more information, see “Updating the License Key” on page 111.

1.2 Understanding Authentication for Identity Governance

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

1.2.1 Understanding Authentication with Single Sign-On

Identity Governance allows the following authentication service configurations to achieve single sign-on 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 authentication server. Identity Governance works with eDirectory and Microsoft Active Directory. You must deploy the LDAP server before you install Identity Governance.

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

Access Manager supports a number of 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.

How do OSP, Access Manager, and SSO work?

If you use the Identity Vault as your authentication 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 authentication is required and temporarily redirects the browser to the OSP or to the Access Manager authentication service. The OSP or the Access Manager service authenticates the user, either by asking the user for a name/password or, if so configured, by asking the Kerberos or a SAML provider to authenticate 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 users’ session’ time out, authorization occurs automatically and without the users 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.

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

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

1.2.2 Using One SSO Provider for Authentication

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

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

1.2.3 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 single sign-on 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.

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

1.2.4 Using Access Manager with One SSO Provider

Identity Governance can use Access Manager to connect with OSP as the authentication service. With Access Manager, you can provide single sign-on access among Identity Governance and other applications in your environment that use Access Manager for authentication.

1.2.5 Understanding the Bootstrap Administrator for Identity Governance

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

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

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

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

The bootstrap administrator account does not link to an account for a real person. You should not continue using this account after you have Identity Governance running in a production environment. Instead, as soon as you have collected user accounts, assign one of the collected accounts as a global administrator. For more information about assigning authorizations, see "Understanding Authorizations in Identity Governance" in *NetIQ Identity Governance Administrator Guide*.

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

1.2.6 Understanding the Keystore for the Authentication Server

During installation, you must provide a password that the Identity Governance service uses for authorized interactions with the authentication server. The installation process assumes that you want to use OSP 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 `/opt/netiq/idm/apps/osp/osp-truststore.pkcs12` or `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 `/opt/netiq/idm/apps/osp/osp.pkcs12` or `c:\netiq\idm\apps\osp\osp.pkcs12`.

By default, the Identity Governance and Identity Reporting installation program places TLS/SSL trust certificates in `/opt/netiq/idm/apps/tomcat/conf/apps-truststore.pkcs12` or `c:\netiq\idm\apps\tomcat\conf\apps-truststore.pkcs12`. This file stores certificates from the following secured servers:

- Authentication server when you specify https for OSP or when you use Access Manager for authentication and when the authentication server 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 GUI 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 NetIQ Advanced Authentication servers, you can install the CA's trusted root certificate into the trust store and remove any server-specific certificates. For more information, see Section 3.2, "Prerequisites for One SSO Provider," on page 36.

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 utility. For more information, see "Running the Identity Governance Configuration Utility" on page 133.

1.3 Understanding the Identity Governance Databases

Identity Governance and Identity Reporting databases run on Microsoft SQL Server, Oracle, and PostgreSQL databases. You can have the installation program do most of the work for building the databases, schemas, tables, and views for each component.

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

- **Linux:** "Installing Identity Manager " in the *NetIQ Identity Manager Setup Guide for Linux*.
- **Windows:** "Installing Identity Reporting" in the *NetIQ Identity Manager Setup Guide for Windows*.

Identity Governance uses five databases: operations, archive, data collection, workflow, and analytics. By default, Identity Governance names these databases `igops`, `igarc`, `igdcs`, `igwf`, and `igara`, respectively. You can establish these databases in the following ways:

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

IMPORTANT

- For Oracle, you must create the database (SID) before installation, and the installation program can create the schemas, tables, and views for you. Alternatively, you can add the schemas to the database before installing Identity Governance.
- For Oracle, Identity Governance supports Pluggable and Container type databases. If you use a Container type database, you must prepend C## to the common user name. Identity Governance requires a common user to function, so the user name must start with C##.

- Have the installation program generate a SQL file instead of creating schemas, tables, views, and artifacts in the databases. The installation program generates a SQL file for each schema, which your database administrator can run to update the database for Identity Governance. You might use this method if your database administrator wants to review the changes that will be made to the database.
- Ensure that the database runs in the same subnetwork as your Identity Governance server.
- Set up the schema for your users for your specific database type. You initialize (or reset) the database with Liquibase commands. To initialize or rest the database, use the following command:
  - **Linux:** Default location in `/opt/netiq/idm/apps/idgov/bin`

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

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

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

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

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

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

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

  - **MS SQL:** Use the following 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" -script "/opt/netiq/idm/apps/idgov/
    scripts/all-import-configs.script"
    ```

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

- “Preparing an MS SQL Server Database for Identity Governance” on page 44
- Section 4.3, “Preparing an Oracle Database for Identity Governance,” on page 47
- “Preparing a PostgreSQL Database for Identity Governance” on page 50
- Section 6.1, “Configuring the Databases after Installation,” on page 81

1.4 Understanding Identity Reporting

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

There are two different versions of Identity Reporting you can install. You can install the version that comes with Identity Governance and 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 this version of Identity Reporting. It uses the Identity Manager security module to determine who has access to the reports. It can run both the Identity Manager and Identity Governance reports by configuring an external data source where you store the data.

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

1.4.1 Understanding the Identity Reporting Database

Identity Reporting uses one database. Use the following information to help you correctly complete the Identity Reporting installation with the datase:

- If you use a PostgreSQL database, you must allow the installation program for Identity Governance to create the schema, tables, and views for the PostgreSQL database.
- 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.
- You must run the Identity Reporting database in the same subnetwork as your Identity Governance server.

You can establish the Identity Reporting database in the same way as you do for the Identity Governance database. For more information, see Section 1.3, “Understanding the Identity Governance Databases,” on page 15.

1.5 Understanding Auditing

You can configure Identity Governance to send audit events to an auditing server to integrate these activities into your overall auditing solution. Identity Governance events contain an authentication tracking identifier to correlate audit events from multiple systems.

If you have the audit server details when you install Identity Governance, you can configure them during the installation. You can also add or change your audit server details after you install Identity Governance. For more information, see “Enabling Auditing” on page 91.

Identity Governance supports the following auditing servers:

- NetIQ Sentinel
- ArcSight Enterprise Security Manager
- Splunk

For more information about supported versions, see “Auditing Server System Requirements” on page 30.

1.6 Understanding the Identity Governance Installation and Configuration Utilities

Identity Governance contains two installation and configuration utilities. You use the two utilities for different tasks. The utilities are:

- **Configuration Update Utility:** Three of the Identity Governance components use the Configuration Update utility to change settings instead of using the Identity Governance Configuration Utility. There is a separate utility because you can install and use some of these components with Identity Manager. The three components that use the Configuration Update utility are OSP, Identity Reporting, and Auditing.
- **Identity Governance Configuration Utility:** The Identity Governance Configuration Utility allows you to modify settings for Identity Governance, such as the URL for Identity Governance, the authentication server, OSP, and email notifications. You can also specify an external provisioning system for workflows and the settings for collection and publication.

Identity Governance contains multiple components and you can install the components on the same servers or on 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 servers, the GLOBAL configuration databases and the `ism-configuration.properties` file might contain duplicate settings.

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 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.

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

1.7 Recommended Installation Scenarios and Server Setup

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

- Tomcat application server
- Java Runtime Environment
- An external database of Microsoft SQL Server, Oracle, or PostgreSQL (must be on the same subnetwork as the Identity Governance server)
- Authentication service, such as OSP or Access Manager
- (Optional) ActiveMQ
- (Optional) Identity Reporting
- (Optional) Audit server

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

1.7.1 Selecting an Operating System Platform for Identity Governance

You can install Identity Governance components on a variety of operating system platforms. The following table helps you determine which servers you might want to use for your Identity Governance components. For more information about supported operating system versions, see “Hardware and Software Requirements” on page 25.

Platform	Component
Red Hat Enterprise Linux (RHEL), SUSE Linux Enterprise Server (SLES) Windows Server	Identity Governance Identity Reporting OSP or Access Manager ActiveMQ Tomcat Browser access to Identity Governance
Windows desktop	Browser access to Identity Governance Browser access to Identity Reporting

1.7.2 Identity Governance in a New Environment

You must prepare a new environment with required components for Identity Governance if you do not have all of the required components in your environment. The Identity Governance installer includes an installer for Identity Reporting. In addition to the Identity Governance installer, the software download page provides the installer for OSP.

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

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

- Section 1.7.7, “Component Installation Order,” on page 23
- Section 1.7.6, “Recommended Server Setup,” on page 22

1.7.3 Identity Governance and Existing Components

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

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

1.7.4 Identity Governance and Identity Manager

To integrate Identity Governance with Identity Manager Advanced Edition, you can use some of the components that you installed with Identity Manager: OSP 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.

You will also need to perform the following tasks:

- Create the databases for Identity Governance
- Integrate OSP to define and provision Identity Governance user accounts
- (Optional) Integrate with Identity Reporting

For more information about these activities, see “Integrating Single Sign-on Access with Identity Manager” on page 104 and Chapter 5, “Installing Identity Reporting,” on page 67.

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

- Section 1.8.1, “General Prerequisites for Identity Governance,” on page 23
- Section 2.3, “Prerequisites for the Identity Governance Databases,” on page 32
- Section 1.9.1, “Identity Governance Server System Requirements,” on page 26
- Section 1.9.2, “Database Server System Requirements,” on page 27
- Chapter 4, “Installing Identity Governance,” on page 43

1.7.5 Ensuring High Availability for Identity Governance

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

- To manage the availability of your network resources for Identity Governance, use the High Availability tools provided with your operating system. Always have the latest patches installed for your operating system.
- You can run Identity Governance in a stateless cluster where the load balancers shift authentication requests among the various OSP servers. During installation, you must specify a URL that drives client access through your L4 switch or load balancer rather than specifying the hostname and port for the Tomcat server.
- Each node in the cluster must have a persistent unique runtime identifier. For example, `node1` or `ProdNode1`. For more information, see Section 6.3.1, “Configuring the Nodes in the Tomcat Cluster,” on page 88.

  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 other identifier might not remain the same.
- The configuration settings for OSP and Identity Governance must be identical for all nodes in the cluster.
- When installing an authentication server, consider the following requirements:
  - Configure a load balancer with a DNS host name and port for the authentication server (OSP or Access Manager server).

    The authentication server can use the same load balancer specified for Identity Governance, a dedicated load balancer, or a single Tomcat instance.
  - Specifying the values for the appropriate load balancer instead of the connection settings to the Tomcat instance. For more information, see **Application address** in Step 6 on page 37.
  - The configuration files must be on each authentication server deployment in the environment. For example, if using OSP, the `osp.war` file must be on each deployment of OSP in the environment. Use the same Keystore file for all deployments. For more information, see Chapter 3, “Installing an Authentication Service,” on page 35.
- When installing Identity Governance, consider the following requirements:
  - Configure a load balancer with a DNS host name and port for Identity Governance use.

    Identity Governance can use a dedicated load balancer or the same load balancer as for the authentication server.
  - Specify the values for the load balancer instead of the host and port for the Tomcat connection. For more information, see **Application address** in Step 7 on page 53.

- On the primary (or master) node, perform the steps for configuring the databases. For more information, see **Database details** in Step 7 on page 53.
- For each installation on a secondary node, do not perform any database configuration steps. Instead, specify the settings for connecting to the previously configured databases. For more information, see **Database details** in Step 7 on page 53.

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

  For more information, see Section 3.4.1, “Creating a Silent Properties File for Installing on a Secondary Node,” on page 40.

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

  NOTE: In the `silent.properties` file for Identity Governance, change the following settings:
  - `install.db.configure=false`
  - `install.tomcat.runtime.id=`

1.7.6 Recommended Server Setup

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

The following table provides examples for an Identity Governance setup.

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

1.7.7 Component Installation Order

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

- Section 1.7.7.1, “Using Identity Governance without Identity Manager,” on page 23
- Section 1.7.7.2, “Using Identity Governance with Identity Manager,” on page 23

1.7.7.1 Using Identity Governance without Identity Manager

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

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

   To use an authentication server for the data source, ensure that you have Active Directory or eDirectory already installed.
2. (Optional) Audit server if enabling auditing during product installation
3. Database and Tomcat
4. OSP or Access Manager
5. Identity Governance and Identity Reporting
6. (Optional) Identity Reporting, if not installed at the same time as Identity Governance
7. (Optional) Audit server if enabling auditing after product installation

1.7.7.2 Using Identity Governance with Identity Manager

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

1. Identity Manager Advanced Edition
2. Identity Governance

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

1.8 Prerequisites for Installing Identity Governance

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

- Section 1.8.1, “General Prerequisites for Identity Governance,” on page 23
- Section 1.8.2, “Prerequisites for Identity Reporting,” on page 25

1.8.1 General Prerequisites for Identity Governance

- You can install Identity Governance and OSP in a stateless cluster. For more information about the installation requirements, see Section 1.7.5, “Ensuring High Availability for Identity Governance,” on page 21.

- For best performance, do not install Identity Governance on the same server as its databases. However, the Identity Governance server must include the supported versions of Java, and Tomcat application server.
- Do not install Identity Governance or its database on a server that is already running components for Identity Manager. For example, do not install on the same server as Identity Manager Home and Provisioning Dashboard.
- You must use Latin-1 characters in the installation path.
- Do not use mixed case domains. Identity Governance utilizes 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 authentication server as your data source for Identity Governance users, ensure that you have Active Directory or eDirectory already installed. For more information, see "Adding Identity Governance Users" in *NetIQ Identity Governance Administrator Guide*.
- When you point to the installation directory for Java, it must be a supported OpenJDK instance used by the Tomcat server.
- Ensure that the communication ports that you want to use are open in the firewall. For more information, see Appendix B, "Ports Used in Identity Governance," on page 141.
- To integrate Identity Governance with Identity Manager, the Identity Manager component must already be installed and configured with OSP.
- To use TLS auditing, the audit server should be up and running when you install Identity Governance so that the installer can connect to the audit server and retrieve the certificate to add to the keystore.
- Before installing Identity Governance, you need the following information:
  - Paths to your Tomcat and Java directories.
  - Credentials of a database administrator (DBA) account that can access and modify data in the databases to create database tables, views, and other artifacts.

    NOTE: If you do not have credentials for the DBA, the installation process can generate a SQL script that the DBA runs to configure the databases.
  - DNS host name and port of your Identity Governance server. Identity Governance uses the IP address or DNS name as the URL for users to access Identity Governance.
  - (Conditional) When using an LDAP authentication server, you need the following information:
    - Credentials of an administrator account for the server.
    - The container in the server where you store administrator accounts.
    - The container in the server where you store the accounts for users who can log in to Identity Governance.
  - (Conditional) To use an Identity Manager authentication server, you must have the distinguished name (DN), password, user container, and admin container of an administrator account for the server.
  - (Conditional) To use an Identity Manager authentication server or TLS auditing, you must have the trust store password for the server.
  - For best performance, do not install Identity Governance on the database server, however, the database server and the Identity Governance server must run in the same subnetwork. Also, ensure that the database is running the supported versions of Java and the Tomcat application server.
  - DNS host name and port of your database server.

- DNS host name and port of your ActiveMQ server if it is installed on a separate server.
- (Conditional) If using Access Manager for the authentication service, the Access Manager administrator account distinguished name (DN) and password.

1.8.2 Prerequisites for Identity Reporting

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

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

- This guide provides information about installing Identity Reporting for use with Identity Governance only. If you have already installed Identity Reporting with Identity Manager 4.5 or later, you might not need to install it again for Identity Governance. Ensure that you have the appropriate version of Identity Reporting. For more information about installing with Identity Manager, see:
  - **Linux:** "Installing Identity Manager " in the *NetIQ Identity Manager Setup Guide for Linux*.
  - **Windows:** "Installing Identity Reporting" in the *NetIQ Identity Manager Setup Guide for Windows*.
- You can install Identity Reporting on the same server as Identity Governance, and the two products use the same Tomcat instance, or you can install it on a separate server running Tomcat.
- (Conditional) To run reports against a Microsoft SQL Server database, you must install the appropriate JDBC driver file. For example, `mssql-jdbc-7.0.0.jar`. For more information, see https://docs.microsoft.com/en-us/sql/connect/jdbc/microsoft-jdbc-driver-for-sql-server?view=sql-server-2017.
- (Conditional) To run reports against an Oracle 12c database, you must install the appropriate JDBC driver file. For example, `ojdbc8.jar`. For more information, see https://www.oracle.com/technetwork/database/features/jdbc/jdbc-drivers-12c-download-1958347.html.
- Assign the Report Administrator authorization to any users that you want to be able to access the reporting functionality.
- Ensure that all servers in your Identity Governance environment are set to the same time, particularly the servers for the database and events auditing components. If you do not synchronize the time on your servers, some reports might be empty when executed. For example, this issue can affect data related to new users when the servers hosting Identity Governance and the reporting databases have different time stamps.

1.9 Hardware and Software Requirements

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

1.9.1 Identity Governance Server System Requirements

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

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

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

Category	Minimum Requirement
Processor	◆ 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
Operating System	◆ Red Hat Enterprise Linux 7.4 (64-bit) ◆ SUSE Linux Enterprise Server 12 SP3 (64-bit) ◆ SUSE Linux Enterprise Server 15 ◆ Microsoft Windows Server 2016 (64-bit) **IMPORTANT:** Before installing Identity Governance, apply the latest operating system patches.
Java	Zulu JRE 8u181 from Azul
Application Server	Apache Tomcat 9.0.12 **NOTE:** (Conditional) For guaranteed delivery of email notifications, your application server must include support for Apache ActiveMQ Java Message Service (JMS) and clustering.
LDAP Authentication Server	◆ Microsoft Active Directory ◆ NetIQ eDirectory 9.1.1 ◆ NetIQ Identity Manager 4.7.2

Category	Minimum Requirement
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 Tomcat server. ◆ **Linux:** Default location of Apache Tomcat is `/opt/netiq/idm/apps/tomcat` ◆ **Windows:** Default location of Apache Tomcat is `c:\netiq\idm\apps\tomcat`
Additional Software	(Optional) Apache ActiveMQ 5.15.6, which guarantees that notifications are sent using SMTP

1.9.2 Database Server System Requirements

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

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

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

Category	Minimum Requirement
Processor	◆ 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

Category	Minimum Requirement
Memory	◆ 16 GB (small catalog) ◆ 32 GB
Operating System	◆ Red Hat Enterprise Linux 7.4 (64-bit) ◆ SUSE Linux Enterprise Server 12 SP3 (64-bit) ◆ SUSE Linux Enterprise Server 15 ◆ Microsoft Windows Server 2016 (64-bit) **IMPORTANT:** Before installing Identity Governance, apply the latest operating system patches.
Database	One of the following: ◆ Microsoft SQL Server 2017 with JDBC driver 7.0 (`mssql-jdbc-7.0.0.jar` for jre8) ◆ Oracle 12c SP2 with JDBC driver `ojdbc8.jar` **NOTE:** If using Oracle 12c SP2, Identity Governance requires that you install all patches available from Oracle. ◆ PostgreSQL 10.5 with JDBC driver `postgresql-42.2.5.jar`

1.9.3 Identity Reporting Server System Requirements

This section lists the requirements for the server that hosts Identity Reporting when installed only for Identity Governance. For more information about whether to install the components on the same server, see Section 1.7, “Recommended Installation Scenarios and Server Setup,” on page 19. For more information about the system requirements for installing in an Identity Manager environment that includes Identity Governance, see:

- **Linux:** “Planning Overview” in the *NetIQ Identity Manager Setup Guide for Linux*.
- **Windows:** “Installing Identity Reporting” in the *NetIQ Identity Manager Setup Guide for Windows*.

Category	Minimum Requirement
Processor	Pentium 4
Disk Space	50 GB
Memory	16 GB
Operating System	◆ Red Hat Enterprise Linux 7.4 (64-bit) ◆ SUSE Linux Enterprise Server 12 SP3 (64-bit) ◆ SUSE Linux Enterprise Server 15 ◆ Microsoft Windows Server 2016 (64-bit) **IMPORTANT:** Before installing Identity Governance, apply the latest operating system patches.

Category	Minimum Requirement
Virtualization Systems	VMWare ESX 6.5 U1 **IMPORTANT:** NetIQ supports Identity Reporting on enterprise-class virtualization systems that provide official support for the operating systems where NetIQ products are running. As long as the vendors of the virtualization systems officially support these operating systems, NetIQ supports the Identity Reporting stack on them.
Application Server	Apache Tomcat 9.0.12
Java	Zulu JRE 8u181
Databases	Identity Reporting database runs on the following platforms: ◆ Microsoft SQL Server 2017 ◆ Oracle 12c **NOTE:** If using Oracle 12c SP 2, Identity Governance requires that you install all patches available from Oracle. ◆ PostgreSQL 10.5 You can run reports against the following databases: ◆ Microsoft SQL Server 2017 ◆ Oracle 12c ◆ PostgreSQL 10.5
Third-Party Connector Libraries	(Optional) If connecting to a Vertica data source, include the following: Vertica: `com.microfocus.vertica`

1.9.4 Identity Governance and Reporting Browser Requirements

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

Computers

- Apple Safari 11.1.2
- Google Chrome 60.0.3112.90
- Microsoft Edge Browser 42.17134.1.0
- Microsoft Internet Explorer 11
- Mozilla Firefox 63
- Mozilla Firefox (Mac) 57

iPad (iOS 10.3.3)

- Safari 10.0
- Chrome 62.0.3202.70
- Firefox 10.3

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

1.9.5 Auditing Server System Requirements

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. NetIQ certifies the following audit servers using syslogger for use with Identity Governance:

- Splunk 7.2.0 (build 8c86330ac18)
- ArcSight ESM Suite 6.11.0.2149
- Sentinel 8.0.0.1_3404

2 Installing Components Required for Identity Governance

Several software components must be present in your environment before you install Identity Governance. Apache Tomcat, a database platform, and a Java Runtime Environment must be available when you install Identity Governance. Optionally, you can also install Apache ActiveMQ if you want to guarantee that Identity Governance sends notifications using SMTP.

If possible, install these components in the following directories:

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

To prepare for the installation, review the entire installation process and the latest release notes before beginning:

- "Checklist for Installing Identity Governance" on page 9
- *NetIQ Identity Governance 3.5.0 Release Notes*

2.1 Checklist for Installing Required Components

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

	Checklist Items
❑	1. Decide which servers you want to use for your Identity Governance components. For more information, see the following sections: ◆ Section 1.7.6, "Recommended Server Setup," on page 22 ◆ "Identity Governance Server System Requirements" on page 26 ◆ Section 1.9.2, "Database Server System Requirements," on page 27
❑	2. Review the considerations for installing the applications to ensure that the computers meet the requirements: ◆ Section 2.2, "Prerequisites for the Tomcat Application Server," on page 32 ◆ Section 2.3, "Prerequisites for the Identity Governance Databases," on page 32
❑	3. Review the minimum required versions for the components. For more information, see "Identity Governance Required Component Software Versions" on page 33.
❑	4. Install supported versions of Tomcat, a database platform, JRE, and, optionally, ActiveMQ. If possible, install these components in the following directories: ◆ **Linux:** Default location of `/opt/netiq/idm/apps/` ◆ **Windows:** Default location of `C:\netiq\idm\apps\` For sample installation scripts, go to the product documentation site and look under the References section.

	Checklist Items
❑	5. (Conditional) To use a Microsoft SQL Server or Oracle database, see one of the following sections: ◆ "Preparing an MS SQL Server Database for Identity Governance" on page 44 ◆ Section 4.3, "Preparing an Oracle Database for Identity Governance," on page 47
❑	6. Install an authentication service and then install Identity Governance. For more information, see Section 1.2, "Understanding Authentication for Identity Governance," on page 11.

2.2 Prerequisites for the Tomcat Application Server

Review the following considerations before installing Tomcat:

- We highly recommend that you configure Tomcat to use https with either TLSv1.2 or TLS1.1. Any prior version of TLS should not be used. For more information, see "Securing Tomcat".
- You can install Tomcat, PostgreSQL, and ActiveMQ on the same server or on separate servers.
- When you install Tomcat or ActiveMQ, the OpenJDK JRE is automatically included.
- To use ActiveMQ, which guarantees that Identity Governance sends notifications using SMTP, install MQServer.
- The installation process sets the JRE location in the `setenv.sh` or the `sentenv.bat` file.
  - **Linux:** Default location in `/opt/netiq/idm/apps/tomcat/bin/`
  - **Windows:** Default location in `c:\netiq\idm\apps\tomcat\bin\`
- (Conditional) If you use Linux, do not run Tomcat as `root`. The installation process creates a user account for the Tomcat service, which should not be `root`.

2.3 Prerequisites for the Identity Governance Databases

Review the following considerations before installing Identity Governance:

- For best performance, do not install Identity Governance on the database server, however, the database server and the Identity Governance server must run in the same subnetwork. Also, ensure that the database is running the supported versions of Java and Tomcat.
- 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 files.
- (Conditional) To use an Oracle database with Identity Governance, you must install the database with the Identity Governance admin user for the database before installing Identity Governance. For more information, see Section 6, "Completing the Installation Process," on page 81.
- (Conditional) To install the databases in a clustered environment, see Section 1.7.5, "Ensuring High Availability for Identity Governance," on page 21.

2.4 Identity Governance Required Component Software Versions

Identity Governance requires the following minimum versions of these software components:

- Tomcat 9.0.12
- (Optional) MS SQL Server 2017
- (Optional) Oracle 12c SP2
- (Optional) PostgreSQL 10.5
- Zulu JRE 8u181 from Azul
- ActiveMQ 5.15.6

2.5 Stopping, Starting, and Restarting Tomcat

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

NOTE: If you have installed Tomcat and ActiveMQ using the sample scripts provided on the product documentation site, the following examples guide these processes.

2.5.1 Linux Examples for Tomcat

To stop Tomcat:

```
systemctl stop identity_tomcat.service
```

To start Tomcat:

```
systemctl start identity_tomcat.service
```

To restart Tomcat:

```
systemctl restart identity_tomcat.service
```

To show the status of Tomcat.service:

```
systemctl status identity_tomcat.service
```

2.5.2 Windows Examples for Tomcat

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

To use the Services window:

1. Open the **Services** window (`C:\Windows\system32\services.msc`).
2. Locate **IDM Apps Tomcat Service**.
3. Select **Start**, **Stop**, or **Restart**.

To use Task Manager:

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

2 Select the **Services** tab.

3 Locate 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.

2.6 Stopping, Starting, and Restarting ActiveMQ

If you have installed ActiveMQ, Identity Governance starts it from within the 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.

2.6.1 Linux Examples for ActiveMQ

To stop ActiveMQ:

```
systemctl stop identity_activemq.service
```

To start ActiveMQ:

```
systemctl start identity_activemq.service
```

To restart ActiveMQ:

```
systemctl restart identity_activemq.service
```

To show the status of the ActiveMQ service:

```
systemctl status identity_activemq.service
```

2.6.2 Windows Examples for ActiveMQ

On Windows, you start, stop, and restart ActiveMQ by starting, stopping, and restarting Tomcat. For more information, see “Windows Examples for Tomcat” on page 33.

3 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 access.

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

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

- OSP 6.3
- Access Manager 4.4.3
- Access Manager configured to connect to OSP

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

3.1 Checklist for Installing One SSO Provider

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

	Checklist Items
❑	1. Decide which servers you want to use for your Identity Governance components. For more information, see Section 1.7, “Recommended Installation Scenarios and Server Setup,” on page 19.
❑	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 1.7.5, “Ensuring High Availability for Identity Governance,” on page 21.
❑	3. Decide which authentication service you will install. For more information, see Section 1.2, “Understanding Authentication for Identity Governance,” on page 11.
❑	4. Ensure that Tomcat has been installed. For more information, see Chapter 2, “Installing Components Required for Identity Governance,” on page 31.
❑	5. (Optional) If you will install OSP, review the prerequisites for installing it. For more information, see “Prerequisites for One SSO Provider” on page 36.

	Checklist Items
❑	6. Install the components: ◆ For a guided installation of OSP, see Section 3.3, “Using the Wizard to Install One SSO Provider (OSP),” on page 36. ◆ For a silent installation of OSP, see Section 3.4, “Silently Installing One SSO Provider,” on page 40. ◆ To install Access Manager, see Section 3.5, “Installing Access Manager,” on page 42

3.2 Prerequisites for One SSO Provider

Before installing OSP, review the following considerations:

- (Conditional) Even if you installed OSP with Identity Manager 4.5 or later, if you want to use OSP as your authentication service, you must install a separate instance of OSP for use with Identity Governance.
- (Conditional) OSP requires trust certificates configured for secure communication for user authentication in a production environment. Depending on your Identity Governance solution, OSP might need to communicate with an authentication server, a SAML provider, or one or more Advanced Authentication servers. For more information, see Section 1.2.6, “Understanding the Keystore for the Authentication Server,” on page 14.
- 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.
- (Conditional) If you set up multiple instances of OSP for use in a high availability cluster, copy the `osp.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 key material.

3.3 Using the Wizard to Install One SSO Provider (OSP)

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

- Section 3.2, “Prerequisites for One SSO Provider,” on page 36
- Section 1.9.1, “Identity Governance Server System Requirements,” on page 26

To perform a silent, unattended installation, see Section 3.4, “Silently Installing One SSO Provider,” on page 40.

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

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

To install OSP:

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

2 Stop Tomcat. For examples, see "Stopping, Starting, and Restarting Tomcat" on page 33.

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

- **Linux (console)**: Enter `./osp-install-linux.bin -i console`
- **Linux (GUI)**: Enter `./osp-install-linux.bin`
- **Windows (console)**: Enter `cmd /c "osp-install-win.exe -i console"`
- **Windows (GUI)**: Double-click `osp-install-win.exe`

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

---

4 Accept the license agreement, and then select **Next**.

5 Specify a path for the installed files.

6 Complete the guided process, using the following parameters:

- **Tomcat details**

  Specify a directory that represents the home directory for the Tomcat server. The installation process adds some files for OSP to this folder.

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

- **Tomcat Java home**

  Specify the directory that represents the home directory for Java on the Tomcat server. The installation process uses Java for several processes, such as to run commands and create security stores.

- **Application address**

  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.

  Protocol

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

  If you specify https, ensure that you have configured your server for SSL communications. For more information, see Section 1.2.6, "Understanding the Keystore for the Authentication Server," on page 14.

  Host Name

  Do not use `localhost`.

  In a non-clustered environment, specify the DNS name of the Tomcat server where you are installing OSP.

  In a clustered environment, specify the DNS name of the server that hosts the load balancer that you want to use. For more information about installing in a clustered environment, see Section 1.7.5, "Ensuring High Availability for Identity Governance," on page 21.

  Port

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

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

- **Login screen customization**

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

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

- **Expected setup**

  Represents the relative server locations for how you plan to install Identity Governance and Identity Reporting. Select one option.

  External

  Specifies that you will have Identity Governance and Identity Reporting installed on different servers.

  Local

  Specifies that you will have Identity Governance and Identity Reporting installed on the same server.

  None

  Specifies that you will not have Identity Governance and Identity Reporting installed on any server that this server will know about.

- **Authentication details**

  Represents the requirements for connecting to an authentication server that contains the list of users who can log in to the application. For more information about the authentication server, see Section 1.2.1, “Understanding Authentication with Single Sign-On,” on page 12.

  LDAP host

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

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

  LDAP port

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

  Use SSL

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

  Admin DN

  Applies only when installing a new authentication server.

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

  Admin password

  Applies only when installing a new authentication server.

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

User container

Applies only when installing a new authentication server.

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

Admin container

Applies only when installing a new authentication server.

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

Trust store password

Specifies the password for the trust store. The trust store is empty unless you specify to use SSL for LDAP or audit.

Keystore Password

Applies only when installing a new authentication server.

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

The password must be a minimum of six characters.

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

- **Auditing details**

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

Enable auditing for OSP

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

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

Protocol

Applies only when you enable auditing for OSP.

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

Audit server

Applies only when you enable auditing for OSP.

Specifies name of the auditing server.

Audit port

Applies only when you enable auditing for OSP.

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

Audit events cache

Applies only when you enable auditing for OSP.

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

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

7 (Conditional) If prompted, accept or reject any untrusted 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

8 Review the pre-installation summary.

9 Start the installation process.

10 When the installation process completes, select **Done**.

3.4 Silently Installing One SSO Provider

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

- Section 3.2, “Prerequisites for One SSO Provider,” on page 36
- Section 1.9.1, “Identity Governance Server System Requirements,” on page 26

To perform a guided installation, see Section 3.3, “Using the Wizard to Install One SSO Provider (OSP),” on page 36.

3.4.1 Creating a Silent Properties File for Installing on a Secondary Node

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

1 After installing OSP on the primary node, locate the `osp_install_log.log` file.

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

2 Locate the sample `osp-install-silent.properties` file, by default in the same directory as the installation scripts for OSP.

3 Open the files in a text editor.

4 Copy the parameter values from the log file to their corresponding parameters in the silent properties file.

Your silent properties file should contain all the parameters listed between `User Interactions` and `Summary` in the log file.

5 Change the values that represent true/false settings:

Log file	Silent.properties file
0	false
1	true

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

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

7 (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 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.

8 Save and close the files.

3.4.2 Running a Silent Installation

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

2 Stop Tomcat. For examples, see "Stopping, Starting, and Restarting Tomcat" on page 33.

3 (Conditional) If you have the `.iso` image file for the Identity Governance installation package, navigate to the directory containing the OSP installation files, located by default in the `osp` directory.

4 (Conditional) If you downloaded the installation files from the NetIQ Downloads website, complete the following steps:

4a Navigate to the `.zip` file for the downloaded image.

4b Extract the contents of the file to a folder on the local computer.

5 Locate the `osp-install-silent.properties` file, by default in the same directory as the OSP installation file

6 (Conditional) In a non-clustered environment or when installing on the primary node, complete the following steps:

6a In a text editor, open the silent properties file.

6b Specify the parameter values.

For more information about the settings for installation, see Step 5 through Step 6 on page 37.

6c Save and close the file.

7 (Conditional) When installing on a secondary node in a cluster, you can modify the silent properties file using the steps in Section 3.4.1, “Creating a Silent Properties File for Installing on a Secondary Node,” on page 40.

8 To run the silent installation:

- **Linux:** Issue the following command:

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

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

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

3.5 Installing Access Manager

If you plan to use Access Manager as the authentication service for Identity Governance, see the Access Manager documentation.

4 Installing Identity Governance

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

4.1 Checklist for Installing and Configuring Identity Governance

Before beginning the installation process, it is important that you 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 1.8, “Prerequisites for Installing Identity Governance,” on page 23 and Section 1.9, “Hardware and Software Requirements,” on page 25.
❑	2. Decide whether you want to install Identity Governance in a clustered environment. For more information about the requirements, see Section 1.7.5, “Ensuring High Availability for Identity Governance,” on page 21.
❑	3. Ensure that your environment has a supported version of Tomcat already installed. For more information about installing Tomcat, see Chapter 2, “Installing Components Required for Identity Governance,” on page 31.
❑	4. Ensure that your environment has a supported version of OSP or Access Manager installed. For more information, see Chapter 3, “Installing an Authentication Service,” on page 35.
❑	5. (Conditional) To use a Microsoft SQL Server database, ensure that your environment has a supported version already installed. For more information, see the following sections: ◆ Section 1.3, “Understanding the Identity Governance Databases,” on page 15 ◆ Section 4.2, “Preparing an MS SQL Server Database for Identity Governance,” on page 44
❑	6. (Conditional) To use an Oracle database, ensure that your environment has a supported version already installed. For more information, see the following sections: ◆ Section 1.3, “Understanding the Identity Governance Databases,” on page 15 ◆ Section 4.3, “Preparing an Oracle Database for Identity Governance,” on page 47

	Checklist Items
❑	7. (Conditional) To use a PostgreSQL database, ensure that your environment has a supported version already installed. For more information, see the following sections: ◆ Section 1.3, “Understanding the Identity Governance Databases,” on page 15 ◆ Chapter 2, “Installing Components Required for Identity Governance,” on page 31 ◆ Section 4.4, “Preparing a PostgreSQL Database for Identity Governance,” on page 50
❑	8. (Conditional) To use TLS auditing, the audit server should be up and running when you install Identity Governance so that the installer can connect to the audit server and retrieve the certificate to add to the trust store.
❑	9. Install Identity Governance and Identity Reporting (optional): ◆ For a guided installation, see Section 4.5, “Using a Guided Process to Install Identity Governance and Identity Reporting,” on page 53. ◆ For an unattended installation, see Section 4.6, “Performing a Silent Installation of Identity Governance,” on page 62.
❑	10. To use third-party client connector software for gathering identity and application data, ensure that you add the appropriate `.jar` files. For more information, see Section 1.9.1, “Identity Governance Server System Requirements,” on page 26.
❑	11. Complete the setup for Identity Governance and its database. For more information, see Section 6, “Completing the Installation Process,” on page 81.
❑	12. (Optional) Modify the SSL settings for communication with the authentication server. For more information, see Section 6.4, “Using the TLS/SSL Protocol for Secure Connections,” on page 90.
❑	13. (Optional) Modify the configuration settings for Identity Governance. For more information, see Chapter 7, “Configuring Identity Governance Settings,” on page 113.
❑	14. (Optional) Add users who can log in to Identity Governance and assign them to authorizations in the application. For more information, see “Adding Identity Governance Users” in *NetIQ Identity Governance Administrator Guide*.
❑	15. (Optional) Customize the user interface. For more information, see “Customizing the User Interface” on page 115.
❑	16. (Optional) Customize the templates for email notifications and collectors. For more information, see “Customizing the Email Notification Templates” and “Customizing the Collector Templates for Data Sources” in *NetIQ Identity Governance Administrator Guide*.
❑	17. (Optional) Create a single sign-on experience for users between Identity Governance and Identity Manager Home and Provisioning Dashboard. For more information, see Section 6.10.1, “Checklist for Integrating Identity Governance with Identity Manager,” on page 104.

4.2 Preparing an MS SQL Server Database for Identity Governance

Before installing, you need the MS SQL Server JDBC file for the application server and an existing database for Identity Governance to use. You can install MS SQL Server and create the databases for Identity Governance if you do not want the installation program to create these. The installation

program can create the databases, tables, views, and other artifacts in the databases. The program needs the name of the databases to represent the operations, archive, data collection, provisioning workflow, and analytics databases for Identity Governance.

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

- Section 4.2.1, “Adding the JDBC File to the Application Server,” on page 45
- Section 4.2.2, “Creating the MS SQL Server Databases Before Installation,” on page 45
- Section 4.2.3, “Creating a Temporary MS SQL Server Database Administrator for the installation process,” on page 47

4.2.1 Adding the JDBC File to the Application Server

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

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

4.2.2 Creating the MS SQL Server Databases Before Installation

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

1. Install a supported version of SQL Server. For more information, see “Database Server System Requirements” on page 27.
2. 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 [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
```

3 (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];
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
```

4 Specify the same password for all databases.

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

---

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

- **Configure database now** > **Update**, if you want the installation program to generate or update the schemas, tables, and views when you migrate from Identity Governance 3.0 to 3.5
- **Configure database now > Use only existing**, if your database is already set up correctly with all schemas, roles, and users

- **Generate SQL for later**, if your database administrator wants to generate the schemas, tables, and views
- **No database configuration**, for using additional nodes in clustered environment

For more information about using SQL statements after installation, see Section 6.1, “Configuring the Databases after Installation,” on page 81.

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

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

The temporary account must have the following properties:

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

During installation, you can also select **Generate SQL for later**, which prevents the installation program from creating the tables, views, and artifacts in the Identity Governance or Identity Reporting database. Instead, the program generates a SQL file for each schema, which your database administrator can run to update the database. For more information about using the SQL files, see “Configuring the Databases after Installation” on page 81.

4.3 Preparing an Oracle Database for Identity Governance

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

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

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

- Section 4.3.1, “Adding the Oracle JDBC File to the Application Server,” on page 48
- Section 4.3.2, “Creating the Schemas for the Oracle Database before Installation,” on page 48
- Section 4.3.3, “Creating a Temporary Oracle Database Administrator for the Installation Process,” on page 50

After you install Identity Governance, the database administrator might need to update the schemas and global configuration values. For more information, see Chapter 6, “Completing the Installation Process,” on page 81.

4.3.1 Adding the Oracle JDBC File to the Application Server

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

1. Download the `ojdbc7.jar` file from the Oracle website.
2. Copy the file to a temporary directory on the *`tomcat_install`* server.

   The installation process then places the file in the:

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

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

4.3.2 Creating the Schemas for the Oracle Database before Installation

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

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

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

To create the schemas:

1. Install a supported version of Oracle.

   For more information, see Section 1.9.2, “Database Server System Requirements,” on page 27.
2. Create or identify the database that you want Identity Governance to use.
3. In the database, create the schema 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
   - Analyze any (`igops` and `igarc` only)
   - Create public synonym (`igops` and `igarc` only)
   - Drop public synonym (`igops` and `igarc` only)

4 Specify the same password for all schemas.

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

5 Issue the following commands:

NOTE: If you use the default values of `users` and `temp`, skip 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 idm_rpt_cfg IDENTIFIED BY "<password>";
GRANT CREATE SESSION, CREATE TABLE, CREATE VIEW, CREATE PROCEDURE, CREATE
SEQUENCE, CREATE TRIGGER, UNLIMITED TABLESPACE TO idm_rpt_cfg;
create role ig_report_role not identified;
grant EXECUTE ON igops.max_risk_level to igrptuser;
grant EXECUTE ON igops.min_risk_level to igrptuser;
grant EXECUTE ON igops.risk_value to igrptuser;
```

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

```
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
```

7 Create the reporting user `igrptuser`.

```
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;
ALTER USER igrptuser DEFAULT TABLESPACE USERS;
ALTER USER igrptuser TEMPORARY TABLESPACE TEMP;
```

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

- **Configure database now** > **Update**, if you want the installation program to generate or update the schemas, tables, and views when you migrate from Identity Governance 3.0 to 3.5
- **Configure database now > Use only existing**, if your database is already set up correctly with all schemas, roles, and users

- **Generate SQL for later**, if your database administrator wants to generate the schemas, tables, and views
- **No database configuration**, for using additional nodes in a clustered environment

For more information about using SQL statements after installation, see Section 6.1, “Configuring the Databases after Installation,” on page 81.

4.3.3 Creating a Temporary Oracle Database Administrator for the Installation Process

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

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

- Alter user
- Create public synonym
- Create user
- Drop public synonym
- Drop user
- Grant any object privilege
- Grant any privilege
- Grant any role

During installation, you can also select **Generate SQL for later**, which prevents the installation program from creating the tables, views, and artifacts in the Identity Governance or Identity Reporting database. Instead, the program generates a SQL file for each schema, which your database administrator can run to update the database. For more information about using the SQL files, see Section 6.1, “Configuring the Databases after Installation,” on page 81.

4.4 Preparing a PostgreSQL Database for Identity Governance

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

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

- Section 4.4.1, “Adding the JDBC File to the Application Server,” on page 51
- Section 4.4.2, “Creating the PostgreSQL Databases Before Installation,” on page 51
- Section 4.4.3, “Creating a Temporary PostgreSQL Database Administrator for the Installation Process,” on page 52

4.4.1 Adding the JDBC File to the Application Server

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

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

4.4.2 Creating the PostgreSQL Databases Before Installation

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

1. Install a supported version of PostgreSQL. For more information, see Section 1.9.2, “Database Server System Requirements,” on page 27.
2. Create the databases and roles for `igops`, `igdcs`, `igwf`, and `igara` using the following commands:

```
CREATE ROLE operations_db_name LOGIN password 'password';
CREATE ROLE 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';
GRANT EXECUTE ON igops.max_risk_level to igrptuser;
GRANT EXECUTE ON igops.min_risk_level to igrptuser;
GRANT EXECUTE ON igops.risk_value to igrptuser;
```

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

```
CREATE DATABASE "igrpt" WITH OWNER "pg_admin_user" TEMPLATE = template0
ENCODING = 'UTF8';
CREATE ROLE idm_rpt_cfg WITH LOGIN PASSWORD 'idm_rpt_cfg_password';
GRANT CREATE ON SCHEMA public TO idm_rpt_cfg;
FOR table_info IN SELECT * from pg_tables where schemaname = 'idm_rpt_cfg' and
tableowner != 'idm_rpt_cfg' LOOP
  cmd := 'ALTER TABLE idm_rpt_cfg.' || table_info.tablename || ' OWNER TO
idm_rpt_cfg';
  EXECUTE cmd;
END LOOP;
```

4. Specify the same password for all databases.

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

---

5 Create the reporting user `igrptuser`.

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

6 Grant the reporting role to the reporting user.

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

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

- **Configure database now** > **Update**, if you want the installation program to generate or update the schemas, tables, and views when you migrate from Identity Governance 3.0 to 3.5
- **Configure database now > Use only existing**, if your database is already set up correctly with all schemas, roles, and users
- **Generate SQL for later**, if your database administrator wants to generate the schemas, tables, and views
- **No database configuration**, for using additional nodes in clustered environment

For more information about using SQL statements after installation, see Section 6.1, “Configuring the Databases after Installation,” on page 81.

4.4.3 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.

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 6.1, “Configuring the Databases after Installation,” on page 81.

4.5 Using a Guided Process to Install Identity Governance and Identity Reporting

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

- Section 1.8, “Prerequisites for Installing Identity Governance,” on page 23
- Section 1.9.1, “Identity Governance Server System Requirements,” on page 26
- Release Notes accompanying the release

To perform a silent, unattended installation, see Section 4.6, “Performing a Silent Installation of Identity Governance,” on page 62.

To install Identity Governance:

1. Log in as `root` on Linux server or as an administrator on Windows server to the server where you want to install Identity Governance.
2. (Conditional) Stop Tomcat if you are not using TLS. For examples, see “Stopping, Starting, and Restarting Tomcat” on page 33.
3. From the directory that contains the installation files, complete one of the following actions:
   - **Linux:** Use one of the following commands to install Identity Governance on Linux.
     - **To use the console**: enter `./identity-governance-install-linux.bin -i console`
     - **To use the wizard**: enter `./identity-governance-install-linux.bin`
   - **Windows:** Use one of the following commands to install Identity Governance on Windows.
     - **To use the console**: enter `cmd /c "identity-governance-install-win.exe -i console"`
     - **To use the wizard:** double-click `identity-governance-install-win.exe`

   NOTE: To execute the file, you might need to use the `chmod +x` or `sh` command for Linux or use **Run as administrator** if you did not log in to your Windows server as an administrator.
4. Accept the license agreement, and then select **Next**.
5. Select whether to install Identity Governance, Identity Reporting, or both.
6. Specify an installation path for each installed feature.
7. Complete the guided process, using the following parameters:
   - **Tomcat installation**

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

     Specify the Tomcat folder

     Specifies the path to the Tomcat installation.
     - **Linux:** `/opt/apache-tomcat-x.x.xx`
     - **Windows:** `c:\netiq\idm\apps\tomcat-x.x.xx`

Runtime host name

Applies only when installing Identity Governance.

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

Runtime port

Applies only when installing Identity Governance.

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

Runtime identifier

Applies only when installing Identity Governance.

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

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

- **Tomcat Java Home**

  Represents the path to the Java instance that Tomcat uses. For example, `/root/jdk1.x.x_xx`. The installation process uses Java for several processes, such as to run commands and create security stores.

- **Trust store details**

  Specifies the password for the trust store. The password must be 6 characters and must not contain spaces.

- **Authentication provider**

  Specifies the authentication service you are using, either OSP or Access Manager.

- **Application address**

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

  Application protocol

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

  Application host name

  Do not use `localhost`.

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

  In a clustered environment, specifies the DNS name of the server that hosts the load balancer that you want to use. For more information about installing in a clustered environment, see Section 1.7.5, “Ensuring High Availability for Identity Governance,” on page 21.

  Application port

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

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

  Connect to an external authentication server

  Select to use OSP as the authentication service. Do not select to use Access Manager as the authentication service.

Optional OSP authentication service settings

The following apply only when using OSP as the authentication service.

OSP Protocol

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

OSP Host name

In a non-clustered environment, specifies the DNS name or IP address of the authentication server. In a clustered environment, specifies the DNS name of the server that hosts the load balancer.

OSP Port

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

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

Optional Access Manager authentication service settings

The following apply only when using Access Manager as the authentication service.

IDP host name

In a non-clustered environment, specifies the DNS name or IP address of the authentication server. In a clustered environment, specifies the DNS name of the server that hosts the load balancer.

IDP port

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

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

Access Manager Console host name

In a non-clustered environment, specifies the DNS name or IP address of the Access Manager administration console. In a clustered environment, specifies the DNS name of the server that hosts the load balancer.

Access Manager Console port

Specifies the port that you want the server to use for communication with the Access Manager administration console.

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

Optional Identity Reporting settings

Applies only when installing Identity Reporting.

Specifies the URL settings that connect to the Identity Governance client on the server that hosts Tomcat.

Protocol

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

Host name

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

In a clustered environment, specifies the DNS name of the server that hosts the load balancer.

Port

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

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

- **Authentication details**

Represents the requirements for connecting Identity Governance to the LDAP authentication server (for example, OSP or Access Manager) that contains the list of users who can log in to the application. For more information about the authentication server, see Section 1.2, “Understanding Authentication for Identity Governance,” on page 11.

NOTE: In a clustered environment, specify the host and port for the load balancer's server rather than the authentication server.

Protocol

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

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

Host

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

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

Port

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

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

Service password

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

- **Bootstrap administrator details**

Represents the credentials for the bootstrap administrator. For more information, see Section 1.2.5, “Understanding the Bootstrap Administrator for Identity Governance,” on page 14.

Bootstrap admin name

Applies only if you are using OSP for the authentication service.

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

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

NOTE

- If you use an Identity Vault user as a bootstrap administrator, you must configure Identity Governance to use Identity Vault instead of File in the Identity Governance Configuration Utility (`/idgov/bin/configutil.sh` or `\idgov\bin\configutil.cmd`). The **Bootstrap Administrator** section on the Authentication Server Details tab contains this setting.
- The name of this account must be unique. Do not duplicate any accounts in the `adminusers.txt` file or in the container source or subtrees that you use for authentication.

Password

Applies only if you are using OSP for the authentication service.

Specifies the password for the bootstrap administrator account.

Bootstrap admin DN

Applies only if you are using Access Manager for the authentication service.

Specifies the distinguished name of the bootstrap administrator account.

Bootstrap admin password

Applies only if you are using Access Manager for the authentication service.

Specifies the password for the bootstrap administrator account.

Access Manager admin DN

Applies only if you are using Access Manager for the authentication service.

Specifies the distinguished name of the Access Manager administrator account. The installation program uses this account to log in to Access Manager to configure ISM properties to work with Access Manager.

Access Manager

Applies only if you are using Access Manager for the authentication service.

Specifies the password for the Access Manager administrator account.

- **ActiveMQ details**

Applies only when installing Identity Governance.

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

For more information about configuring ActiveMQ in a clustered environment, see Section 6.3.2, “Configuring ActiveMQ Failover in the Tomcat Cluster,” on page 89.

Host name

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

Port

Specifies the port that the server uses for ActiveMQ.

- **Database Type**

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

For more information about supported versions, see Section 1.9.2, “Database Server System Requirements,” on page 27.

- **Database details**

Represents the settings for the Identity Governance databases. For more information, see Section 1.3, “Understanding the Identity Governance Databases,” on page 15.

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

In a clustered environment, perform the configuration steps only on the primary node in the cluster. For more information about installing in a clustered environment, see Section 1.7.5, “Ensuring High Availability for Identity Governance,” on page 21.

Configure database now

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

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

Generate SQL for later

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

The installation process stores the scripts for Identity Governance in the `./idgov/sql` directory and the scripts for Identity Reporting in the `./idrpt/sql` directory. For more information about using the files, see Section 6, “Completing the Installation Process,” on page 81.

No database configuration

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

Use this setting when you install Identity Governance on a secondary node in the cluster. For more information, see Section 1.7.5, “Ensuring High Availability for Identity Governance,” on page 21.

Host

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

Port

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

Microsoft SQL Server JDBC Jar

Applies only when using an MS SQL Server database

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

Oracle JDBC Jar

Applies only when using an Oracle database

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

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

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

Database name

Applies only when using an Oracle database

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

User tablespace

Applies only when using an Oracle database

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

Temporary tablespace

Applies only when using an Oracle database

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

Administrator user

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

Administrator password

Specifies the password for the database administrator.

Operations

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

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

Archive

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

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

Data collection

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

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

Workflow

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

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

Analytics

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

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

Password (for database owners)

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

Reporting user

Applies only when installing Identity Governance and not installing Identity Reporting at the same time.

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

Reporting user password

Specifies the password for the reporting user specified above.

Update / Use only existing

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

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

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

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

- Operations, Archive, Data collection, Workflow, and Analytics, and Reporting user
- Identity Reporting database name and user if also installing Identity Reporting

- **Report default language**

  Applies only when you install Identity Reporting.

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

  Target locale

  Specifies the locale. Default selection is English.

- **Report email delivery**

  Applies only when you install Identity Reporting.

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

  Default email address

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

  SMTP server

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

  SMTP server port

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

  Use SSL for SMTP

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

Require server authentication

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

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

SMTP user name

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

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

SMTP password

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

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

- **Report retention details**

Applies only when you install Identity Reporting.

Represents the settings for maintaining completed reports.

Keep finished reports for

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

Location of report definitions

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

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

- **Identity Audit**

Represents the settings for collecting auditing events that occur in the Identity Governance and Identity Reporting servers. For more information, see “Enabling Auditing” on page 91.

Enable auditing

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

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

Audit server

Applies only when you enable identity auditing.

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

Audit port

Applies only when you enable identity auditing.

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

Audit cache location

Applies only when you enable identity auditing.

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

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

Secure layer

Applies only when you enable identity auditing.

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

Test certificate trust

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

Specifies whether to attempt to connect to the audit server and trust the retrieved certificate within a temporary trust store file. The actual trust occurs immediately before the summary pages display.

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

8 Review the pre-installation summary.

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

9 (Conditional) Stop Tomcat if it is still running. For examples, see "Stopping, Starting, and Restarting Tomcat" on page 33.

10 (Conditional) If prompted, accept or reject any untrusted 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 Start the installation process.

12 When the installation process completes, select **Done**.

13 Continue to Section 6, "Completing the Installation Process," on page 81.

NOTE: Do **not** start Tomcat.

4.6 Performing a Silent Installation of Identity Governance

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

This section provides guidance for the following activities:

- Section 4.6.1, "Understanding the Passwords that Identity Governance Reads from Environment Variables During the Installation Process," on page 63
- Section 4.6.2, "Creating a Silent Properties File for Installing on a Secondary Node," on page 63
- Section 4.6.3, "Running the Silent Installation," on page 65

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

- Section 1.8, “Prerequisites for Installing Identity Governance,” on page 23
- Section 1.9.1, “Identity Governance Server System Requirements,” on page 26
- Release Notes accompanying the release

To perform a guided installation, see Section 4.5, “Using a Guided Process to Install Identity Governance and Identity Reporting,” on page 53.

4.6.1 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 GUI installation processes. You must set these in the silent properties file.

- `install_authserver_client_secret`: It is the password for OSP.
- `install_bootstrap_secret`: It is the password for the bootstrap administrator. When using OSP, this password gets encrypted and written to a file. 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`.
- `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 generated trust store.
- `install_smtp_secret_auth_user`: It is the password for the SMPT authentication user (used only in Identity Reporting installations).
- `install_nam_admin_secret`: It is the password for the Access Manager console administrator.

4.6.2 Creating a Silent Properties File for Installing on a Secondary Node

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

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

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

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

Log file	Silent.properties file
0	false
1	true

6 Change the values as specified in the following table:

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

7 (Conditional) If installing only Identity Reporting, 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.

4.6.3 Running the Silent Installation

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

2 Stop Tomcat. For examples, see “Stopping, Starting, and Restarting Tomcat” on page 33.

3 Locate the sample `identity-governance-install-silent.properties` file, by default in the same directory as the installation scripts for Identity Governance.

4 (Conditional) In a non-clustered environment or when installing on the primary node, complete the following steps:

4a In a text editor, open the `identity-governance-install-silent.properties` file.

4b Specify the parameter values. For a description of the parameters, see Step 7 on page 53.

4c Save and close the file.

5 (Conditional) When installing on a secondary node in a cluster, you can create the `.properties` file using the steps in Section 4.6.2, “Creating a Silent Properties File for Installing on a Secondary Node,” on page 63.

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

- **Linux:** `./identity-governance-install-linux.bin -i silent -f` *`path_to_silent_properties_file`*
- **Windows:** From a command line, enter: `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 script, you must specify the full path to the file. The script unpacks the necessary files to a temporary directory and then launches the silent installation.

---

7 When the installation process completes, continue to Section 6, “Completing the Installation Process,” on page 81.

NOTE: Do **not** start Tomcat.

5 Installing Identity Reporting

Before you install Identity Reporting, you must decide if you want Identity Reporting to use the Identity Governance security module or the Identity Manager security module. For more information, see "Understanding Identity Reporting" on page 17.

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

- **Linux:** "Installing Identity Manager " in the *NetIQ Identity Manager Setup Guide for Linux*.
- **Windows:** "Installing Identity Reporting" in the *NetIQ Identity Manager Setup Guide for Windows*.

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

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

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

5.1 Checklist for Installing Identity Reporting

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

	Checklist Items
❑	1. Learn about the interaction among Identity Reporting components. For more information, see Section 1.4, "Understanding Identity Reporting," on page 17.
❑	2. Decide which server you want to use for your Identity Reporting components. For more information, see Section 1.7, "Recommended Installation Scenarios and Server Setup," on page 19.
❑	3. Review the considerations for installing Identity Reporting. For more information, see Section 1.8.2, "Prerequisites for Identity Reporting," on page 25.
❑	4. Review the hardware and software requirements for the computer that will host Identity Reporting. For more information, see Section 1.9.3, "Identity Reporting Server System Requirements," on page 28.

	Checklist Items
❑	5. Ensure that the server where you want to install Identity Reporting has the Tomcat application server. For more information, see Chapter 2, “Installing Components Required for Identity Governance,” on page 31.
❑	6. Ensure that you have a database to which the installation process can connect. For more information, see Section 5.3, “Preparing the Database Environment for Identity Reporting,” on page 69.
❑	7. (Conditional) To use an Oracle database, ensure that the schema exists for the reporting user. For more information, see Section 4.3, “Preparing an Oracle Database for Identity Governance,” on page 47 and Section 5.2.2, “Understanding the Users that the Installation Process Creates,” on page 69.
❑	8. Install Identity Reporting: ◆ For a guided installation, see Section 5.4, “Using the Guided Process to Install Identity Reporting,” on page 71. ◆ To install reporting silently, see Section 5.5, “Installing Identity Reporting Silently,” on page 78.
❑	9. Complete the installation and setup for Identity Reporting. For more information, see the following sections: ◆ Section 6.1.4, “Configuring the Identity Reporting Databases,” on page 84 ◆ Section 6.9.2, “Preparing Identity Reporting for Use,” on page 101

5.2 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 1.7, “Recommended Installation Scenarios and Server Setup,” on page 19.

- Section 5.2.1, “Understanding the Installation Process for Identity Reporting,” on page 68
- Section 5.2.2, “Understanding the Users that the Installation Process Creates,” on page 69

5.2.1 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

5.2.2 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
igrptuser	Has the credentials to access the report views and run the reports for Identity Governance
idm_rpt_cfg	Owns the reporting configuration data and the Identity Manager reporting views

5.3 Preparing the Database Environment for Identity Reporting

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

- Section 5.3.1, “Preparing MS SQL Server,” on page 69
- Section 5.3.2, “Preparing Oracle,” on page 70
- Section 5.3.3, “Preparing PostgreSQL,” on page 70

5.3.1 Preparing MS SQL Server

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

5.3.1.1 Obtaining the MS SQL Server JDBC File for the Application Server

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

1. Download the `mssql-jdbc-7.0.0.jar` file from the Microsoft website.
2. Copy the file so that it is accessible during the installation.

5.3.1.2 Creating an MS SQL Server Database for 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 MS SQL Server Database Administrator for the installation process” on page 47.

5.3.2 Preparing Oracle

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

5.3.2.1 Obtaining the Oracle JDBC File for the Application Server

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

1. Download the `ojdbc8.jar` file from the Oracle website.
2. Copy the file so that it is accessible during the installation.

5.3.2.2 Creating an Oracle Database for Reporting

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

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

1. Install a supported version of Oracle.

   For more information, see Section 1.9.2, “Database Server System Requirements,” on page 27.

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

   ---

2. To prepare the database, complete the following steps:
   - **2a** Create or identify the database that you want Identity Reporting to use, such as `igrpt`.
   - **2b** In the database, create the schema for `idm_rpt_cfg` with the `connect` privilege.

     or

     You can allow the installation program to create the schema for you.
   - **2c** Specify a password for the schema.
3. When installing Identity Reporting, specify **Configure database now or at startup** if you want the installation program to generate the schema, tables, and views.

   For more information about using SQL statements after installation, see Section 6.1, “Configuring the Databases after Installation,” on page 81.

5.3.3 Preparing PostgreSQL

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

5.3.3.1 Creating a PostgreSQL Database for Reporting

As a Postgres 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 Section 4.4.3, “Creating a Temporary PostgreSQL Database Administrator for the Installation Process,” on page 52.

5.4 Using the Guided Process to Install Identity Reporting

This procedure describes how to install Identity Reporting for Identity Governance using an installation wizard, either in GUI format or from the console. To perform a silent, unattended installation, see Section 5.5, “Installing Identity Reporting Silently,” on page 78.

To prepare for the installation, review the prerequisites and system requirements listed in Section 1.9.3, “Identity Reporting Server System Requirements,” on page 28. Also see the Release Notes accompanying the release.

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

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

2. Stop Tomcat. For examples, see “Stopping, Starting, and Restarting Tomcat” on page 33.
3. From the directory that contains the installation files, complete one of the following actions:

   NOTE: To execute the file, you might need to use the `chmod +x` or `sh` command for Linux or use **Run as administrator** if you did not log in to your Windows server as an administrator.

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

     Specifies the location for the installation files.
   - **Tomcat installation**

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

Specify the Tomcat folder

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

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

- **Tomcat Java Home**

  Represents the path to the Java instance that Tomcat uses. For example:

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

- **Trust store details**

  Specifies the password for the trust store. The password must be 6 characters and must not contain spaces.

- **Authentication provider**

  Specifies the authentication service you are using, either OSP or Access Manager.

- **Application address**

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

  Application protocol

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

  Application host name

  Do not use `localhost`.

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

  In a clustered environment, specifies the DNS name of the server that hosts the load balancer that you want to use. For more information about installing in a clustered environment, see Section 1.7.5, “Ensuring High Availability for Identity Governance,” on page 21.

  Application port

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

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

  Connect to an external authentication server

  Select to use OSP as the authentication service. Do not select to use Access Manager as the authentication service.

  Optional OSP authentication service settings

  The following apply only when using OSP as the authentication service.

  OSP Protocol

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

  OSP Host name

  In a non-clustered environment, specifies the DNS name or IP address of the authentication server. In a clustered environment, specifies the DNS name of the server that hosts the load balancer.

OSP Port

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

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

Optional Access Manager authentication service settings

The following apply only when using Access Manager as the authentication service.

IDP host name

In a non-clustered environment, specifies the DNS name or IP address of the authentication server. In a clustered environment, specifies the DNS name of the server that hosts the load balancer.

IDP port

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

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

Access Manager Console host name

In a non-clustered environment, specifies the DNS name or IP address of the Access Manager administration console. In a clustered environment, specifies the DNS name of the server that hosts the load balancer.

Access Manager Console port

Specifies the port that you want the server to use for communication with the Access Manager administration console.

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

Identity Reporting settings

Specifies the URL settings that connect to the Identity Governance client on the server that hosts Tomcat.

Protocol

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

Host name

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

In a clustered environment, specifies the DNS name of the server that hosts the load balancer.

Port

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

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

- **Authentication details**

Represents the requirements for connecting Identity Governance to the LDAP authentication server (for example, OSP or Access Manager) that contains the list of users who can log in to the application. For more information about the authentication server, see Section 1.2, “Understanding Authentication for Identity Governance,” on page 11.

NOTE: In a clustered environment, specify the host and port for the load balancer’s server rather than the authentication server.

Protocol

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

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

Host

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

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

Port

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

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

Service password

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

- **Database Type**

  Specifies the platform you want to use for the reporting database.

  For more information about supported versions, see Section 1.9.2, “Database Server System Requirements,” on page 27.

- **Database details**

  Represents the settings for the reporting database. For more information, see Section 1.3, “Understanding the Identity Governance Databases,” on page 15.

  To connect to an existing database instance, you must specify the name of the existing reporting database.

  In a clustered environment, perform the configuration steps only on the primary node in the cluster. For more information about installing in a clustered environment, see Section 1.7.5, “Ensuring High Availability for Identity Governance,” on page 21.

  Configure database now

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

  NOTE: Ensure that you specified the correct name for the existing database.

  Generate SQL for later

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

  The installation process stores the scripts in the following directory:

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

    For more information about using the files, see Section 6, “Completing the Installation Process,” on page 81.

No database configuration

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

Use this setting when you install Identity Reporting on a secondary node in the cluster. For more information, see Section 1.7.5, “Ensuring High Availability for Identity Governance,” on page 21.

Host

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

Port

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

Microsoft SQL Server JDBC Jar

Applies only when using an MS SQL Server database

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

Oracle JDBC Jar

Applies only when using an Oracle database

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

- **Linux:** `opt/oracle/ojdbc8.jar`
- **Windows:** `c:\ProgramFiles\Oracle\ojbc8.jar`

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

Database name

Applies only when using an Oracle database

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

User tablespace

Applies only when using an Oracle database

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

Temporary tablespace

Applies only when using an Oracle database

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

Administrator user

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

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

Administrator password

Specifies the password for the database administrator.

Test Connection

Checks that the installation program can connect to the Identity Reporting database.

Reporting database name

Does not apply when using an Oracle database

Specifies the name of the Identity Reporting database. The default name is `igrpt`.

Reporting database user password

Specifies the password for the reporting database user, `idm_rpt_cfg`.

Update / Use only existing

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

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

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

- **Report default language**

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

Target locale

Specifies the locale. Default selection is English.

- **Report email delivery**

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

Default email address

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

SMTP server

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

SMTP server port

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

Use SSL for SMTP

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

Require server authentication

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

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

SMTP user name

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

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

SMTP password

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

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

- **Report retention details**

Represents the settings for maintaining completed reports.

Keep finished reports for

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

Location of report definitions

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

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

- **Identity Audit**

Represents the settings for collecting auditing events that occur in the Identity Reporting server. For more information, see "Enabling Auditing" on page 91.

Enable auditing

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

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

Audit server

Applies only when you enable identity auditing.

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

Audit port

Applies only when you enable identity auditing.

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

Audit cache location

Applies only when you enable identity auditing.

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

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

Secure layer

Applies only when you enable identity auditing.

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

Test certificate trust

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

Specifies whether to attempt to connect to the audit server and trust the retrieved certificate within a temporary trust store file. The actual trust occurs immediately before the summary pages display.

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

---

7 Review the pre-installation summary.

8 (Conditional) Stop Tomcat if it is still running. For examples, see "Stopping, Starting, and Restarting Tomcat" on page 33.

9 (Conditional) If prompted, accept or reject any untrusted 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

10 Start the installation process.

11 When the installation process completes, select **Done**.

12 Continue to Section 6, “Completing the Installation Process,” on page 81.

NOTE: Do **not** start Tomcat.

5.5 Installing Identity Reporting Silently

A silent (non-interactive) installation does not display a user interface or ask the user any questions. Instead, the system uses information from a silent properties file. You can run the silent installation after editing the file to customize the installation process for your environment. To perform a guided installation, see Section 5.4, “Using the Guided Process to Install Identity Reporting,” on page 71.

To prepare for the installation, review the prerequisites and system requirements listed in Section 1.9.3, “Identity Reporting Server System Requirements,” on page 28. Also see the Release Notes accompanying the release.

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

2 (Conditional) To avoid specifying passwords for the installation in the silent properties file for a silent installation, use the `export` or `set` command. For example:

```
export install_db_reporting_secret=myPassWord
```

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

Specify the following passwords:

install_db_admin_secret

Specify the password for the administrator for the reporting database.

install_db_reporting_secret

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

install_smtp_secret_auth_user

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

install_authserver_client_secret

Specify the client ID password for authenticating using Access Manager or OSP.

install_truststore_secret

Specify the password for the trust store.

3 To specify the installation parameters, complete the following steps:

3a Locate the sample `identity-governance-install-silent.properties` silent properties file, by default in the same directory as the installation scripts for Identity Governance.

3b In a text editor, open the silent properties file.

3c Specify the parameter values. For a description of the parameters, see Step 6 on page 71.

3d Save and close the file.

4 Stop the application server, such as Tomcat. For examples, see “Stopping, Starting, and Restarting Tomcat” on page 33.

5 To launch the installation process, enter the following command:

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

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

---

6 When the installation process completes, continue to Section 6, “Completing the Installation Process,” on page 81.

6 Completing the Installation Process

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

6.1 Configuring the Databases after Installation

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

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

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

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 6.1.1, “Configuring the PostgreSQL Databases for Identity Governance,” on page 82
- Section 6.1.2, “Configuring the Oracle Database for Identity Governance,” on page 83
- Section 6.1.3, “Configuring the MS SQL Database for Identity Governance,” on page 84
- Section 6.1.4, “Configuring the Identity Reporting Databases,” on page 84

6.1.1 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`, and `igara` database passwords rather than the database administrator password.

---

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

```
CREATE ROLE operations_db_name LOGIN password 'password';
CREATE ROLE 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` and `/opt/netiq/idm/apps/idrpt/sql`
- **Windows:** `c:\netiq\idm\apps\idgov\sql` and `c:\netiq\idm\apps\idrpt\sql`

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

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

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

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

6.1.2 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.

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

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

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

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

6.1.3 Configuring the MS SQL Database for Identity Governance

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

NOTE: You must create the roles with the `igops`, `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` and `/opt/netiq/idm/apps/idrpt/sql`
   - **Windows:** `c:\netiq\idm\apps\idgov\sql` and `c:\netiq\idm\apps\idrpt\sql`
3. To populate the global configuration values in the database, enter the following command:

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

   For 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 netiq -
   dbUrl "jdbc:sqlserver://mysever.netiq.com:1433;databaseName=igops" -script "/
   opt/netiq/idm/apps/idgov/scripts/all-import-configs.script"
   ```

6.1.4 Configuring the Identity Reporting Databases

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

- **Linux:** `/opt/netiq/idm/apps/idrpt/sql`

- **Windows:** `c:\netiq\idm\apps\idrpt\sql`

If you cannot access the SQL scripts, see Section 6.9.1, “Manually Generating the Database Schema,” on page 100.

6.2 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 authentication server require some additional steps. Also, if you did not enable auditing during the installation process and want to enable it for OSP, you must run some additional steps.

6.2.1 Ensuring the Configuration Update Utility Can Run OSP

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

1 Create a backup copy of the `ism-configuration.properties` file.
   - **Linux:** Default location in `/opt/netiq/idm/apps/tomcat/conf`
   - **Windows:** Default location in `C:\opt\netiq\idm\apps\tomcat\conf`
2 In a text editor, open the `configupdate.sh.properties` or `configupdate.bat.properties`.to update values.
   - **Linux:** Default location in `/opt/netiq/idm/apps/configupdate`
   - **Windows:** Default location in `c:\netiq\idm\apps\configupdate`

   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 Configuration Update utility in GUI mode

   2b Save and close the file.
3 Update settings in the Configuration Update utility.

   3a Launch the Configuration Update utility.
      - **Linux:** Default location in the `/opt/netiq/idm/apps/configupdate`

        ```
        ./configupdate.sh edition=none
        ```

- **Windows:** Default location in `C:\netiq\idm\apps\configupdate`

  ```
  configupdate.bat edition=none
  ```

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

3b Select **SSO Clients**.

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

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

- **OAuth client ID**

  For example, `rpt`.
- **OAuth client secret**
- **URL link to landing page**

  For example, `http://123.456.78.90:8180/#/landing`
- **URL link to Identity Governance**

  For example, `http://123.456.78.90:8080/#/nav`
- **OSP Oauth redirect url**

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

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

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

- **OAuth client ID**

  For example, `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 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 Tomcat.

6.2.2 Preparing OSP to Use an Active Directory LDAP Server

To use Active Directory for your LDAP authentication server, you need to update the settings using the Configuration Update utility.

1. Ensure that you have prepared the Configuration Update utility for OSP. For more information, see Section 6.2.1, “Ensuring the Configuration Update Utility Can Run OSP,” on page 85.
2. Stop Tomcat, if it is running. For examples, see “Stopping, Starting, and Restarting Tomcat” on page 33.

3 Launch the Configuration Update utility.

- **Linux:** Default location in the `/opt/netiq/idm/apps/configupdate`

  ```
  ./configupdate.sh edition=none
  ```

- **Windows:** Default location in `C:\netiq\idm\apps\configupdate`

  ```
  configupdate.bat edition=none
  ```

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

4 Select **Reporting > Identity Vault Settings > Identity Vault User Identity > Login Attribute**.

5 For **Login Attribute**, specify the attribute in Active Directory that you want to use for logging in to Identity Governance. For example, `sAMAccountName`.

NOTE: This value is case-sensitive.

6 To save your change, select **OK**.

7 Update settings in the Identity Governance Configuration utility:

7a Launch the Identity Governance Configuration utility.

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

  ```
  ./configutil -password database_password
  ```

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

  ```
  configutil -password database_password
  ```

7b Select **Security Settings**.

7c For **Auth Matching Rules**, add the same attribute from Active Directory that you specified for **Login Attribute** in Step 5.

Do not delete `dn`. For example, the setting should now list `dn` and `sAMAccountName`.

7d Select **Save**.

8 Continue with the post-installation tasks, as required.

6.2.3 Enabling Auditing for OSP after the Installation

If during the OSP installation process you did not enable auditing, you can enable it at anytime. For more information, see “Enabling Auditing after the Installation” on page 92.

6.3 Completing the Cluster Configuration for Identity Governance

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

6.3.1 Configuring the Nodes in the Tomcat Cluster

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

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

For more information, see Section 1.7.5, “Ensuring High Availability for Identity Governance,” on page 21.

1. Stop Tomcat, if the application server is running. For examples, see “Stopping, Starting, and Restarting Tomcat” on page 33.
2. To specify a unique runtime identifier, complete the following steps:
   - **2a** Log in to primary node in the cluster.
   - **2b** In a text editor, open the `ism-configuration.properties` file.
     - **Linux:** Default location in `/opt/netiq/idm/apps/tomcat/conf`
     - **Windows:** Default location in `c:\netiq\idm\apps\tomcat\conf`
   - **2c** Ensure that `com.netiq.iac.runtime.id` is a unique value that represents the node.

     For example, `node1` or `ProdNode1`.
   - **2d** Save and close the file.
   - **2e** Repeat this procedure for each node in the cluster.
3. To specify a different port for a node than the port exposed by the load balancer, complete the following steps:
   - **3a** Log in to the node where you want to change the port.
   - **3b** In a text editor, open the `ism-configuration.properties` file.
     - **Linux:** Default location in `/opt/netiq/idm/apps/tomcat/conf`
     - **Windows:** Default location in `c:\netiq\idm\apps\tomcat\conf`
   - **3c** For `com.netiq.iac.url.local.port`, specify the Tomcat port for the local node.
   - **3d** Save and close the file.

6.3.2 Configuring ActiveMQ Failover in the Tomcat Cluster

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

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

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

   For more information, see Appendix A, “Running the Identity Governance Configuration Utility,” on page 133.
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.

6.3.3 Cleaning Up Unfinished Data Production Jobs

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

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

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

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

3 For each production record from the SQL statement results do the following:

3a Execute a REST API call GET /dataprod/mgt/id using the production ID.

3b Modify the payload by setting the runtime identifier in the payload to the node identifier where you want to reassign the production process.

3c Execute a REST API call PUT /dataprod/mgt/id using the production ID and modified payload from step 3b.

6.4 Using the TLS/SSL Protocol for Secure Connections

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

- HTTP, which provides end-user access to and from Identity Governance
- LDAP, which ensures secure communication between Identity Governance and the authentication server
- JDBC, which ensures secure communication between Identity Governance and the database server

TLS/SSL protocols are not configured by default. During installation, you should specify *https* as the protocol for communication with the database and authentication server. The OSP installation process creates symmetric keys and key pairs for signing, encryption, and TLS and stores them in the OSP key store. The Identity Governance installer places a single invalid certificate in its trust store. Both installation programs place trusted certificates from external servers into their respective trust stores to allow communications with the external servers. You can configure Identity Governance to use the TLS/SSL protocol before putting the system into production.

We highly recommend that you configure Tomcat to use https with either TLSv1.2 or TLS1.1. Any prior version of TLS should not be used. For more information, see “Securing Tomcat.”

For more information about the Identity Governance Configuration Utility, see Appendix A, “Running the Identity Governance Configuration Utility,” on page 133.

To configure secure communication with the authentication server:

1 Stop Identity Governance (and Tomcat). For examples, see “Stopping, Starting, and Restarting Tomcat” on page 33.

2 Run the Identity Governance Configuration Utility.

3 For **Authentication Server Details** and **Network Topology**, verify that the connection protocol for the servers is set to *https*.

4 Select **Save**, and then close the utility.

5 Ensure that the specified host and port for the authentication server support TLS/SSL communication.

6 Start Identity Governance (and Tomcat). For examples, see “Stopping, Starting, and Restarting Tomcat” on page 33.

6.5 Ensuring Rapid Response to Authentication Requests

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

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

---

1 If using with Identity Manager, to specify the login attribute, complete the following steps:

   1a Run the RBPM Configuration utility.

   For more information, see “Configuring the Identity Manager Components” in the *NetIQ Identity Manager Setup Guide for Linux*.

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

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

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

   1d Save your changes.

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

   2a Create the index.

   For more information, see “Creating an Index” in the *NetIQ eDirectory Administration Guide*.

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

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

   2d Complete the process for creating the index.

6.6 Enabling Auditing

Identity Governance generates common event format (CEF) events that you can forward on 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:

- Identity Governance
- Identity Reporting
- OSP

You can enable auditing during the installation of Identity Governance, or you can use the Identity Governance Configuration Update utility to enable auditing any time after you have installed Identity Governance.

6.6.1 Enabling Auditing after the Installation

In prior releases of Identity Governance you would edit the `ig-server-logging.xml` file to enable auditing for the different components. Use the Identity Governance Configuration Update utility to enable auditing if you did not enable auditing during the installation of the components. Use the Identity Governance Configuration Update utility to change the server details, TLS settings, and to enable auditing for the different components instead of editing the `ig-server-logging.xml` file.

WARNING: If you make changes for the server details, TLS settings, or if you enable auditing for Identity Governance in the `ig-server-logging.xml file`, it can cause the Identity Governance Configuration Update utility to no longer affect these audit settings.

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

To enable auditing after the installation:

1. Stop the application server. For more information, see Section 2.5, “Stopping, Starting, and Restarting Tomcat,” on page 33.
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**. Options you can choose are:

   Send audit events

   Select this option to enable auditing for this server.

   Destination host

   Specify 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 6.4, “Using the TLS/SSL Protocol for Secure Connections,” on page 90.

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** to save the changes and the Identity Governance Configuration Update utility automatically closes.

5 Start the application server. For more information, see Section 2.5, “Stopping, Starting, and Restarting Tomcat,” on page 33

You can see a list of the audit events here AuditEventTable.pdf (https://www.netiq.com/documentation/identity-governance-35/references/AuditEventTable.pdf).

6.6.2 Audit Properties

The Identity Governance installation program creates a properties file, `tomcat/conf/ig-server-logging.xml`, to use for audit settings. It contains default values on the right-side of the colon for each property that cannot be found during the installation. Identity Governance supports TCP and TLS protocols. OSP supports TCP, TLS, and UDP protocols.

Identity Governance and OSP define and use the following properties for audit events:

- `com.netiq.ism.audit.cef.cache-file-dir`
- `com.netiq.ism.audit.cef.enabled`
- `com.netiq.ism.audit.cef.host`
- `com.netiq.ism.audit.cef.port`
- `com.netiq.ism.audit.cef.protocol`

Identity Governance also defines and uses the following properties for audit events:

- `<cache-file>ig-server</cache-file>`
- `com.netiq.iac.product`
- `com.netiq.iac.companyName`
- `com.netiq.iac.productVersion`

When `com.netiq.ism.audit.cef.protocol` is set to TLS, the following properties indicate which trust stores contain the certificates for connecting to the audit server:

- `com.netiq.idm.osp.ssl-keystore.file`
- `com.netiq.idm.osp.ssl-keystore.pwd`
- `com.netiq.idm.osp.ssl-keystore.type`

In OSP environments, the following properties contain trust store information:

- `com.netiq.idm.osp.oauth-truststore.file`
- `com.netiq.idm.osp.oauth-truststore.pwd`
- `com.netiq.idm.osp.oauth-truststore.type`

6.7 Configuring the Mail Server for Notifications

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

You can also configure Identity Governance to send reminders of tasks, based on the escalation timeout setting. For more information, see "Creating and Modifying Review Definitions" in *NetIQ Identity Governance Administrator 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 emails use the default language for the system. You can customize the content in the emails. For more information, see "Customizing the Email Notification Templates" in *NetIQ Identity Governance Administrator Guide*.

To configure the mail server for notifications:

1. In the Identity Governance Configuration Utility, select **Workflow Settings**.
2. Under **Notification System**, specify the settings for the mail server.
3. Select **Save**.
4. (Conditional) To ensure guaranteed delivery of the notifications by using ActiveMQ, complete the following steps:
   - **4a** Select **Enable persistent notification message queue**.
   - **4b** Enter the settings for the JMS broker.
   - **4c** (Optional) To use TLS/SSL protocol for messaging, select **SSL** and then specify the keystore settings.
   - **4d** Select **Save**.
   - **4e** Navigate to the installation directory for ActiveMQ. For example, .
     - **Linux:** `/opt/netiq/idmapps/apache-activemq-x.x.x`
     - **Windows:** `c:\netiq\idmapps\apache-activemq-x.x.x`
   - **4f** Copy the `activemq-all-x.x.x.jar` file.
   - **4g** Navigate to the installation directory for the Tomcat server supporting Identity Governance. For example, .
     - **Linux:** `/opt/apache-tomcat-x.x.xx`
     - **Windows:** `c:\ProgramFiles\apache-tomcat\x.x.xx`
   - **4h** In the `lib` directory of the Tomcat installation, paste the `activemq-all-x.x.x.jar` file.
   - **4i** Restart Tomcat after copying the `activemq-all-x.x.x.jar` file. For examples, see "Stopping, Starting, and Restarting Tomcat" on page 33.
5. (Optional) To change the text in the email notifications, see "Customizing the Email Notification Templates" in *NetIQ Identity Governance Administrator Guide*.

6.8 Configuring Identity Governance for Two-Factor Authentication

If you want to configure Identity Governance to use two-factor authentication, this section shows how to configure OSP on your Identity Governance server with NetIQ Advanced Authentication. For more information, see the Advanced Authentication documentation.

After you have an Identity Governance server and an Advanced Authentication server running and reachable in your environment, use the following sections to configure the two-factor authentication:

6.8.1 Prerequisites for Configuring Two-Factor Authentication

Before configuring the servers for two-factor authentication, ensure the following conditions exist:

- ❒ Server time is in sync for the Identity Governance and Advanced Authentication servers
- ❒ Each server can correctly resolve the DNS name of the other server
- ❒ You must have OSP installed and running on the Identity Governance server

6.8.2 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 the Identity Vault Identity Governance uses for authentication for the two-factor authentication to work.

This section assumes you have a good working knowledge and understanding of Advance Authentication. For more information, see the Advanced Authentication documentation.

1. Log in with administrator credentials to the Advanced Authentication Administration portal.
2. Click **Repositories**, then click **Add**.
3. Complete the guided process, using the following parameters:

   LDAP type

   Select the appropriate type for the Identity Vault you use with your Identity Governance server.

   Name

   Specify a name for this repository.

   Base DN

   Specify the base DN where Advances Authentication searches for the users in the Identity Vault. For example, `o=data`.

User

Specify the administrator user name in LDAP format. For example, `cn=admin,ou=sa,o=system`.

Password

Specify the password for the administrative user.

Group DN

(Optional) Specify a group DN if you want to collect groups.

4 Under **LDAP Servers**, click **Add Server**, then specify the DNS name of the LDAP server and the port.

5 Save the server details.

6 (Optional) To change default attributes or collect a new attribute, click **Advanced settings** and then edit the following settings:

User Lookup Attributes

These attributes specify the LDAP attributes Advanced Authentication uses to find a user object in the directory. The attribute names used must match the names configured in the Identity Governance Configuration Update utility. **Identity Vault:Login** attribute (by default, `cn`) and **Authentication:Duplicate** resolution naming attribute (by default, `mail`).

IMPORTANT: Expand **Advanced settings** and ensure that the **User lookup** attribute is configured. If you are using the **Email OTP** method, then you must configure the **User mail** attributes.

If using Active Directory with Identity Governance, use `sAMAccountName` instead of `cn`.

User Mail Attributes

This option must contain the names of LDAP attributes used to hold a user's email address. The default values are typically sufficient.

IMPORTANT: Ensure that all users in your Repository have unique email IDs.

---

7 Click **Save** to save the repository details.

For more information, see "Adding a Repository" in the *Advance Authentication Administration Guide*.

8 Find the new repository that you just created, then click **Edit > Full sync** to sync the users and groups from the LDAP server.

9 Define the method for two-factor authentication of **EMail OTP** and **LDAP Password**.

9a Click **Methods > Email OTP** to it edit this method.

9b Change the different setting for your environment. For example, change **OTP Period**, **OTP Format, Sender Email**, and **Subject**.

9c Click **Save** to save the **Email OTP** method.

9d Click **LDAP Password**.

9e Change the different settings for the LDAP Identity Vault Identity Governance uses, then click **Save**.

For more information, see "Configuring Methods" in the *Advance Authentication Administration Guide*.

10 Configure the mail sender for the **Email OTP** method.

10a Under **Policies**, click **mail sender**.

10b Specify the host, port, user name, password, and whether you want to enable TLS/SSL.

10c Click **Save** to save the changes for your environment.

11 Create a chain to make the authentication methods available for OSP.

11a Click **Chains** to make the chain available to the users.

11b Click **Add** to create a new chain.

11c In the **Name** filed, specify a name for this new chain.

11d Set **Is enable** to **On**.

11e Select the methods you created in Step 9 This allows the users to enter their LDAP password and then perform an OTP validation.

11f In the **Roles and Group** field, type `A` to find the **ALL USERS** group, then select the **ALL USERS** group.

11g Set any additional option that you require, then click **Save**.

For more information, see "Creating a Chain" in the *Advance Authentication Administration Guide*.

12 Create an event to define the type of authentication event you use.

12a Click **Events**.

12b Click the **Edit** icon next to the authentication event.

12c Ensure that **Is enabled** is set to **ON**.

12d Select the event type.

For example, you would select **Windows logon** if your Identity Vault is Active Directory.

12e Select the chain you created in Step 11.

12f Set any additional options that you require, then click **Save**.

For more information, see "Configuring Events" in the *Advanced Authentication Administration Guide*.

6.8.3 Configure OSP for Two-Factor Authentication

Ensure that you have created the methods, chain, and events in Advanced Authentication before proceeding. You must configure OSP to accept the authentications from Advance Authentication.

1 Execute the Identity Governance Configuration Update utility.

- **Linux:** The utility is `configupdate.sh` on Linux.

```
/opt/netiq/idm/apps/osp/bin/configupdate.sh edition=none
```

- **Windows:** The utility is `configupdate.bat` on Windows.

```
C:\netiq\idm\apps\osp\bin\configupdate.bat edition=none
```

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

---

2 Click the **Authentication** tab, then click **show advanced options**.

3 Under **Authentication method**, select the **Enable two factor authentication** option.

4 Click the **Second factor** tab, then fill out the following fields:

Advanced Authentication Administrator > Admin Name

Specify the repository-qualified name of the Advanced Authentication administrator account that OSP uses to interface with Advanced Authentication. Typically, the account is in the `LOCAL` repository.

The default Advanced Authentication administrator account is named `admin`. If you used this account, then the **Admin name** value is:

`LOCAL\admin` (repository name + \ + user name)

Advance 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 95. This repository corresponds to the Identity Vault for Identity Governance.

Advanced Authentication Servers

Click **Add**, then specify the DNS name or IP address of the Advanced Authentication server. If you use a different port than 443, specify that port as well.

(Conditional) If you have clustered the Advanced Authentication server, then click **Add** again, and specify each DNS name or IP address for each server in the cluster.

Advanced Authentication Endpoint

An Advanced Authentication endpoint is an identifier and secret that ensures that the entity performing authentication with the Advanced Authentication server is authorized to do so.

If no endpoint data is found in the configuration (or if the endpoint data in the configuration cannot be resolved with the Advanced Authentication server) then the **Create new endpoint** box is checked. Specify a name and description for the new endpoint you want to create. The name and description appear in the **Endpoints** section of the Advanced Authentication administrator interface.

If you have already created an endpoint, and the endpoint information is in the configuration, and Identity Governance the endpoint data can resolve with the Advanced Authentication server, then the Identity Governance Configuration Update utility does not select **Create new endpoint box** and it displays the endpoint identifier and a representation of the endpoint secret.

Second Factor Conditions

If you want to require all users to supply a second authentication factor at all times then check **All users, all the time**.

Otherwise deselect the option, then specify conditions for your environment using the following information:

User Login Condition

When you deselect **All users, all the time**, the **User Login Condition** editor appears. This editor allows you to configure an expression that defines under which conditions Identity Governance uses the second factor authentication.

For example, if users do not have mobile devices then you should use **Email OTP** as a second factor authentication.

You build a login condition of expressions that evaluate various operands including user LDAP attributes, server attributes like time-of-day, and date, and HTTP request values like originating IP address, session attributes like session age and so forth. You can negate the expressions and combine the expressions using logical AND and OR operators.

Second Factor Authentication Methods

Use this advanced option to enable and disable the available second factor methods and define the relative priority of each method you want to set.

If you disable a method by deselecting the box next to the method name, then that method is not available for authentication even if a user is enrolled in that method.

Identity Governance uses the relative priority of second factor methods to determine which method it should use if a user is enrolled in more than one method.

For example, using the default values configuration the **Email OTP** has a higher priority than the **LDAP password** method. Therefore, even if a user has enrolled in both methods, Identity Governance selects the **Email OTP** method for that user. You can change the behavior such that Identity Governance selects the LDAP Password by making the **TOTP** priority higher than **Email OTP**.

NOTE: **Email OTP** methods do not need enrollment to be available for a user. It is enabled by default.

---

5 Click **OK** to save the configuration, then exit out of the Identity Governance Configuration Update utility.

6.8.4 Testing the Enrolled Methods

After you have configure Advanced Authentication and Identity Governance for two-factor authentication, you can test the methods to ensure that they work.

1 Log in to the Advanced Authentication server as an end user.

2 View the **Enrolled** and **Not Enrolled** methods.

3 Enroll the methods for the test user by clicking on the appropriate method, then click **Test**.

4 Ensure that the test is successful, then save the method for the user.

5 Log in to Identity Governance and OSP redirects you to use the second factor authentication.

6.9 Setting Up Identity Reporting

After installing Identity Reporting, you can modify many of the installation properties. To make changes, run the configuration update utility.

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

If you change any setting for Identity Reporting with the configuration utility, you must restart the application server that hosts Identity Reporting for the changes to take effect. However, you do not need to restart the server after making changes in the web user interface for Identity Reporting.

For more information about installing this component, see Chapter 5, “Installing Identity Reporting,” on page 67.

6.9.1 Manually Generating the Database Schema

You can recreate the database tables after installation without having to reinstall.

1. Stop the application server, such as Tomcat. For more information, see “Stopping, Starting, and Restarting Tomcat” on page 33.
2. (Conditional) Delete the existing database.
3. (Conditional) Create a new database with the same name as the one that you deleted in Step 2.
4. (Conditional) Clear the database checksums.
   - **4a** Log in to your database as `idm_rpt_cfg`.
   - **4b** Execute the following command for PostgreSQL:

```
  DO
$do$
 BEGIN
  IF EXISTS
   (select table_name from information_schema.tables where table_schema =
'public' and table_name = 'databasechangelog')
  THEN
   update databasechangelog set md5sum = null;
  END IF;
END $do$
```

   or

   Execute the following command for Oracle:

```
  BEGIN
 FOR i IN
  (select null from ALL_TABLES where OWNER = user and TABLE_NAME =
'DATABASECHANGELOG')
 LOOP
  EXECUTE IMMEDIATE 'update DATABASECHANGELOG set MD5SUM = NULL';
 END LOOP;
END;
```

   or

   Execute the following command for MSSQL:

```
IF EXISTS (SELECT * FROM INFORMATION_SCHEMA.TABLES WHERE TABLE_NAME =
'DATABASECHANGELOG')
UPDATE idm_rpt_cfg.DATABASECHANGELOG
SET MD5SUM = NULL
```

5. Define the `JAVA_HOME` variable. For example:
   - **Linux:** `export JAVA_HOME=/opt/netiq/idm/apps/jre`
   - **Windows:** For instructions, see “Add Paths to Zulu on Windows (https://docs.azul.com/zulu/zuludocs/ZuluUserGuide/PostInstallationTasks/AddPathsToZulu_Windows.htm)”.

6 Re-initialize the database using the installed script:

- `/opt/netiq/idm/apps/idrpt/bin/db-init.sh -password ***`
- `/opt/netiq/idm/apps/idrpt/bin/db-init.sh -password *** -sql > /opt/netiq/idm/apps/idrpt/sql/output.sql`

7 Start the application server such as Tomcat. For more information, see “Stopping, Starting, and Restarting Tomcat” on page 33.

6.9.2 Preparing Identity Reporting for Use

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. In general, your data source is the Identity Governance database.

To prepare Identity Reporting for daily use, complete the following activities:

- Section 6.9.2.1, “Starting Identity Reporting,” on page 101
- Section 6.9.2.2, “Assigning the Report Administrator Authorization,” on page 102
- Section 6.9.2.3, “Testing the Integration with Identity Governance,” on page 102
- Section 6.9.2.4, “Adding Data Sources to Identity Reporting,” on page 103

You should also update to the latest version of the Identity Governance reports. For more information, see “Using the Download Page” in *NetIQ Identity Governance Identity Reporting Guide*.

6.9.2.1 Starting Identity Reporting

To verify installation and to initialize the Identity Reporting database, you must start the application server.

1 Log in to the application server that hosts Identity Reporting.

2 (Conditional) If this is the first time for starting Identity Reporting, complete the following steps:

2a Delete all files and folders in the following directories for your application server:

- **Linux:** Temporary directory, located by default in
  - `/opt/netiq/idm/apps/tomcat/temp`
  - Catalina directory, located by default in `/opt/netiq/idm/apps/tomcat/work/Catalina`
- **Windows:** Temporary directory, located by default in:
  - `C:\netiq\idm\apps\tomcat\temp`
  - Catalina directory, located by default in `C:\netiq\idm\apps\tomcat\work\Catalina`

2b Delete all log files from the logs directory of your application server, located by default in: .

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

3 Start Tomcat. For examples, see “Stopping, Starting, and Restarting Tomcat” on page 33.

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

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

When the process completes, the file contains the following message:

```
Server startup in nnnn ms
```

5 To log in to Identity Reporting, you need an account with the Report Administrator authorization.

For more information, see Section 6.9.2.2, “Assigning the Report Administrator Authorization,” on page 102.

6.9.2.2 Assigning the Report Administrator Authorization

To log in to Identity Reporting, your account must have the Report Administrator authorization in Identity Governance.

1 Log in to Identity Governance as the Global Administrator.
2 Select **Administration > Authorization Assignments**.
3 Assign users or groups to the Report Administrator authorization.
4 Save the change.
5 Select **Identity Manager System Connection Information**.
6 For **Identity Manager URL**, specify the URL for Identity Reporting.

For example, `http://myserver.mydomain.com:8080/IDMRPT`.

7 Save the change, then refresh the browser to see the change.

6.9.2.3 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 URL. Only accounts with the Report Administrator authorization should be able to log in to Identity Reporting.

1 To verify that you can access Identity Reporting from Identity Governance, complete the following steps:
   1a Log in to Identity Reporting, select **Home** in the upper right corner.
   1b Select the **Reporting** module icon near your user name.
   1c Verify that you are redirected to Identity Reporting.
2 To verify that other authorizations are denied access to Identity Reporting, complete the following steps:
   2a Log in to Identity Governance, as a Global Administrator or Security Officer.
   2b Remove the Report Administrator authorization from the account that successfully logged in to Identity Reporting.
   2c Log in to Identity Reporting with that account, which no longer has the authorization.

   You should attempt the log in from both Identity Governance and the reporting URL.
   2d Verify you cannot access Identity Reporting.

   You can also attempt to log in to Identity Reporting by using a Global Administrator or Security Officer account to verify that accounts with high-level privileges cannot access Identity Reporting without the Report Administrator authorization.

6.9.2.4 Adding Data Sources to Identity Reporting

Identity Reporting runs reports against your connected data sources. Before you can run reports, you need to add the data sources.

NOTE: You must add the Identity Governance `igops` database as a data source in Identity Reporting.

1. Log in to Identity Reporting as the Report Administrator.
2. Select **Data Sources**.
3. Select **Add**.
4. Specify whether you want to select from the list of data sources or provide the details for the source.
5. (Conditional) If you selected **Provide database details**, specify the values for the data source. For example, database platform, the host name or IP address of the database server, and include the following settings:

   Database

   Specifies the name of the database. For example, to add the Identity Governance database, specify `igops` for PostgreSQL and `orcl` or whatever name you gave the Oracle database.

   Username

   Specifies an account that can access the tables and views in the database. For example, when adding the Identity Governance database, specify `igrptuser`.
6. (Optional) Test the connection to your data source.
7. Select **Save**.
8. Clean up the Tomcat folders as described in Step 2 on page 101.

   You might need to restart Tomcat.
9. Run a test report to verify functionality in Identity Reporting.

   For more information about running reports, see [add xref to correct section in admin guide].

6.9.3 Enabling Auditing for Identity Reporting after Installation

If you did not enable auditing for Identity Reporting during the installation, you must perform additional steps to enable auditing for Identity Reporting.

1. Stop the application server. For more information, see "Stopping, Starting, and Restarting Tomcat" on page 33.
2. Launch the configuration update utility:
   - **2a** Navigate to one of the following directories:
     - **Linux:** `/opt/netiq/idm/apps/configupdate/configupdate.sh`
     - **Windows:** `C:\netiq\idm\apps\configupdate\configupdate.bat`
   - **2b** Launch the configuration update utility:
     - **Linux:** `./configupdate.sh`
     - **Windows:** `configudate.bat`
   - **2c** In GUI mode, click **CEF Auditing > Auditing Settings**, then click **Send audit events**.

2d In Console mode:

2d1 Enter the number for **CEF Auditing**. By default it is #4.

2d2 Enter the number for the Auditing settings. By default it is #1.

2d3 Enter number 1 to enable auditing.

2d4 Enter the destination host and port.

2d5 Enter the network protocol.

2d6 Enter whether to use TLS.

2d7 Enter the intermediate event store directory. This file location must exist.

2e Save and close the configuration update utility.

3 Edit the corresponding auditing file for Identity Reporting. For more information, see "Enabling Auditing after the Installation" on page 92.

4 Start the application server. For more information, see "Stopping, Starting, and Restarting Tomcat" on page 33.

6.10 Integrating Single Sign-on Access with Identity Manager

If you have installed Identity Manager, your users can log in a single time to access the Identity Manager applications, Identity Reporting, and Identity Governance. NetIQ uses the OSP service for OAuth authentication, which provides users single sign-on access from the Identity Manager Home page. To ensure single sign-on access, you must configure both Identity Manager and Identity Governance. Users can easily shift between the two applications without needing to enter their credentials a second time.

Identity Governance must use the same authentication server that the identity applications use.

6.10.1 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/).
❑	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 6.5, "Ensuring Rapid Response to Authentication Requests," on page 91.

	Checklist Items
❑	3. Ensure that users can link to Identity Manager Home from Identity Governance. For more information, see Section 6.10.2.1, “Adding a Link to Identity Manager Home in the Identity Governance Menu,” on page 105.
❑	4. Ensure that Identity Governance connects to the authentication server for Identity Manager. For more information, see Section 6.10.2.2, “Using the Same Authentication Server as Identity Manager,” on page 106.
❑	5. Update Identity Manager Home to connect to Identity Governance. For more information, see Section 6.10.3, “Configuring Identity Manager for Integration,” on page 106.
❑	6. (Optional) Integrate Identity Governance with the workflows used in Identity Manager. For more information, see “Using Workflows to Fulfill the Changeset” and “Configuring Fulfillment” in *NetIQ Identity Governance Administrator Guide*.

For more information about Identity Manager, see the *NetIQ Identity Manager Overview and Planning Guide*.

6.10.2 Configuring Identity Governance for Integration

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

- Section 6.10.2.1, “Adding a Link to Identity Manager Home in the Identity Governance Menu,” on page 105
- Section 6.10.2.2, “Using the Same Authentication Server as Identity Manager,” on page 106

6.10.2.1 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 **Administration > General Settings**.
3. For **Home Page URL**, specify the URL for Identity Manager Home.
4. Select **Save**.
5. Sign out of Identity Governance.
6. (Optional) To verify the integration, complete the following steps:
   - **6a** Log in to Identity Governance. Verify that Identity Governance lists **Home** in the navigation pane.
   - **6b** Select **Home**, and verify that it takes you to the Identity Manager Home page.

6.10.2.2 Using the Same Authentication Server as Identity Manager

This section describes how to configure Identity Governance to use the same authentication server as Identity Manager identity applications for verifying users who log in. This section assumes that, when you installed Identity Governance, you did not specify the Identity Manager authentication server. For example, you might have installed Identity Governance before adding Identity Manager to your environment.

1. Stop Identity Governance and Tomcat. For examples, see "Stopping, Starting, and Restarting Tomcat" on page 33.
2. In the Identity Governance Configuration Utility, select **Authentication Server Details**.
3. Clear **Same as IG Server**.
4. Specify the protocol, DNS host name or IP address, and port that represent the authentication server for Identity Manager identity applications.

   NOTE: To use TLS/SSL protocol for secure communications, select **https**.
5. Select **Save**.
6. Make a note of the settings for the authentication server.

   The values for these settings must match the settings that you specify for Identity Governance in the RBPM Configuration utility. For more information, see Section 6.10.3, "Configuring Identity Manager for Integration," on page 106.
7. Select **Security Settings**, and make a note of the settings in the **General Service** section.

   The values for these settings must match the settings that you specify for Identity Governance in the RBPM Configuration utility. For more information, see Section 6.10.3, "Configuring Identity Manager for Integration," on page 106.
8. Close the utility.
9. Start Identity Governance and Tomcat. For examples, see "Stopping, Starting, and Restarting Tomcat" on page 33.

6.10.3 Configuring Identity Manager for Integration

To ensure proper integration, you must update your version of Identity Manager identity applications to recognize Identity Governance. The process includes copying files from the Identity Governance installation to the Identity Manager identity applications installation.

NOTE: Ensure that you have configured single sign-on for the Identity Manager identity applications. For more information, see

- **Linux:** "Configuring Single Sign-on Access in Identity Manager" in the *NetIQ Identity Manager Setup Guide for Linux*.
- **Windows:** "Configuring Single Sign-on Access in Identity Manager" in the *NetIQ Identity Manager Setup Guide for Windows*.

1. On the server where you installed Identity Governance, log in as an administrator.
2. Navigate to the `/osp` folder in the installation directory for Identity Governance. For example:
   - **Linux:** Default location of `/opt/netiq/idm/apps/configupdate`
   - **Windows:** Default location of `C:\netiq\idm\apps\configupdate`

3 Copy the `uaconfig-ig-defs.xml` file to a location or thumb drive that you can access from the server running Identity Manager identity applications.

4 Sign out of the server.

5 On the server where you installed the identity applications, log in as an administrator.

6 Stop the application server. For examples, see "Stopping, Starting, and Restarting Tomcat" on page 33.

7 Navigate to the `conf` directory of the application server.

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

8 Place the `uaconfig-ig-defs.xml` file from the Identity Governance installation in the `/conf` directory.

9 In a text editor, open the `configupdate.sh` or `configupdate.bat` file.

- **Linux:** Default location of `/opt/netiq/idm/apps/UserApplication/configupdate.sh`
- **Windows:** Default location of `c:\netiq\idm\apps\UserApplication\configudate.bat`

10 In the file, add the following line before the `-Duser.language` entry:

```
-Dcom.netiq.uaconfig.impl.custom.clients=path_to_conf_dir/uaconfig-ig-defs.xml
```

For example:

```
-Dcom.netiq.uaconfig.impl.custom.clients=/opt/netiq/idm/apps/tomcat/server/
IDMProv/conf/uaconfig-ig-defs.xml
```

11 Save and close the file.

12 Launch the configuration update utility by running from the command prompt.

- **Linux:** Enter:

  ```
  ./configupdate.sh
  ```

- **Windows:** From a command line enter:

  ```
  configupdate.bat
  ```

13 In the utility, select **Identity Governance SSO Client**.

NOTE: If the utility does not display the **Identity Governance SSO Client** tab, ensure that you copied the correct files from the Identity Governance installation to the identity applications installation.

---

14 Specify the values based on the **OAuth SSO Client** and **Security Settings > General Service** settings that you observed in Step 6 through Step 7 in Section 6.10.2.2, "Using the Same Authentication Server as Identity Manager," on page 106.

Observe the following considerations for these settings:

- By default, the **OAuth client ID** is `iac`. You specified the client ID and its password when you specified the client secret during the Identity Governance installation.
- **OAuth redirect URL** must be an absolute URL and include the specified value for OAuth client ID. For example, `http://myserver.host:8080/oauth.html`. By default, the configuration utility provides some of this URL. However, you must ensure that you add the server and port information.

15 Save your changes and close the utility.

16 In the directory of the application server, clear out the `/temp` and `/work` directories.

17 Start the application server. For examples, see “Stopping, Starting, and Restarting Tomcat” on page 33.

18 Add a link to Identity Governance on the Identity Manager Home page.

For more information, see “Configuring the Settings for the Identity Applications” in the *NetIQ Identity Manager Setup Guide for Linux*.

19 On the Identity Governance server, start Identity Governance (and Tomcat). For examples, see “Stopping, Starting, and Restarting Tomcat” on page 33.

6.10.4 Configuring a File Authentication Source for the Bootstrap Administrator

If you want to use a file as the authentication source for the bootstrap administrator instead of LDAP authentication, complete the following steps. You might need to modify the files Configuration Update utility files (`configupdate.sh.properties` or `configupdate.bat.properties` and `configupdate.sh` or `configupdate.bat`) similar to Step 9 through Step 12 in Section 6.10.3, “Configuring Identity Manager for Integration,” on page 106.

1 (Optional) Make a backup copy of both the Configuration Update utility and properties files for the identity applications.

- **Linux:** `/opt/netiq/idm/apps/UserApplication` and the files are `configupdate.sh.properties` and `configupdate.sh`.
- **Windows:** `c:\netiq\idm\apps\UserApplication` and the files are `configupdate.bat.properties` and `configupdate.bat`.

2 (Optional) Copy both the Configuration Update utility and the properties files to the `/conf` directory of the application server.

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

3 In a text editor, open the `configupdate.sh` or `configupdate.bat` file.

4 In the file, add the following line before the `-Duser.language` entry in the `JAVA_OPTS` shell variable.

For example:

- **Linux:** Using the default installation path:

```
-Dcom.netiq.uaconfig.impl.custom.clients=/opt/netiq/idm/apps/tomcat/
server/IDMProv/conf/uaconfig-ig-defs.xml
```

- **Windows:** Using the default installation path:

```
-Dcom.netiq.uaconfig.impl.custom.clients=c:\netiq\idm\apps\tomcat\server\I
DMProv\conf\uaconfig-ig-defs.xml
```

5 Save and close the file.

6 In a text editor, open the `configupdate.sh.properties` or the `configupdate.bat.properties` file.

7 Set `INSTALL_JAVA_BASE` as the path to the Oracle Java instance that Tomcat uses.

For example:

- **Linux:** `INSTALL_JAVA_BASE="/root/jdk1.x.x_xx"`
- **Windows:** `INSTALL_JAVA_BASE="c:\Program_Files\jdk1.x.x.xx"`

8 Set `CONFIG_FILENAME` as `"ism-configuration.properties"`.

For example:

```
CONFIG_FILENAME="ism-configuration.properties"
```

9 Save and close the file.

10 Launch the Configuration Update utility.

- **Linux:** From the command line, enter `./configupdate.sh`
- **Windows:** From the command line, enter `configupdate.bat`

11 In the Configuration Update utility, select **Identity Governance SSO Client** and select **Show Advanced Options**.

12 Enter the file location in the **File Authentication Source** field and the file name in the **File Name** field. The default file name is `adminusers.txt`.

13 Save your changes and close the utility.

6.11 Starting and Initializing Identity Governance

To verify installation and to initialize the Identity Governance databases, you must start Tomcat. In a clustered environment, start the primary node first to ensure that the initial database load occurs before the other nodes start.

1 (Optional) Verify that the schemas (Oracle) or databases (MS SQL or PostgreSQL) exist in your database platform.

2 To initialize Identity Governance and its databases, start Tomcat. For examples, see "Stopping, Starting, and Restarting Tomcat" on page 33.

NOTE: In a clustered environment, start Tomcat only on the primary (or master) node.

---

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

```
tail -f path_to_Tomcat_folder/logs/catalina.yyyy-mm-dd.log
```

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

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

4 Open a web browser and navigate to one of the following URLs, depending on how you installed Identity Governance:

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

For example:

```
http://texasone:8080/
https://172.16.254.1:8443/
```

The browser should display the login page for Identity Governance.

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

5a Log in as an administrator to the server where you installed Identity Governance.

5b In a terminal, navigate to the following directory:

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

5c Enter the following command:

```
tail -n 1 *
```

5d Verify that all `.txt` log files in the directory end with the following text:

```
Exit code: 0
```

NOTE

- `Identity_Governance_InstallLog.log` contains the results of all the log files. It does not have an individual exit code.
- The `checksums-log.txt` file contains multiple command and multiple `Exit code: 0` for each command.
- If a log file ends with a nonzero exit code, an error occurred in that part of the installation process.

6 Use the bootstrap administrator account to log in to Identity Governance.

Until you collect and publish data from an identity source that contains login accounts for Identity Governance, you must use the bootstrap administrator account. For more information, see "Creating and Managing Data Sources" in *NetIQ Identity Governance Administrator Guide*.

7 (Conditional) If you can verify installation but cannot get Identity Governance to load in a web browser, complete the following steps:

7a Stop Identity Governance (and Tomcat). For examples, see "Stopping, Starting, and Restarting Tomcat" on page 33.

7b Navigate to the following directory:

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

7c In a text editor, open `setenv.sh` or `setenv.bat`.

This file defines global variables and export paths needed to host Identity Governance under Apache Tomcat.

7d Verify that the file lists the correct host name for the authentication server and paths to Tomcat.

7e Save and close the file.

7f Start Identity Governance (and Tomcat). For examples, see "Stopping, Starting, and Restarting Tomcat" on page 33.

8 (Conditional) In a clustered environment, start Tomcat on the secondary nodes.

9 (Conditional) To configure Identity Reporting, continue to "Setting Up Identity Reporting" on page 99.

10 (Conditional) To integrate Identity Governance with Identity Manager, continue to "Integrating Single Sign-on Access with Identity Manager" on page 104.

11 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 *NetIQ Identity Governance Administrator Guide*.

12 (Optional) Configure Identity Governance, such as customizing the email templates and displayed labels. For more information, see Chapter 7, "Configuring Identity Governance Settings," on page 113.

6.12 Updating the License Key

You must enter a valid license key to continue using Identity Governance past the 90-day trial period.

1. Log in as a Global Administrator.
2. Select your user name, and then select **About**.
3. Enter a license key in the appropriate field.
4. Select **Submit license**.
5. Close the window.

7 Configuring Identity Governance Settings

To configure Identity Governance, you use the Identity Governance Configuration Utility, which allows you to modify the settings for the product.

7.1 How to Change the Password for the Bootstrap Administrator

If you have the bootstrap administrator coming from the file system, use the following steps to change the password if you use OSP as the authentication service.

1. Stop Tomcat. For more information, see “Stopping, Starting, and Restarting Tomcat” on page 33.
2. Access the following directory in a terminal:
   - **Linux:** `/opt/netiq/idm/apps/idgov/lib`
   - **Windows:** `C:\netiq\idm\apps\idgov\lib`
3. With Java in your path enter:

   ```
   java -jar ig-pwtool.jar%new-password-value%
   ```

   For example:

   ```
   java -jar ig-pwtool.jar Netiq123
   ```
4. Copy the value that is returned.
5. Navigate to the following directory:
   - **Linux:** `/opt/netiq/idm/apps/idgov/osp`
   - **Windows:** `C:\netiq\idm\apps\idgov\osp`
6. Edit the `adminsuers.txt` file.
   - **6a** In a text editor, open the file `adminusers.txt`.
   - **6b** Replace the current value (which will be the second entry in the file) with the one you copied from Step 4.
   - **6c** Save and close the file.
7. Restart Tomcat. For more information, see “Stopping, Starting, and Restarting Tomcat” on page 33.

7.2 How to Change the Password for the Database Users

If you must change the password for the database users, use the following steps.

1. Stop Tomcat. For more information, see "Stopping, Starting, and Restarting Tomcat" on page 33.
2. Log in to the database server with the appropriate administrator tool and update the necessary users passwords. For example, `igops`
3. Access the following directory in a terminal:
   - **Linux:** `/opt/netiq/idm/apps/idgov/bin`
   - **Windows:** `C:\netiq\idm\apps\idgov\bin`
4. Enter the following command:
   - **Linux:** `./encode-password.sh` *`%password-set-above%`*
   - **Windows:** `encode-password.cmd` *`%password-set-above%`*

   For example:

   ```
   ./encode-password.sh Netiq123
   ```
5. Record the value that is returned.
6. Repeat Step 4 and Step 5 for each database user.
7. Navigate to the following directory:
   - **Linux:** `/opt/netiq/idm/apps/tomcat/conf`
   - **Windows:** `C:\netiq\idm\apps\tomcat\conf`
8. Edit the `server.xml` file.
   - **8a** Open the `server.xml` file in a text editor.
   - **8b** Find the user name that you updated above:

     For example: `username="igops"`
   - **8c** Find the `password=` entry fir that database connection, then replace the current value with the value you recorded in Step 5.
   - **8d** Repeat these steps for each database user.
   - **8e** Save and close the file.
9. Restart Tomcat. For more information, see "Stopping, Starting, and Restarting Tomcat" on page 33.

7.3 Localizing to the User's Preferred Language

Identity Governance automatically localizes the attributes and email text according to the user's preferred language:

- Chinese Simplified
- Chinese Traditional
- Danish
- Dutch
- English
- French

- German
- Italian
- Japanese
- Polish
- Portuguese
- Russian
- Spanish
- Swedish

Identity Governance cannot always reconcile the differences in language that occur when different users collect data and run reports on that collection. For example, a user in Spain runs a collection for a set of data. Then a user in Russia runs a report against that collection. The fields in the report appear in Russian since that is the report user's default language. However, the reported data is in Spanish because the collection occurred on a computer with Spanish as the default language.

You can customize the content in the provided languages. Alternatively, you can apply a new language to Identity Governance and OSP.

7.4 Customizing the User Interface

Identity Governance and OSP automatically display content in the user interface according to your preferred language. You can customize content such as attribute names and informational messages using a text editor.

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

- Section 7.4.1, "Customizing the Labels in the Identity Governance Interface," on page 115
- Section 7.4.2, "Customizing Strings in the JAR Properties Files," on page 116

For more information about translating the content to a new language instead of customizing it, see Section 7.5, "Translating Content for Identity Governance and One SSO Provider," on page 117.

7.4.1 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 **Administration > Localization Import and Export**.

   Identity Governance lists the `.properties` files by language.
3. For the language that you want to customize, select **Download**.

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

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

---

4 In a text editor, customize the displayed text for the attributes that you want to change.

For example, you want to change all instances of *user ID* to *account name*. When you search for *user ID*, you will find the following type of string:

```
com.netiq.iac.persistence.ops.AttributeDefinition.USER.userID=User ID from source
```

Change `User ID from Source` to `Account Name from Source`.

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

---

5 Save and close the file.

6 To submit the modified file, select **Upload** for the language that you customized.

7 Refresh the browser window to view the changes.

NOTE: Depending on the browser settings, you might need to sign out of Identity Governance, clear the cache in the browser, then log in again.

7.4.2 Customizing Strings in the JAR Properties Files

By editing the various `.properties` files in the Identity Governance and OSP `.jar` files, you can customize the content displayed in the Identity Governance Configuration Utility as well as most of the Identity Governance and OSP interface. For example, you might want to use different terminology in the Identity Governance Configuration utility.

The `.jar` files are located:

- **Linux:** Default directories:
  - **Identity Governance**: `/opt/netiq/idm/apps/idgov/localization`
  - **OSP**: `/opt/netiq/idm/apps/osp/osp-extras/l10n-resources`
- **Windows:** Defaul directories:
  - **Identity Governance**: `c:\netiq\idm\apps\idgov\localization`
  - **OSP**: `c:\netiq\idm\apps\osp\osp-extras\l10n-resources`

To customize strings for Identity Governance or OSP:

1 Log in to the server where you installed Identity Governance or OSP.

2 To modify the `.properties` files, complete the following steps:

2a Locate the `.jar` file that you want to update.

For example, the `iac-configutil-strings.jar` file contains all displayed text for the Identity Governance Configuration Utility.

2b Copy the `.jar` files that you want to update to a temporary directory.

2c In the temporary directory, extract the `.jar` that you want to edit.

WARNING: Do not change the file names or directory structure of the `.jar` files.

2d Browse the file directory to the `.properties` file that you want to edit.

For example, `iac-ConfigUIstringsRsrc_fr.properties`.

2e In a text editor, customize the displayed text for the content that you want to change.

WARNING: Do not modify any text in the code string before the = sign. For example, `ADMIN_PASSWORD=`. Identity Governance might not function appropriately if you change the code string incorrectly.

2f Save and close the editor.

3 Copy the customized `.properties` files to their appropriate locations in the original `.jar` files in the temporary directory.

For example, replace the `iac-ConfigUIstringsRsrc_fr.properties` file with the modified version of the file in the following location:

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

4 Copy the `.jar` file(s) with the customized content to the `lib` directory.

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

5 Stop Tomcat. For examples, see "Stopping, Starting, and Restarting Tomcat" on page 33.

6 Delete all files and folders in the following directories:

- **Linux:** Default location of the:
  - Tomcat temporary directory in `/opt/netiq/idm/apps/tomcat/temp`
  - Catalina directory `/opt/netiq/idm/apps/tomcat/work/Catalina`
- **Windows:**
  - Tomcat temporary directory in `c:\netiq\idm\apps\tomcat\temp`
  - Catalina directory `c:\netiq\idm\apps\tomcat\work\Catalina`

7 Delete all log files from the `logs` directory for Tomcat.

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

8 Start Tomcat. For examples, see "Stopping, Starting, and Restarting Tomcat" on page 33.

9 Before logging in to Identity Governance, clear the browser cache to ensure that the browser displays your changes.

7.5 Translating Content for Identity Governance and One SSO Provider

If the default languages for Identity Governance and OSP do not meet your organization's needs, you can translate the strings and user interface content to a different language. For example, you might want to interact with Identity Governance in Norwegian (language code=`nb`). To use a non-default language, you need to translate the `.properties` files of an existing language.

For more information about customizing the content for a current new language instead of adding a language, see Section 7.4, “Customizing the User Interface,” on page 115.

7.5.1 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 7.4.1, “Customizing the Labels in the Identity Governance Interface,” on page 115.

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.

7.5.2 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:** `./bin/configutil.sh -password db_password -console`
  - **GUI mode:** `./bin/configutil.sh -password db_password`
- **Windows:** Enter the following command:
  - **Console mode:** `configutil.bat -password db_password -console`
  - **GUI mode:** `configutil.bat -password db_password`

3 Select **Miscellaneous**.

4 For **Supported Locales**, add the locale code that represents the language(s) that you want to include. Use a pipe sign to separate entries.

   For example, enter `nb` for Norwegian 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.

7.5.3 Adding the Translated Labels to the Identity Governance Interface

1 Complete the steps in Section 7.5.2, “Ensuring that Identity Governance Recognizes the New Language,” on page 119.

2 Log in to Identity Governance as a Global Administrator.

3 Select **Administration > Localization Import and Export**.

   Identity Governance lists the `.properties` files by language.

4 For the language that you added to Identity Governance, select **Upload**.

   For example, if you added the locale code for Norwegian to the Identity Governance Configuration Utility, upload the `localizedLabels_nb.properties` file.

5 Refresh the browser window to view the changes.

NOTE: Depending on the browser settings, you might need to sign out of Identity Governance, clear the cache in the browser, then log in again.

7.5.4 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 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 7.5.2, “Ensuring that Identity Governance Recognizes the New Language,” on page 119 before starting this procedure.

1 Navigate to the temporary directory where you had copied the original `.jar` files in Step 2b on page 118.

2 Add the translated `.jar` files to the temporary directory.

3 For each translated `.jar` file, extract the translated `.properties` file(s).

4 Copy the translated `.properties` file(s) to their appropriate locations in the original `.jar` files in the temporary directory.

   - **Linux:** For example, place the `iac-ConfigUIstringsRsrc_nb.properties` file in the `/com/netiq/iac/config/util` directory of the `iac-configutil-strings.jar` file.
   - **Windows:** For example, place the `iac-ConfigUIstringsRsrc_nb.properties` file in the `c:\netiq\com\iac\config\util` directory of the `iac-configutil-strings.jar` file.

5 Delete the translated `.jar` file(s) from the temporary directory.

6 Copy the `.jar` file(s) with the added translations to the `lib` directory for Tomcat.
   - **Linux:** Default directory of `/opt/netiq/idm/apps/tomcat/lib`
   - **Windows:** Default directory of `c:\netiq\idm\apps\tomcat\lib`
7 Stop Tomcat. For examples, see "Stopping, Starting, and Restarting Tomcat" on page 33.
8 Delete all files and folders in the following Tomcat directories:
   - **Linux:** Default locations of
     - `/opt/netiq/idm/apps/tomcat/temp`
     - `/opt/netiq/idm/apps/tomcat/work/Catalina`
   - **Windows:** Default locations of:
     - `c:\netiq\idm\apps\tomcat\temp`
     - `c:\netiq\idm\apps\tomcat\work\Catalina`
9 Delete all log files from the Tomcat `logs` directory.
   - **Linux:** Default location of `/opt/netiq/idm/apps/tomcat/logs`
   - **Windows:** Default location of `c:\netiq\idm\apps\tomcat\logs`
10 Start Tomcat. For examples, see "Stopping, Starting, and Restarting Tomcat" on page 33.
11 Before logging in to Identity Governance, clear the browser cache to ensure that the browser displays your new language.

7.5.5 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.

7.6 Customizing the Identity Governance Style Sheet

You can modify the stylesheet (CSS file) that Identity Governance uses to display enterprise-specific branding. Identity Governance defaults to the NetIQ template.

1 Log in as the Tomcat server administrator to the Tomcat server that hosts Identity Governance.
2 In the home directory of the Tomcat server administrator, create a directory named `netiq_custom_css`. For example:

   `/home/`*`name_of_Tomcat_admin`*`/netiq_custom_css`
   - **Linux:** `/home/SmithJ/netiq_custom_css`
   - **Windows:** `C:\Windows\System32\config\systemprofile\netiq_custom_css`

NOTE: For Windows environments, you might need to create the directory in a different location. To determine the correct location, you can use the Process Monitor tool from Microsoft. For more information, see Process Monitor (https://technet.microsoft.com/en-us/sysinternals/processmonitor.aspx) in the Windows Sysinternals documentation.

---

3 (Optional) If you are using Process Monitor, include the following steps:

3a Create a filter including the following:

- Process name is `java.exe`
- Operation is `CreateFile`
- Result contains PATH NOT FOUND
- PATH contains `custom.css`

3b Log in to Identity Governance.

3c When the product loads in your browser, look back at Process Monitor to see the path for your Windows environment.

4 Create a file named `custom.css`.

5 Edit the `custom.css` file to include your branding and other custom style settings that you want Identity Governance to use.

6 (Conditional) To use custom images, add the images to the `netiq_custom_css` directory.

7 To preview your changes, log in to Identity Governance.

You might need to refresh the page in the browser. You do not need to restart the Tomcat server.

8 Upgrading Identity Governance

You can upgrade to Identity Governance 3.5 from Identity Governance 3.0.1 or later. As part of the upgrade process, you must also migrate data because some of the collector templates and database tables and views changed between the releases.

NOTE: If you are upgrading and changing database platforms, you cannot migrate your existing data to the new platform. For example, if you are running Identity Governance with PostgreSQL as your database and you plan to upgrade and use Microsoft SQL Server as your database, your existing data cannot move to the new database.

Upgrading to the latest Identity Governance version is a process you must follow. You must backup your current data, uninstall the current version of Identity Governance and Identity Reporting, if you installed it, upgrade the required hardware and software, and then reinstall the current version of Identity Governance. With the Identity Governance 3.0 and later releases, Identity Reporting is part of the installation process instead of running a separate installer.

8.1 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 1.9, “Hardware and Software Requirements,” on page 25.
- ❒ 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, you can run reports before you upgrade to capture these details and make them available to other users after the upgrade.
- ❒ Open fulfillment requests will be available after the upgrade.
- ❒ Ensure you have the DNS names to identify server hosts before beginning the upgrading 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.

  If you installed the current or previous version of Identity Governance using IP addresses, you must replace the IP addresses with the fully qualified DNS names for these hosts in several configuration files. You can do this either before or after the upgrading procedure. For more information, see Section 8.5, “Changing Host File IP Addresses to DNS Names,” on page 128.
- ❒ 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.

❒ Before you upgrade, make a note of the values for the following settings. The installation process fails to restore or adversely modifies these settings:

Location of settings	Affected Settings
Administration settings in Identity Governance	All settings in the following areas: ◆ General Settings ◆ Identity Manager System Connection Information
Reviews > Definitions in Identity Governance	◆ Escalation timeout ◆ Reminder notification
Workflow Setting > Notification System in the Configuration utility	◆ Mail Server ◆ From Address
Policy > Risk in Identity Governance	Customized risk settings

❒ (Conditional) If you customized attributes in the Identity Governance catalog, save those settings before you upgrade. For more information, see "Saving Customized Settings for Attributes in the Catalog" on page 124.

❒ (Conditional) To upgrade your Identity Governance Oracle database, you must grant the `CREATE PUBLIC SYNONYM` and `DROP PUBLIC SYNONYM` privileges to the `igops` schema.

8.2 Saving Customized Settings for Attributes in the Catalog

Identity Governance allows you to customize some of the attributes, such as `email` or `Account name`, in the Catalog. However, when you migrate collected data from a previous version of Identity Governance to this release, all customizations that you applied in the Catalog will be lost. For example, you changed the displayed name of the user attribute `Title` to `Job Title` and specified that it is an editable value. The migration process overrides this type of customization.

To maintain your custom settings, you must save those settings before upgrading to Identity Governance or migrating your collections for this release.

1 Before upgrading Identity Governance, run the following query against the `igops` database for the `USER` entity type:

PostgreSQL:

```
select attribute_key as attrKey,
attribute_type as attrType,
curatable as editable,
entity_type as entityType,
listable as displayable,
quick_info as quickInfo,
searchable as advanceSearch
from attribute_definition
where extended = false and (attribute_type = 'ARC_MANAGED' or attribute_type =
'COLLECTED') and entity_type = 'USER';
```

Oracle or Microsoft SQL Server:

```
select attribute_key as attrKey,
attribute_type as attrType,
curatable as editable,
entity_type as entityType,
listable as displayable,
quick_info as quickInfo,
searchable as advanceSearch
from attribute_definition
where extended = '0' and (attribute_type = 'ARC_MANAGED' or attribute_type =
'COLLECTED') and entity_type = 'USER';
```

2. Save the output from the query.
3. Run the same query for the other entity types in the Catalog. For each query, change the two instances of `entity_type = USER` to specify the type of attribute that you want to query: `GROUP`, `ACCOUNT`, or `PERMISSION`.
4. Save the output from each query that you run.
5. After migrating your collected data to the new release, manually reapply your customized settings to the affected attributes based on the query output.

8.3 Changes to Passwords Stored in Environment Variables

To allow the silent installation of Identity Governance to work, Identity Governance reads passwords stored in environment variables. For more information, see "Understanding the Passwords that Identity Governance Reads from Environment Variables During the Installation Process" on page 63.

In prior versions of Identity Governance, some of these environment variables had different names. Here is a list of the changes:

Current Name	Prior Name
`install_authserver_client_secret`	`NETIQ_RPT_OSP_PWD`
`install_db_admin_secret`	`NETIQ_DB_USER_PASSWORD`
`install_db_reporting_secret`	`NETIQ_DB_CFG_PWD`
`install_truststore_secret`	`NETIQ_SSL_KEYSTORE_PWD`
`install_smtp_password_auth_user`	`NETIQ_SMTP_PASSWORD`

8.4 Upgrading Procedure

Before starting the upgrade procedure, ensure that you review the considerations in "Planning to Upgrade Identity Governance" on page 123.

1. (Optional) Run reports for any review run details you want to make available after the upgrade.
2. Run the Identity Governance Configuration utility with the `-es` option to get a list of system settings for your current environment. Keep the list to compare to the list you generate after upgrading.
3. Complete or stop all scheduled items, running reports, and running reviews before starting the upgrade process.

4 Use the Data Purge utility to delete unwanted data before upgrading. For more information, see "Identifying Purgeable Data" in the *NetIQ Identity Governance Administrator Guide*.

5 Stop Identity Governance (and Tomcat). For more information, see "Stopping, Starting, and Restarting Tomcat" on page 33.

6 Back up and export (PostgreSQL only) your full Identity Governance data and confirm that you can restore it with no problems.

Include the following databases:

- `igops`
- `igdcs`
- `igwf`
- `igara`
- `reporting` (or your reporting database name)

For more information, see "Backup and Restore" in the *PostgreSQL Documentation*.

7 (Conditional) If you have an Oracle database, perform the following steps:

7a Backup the `igops` schema.

7b 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';
```

7c Run the following script, modified for your specific environment details, to drop extended statistics and so the 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 "Tips and Tricks Invisible Columns in Oracle Database 12c".

8 Move your generated reports (`pdf` and `csv`) from the Reporting home folder to a backup directory.

9 Stop PostgreSQL.

10 Uninstall Identity Governance and Identity Reporting. For more information, see Chapter 9, "Uninstalling Identity Governance," on page 131.

11 Uninstall OSP and clean up any remaining files and folders. The default installation directory is:

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

12 Uninstall Tomcat and clean up any remaining files and folder.

13 (Conditional) If using PostgreSQL, uninstall PostgreSQL. For more information, see PostgreSQL Installation Procedure in the PostgreSQL documentation. The uninstall information is at the end of the section.

14 Ensure that your servers meet the minimum hardware and software requirements for this version of Identity Governance. For more information, see Section 1.9, “Hardware and Software Requirements,” on page 25. Update any required components.

15 (Conditional) If you are running on Windows, reboot the Windows server.

16 (Conditional) Upgrade the database server if you are running Microsoft SQL Server or Oracle to the latest supported version by following the database platform instructions.

17 (Conditional) Install the most recent version of Postgres. For more information, see Chapter 2, “Installing Components Required for Identity Governance,” on page 31

18 (Conditional) If using PostgreSQL, add the following users and role:

- idm_rpt_cfg
- igara
- igarc
- igdcs
- igops
- igrptuser
- igwf
- ig_rpt_role

19 (Conditional) If you have exported the PostgreSQL data, import your data to the new database.

20 Install Tomcat and any other required or optional components for Identity Governance. For more information, see Chapter 2, “Installing Components Required for Identity Governance,” on page 31.

21 Install the current version of OSP. For more information, see Chapter 3, “Installing an Authentication Service,” on page 35.

22 Install the current version of Identity Governance and Identity Reporting. For more information, see Chapter 4, “Installing Identity Governance,” on page 43.

23 (Conditional) Add the virtual columns back into the Oracle database. For more information, see “Tips and Tricks Invisible Columns in Oracle Database 12c”.

24 Start Identity Governance (and Tomcat). For more information, see “Stopping, Starting, and Restarting Tomcat” on page 33.

25 (Optional) If you want to install the current version of Identity Reporting at a time other than when you install Identity Governance, see Chapter 5, “Installing Identity Reporting,” on page 67.

26 After the installation completes, copy the generated `pdf` and `csv` report files to the location specified during the installation.

27 (Conditional) Log in to Identity Governance to review any customized settings you have made to the UI. 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.

28 Review changes to existing collectors and adjust mappings as necessary.

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.

29 (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 "Migrating an Identity Collector to a Change Event Identity Collector" in the *NetIQ Identity Governance Administrator Guide*.

30 Publish the collected data again to populate the business roles and other items. For more information, see "Publishing the Collected Data" in the *NetIQ Identity Governance Administrator Guide*.

31 Activate schedules or create new schedules, if needed.

32 To restore your **Administration** settings, complete the following steps:

32a Log in to Identity Governance as a Global Administrator.

32b Select **Administration**.

32c Restore your values in the following **Administration** sections, as needed:

- **Risk Level Configuration**
- **General Settings**
- **Identity Manager System Connection Information**

32d Save your changes.

33 Restore your values for **Escalation timeout** and **Reminder notification** in your review definitions.

34 Run the Configuration utility to restore your values for **Workflow Settings > Notification System**. For more information, see "Running the Identity Governance Configuration Utility" on page 133.

35 Run the Configuration utility with the `-es` option 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.

8.5 Changing Host File IP Addresses to DNS Names

Beginning with Identity Governance 3.5.0, the product installation requires you to identify host servers using only fully-qualified DNS names. In previous releases, you could specify either the IP address or the DNS name to identify host servers.

If you used IP addresses when you installed a previous version of the product, ensure you use fully-qualified DNS names when you install the latest version. If you are able to successfully install the product using IP addresses, users might get an OAuth2 error when logging in to the product. If this happens, you must modify settings in three places after you upgrade to use the latest version of Identity Governance.

To update DNS names in setenv:

1 Stop Tomcat.

2 Open the `setenv` file in a text editor. In Linux environments, the file location is `/opt/netiq/idm/apps/tomcat/bin/setenv.sh`. In Windows environments, the file location is `C:\netiq\idm\apps\tomcat\bin\setenv.bat`.

3 Change the IP address associated with `com.netiq.idm.osp.client.host` to the fully-qualified DNS name.

4 Save and close the file.

To update DNS names in ism-configuration.properties:

1. Open the `ism-configuration.properties` file in a text editor. In Linux environments, this file is located in the `/opt/netiq/idm/apps/tomcat/conf` directory. In Windows environments, this file is located in the `C:\netiq\idm\apps\tomcat\conf` folder.
2. Change the IP address associated with the following attributes to the 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.redirect.url`
3. Save and close the file.

To update DNS names in the Identity Governance Configuration utility:

1. Ensure that the Identity Governance database is running.
2. Start the Identity Governance Configuration utility with the database password. In Linux environments, run `/opt/netiq/idm/apps/idgov/bin/configutil.sh`. In Windows environments, run `C:\netiq\idm\apps\idgov\bin\configutil.bat`.

   For example, use the following command in Linux environments:

   ```
   ./configutil.sh -password %PASSWORD%
   ```
3. Change the IP address associated with the following attributes on the specified tabs to the 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

4. Exit the utility.
5. Start Tomcat.

8.6 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.

9 Uninstalling Identity Governance

There are times where you are required to uninstall Identity Governance. You would uninstall Identity Governance in a lab environment or during an upgrade procedure. For more information about upgrading, see Chapter 8, “Upgrading Identity Governance,” on page 123.

Identity Governance does come with an uninstall utility that you use to uninstall the product, however, you must ensure that all of the files are removed from the server before reinstalling the same version of Identity Governance or a new version of Identity Governance.

To uninstall Identity Governance:

1. Define the Java path to the `jre bin` directory as an environment variable.
2. Stop Tomcat. For more information, see “Stopping, Starting, and Restarting Tomcat” on page 33.
3. (Conditional) If you are running any version of Identity Governance prior to 3.0, you must uninstall Identity Reporting separately from Identity Governance.
   - **3a** Access and run the uninstall utility for Identity Reporting.
   - **3b** If you are running Linux, access the uninstall directory located here: `/opt/netiq/idm/apps/IdentityReporting/Uninstall_IdentityReporting`.

     To execute the script, enter:

     ```
     ./LaunchUninstall.sh
     ```
   - **3c** If you are running Windows, access the **Control Panel**, then search for Identity Reporting and click **Uninstall**.
4. Access and run the uninstall utility for Identity Governance.
   - **4a** If you are running Linux, access the uninstall directory located here: `/opt/netiq/idm/apps/idgov/Uninstall_IdentityGovernance` or `/opt/netiq/idm/apps/idrpt/Uninstall_IdentityGovernance` if you installed Identity Reporting separately.

     To execute the script, enter:

     ```
     ./LaunchUninstall.sh
     ```

     or
   - **4b** If you are running Windows, access the **Control Panel**, search for and select Identity Governance, and then select **Uninstall**.
5. When the uninstall completes, delete the following files and folders:
   - **Linux:** The default installation path is `/opt/netiq/idm/apps`.
     - `/opt/netiq/idm/apps/idrpt`
     - `/opt/netiq/idm/apps/idgov`
     - `/opt/netiq/idm/apps/tomcat/webapps/api`
     - `/opt/netiq/idm/apps/tomcat/webapps/cx`
     - `/opt/netiq/idm/apps/tomcat/webapps/daas`
     - `/opt/netiq/idm/apps/tomcat/webapps/doc`
     - `/opt/netiq/idm/apps/tomcat/webapps/dtp`
     - `/opt/netiq/idm/apps/tomcat/webapps/IDMRPT`

- `/opt/netiq/idm/apps/tomcat/webapps/IDMRPT-CORE`
- `/opt/netiq/idm/apps/tomcat/webapps/ROOT`
- `/opt/netiq/idm/apps/tomcat/webapps/rptdoc`
- `/opt/netiq/idm/apps/tomcat/webapps/workflow-api`
- `/opt/netiq/idm/apps/tomcat/work/Catalina/localhost`
- `/opt/netiq/idm/apps/tomcat/temp`

- **Windows:** The default installation path is `C:\netiq\idm\apps`.
  - `C:\netiq\idm\apps\idrpt`
  - `C:\netiq\idm\apps\idgov`
  - `C:\netiq\idm\apps\tomcat\webapps\api`
  - `C:\netiq\idm\apps\tomcat\webapps\cx`
  - `C:\netiq\idm\apps\tomcat\webapps\daas`
  - `C:\netiq\idm\apps\tomcat\webapps\doc`
  - `C:\netiq\idm\apps\tomcat\webapps\dtp`
  - `C:\netiq\idm\apps\tomcat\webapps\IDMRPT`
  - `C:\netiq\idm\apps\tomcat\webapps\IDMRPT-CORE`
  - `C:\netiq\idm\apps\tomcat\webapps\ROOT`
  - `C:\netiq\idm\apps\tomcat\webapps\rptdoc`
  - `C:\netiq\idm\apps\tomcat\webapps\workflow-api`
  - `C:\netiq\idm\apps\tomcat\work\Catalina\localhost`
  - `C:\netiq\idm\apps\tomcat\temp\`

6 Restart Tomcat, if needed. For more information, see “Stopping, Starting, and Restarting Tomcat” on page 33.

A Running the Identity Governance Configuration Utility

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

You can run this utility in GUI or console mode from the Identity Governance installation location. To script changes to the configuration of Identity Governance, use the console mode option.

In the command line, navigate to the installation directory for Identity Governance.

- **Linux:** Default location of `/opt/netiq/idm/apps/idgov`, then enter one of the following commands:
  - **Console mode:** `./bin/configutil.sh -password db_password -console`
  - **GUI mode:** `./bin/configutil.sh -password db_password`
- **Windows:** Default location of `c:\netiq\idm\apps\idgov`, then enter one of the following from a command prompt:
  - **Console mode:** `cmd /c "configutil.bat -password db_password -console"`
  - **GUI mode:** `cmd /c "configutil.bat -password db_password"`

The utility provides settings under the following tabs:

A.1 Identity Governance Server Details

This tab allows you to display your organization’s branding instead of the default branding displayed when your users run Identity Governance.

NOTE: In early versions of Identity Governance (formerly named Access Review), this tab included values for the login page, such as protocol, host name, and port. Starting with Access Review 1.5, those values are on the **Authentication Server Details** tab.

A.2 Authentication Server Details

This tab defines the values for the LDAP authentication server, OSP authentication service, and bootstrap administrator. This tab provides the following groups of settings:

A.2.1 OAuth Server

This section represents the values for the LDAP authentication server.

Same as IG Server

Specifies whether the authentication server runs on the same computer as Identity Governance.

Protocol

Applies only when the authentication server and the Identity Governance server run on different computers.

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

Host Name

Applies only when the authentication server and the Identity Governance server run on different computers.

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

Port

Applies only when the authentication server and the Identity Governance server run on different computers.

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

A.2.2 OAuth SSO Client

This section represents the values for OAuth authentication services to Identity Governance.

IG Client ID

Specifies the client ID of Identity Governance with which it is registered to the authentication service.

IG Client Secret

Specifies the client password of Identity Governance with the authentication service.

IG Redirect URL

Specifies the URL used by the authentication service to redirect to the Identity Governance login page if authentication token is valid.

IG Request Client ID

Specifies the client ID of Identity Governance Access Request with which it is registered to the authentication service.

IG Request Client Secret

Specifies the client password of Identity Governance Access Request with the authentication service.

IG Request Redirect URL

Specifies the URL used by the authentication service to redirect to the Identity Governance Access Request page if authentication token is valid.

A.2.3 Bootstrap Admin

This section represents the values for the bootstrap administrator.

Bootstrap Admin

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

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

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

Authentication Source

Specifies whether the credentials for the bootstrap admin reside in an Identity Vault (LDAP authentication server) or a text file.

(Conditional) If you specify **File**, you must also specify values for **Directory** and **Filename** that correspond to the file that stores your bootstrap admin information.

- **Linux:** Default location of `/opt/netiq/idm/apps/idgov/osp/adminusers.txt`
- **Windows:** Default location of `c:\netiq\idm\apps\idgov\osp/adminusers.txt`

A.3 Security Settings

This tab defines the values for authentication matching and Identity Governance services.

Auth Matching Rules

Specifies how Identity Governance authenticates login requests and grants the appropriate permissions to users. Enter one or more rules that Identity Governance uses to compare attributes in the SUSER table, such as `dn`, with attributes retrieved from 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 "Adding or Editing Attributes to Extend the Schema" in *NetIQ Identity Governance Administrator 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.

IG Client ID

Specifies the name that you want to use to identify Identity Governance to each service listed.

IG Client Secret

Specifies the password for the corresponding client ID.

Enable test client for utilities

Specifies that you want to use test IDs to run utilities that interact with Identity Governance without creating client IDs for each utility.

A.4 Network Topology Settings

This tab defines network connection settings that Identity Governance uses to connect to the single Tomcat instance or to the load balancer if you are running Identity Governance in a cluster. If you select **https** for the protocol, the **Keystore File** and **Keystore Password** fields become active.

This tab also defines runtime instance settings.

A.5 Miscellaneous Settings

This tab defines additional settings for your configuration. Some fields are self explanatory and some should not be changed. This tab provides the following groups of settings:

A.5.1 Miscellaneous

Do not change the settings in this section except for the **Default Locale**, if needed.

A.5.2 Collection and Publication Batch Sizes

These settings allow an administrator to tune the size of the record chunks that Identity Governance uses for the data collection and publication operations to achieve optimal performance in each environment.

A.5.3 Collection and Publication Settings

Do not clear **Clean DAAS Configuration post collection**. The **Max supported Depth of permission relations** field prevents loops of relationship mappings in deeply nested permissions environments. The default setting should be best for most environments.

A.5.4 Identity Manager Integration

If you also have Identity Manager installed, these settings help you integrate Identity Governance with Identity Manager.

Enable integration using Identity Manager Driver for Identity Governance

Requires the Identity Manager Driver for Identity Governance (Identity Governance Driver)

Specifies whether you want to integrate the permissions and permission assignment tasks in the Identity Governance catalog with the role and resource catalog in Identity Manager.

For more information, see "Understanding Synchronization and Reflection" in the *NetIQ Identity Governance Administrator Guide*.

Exclude Identity Manager permissions from review when they provision any native permissions in the same review

Specifies whether you want to review Identity Manager permissions that duplicate native permissions along with the native permissions in a review.

A.5.5 Data Production Timeouts

These settings allow an administrator to tune the timeout values for various data production operations to achieve optimal performance in each environment. The timeout values are expressed in milliseconds. The default values should suffice for the majority of installations.

Heartbeat interval (com.netiq.iac.dataProduction.heartbeat.interval)

The interval between heartbeat updates for data production jobs. The default is 2 minutes (120000 ms).

Job idle cutoff timeout (com.netiq.iac.dataProduction.cutoff.timeout)

The amount of time, after the last heartbeat update, that a running job is deemed to be in an idle state where the data production processing has halted. The default is 6 hours (21600000 ms).

Orphaned job idle add-on timeout (com.netiq.iac.dataProduction.orphan.addon.timeout)

The additional amount of time, combined with the **Job idle cutoff timeout**, that will pass before a runtime instance can detect and clean up data production jobs with a different runtime identifier that have an idle state. The default is 1 hour (3600000 ms), which combined with the default cutoff timeout sets up an overall 7 hour default.

A.6 Bulk Data Update Settings

This tab defines settings that you use to submit multiple attribute updates to objects in the catalog by using a CSV file. For more information about performing bulk data updates, see "Editing Attribute Values in Bulk" in *NetIQ Identity Governance Administrator Guide*.

Base Folder

Create a folder on your Identity Governance server for update files. Specify that full path name of that folder in this field. You must also create sub-folders named `input` and `output`. The Identity Governance service must have read/write access permission on both of these folders. Identity Governance creates the CSV data template files in the output folder, and you submit edits by copying the updated template in the input folder.

Batch Size

(Optional) Specifies the maximum number of CSV data rows processed at one time. This option is useful for tuning the memory usage of the Bulk Update process. The default value is 1000.

When you place the `csv` file in the `input` directory, Identity Governance changes the extension name of the file as it process the file. Here are the different extensions and process the file goes through during the bulk process:

File Extension Name	Process
`.csv`	Identity Governance start the bulk process. It is the name on the file when you add it into the `input` directory.
`.ph1`	Phase 1 of the bulk process.
`.fail`	If the bulk process fails, the file name becomes `.fail`.
`.done`	If the bulk process completed, the name becomes `.done`.

A.7 Workflow Settings

This tab defines settings that you use to automate external provisioning and notifications. This tab provides the following groups of settings:

- Section A.7.1, “External Provisioning System,” on page 138
- Section A.7.2, “Notification System,” on page 139
- Section A.7.3, “Message Queue,” on page 139

A.7.1 External Provisioning System

To use an external provisioning system, specify the **URL**, **User ID**, and **Password** that Identity Governance needs to connect to the system. For example:

URL

```
http://$test:8180/IDMProv
```

User ID

```
globaladmin
```

Password

```
adminpassword
```

For more information, see “Using Workflows to Fulfill the Changeset” in *NetIQ Identity Governance Administrator Guide*.

A.7.2 Notification System

This section represents the values that Identity Governance uses to send email notifications.

Mail Server

Specifies the IP address or DNS name and port for the mail server. For example, `12.345.675.90:25`.

From Address

Specifies the email address that you want Identity Governance to use as the origination for email notifications.

NOTE: If you are using a Gmail SMTP server for your mail server, Gmail ignores this value and uses the actual Gmail address as the origination for email notifications.

Enable SMTP TLS

Specifies to use secure email delivery.

User ID

Specifies the email address that you want to use for authenticating Identity Governance to the mail server.

Password

Specifies the password associated with the specified **User ID**.

Enable persistent notification message queue

Specifies whether you want to use message queuing functionality.

A.7.3 Message Queue

This section represents the values for the message queue for email notifications. The queue can use TLS/SSL protocol for secure communication.

JMS broker URI

Specifies the Uniform Resource Identifier (URI) for the Java Message Service (JMS) that the mail server uses. For example, `tcp://12.345.675.90:61616`.

(Conditional) In a clustered environment, add `failover:` to the prefix, then specify the host name or IP address and port for each ActiveMQ server. Use commas to separate the server values. For example, `failover:tcp://amq1.mycompany.com:61616,tcp://amq2.mycompany.com:61616`.

SSL

Specifies whether you want to use TLS/SSL protocol for secure communication when sending notifications.

Queue Keystore

Applies when you want to use the SSL protocol.

Specifies the path and filename of the keystore file that contains the authentication server trust certificate for the mail server.

Queue Keystore Password

Applies when you want to use the SSL protocol.

Specifies the password used to load the keystore file.

Queue Trust Store

Applies when you want to use the SSL protocol.

Specifies the path to the Trusted Key Store that contains all trusted signers' certificates.

Queue Trust Store Password

Applies when you want to use the SSL protocol.

Specifies the password for the Trusted Key Store.

B Ports Used in Identity Governance

Identity Governance uses the following ports by default:

Transport Protocol	TCP Port	Secure Channel
HTTPS	8443 (all greens)	TLS
LDAP(S)	636 (OSP)	TLS
JDBC	1433 (Microsoft SQL Server) 1521 (Oracle) 5432 (PostgreSLQ)	TLS
SMTP	25, 465, 587	TLS
Audit	6514 (default)	TLS
AMQP	61616 (IG)	TLS

If in your environment, you have polices that require different ports, ensure to change the ports during the installation to match your environment.