Data Center Discovery 2021.2

Scan Engine Installation Guide

Rev 06/20

Contents

Overview

Use this document as a guide through the installation process of the Ivanti Data Center Discovery scan engine. You'll need to access the files from the table below to ensure a smooth installation.

File	Description
Scan Engine Prerequisites Guide	This document outlines system requirements for installation.
Data Center Discovery installer	This installer includes the scan engine software.
Activation code	You'll need this code to enable full functionality of the scan engine software on your site.

> **Note:** You should have received or downloaded these files in advance of the installation. If you have any difficulties with the installation, please contact Ivanti support.

Pre-installation

It's highly recommended that you dedicate a Windows server to the Data Center Discovery scan engine for the scanning process. This will ensure optimal performance for the scanning server.

The hardware and software requirements of the scan engine are supplied in the *Data Center Discovery—Scan Engine Prerequisites Guide,* where you can review information on Windows Server Internet Information Service (IIS) configuration, SQL Server configuration, and much more.

If you want to use Secured Sockets Layer (SSL), it's recommended that you have a certificate and https binding configured for the default website **before** installation.

Prerequisite testing

During the installation, as well as upgrades, prerequisites are tested.

If a prerequisite check fails, then the installation cannot proceed. To proceed, you must make the required components available. Details of the prerequisites that pass or fail are seen in the prerequisites check during the installation.

During an upgrade, the same checks are performed. Should any of these checks fail, then a prerequisite check will appear detailing the failures, and the upgrade will not be able to proceed.

Retrieving the installation software

You'll receive an email (or similar delivery method) from Ivanti that provides a download link for the Data Center Discovery scan engine installer. Once you have that information, download the **.msi** zip file to any directory on your server, then extract the contents to your chosen temporary directory.

Installation

The Data Center Discovery scan engine is composed of three components:

- Scanning service
- Configuration user interface
- REST API

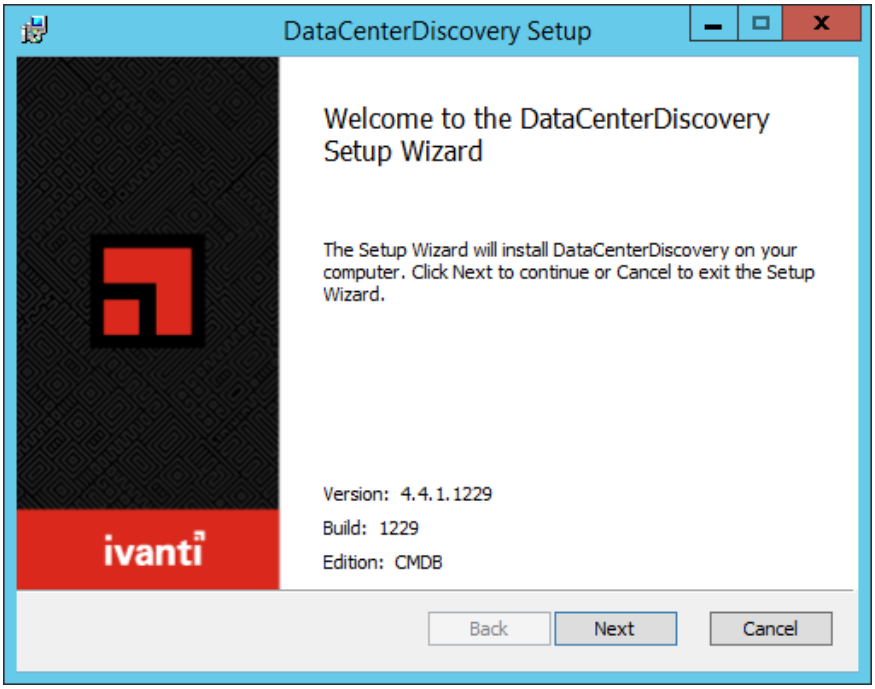
These components can be installed onto separate devices, although this is not a requirement.

The following installation process assumes that the scan engine, user interface, and API are installed on the *same* device. The device is used to execute the scan engine service (and potentially host the SQL Server that stores the scan database) and host the scan-engine configuration IIS installation and REST API.

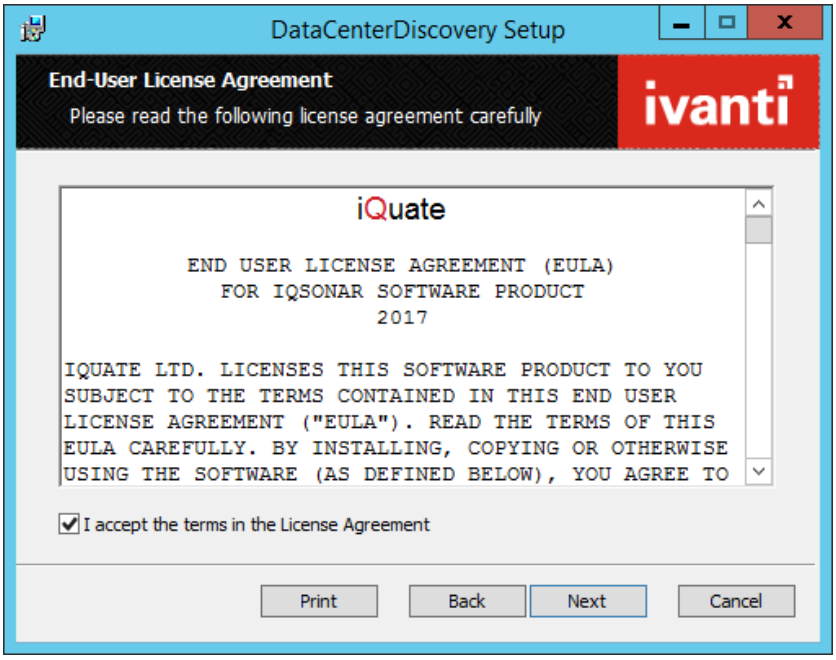
- Prerequisites approximate installation time: 2 hours
- Approximate installation time: 5 minutes

To install the scanning service

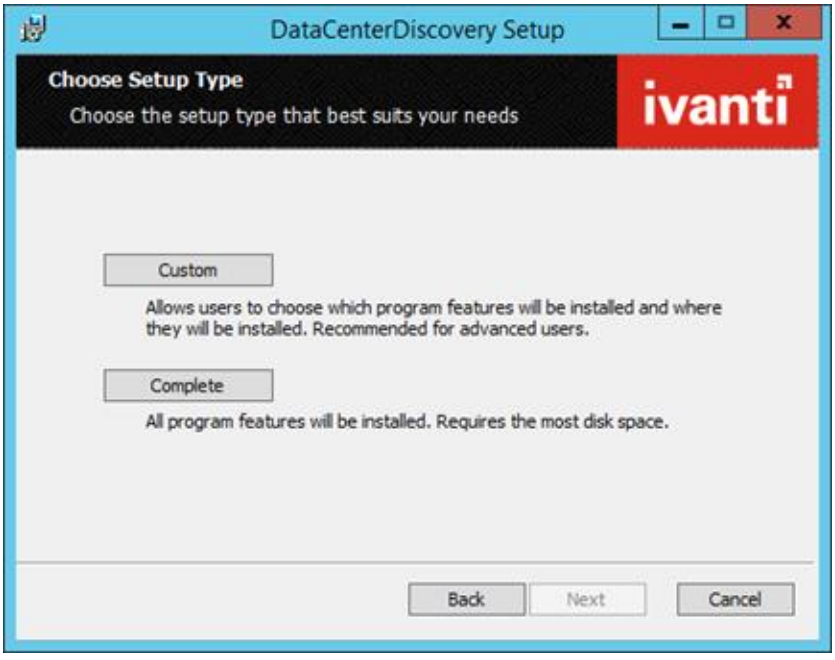
Right-click the Data Center Discovery scan engine installer and click **Install**. You may receive a pop-up asking for permission to continue; if this happens, enter your appropriate administrator login details. Click **Next**.



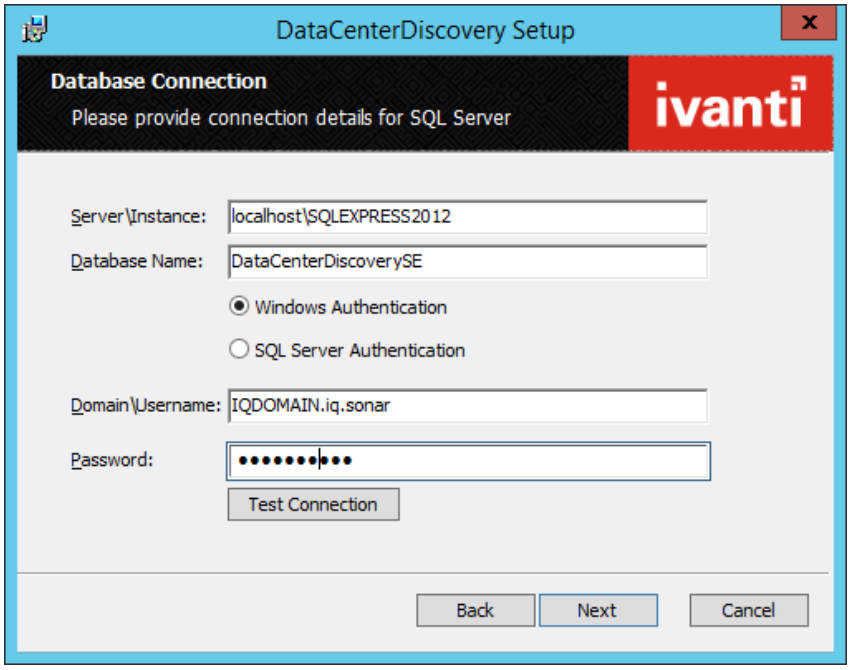
Read and accept the End-User License Agreement. Click **Next**.



You can customize the installation to suit your needs. The **Complete** option installs the scanning service, UI, and API on a single device (POC and basic-estate scenario). More complex setups will separate the other components from the scan engine. This document explains how to install the scanning service, UI, and API on a single device. Click the **Complete** button to start the install.



Option 1: Provide the name of a local database to be used by the scan engine.

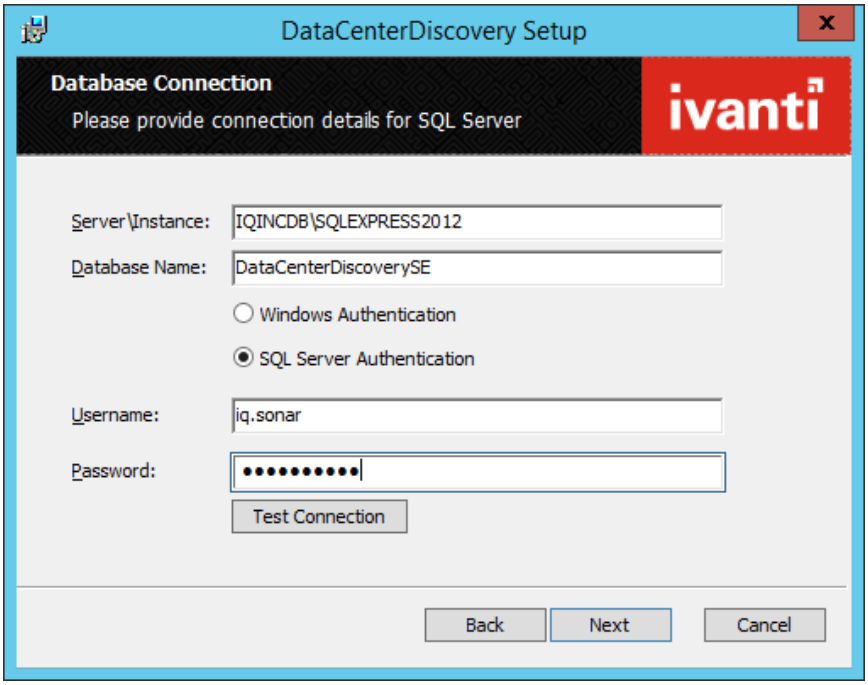


This example uses:

- A database server on the same device as the scan engine. If this is the first installation, the specified database will be created. Subsequent installations will reuse the existing database.
- Windows Authentication to connect to the database server.
- The current identity (username) of the logged-in user to create and populate the scan database. The user must have appropriate database permissions.

> **Note:** You must use a domain account. If the logged-in user is a local machine account (e.g., ".\user.name"), you'll be unable to use Windows Authentication.

Option 2: Select a remote database to be created and used by the scan engine.



This example uses:

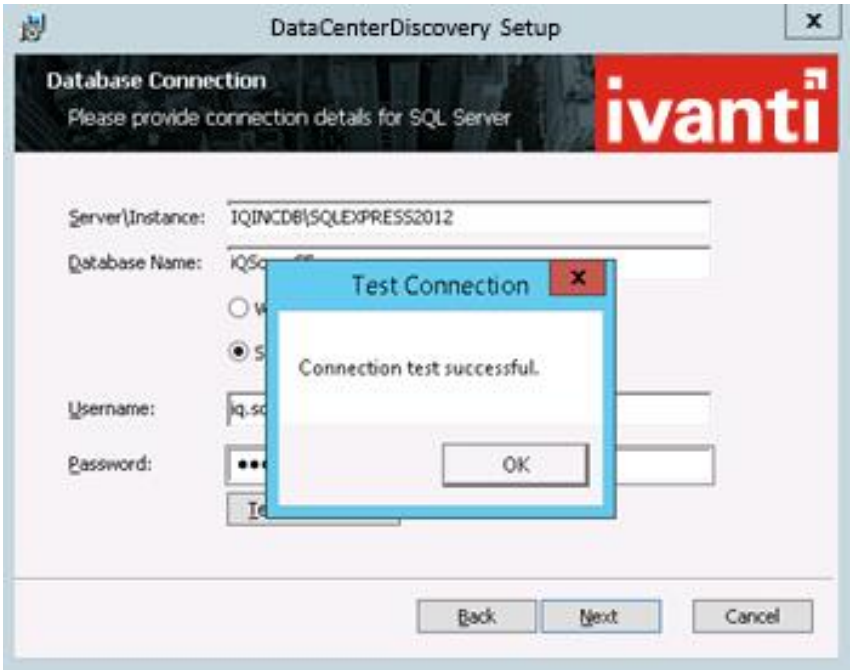
- A database on a different device from the scan engine. If this is the first installation, the specified database will be created. Subsequent installations will reuse the existing database.
- A database-specific user to create and populate the scan database. The user must have appropriate database permissions.

Additional information on database setup

The scan database stores scan configuration information provided by the UI, as well as data from the scanned devices and/or applications identified during the scan operation.

✓	Description
	Server\instance: Define the server/instance on which the new database is installed. If the server is located on the device, then the server value can be omitted or replaced with **localhost**; otherwise, provide the server name of the device hosting the SQL Server instance.
	Database name: Define the database name to be created.
	Authentication type: Select Windows or SQL Server authentication. • **Windows Authentication** uses a domain-defined username that's provided with access to the database. This will be the username of the logged-in user. A local machine account can't be used. • **SQL Server authentication** uses a SQL-Server-defined local user
	Username: Enter the username to access the database. This name identifies who accesses the database server to create the required database and save scanned information.
	Password: Specify the password to access the database.
	Test Connection (button): Test the login details for the database.

Test the connection. Click **OK** to close the test window. Click **Next**.



If the connection fails, you'll need to correct the details or ensure that the connection is available. You can't continue the installation without a valid connection.

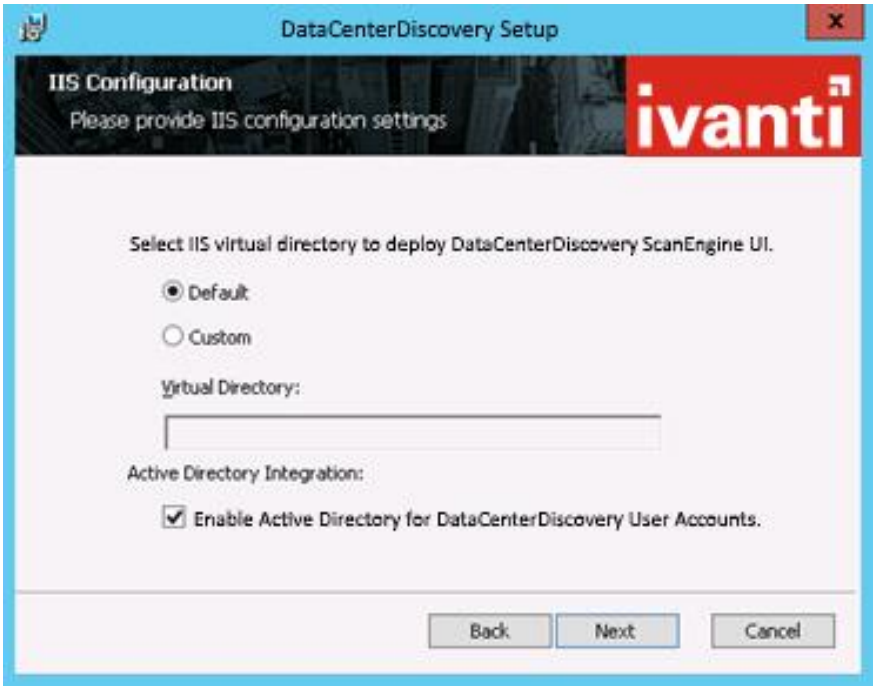
Confirm that the prerequisites for the install have passed; if necessary, correct any failed test. Click **View Details** to see the criteria that were checked, or if a failure has occurred. Click **Next**.

Select the **Create a new key** option. Click **Next**.

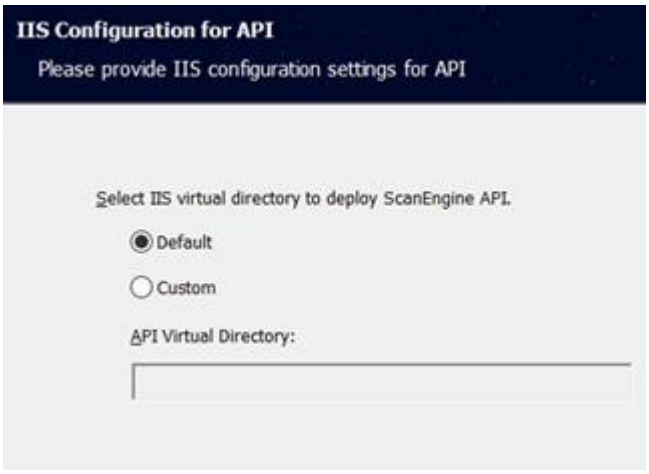
This encryption key is a customer-specific key that controls access to credentials used within the scanning server. The generated key will be displayed at the end of the install process. **It's important that you retain this key for future use.** The *Data Center Discovery—Scan Engine Security Guide* provides additional information about this feature.

Next, you need to define the connection details for the web interface components.

Select your scan-engine UI virtual directory. This will modify the URL used to access the user interface. Enable an Active Directory account login if an AD user login is required for the UI. Click **Next**.



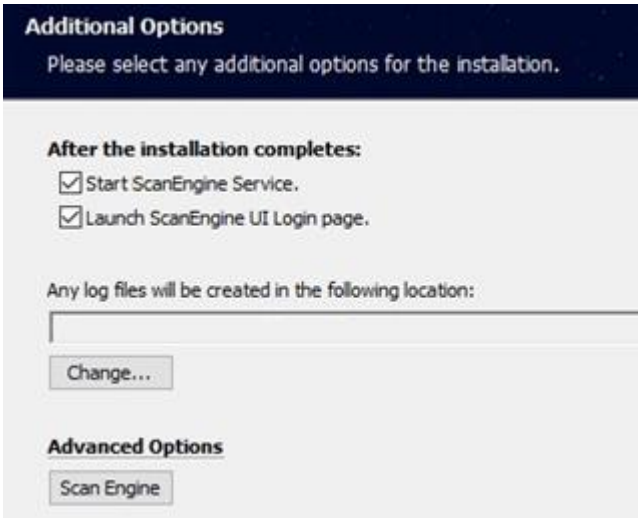
On the IIS Configuration for API screen, select your scan-engine API virtual directory. This will modify the URL used to access the API. Click **Next**.



On the Additional Options screen, click the check boxes if the scan engine service and UI are to be started after installation.

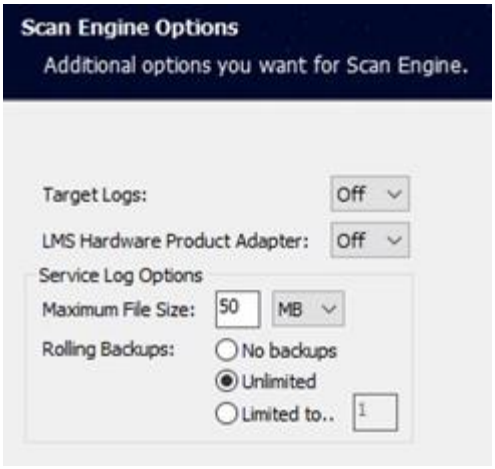
If you want to install third-party libraries, clear the **Start Scan Engine Service** option and click **Change** to modify the location where the log files will be located. By default, this location will hold the service log, UI log, and any target logs.

For details about third-party libraries, see the “License activation” section below.



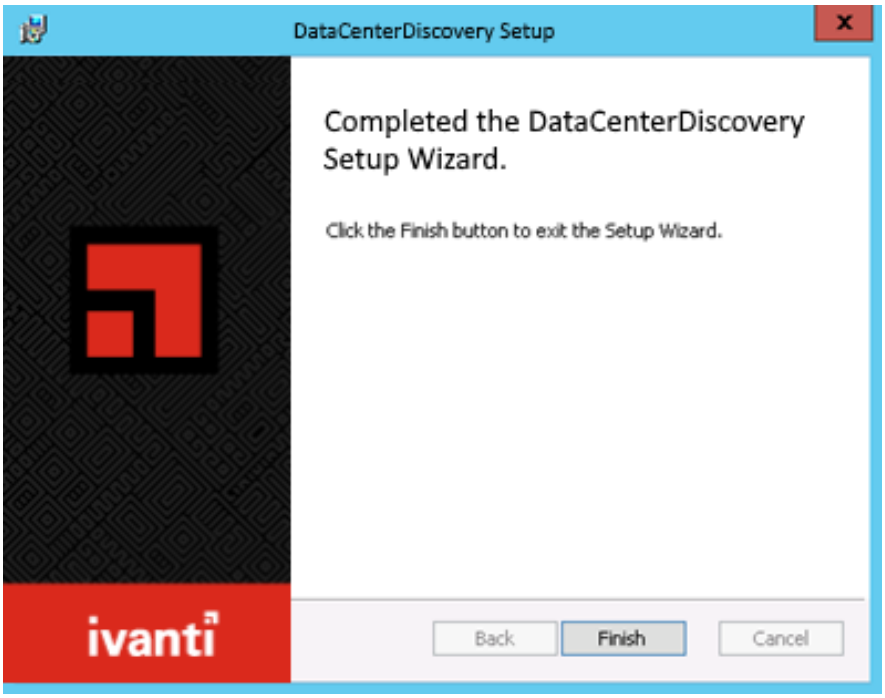
Click the **Scan Engine** button to modify additional advanced options for the scan engine:

- Only enable the Target Logs if you want verbose logging on each scanned target.
- The LMS Hardware Product Adapter is not enabled by default. This product adapter requires that the strategy results get written temporarily to the target hard drive as the strategies execute.
- Service Log Options allow you to modify the size of the service log and any potential backups:
    - **No backups** means a single service log is maintained.
    - **Unlimited** means that the complete history of the service log is maintained.
    - **Limited to** allows only a certain number of previous files.



When finished, click **Back** to return to the previous screen, then click **Next.** A screen will display showing a summary of the install details. Click **Install**.

After installation is complete, click **Finish**. The scan engine service and UI will launch at the completion of the installation (unless you previously cleared this option).



If you chose to create a new encryption key, the key will now be in the location specified during the installation. This key is used to control access to credentials used within the scanning engine and should be retained for future use. See the *Data Center Discovery—Scan Engine Security Guide* for additional information.

> **IMPORTANT:** Make a backup of this file. If it's not saved, it could be permanently lost.

At this point, the Data Center Discovery scan engine should be installed and running. If the scan engine service fails to start, the most likely problem is that the server hosting the service does not trust the Authenticode certificates used by Ivanti to sign the code. "Appendix B" lists the steps necessary to address this issue.

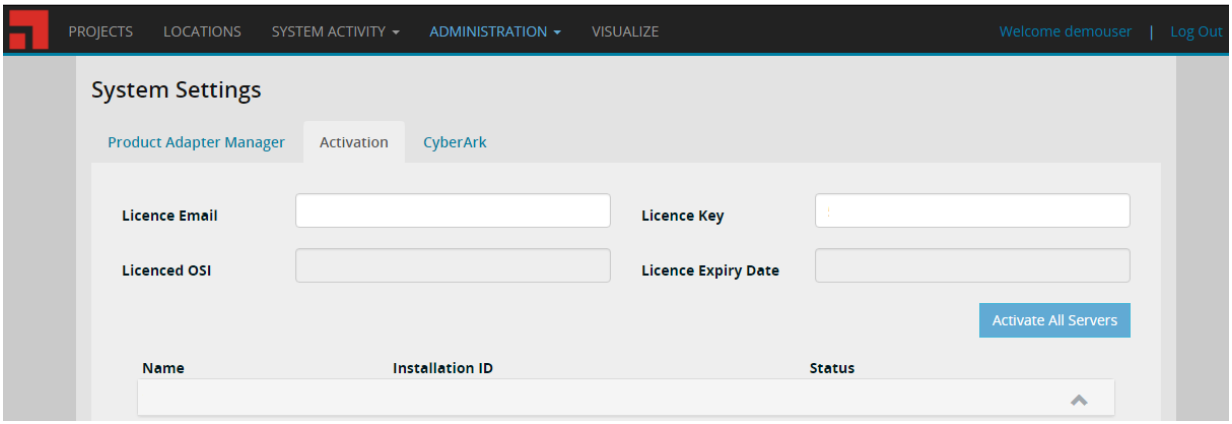
License activation

Licenses for the scan engine must be valid to begin the scanning process.

To activate automatically

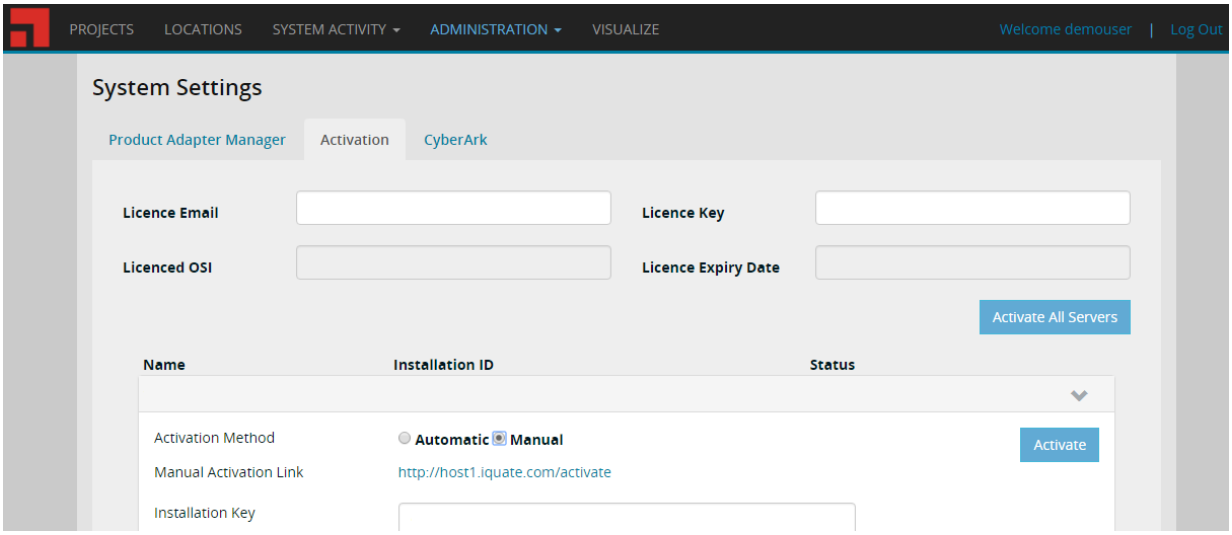
If the scan engine isn't currently licensed, the UI will direct you to the scan-engine activation page. If prompted in this way, then complete the instructions from step 4 onward.

1. Launch the scan engine UI.
2. Log into the UI as **Admin**.
3. Select **Administration > System Settings > Activation**.
4. Provide the **License Email** and **License Key**.
5. Click the **Activate All Servers** button.



To activate manually

1. Launch the scan engine UI.
2. Log into the UI as **Admin**.
3. Select **Administration > System Settings > Activation**.
4. Identify the scanning engine to be activated.
5. Expand the scanning engine to be activated using the down arrow.
6. Select the **Manual** option for activation.
7. Go to the Product Activation site (as provided by Ivanti) and select the appropriate product from the drop-down menu.
8. Enter your email, CD-Key, Installation ID, and Version.
9. Click **Activate**.
10. Copy the activation code.
11. Enter the installation key into the Installation Key text box.
12. Click the **Active** button.



Third-party libraries

Installations of the third-party libraries do not require a scan engine service restart or device reboot. The new libraries will become available to the scan engine once they're installed.

DB2 runtime client

To enable the scan of an **IBM DB2** database, a special client application must be installed on the scanning server.

Ensure that you've downloaded and installed the **IBM Data Server Runtime Client** from IBM. Refer to the *Data Center Discovery—Scan Engine Prerequisites Guide* for information on IBM DB2 access. See the "IBM DB2 support libraries" section for a full discussion.

Informix client SDK developer edition

To enable the scan of an **Informix** database, a special client application must be installed with the scanning server.

Ensure that you've downloaded and installed the latest version of **Informix Client SDK Developer Edition** from IBM. Refer to the *Data Center Discovery—Scan Engine Prerequisites Guide* for information on Informix access. See the "Informix support libraries" section for a full discussion.

Oracle runtime client

No additional client libraries are required to support the current releases of Oracle. These are packaged and installed automatically with the scan-engine installation package. No additional configuration is required.

Note that the Oracle 11 Client (Oracle.DataAccess-4.122.3), which is used to scan older versions of Oracle, is now disabled by default. You can enable this post-installation by changing the default value of “false” to “true” in the application settings if needed. Modify the file ScanEngine.EXE.CONFIG file as shown:

```
<add key=“EnableOracle11Client” value=“true” />
```

You’ll need to restart the service for this change to take effect.

SQL Server runtime client

No installation is required to access SQL Server targets. Native Windows SQL interfaces are used by the scanning server. No additional configuration is required.

Upgrading

To facilitate a software upgrade on the same server, the upgrade performs an uninstall operation and then an install operation. The uninstall leaves the current scan engine configuration files in place. These files are reused to provide the configuration information needed to reproduce the original setup.

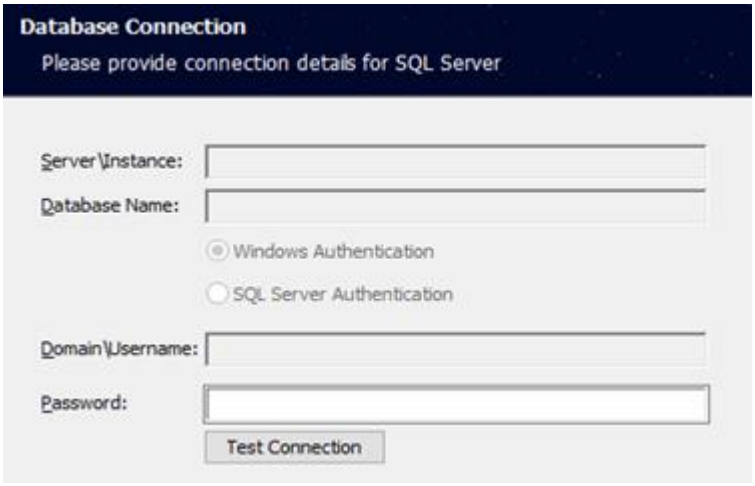
As part of the upgrade, the database itself will be upgraded. It's therefore important that all database activity stop prior to the upgrade. This means that all scan engines connected to the database must stop scanning and the scan service must be stopped for all these servers.

Approximate upgrade time is 5 minutes.

To upgrade the scanning service

Right-click the scan engine installer and run. You may receive a popup asking for permission to continue; if this happens, enter your appropriate administrator login details.

The Database Connection screen may display at the beginning of an upgrade that uses Windows Authentication. In that case, only the password will be editable, which is the password for the Windows Authentication user.



Click **Next**. The current settings will be displayed. Click **Install** to begin the upgrade. When installation is complete, click **Finish**.

Upgrade notes

Service stop error: As part of the standard upgrade process, the scan service should have been stopped as mentioned above.

If this has not happened, the upgrade itself will attempt to stop the service. Depending on the current activities within the service, the stop operation may take longer than the standard service controller timeout period. In this case, the upgrade process will raise a stop service error. If this occurs, it's recommended that you stop the service manually, then continue the upgrade.

Restart service settings: By default, during the install, the product is configured to restart when the service stops due to an error. During the upgrade process, the service restart values are reset to the default values. If you've modified the service restart parameters, then, following an upgrade, your settings for service restart must be re-instated.

Multiple scanning servers: In the case where you have multiple scanning servers connected to a central database, each of the scan services must be stopped prior to starting the upgrade.

You must then upgrade each scanning server separately. Any scanning server that is not upgraded will be unable to start until the upgrade is complete.

Uninstalling

To fully uninstall the application

1. Locate the scan engine software in the **Windows Programs and Features configuration**.
2. Select the scan engine software in the installed software list.
3. Select **Uninstall** and execute the uninstall operation to completion.

> **Note:** To facilitate the re-installation of software on the same device, the uninstall operation leaves the current scan-engine configuration files in place from the current install. These files are then re-used to provide the configuration information to reproduce the original setup.

If the configuration is to be changed for the re-install, then the original configuration files must be deleted. These files are located in the Program Files folder as detailed during the installation.

Changing installation features

It's possible to modify certain settings for your installation; these include the database credentials and the advanced scan engine options.

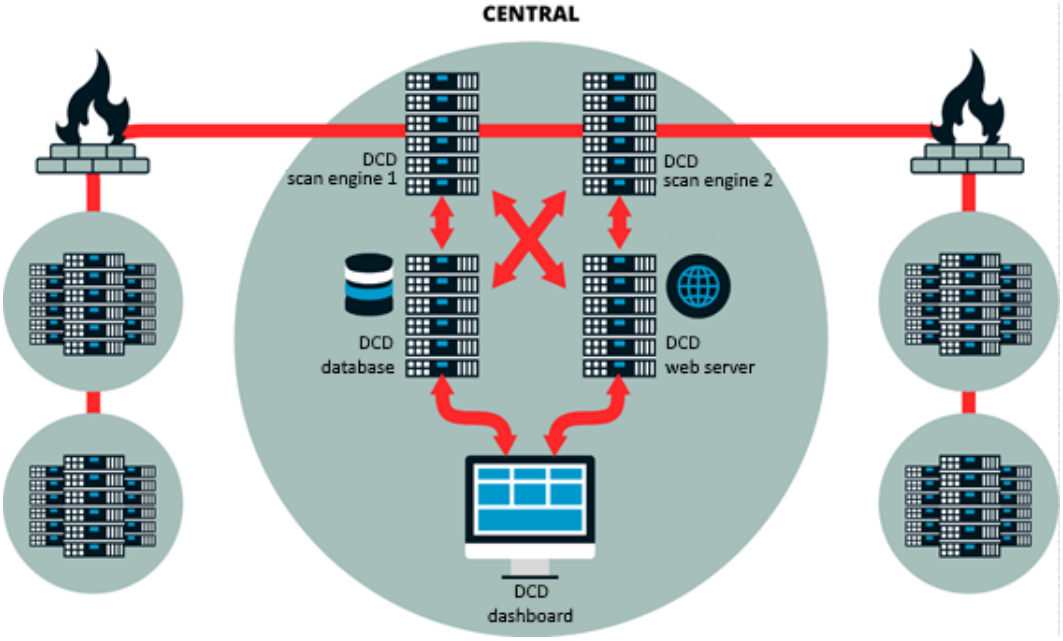
You may need to modify the database credentials when the existing credentials no longer work due to a company policy requiring periodic password changes.

To modify settings

1. Locate the scan engine software in the **Windows Programs and Features configuration**.
2. Select the scan engine software in the installed software list.
3. Select the **Change** option. You may see a dialog asking for permission to continue; if this happens, enter your appropriate administrator login details. Click **Next**.
4. Update the database connection settings. You can use the **Test Connection** button to ensure these are correct. Click **Next**.
5. Update any additional options, such as the location for the log files or advanced settings for the scan engine. When finished, click **Next**.
6. Click **Update**.
7. Once the update is complete, click **Finish**. Your database credentials will successfully update for all installed components and any advanced settings will be applied.

Installing a 2nd scanning server

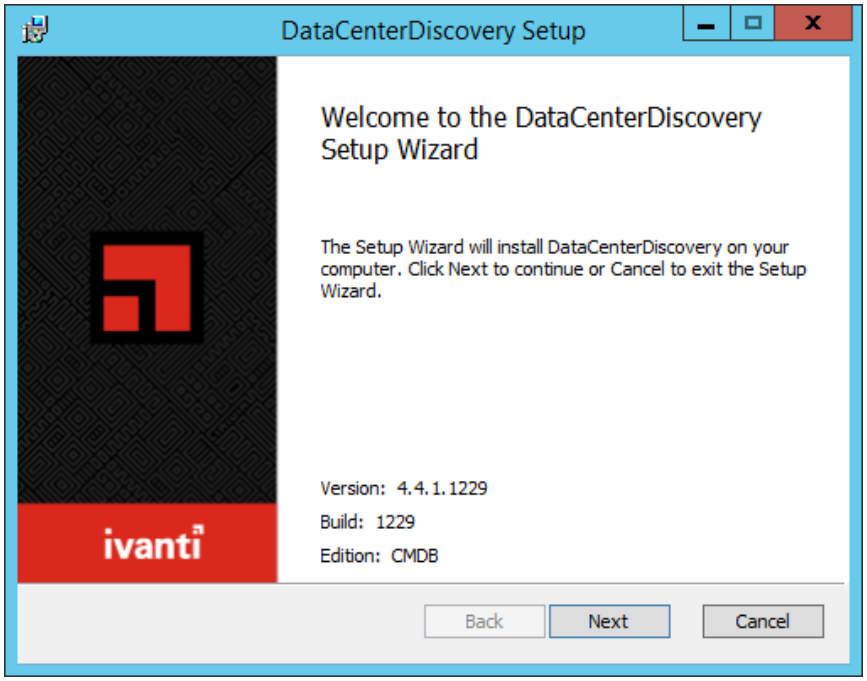
Installing a second scan engine for Data Center Discovery provides a means to add additional scanning resources to an existing estate scan operation.



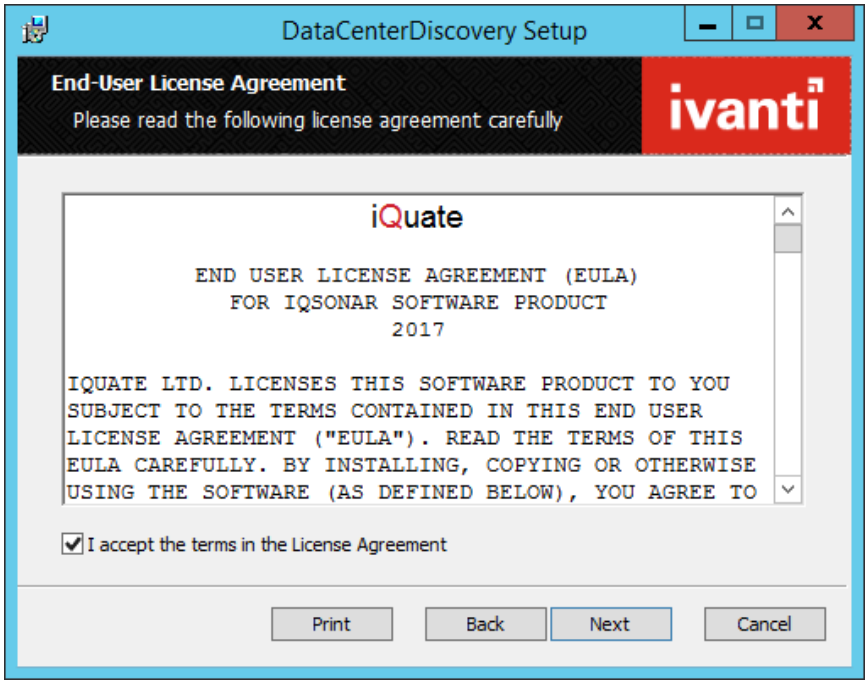
This is a requirement for the load balancing of scanning operations (i.e., more than one scanning engine is required to carry the CPU load). The results of the scanning operation are written back to a shared scan engine database. The resources for scanning can be shared across the entire estate, or each scan engine can be assigned exclusively to a section of the estate.

To install a 2nd scanning server

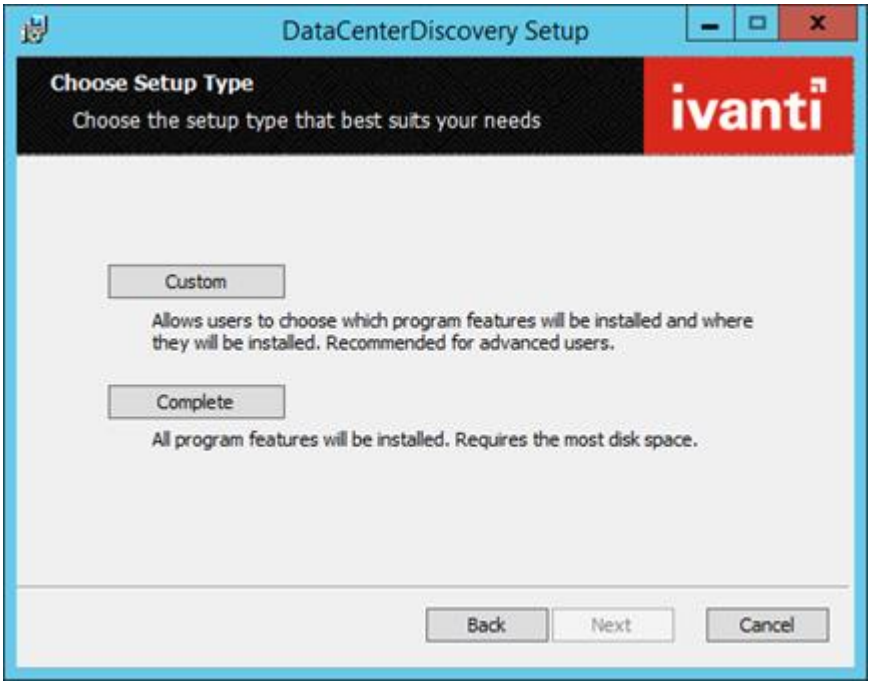
Start the Setup wizard and click **Next**.



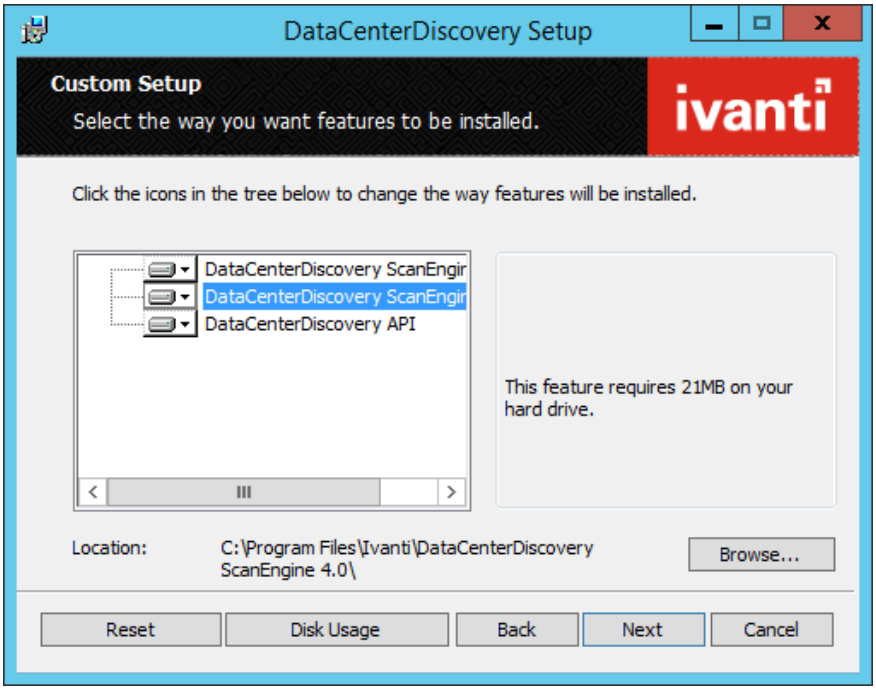
Read and accept the end-user license agreement. Click **Next**.



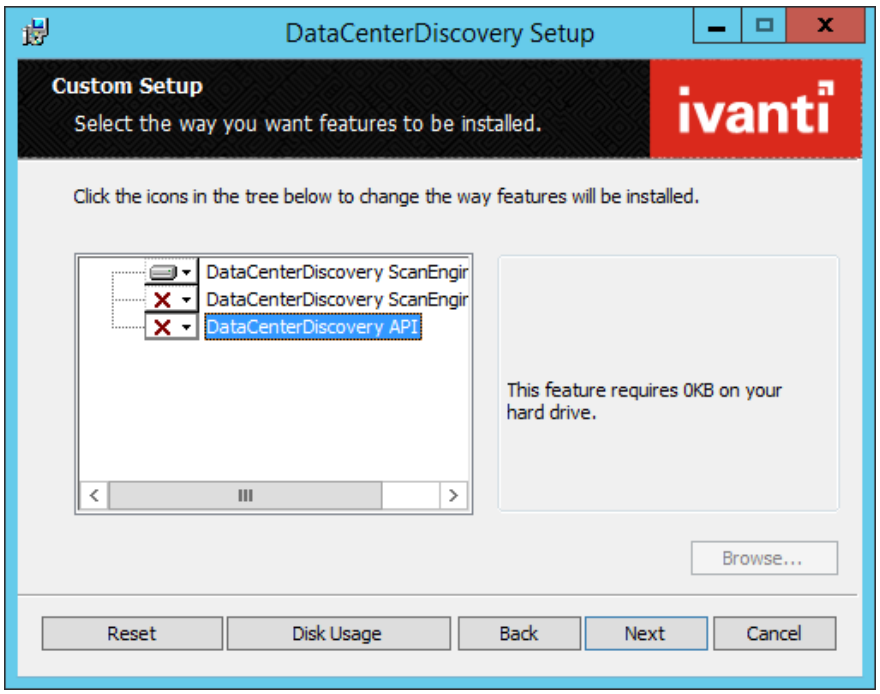
Click the **Custom** button to start the install.



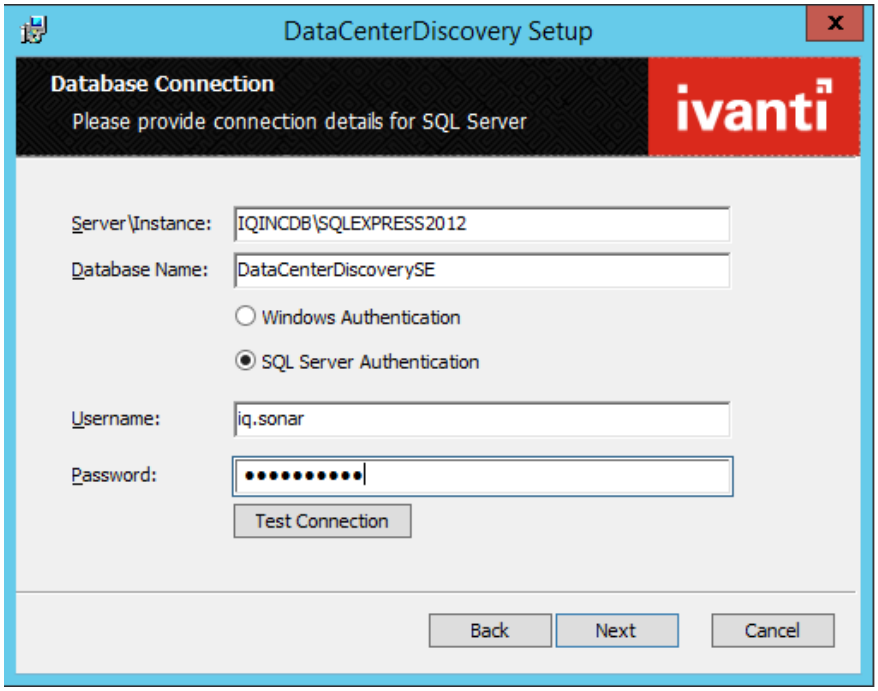
Select the scan engine UI, then from the drop-down menu, select the **Entire feature will be unavailable** option to make it unavailable. Repeat this step for the API component.



Identify that these options have been disabled. Click **Next**.



Select the remote database to be used by the scan engine. (See note below *before* selecting.)



> **Note:** This step requires replication of the database that you used in the first scan engine setup. It's important to use information that was provided with the original setup. If the same configuration isn't given, then two independent scan engines will be created rather than a single shared scanning resource.
>
> Since a second scan engine is to be installed on a different device from the original, the use of the localhost setup as the database server is not appropriate.

This example uses:

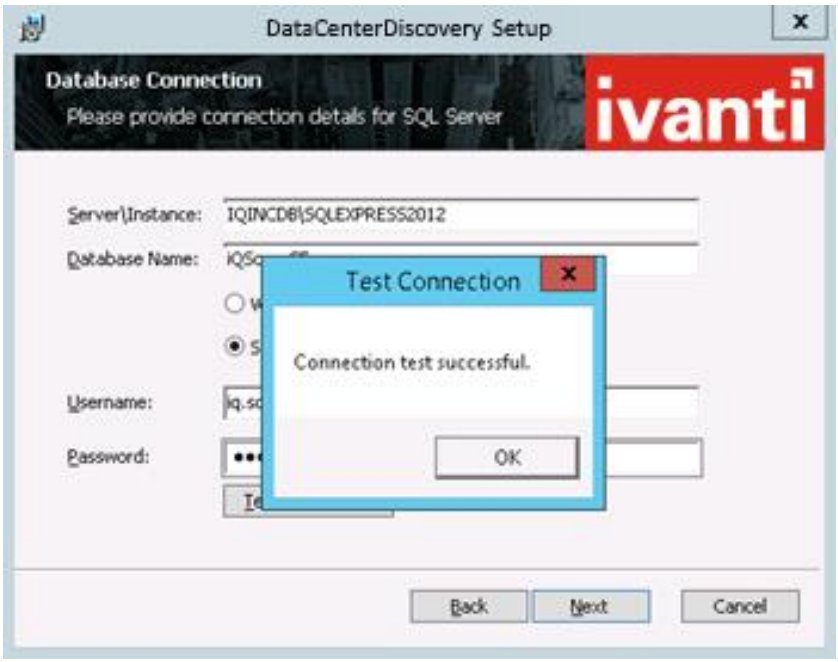
- The database for the first scan engine installation. Since this is the second installation, the specified database will already exist.
- The database-specific user to create and populate the scan engine database. The user must have appropriate database permissions (See the *Data Center Discovery—Scan Engine Prerequisites Guide* for details).

Additional information on database setup

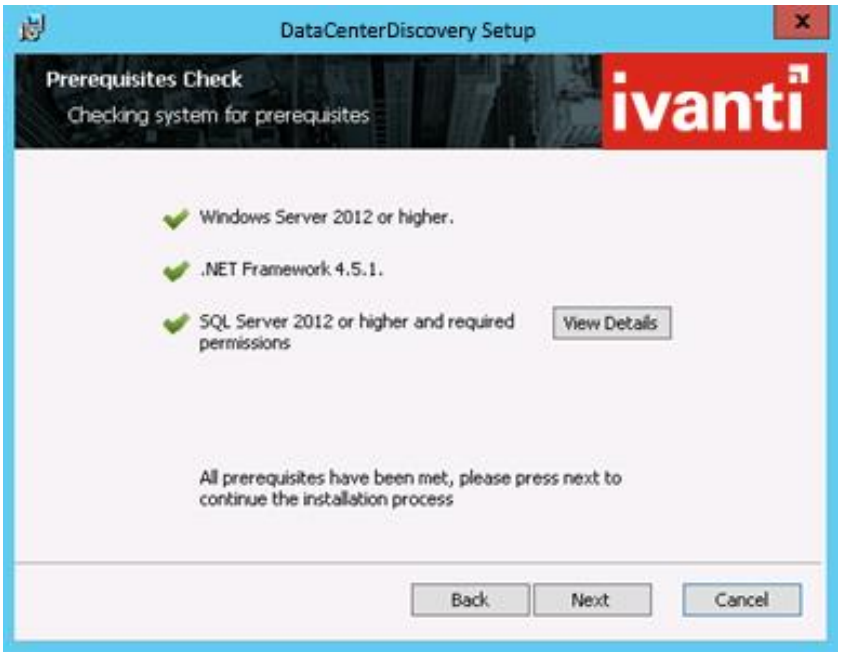
The scan database stores scan configuration information provided by the UI, as well as data from the scanned devices and/or applications identified during the scan operation.

✓	Description
	Server\instance: Define the server/instance on which the existing database is installed.
	Database name: Define the database name to be used**.**
	Authentication type: Select Windows or SQL Server authentication. • **Windows Authentication** uses a domain-defined username provided with access to the database. This will be the username of the logged-in user. A local machine account can't be used. • **SQL Server authentication** uses a SQL-Server-defined local user.
	Username: Enter the username to access the database. This name identifies who accesses the database to create the required database and save scanned information.
	Password: Specify the password to access the database.
	Test Connection (button): Test the login details for the database.

Test the connection. Click **OK** to close the test window. Click **Next**. Confirm that the prerequisites for the install have passed and correct any failed tests.



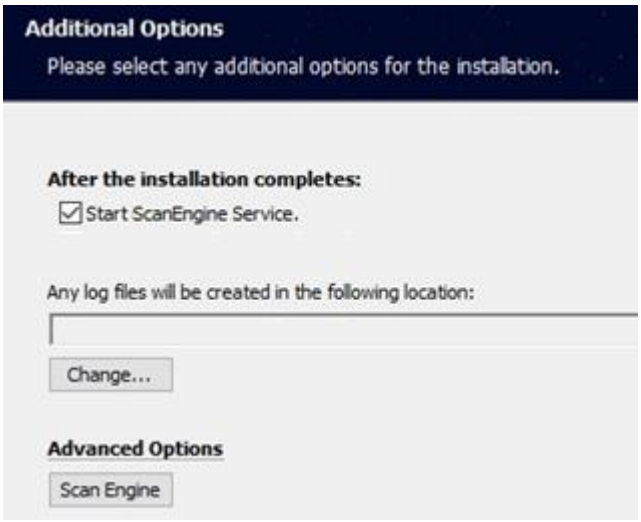
Click **View Details** to see the criteria that were checked or if a failure occurred. Click **Next**.



Select the **Use an Existing Key** option. Click **Browse** to select the file which holds the encryption key that was created during the first scan engine install.

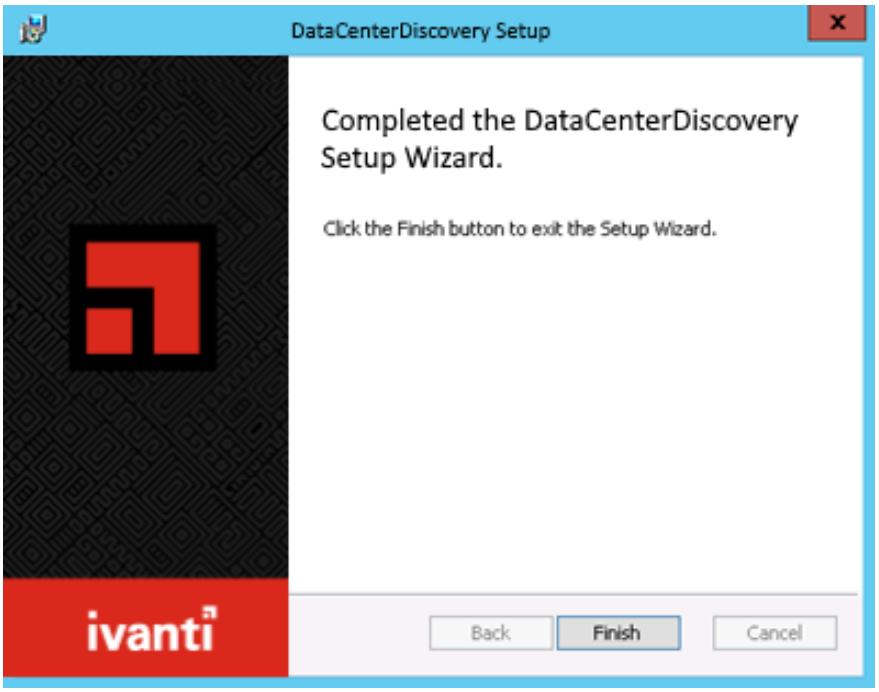
The sharing of this customer encryption key between the two scan engines allows credentials (used in the scanning process) to be accessible to **both** scanning engines. Click **Next**.

On the Additional Options screen, click the **Start Scan Engine Service** option. Click the **Change** button if you want to modify the location where the log files (service log and any target logs) will be located, then click the **Scan Engine** button to modify additional options for the scan engine if required. Click **Next**.



Once finished, click **Back** to return to the previous screen and continue the installation. Click **Next**. Review the screen showing a summary of the install details, then click **Install**.

When setup is complete, click **Finish**. The scan engine service will launch at the completion of the install (unless you previously cleared this option).



A second scanning server is now available for configuring in the UI. It must be activated in the standard way.

Post-installation

Once you've successfully set up the scan engine, refer to the *Data Center Discovery—Scan Engine User Guide* for help with using the product. Use this guide to become familiar with the scan engine and scan database.

Database recovery model

The suggested Recovery Model setting is simple for scan engine-related databases, unless local requirements dictate otherwise. This can be done from:

SQL Server Management Studio > Database > Properties > Options > Recovery Model

Appendix A: Key information

Item	Information

CLR	Common Language Runtime
	Query to run in SQL Management Studio to enable CLR:
	`sp_configure 'clr enabled', 1;`
	`GO RECONFIGURE;`

Scan database	The database in which the data from the scan engine is initially stored.
Ivanti support	https://www.ivanti.com/support/ivanti-support
SQL Server instance	A SQL Server instance is a complete SQL server; you can install many instances on a device, but only one default instance.

Appendix B: Authenticode certificate not trusted

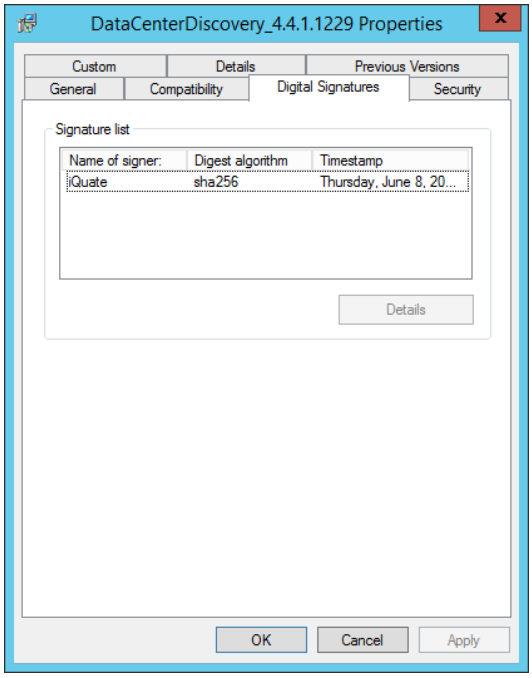
If the scan engine fails to start after installation, the most likely cause is that the server hosting the scan engine service doesn't trust the Authenticode certificates used by Ivanti.

In such a scenario, the service log will contain error messages such as "Unable to find Authenticode certificate on plugin" or "An error occurred during server initialization > System.Exception: Unable to find any Product Adapters."

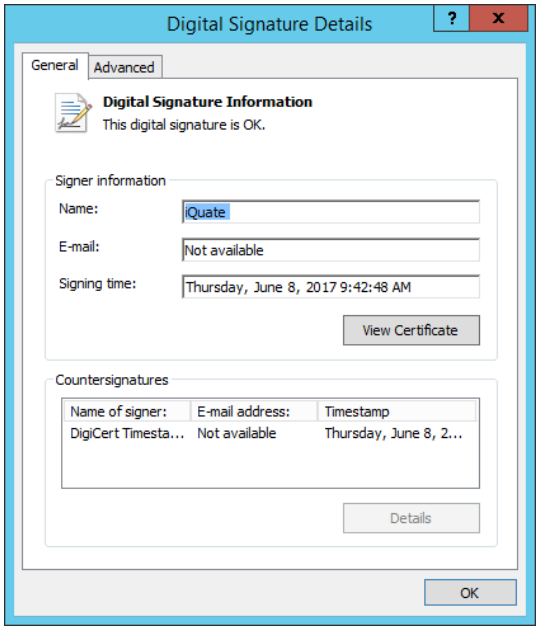
To address this problem, it's necessary to add the certificates to the local device trusted stores.

To add certificates to the local device trusted stores

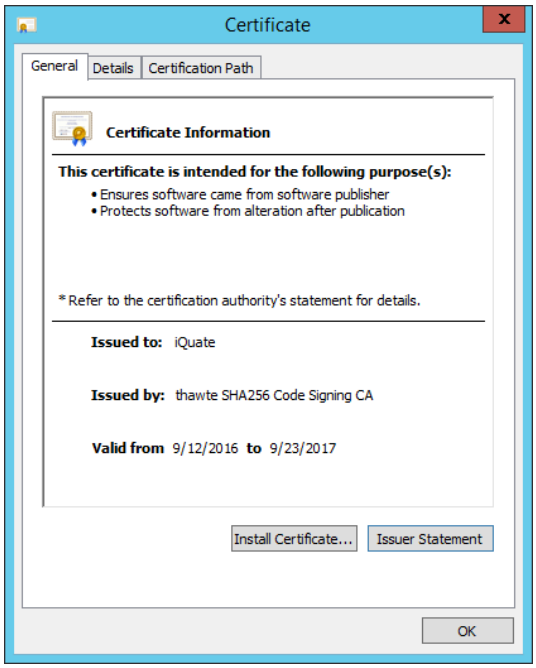
1. Right-click the scan engine **msi** installer file and open the **Properties** dialog. Click the **Digital Signatures** tab.
2. In the Signature list, select the **iQuate Limited** entry. Click the **Details** button to view the signature details.



3. Click the **View Certificate** button.

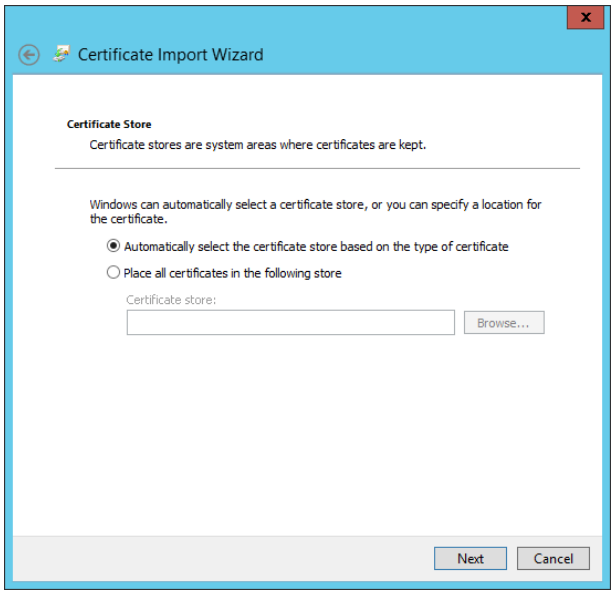


4. Click the **Install Certificate** button.



5. Select the **Local Machine** option and click **Next**.

6. Click **Next**. Once completed, click **Finish**.



7. Return to the Digital Signature Details dialog, select the countersignature, and click **Details**.
8. Install this certificate in the same way.