

Aurora 2.5

Installation & Deployment Guide

Condrey Corporation
August 9, 2022

Condrey Corporation makes no representations or warranties with respect to the contents or use of this documentation, and specifically disclaims any express or implied warranties of merchantability or fitness for any particular purpose. Further, Condrey Corporation reserves the right to revise this publication and to make changes to its content, at any time, without obligation to notify any person or entity of such revisions or changes.

Further, Condrey Corporation makes no representations or warranties with respect to any software, and specifically disclaims any express or implied warranties of merchantability or fitness for any particular purpose. Further, Condrey Corporation reserves the right to make changes to any and all parts of the software at any time, without obligation to notify any person or entity of such revisions or changes. See the Software EULA for full license and warranty information with regard to the Software.

Any products or technical information provided under this Agreement may be subject to U.S. export controls and the trade laws of other countries. You agree to comply with all export control regulations and to obtain any required licenses or classification to export, re-export, or import deliverables. You agree not to export or re-export to entities on the current U.S. export exclusion lists or to any embargoed or terrorist countries as specified in the U.S. export laws. You agree to not use deliverables for prohibited nuclear, missile, or chemical biological weaponry end uses. Condrey Corporation assumes no responsibility for your failure to obtain any necessary export approvals.

Copyright © 2022 Condrey Corporation. All Rights Reserved.

No part of this publication may be reproduced, photocopied, or transmitted in any fashion without the express written consent of the publisher.

Condrey Corporation
122 North Laurens St.
Greenville, SC, 29601
U.S.A.
http://condrey.co

CONTENTS

1 SYSTEM REQUIREMENTS 3

1.1 Database 3
1.2 Aurora 3
1.2.1 Hardware *3*
1.2.2 Operating System *3*
1.2.3 .NET Framework *4*
1.3 Aurora .Ext 5
1.3.1 Hardware *5*
1.3.2 Operating System *5*
1.3.3 .NET Framework *5*
1.4 Supported Web Browsers 5
1.5 Aurora License 5

2 DEPLOYMENT PLANNING 6

2.1 Application Overview and Structure 6
2.1.1 Aurora *6*
2.1.2 Aurora .Ext *7*
2.2 SQL Server Database 7
2.2.1 SQL Server Edition *7*
2.2.2 Capacity Planning *7*
2.3 Access for Internal Users 9
2.3.1 User Authentication *9*
2.3.2 User Authorization *9*
2.3.3 Storage Locations *9*
2.4 Access for Guest Users 10
2.4.1 Sharing Enablement *10*
2.4.2 Mail Delivery System *10*
2.4.3 Guest User Password Policy *11*
2.5 Security Considerations 11
2.5.1 Secure Web Communication *11*
2.5.2 File System Access – Internal Users *11*
2.5.3 File System Access – Guest Users *12*
2.5.4 Provider Sharing Rules *12*
2.5.5 Stored Credentials *13*
2.5.6 Firewall *14*

3 DEPLOYMENT REQUIREMENTS CHECKLIST 15

4 INSTALLING MICROSOFT SQL SERVER 17

4.1 SQL Server Installation 17
4.2 SQL Post Configuration Considerations 22

5 INSTALLING THE AURORA WEB APPLICATION 23

5.1 Installing the Aurora Package 23
5.2 Running the Aurora Configuration Dashboard 28
5.2.1 Aurora Database Configuration Wizard 28
5.2.2 Aurora License Configuration 33
5.2.3 Aurora Web Application Configuration 36
5.2.4 Complete the Dashboard Configuration 49
5.2.5 Reset Two-Factor Authentication 49
6 INSTALLING THE AURORA .EXT WEB APPLICATION 50
6.1 Installing the Aurora .Ext Package 50
6.2 Running Aurora .Ext Configuration 56

1 System Requirements

1.1 Database

Aurora requires one of the following versions of Microsoft SQL Server:

- SQL Server 2019
- SQL Server 2017
- Any of the following editions: Express[1], Standard, and Enterprise
- Both Windows and Linux platforms supported

[1] Depending on sizing considerations for licensed users and audit log retention, SQL Server Standard or Enterprise edition may be required.

For hardware requirements and recommendations for SQL Server, please see:

- SQL Server 2017 - https://msdn.microsoft.com/en-us/library/ms143506(v=sql.130).aspx
- SQL Server 2019 - https://docs.microsoft.com/en-us/sql/sql-server/install/hardware-and-software-requirements-for-installing-sql-server-2019?view=sql-server-ver16
- SQL Server on Linux - https://docs.microsoft.com/en-us/sql/linux/sql-server-linux-setup?view=sql-server-ver16#system

1.2 Aurora

1.2.1 Hardware

The Aurora web application requires the following minimum hardware:

- Quad-core processor
- 8 GB RAM
- 4 GB disk space minimum, plus additional space for document viewer cache

If Aurora is hosted on the same server as Aurora .Ext or SQL Server, additional RAM and disk space are required.

1.2.2 Operating System

Aurora is supported on the following operating systems:

- Windows Server 2019
- Windows Server 2022

Recent service packs and updates should be maintained, as support for Aurora may require current updates to be in place.

1.2.3 .NET Framework

Aurora requires .NET Framework 4.8.
The Aurora installer packages will install .NET Framework 4.8 if not already present on the system.

1.3 Aurora .Ext

1.3.1 Hardware

The Aurora .Ext web application requires the following minimum hardware:

- Quad-core processor
- 8 GB RAM
- 4 GB disk space minimum, plus additional space for document viewer cache

If Aurora .Ext is hosted on the same server with Aurora or SQL Server, additional RAM and disk space is required.

1.3.2 Operating System

Aurora. Ext is supported on the following operating systems:

- Windows Server 2019
- Windows Server 2022

Recent service packs and updates should be maintained, as support for Aurora .Ext may require current updates to be in place.

1.3.3 .NET Framework

Aurora requires .NET Framework 4.8.
The Aurora installer packages will install .NET Framework 4.8 if not already present on the system.

1.4 Supported Web Browsers

Aurora and Aurora .Ext support the latest versions of the following desktop web browsers:

- Chrome
- Firefox
- Microsoft Edge
- Safari



The *Limit Share Time* property of Provider Rules only applies to the rule with the closest matching path.

1.5 Aurora License

Aurora is licensed for the Active Directory forest where the product is installed. For other licensing considerations and limits, see the associated End User License Agreement.

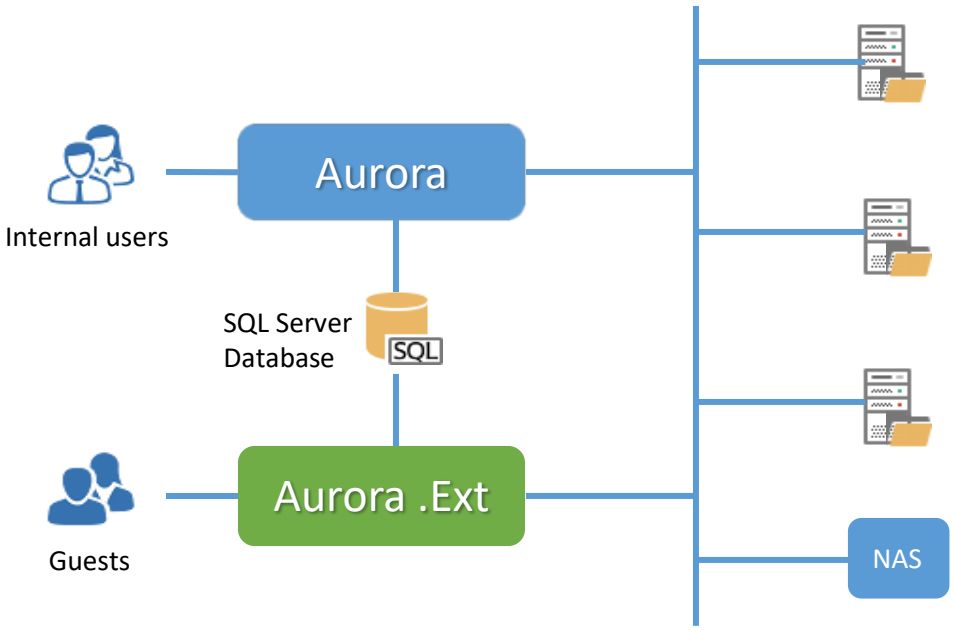
A Condrey Corporation sales representative will provide you with a license file at the time of purchase. This file is required to complete the initial configuration of the Aurora product suite.

2 Deployment Planning

2.1 Application Overview and Structure

The Aurora product suite consists of a set of products working in concert with your enterprise Active Directory environment.

- **Aurora** – The main web application. It is used for the following purposes:
  - Administrative configuration and management
  - End-user remote access for network file systems
  - End-user creation and management of sharing relationships with guest users outside of the organization
- **Aurora .Ext** – The access portal provides remote file access for Guest users. Self-service account registration and management are provided through the portal as well. This subsystem may be enabled or disabled, and the security is governed by the Aurora administrator.
- **Database** – A Microsoft SQL Server database provides storage for key configuration and management structures as well as storage for Guest accounts and Guest Shares.



2.1.1 Aurora

When internal users authenticate to Aurora, they are accessing the network file system with their own credentials and their access to files is governed solely by security in NTFS and Active Directory. That is, a user session is created and the user accesses files just as he would on a Windows workstation attached to the domain. As a result, there is no proxy-based access to the file system.

For more information, see *Managing Aurora for Internal User Access* and *Understanding File Access* in the *Aurora 2.5 Administration Guide*.

2.1.2 Aurora .Ext

Guest users always access files though the Aurora .Ext application. A Guest user may register his account as his email address and the account must be confirmed via email before any access of files is permitted.

Guest access is governed by Guest Share records stored in the database. A Guest Share record includes the path to be accessed as well as other information such as the internal user that created the share, access rights, and share expiration.

All Guest account access to the file system is performed via a proxy account created specifically for this purpose. All access is logged in the auditing table in the SQL database. Administrators govern what areas of the network file system can be shared and the maximum rights that may be assigned.

For more information, see *Managing Aurora Ext for Guest Access* and *Understanding File Access* in the *Aurora 2.5 Administration Guide*.

2.2 SQL Server Database

Aurora database deployment considerations include estimation of storage capacity and deciding which edition of SQL Server to deploy.

2.2.1 SQL Server Edition

The Aurora packaging includes a version of SQL Server Express which should be adequate for general use cases. Recent versions of SQL Server Express are restricted to a maximum size of 10GB for all tables and indexes in the instance, so keep this in mind when planning for data base storage capacity.

2.2.2 Capacity Planning

Aurora manages storage of configuration, Guest Accounts, Guest Shares, and audit logs in the database. Except for audit logs, storage requirements are quite small. Consequently, the majority of database capacity planning will focus on Aurora's audit logs.

Depending on the number of users, the amount of daily activity, and the length of audit log retention, your SQL Server database may require relatively little disk space, or it may require many gigabytes of disk space. Use the following example scenarios to get a baseline understanding of space requirements. As you initially deploy Aurora in your environment, take note of audit log usage to establish a baseline suitable for your needs.

File System Activity Log

The file system activity audit log table (**audit.fs_activity_log)** is, by far, the table with the largest space requirements. Its maximum size could vary dramatically based on the following criteria:

- Number of active Internal Users
- Number of active Guest users and Guest Shares.
- Amount of activity per user
- Frequency of use by user
- Maximum lifespan of active Guest Shares

A single record may range anywhere from several hundred bytes to a couple thousand bytes in size or more depending on the length of accessed paths, account names, and the activity itself.

By default, the file system activity log for Internal Users is set to hold only the last 30 days of activity data. In addition, activity logs for all active Guest Shares are retained for the lifetime of each share. (Refer to *Configuration Settings* > *Logging* in the *Aurora 2.5 Administration Guide* for details on modifying this parameter.)

As an example, assume the following criteria:

Table 1 - Example File System Audit Log Size Calculator

Criteria	Example Value
Average record size	1K bytes
Average number of daily active Internal Users	100
Average number of activities performed per user per day	500
Number of days audit log is retained	30 days
Subtotal	*1.5 GB*
Average lifetime of Guest Shares	60 days
Average number of activities performed per Guest Share per day	50
Subtotal	*3 GB*
Approximate maximum log size	**4.5 GB**

In this example, over 4.5 GB of disk space would be needed to meet the threshold of audit log retention requirements. Depending on your usage patterns and retention needs, this number could be substantially less or significantly more. This does not include the space also needed for the timestamp column index.

Guest Share Management Log

Another possible exception is the Guest Share management table (**audit.guest_share_management_log**), which is set by default to 365 days of retention. (Refer to *Configuration Settings* > *Logging* in the *Aurora 2.5 Administration Guide* for details on modifying this parameter.)

This audit log tracks the management (create, update and delete) of Guest Shares, and should be relatively minor in the number of added entries compared to the file system activity log.

Records for this log could be somewhat larger due to description fields, and copies of modification data, but the number of entries should be fairly small compared to the file system activity log.

As an example, assume the following criteria:

Table 2 - Example Guest Share Management Audit Log Calculator

Criteria	Example Value
Average record size	4K bytes
Average number of daily share creates, updates, deletes	10
Number of days audit log is retained	365
Approximate maximum log size	**14.6 MB**

Even with a 10-year retention policy (which would bump the base size to 146 MB, not including indexes), this metric would not impact size greatly.

2.3 Access for Internal Users

2.3.1 User Authentication

Internal Users authenticate using their Active Directory credentials. In addition, requirements for two-factor authentication are available. For details on configuring two-factor authentication system options, refer to *Configuration Settings* > *User Access* in the *Aurora 2.5 Administration Guide*.

2.3.2 User Authorization

Internal Users may be granted access to Aurora via an authorization group. For details on defining this group during initial setup, refer to *5.2.3 Aurora Web Application Configuration*.

2.3.3 Storage Locations

To make full use of Aurora, not only must users be configured for access, but storage locations must also be determined for users to navigate and manage.

Aurora provides configuration for both automatic and manually defined storage locations:

- Home Folders, based on the *homeDirectory* attribute of user accounts in Active Directory
- Managed group folders, via integration with *Senergy*
- Managed auxiliary folders, via integration with *Senergy*
- Manually-defined storage locations defined in Aurora

To enable or disable the automatic mapping of Home Folders, refer to *Configuration Settings* > *General Configuration* in the *Aurora 2.5 Administration Guide*.

Senergy is a file system management product from Condrey Corporation that assists with the automation of user and collaborative storage management. Aurora can take advantage of the following aspects of user and collaborative storage managed by a *Senergy* installation:

- Home Folders managed by *Senergy* update the associated *homeDirectory* attribute of any managed users in Active Directory. This ensures a consistent experience for accessing Home Folders by Aurora.
- Users managed by *Senergy* may have additional data on their user object identifying Auxiliary Storage paths. These paths are managed by *Senergy* and act as secondary storage mappings in addition to any Home Folder. Aurora can automatically identify and present any Auxiliary Storage paths associated with users.
- Security groups managed by *Senergy* have additional data stored in their Active Directory objects identifying associated managed storage paths. Aurora can automatically identify and present these associated paths for users that are members of these groups.

To enable *Senergy* integration with Aurora, refer to *Configuration Settings* > *General Configuration* in the *Aurora 2.5 Administration Guide*.

2.4 Access for Guest Users

Guest Users are typically users external to the organization. Technically speaking, a Guest is any user having a Guest account with Aurora that can access files via the Aurora .Ext web application. Since Guest accounts are based on email addresses, anyone with a valid email address could potentially register as Guest user.

Just having a registered Guest account does not, however, grant access to any files or folders in the organization. A trusted Internal User within the organization must first provide a **Guest Share** to the Guest. This Guest Share defines the Guest account name, the target file system path within the organization, and a set of shared permissions for performing actions in the target path.

Refer to *Managing Aurora .Ext for Guest Access* in the *Aurora 2.5 Administration Guide* for more information.

2.4.1 Sharing Enablement

Sharing must be enabled in the Aurora configuration settings to use Aurora .Ext and provide Guest User access.

To enable Sharing, see *Managing Aurora .Ext for Guest Access* > *Enable Sharing* in the *Aurora 2.5 Administration Guide*.

2.4.2 Mail Delivery System

Sharing with Guest Users and self-management of the Guest Users themselves relies on proper configuration of the SMTP mail system parameters.

It is necessary to provide the following for proper SMTP configuration:

- Host address and port
- Usage of clear text or TLS communication with the SMTP server
- Optional name and password for authentication to the SMTP server
- A “Mail From” email address for emails originating from Aurora and Aurora .Ext systems
- An optional “Mail From” display name

To configure the SMTP mail parameters for Aurora and Aurora .Ext, see *Configuration Settings* > *Mail* in the *Aurora 2.5 Administration Guide*.

2.4.3 Guest User Password Policy

Just as with Internal Users and their associated password and account policies in Active Directory, it is necessary to determine a similar set of policies for Guest Accounts which are managed by Aurora.

Policy settings include:

- Number of bad password attempts before account lockout
- Account lockout duration
- Password policy settings such as minimum length and required alpha, numeric and special characters.

For details on these policy settings and how to manage the policy, see *Managing Aurora .Ext for Guest Accounts* > *Modify the Account Policy* in the *Aurora 2.5 Administration Guide*.

2.5 Security Considerations

2.5.1 Secure Web Communication

Both the Aurora and Aurora .Ext sites make use of HTTP over TLS/SSL.

By default, the configuration wizards create self-signed, untrusted certificates for the site specified during the initial configuration. For a proper experience with both remote and guest users, these certificates should be replaced with valid, signed certificates from a trusted third-party certificate vendor.

Most certificate vendor sites provide instructions on how to set up a valid certificate for IIS, some of which are referenced below:

- https://www.digicert.com/kb/csr-creation-ssl-installation-iis-10.htm
- https://www.godaddy.com/help/manually-install-an-ssl-certificate-on-my-iis-10-server-27349
- https://www.entrust.com/knowledgebase/ssl/ssl-tls-certificate-installation-help
- https://sectigo.com/resource-library/install-certificates-microsoft-iis-8-x
- https://help.comodosslstore.com/support/solutions/articles/22000253004-microsoft-iis-10

2.5.2 File System Access – Internal Users

File system access for Internal Users is based on the user’s rights in the file system itself. When the user authenticates with Aurora, he is creating a logon session within Active Directory as well, which takes advantage of the same permissions and access restrictions already present in the network.

For more information, refer to *Understanding File Access* in the *Aurora 2.5 Administration Guide*.

2.5.3 File System Access – Guest Users

File system access for Guest Users requires proxy-based access. The proxy account and its associated proxy-rights group are defined during the initial configuration. It is the administrator's responsibility to assign the necessary Windows share and NTFS permissions to areas of the file system where Guest access is required.

For more information, refer to *Understanding File Access* in the *Aurora 2.5 Administration Guide*.

2.5.4 Provider Sharing Rules

Internal Users may not share anything with Guests until Provider Rules have first been established. Provider rules determine the following:

- Which file system paths may be shared with Guests?
- Which Internal Users are allowed to share those paths?
- What permissions may the Internal Users provide Guests for those paths?

As part of pre-deployment, it is helpful to start identifying the target paths for shared access, the set of trusted Internal Users (who become delegated Providers), and the allowed permissions those Providers may give to other users (Guests).

A general Sharing Policy should be established, and Provider Rules may then be defined to help enforce that policy.

2.5.5 Stored Credentials

Both Aurora and Aurora .Ext maintain the following credentials with the security considerations:

Credential	Storage
Database credentials	Local Windows registry using Windows DPAPI encryption
SMTP Mail relay credentials	Database, clear text
Aurora Service Account / Application Pool Identity	Stored using the built-in identity and password management for Windows services with “logon as user” Note that this credential is required to be an Active Directory account for basic query access to Active Directory, however, this account should not be given any more privileges than necessary, and should typically be limited to the default privileges of a standard user.
Aurora .Ext Proxy Account	Local Windows registry using Windows DPAPI encryption This account should be given the minimum permissions needed for shares and folders that Guest users may potentially access.
Guest Accounts	Database, uses default security with Windows Identity framework.
TOTP Secrets	Encrypted data is stored in the database, after salted encryption using a separate private key stored in the local file system.

As with most services needing credentials, the security of encrypted stored credentials is generally only as safe as access to the local server itself where those credentials are stored.

2.5.6 Firewall

The Aurora and Aurora .Ext configuration utilities add default inbound rules for access on ports 80 and 443 (or whichever ports were defined for web access) to the Windows Firewall rule set.

The addition of other Windows firewall rules may be required for accessing SQL Server or remote file systems, depending on how the Aurora and file system server firewalls are configured.

In addition, consideration should be made for any edge security with external corporate firewalls and NAT (network address translation) configurations that may be required for the successful operation of Aurora and Aurora .Ext.

3 Deployment Requirements Checklist

Use the following checklist to aid with pre-deployment planning.

Hardware

- ☐ Aurora
  - ☐ Quad-core processor
  - ☐ 8 GB RAM minimum
  - ☐ 4 GB disk space + document view cache space
- ☐ Aurora .Ext
  - ☐ Quad-core processor
  - ☐ 8 GB RAM minimum
  - ☐ 4 GB disk space + document view cache space
- ☐ SQL Server
  - ☐ Quad-core processor
  - ☐ 8 GB RAM minimum
  - ☐ 10 GB disk space minimum
  - ☐ See SQL Server documentation for additional recommendation

    SQL Server 2017 - https://msdn.microsoft.com/en-us/library/ms143506(v=sql.130).aspx

    SQL Server 2019 - https://docs.microsoft.com/en-us/sql/sql-server/install/hardware-and-software-requirements-for-installing-sql-server-2019

Active Directory Environment

- ☐ Active Directory Forest Functional Level of Windows 2003 or later
- ☐ Domain Functional Level of Windows 2003 or later for all domains where users or resources are located.

System Software (Aurora and Aurora .Ext)

- ☐ Windows Server 2019 , Windows Server 2022 with Updates
- ☐ .NET Framework 4.8
- ☐ The server is joined as a Member Server to a domain in the Active Directory forest

Aurora License

- ☐ Obtained a license for Aurora 2.5 for the current Active Directory forest

Database Installation

- ☐ SQL Server instance installed with the following configuration
  - ☐ Installed components include Database Engine Services and optional Management Tools
  - ☐ Instance name defined
  - ☐ Service Accounts defined
  - ☐ Collation set for Windows Collation (not SQL collation)

    Accent-sensitive selected

    Case-sensitive **unselected**

    Latin1_General_100 preferred

    Example: **Latin1_General_100_CI_AS**

- ☐ Authentication set for Mixed Mode
  Password set for **sa** (System Admin) account
- ☐ Data directories verified

Database Configuration

- ☐ TCP/IP Protocol Enabled
- ☐ TCP Port Defined for All Addresses or specific IP Address (default port 1433)

Internal User Access

- ☐ DNS name for Aurora web application identified
- ☐ IP Address and port for Aurora web application identified
- ☐ Aurora Administrators identified
- ☐ Authorized (licensed) Aurora users identified
- ☐ Optional – Excluded Aurora users identified
- ☐ Optional – Senergy integration considered
- ☐ Storage location mappings identified – static file system mappings for target groups

External Sharing

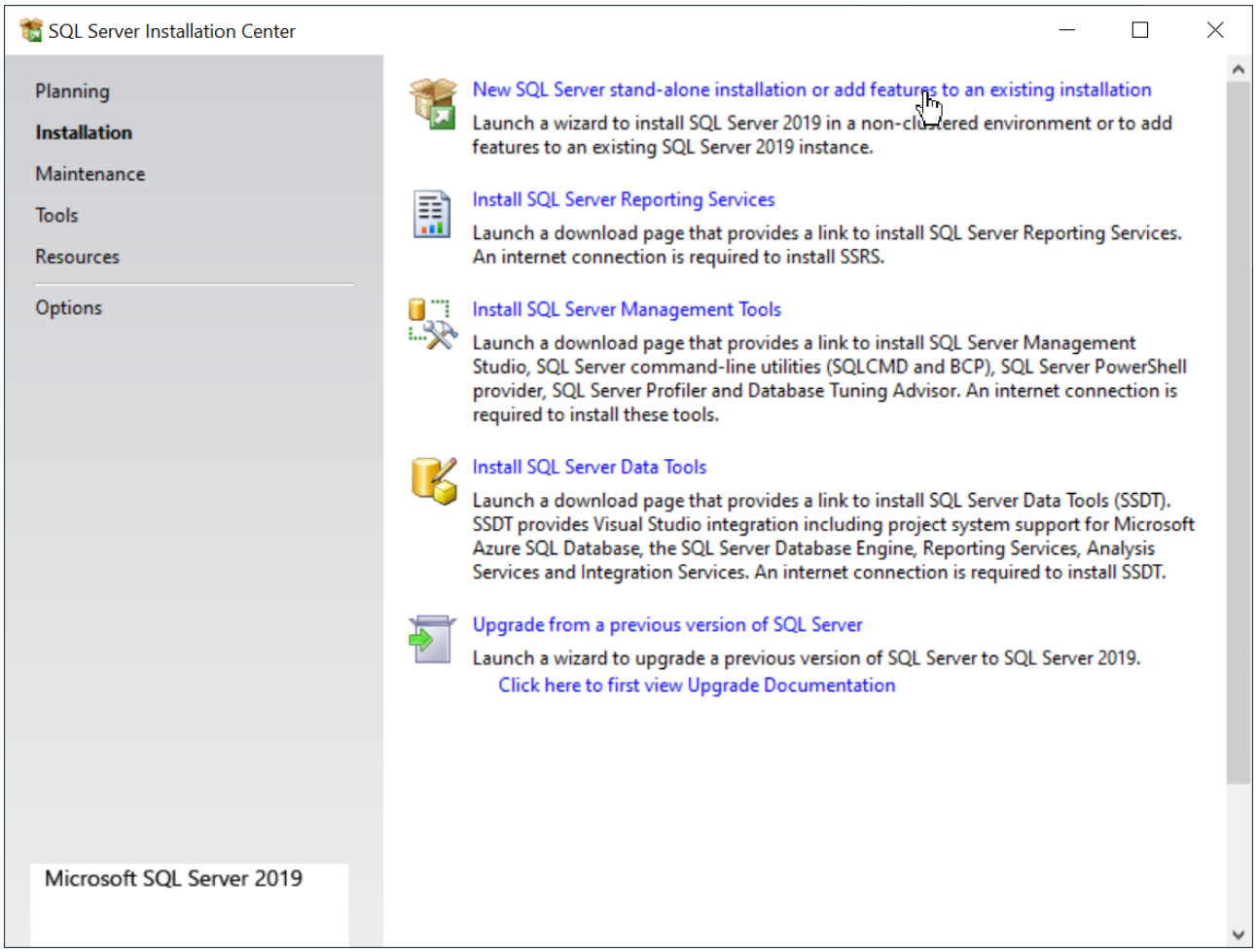
- ☐ DNS name for Aurora .Ext web application identified
- ☐ IP Address and port for Aurora .Ext web application identified
- ☐ Identified SMTP mail relay connection requirements (address, port, authentication)
- ☐ A general Sharing policy has been defined
- ☐ Shares and file systems identified for Guest access, according to the Sharing policy
- ☐ Restricted share and file system rights granted to the **auroraext_proxyrights** group
- ☐ Provider Rules designed to enforce the Sharing policy
- ☐ Password Policy established for Guest accounts
- ☐ Mail templates designed

4 Installing Microsoft SQL Server

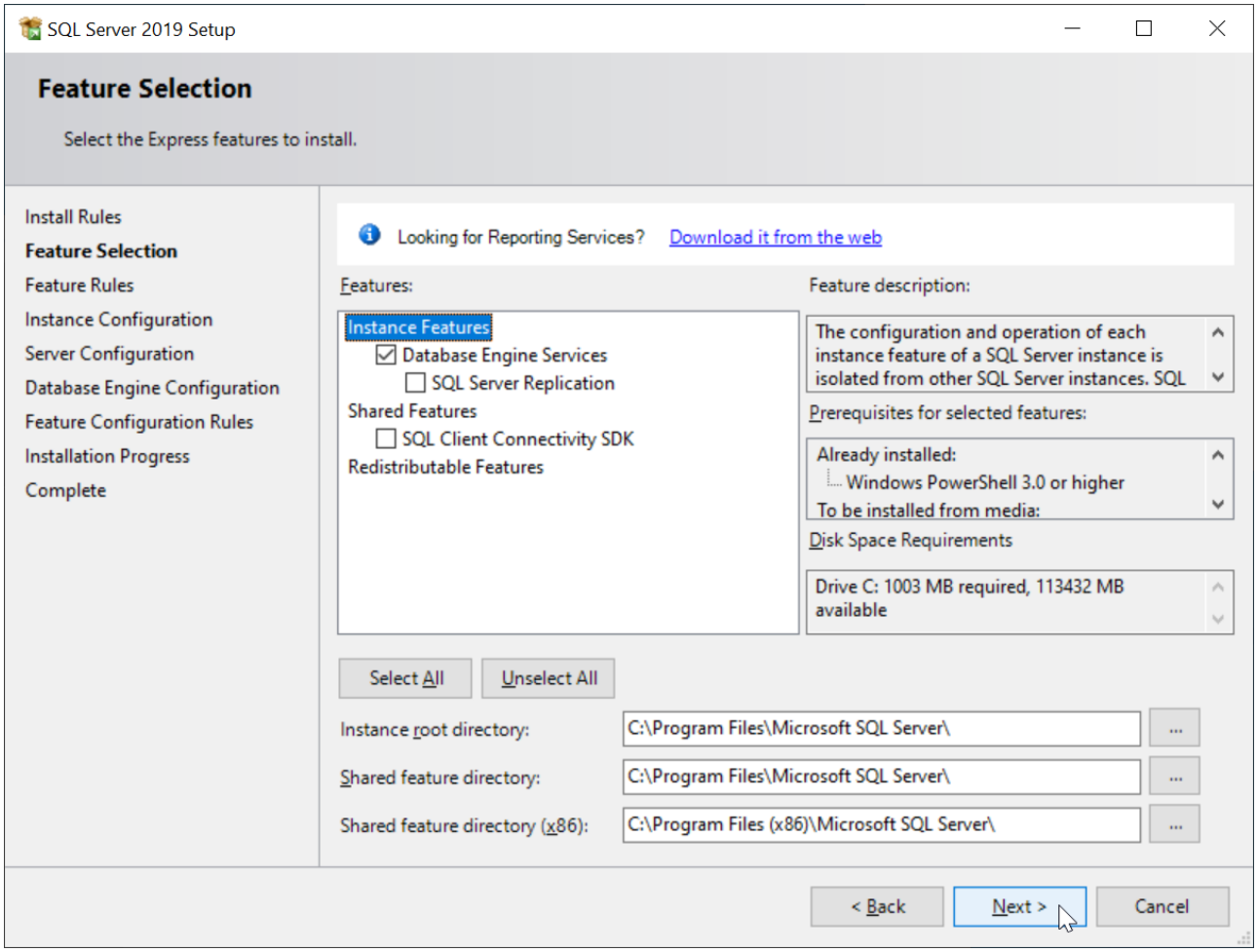
4.1 SQL Server Installation

The following procedures are specific to Microsoft SQL Server 2019 Express. Procedures will vary based on your version of SQL Server.

1. From the Microsoft SQL Server ISO, double-click `setup.exe`.
2. On the SQL Server Installation Center page, click **Installation**.
3. Select **New SQL Server stand-alone installation or add features to an existing installation**.



4. When the **Setup Support Rules** operation is complete, click **OK**.
5. When prompted, enter your product key, then click **Next**.
6. Accept the license terms, then click **Next**.
7. Include all Microsoft SQL Server product updates, then click **Next**.
8. When the **Setup Support Rules** operation has completed again, click **Next**.

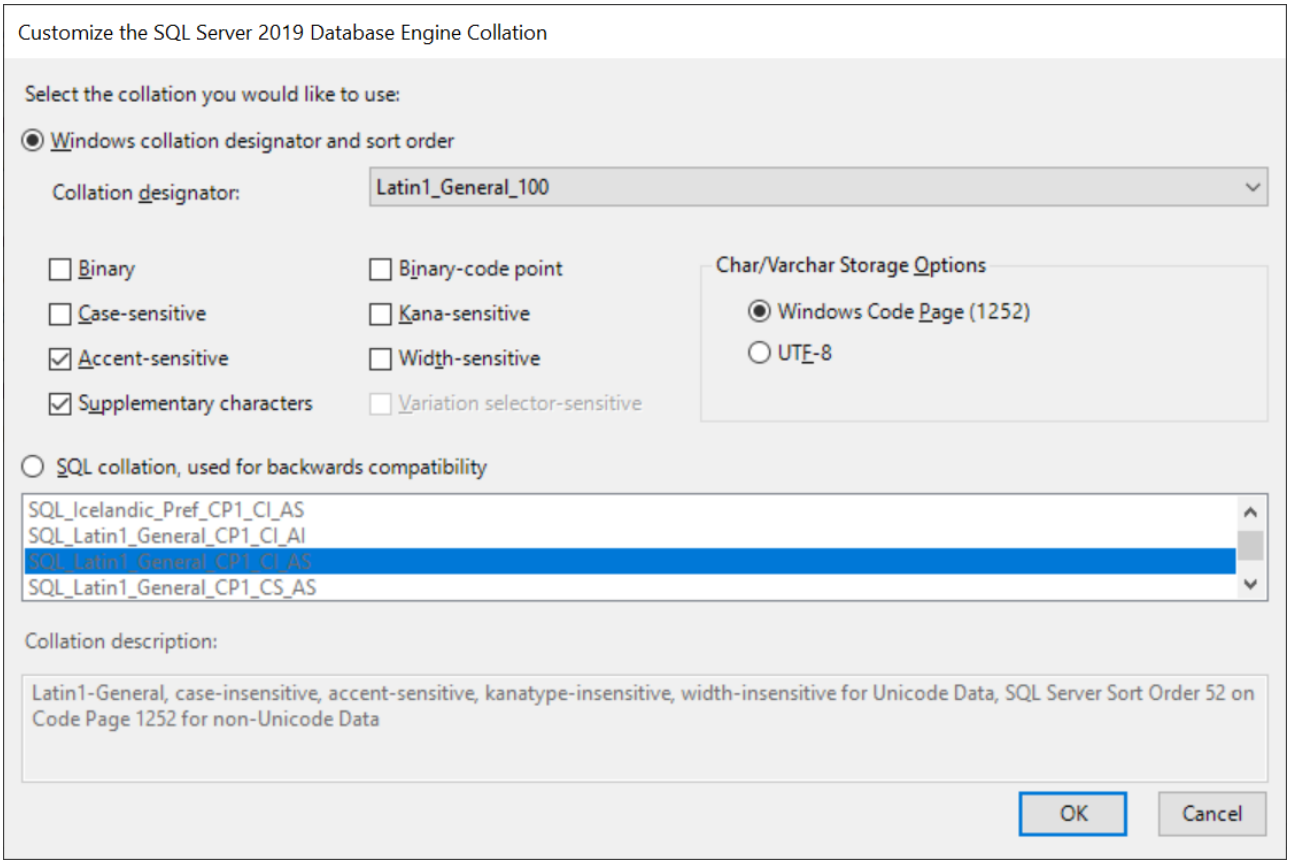


9. On the Feature Selection page, select **Database Engine Services**.
10. Optionally specify custom paths or use the defaults for the installation paths, then click **Next**.
11. In the Instance Configuration page, click the **Named Instance** option and specify a descriptive name for the instance such as `AURORADB` and click **Next**.
12. On the Server Configuration page, click the **Collation** tab.
13. Click **Customize**.
14. Click the **Windows collation designator and sort order** option.

15. From the **Collation designator** drop-down menu, select an acceptable collation and settings for your locale. For example, in North America, the recommend collation would be **Latin_General_100_CI_AS_SC** built from the following options:
    - Collation designator: **Latin_General_100**
    - Selected options: **Accent-sensitive** and **Supplementary characters**
    - Char/Varchar Storage Options (SQL Server 2019 only): **Windows Code Page (1252)**

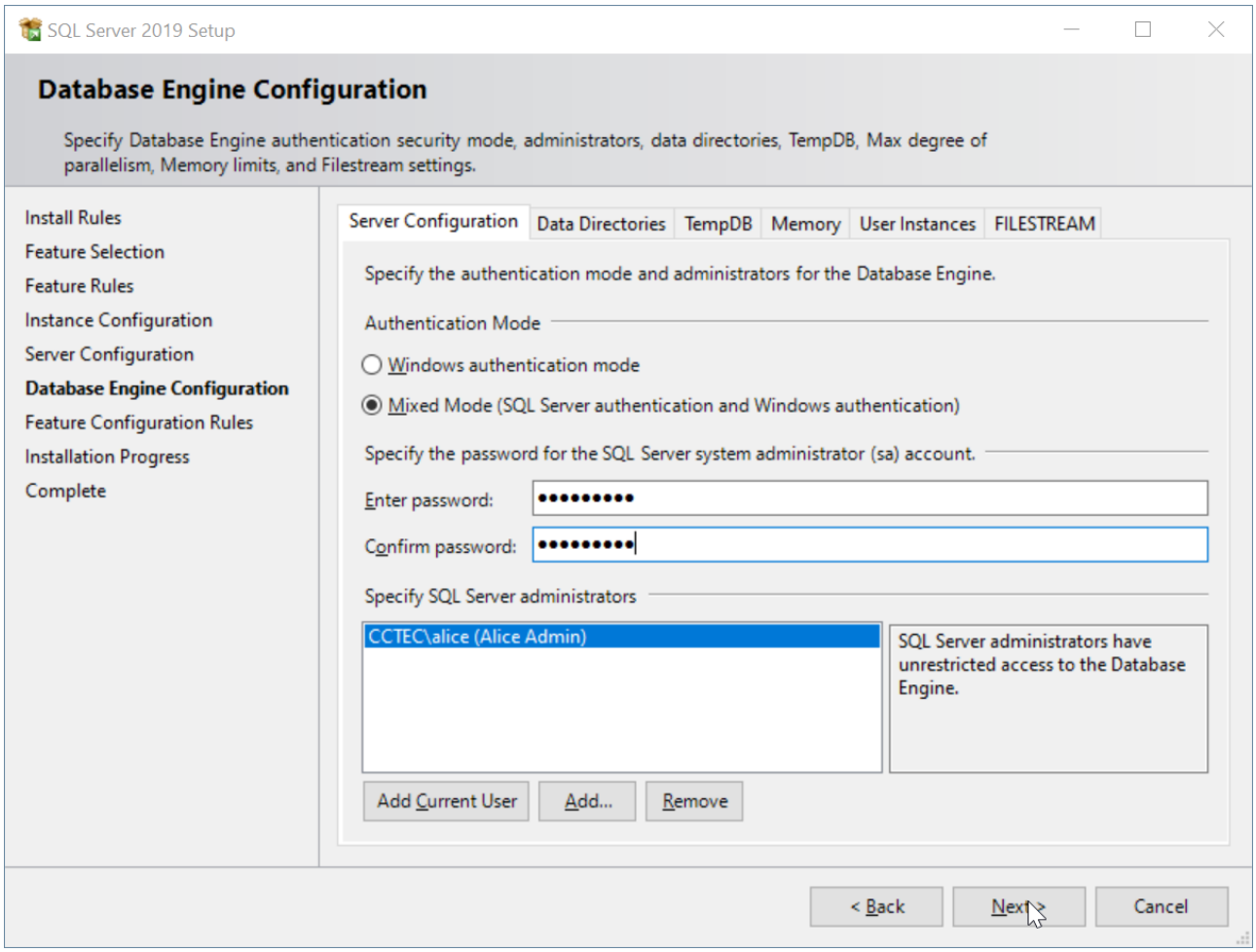
    We recommend that you select a collation that aligns with the Windows locale of the server where the Engine is installed.

    For more information on collation and locales, refer to https://docs.microsoft.com/en-us/sql/relational-databases/collations/collation-and-unicode-support.

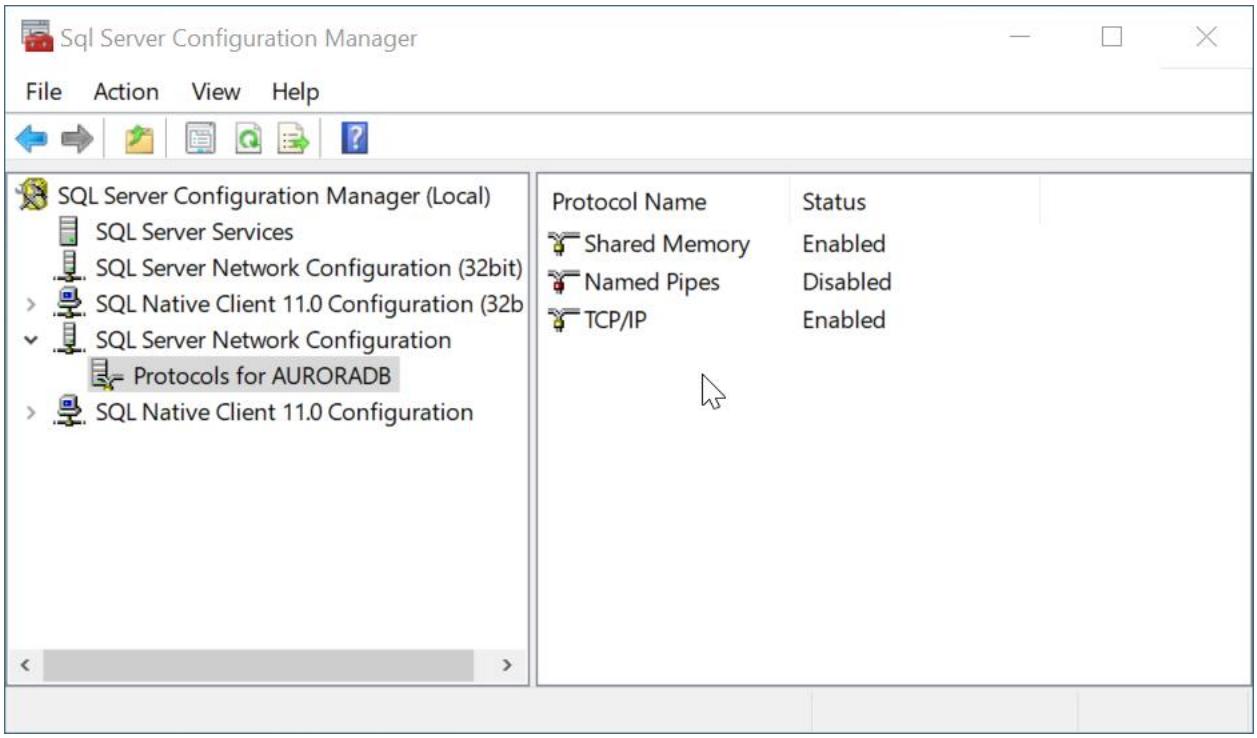


Aurora currently does not support the UTF-8 char/varchar storage options.

16. Click **OK**.
17. Click **Next**.
18. On the Database Engine Configuration page, select the **Mixed Mode (SQL Server authentication and Windows authentication)** option, enter and confirm the SQL Server administrator password, then click **Add Current User**.



19. Click **Next**.
20. Click **Install**.
21. When the installation is complete, click **Close** to close the Wizard.
22. Launch SQL Server Configuration Manager.
23. In the left pane, expand **SQL Server Network Configuration**.
24. Click **Protocols for AURORADB** (or the name of the database instance you chose earlier).



25. Right-click **TCP/IP** and select **Properties**.
26. Select the **Protocol** tab.
27. Under the **Enabled** field, click the drop-down and select **Yes**.
28. Select the **IP Addresses** tab.
29. Under the **IPAll** heading, set the **TCP Port** field to an available port such as 1433.
30. For the **TCP Dynamic Ports** field, set the value to 0 (zero).
31. Click **Apply**.
32. When the warning dialog box appears, click **OK**.
33. Click **OK** to close the TCP/IP Properties window.
34. Close the SQL Server Configuration Manager.

Firewall rules on the server hosting SQL Server may need configuration to allow for TCP port access to the TCP port specified during configuration.

4.2 SQL Post Configuration Considerations

Review these points and make any needed adjustments to your SQL database settings before installing and configuring the Aurora Web Application:

- The SQL Server service must be listening via TCP/IP v4 as the Aurora components require that for access.
- Some editions of SQL Server do not have TCP/IP enabled by default. If there are multiple instances, the instance that you just installed and configured might not be listening on the default port of 1433.
- Firewall rules might need to be modified.

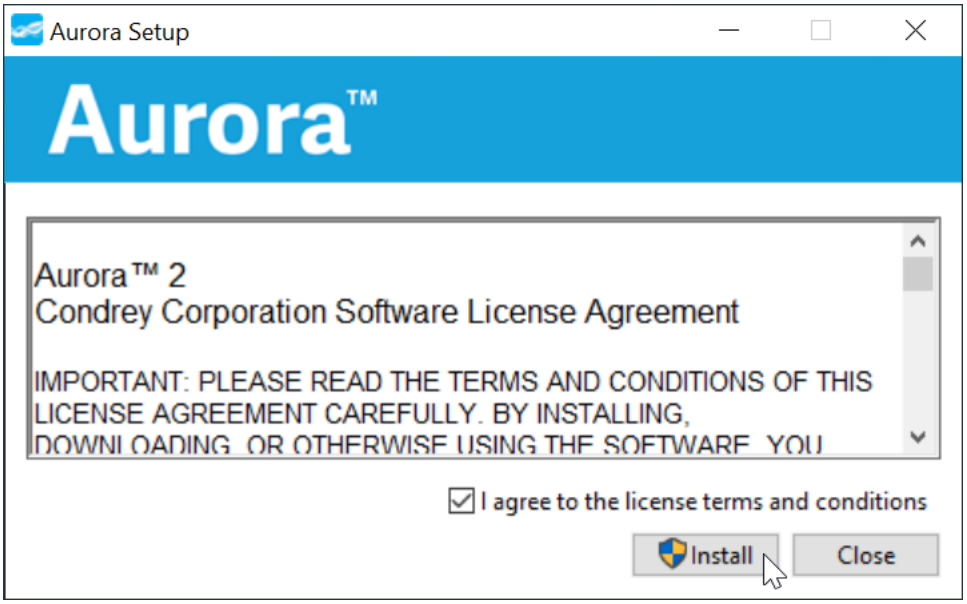
5 Installing the Aurora Web Application

The Aurora web application provides access for internal users via a web portal.

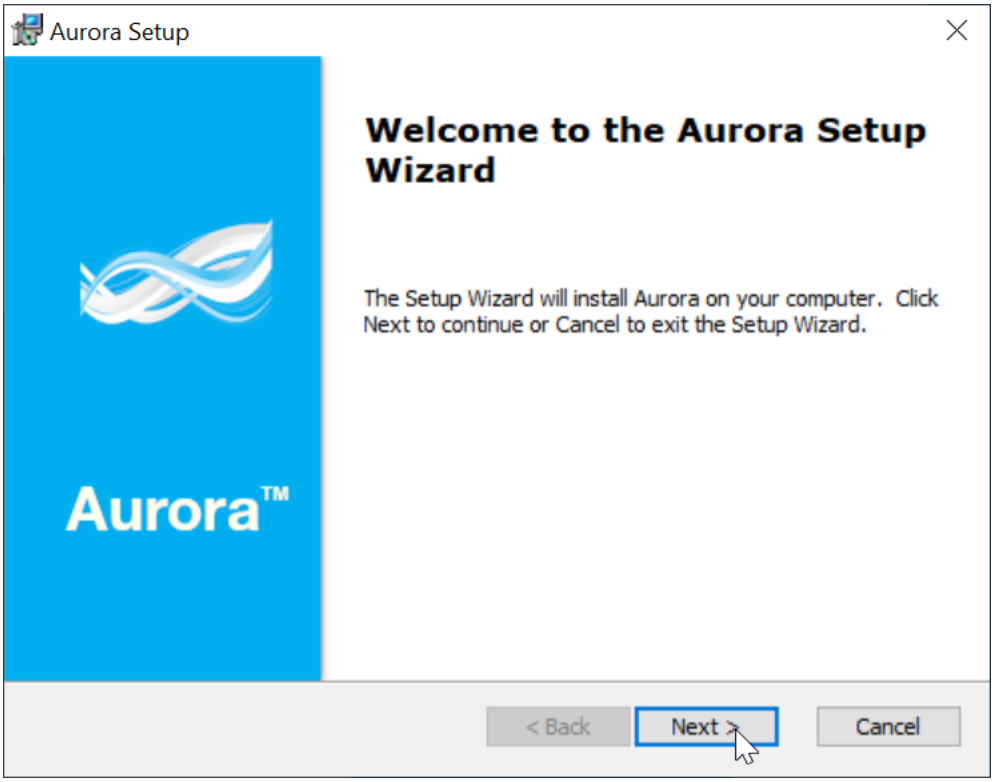
This application may be installed on the same server as the Aurora .Ext web application or on a separate server altogether.

5.1 Installing the Aurora Package

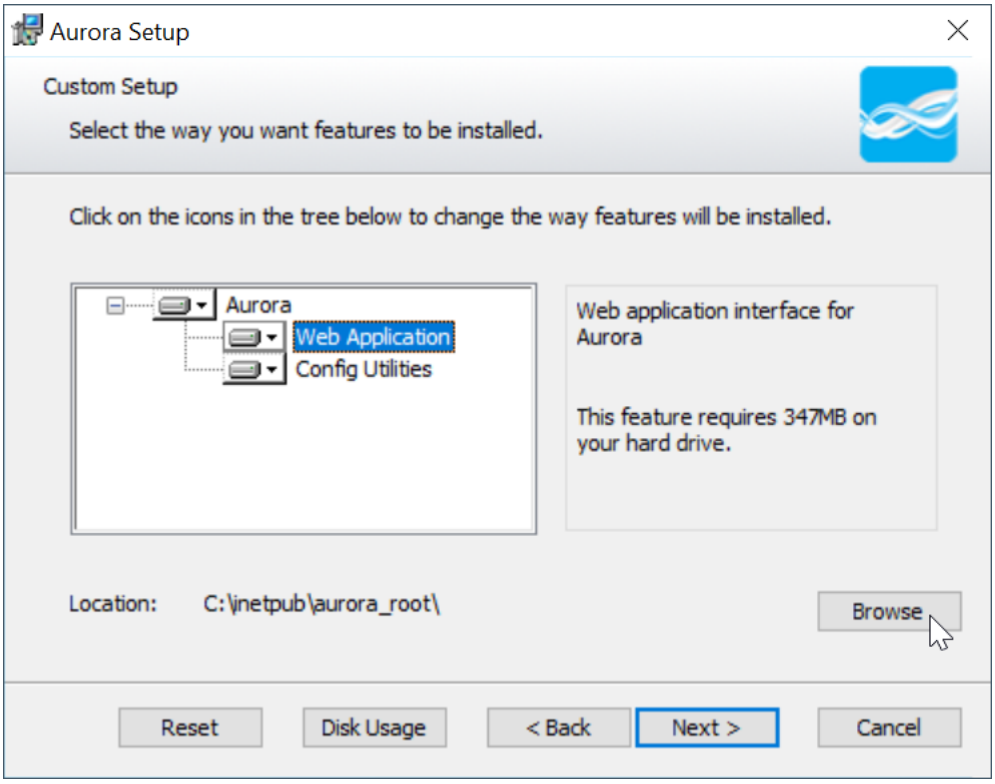
1. Before starting, be sure that you are signed into the target server with an Active Directory account that has the following privileges:
    - Full access to install software on the local server
    - Access to create or modify Active Directory users and security groups in the server's current domain
2. Copy the provided Aurora installer package **Aurora-Installer-2.5.0-x64-xx.exe** to the server where Aurora will be installed.
3. Double-click or run the installer package to start the installation process.
4. Review the license, select the license agreement check box, then click **Install**.



5. Click **Next** to continue.



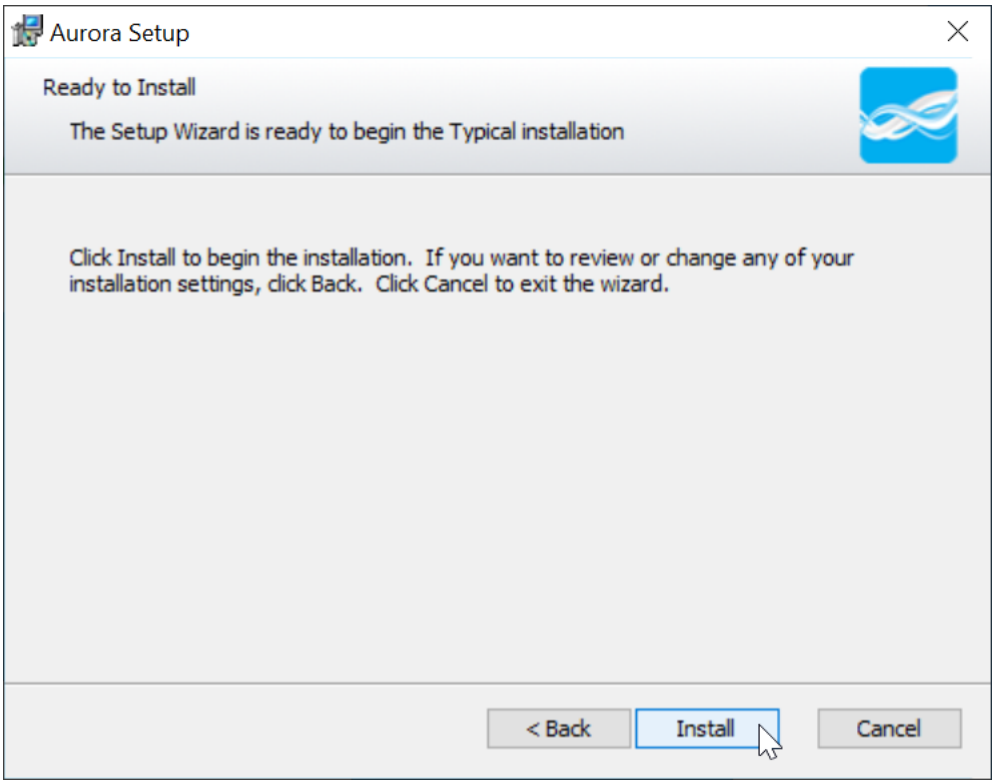
6. Review the locations where the software components will be installed.



The **Web Application** feature contains the ASP.NET files that will be served by IIS. By default, this in placed on the system drive in the default location for IIS web files, but the location may be directed to a separate disk if desired.

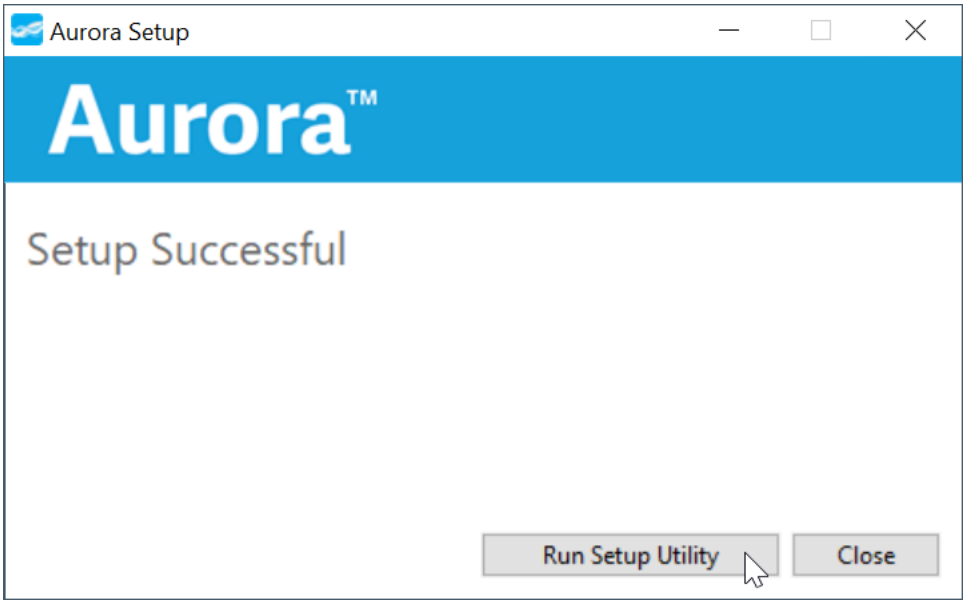
The **Config Utilities** feature contains the initial configuration dashboard and utilities for setting up the Aurora web application, database, and licensing.

7. Click **Install** to perform the installation.



8. Click **Finish** to complete the installation.

9. Click **Run Setup Utility** to launch the Aurora Configuration Dashboard.



If the required .NET Framework was installed as part of this process, a system reboot will be required before the Configuration Dashboard utility can run. Please reboot the system, then launch the Aurora Configuration Dashboard via the Start Menu as mentioned in the next step.

5.2 Running the Aurora Configuration Dashboard

The **Aurora Configuration Dashboard** is automatically launched at the end of the installation process if the **Launch config utility** checkbox was selected. This dashboard gives a quick overview of the basic configuration requirements for Aurora, and includes wizards for Database, License and Web Application configuration.

If the **Launch config utility** checkbox was not selected, or if you need to run the Aurora Configuration Dashboard again, simply launch the utility from the **Windows Start Menu > Condrey Corporation > Aurora Configuration Dashboard** start menu entry.

5.2.1 Aurora Database Configuration Wizard

1. Verify that the Active Directory forest has been properly identified, then click **Configure Database** to launch the Aurora Database Configuration Wizard.

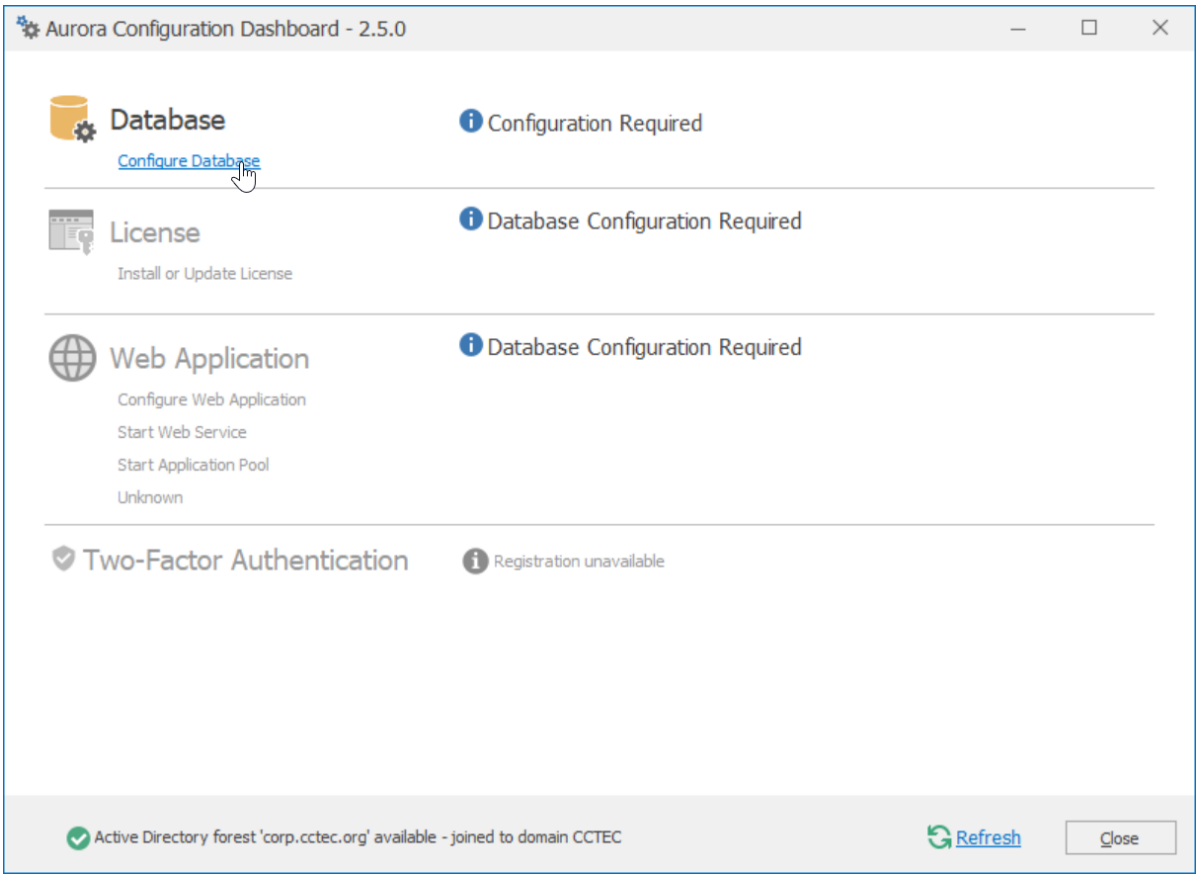
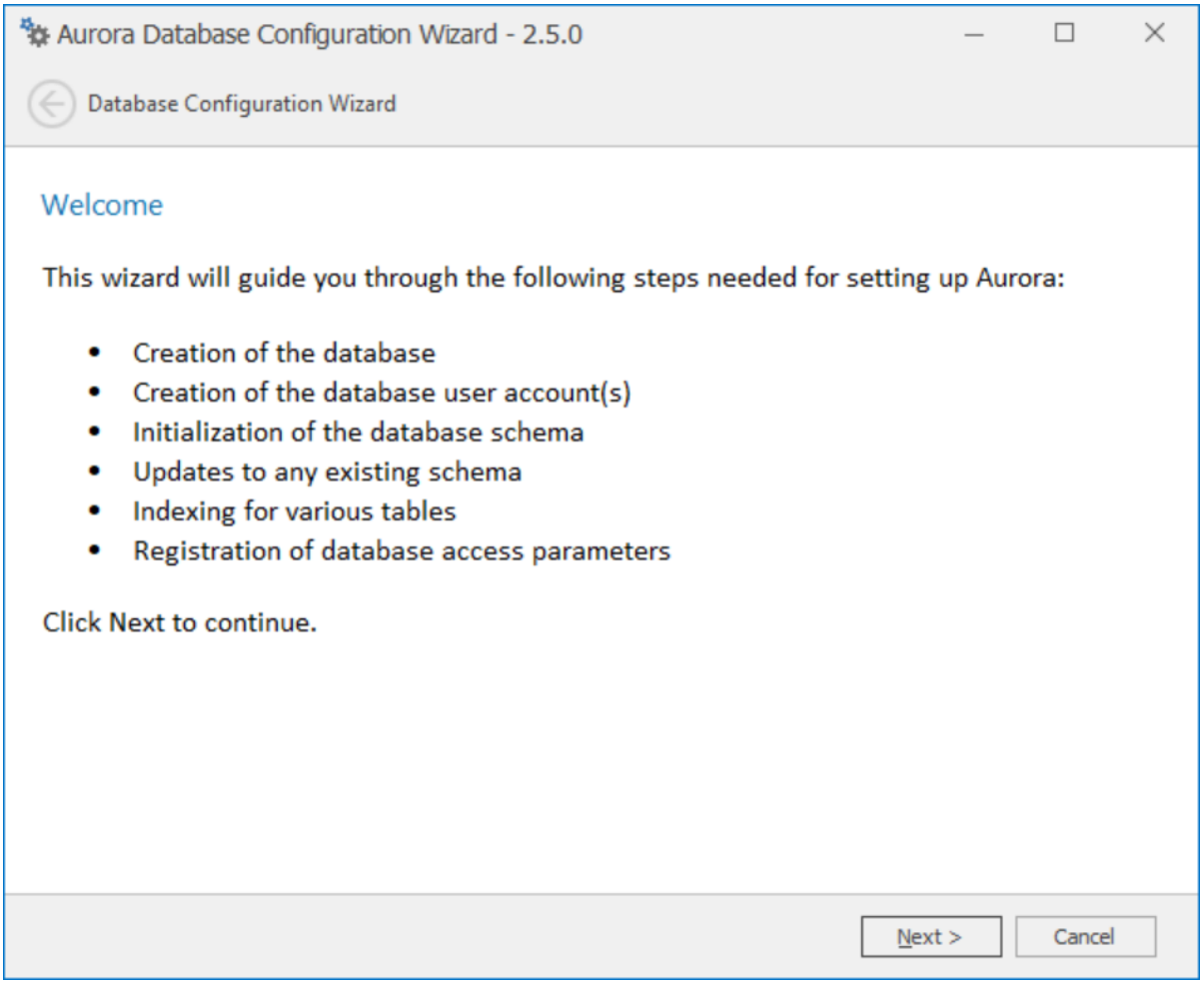
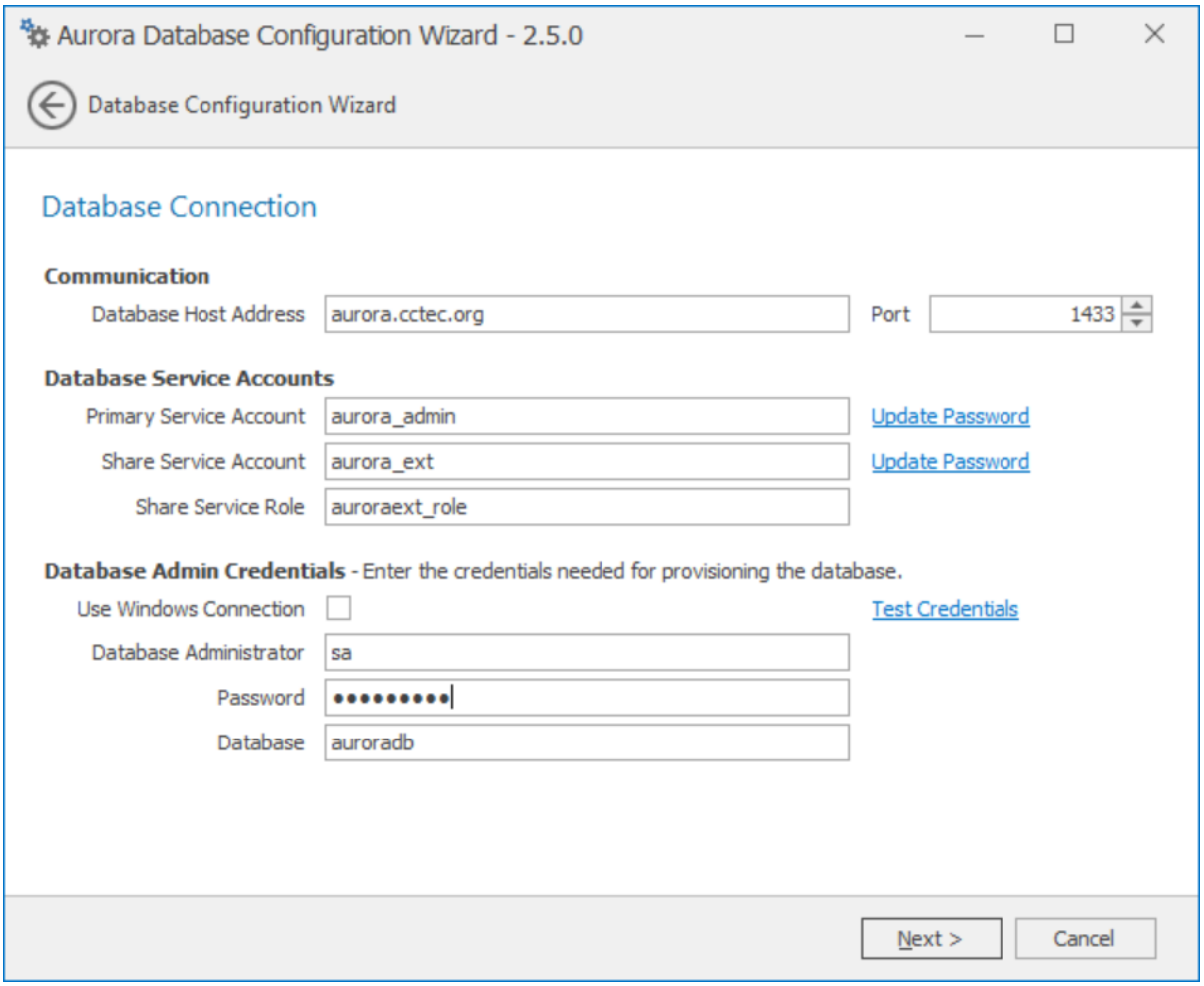


Figure 1 - Configuration Dashboard, launch Database Configuration Wizard

2. Click **Next** to continue.



3. Enter the required fields for the database configuration, then click **Next**.



Overview

Aurora and Aurora. Ext communicate with a single database instance, which may be standalone or part of a high-availability cluster. The Aurora application suite currently requires TCP/IP connectivity to the database, along with SQL Authentication, which makes use of a SQL login and password.

For each application, a SQL credential is defined for both the SQL Server instance as well as a SQL database user account. The configuration utility creates or updates the specified credentials, as well as any database roles, then securely stores the credentials on the local server for use by the Aurora and Aurora. Ext applications.

Communication

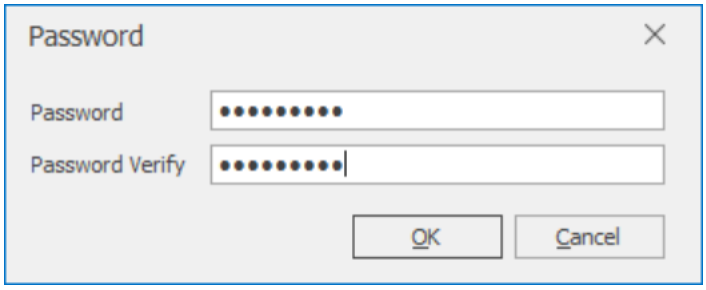
- *Database Host Address* – DNS name or IP address of SQL Server instance
- *Port* – TCP port that the SQL Server instance listens on

Database Service Accounts

- *Aurora Admin Account* – primary database account used by the Aurora service. This field specifies both a SQL Server Login as well as an Aurora database account of the same name.
- *Aurora .Ext Account* – primary database account used by the Aurora .Ext service This field specifies both a SQL Server Login as well as an Aurora database account of the same name.
- *Aurora .Ext Role* – database role used by the Aurora .Ext service for limited access.

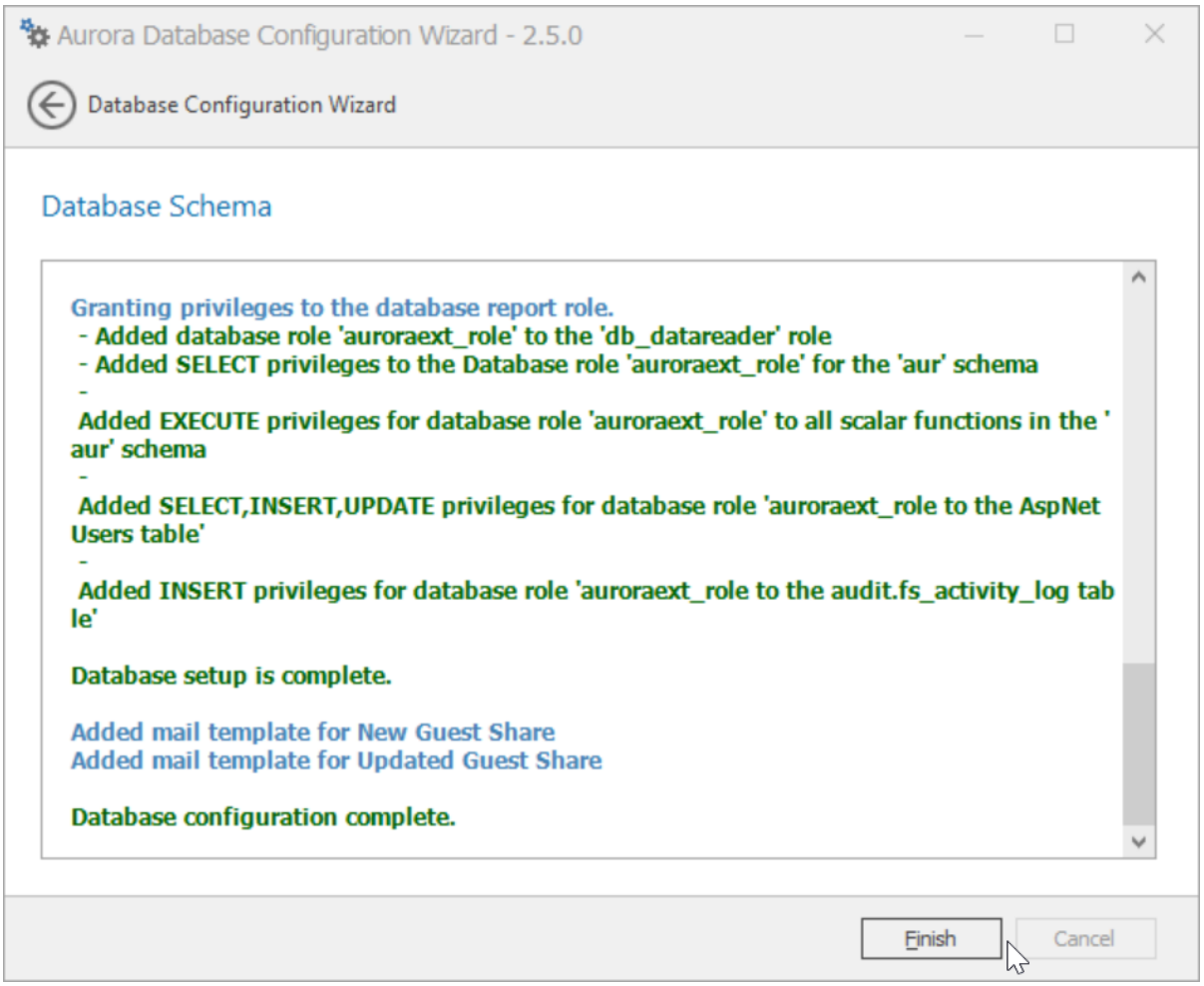
Database Admin Credentials

- *Use Windows Connection* – select this to use the current Windows account you have signed in with to the Windows server
- *Database Administrator* – if *Use Windows Connection* is not selected, enter the name of a SQL Server database administrator account
- *Password* – if *Use Windows Connection* is not selected, enter the password for the *Database Administrator* account
- *Database* – enter the name of the database to create or update for the Aurora application suite
- *Set Password / Update Password* – be sure to set or update the password for both the Aurora and Aurora .Ext database accounts.



- Optionally click *Test Credentials* to verify whether the current Windows Connection or Database Administrator credentials can connect to the specified SQL Server instance.

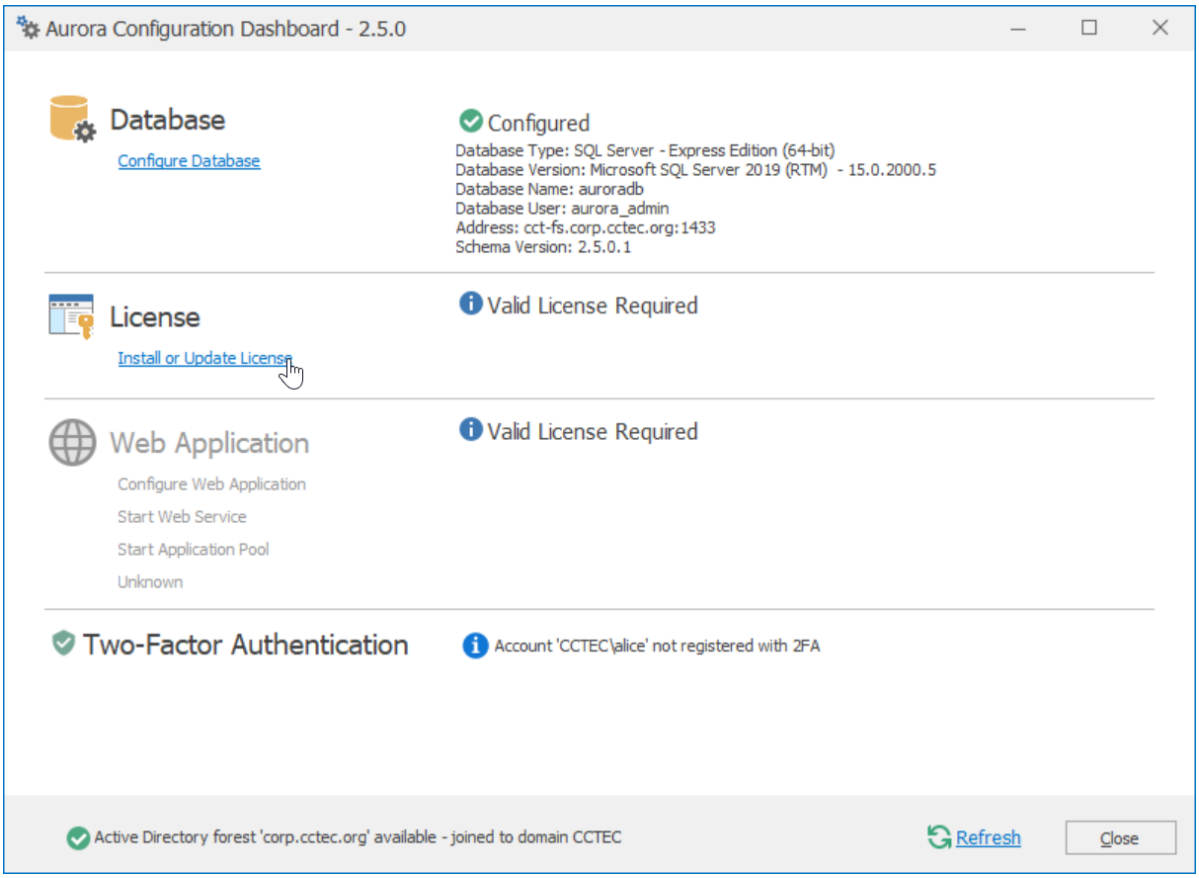
4. Review the database schema and account creation log, then click **Finish** when complete. If any errors are present, you may need to navigate to the previous step by clicking the **Back** arrow at the top of the wizard and re-entering database configuration fields.



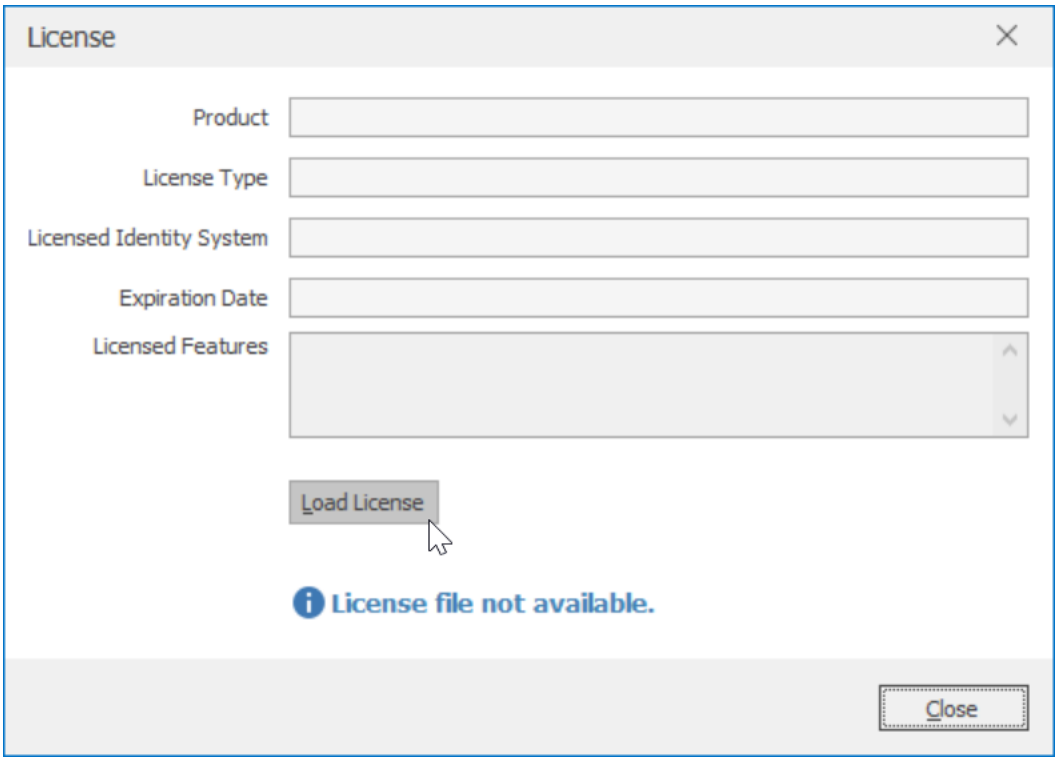
5.2.2 Aurora License Configuration

Once the database configuration is complete, the Aurora Configuration Dashboard enables the License configuration.

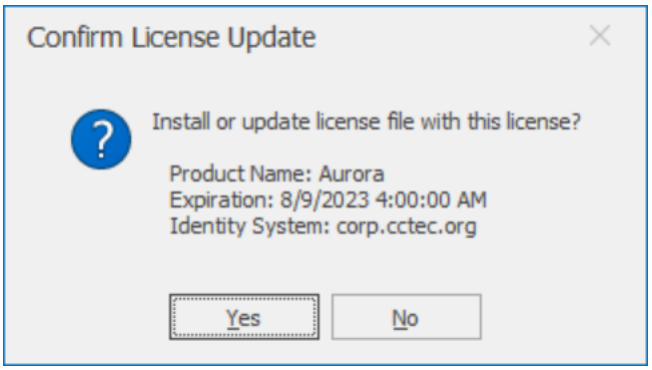
1. Click **Install or Update License** to launch the License wizard.



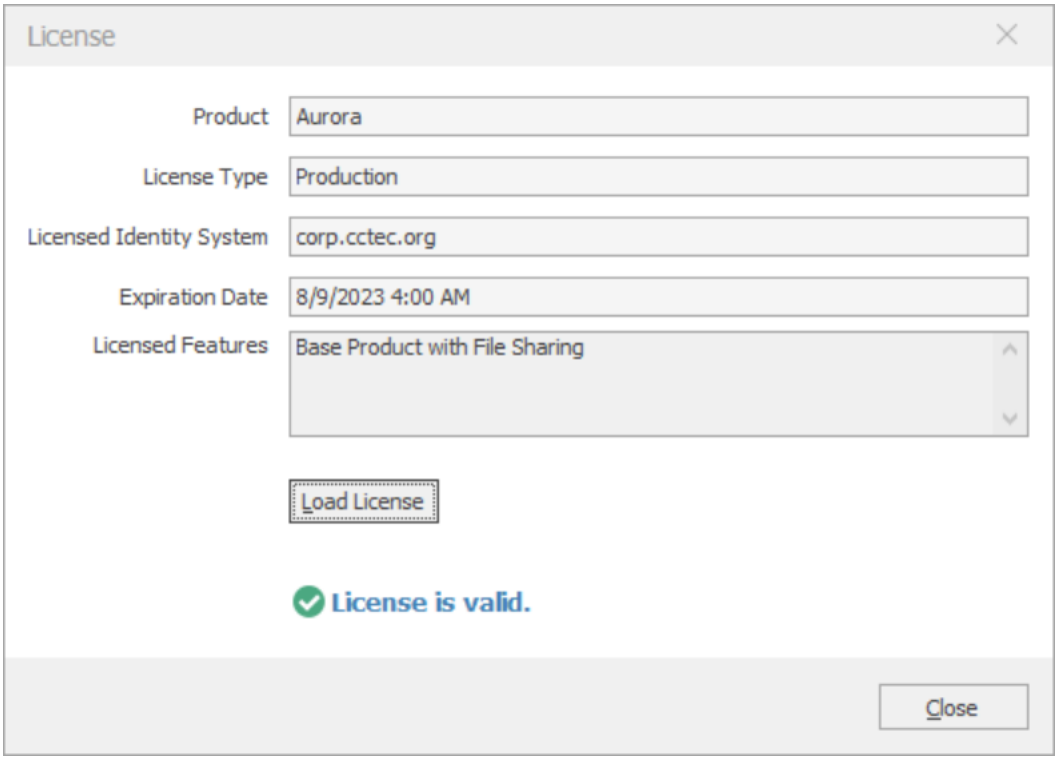
2. Click the **Load License** button.



3. Select the license file and click **Open**.
4. Review the confirmation dialog and click **Yes** to continue. If the selected license does not match the licensed product or Active Directory forest, or has already expired, a warning will appear in the dialog indicating such.



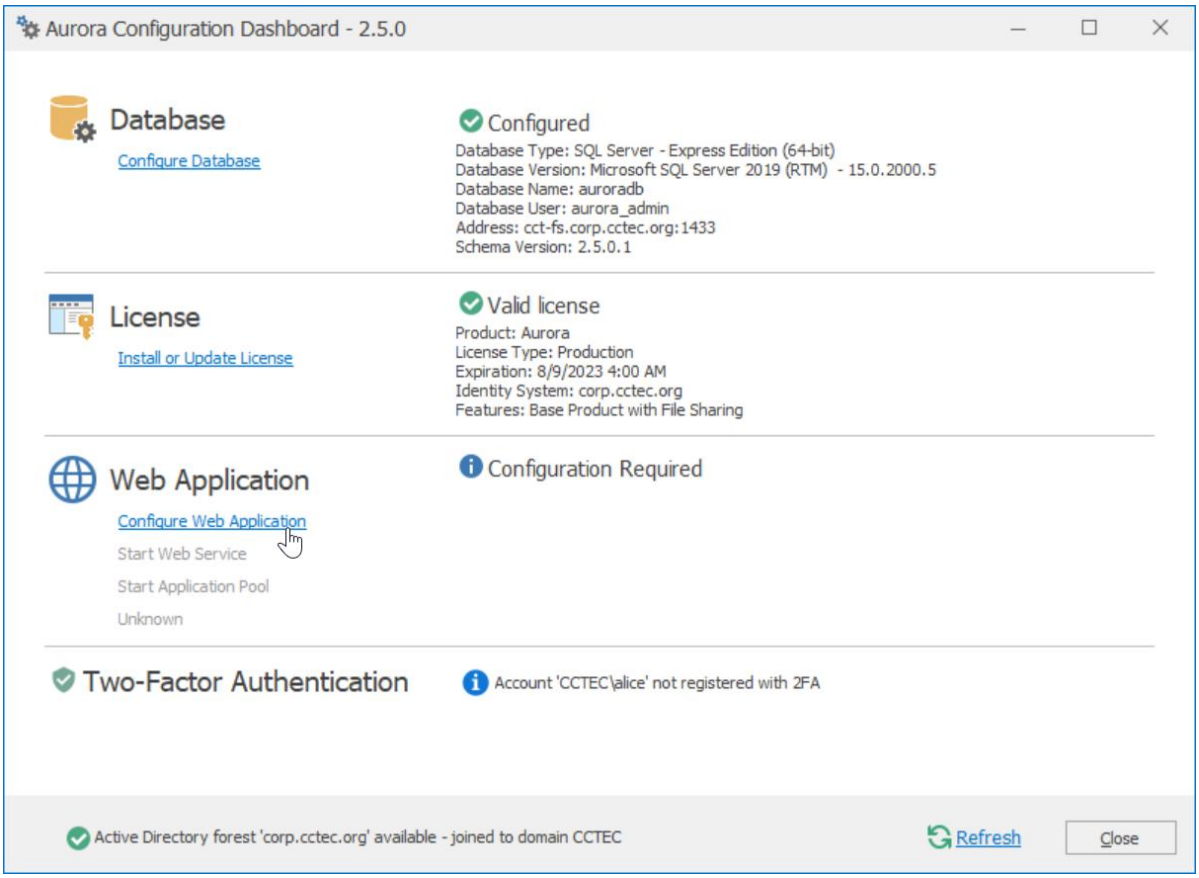
5. Verify the license is Valid, then click **Close**.



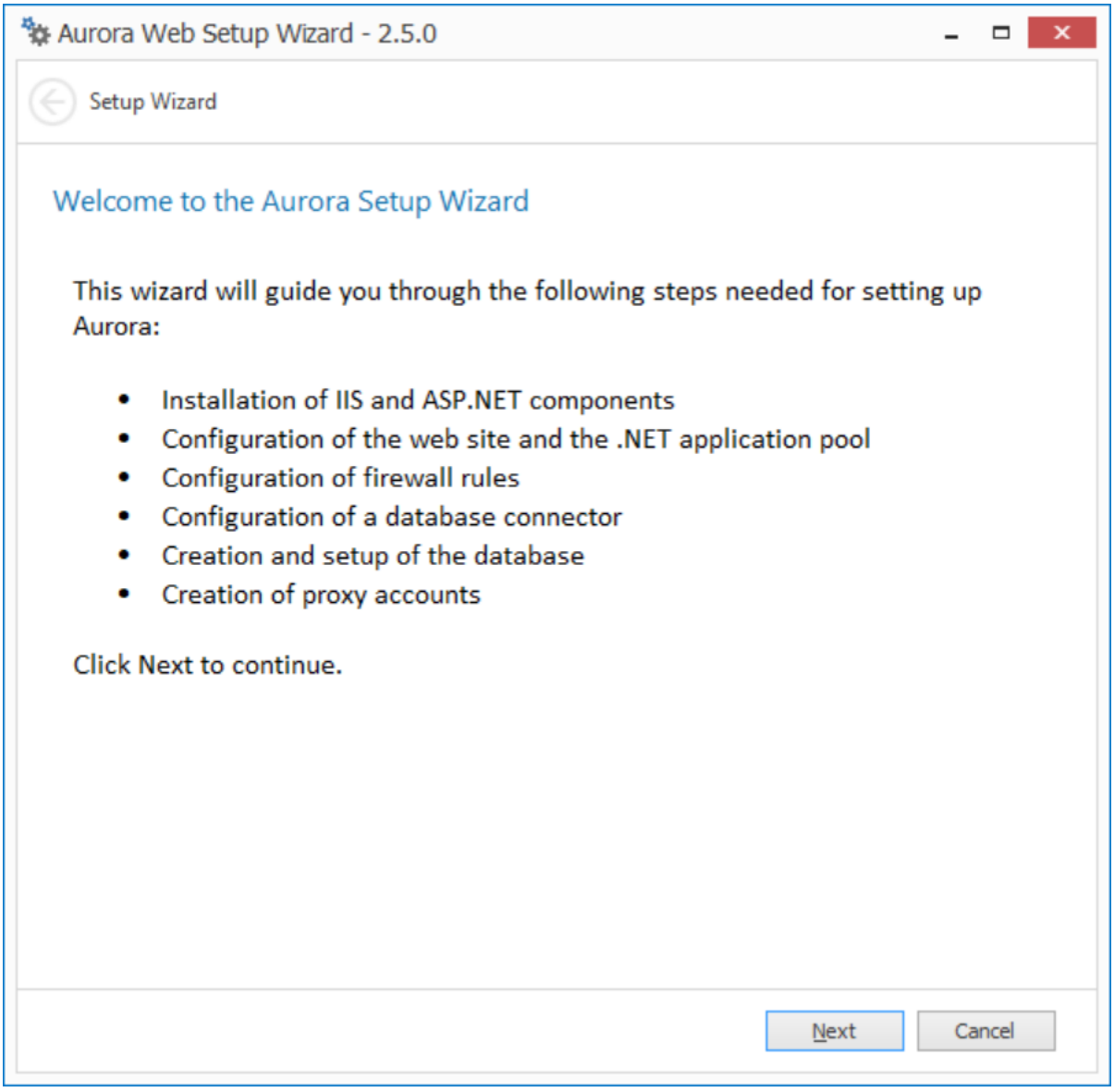
5.2.3 Aurora Web Application Configuration

Once a valid License has been installed, the Web Application configuration is enabled.

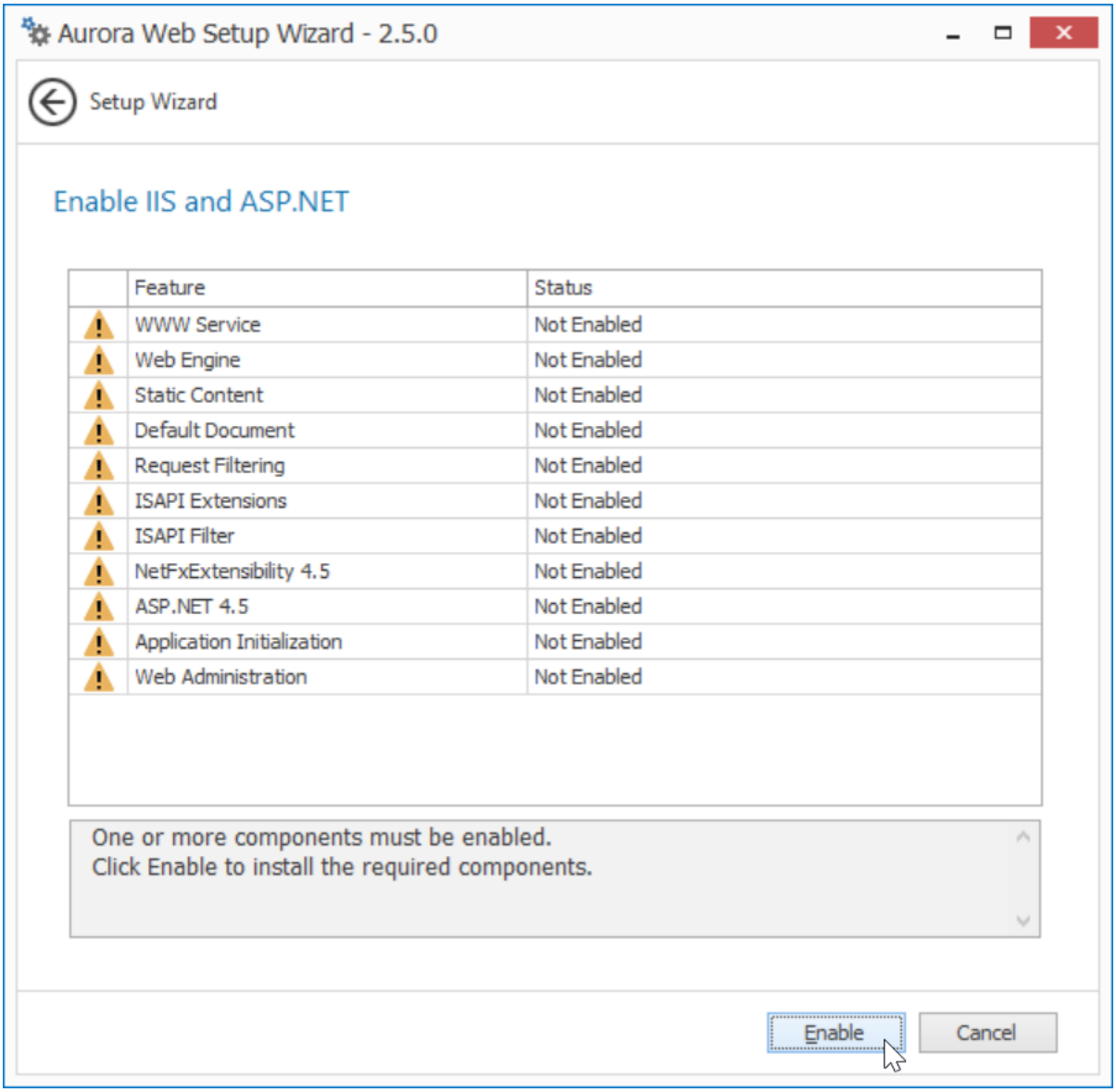
1. Click **Configure Web Application** to launch the Aurora Web Configuration utility.



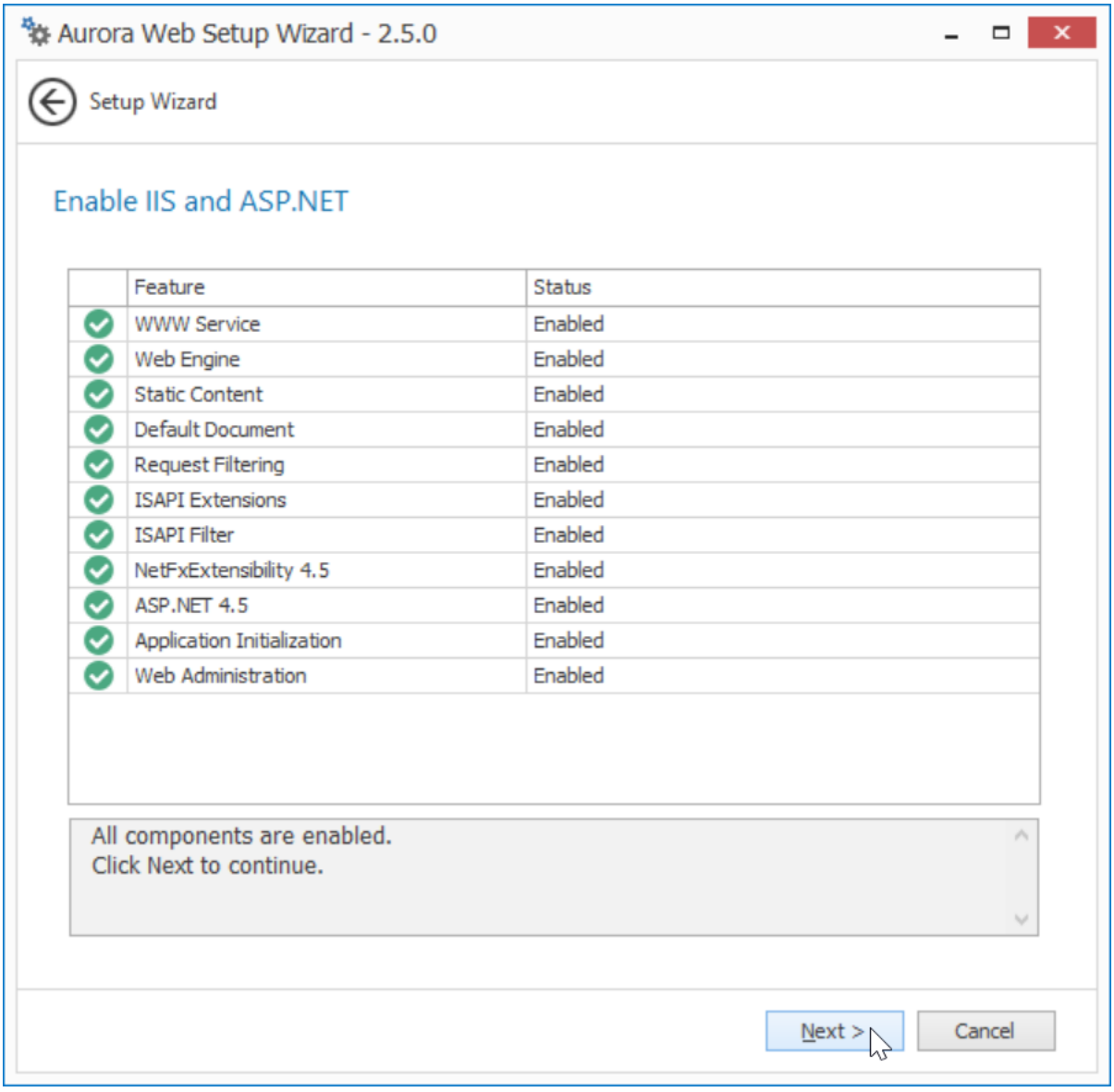
2. Click **Next** to continue



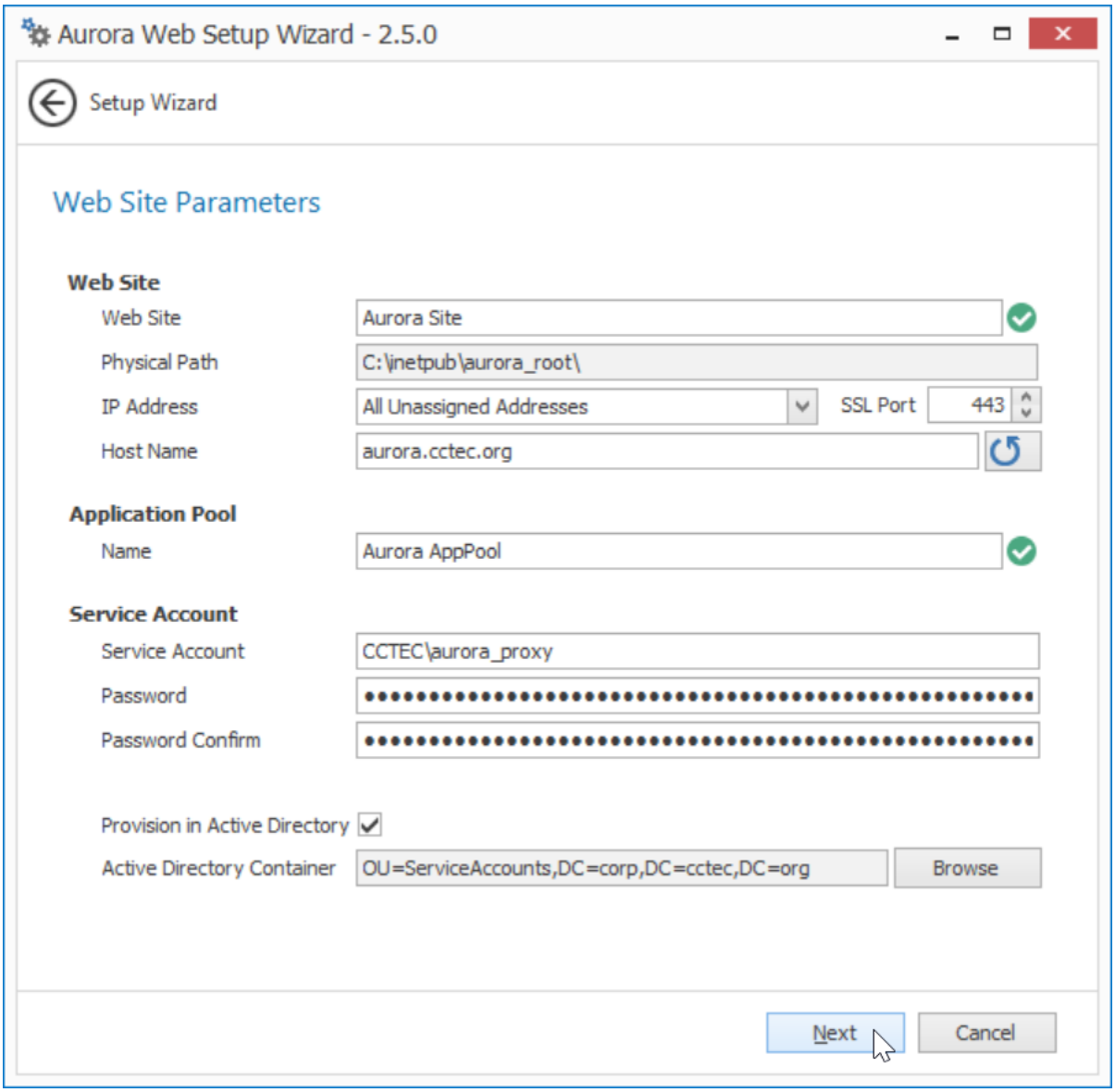
3. If one or more IIS or ASP.NET components are not yet enabled, click **Enable** to install them from the system image.



4. Once all required IIS and ASP.NET components have been installed, click **Next**.



5. Enter the Web Site parameters, then click **Next**.



The **Web Site Parameters** page specifies the details of the ASP.NET Web Site, Application Pool, and credentials that the Application Pool will run under.

Web Site

- *Web Site* – Specify a site name unique to this server
- *Physical Path* – this displays the current path where the Aurora web files were placed during the install
- *IP Address* – select either **All Unassigned Addresses** to use all available addresses or select one of the IPv4 addresses from the drop-down list.

- *Host Name* – specify the DNS name used for accessing the Aurora web application. This name must be used when accessing the service, as the configuration makes use of virtual server addressing.



If the specified *Host Name* cannot be resolved by the local server, a warning icon  will appear with a tooltip indicating such. Issues can include missing DNS definition, or multiple addresses resolved, with one or more addresses not configured on the local server. Please correct any DNS naming issues, then click the refresh button  to verify proper name resolution.

Application Pool

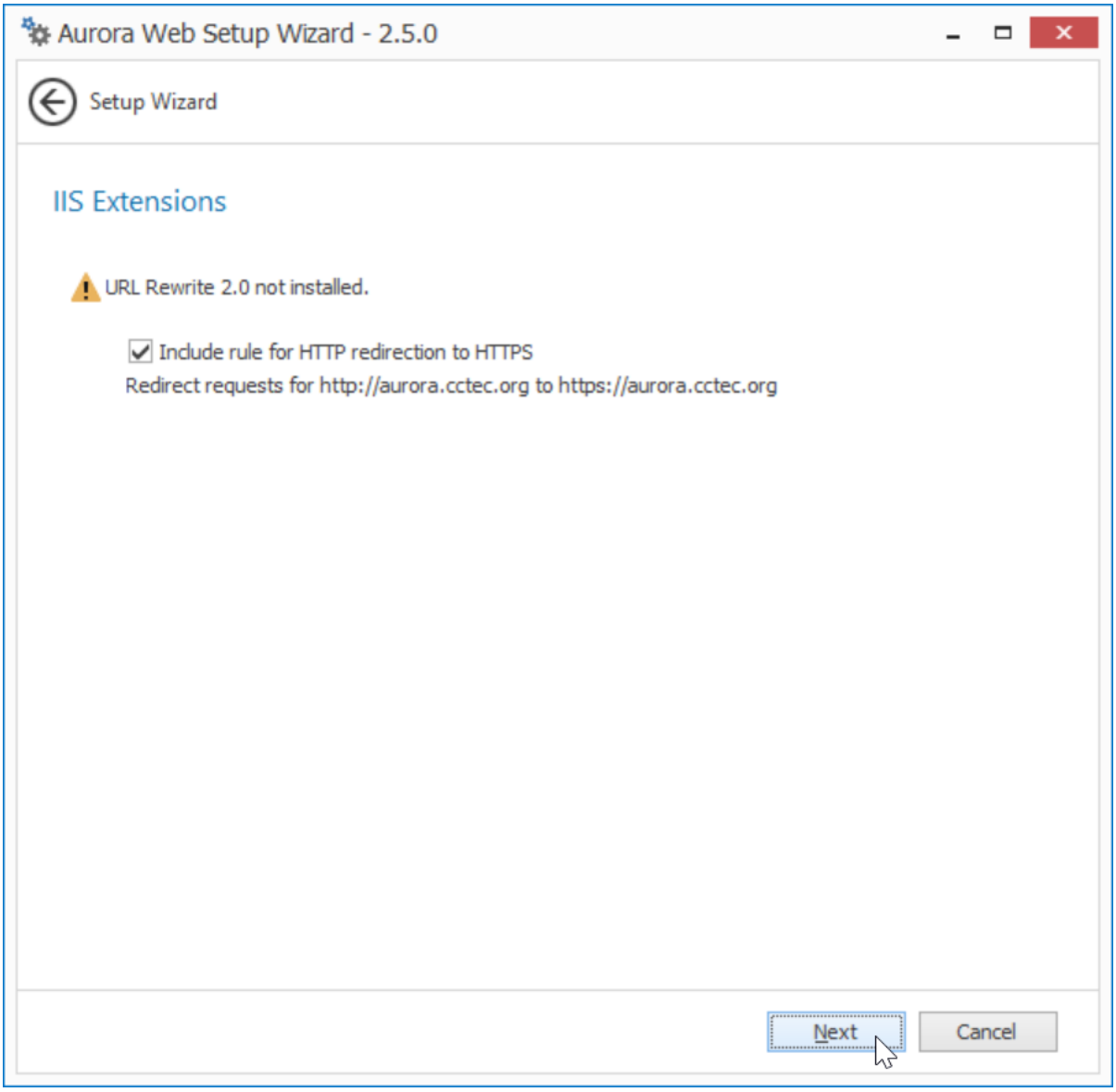
- *Name* – unique name of the Application Pool to setup for this application. Note that this Application Pool should be exclusively used with this application, and not shared with other applications or sites.

Service Account

- *Service Account* – an Active Directory user account for use exclusively with this Application Pool. Note that the account must exist in the same domain as the server. A strong random password is generated for this account, so only the account name is required here.
- *Password / Password Confirm* – by default, a random password is generated, however this can be replaced with an admin-provided password.
- *New Accounts Container* – a container in Active Directory where the service account will be created if it is a new account. Note that existing accounts will only be modified but not moved to this location.
- *Provision Accounts in Active Directory* – If selected, the account information provided will be used to create a new account or modify an existing account in Active Directory. If unselected, the information provided will be used for the Aurora Web Application configuration but will not create or modify an Active Directory account.

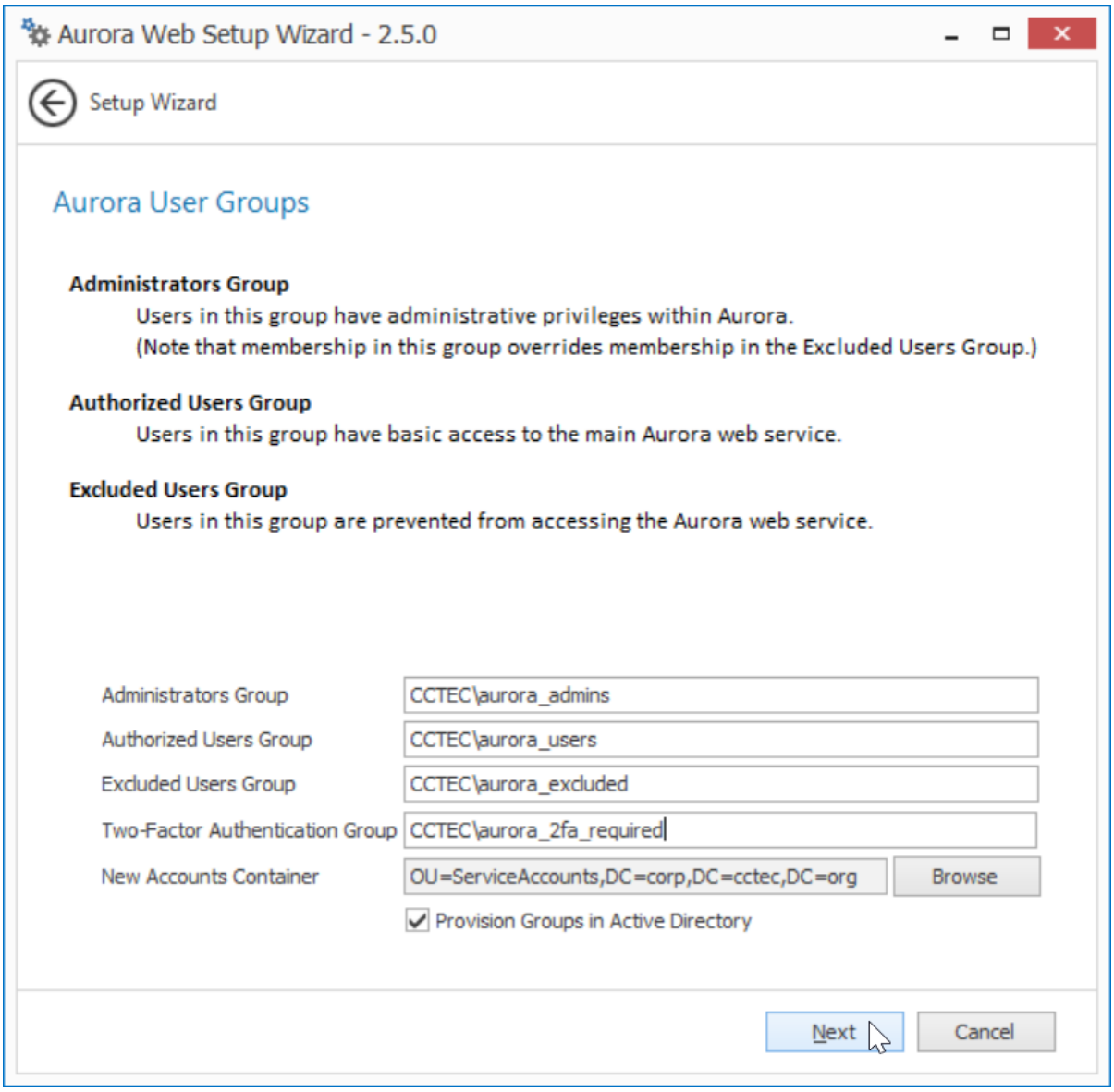
The *New Accounts Container* and *Provision Accounts in Active Directory* options are useful in scenarios where delegated administration is in place. In these cases, select the container where the administrator has been delegated management permissions, or optionally have an administrator create the accounts beforehand, and uncheck the *Provision Accounts in Active Directory* checkbox.

6. Click **Next** to install or update the **URL Rewrite 2.0** IIS module.



This step also adds rewrite rules into the Aurora application that redirect calls for the unsecured site to the SSL/TLS secured address.

7. Enter the required group names then click **Next**.



- *Administrators Group* –domain local group that determines who may perform administrative actions in Aurora
- *Authorized Users Group* - domain local group that determines who may use Aurora
- *Excluded Users Group* – optional domain local group specifying who may not use Aurora
- *Two-Factor Authenticatoin Group* – optional domain local group specifying which users are required to authentication using two-factor authentication

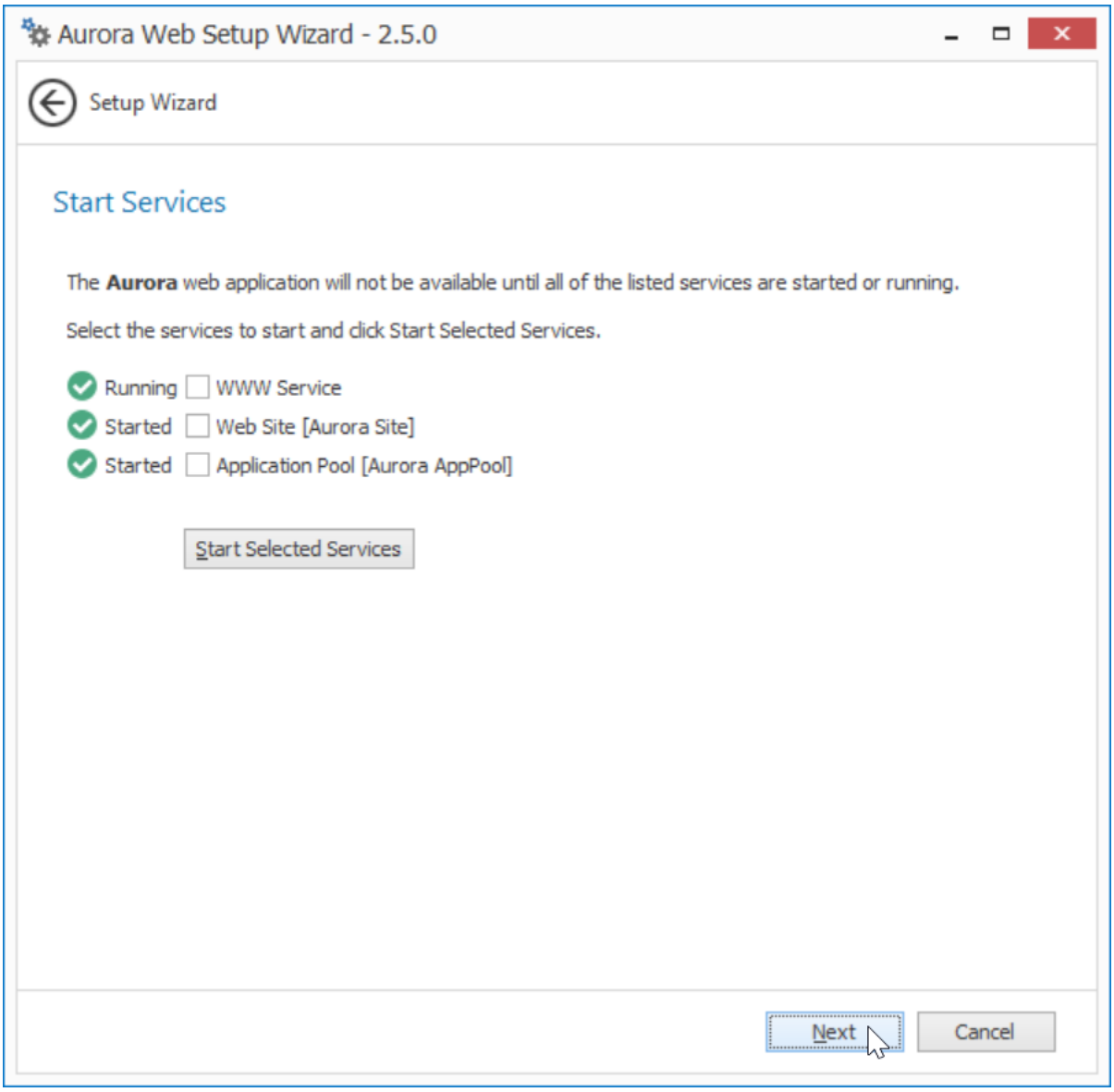
- *New Accounts Container* - a container in Active Directory where the groups will be placed, if they are new groups. Note that existing groups will only be modified, but not moved to this location.
- *Provision Accounts in Active Directory* – If selected, the account information provided will be used to create new groups or modify existing groups in Active Directory. If unselected, the information provided will be used for the Aurora Web Application configuration, but will not create or modify any Active Directory groups.

The *Excluded Users Group* is optional, and is not required. This group is primarily for excluding users that may be in the *Authorized Users Group**,*** but should not have access or be counted against the licensed user count.

The currently signed-in Windows user is automatically added to the *Administrators Group* allowing the current user to become an Aurora administrator.

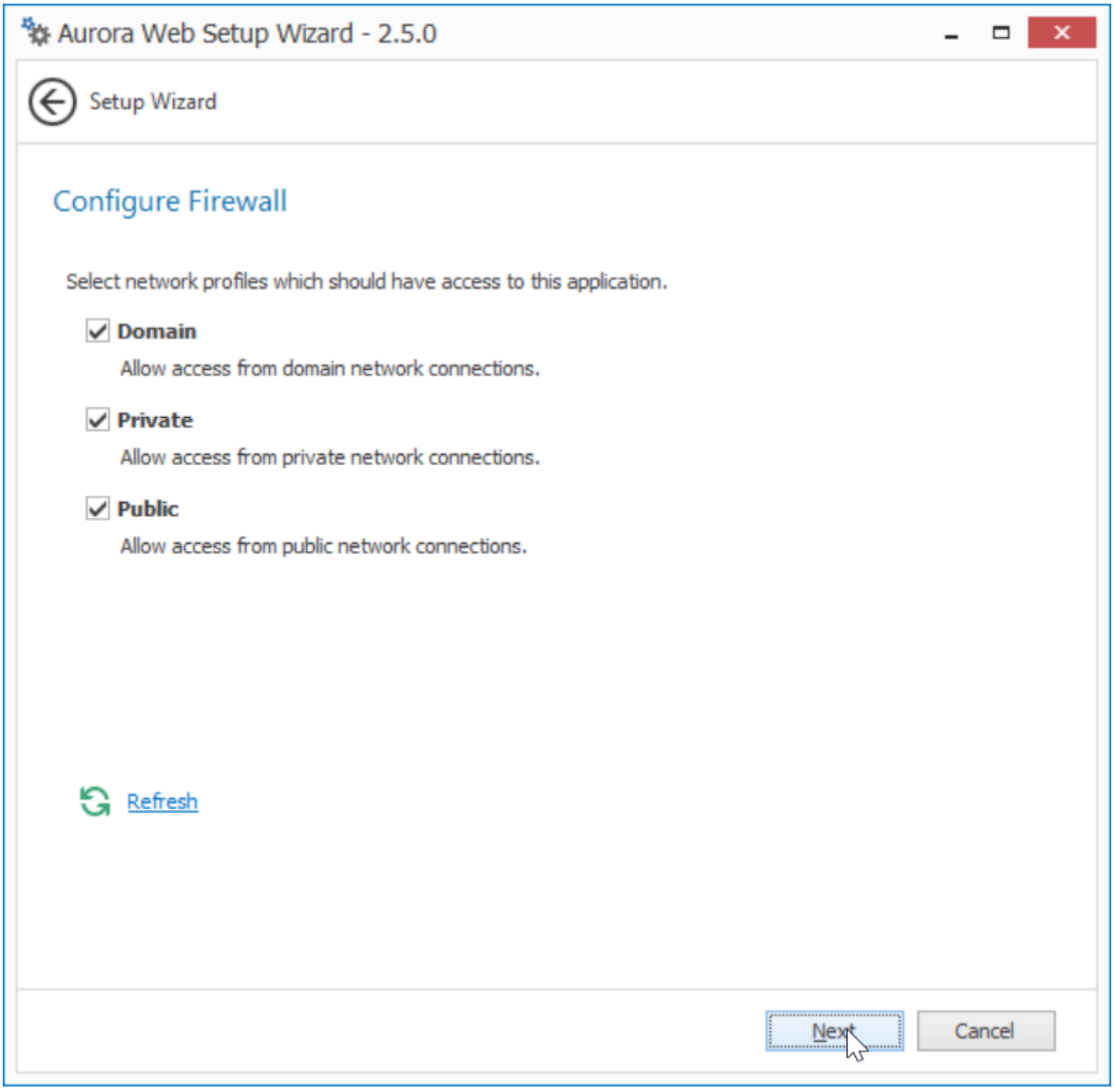
The *New Accounts Container* and *Provision Accounts in Active Directory* options are useful in scenarios where delegated administration is in place. In these cases, select the container where the administrator has been delegated management permissions, or optionally have an administrator create the accounts beforehand, and uncheck the *Provision Accounts in Active Directory* checkbox.

8. [Optional] Click **Start Selected Services**, then click **Next**.

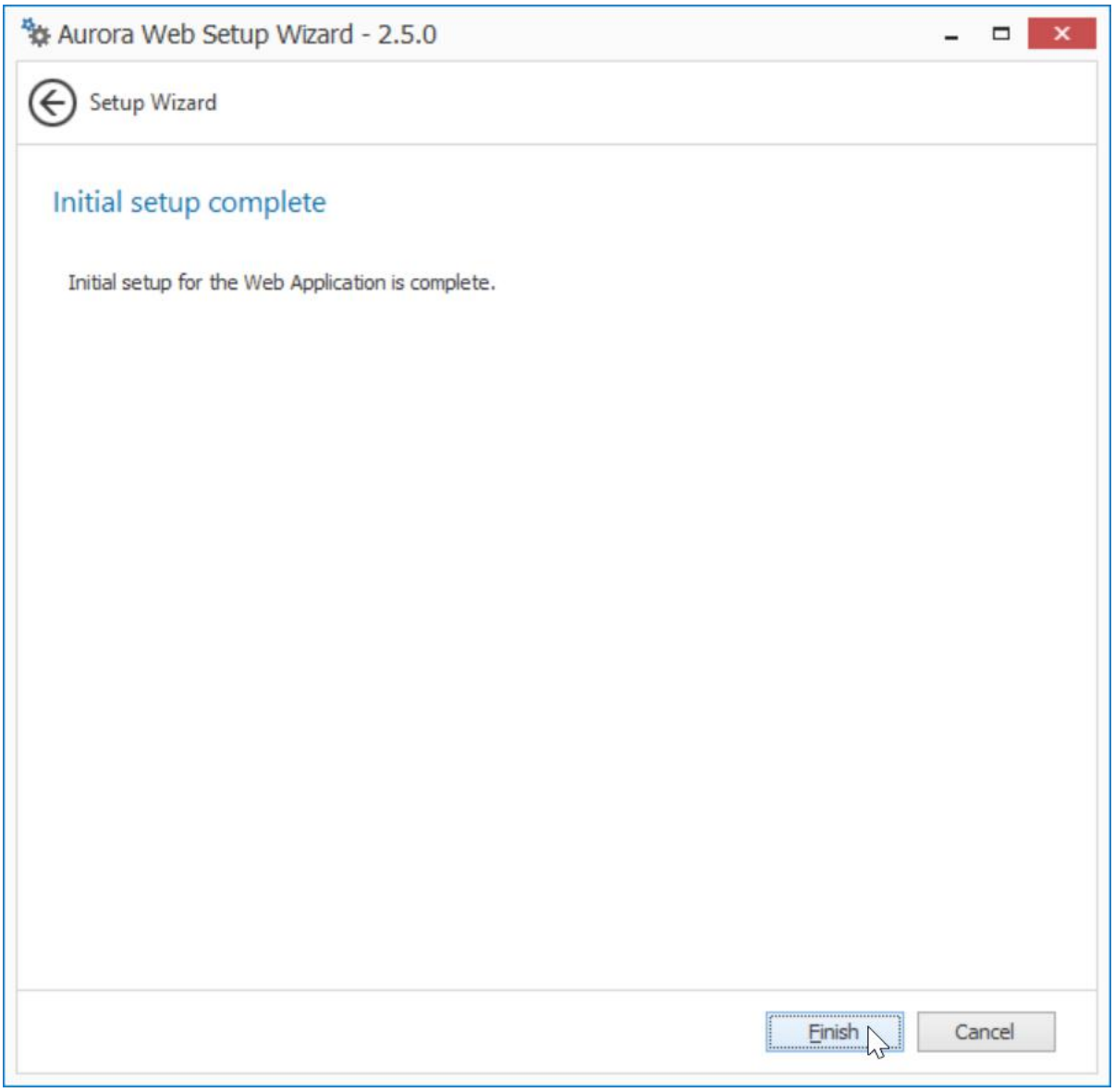


The **Start Services** page will only be displayed if one or more of the required services are not running. Simply start the services using the provided interface, then click **Next** to continue.

9. Click **Next** to accept the default Windows Firewall rules.



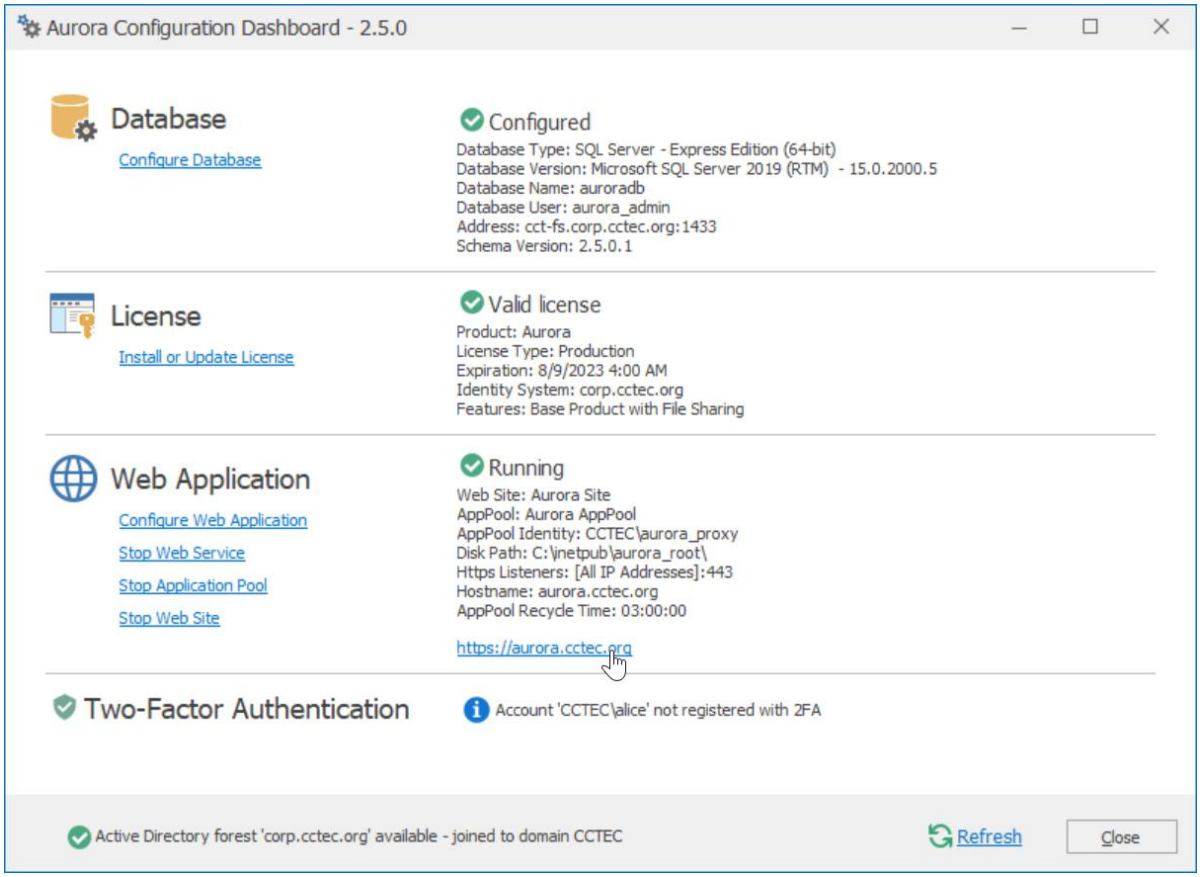
10. Click **Finish** to complete the Aurora Web Configuration wizard.



5.2.4 Complete the Dashboard Configuration

Once the Database, License, and Web Configuration wizards are complete, the target URL for the Aurora application is displayed at the bottom of the **Web Application** details panel.

Copy the URL into a web browser, or simply click the link to launch the default web browser with the configured URL.



At this point, the Aurora web application is initially configured and ready for access by an Administrator account.

To continue with configuration of Aurora for end-user access, please refer to the Aurora Administration Guide included with this product.

5.2.5 Reset Two-Factor Authentication

This option provides a means for resetting a lost or corrupt two-factor authentication registration for an Aurora administrator. For details on when and how to use this option, see *Appendix B – Troubleshooting Two-Factor Authentication* in the *Aurora 2.5 Administration Guide*.

6 Installing the Aurora .Ext Web Application

The Aurora .Ext web application provides access for external guests via a separate web portal.

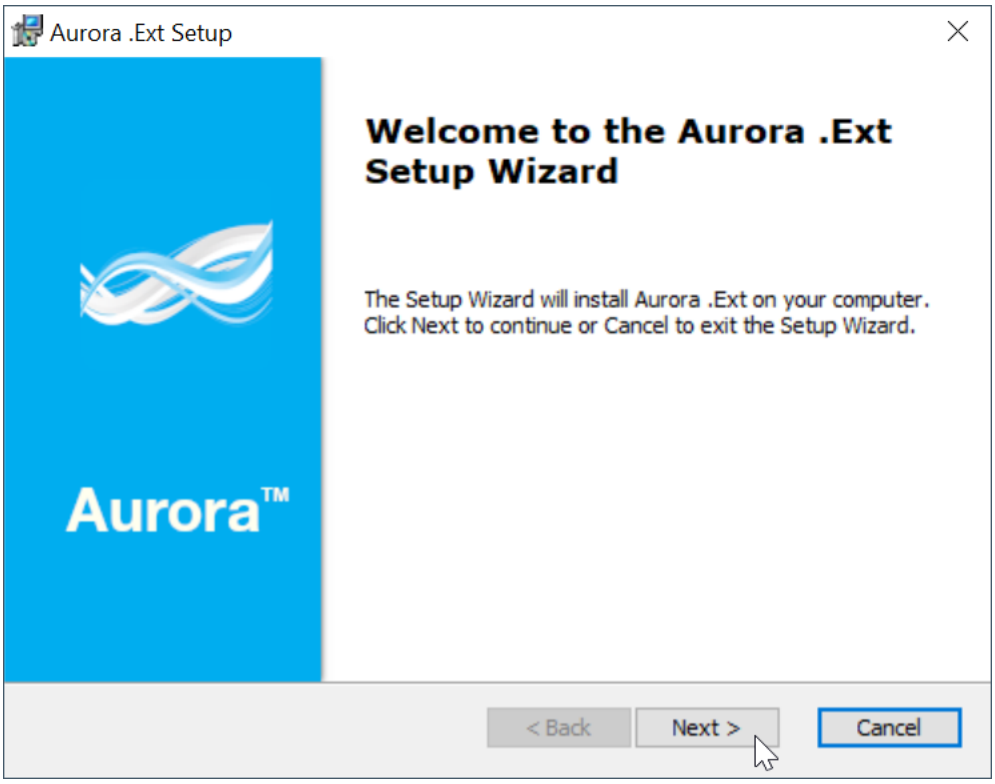
This application may be installed on the same server as the Aurora web application or on a separate server altogether.

6.1 Installing the Aurora .Ext Package

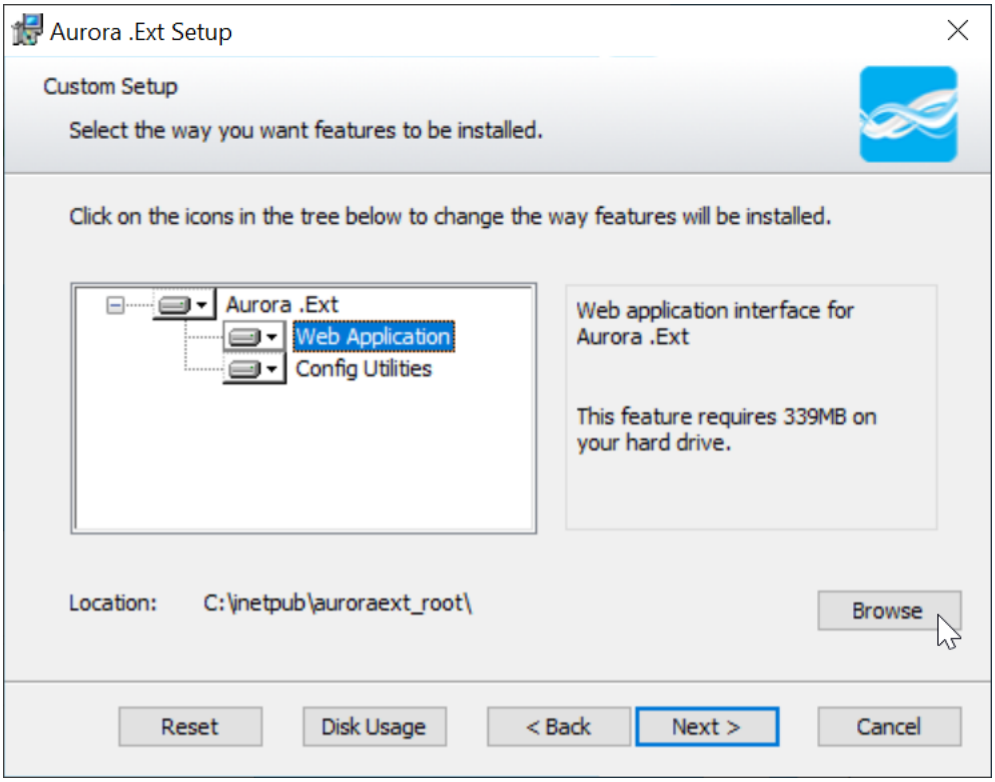
1. Before starting, be sure that you are signed into the target server with an Active Directory account that has the following privileges:
    - Full access to install software on the local server
    - Access to create or modify Active Directory users and security groups in the server's current domain
2. Copy the provided Aurora installer package **Aurora.Ext-Installer-2.5.0-x64-xx.exe** to the server where Aurora .Ext will be installed.
3. Double-click or run the installer package to start the installation process.
4. Review the license, select the license agreement check box, then click **Install**.



5. Click **Next** to continue.



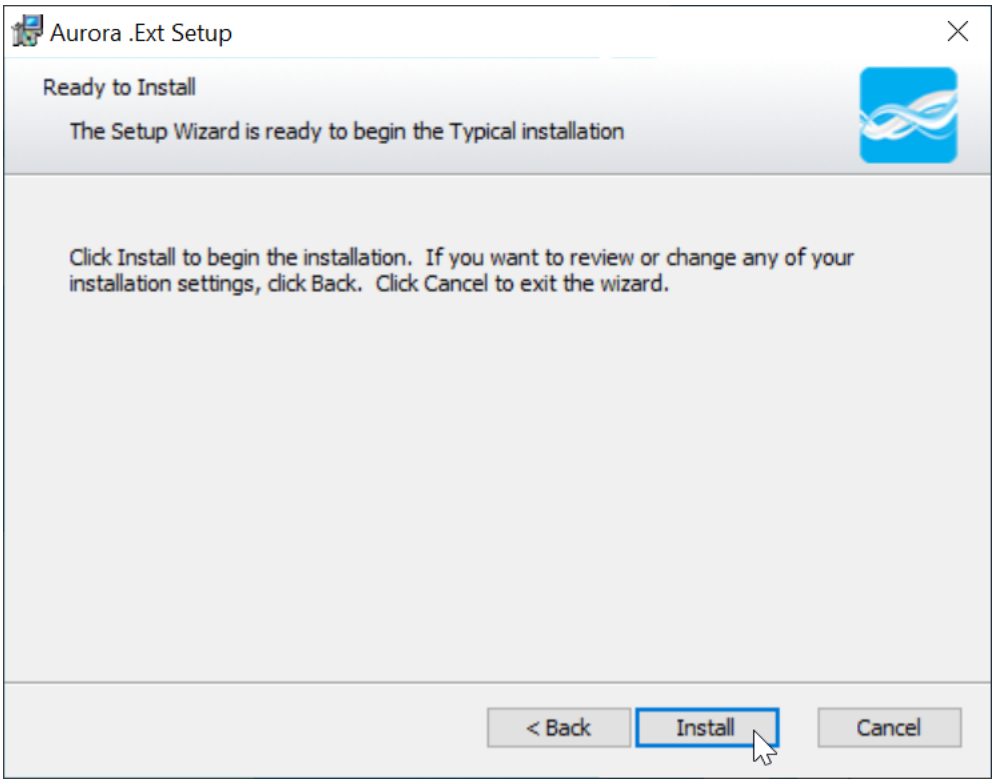
6. Review the locations where the software components will be installed.



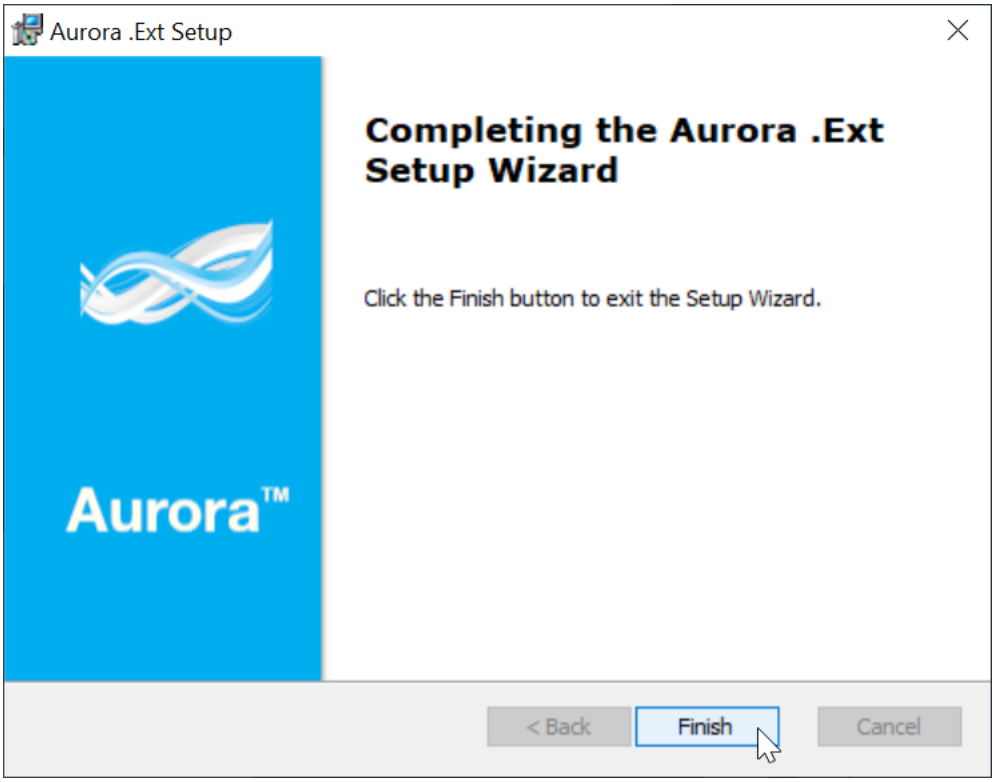
The **Web Application** feature contains the ASP.NET files that will be served by IIS. By default, this in placed on the system drive in the default location for IIS web files, but the location may be directed to a separate disk if desired.

The **Config Utilities** feature contains the initial configuration dashboard and utilities for setting up the Aurora .Ext web application.

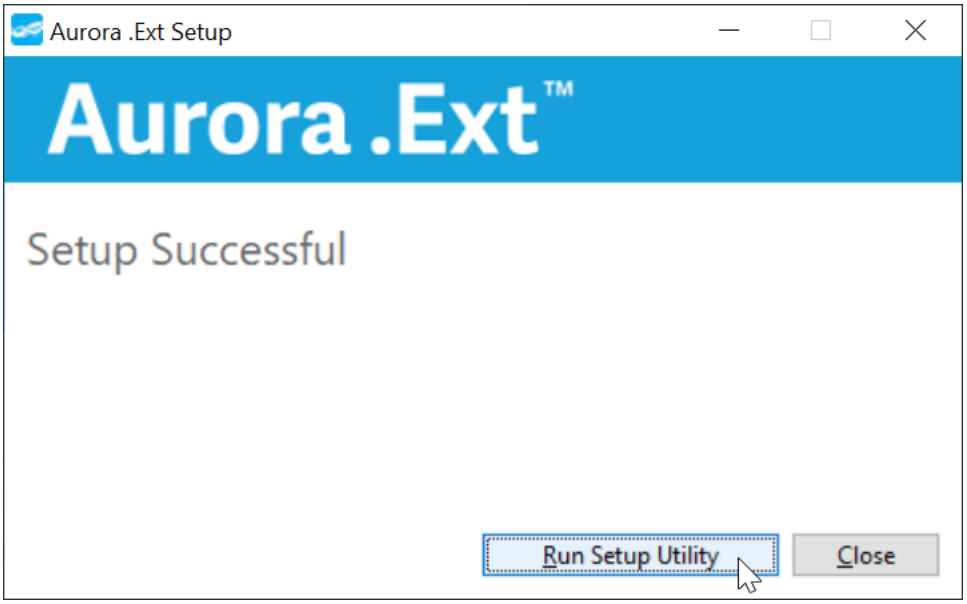
7. Click **Install** to perform the installation.



8. Click **Finish** to complete the installation.



9. Click **Run Setup Utility** to close the installer and launch the Aurora .Ext Configuration.



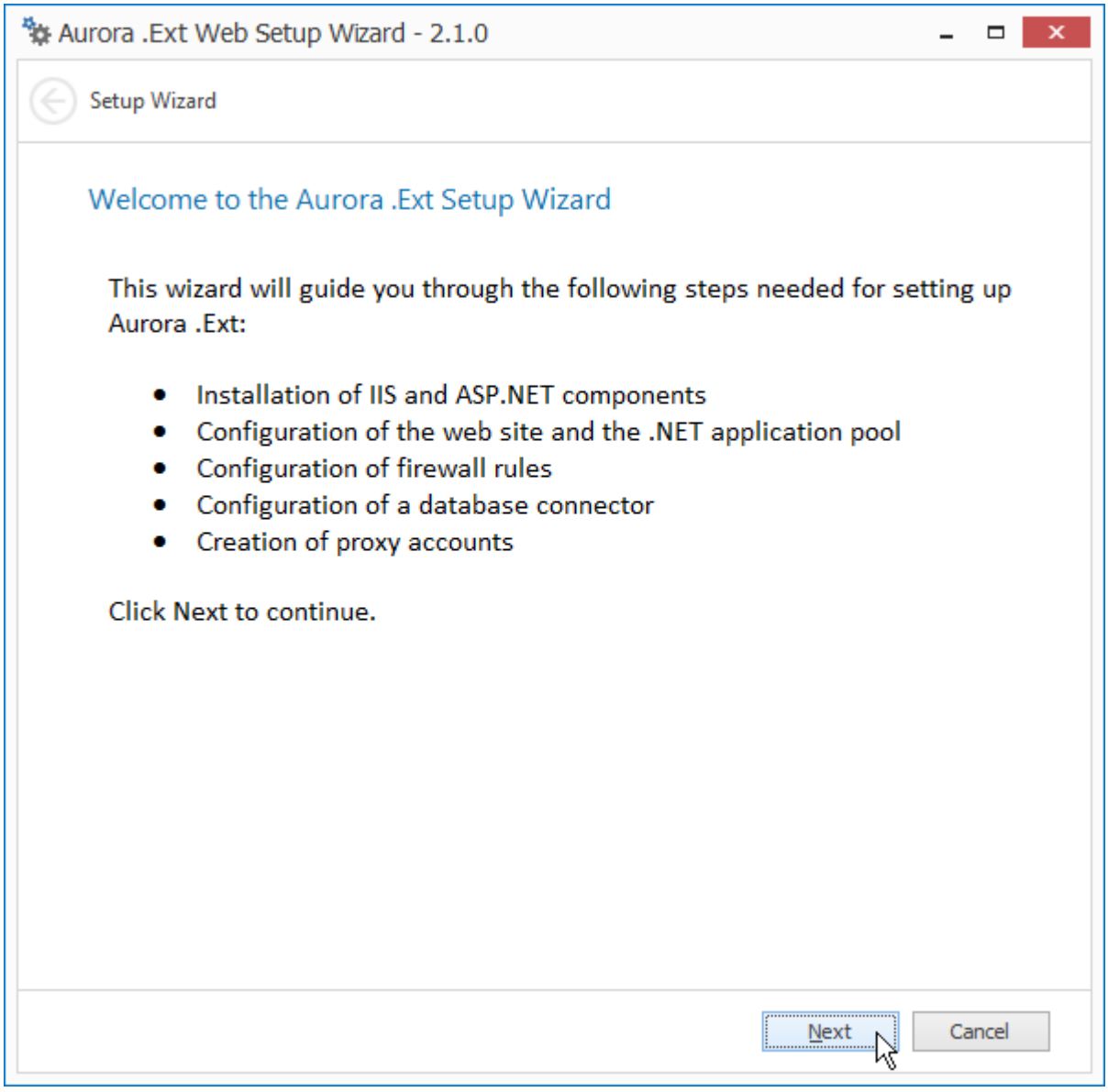
If the required .NET Framework was installed as part of this process, a system reboot will be required before the Aurora .Ext Configuration utility can run. Please reboot the system, then launch the Aurora .Ext Configuration utility via the Start Menu as mentioned in the next step.

6.2 Running Aurora .Ext Configuration

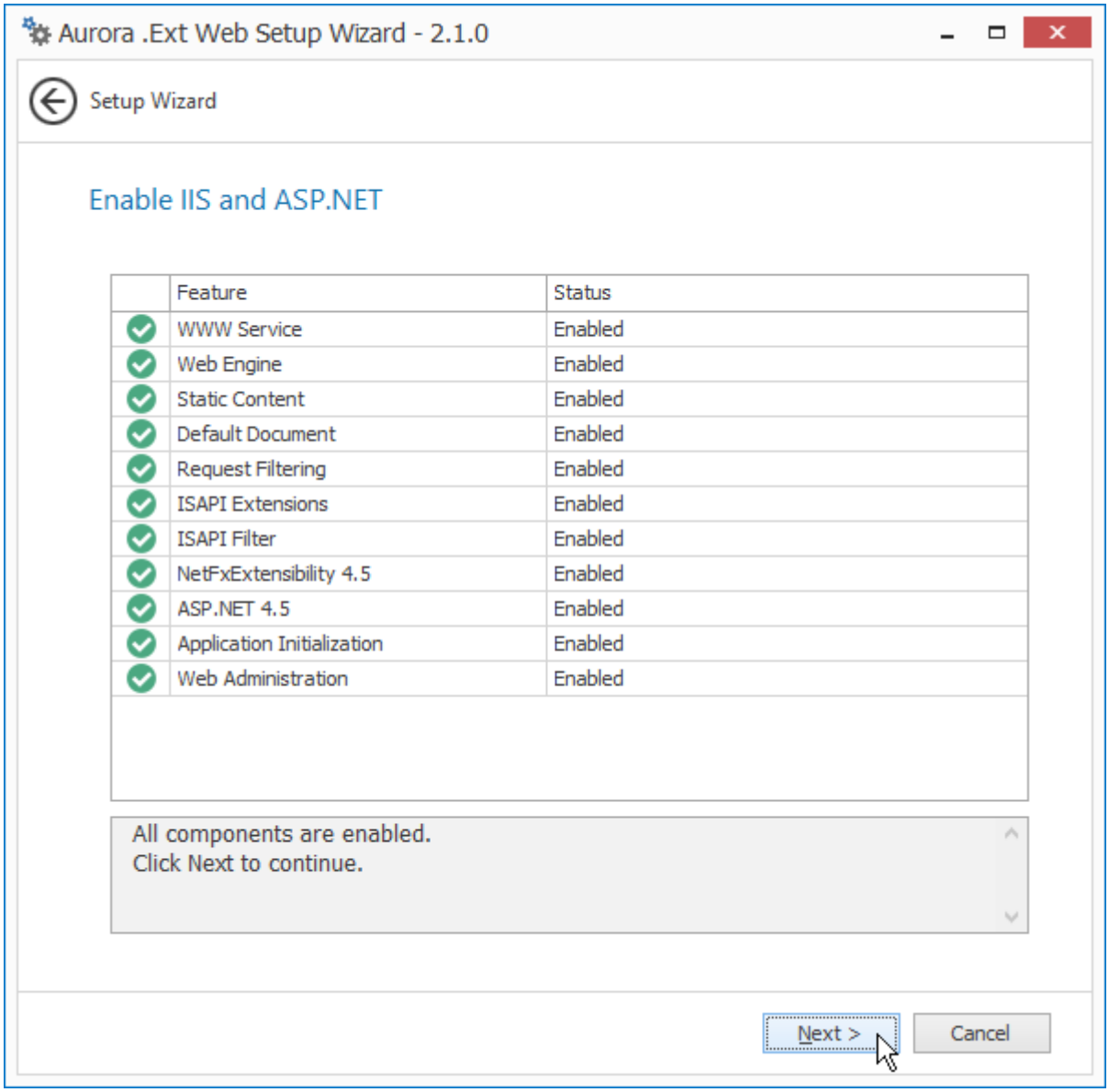
The **Aurora .Ext Configuration** utility is automatically launched at the end of the installation process if the **Launch config utility** checkbox was selected.

If the **Launch config utility** checkbox was not selected, or if you need to run the Aurora .Ext Configuration utility again, simply launch the utility from the **Windows Start Menu > Condrey Corporation > Aurora .Ext Configuration** start menu entry.

1. At the Welcome screen, click **Next** to continue.

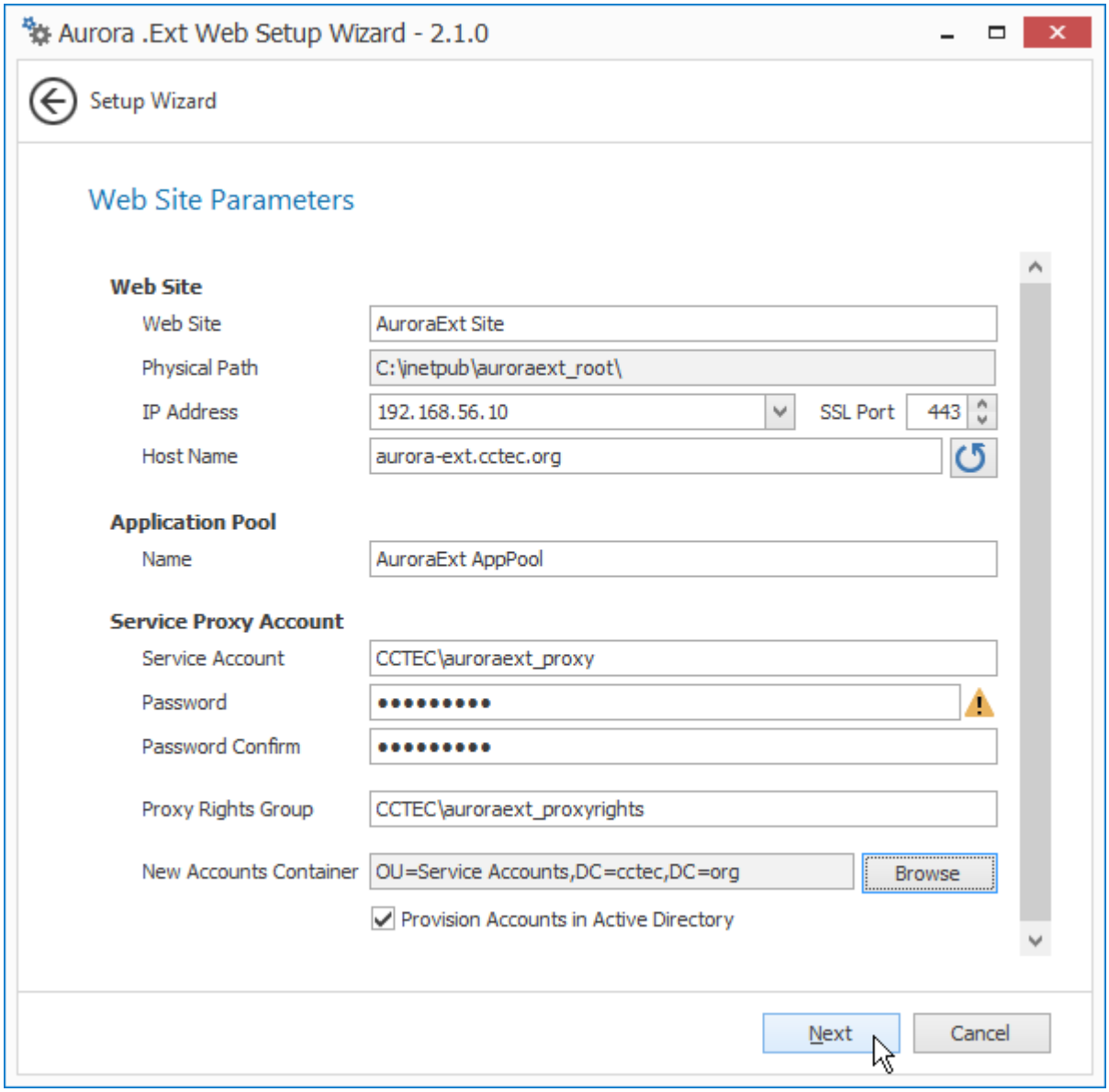


2. If one or more IIS or ASP.NET components are not yet enabled, click **Enable** to install them from the system image.



Once all required IIS and ASP.NET components have been enabled, click **Next** to continue.

3. Enter the required Web Site parameters



The **Web Site Parameters** page specifies the details of the ASP.NET Web Site, Application Pool.

Web Site

- *Web Site* – Specify a site name unique to this server
- *Physical Path* – this displays the current path where the Aurora web files were placed during the install
- *IP Address* – select either **All Unassigned Addresses** to use all available addresses, or select one of the IPv4 addresses from the drop-down list.

- *Host Name* – specify the DNS name used for accessing the Aurora web application. This name must be used when accessing the service, as the configuration makes use of virtual server addressing.

If the specified *Host Name* cannot be resolved by the local server, a warning icon will appear with a tooltip indicating such. Issues can include missing DNS definition, or multiple addresses resolved, with one or more addresses not present on the local server. Please correct any DNS naming issues, then click the refresh button to verify proper name resolution.

Application Pool

- *Name* – unique name of the Application Pool to setup for this application. Note that this Application Pool should be exclusively used with this application, and not shared with other applications or sites.

Service Proxy Account

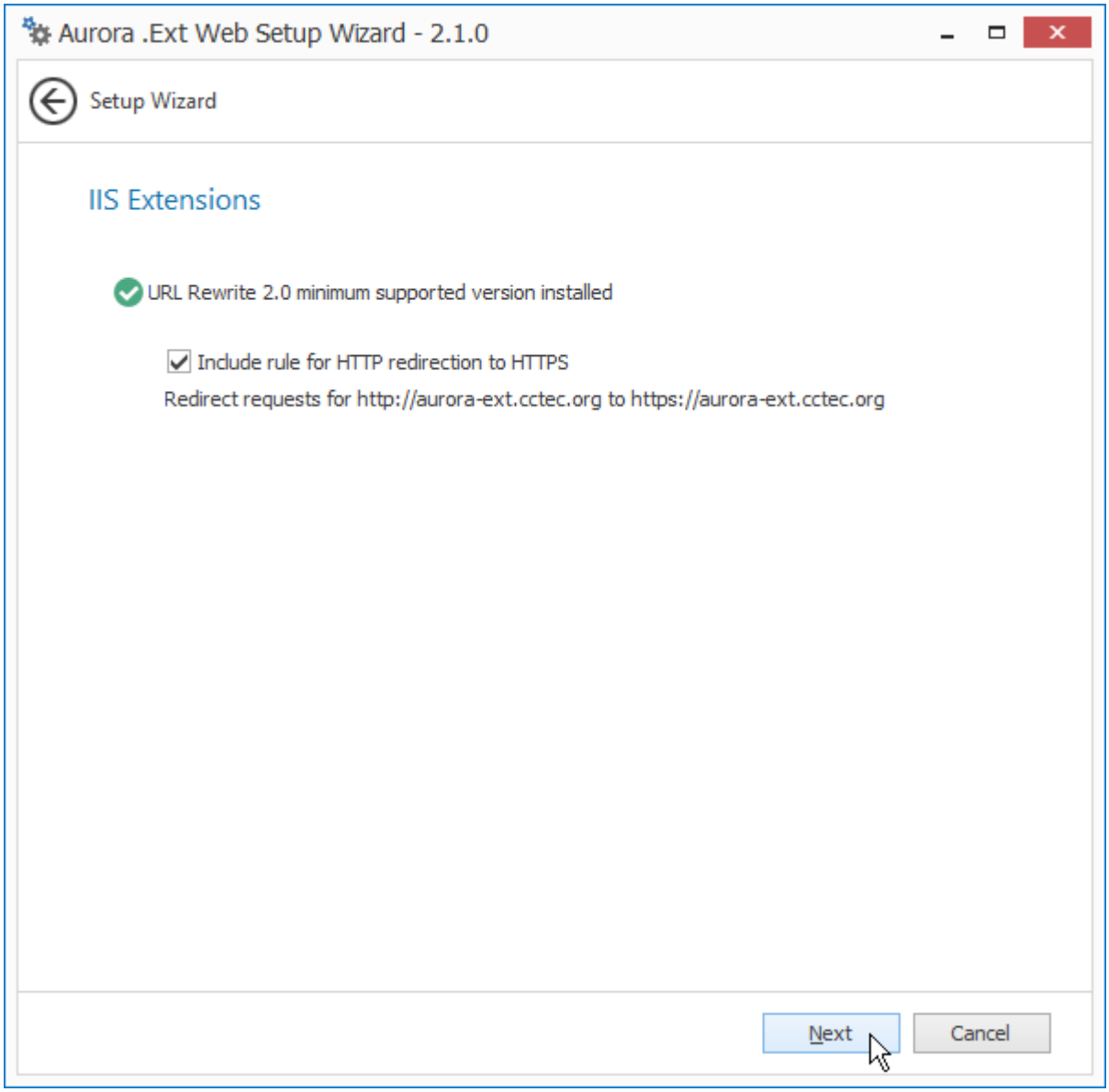
- *Service Account* – an Active Directory user account for use exclusively with this Application Pool. Note that the account must exist in the same domain as the server. A strong random password is generated for this account, so only the account name is required here.
- *Password / Password Confirm* – enter a password that will be used with the Service Account.
- *Proxy Rights Group* – an Active Directory security group which the Service Account will be a member of. File system and Share Rights for the Service Account should be managed using this group.
- *New Accounts Container* – a container in Active Directory where the service account will be placed, if it is a new account. Note that existing accounts will only be modified, but not moved to this location.
- *Provision Accounts in Active Directory* – If selected, the account information provided will be used to create a new account or modify an existing account in Active Directory. If unselected, the information provided will be used for the Aurora .Ext Web Application configuration, but will not create or modify an Active Directory account.

The *New Accounts Container* and *Provision Accounts in Active Directory* options are useful in scenarios where delegated administration is in place. In these cases, select the container where the administrator has been delegated management permissions, or optionally have an administrator create the accounts beforehand, and uncheck the *Provision Accounts in Active Directory* checkbox.

Unlike the Aurora web application, Aurora .Ext runs the Application Pool using the default Application Pool Identity. The proxy account is only used for specific calls where file system access is needed by a guest account. Due to the nature of how security is handled differently for internal users accessing their files via Aurora and guest accounts that access shared folders via Aurora .Ext, the management of the associated proxy accounts is somewhat different as well.

For more information regarding the security aspects of these web services and the role that the proxy/service accounts play, see the *Deployment Planning* > *Security Considerations* section of the *Aurora Administration Guide*.

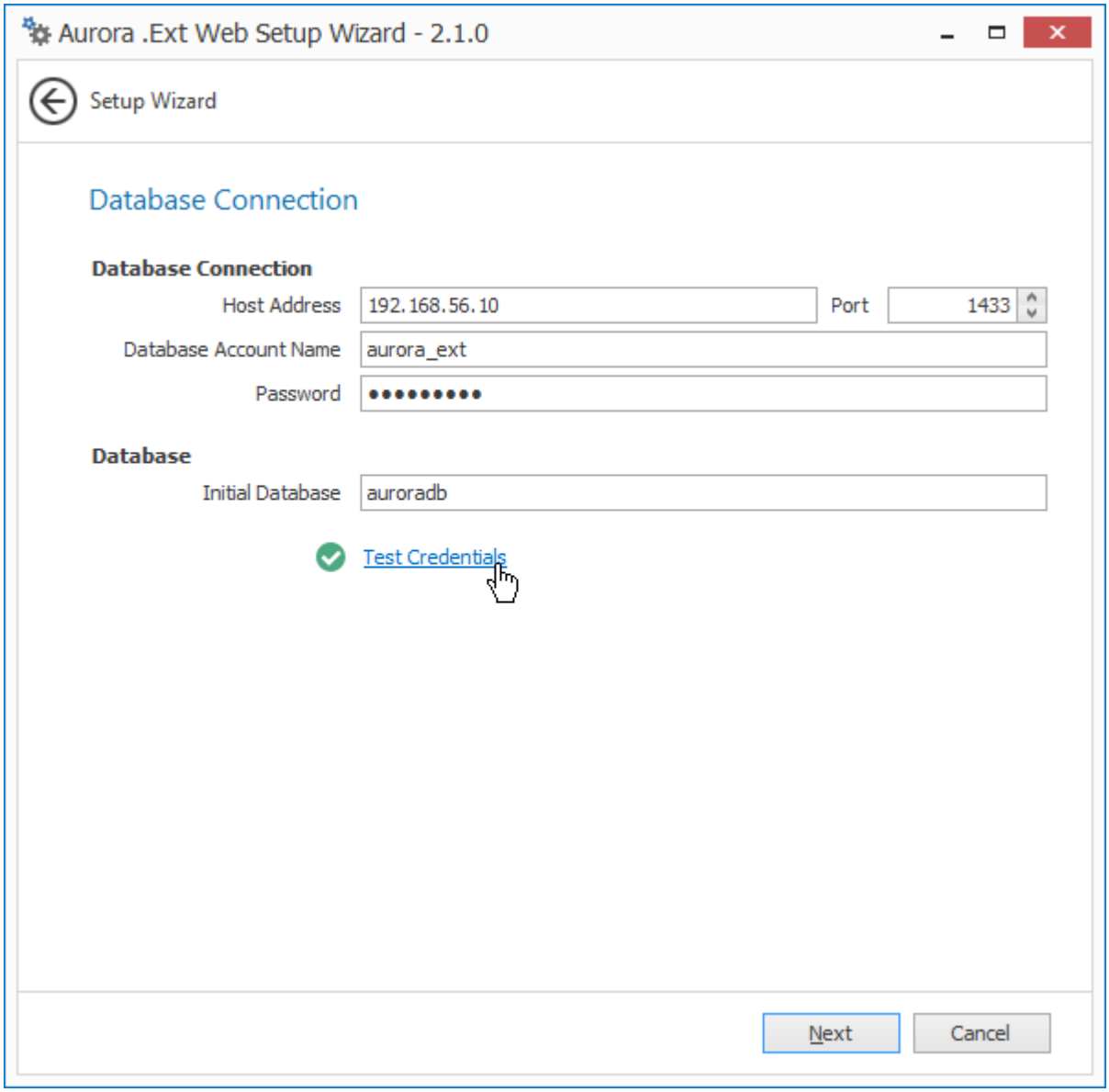
4. Click **Next** to install or update the **URL Rewrite 2.0** IIS module.



This step also adds rewrite rules into the Aurora .Ext application that redirect calls for the unsecured site to the SSL/TLS secured address.

Click **Next** to continue.

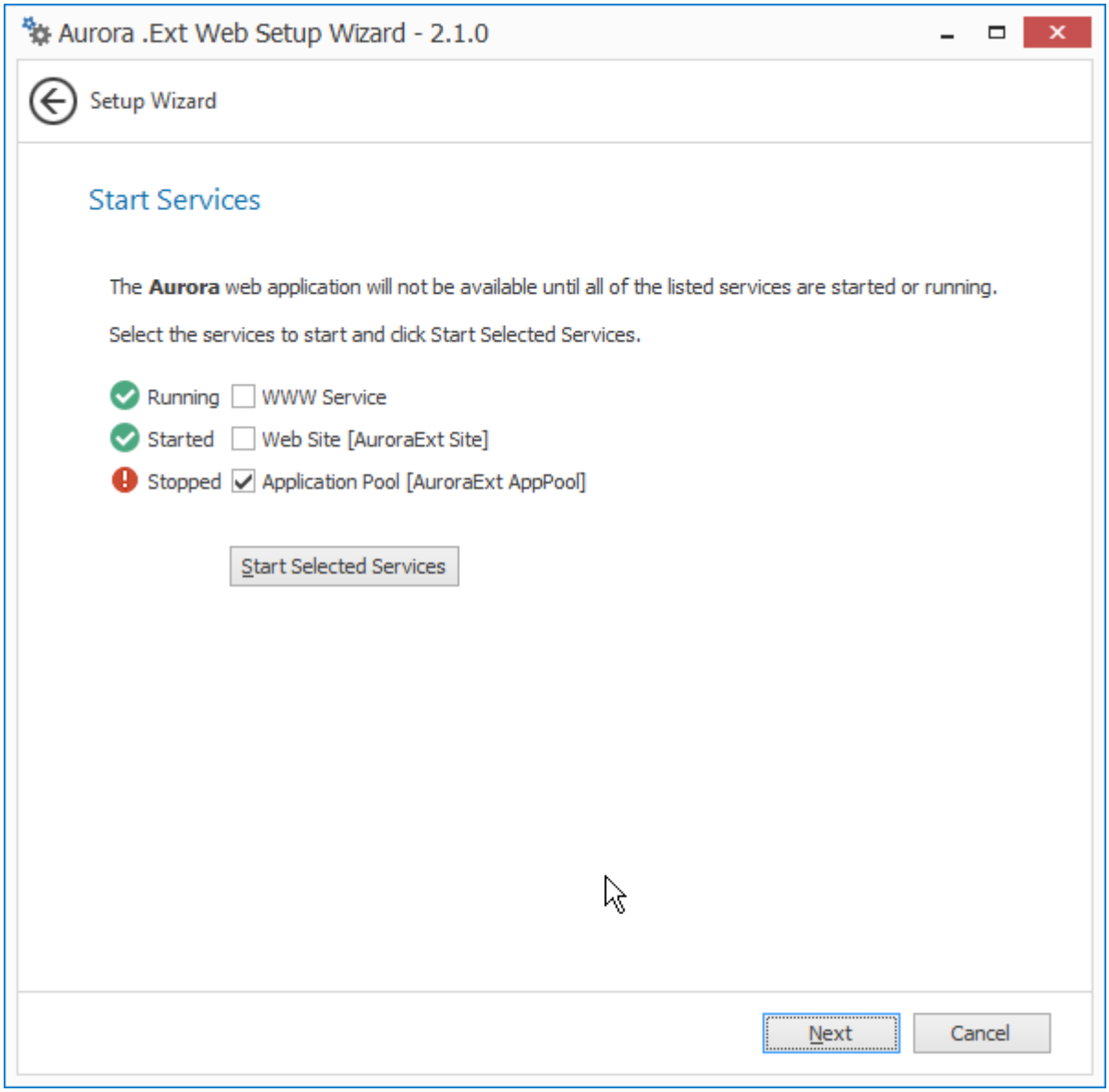
5. Enter the database connection parameters.



If Aurora .Ext was installed on the same server as Aurora, this information will already be filled in.

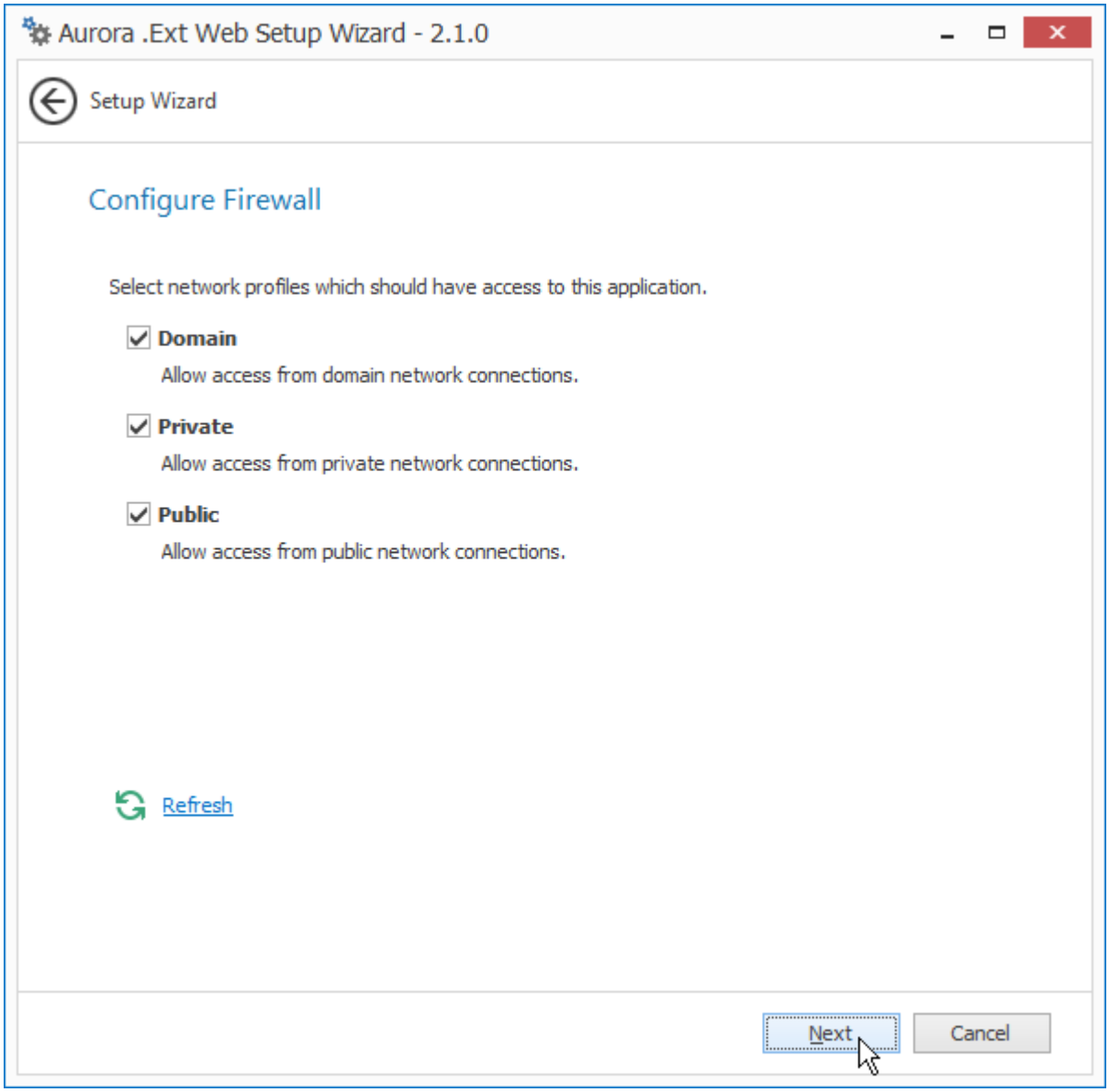
Test the database connection by clicking **Test Credentials**,, then click **Next** to continue when complete.

6. [Optional] Click **Start Selected Services**, then click **Next**.

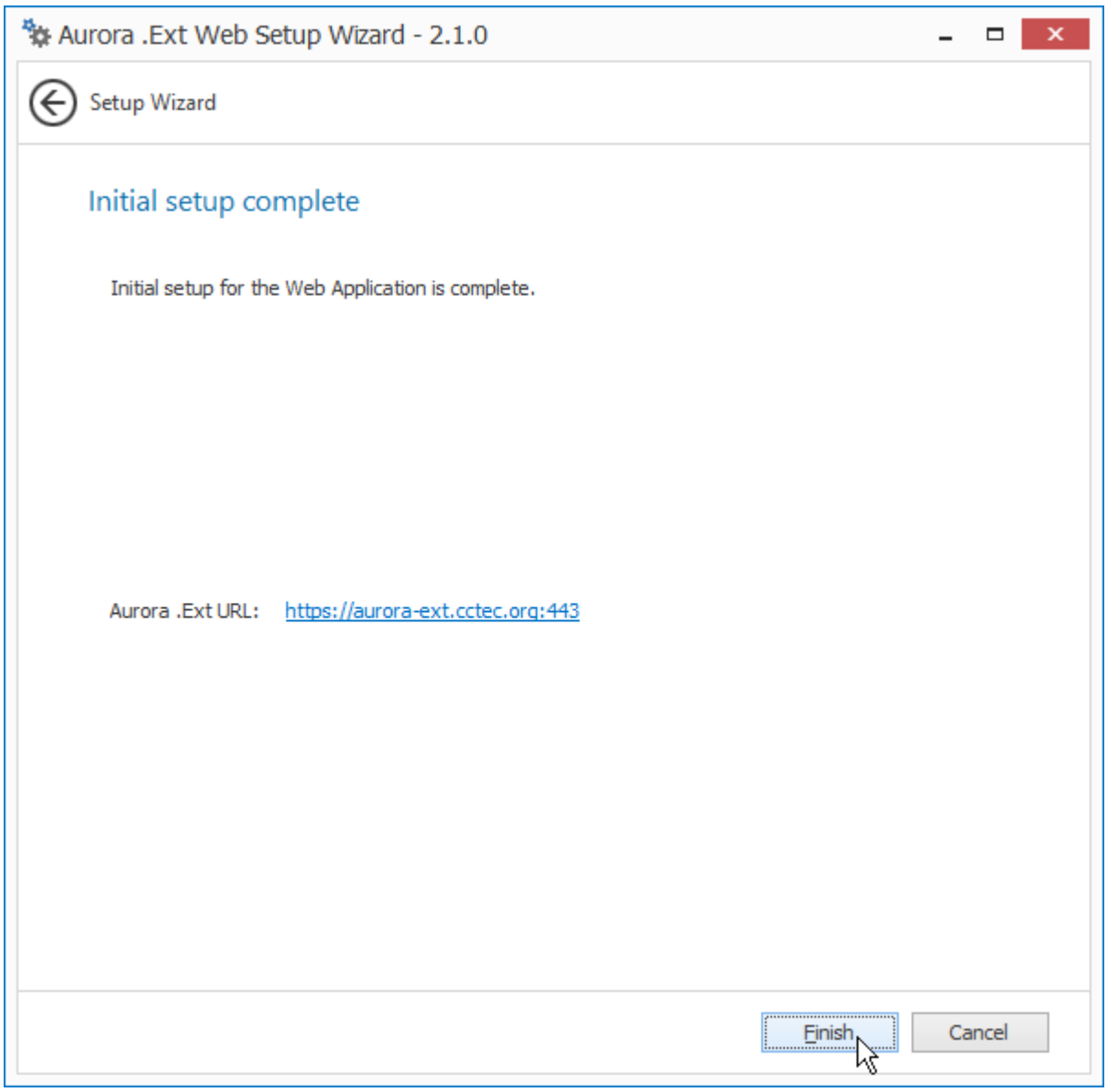


The **Start Services** page will only be displayed if one or more of the required services are not running. Simply start the services using the provided interface, then click **Next** to continue.

7. Click **Next** to accept the default Windows Firewall rules.



8. The Aurora .Ext configuration wizard is now complete.



The configured URL for Aurora .Ext guest access is displayed, however access may not be fully configured yet. See the section on *Configuring Guest Access* in the *Aurora 2.5 Administration Guide* for more details.