Oracle® Hospitality Simphony

Installation Guide

Release 2.10

E89800-07

August 2018

Contents

Tables vi

Figures vii

Preface viii

Audience viii
Customer Support viii
Documentation viii
Revision History viii

1 Getting Started 1-1

Installation Process 1-1
Deployment Scenarios Using R&A version 9.0 and Later 1-2
Installing Application Components and Databases on Two Servers 1-2
Installing Both Application Components and Databases on Separate Servers 1-2
Deployment Scenarios Using R&A version 8.5.1 1-3
Installing All-In-One 1-3
Installing Application Components and Databases on Separate Servers 1-3
Installing Application Components and Databases on Three Servers 1-4
Installing Both Application Components and Databases on Separate Servers 1-4

2 Pre-Installation Tasks 2-1

Property Network Considerations 2-1
Pre-install Reporting and Analytics Installation Requirements 2-1
Install Microsoft Internet Information Services (IIS) 2-1
Installing Oracle Database 11g or 12c 2-8
Creating Oracle Database Tablespaces 2-8
Database User Passwords 2-9
Increasing Database Process Count 2-9

3 Simphony Installation Tasks 3-1

Before Installing Simphony 3-1
Multi-Factor Authentication 3-1
MFA Configuration Prerequisites 3-1
Simphony MFA Configuration During the Installation of Simphony 3-1
Accessing the Simphony EMC Using MFA for the First Time 3-2
Assigning MFA EMC Access Privileges 3-3
Enrolling Users MFA Email Addresses and Passwords 3-4
Setting the Max Allowed Failed Logins for EMC Access 3-5
Configuring the SMTP and Backup SMTP Servers in the EMC 3-6
Simphony Installation for an All-in-One Server 3-7

4 Installing Simphony on Multiple Servers 4-1

Installing Simphony on Multiple Servers 4-1
Installing Simphony Database Components on Microsoft SQL Server 4-2
Installing Simphony Application Components on One or More Servers 4-3

Preparing a Multi-Server Environment Using a Load Balancer for the Simphony Import/ Export Service 4-4

5 Upgrading from a Previous Release 5-1

Upgrading Reporting and Analytics (R&A) 5-1

R&A version 9.0 5-1

R&A version 8.5.1 5-1

Upgrading to Simphony 2.10 5-1

Upgrades with Separate Transaction and Security Database Servers (when adding a new database server) 5-2

Upgrades without Separate Transaction and Security Database Servers 5-5

Upgrades with Existing Separated Transaction and Security Database Servers 5-7

Upgrading Simphony Prior to Simphony version 2.10 5-8

Post-Upgrade Tasks 5-10

Post-Upgrade Steps for CAPS on IIS for Simphony 2.9 Users 5-10

Step 1- Close and Post All Transactions 5-10

Step 2- Access the IIS Manager Console 5-10

Step 3- Rename the IIS Folder 5-13

Step 4- Enable an Option and Configure CAPS 5-14

Step 5- Stop IIS 5-14

Step 6- Move the DbSettings.xml to the Newly Defined IIS CAPS Path 5-15

Step 7- Start IIS 5-15

Step 8- Verify Log Creation, Database Tables, and Delete the Old Directory 5-15

6 Post-Installation Tasks 6-1

Update the Property EMC Client 6-1

Updating Simphony License Counts 6-1

Updating Property Administrator and Database Logon Credentials 6-2

Configuring IIS Application Pool Settings 6-3

Configure Recycle Settings for the IIS Application Pool 6-3

After the Simphony Installation 6-3

If You Installed the Blank Database 6-3

If You Installed the Sample Database 6-3

Setting the Start-Of-Day Sequencer Machine and the App Server Time Zone 6-4

Connecting Reporting and Analytics to Simphony 6-5

Enabling Communication Between the Enterprise and Workstations 6-6

Binding SSL Certificates to IIS 6-6

7 Uninstalling Simphony 7-1

8 Troubleshooting 8-1

Insufficient System Privileges 8-1

Cannot Connect to the Database Server During the Simphony Installation 8-1

Adding Simphony to the Windows Firewall Exceptions 8-1

Starting the Oracle Listener 8-1

9 List of Simphony Components and Services 9-2

10 List of Simphony Database Configuration Fields 10-1

Appendix A **A-1**

Sample Script for Creating Oracle Tablespaces.. A-1

Appendix B **B-1**

Post-Installation Best Practices B-1

Creating Database Backups B-1

Changing the Application Server’s Name B-1

Changing an Oracle Database Server’s Name B-3

Changing a Microsoft SQL Server’s Computer Name B-3

Tables

Table 1 Pre-Installation Tasks for Simphony Version 2.10 ... 2-7
Table 4-1 Overview of Installing Simphony on Multiple Servers ... 4-1
Table 4-2 Preparing a Multi-Server Simphony Installation Using a Load balancer for the Import/Export Service ... 4-4
Table 3 Post-Upgrade Tasks for Simphony Version 2.9 (or later) ... 5-10
Table 9-1 - List of Application and Database Services ... 9-2
Table 10-1 - List of Database Configuration Fields ... 10-1
Table 10-2 - Host Files ... B-1
Table 10-3 - Oracle Database Files ... B-1
Table 10-4 - Simphony Services and Reporting and Analytics Files ... B-2
Table 10-5 - Simphony Install ... B-2

Figures

Figure 1-1 Example of Application and DB Components on Different Servers....1-2
Figure 1-2 Example of Application and DB Components on Separate Servers 1-2
Figure 1-3 Example of an All-In-One Installation 1-3
Figure 1-4 Example of Application Components and DBs on Separate Servers....1-3
Figure 1-5 Example of Application Components and DBs on 3 Separate Servers....1-4
Figure 1-6 Example of Each Application and DB Component on Separate Servers....1-4
Figure 2-1 Server Manager – Adding Roles and Features 2-1
Figure 2-2 Server Manager – Select Server....2-2
Figure 2-3 Server Manager – Web Server Role Services....2-3
Figure 2-4 Server Manager – Performance and Security Role Services....2-4
Figure 2-5 Server Manager – Application Development Role Services....2-5
Figure 2-6 Server Manager – Management Tools 2-6
Figure 2-7 Database Configuration Options - Character sets - Use Unicode Option 2-8
Figure 3-1 Enabling Multi-Factor Authentication....3-2
Figure 3-2 MFA Access Privilege Roles Configuration 3-3
Figure 3-3 MFA Access Privilege Roles Configuration - continued 3-4
Figure 3-4 Employee Email Address Configuration....3-5
Figure 3-5 EMC MFA Configuration 3-6
Figure 3-6 Simphony Installation Application 3-7
Figure 3-7 Simphony Services....3-8
Figure 3-8 Security Enforcement | Certificate Check 3-9
Figure 3-9 Service Host & Port Number....3-10
Figure 5-1 Simphony Component Upgrade Choices....5-2
Figure 5-2 Security Database Connection for the Secondary DB Server 5-4
Figure 5-3 IIS CAPS Site 5-11
Figure 5-4 Simphony Application Pools....5-12
Figure 5-5 IIS CAPS Application Pool 5-12
Figure 5-6 CAPSConfigurator.exe.config IIS CAPS Directory Installation Folder Path 5-13
Figure 5-7 Default IIS CAPS Folder Installation Path....5-13
Figure 5-8 CAPS Configurator Tool....5-14
Figure 6-1 AppLoader Icon....6-1
Figure 6-2 Property Report Location 6-5

Preface

Audience

This installation guide is intended for installers, programmers, technical support teams, product specialists, and others who are responsible for setting up Oracle Hospitality Simphony version 2.10.

Customer Support

To contact Oracle Customer Support, access My Oracle Support at the following URL:
https://support.oracle.com

When contacting Customer Support, please provide the following:

- Product version and program/module name
- Functional and technical description of the problem (include business impact)
- Detailed step-by-step instructions to re-create
- Exact error message received and any associated log files
- Screen shots of each step you take

Documentation

Oracle Hospitality product documentation is available on the Oracle Help Center at
http://docs.oracle.com/en/industries/hospitality/

Revision History

Date	Description of Change
February 2018	• Initial publication
February 2018	• Updates to Chapter 6 within the Connecting Reporting and Analytics to Simphony section
May 2018	• Corrected the support for Microsoft SQL Server 2012
July 2018	• Updates to Chapter 5, specifically the post-upgrade steps for CAPS on ISS
August 2018	• Updates to Chapter 2’s Install Microsoft Internet Information Services (IIS) section

1 Getting Started

This guide provides instructions on how to install, upgrade, and configure Simphony version 2.10 or later.

Beginning with Simphony version 2.9 (or later), users must install Reporting and Analytics (R&A) separately from Simphony using the Back Office R&A installation application. For upgrades from versions prior to Simphony 2.9, users must upgrade to Reporting and Analytics version 8.5.1 Patch 3 prior to installing or upgrading to Simphony version 2.9. Simphony version 2.10 is compatible with both R&A versions 8.5.1 Patch 3 and 9.0 Patch 8.

Installation Process

1. **Select the appropriate deployment scenario**

   Prior to installation and configuration, you need to determine which deployment scenario meets your requirements. See Deployment Scenarios for more information.

2. **Install the database server application**

   You need to install one of the following database platforms prior to installing Simphony application components:

   - Oracle Database 11g
   - Oracle Database 12c
   - Microsoft SQL Server 2008 R2
   - Microsoft SQL Server 2012

3. **Upgrade or install Simphony**

   You can run the Simphony version 2.10 or later installation application to upgrade Simphony, to perform a clean installation, or to install and add application servers.

   See Upgrading from a Previous Release and List of Simphony Components and Services for more installation information.

4. **Configure post-installation settings**

   The post-installation configuration ensures that the application components and the database are configured correctly.

5. **Verify the installation**

   Perform the verification step to ensure that the Simphony application and the database applications are set correctly.

6. **Troubleshooting**

   Follow the instructions in this section to resolve common problems you might encounter when installing Simphony version 2.10.

Deployment Scenarios Using R&A version 9.0 and Later

Installing Application Components and Databases on Two Servers

You can install the Simphony and R&A databases along with the Simphony components on one server and the R&A components on another server.

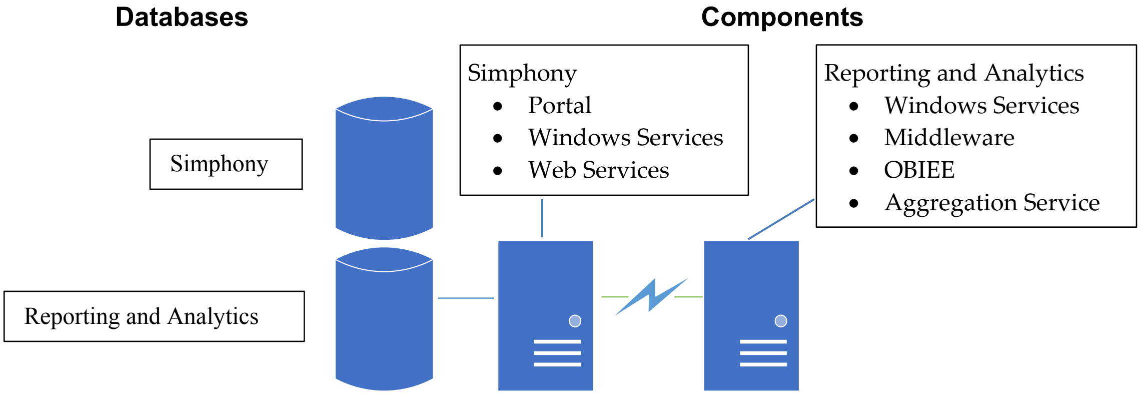


Figure 1-1 Example of Application and DB Components on Different Servers

Installing Both Application Components and Databases on Separate Servers

You can install the Simphony and R&A components and each application's database on separate servers.

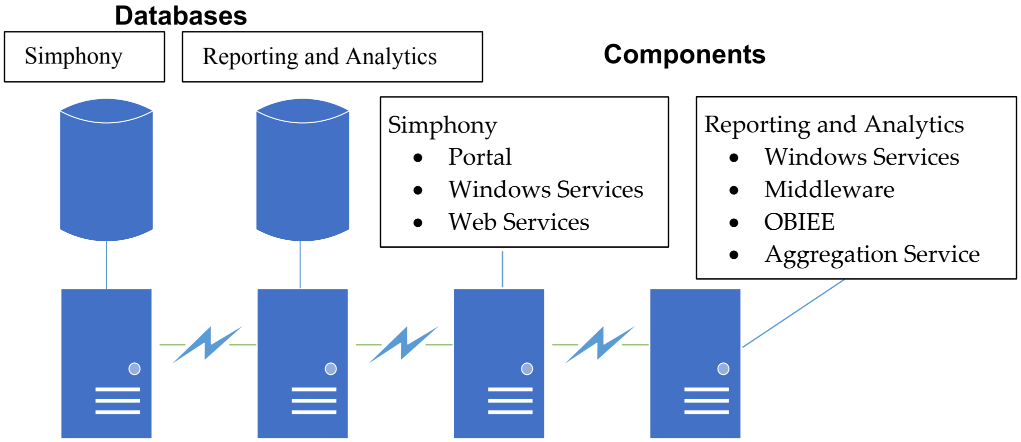


Figure 1-2 Example of Application and DB Components on Separate Servers

Deployment Scenarios Using R&A version 8.5.1

Installing All-In-One

With an all-in-one installation, you install the Simphony and Reporting and Analytics (R&A) databases and the Simphony and R&A components on one server. If using an all-in-one installation scenario, Oracle Hospitality recommends that you install the Simphony application on a separate partition from where the Microsoft Windows operating system resides.

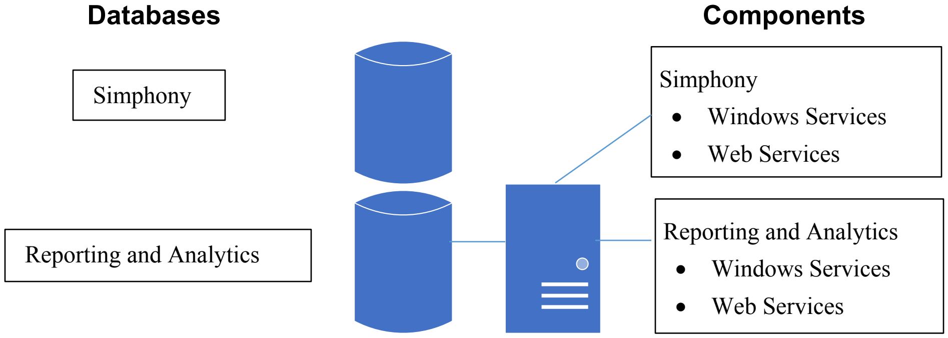


Figure 1-3 Example of an All-In-One Installation

Installing Application Components and Databases on Separate Servers

You can install the Simphony and Reporting and Analytics components on one physical or virtual server and install the databases on a separate server.

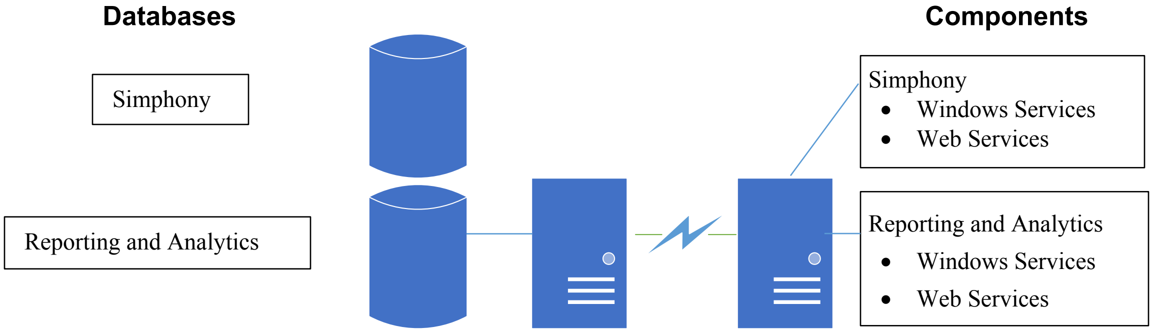


Figure 1-4 Example of Application Components and DBs on Separate Servers

Installing Application Components and Databases on Three Servers

You can install the Simphony and R&A databases along with the Simphony components on one server and the R&A components on a third server.

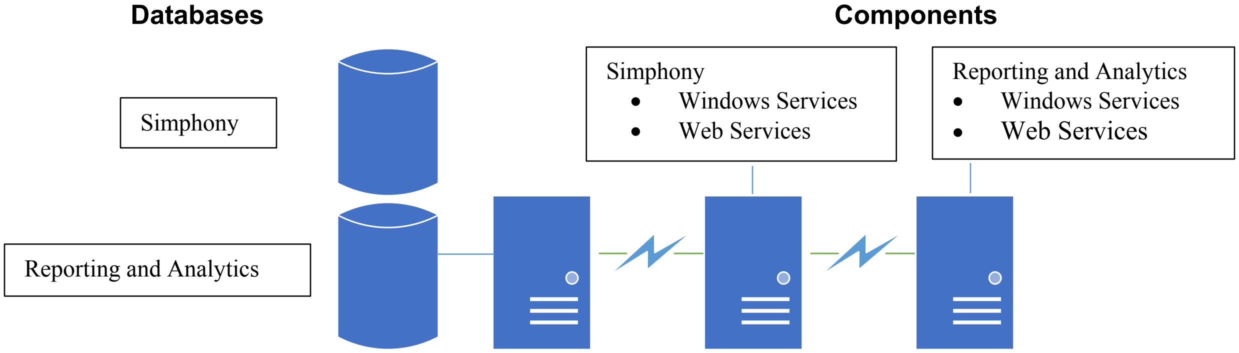


Figure 1-5 Example of Application Components and DBs on 3 Separate Servers

Installing Both Application Components and Databases on Separate Servers

You can install the Simphony and Reporting and Analytics components and each database on separate servers.

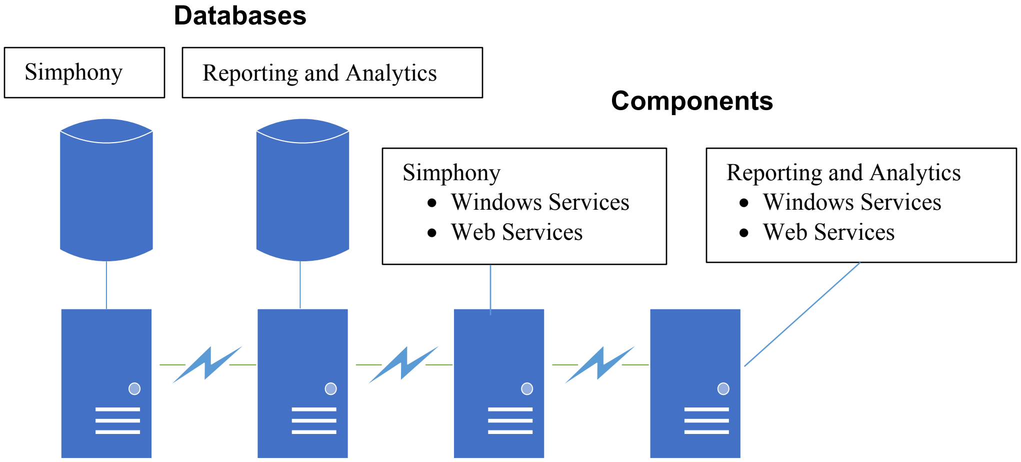


Figure 1-6 Example of Each Application and DB Component on Separate Servers

2 Pre-Installation Tasks

There are several pre-installation tasks that must be performed on the Simphony application server. After completing the steps in this chapter, see page 2-7 for database platform installation instructions.

Property Network Considerations

Prior to installing Reporting and Analytics or Simphony, property networks using Oracle RAC or Load Balancing environments must be operational.

If you are using a Load Balancing server and installing the Simphony Import/Export Service or plan to use the Simphony Engagement Cloud Service, select **LoadBalancer** for the required **CA Certificate Location** field.

If you define a Service Host Secure Port number other than the default of 443, you need to enable that port on the Load Balancing server.

Pre-install Reporting and Analytics Installation Requirements

Beginning with the Simphony version 2.9 (or later) release, users must install Reporting and Analytics (R&A) separately from Simphony using the Back Office R&A installation application. For upgrades from versions prior to Simphony 2.9, users must upgrade to Reporting and Analytics version 8.5.1 Patch 3 prior to installing or upgrading to Simphony version 2.9. Simphony version 2.10 is compatible with both R&A versions 8.5.1 Patch 3 and 9.0 Patch 8.

The *Oracle Hospitality Reporting and Analytics 8.5 Deployment Guide* provides instructions for installing Reporting and Analytics 8.5 and later.

The *Oracle Hospitality Reporting and Analytics 9.0 Installation Guide* provides instructions for installing Reporting and Analytics 9.0.

Install Microsoft Internet Information Services (IIS)

For more information about the Server Manager - Add Roles and Features Wizard, refer to the Microsoft TechNet Library at `https://technet.microsoft.com/en-us/`.

On Microsoft Windows Server 2012 R2, perform the following steps:

1. Using the Server Manager – Select **2 - Add roles and features**.

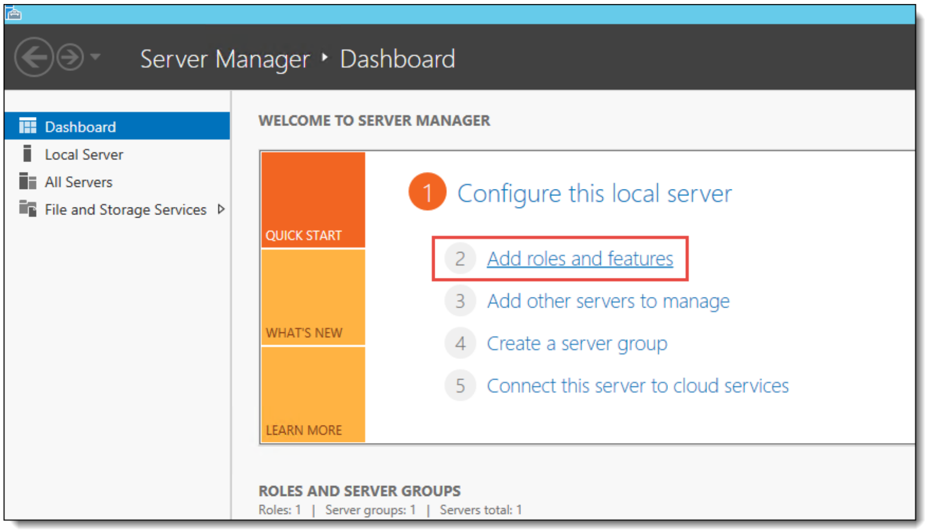
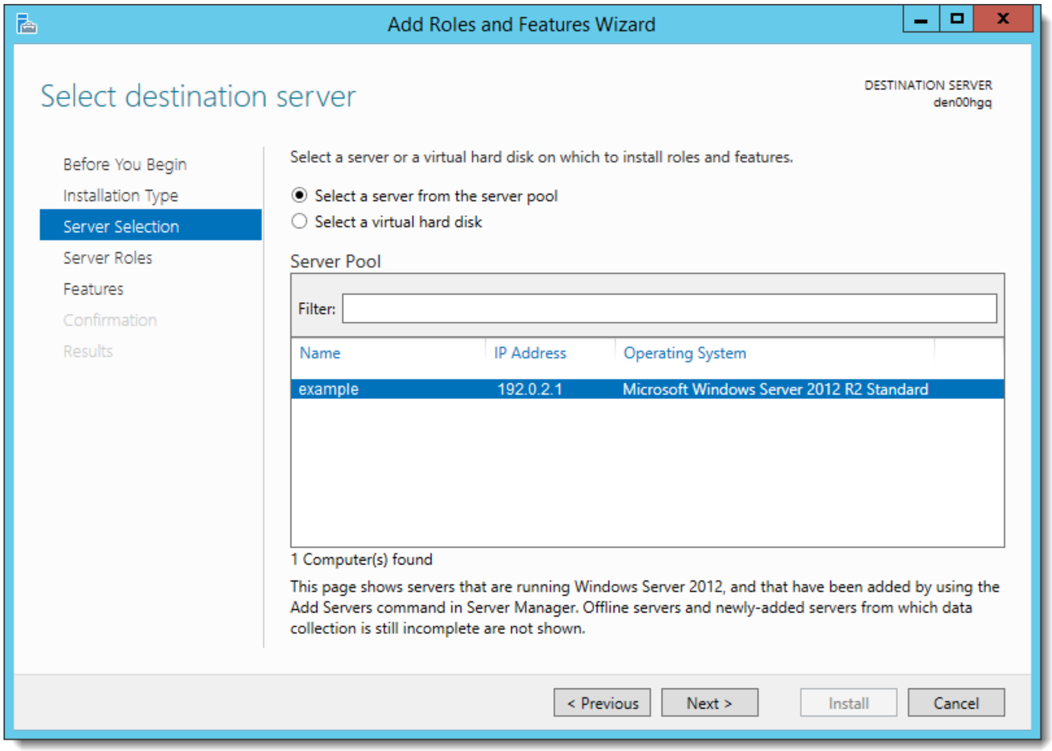

Server Manager ‣ Dashboard
Dashboard
Local Server
All Servers
File and Storage Services
WELCOME TO SERVER MANAGER
QUICK START
WHAT'S NEW
LEARN MORE
1 Configure this local server
2 Add roles and features
3 Add other servers to manage
4 Create a server group
5 Connect this server to cloud services
ROLES AND SERVER GROUPS
Roles: 1 | Server groups: 1 | Servers total: 1

Figure 2-1 Server Manager – Adding Roles and Features

2. Select **Role-based or feature-based installation**, and then click **Next**.
3. Choose **Select a server from the server pool**.

4. Select the server you are configuring, and then click **Next**.



Add Roles and Features Wizard

Select destination server

DESTINATION SERVER
den00hgq

Select a server or a virtual hard disk on which to install roles and features.

● Select a server from the server pool
○ Select a virtual hard disk

Server Pool

Filter:

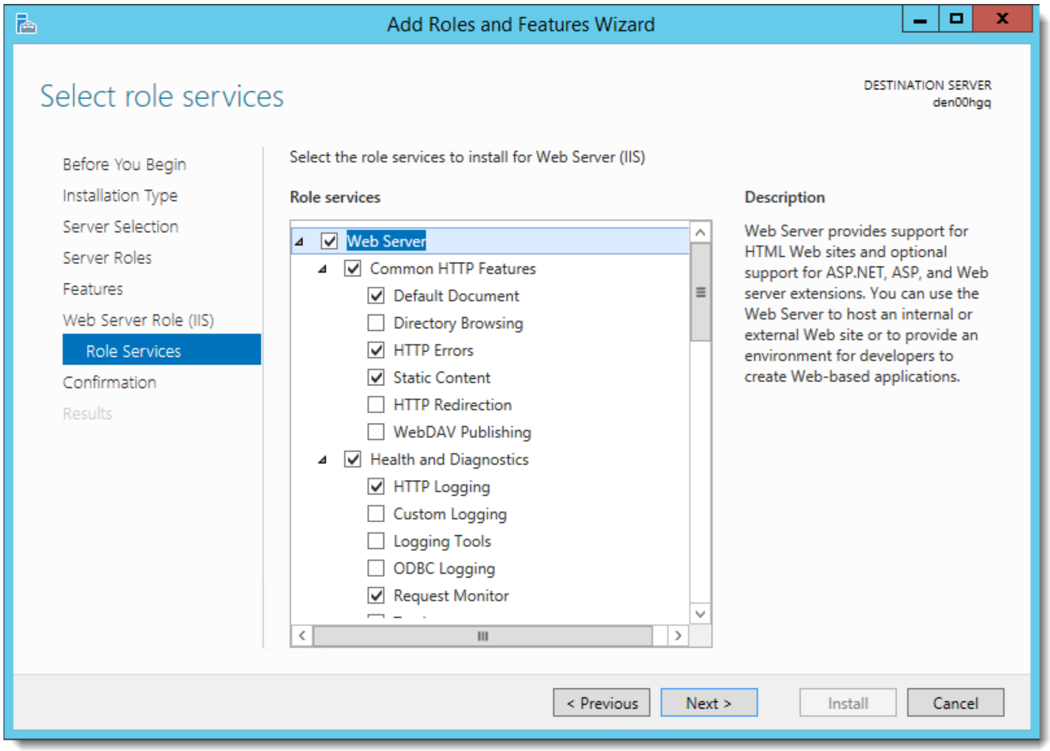
Name	IP Address	Operating System
example	192.0.2.1	Microsoft Windows Server 2012 R2 Standard

1 Computer(s) found

This page shows servers that are running Windows Server 2012, and that have been added by using the Add Servers command in Server Manager. Offline servers and newly-added servers from which data collection is still incomplete are not shown.

Figure 2-2 Server Manager – Select Server

5. Expand the Web Server Role (IIS).



Select role services

DESTINATION SERVER
den00hgq

Select the role services to install for Web Server (IIS)

Role services

- ☑ Web Server
  - ☑ Common HTTP Features
    - ☑ Default Document
    - □ Directory Browsing
    - ☑ HTTP Errors
    - ☑ Static Content
    - □ HTTP Redirection
    - □ WebDAV Publishing
  - ☑ Health and Diagnostics
    - ☑ HTTP Logging
    - □ Custom Logging
    - □ Logging Tools
    - □ ODBC Logging
    - ☑ Request Monitor

Description

Web Server provides support for HTML Web sites and optional support for ASP.NET, ASP, and Web server extensions. You can use the Web Server to host an internal or external Web site or to provide an environment for developers to create Web-based applications.

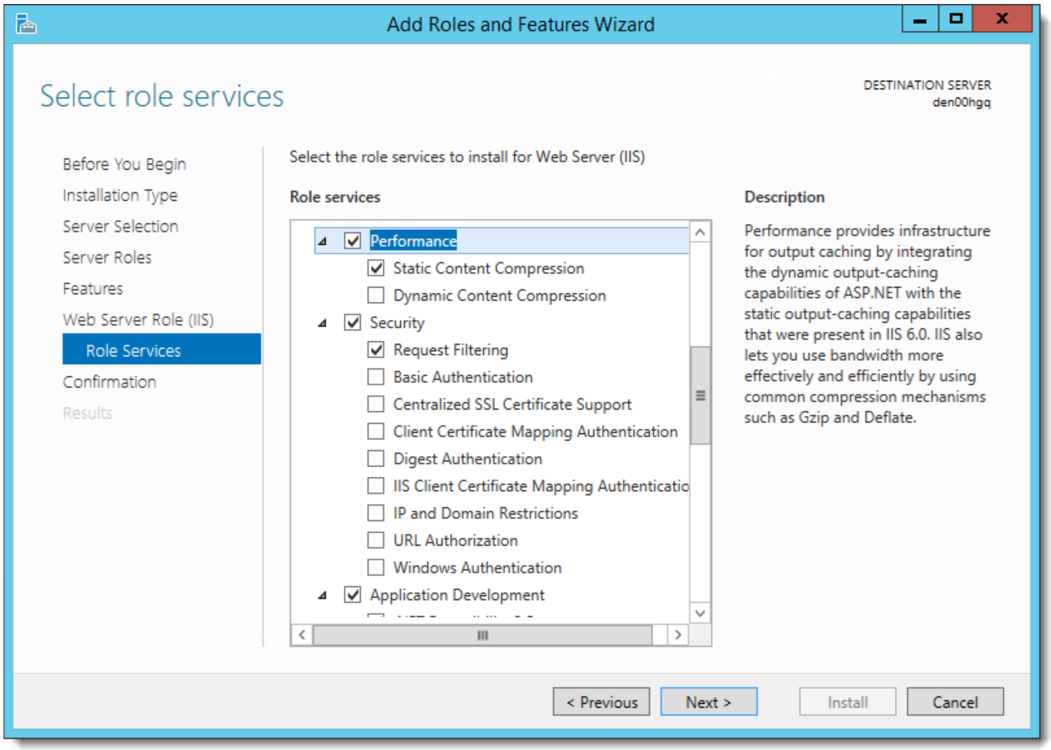
Figure 2-3 Server Manager – Web Server Role Services

6. Expand the **Web Server** options and select the following Common HTTP Features:
   - Default Document
   - HTTP Errors
   - Static Content

From a system security standpoint, the Directory Browsing role service should not be enabled.

7. Select the following Health and Diagnostics options:
   - HTTP Logging
   - Request Monitor

8. Select the **Performance** option **Static Content Compression**.
9. Select the **Security** option **Request Filtering**.



Select role services

DESTINATION SERVER
den00hgq

Select the role services to install for Web Server (IIS)

Role services

- ☑ Performance
  - ☑ Static Content Compression
  - □ Dynamic Content Compression
- ☑ Security
  - ☑ Request Filtering
  - □ Basic Authentication
  - □ Centralized SSL Certificate Support
  - □ Client Certificate Mapping Authentication
  - □ Digest Authentication
  - □ IIS Client Certificate Mapping Authenticatio
  - □ IP and Domain Restrictions
  - □ URL Authorization
  - □ Windows Authentication
- ☑ Application Development

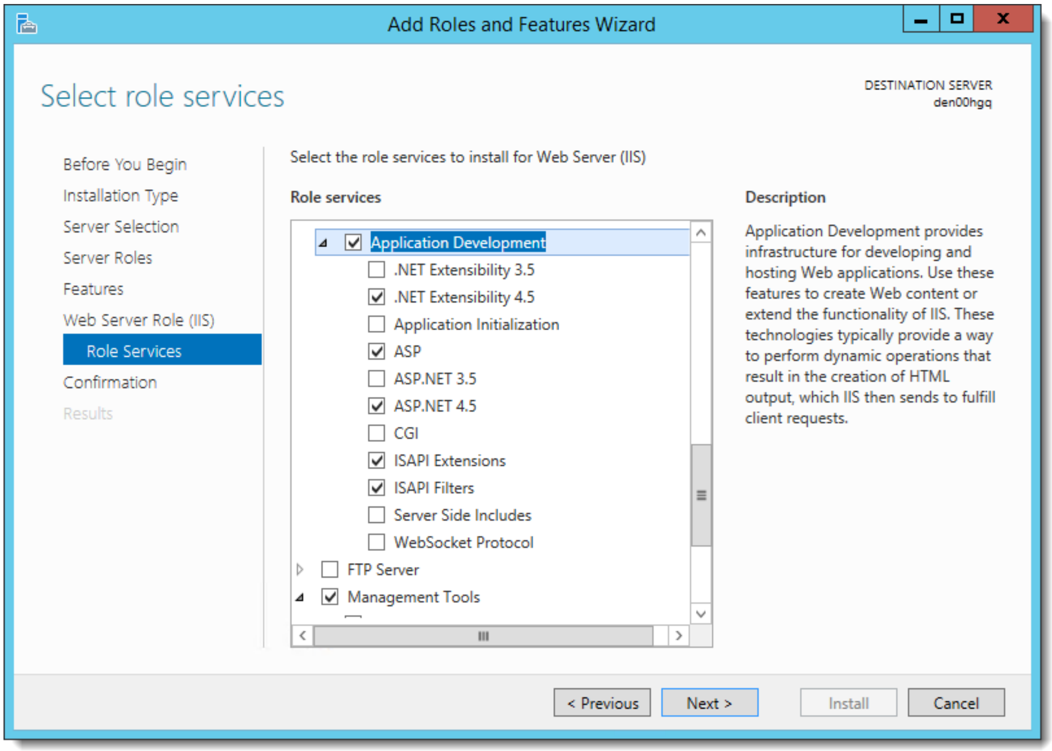
Description

Performance provides infrastructure for output caching by integrating the dynamic output-caching capabilities of ASP.NET with the static output-caching capabilities that were present in IIS 6.0. IIS also lets you use bandwidth more effectively and efficiently by using common compression mechanisms such as Gzip and Deflate.

Figure 2-4 Server Manager – Performance and Security Role Services

10. Select and expand **Application Development**, and then select the following options:

    - .NET Extensibility 4.5
    - ASP
    - ASP .NET 4.5
    - ISAPI Extensions
    - ISAPI Filters



Add Roles and Features Wizard

Select role services

DESTINATION SERVER
den00hgq

Select the role services to install for Web Server (IIS)

Role services

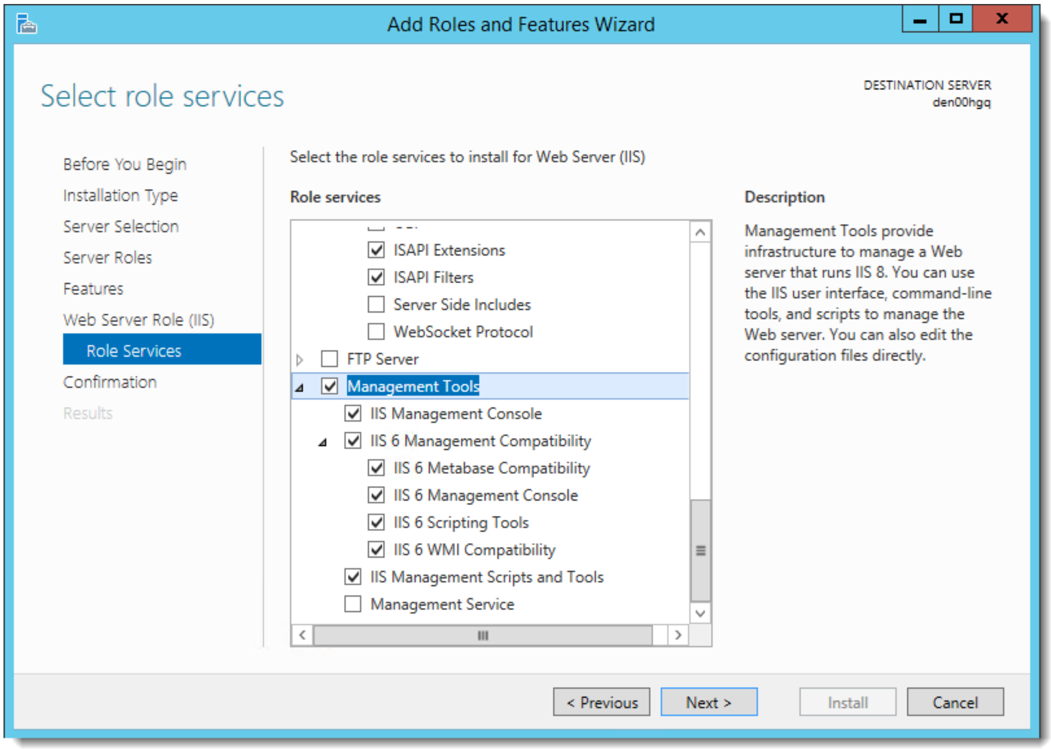
- ☑ Application Development
  - □ .NET Extensibility 3.5
  - ☑ .NET Extensibility 4.5
  - □ Application Initialization
  - ☑ ASP
  - □ ASP.NET 3.5
  - ☑ ASP.NET 4.5
  - □ CGI
  - ☑ ISAPI Extensions
  - ☑ ISAPI Filters
  - □ Server Side Includes
  - □ WebSocket Protocol
- □ FTP Server
- ☑ Management Tools

Description

Application Development provides infrastructure for developing and hosting Web applications. Use these features to create Web content or extend the functionality of IIS. These technologies typically provide a way to perform dynamic operations that result in the creation of HTML output, which IIS then sends to fulfill client requests.

Figure 2-5 Server Manager – Application Development Role Services

11. Select and expand **Management Tools**, and then select the following options:
    - IIS Management Console
    - IIS Management Scripts and Tools
12. Select **IIS 6 Management Compatibility,** and then select the following options:
    - IIS 6 Metabase Compatibility
    - IIS 6 Management Console
    - IIS 6 Scripting Tools
    - IIS 6 WMI Compatibility



Select role services

DESTINATION SERVER
den00hgq

Select the role services to install for Web Server (IIS)

Role services

- ☑ ISAPI Extensions
- ☑ ISAPI Filters
- ☐ Server Side Includes
- ☐ WebSocket Protocol
- ☐ FTP Server
- ☑ Management Tools
  - ☑ IIS Management Console
  - ☑ IIS 6 Management Compatibility
    - ☑ IIS 6 Metabase Compatibility
    - ☑ IIS 6 Management Console
    - ☑ IIS 6 Scripting Tools
    - ☑ IIS 6 WMI Compatibility
  - ☑ IIS Management Scripts and Tools
  - ☐ Management Service

Description

Management Tools provide infrastructure to manage a Web server that runs IIS 8. You can use the IIS user interface, command-line tools, and scripts to manage the Web server. You can also edit the configuration files directly.

Figure 2-6 Server Manager – Management Tools

13. Click **Next** as needed, and then click **Install**.

Table 1 Pre-Installation Tasks for Simphony Version 2.10

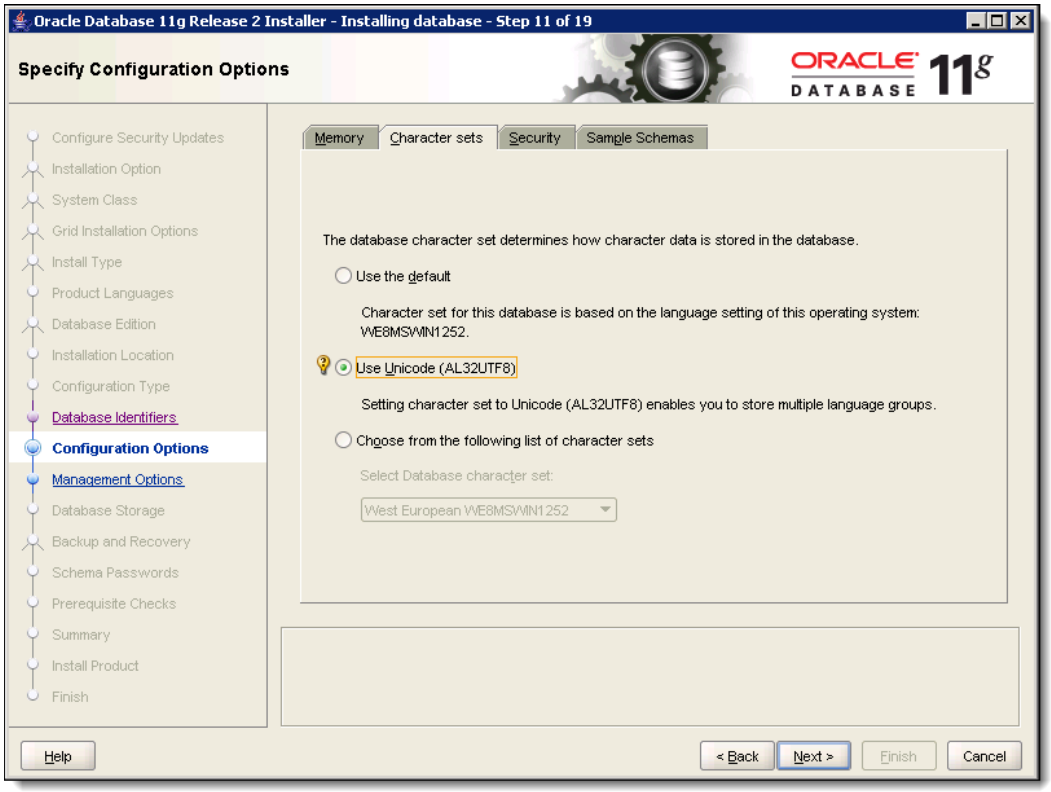
Pre-Installation Task	Instructions
Configure Log File rollover options (IIS)	For instructions on configuring Log file rollover options, refer to the Microsoft TechNet Library at `https://technet.microsoft.com/en-us/`.
Install .NET 4.6.1 Framework	Run the .NET 4.6.1 Framework setup in the `Installation Media\Prerequisites\DotNetFramework46` folder, following the on-screen instructions.
Turn on Data Execution Prevention (DEP)	For instructions on turning on Data Execution Prevention on the server, refer to the Microsoft TechNet Library at `https://technet.microsoft.com/en-us/`.
Disable Anti Denial-Of-Service (Dos) Attacks	If you are installing Simphony with Microsoft SQL Server as the database platform, you need to add the `SynAttackProtect` registry key to the computer that is running Microsoft SQL Server. For instructions on disabling DOS attacks, refer to the Microsoft TechNet Library at `https://technet.microsoft.com/en-us/`.
Install a database platform on the database server	Simphony version 2.10 supports the following database platforms: Oracle Database 11g Enterprise Edition Oracle Database 12c Enterprise Edition Microsoft SQL Server 2008 R2 Enterprise Edition Microsoft SQL Server 2012 R2 Enterprise Edition For instructions on installing and setting up the Oracle Database, see Installing Oracle Database 11g or 12c. For instructions on installing Microsoft SQL Server, refer to the Microsoft TechNet Library at `https://technet.microsoft.com/en-us/`. You can also install Simphony on a Microsoft SQL Server 2008 R2 or 2012 Failover Cluster. For instructions on installing a Microsoft SQL Server 2008 R2 or 2012 Failover Cluster, refer to the Microsoft TechNet Library at `https://technet.microsoft.com/en-us/`.
Manually create the folders to store the Microsoft SQL Server database files	Beginning with the Simphony 2.9.2 patch release (and later), for sites utilizing Microsoft SQL Server (and want to physically separate their Transaction (MCRSPOS) and Security (MCRSCACHE) databases), you must manually create folders on the secondary database server to point the Simphony installation program to, during the upgrade’s database creation steps.

Installing Oracle Database 11g or 12c

To download and install the Oracle Database, refer to the Oracle Technology Network (OTN) website at `http://www.oracle.com/technetwork/database/enterprise-edition/downloads/index.html`.

For Oracle Database 12c users, Oracle Hospitality does not support Pluggable database options at this time.

For Oracle Database users, ensure that the Use Unicode character set option is enabled during your database installation.



Oracle Database 11g Release 2 Installer - Installing database - Step 11 of 19

Specify Configuration Options

The database character set determines how character data is stored in the database.

○ Use the default

Character set for this database is based on the language setting of this operating system: WE8MSWIN1252.

● Use Unicode (AL32UTF8)

Setting character set to Unicode (AL32UTF8) enables you to store multiple language groups.

○ Choose from the following list of character sets

Select Database character set:

West European WE8MSWIN1252

Figure 2-7 Database Configuration Options - Character sets - Use Unicode Option

Creating Oracle Database Tablespaces

If you are using an Oracle database, ensure that you have the Simphony database Tablespaces created on your sever.

Create the following Oracle database Tablespaces on the database server or servers:

- MCRSPOS
- MCRSCACHE

See Appendix A for a sample script to create the database Tablespaces. The *Platform Guide for Microsoft Windows* and the *Administrator's Reference for Linux and UNIX-Based Operating Systems* contain more information about creating database Tablespaces.

Database User Passwords

When performing a database installation, specifically Oracle Database users, passwords must adhere to the following rules:

- Cannot start with a number (for example, 1QasHello)
- Cannot start with a special character (for example, #abc)
- Must have at least 8 characters
- Must have at least one uppercase letter
- Must have at least one number
- Cannot use a dictionary word, although two dictionary words together may pass
- Must have at least one supported special character
- Can only use database supported special characters, which include the underscore (_), dollar sign ($), and pound symbol (#) characters. The following characters are not recognized and should not be used for Oracle Database user passwords: ! @ % ^ & *

For example, **Hello3&there** is not valid because **Hello** and **there** are separated dictionary words by symbols/numbers, but **Hellothere$1** is valid.

Increasing Database Process Count

Run the ALTER SYSTEM SET processes=300 SCOPE=SPFILE; command on the Oracle Database and restart the Oracle Database Service. If you are using the Oracle Linux operating system, run the shutdown immediate; command and then run the `STARTUP pfile=init.ora`; command to restart the service. The Administrator's Reference for Linux and UNIX-Based Operating Systems contains more information about restarting the Oracle Database Service.

If you are using a Microsoft Windows Server, restart the **OracleServiceSIMPHONY** service using the Windows Services dialog. The Platform Guide for Microsoft Windows contains more information about restarting the Oracle Database Service on Microsoft Windows Servers.

3 Simphony Installation Tasks

This chapter provides a list of tasks that you must perform for each of the installation scenarios.

Before Installing Simphony

If you are installing Simphony with an Oracle Database, ensure that the Simphony and SimphonyXDB instances are running. To show the status of the Simphony and SimphonyXDB instances, run the `lsnrctl STATUS` command from a command prompt on the database server.

During a fresh Simphony installation, the Sample Database should not be utilized in a production environment. Rather, users should install the Blank Database.

See If You Installed the Blank Database or If You Installed the Sample Database for initial application logon information after the Simphony installation is completed.

Multi-Factor Authentication

Simphony Multi-factor Authentication (MFA) is enabled by default in order to comply with Payment Card Industry (PCI) version 3.2 standards.

You can configure MFA in Simphony to provide users a one-time password (OTP) through email in two ways. They are:

1. During the installation of the Simphony software.
2. After the installation of the Simphony software, using the Simphony EMC.

MFA Configuration Prerequisites

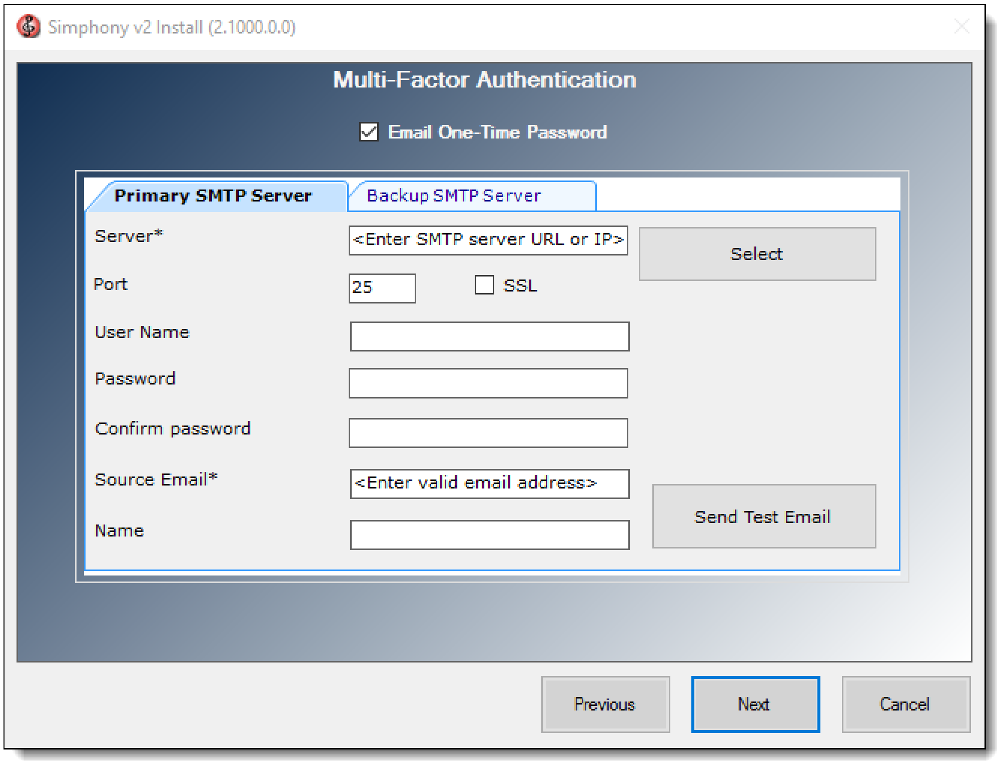
- For MFA implementation, you must install and make network accessible, two separate Simple Mail Transfer Protocol (SMTP) email servers (each to be designated as either a Primary or Backup server). This allows users to receive their OTP via email each time they attempt to log onto the EMC. An SMTP Backup server is required to provide EMC access redundancy in the event that the Primary SMTP server fails for any reason.
- Each employee using the EMC or SWP must have a valid email address configured in their employee record

Simphony MFA Configuration During the Installation of Simphony

When running the Simphony 2.10 installation application, you are prompted to configure MFA. Your choices are:

1. Deselect the **Email One-Time Password** checkbox and click **Next** to bypass this part of the installation until after Simphony has been installed. Bear in mind that when you deselect the Email One-Time Password checkbox, you receive a message that indicates your system is not in compliance with PCI version 3.2 standards.
2. If you choose to configure MFA at this time, the configuration instructions are the same as outlined here: Configuring the SMTP and Backup SMTP Servers in the EMC.

It is important to note that if you are performing a Simphony Standard Cloud Service installation, MFA configuration that is completed during the installation of Simphony is duplicated for each enterprise. After Simphony has been installed, you can go back and make edits in the EMC for individual enterprises (or organizations) that might have differing SMTP servers or settings from each other.



Simphony v2 Install (2.1000.0.0)

Multi-Factor Authentication

☑ Email One-Time Password

Server* <Enter SMTP server URL or IP>

Port 25 □ SSL

User Name

Password

Confirm password

Source Email* <Enter valid email address>

Name

Figure 3-1 Enabling Multi-Factor Authentication

Accessing the Simphony EMC Using MFA for the First Time

To utilize MFA on your Simphony system you need to add and register your email address. Follow the steps outlined below:

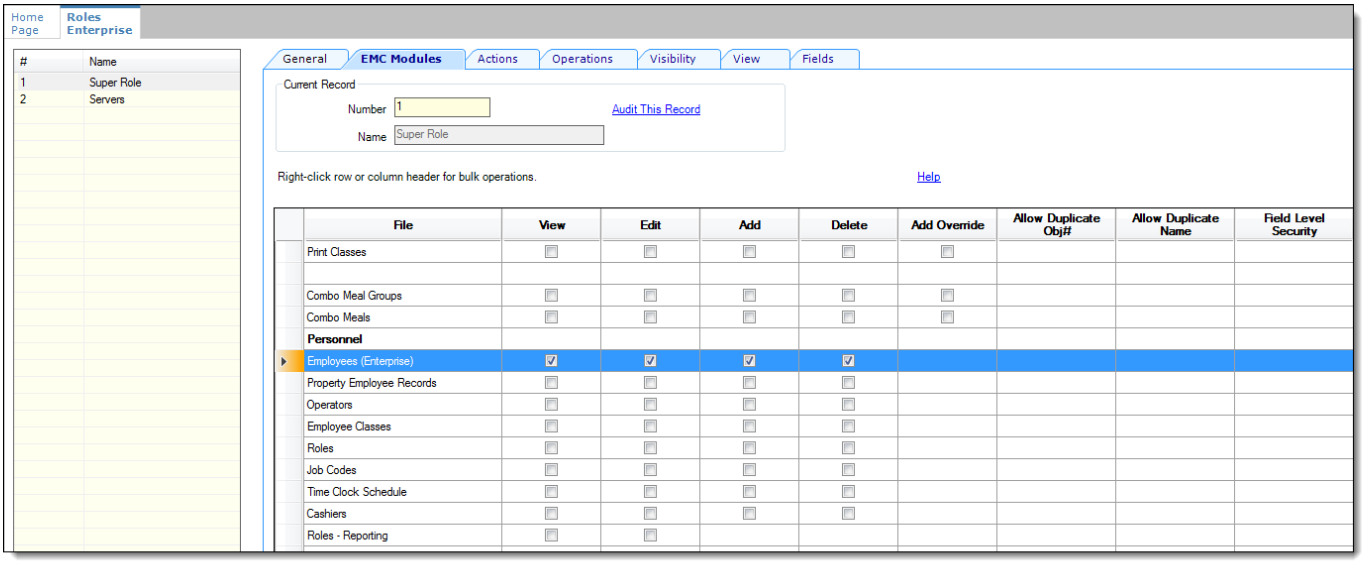
1. When first attempting to log onto the Simphony EMC, when prompted, enter your user name in the **User Name** field, and your email address in the **Email Address** field.
2. Re-enter your email address in the **Confirm Email Address** field and click **Register**. This email address is utilized to send you the OTP. Your registered email address is written to your employee record in the newly added **Email** field.
3. Access the email account you registered in step 1 and open the email containing the OTP.
4. Enter the password in the **One-Time Password** field and click **Enter**.

OTP passwords are only valid for five minutes, so enter your OTP password in a timely fashion. If the 5 minute threshold is exceeded, you are required to re-login to the EMC to generate another OTP. OTPs are valid for one single entry for the individual attempting to log onto the EMC at that time. After entering a valid OTP, the EMC opens.

Assigning MFA EMC Access Privileges

To access and configure MFA security for other users on your system, you need to be assigned the correct privileges in the EMC.

1. Select the **Enterprise** level, click **Configuration**, and then click **Roles**.
2. Click the **EMC Modules** tab and scroll to the Personnel section.
3. Select the checkboxes for the **Employees (Enterprise)** access privileges for each of the following columns:
   - View
   - Edit
   - Add
   - Delete
4. Click **Save**.



#	Name
1	Super Role
2	Servers

Current Record

Number: 1

Name: Super Role

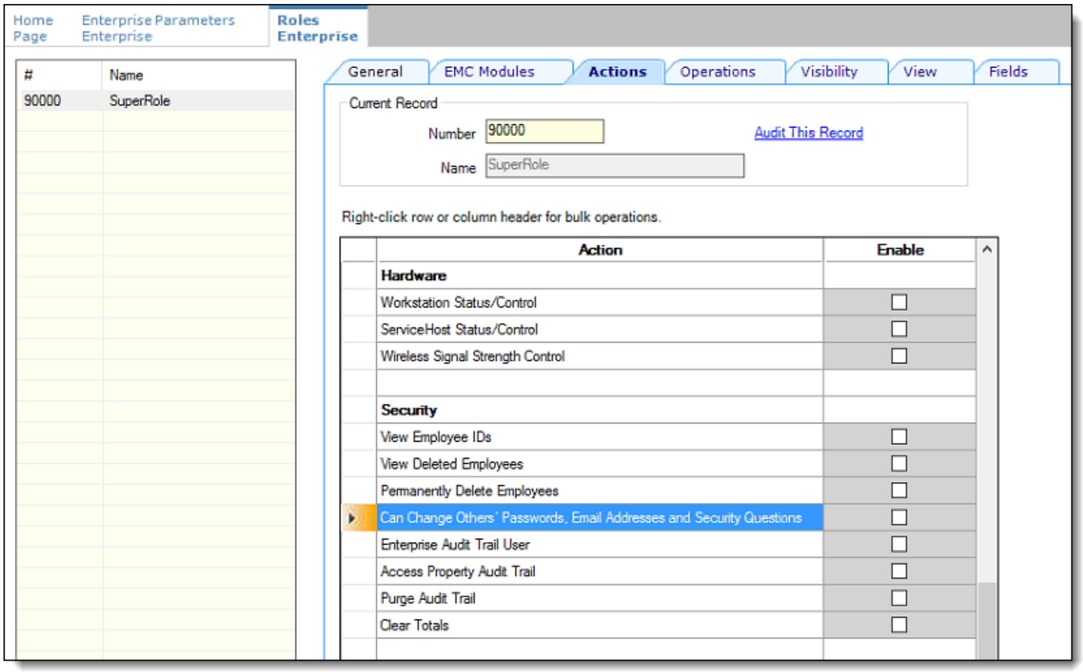
Right-click row or column header for bulk operations.

File	View	Edit	Add	Delete	Add Override	Allow Duplicate Obj#	Allow Duplicate Name	Field Level Security
Print Classes	□	□	□	□	□			
Combo Meal Groups	□	□	□	□	□			
Combo Meals	□	□	□	□	□			
Personnel								
Employees (Enterprise)	☑	☑	☑	☑				
Property Employee Records	□	□	□	□				
Operators	□	□	□	□				
Employee Classes	□	□	□	□				
Roles	□	□	□	□				
Job Codes	□	□	□	□				
Time Clock Schedule	□	□	□	□				
Cashiers	□	□	□	□				
Roles - Reporting	□	□						

Figure 3-2 MFA Access Privilege Roles Configuration

5. Click the **Actions** tab, scroll through the Action column until you reach the Security section, select the **Can Change Others' Passwords and Email Addresses and Security Questions** checkbox, and then click **Save**.

6. Ensure that all users requiring MFA configuration permissions are assigned a Role that have these access privileges enabled.



#	Name
90000	SuperRole

Current Record

Number 90000

Name SuperRole

Right-click row or column header for bulk operations.

Action	Enable
Hardware	
Workstation Status/Control	□
ServiceHost Status/Control	□
Wireless Signal Strength Control	□
Security	
View Employee IDs	□
View Deleted Employees	□
Permanently Delete Employees	□
Can Change Others' Passwords, Email Addresses and Security Questions	□
Enterprise Audit Trail User	□
Access Property Audit Trail	□
Purge Audit Trail	□
Clear Totals	□

Figure 3-3 MFA Access Privilege Roles Configuration - continued

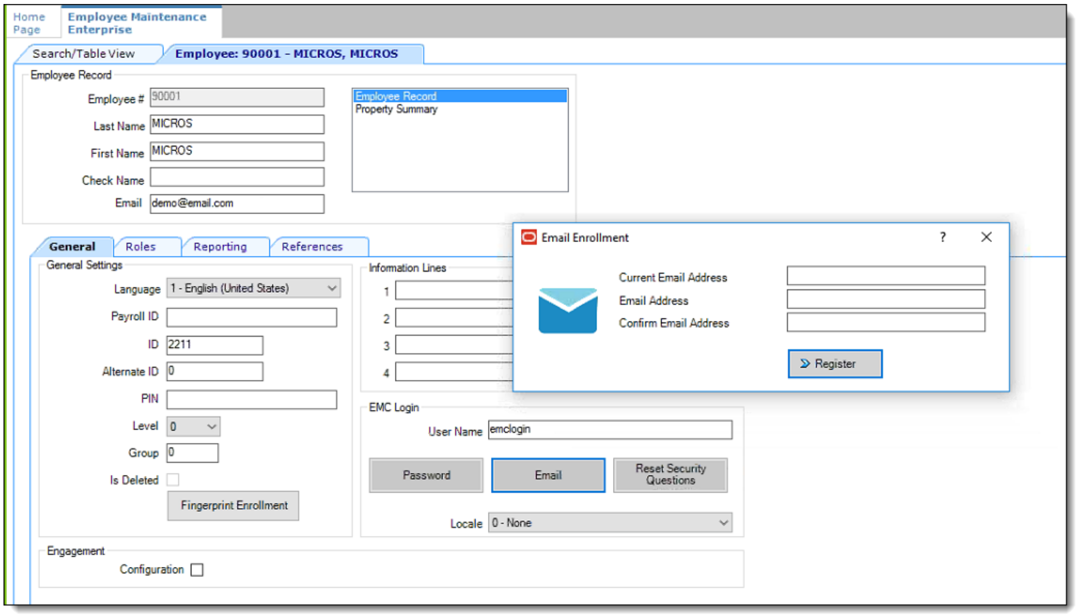
Enrolling Users MFA Email Addresses and Passwords

After enabling MFA, each user that accesses the EMC or Simphony Web Portal (SWP) should register their email address. The system prompts each EMC user to do so. This allows users to receive the OTP via email to complete their EMC login process.

Configuring and Resetting a User’s Email Address for MFA

To enroll a user’s email address using the EMC:

1. Select the **Enterprise** level, click **Configuration**, and then click **Employee Maintenance**.
2. Search for the employee record that requires editing.
3. Click the **Email** button and enter the user’s email address in the **Email Address** field. Re-enter the email address in the **Confirm Email Address** field and click **Register**.



Employee: 90001 - MICROS, MICROS

Employee Record

Employee # 90001

Last Name MICROS

First Name MICROS

Check Name

Email demo@email.com

General Settings

Language 1 - English (United States)

Payroll ID

ID 2211

Alternate ID 0

PIN

Level 0

Group 0

Is Deleted □

EMC Login

User Name emclogin

Locale 0 - None

Engagement

Configuration □

Email Enrollment

Current Email Address

Email Address

Confirm Email Address

Figure 3-4 Employee Email Address Configuration

4. If a user’s email address changes, click the **Email** button and enter the user’s **Current Email Address** (that is already registered on the system), new **Email Address**, and then re-enter the address in the **Confirm Email Address** field and click **Register**.
5. Depending on your Employee Role privilege settings in reference to accessing the Employee Maintenance module, you could also enter or edit the **Email** field for yourself or others.

Setting the Max Allowed Failed Logins for EMC Access

MFA adheres to the following EMC account lock out setting:

1. Select the **Enterprise**, click **Setup**, click **Enterprise Parameters**, and then click the **Login** tab.
2. From the Options section, set the value for the **Maximum Allowed Failed Logins** field.

After reaching the failed login threshold (based on entering an invalid EMC user or OTP password), users are notified that their login was rejected by the system and that their account is currently locked out.

Assigning and Resetting an EMC Password

To assign a user's EMC password (or reset a password due to an account being locked out):

1. Select the **Enterprise** level, click **Configuration**, and then click **Employee Maintenance**.
2. Search for the employee record that requires editing.
3. Click the **Password** button and enter a new password in the **New Password** field. Re-enter the password in the **Confirm New Password** field and click **Accept**.

When the locked out user performs their next successful EMC login, the system prompts to enter a new password (known only to the user).

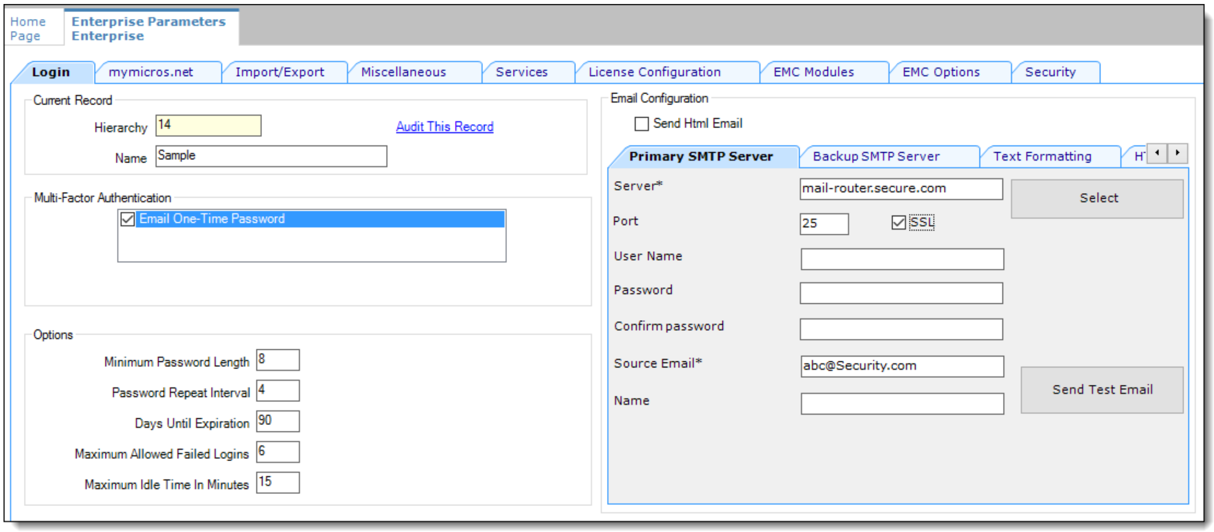
If you are locked out of the EMC, you cannot reset your own password. This is regardless if you have the necessary access privileges assigned to your account. You must notify another privileged user to assist you in resetting your EMC password.

Configuring the SMTP and Backup SMTP Servers in the EMC

SMTP and Backup SMTP server settings are configured and saved at the Enterprise level.

To configure the SMTP servers, navigate the EMC as follows:

1. Select the Enterprise level, click **Setup**, click **Enterprise Parameters**, and then click the **Login** tab.
2. Within the Multi-Factor Authentication section, enable the **Email One-Time Password** option.



Current Record

Hierarchy 14

Name Sample

Multi-Factor Authentication

☑ Email One-Time Password

Options

Minimum Password Length 8

Password Repeat Interval 4

Days Until Expiration 90

Maximum Allowed Failed Logins 6

Maximum Idle Time In Minutes 15

Email Configuration

□ Send Html Email

Server* mail-router.secure.com

Port 25 ☑ SSL

User Name

Password

Confirm password

Source Email* abc@Security.com

Name

Figure 3-5 EMC MFA Configuration

3. From the Email Configuration section, select the **Primary SMTP Server** subtab and enter the required settings in the fields listed below:
   - **Server**: Enter either the IP address or the name of the Primary SMTP server. Click the **Select** button to choose an email provider, and then click **OK**. When you select an email provider, the **Server** field auto-populates with an SMTP server name that includes the selected email provider's naming convention. For example, SMTP.EMAIL.COM.
   - **Port**: Enter a port number or utilize the defaults.
   - **SSL**: Select to enable a secure connection using `HTTPS`.
   - **User Name**: Enter a user name for access to the Primary SMTP server.
   - **Password**: Enter a password for access to the Primary SMTP server and re-enter it in the **Confirm password** field for verification.

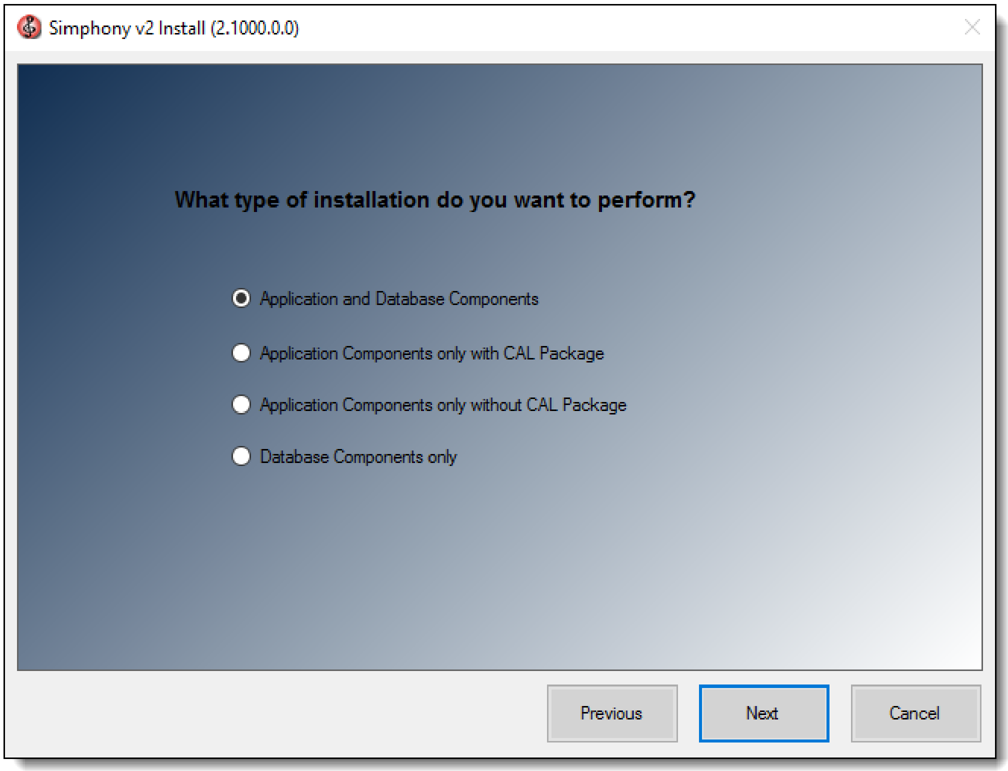
- **Source Email**: Enter your source email address. This email address is used as the sender of all OTP emails.
- (Optional) **Name**: Enter an alternate (alias) name for the Source Email sender.

6. Click the **Backup SMTP Server** subtab and enter the IP address or server name of the Backup SMTP server.
7. Enter information in the fields as listed above for the SMTP Backup server.
8. Click **Save**.
9. On the **Primary SMTP Server** tab, click the **Send Test Email** button to confirm the SMTP server's configuration and that the OTP email is received. Repeat this step on the **Backup SMTP Server** tab to confirm the functionality.

Simphony Installation for an All-in-One Server

The All-in-One server installation scenario is only supported for those using Reporting and Analytics version 8.5.1.

1. Log in and download the Simphony version 2.10 installation application from the Oracle Technology Network (OTN) website at `https://edelivery.oracle.com/`.
2. Run the **Setup** file, and then click **Next** to continue the installation.
3. Select **Application and Database Components,** and then click **Next**.



Simphony v2 Install (2.1000.0.0)

What type of installation do you want to perform?

● Application and Database Components

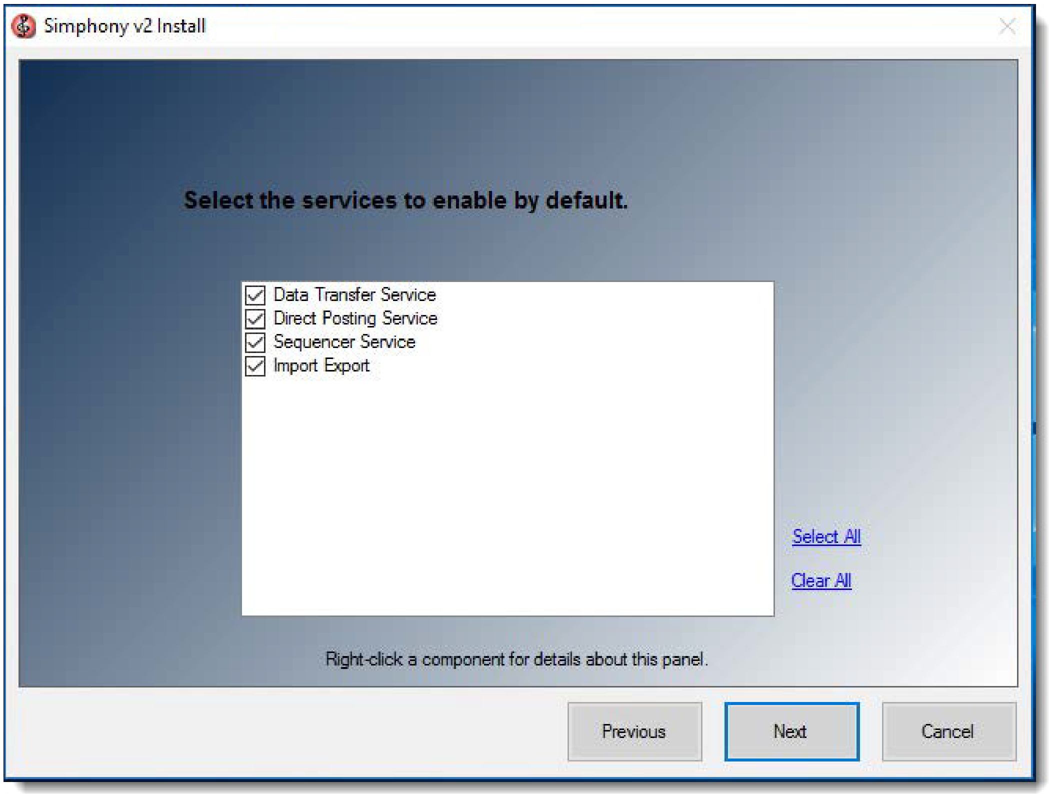
○ Application Components only with CAL Package

○ Application Components only without CAL Package

○ Database Components only

Figure 3-6 Simphony Installation Application

4. Select all **Application and Database Components**, and then click **Next**. See List of Simphony Components and Services for details.
5. Select all of the services, and then click **Next**.



Simphony v2 Install

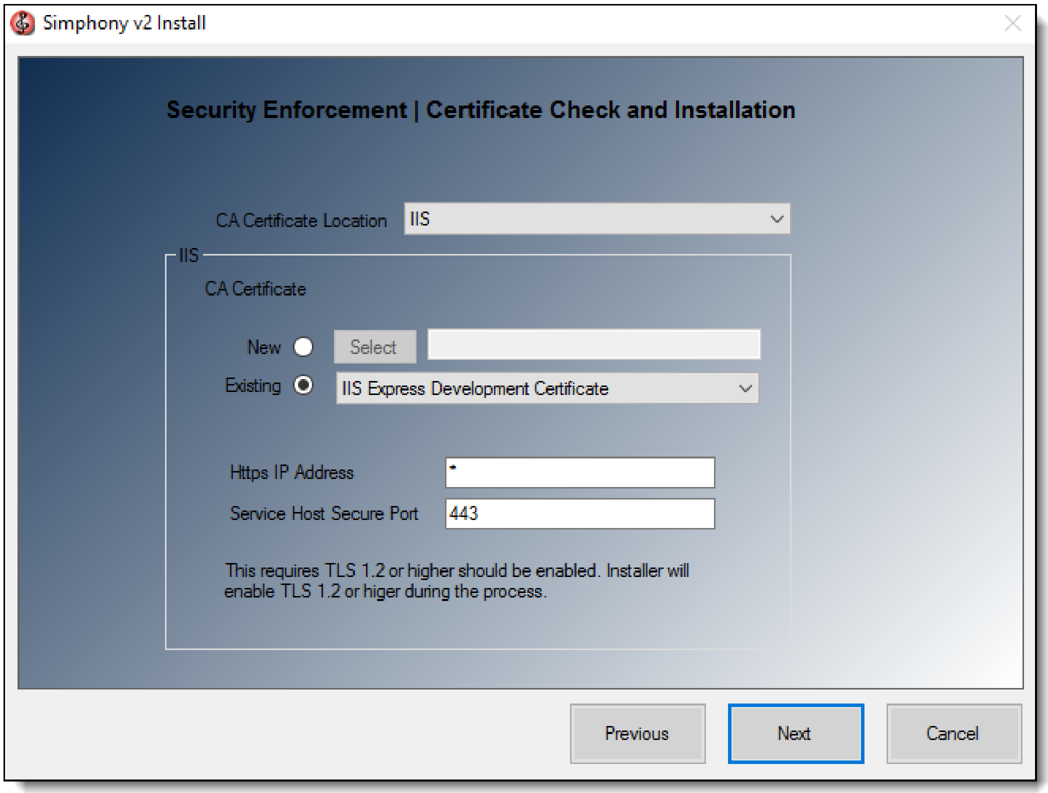
Select the services to enable by default.

☑ Data Transfer Service
☑ Direct Posting Service
☑ Sequencer Service
☑ Import Export

Right-click a component for details about this panel.

Figure 3-7 Simphony Services

6. If are not using a Load Balancing server and are installing the Import/Export Service or plan to use the Engagement Cloud Service:
    a. Select **IIS** for the **CA Certificate Location** field.
    b. To add a new certificate, select New, click Select, enter or select the certificate location, and then enter the Password for the certificate.
    c. To add an existing certificate, select Existing, and then select the certificate from the drop-down.
    d. Enter the **Service Host Secure Port** number.
    If you define a Service Host Secure Port number other than the default of 443, you need to configure the IIS Bindings of each Application Pool to the new port. For information on adding IIS Bindings, refer to the Microsoft TechNet Library at `https://technet.microsoft.com/en-us/` for more information.
7. Click **Next**.



Simphony v2 Install

Security Enforcement | Certificate Check and Installation

CA Certificate Location: IIS

IIS

CA Certificate

New ○ Select

Existing ● IIS Express Development Certificate

Https IP Address: *

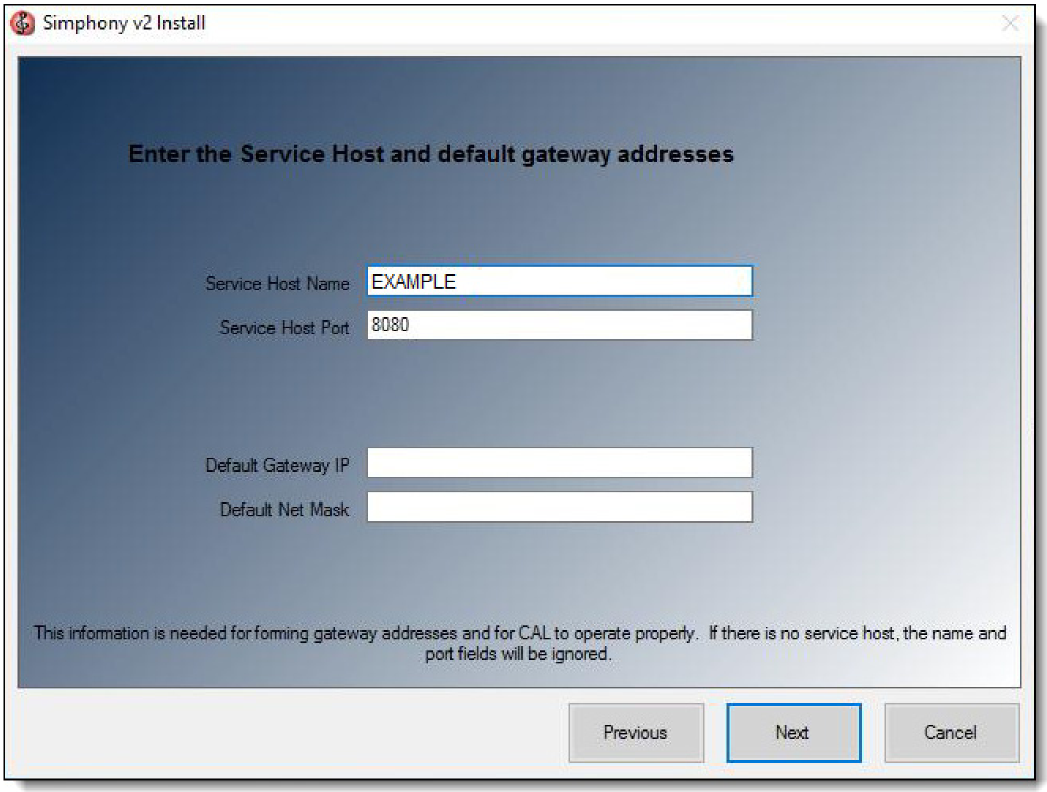
Service Host Secure Port: 443

This requires TLS 1.2 or higher should be enabled. Installer will enable TLS 1.2 or higer during the process.

Figure 3-8 Security Enforcement | Certificate Check

8. Enter the IP address of the server for the **Service Host Name** (computer name). If the server is using a Domain Name System (DNS) or Host file mapping, you can enter the name of the server instead of the IP address. To install Simphony on a named instance of Microsoft SQL Server, enter the Server Host Name as *ServerName\InstanceName*.

9. Enter the **Service Host Port** number.
    - You can define any free port number for the Service Host Port. If you define a port number other than the default 8080, you must manually change the port number when you install subsequent services.
    - If you plan to install Reporting and Analytics on the same server as Simphony, do not assign port number 8081 for the Service Host Port. This is the default port number assigned to the Red Hat JBoss server for Back Office Reports.
10. (Optional) Enter the **Default Gateway IP** and the **Default Net Mask** of the server.
11. Click **Next**.



Simphony v2 Install

Enter the Service Host and default gateway addresses

Service Host Name: EXAMPLE

Service Host Port: 8080

Default Gateway IP:

Default Net Mask:

This information is needed for forming gateway addresses and for CAL to operate properly. If there is no service host, the name and port fields will be ignored.

Figure 3-9 Service Host & Port Number

12. If you are using a Load Balancing server and are installing the Import/Export Service or plan to use the Oracle Hospitality Simphony Engagement Cloud Service, select **LoadBalancer** for the **CA Certificate Location** field.
    If you define a Service Host Secure Port number other than the default of 443, you need to enable that port on the Load Balancer server.

13. Select the database platform, and then click **Next**:
    a. If you are using an Oracle Database, select **Oracle**.
    b. For All-in-One installation scenarios, the installation application installs an Oracle 12c client (even if you are using Oracle Database 11g as a platform). If you are using Oracle Database 12c, the installer will not install an Oracle 12c client.
    c. Click **OK** to install the 12c client if prompted to do so.
    d. If you are using a Microsoft SQL Server database, select **MS-SQL**.
14. Enter or select the location to install Simphony, and then click **Next** twice.

    Oracle Hospitality recommends that you install the Simphony application on a separate partition from where the Microsoft Windows or Oracle Linux operating system resides.
15. To install Simphony with a blank database:
    a. Select **Blank Database**.
    b. Enter a strong **Username** and **Password** to comply with Payment Card Industry (PCI) security guidelines. The credentials that you enter here are used to create the Simphony super user to access the EMC.
    c. Confirm the password, and then click **Next**.
16. To install Simphony with a sample database, select **Sample Database**, click **Next**, and then click **Yes** to continue with the installation.

    Do not use the Sample Database for production systems.
17. If you selected Oracle as the database platform type:
    a. Enter the information to configure the transaction database, and then click **Next**. See List of Simphony Database Configuration Fields for more information on the database setup options.
    b. Enter the credentials for the default SYS user, and then click **OK**.
    c. Enter the information to configure the security database, and then click **Next**.
18. If you selected **MS-SQL** as the database platform type:
    a. Enter or select the location to create the transaction database data files, and then click **Next.** See List of Simphony Database Configuration Fields for more information on the database setup options.
    b. Enter the information to configure the transaction database, and then click **Next**.
    c. Enter the credentials for the SA user, and then click **OK**.
    d. Enter or select the location to create the security DB data files, and then click **Next**.
    e. Enter the information to configure the security database, and then click **Next**.
19. Click **Confirm**.
20. After the installation completes, click **Finish** to exit the Simphony setup.
21. Click **Yes** to restart the computer.

Proceed to the Post-Installation Tasks section to continue.

4 Installing Simphony on Multiple Servers

In a multi-server installation, you install the Simphony application and database components on one or more separate servers.

Installing Simphony on Multiple Servers

The following table outlines the process for installing Simphony on multiple servers, depending on the database platform that you are using.

Table 4-1 Overview of Installing Simphony on Multiple Servers

Database Type	Description	Instructions
Oracle Database	When installing Simphony with an Oracle database, you can install Simphony database components on separate database servers from a remote machine while installing Simphony on the application servers. For property's utilizing separate servers for the Simphony application and databases, an Oracle 12c Client should be installed on all application servers so that it can connect to the remote database server.	1. Create Simphony Database Tablespaces. See Creating Oracle Database Tablespaces. 2. Install the Simphony application components. See Installing Simphony Application Components on One or More Servers. The All-in-One installation scenario is only supported when using R&A version 8.5.1. 3. Run the Simphony installation application to install the Oracle 12c Client on all Simphony application servers.
Microsoft SQL Server	When installing Simphony (prior to the Simphony 2.10 release) with Microsoft SQL Server, you cannot install the databases from a remote machine; you must run the Simphony database setup on the local database servers and install the database components.	1. Install the Simphony database components on the database servers. See Installing Simphony Database Components on Microsoft SQL Server. 2. Install the Simphony application components. Installing Simphony Application Components on One or More Servers. The All-in-One installation scenario is supported when using R&A version 8.5.1.

Installing Simphony Database Components on Microsoft SQL Server

1. Follow all pre-installation tasks for the site. See Pre-Installation Tasks.
2. Follow the instructions in Simphony Installation Tasks.
3. Select **Database Components Only**, and then click **Next**.
4. Select **MS-SQL** as the database platform type, and then click **Next**.
5. Enter or select the location to install Simphony, and then click **Next** twice. Oracle recommends that you install the Simphony application on a separate partition from where the Microsoft Windows operating system resides.
6. To install Simphony with a blank database:
    a. Select **Blank Database**.
    b. Enter a strong **Username** and **Password** to comply with Payment Card Industry (PCI) security guidelines. The credentials that you enter here are used to create the Simphony super user to access the EMC.
    c. Confirm the password, and then click **Next**.
7. To install Simphony with a sample database, select **Sample Database**, click **Next**, and then click **Yes** to continue with the installation.

    Do not install the sample database to be used for an actual food and beverage or retail environment.
8. Enter or select the location to create the transaction database data files, and then click **Next**. See List of Simphony Database Configuration Fields for more information on the database setup options.
9. Enter the information to configure the transaction database, and then click **Next**.
10. Enter the credentials for the SA user, and then click **OK**.
11. Enter or select the location to create the security DB data files, and then click **Next**.
12. Enter the information to configure the security database, and then click **Next**.
13. Click **Confirm**.
14. After the installation completes, click **Finish** to exit the Simphony setup.

Installing Simphony Application Components on One or More Servers

The All-in-One installation scenario is only supported when using R&A version 8.5.1.

1. Ensure that the database server or servers are set up as described in Overview of Installing Simphony on Multiple Servers.
2. On the Simphony application server, follow the instructions in Installing Simphony on Multiple Servers.
3. Select Application Components Only, and then click Next.
4. Select all components, and then click Next. See List of Simphony Components and Services for details.
5. If you are installing all Simphony application components on a single server, select all the services, and then click Next.
6. If you are installing Simphony application components on more than one server:
    a. On the primary application server, select all services and then click **Next**.
    b. On all other application servers, deselect **Sequencer Service**, and then click **Next**.
7. If applicable, follow the instructions in If applicable, follow the instructions in Simphony Installation for an All-in-One Server to complete the installation. When configuring the databases, enter the Server Host Name or IP address, Service Host Name, and logon credentials for the Simphony database servers.
8. Simphony Installation for an All-in-One Server to complete the installation. When configuring the databases, enter the Server Host Name or IP address, Service Host Name, and logon credentials for the Simphony database servers.

Preparing a Multi-Server Environment Using a Load Balancer for the Simphony Import/ Export Service

If you installed Simphony across multiple servers and are using a Load Balancer Server, follow these instructions to prepare the environment for the Import/Export Service:

Table 4-2 Preparing a Multi-Server Simphony Installation Using a Load balancer for the Import/ Export Service

Task	Instructions
Create a shared folder on a central location that all Simphony application servers can access to store the files that you import and export	When creating the shared folder, you must give each application server read/write permissions to the folder. For instructions on how to create a shared folder, refer to the Microsoft TechNet Library at `https://technet.microsoft.com/en-us/library`
On each application server, create a shortcut (map network share drive) to the shared folder, and configure the servers to reconnect to the shared folder upon restarting the server	For instructions on how to map network share drives, refer to the Microsoft TechNet Library at `https://technet.microsoft.com/en-us/library`
Configure the shared folder location in the EMC	In the EMC, select the Enterprise level, click **Setup**, and then click **Enterprise Parameters**. Click the **Import/ Export** tab, and enter the location of the shared folder in the **Root Path for Export/Import File Operations** field (for example, \\HostServerName\ImportExport). Restart the **Data Request Processing Service**.

The *Oracle Hospitality Simphony Configuration Guide* contains more information about the Simphony Import/ Export Service.

5 Upgrading from a Previous Release

Upgrading Reporting and Analytics (R&A)

R&A version 9.0

Prior to upgrading to Simphony version 2.9 or later, upgrade the R&A application server to version 9.0 Patch 8 using the Back Office installation application. See the *Hospitality Enterprise Back Office Installation Guide Release 9.0* for more information about upgrading Reporting and Analytics.

R&A version 8.5.1

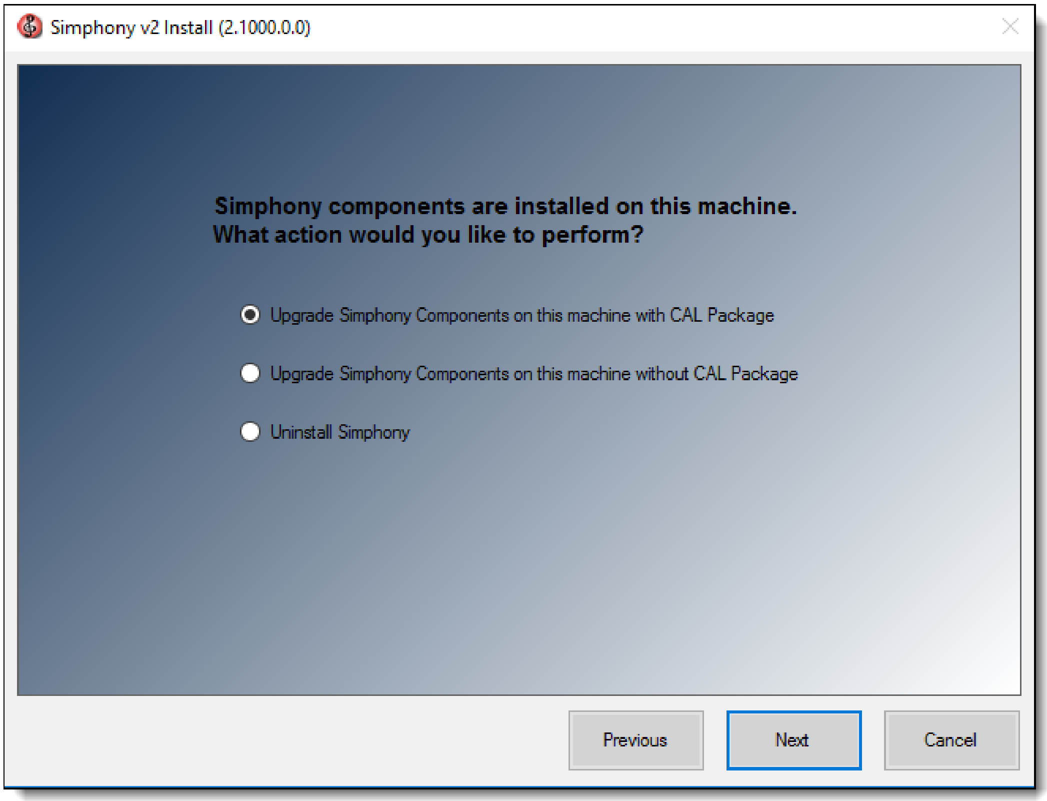
Prior to upgrading to Simphony version 2.9 or later, upgrade the R&A application server to version 8.5.1 Patch 3 using the Back Office installation application. See the *Oracle Hospitality Reporting and Analytics Deployment Guide Release 8.5* for more information about upgrading Reporting and Analytics.

Upgrading to Simphony 2.10

Simphony version 2.10 performs an upgrade to Simphony version 2.7.6.X or later. To enhance your system's security, the Simphony installation application has been recently changed to allow you to physically separate the Transaction (MCRSPOS) database from the Security (MCRSCACHE) database (onto another database server), and then proceed with the upgrade. Oracle Hospitality strongly recommends to store these databases on separate database servers. The following sections review three possible upgrade scenarios:

- Upgrades with Separate Transaction and Security Database Servers (when adding a new database server)
- Upgrades without Separate Transaction and Security Database Servers
- Upgrades with Existing Separated Transaction and Security Database Servers

Beginning with this release you can now upgrade application components on servers with or without downloading CAL Packages. This flexibility helps to speed up the upgrade process on properties utilizing multiple application servers.



Simphony v2 Install (2.1000.0.0)

Simphony components are installed on this machine.
What action would you like to perform?

● Upgrade Simphony Components on this machine with CAL Package

○ Upgrade Simphony Components on this machine without CAL Package

○ Uninstall Simphony

Figure 5-1 Simphony Component Upgrade Choices

Upgrades with Separate Transaction and Security Database Servers (when adding a new database server)

This section provides upgrade instructions to enhance your site's system security. This includes adding a new physical database server to house the site's security database.

If the site uses multiple Simphony application servers, upgrade the initial application server to version 2.10. Then, after upgrading subsequent application servers, ensure that on each application server, that the security database server name matches the `dataSource` entry for the `CACHE` host name located in the application server's DBSettings.xml. This file is located on the initial Simphony application server that was upgraded.

For example:

```
alias="Cache"
dbType="<TYPE> "
dataSource="<SERVERNAME>"
```

To initiate this type of upgrade, perform the following steps:

1. Perform steps 1-5 as shown in Upgrading Simphony Prior to Simphony version 2.10.
2. **Certificate Location** - Throughout the Simphony 2.10 upgrade process, the Simphony installation application checks for the entry of a valid Service Host Name. The following parameters review the installation application's Service Host Name validation behavior:
    a. If Microsoft Internet Information Services (**IIS**) is selected for the **Certificate Location** field, note that the **Service Host Name** (to be entered on the next installation screen) is based on the installed secure certificate's Common Name (CN) field.
    b. **Certificate** - To add a new certificate, select **New**, click **Select**, enter or select the certificate location, and then enter the **Password** for the certificate.

   c. To utilize an existing certificate, select **Existing**, and then select the installed certificate from the drop-down.
   d. If you are using a Load Balancer server and installing the Import/Export Service or plan to use the Oracle Hospitality Simphony Engagement Cloud Service, select **LoadBalancer** for the **Certificate Location** field.

      Note that the **Service Host Name** (to be entered on the next installation screen) is based on the Full Qualified Domain Name (FQDN) of your application server.
   e. **Https IP Address -** Enter the application server's IP address.
   f. **Service Host Secure Port** - If you enter a port number other than the default of 443, you need to enable that port on the Load Balancer server and then click **Next**.

3. When using **IIS**, enter (or verify) the **Service Host Name** (for the Simphony application server).

   If the Service Host Name does not match the installed secure Certificate's CN text, a warning message dialog appears.
   a. Do not ignore the message, select **No**, and then correct the invalid Service Host Name.
   b. Enter the **Default Gateway IP** address and **Default Net Mask** in their corresponding fields, and then click **Next**.
4. When using **LoadBalancer**, enter (or verify) the **Service Host Name** (for the Simphony application server).

   If the Service Host Name does not match the FQDN of your computer, a warning message dialog appears.
   a. Do not ignore the message, select **No**, and then correct the invalid Service Host Name.
   b. Enter the **Default Gateway IP** address and **Default Net Mask** in their corresponding fields, and then click **Next**.
5. Enter the following information that is used to connect to the security database:
   a. **Server Name** - Enter the name of the security database server.
   b. **Service Name** - Oracle Database users - Enter the name of the service (TNS alias).
   c. **Instance Name** - Microsoft SQL Server users - Enter the Microsoft SQL Server's database name (usually contains the database server's name).
   d. **Username** - Enter your security database access user name.
   e. **Password** - Enter your security database access password.
   f. **Database Port** - Enter the port number used to access the security database server, and then click **Next**.
6. Enter your security database administrator **Username** and **Password** logon credentials, and then click **OK** and **Next**.

   If the security database server name and logon credentials entered in step 3, matches the server name where the Transaction database is stored, the installation application prompts and affords users the opportunity to separate the databases onto different database servers. Since you want the two databases separated, click **Yes**.
7. Enter the following information that is used to connect to the secondary database server and then click **Next**:
   a. **Server Name -** Enter the name of the secondary database server. This name should match the `dataSource` entry for the `CACHE` host name located in the application server's DBSettings.xml.

      For example:

      ```
      alias="Cache"
      ```

```
dbType="<TYPE>"
dataSource="<SERVERNAME>"
```

b. **Service Name** - Oracle Database users - Enter the name of the service (TNS alias).

c. **Instance Name** - Microsoft SQL Server users - Enter the Microsoft SQL Server's database name (usually contains the database server's name).

   Per the Pre-Installation Tasks, for Microsoft SQL Server users, the implementation consultant must go to the secondary database server and manually create the folders specified in the **Remote Database Location** field. Alternatively, the implementation consultant can enter the location of previously existing files on the secondary database server. Click **Next**.

d. **Username -** Enter your security database access user name.

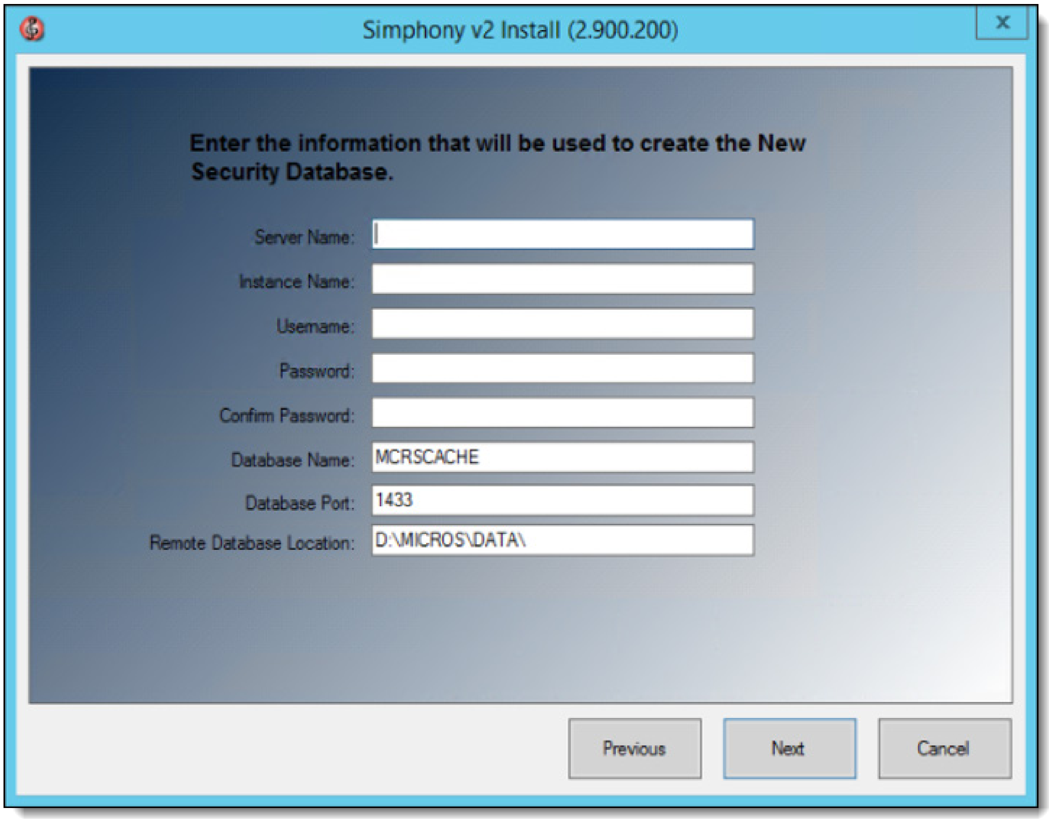
e. **Password -** Enter your security database access password.

f. **Confirm Password -** Re-enter your security database access password.

g. **Database Name** - Enter the name of the security database.

h. **Database Port** - Enter the port number used to access the security database.

i. **Remote Database Location** - Enter the path and folder names where the Security database is to be created.



Enter the information that will be used to create the New Security Database.

Server Name:
Instance Name:
Username:
Password:
Confirm Password:
Database Name: MCRSCACHE
Database Port: 1433
Remote Database Location: D:\MICROS\DATA\

Figure 5-2 Security Database Connection for the Secondary DB Server

8. Enter the logon credentials for a database administrator, and then click **OK**.
   - If you are using an Oracle Database, enter the credentials for the SYS user.
   - If you are using a Microsoft SQL Server database, enter the credentials for the SA user.

9. Enter the following information to connect to the reporting database:

a. **Server Name** – Enter the name of the reporting database server.

b. **Service Name** - Oracle Database users - Enter the name of the service (TNS alias).

c. **Instance Name** - Microsoft SQL Server users - Enter the Microsoft SQL Server's database name (usually contains the database server's name).

d. **Username -** Enter (or verify) your reporting database access user name.

e. **Password -** Enter your reporting database access password.

f. **Database Port** - Enter the port number used to access the reporting database.

g. **Username -** Enter (or verify) your reporting database access user name.

h. **Password -** Enter your reporting database access password, and click **Next**.

10. Enter a database administrator's logon credentials, click **OK**, and then click **Next**.
    - If you are using an Oracle Database, enter the credentials for the SYS user.
    - If you are using a Microsoft SQL Server database, enter the credentials for the SA user.
11. Click **Confirm**. The installation application creates a new user and security database on the secondary database server and drops them from the original database server. When the upgrade is complete, click **Finish**.

Upgrades without Separate Transaction and Security Database Servers

This section provides upgrade instructions for site's that want to maintain their Transaction and Security databases on the same database server.

To initiate this type of upgrade, perform the following steps:

1. Perform steps 1-5 as shown in Upgrading Simphony Prior to Simphony version 2.10.
2. **Certificate Location** - Throughout the Simphony 2.10 upgrade process, the Simphony installation application checks for the entry of a valid Service Host Name. The following parameters review the installation application's Service Host Name validation behavior:

   a. If Microsoft Internet Information Services (**IIS)** is selected for the **Certificate Location** field, note that the **Service Host Name** (to be entered on the next installation screen) is based on the installed secure certificate's Common Name (CN) field.

   b. **Certificate** - To add a new certificate, select **New**, click **Select**, enter or select the certificate location, and then enter the **Password** for the certificate.

   c. To utilize an existing certificate, select **Existing**, and then select the installed certificate from the drop-down.

   d. If you are using a Load Balancer server and installing the Import/Export Service or plan to use the Oracle Hospitality Simphony Engagement Cloud Service, select **LoadBalancer** for the **Certificate Location** field.

   Note that the **Service Host Name** (to be entered on the next installation screen) is based on the Full Qualified Domain Name (FQDN) of your application server.

   e. **Https IP Address -** Enter the application server's IP address.

   f. **Service Host Secure Port** - If you enter a port number other than the default of 443, you need to enable that port on the Load Balancer server and then click **Next**.
3. When using **IIS**, enter (or verify) the **Service Host Name** (for the Simphony application server).

   If the Service Host Name does not match the installed secure Certificate's CN text, a warning message dialog appears.

   a. Do not ignore the message, select **No**, and then correct the invalid Service Host Name.
   b. Enter the **Default Gateway IP** address and **Default Net Mask** in their corresponding fields, and then click **Next**.

4. When using **LoadBalancer**, enter (or verify) the **Service Host Name** (for the Simphony application server).

   If the Service Host Name does not match the FQDN of your computer, a warning message dialog appears.

   a. Do not ignore the message, select **No**, and then correct the invalid Service Host Name.
   b. Enter the **Default Gateway IP** address and **Default Net Mask** in their corresponding fields, and then click **Next**.
5. Enter (or verify) the **Service Host Name** for the Simphony application server, **Default Gateway IP** address, and **Default Net Mask** in their corresponding fields, and then click **Next**
6. Enter the following information that is used to connect to the existing security database, and then click **Next**:
   a. **Server Name** – Enter the name of the database server.
   b. **Service Name** - Oracle Database users - Enter the name of the service (TNS alias).
   c. **Instance Name** - Microsoft SQL Server users - Enter the Microsoft SQL Server's database name (usually contains the database server's name).
   d. **Username** – Enter your security database access user name.
   e. **Password** – Enter your security database access password.
   f. **Database Port** – Enter the port number used to access the security database server, and click **Next**.
7. Enter the following information to connect to the reporting database:
   a. **Server Name** – Enter the name of the reporting database server.
   b. **Service Name** - Oracle Database users - Enter the name of the service (TNS alias).
   c. **Instance Name** - Microsoft SQL Server users - Enter the Microsoft SQL Server's database name (usually contains the database server's name).
   d. **Username -** Enter (or verify) your reporting database access user name.
   e. **Password -** Enter your reporting database access password.
   f. **Database Port** - Enter the port number used to access the reporting database.
   g. **Username -** Enter (or verify) your reporting database access user name.
   h. **Password -** Enter your reporting database access password, and click **Next**.
8. Enter a database administrator's logon credentials, click **OK**, and then click **Next**.
   - If you are using an Oracle Database, enter the credentials for the SYS user.
   - If you are using a Microsoft SQL Server database, enter the credentials for the SA user.
9. Click **Confirm**. The installation application creates a new user and security database on the secondary database server and drops them from the original database server. When the upgrade is complete, click **Finish**.

Upgrades with Existing Separated Transaction and Security Database Servers

This section provides upgrade instructions for site's that already have separate Transaction and Security database servers.

To initiate this type of upgrade, perform the following steps:

1. Perform steps 1-5 as shown in Upgrading Simphony Prior to Simphony version 2.10.
2. **Certificate Location** - Throughout the Simphony 2.10 upgrade process, the Simphony installation application checks for the entry of a valid Service Host Name. The following parameters review the installation application's Service Host Name validation behavior:
   a. If Microsoft Internet Information Services (**IIS)** is selected for the **Certificate Location** field, note that the **Service Host Name** (to be entered on the next installation screen) is based on the installed secure certificate's Common Name (CN) field.
   b. **Certificate** - To add a new certificate, select **New**, click **Select**, enter or select the certificate location, and then enter the **Password** for the certificate.
   c. To utilize an existing certificate, select **Existing**, and then select the installed certificate from the drop-down.
   d. If you are using a Load Balancer server and installing the Import/Export Service or plan to use the Oracle Hospitality Simphony Engagement Cloud Service, select **LoadBalancer** for the **Certificate Location** field.

      Note that the **Service Host Name** (to be entered on the next installation screen) is based on the Full Qualified Domain Name (FQDN) of your application server.
   e. **Https IP Address -** Enter the application server's IP address.
   f. **Service Host Secure Port** - If you enter a port number other than the default of 443, you need to enable that port on the Load Balancer server and then click **Next**.
3. When using **IIS**, enter (or verify) the **Service Host Name** (for the Simphony application server).

   If the Service Host Name does not match the installed secure Certificate's CN text, a warning message dialog appears.
   a. Do not ignore the message, select **No**, and then correct the invalid Service Host Name.
   b. Enter the **Default Gateway IP** address and **Default Net Mask** in their corresponding fields, and then click **Next**.
4. When using **LoadBalancer**, enter (or verify) the **Service Host Name** (for the Simphony application server).
   a. If the Service Host Name does not match the FQDN of your computer, a warning message dialog appears.
   b. Do not ignore the message, select **No**, and then correct the invalid Service Host Name.
5. Enter the **Default Gateway IP** address and **Default Net Mask** in their corresponding fields, and then click **Next**.

6. Enter the following information that is used to connect to the existing security database, and then click **Next**:
    a. **Server Name** – Enter the name of the existing security database server.
    b. **Service Name** - Oracle Database users - Enter the name of the service (TNS alias).
    c. **Instance Name** - Microsoft SQL Server users - Enter the Microsoft SQL Server's database name (usually contains the database server's name).
    d. **Username** – Enter your security database access user name.
    e. **Password** – Enter your security database access password.
    f. **Database Port** – Enter the port number used to access the security database server, and click **Next**.
7. Enter the following information to connect to the Reporting database:
    a. **Server Name** – Enter the name of the reporting database server.
    b. **Service Name** - Oracle Database users - Enter the name of the service (TNS alias).
    c. **Instance Name** - Microsoft SQL Server users - Enter the Microsoft SQL Server's database name (usually contains the database server's name).
    d. **Username -** Enter (or verify) your reporting database access user name.
    e. **Password -** Enter your reporting database access password.
    f. **Database Port** - Enter the port number used to access the reporting database.
    g. **Username -** Enter (or verify) your reporting database access user name.
    h. **Password -** Enter your reporting database access password, and click **Next**.
8. Enter a database administrator's logon credentials, click **OK**, and then click **Next**.
    - If you are using an Oracle Database, enter the credentials for the SYS user.
    - If you are using a Microsoft SQL Server database, enter the credentials for the SA user.
9. Click **Confirm**. When the upgrade is complete, click **Finish**.

Upgrading Simphony Prior to Simphony version 2.10

1. Ensure that the Simphony application and database servers meet the requirements listed in Chapter 2.
2. Log in and download the Simphony version 2.10 installation application from the Oracle Technology Network (OTN) website at `https://edelivery.oracle.com/`.
3. Run the **Setup** and click **Next**.

    If you have the application and the database on separate servers, run the installation application on the application server.
4. Enter the logon credentials for a database administrator, and then click **OK.**
    - If you are using an Oracle Database, enter the credentials for the SYS user.
    - If you are using Microsoft SQL Server, enter the credentials for the SA user.
5. Select **Update Application Components on this machine**, and then click **Next**.
6. If you are using a Load Balancer server and installing the Import/Export Service or plan to use the Oracle Hospitality Simphony Engagement Cloud Service, select **LoadBalancer** for the **Certificate Location** field.

    If you define a **Service Host Secure Port** number other than the default of 443, you need to enable that port on the Load Balancer server.

7. If you are not using a Load Balancer server and are installing the Import/Export Service or plan to use the Engagement Cloud Service:
    a. Select **IIS** for the **Certificate Location** field.
    b. To add a new certificate, select **New**, click **Select**, enter or select the certificate location, and then enter the **Password** for the certificate.
    c. To utilize an existing certificate, select **Existing**, and then select the installed certificate from the drop-down.
    d. Enter the **Service Host Secure Port**.
    If you define a **Service Host Secure Port** number other than the default of 443, you need to configure the IIS Bindings of each Application Pool to the new port. For information on adding IIS Bindings, refer to the Microsoft TechNet Library at `https://technet.microsoft.com/en-us/` for more information.
8. If you are connected to Reporting and Analytics, enter the passwords for the MMSQL and CEDB database users, and then click **Next**.
9. If you have Reporting and Analytics installed and want to connect to it, click **Yes** when prompted, enter the information to connect to the reporting database, and then click **Next**.
10. Click **Next**, and then click **Confirm** to begin the upgrade.

Post-Upgrade Tasks

The following table lists the tasks you must perform after upgrading to Simphony version 2.9 or later from an earlier release.

Table 3 Post-Upgrade Tasks for Simphony Version 2.9 (or later)

Post-Upgrade Task	Instructions
Update the Property's Admin and Database Credentials	Updating Property Administrator and Database Logon Credentials contains more details and instructions.
Update the Simphony License Counts	Updating Simphony License Counts contains more details and instructions.
Update all Check and Posting Service (CAPS) clients prior to updating workstations with the latest CAL Packages.	Post-Upgrade Steps for CAPS on IIS for Simphony 2.9 Users and Oracle Hospitality Simphony Configuration Guide, specifically the *Check and Posting Service (CAPS)* contain more important details and instructions.
Update or verify your CAL Packages and schedule their deployment to your workstation clients.	*Client Application Loader (CAL)* in the Oracle Hospitality Simphony Configuration Guide for more information about configuring and deploying CAL Packages.
If you installed the Simphony Import/ Export Service on a multi-server Simphony installation, create a shared folder on a central location to store the import/export files	Preparing a Multi-Server Environment Using a Load Balancer for the Simphony Import/ Export Service contains more details and instructions.

Post-Upgrade Steps for CAPS on IIS for Simphony 2.9 Users

This section only applies if you are upgrading from the Simphony 2.9 General Release (GR) and are using either an Oracle or Microsoft SQL Server database platform, and are upgrading to Simphony 2.10 or later.

Note: No additional post-upgrade steps are necessary for CAPS on Microsoft Internet Information Services (IIS) if you upgrade from Simphony versions later than Simphony 2.9 GR. For example, Simphony versions 2.9.3, and 2.10 or later.

Perform these steps in IIS after upgrading from Simphony 2.9 GR to the Simphony 2.10 release or later:

Step 1- Close and Post All Transactions

Ensure that all transactions are closed and posted to the Enterprise prior to performing the Simphony upgrade.

Step 2- Access the IIS Manager Console

1. From the desktop of each server running CAPS on IIS, select **Start**, **Control Panel**, **Administrative Tools**, and then select **Internet Information Services (IIS) Manager**.

2. From the IIS Connections column, expand the **Sites** folder and right-click on the site created for IIS CAPS and select **Remove**. The name of the IIS CAPS site should be the same as the *ServiceHostName*. For example, if your service host name is MyIISCapsSvcHost, your site name should be added using the exact same text.

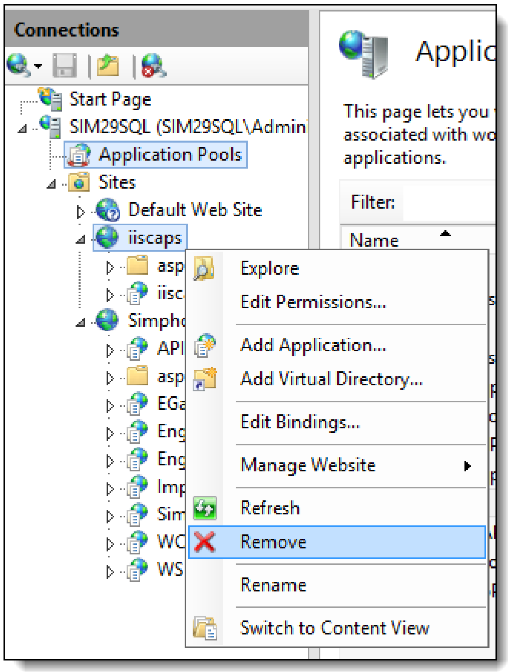


Figure 5-3 IIS CAPS Site

3. From the IIS Connections column, click **Application Pools**.

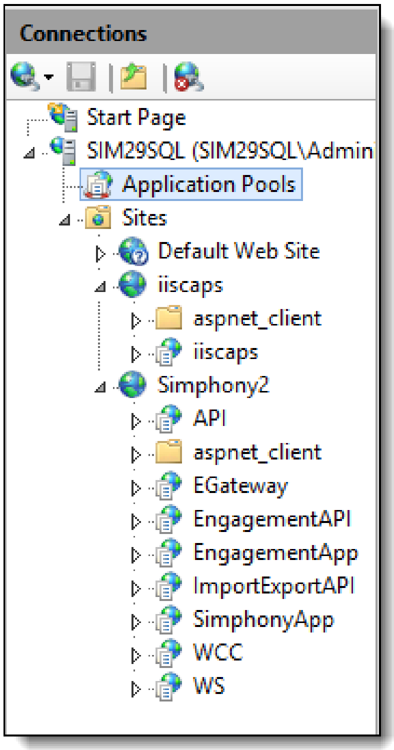


Figure 5-4 Simphony Application Pools

4. Right-click on the application pool created for IIS CAPS and select **Remove**. The name of the IIS CAPS pool should be the *ServiceHostName*Pool. For example, if your service host name is MyIISCapsSvcHost, your IIS CAPS application pool name should be MyIISCapsSvcHostPool.

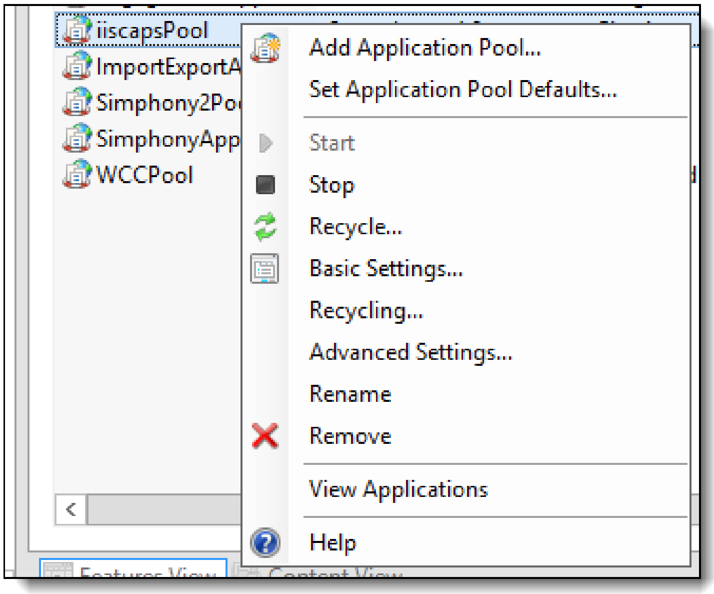
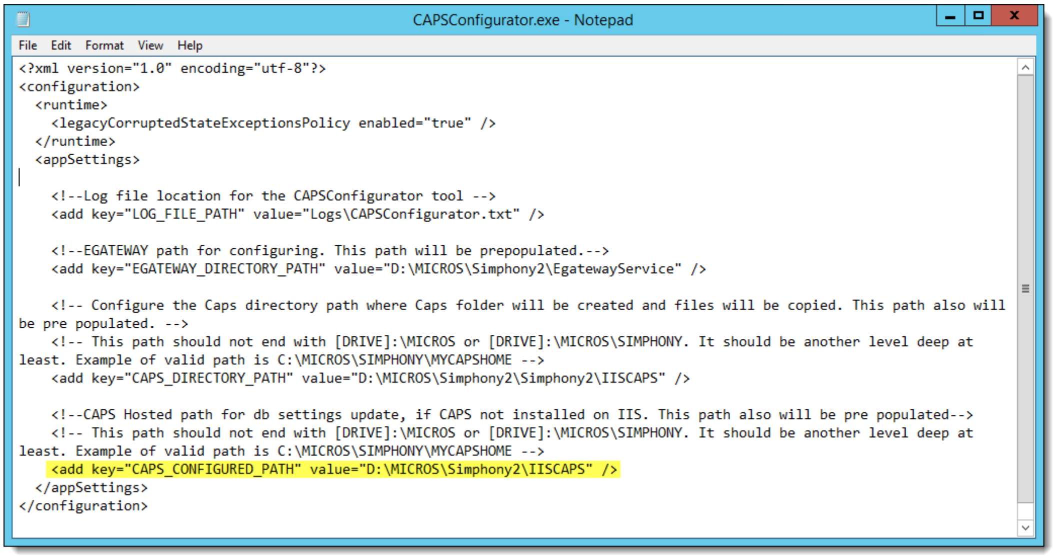


Figure 5-5 IIS CAPS Application Pool

Step 3- Rename the IIS Folder

1. Rename the Simphony version 2.9 IIS CAPS folder.

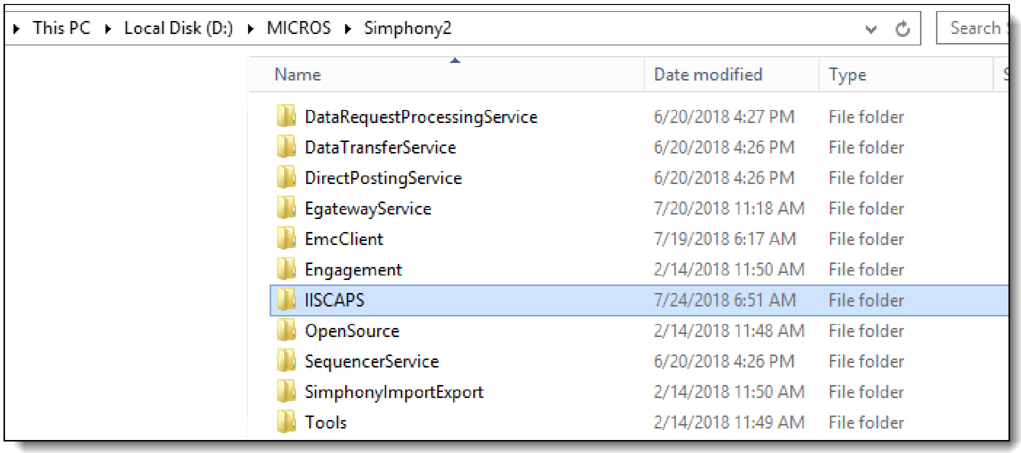
    a. Verify the installed folder path by navigating to the `[Drive]:\MICROS\Simphony2\Tools\CAPSConfigurator\`**`CAPSConfigurator.exe.config`** file and open it with a text editor such as Microsoft Notepad.



```
<?xml version="1.0" encoding="utf-8"?>
<configuration>
  <runtime>
    <legacyCorruptedStateExceptionsPolicy enabled="true" />
  </runtime>
  <appSettings>

    <!--Log file location for the CAPSConfigurator tool -->
    <add key="LOG_FILE_PATH" value="Logs\CAPSConfigurator.txt" />

    <!--EGATEWAY path for configuring. This path will be prepopulated.-->
    <add key="EGATEWAY_DIRECTORY_PATH" value="D:\MICROS\Simphony2\EgatewayService" />

    <!-- Configure the Caps directory path where Caps folder will be created and files will be copied. This path also will
be pre populated. -->
    <!-- This path should not end with [DRIVE]:\MICROS or [DRIVE]:\MICROS\SIMPHONY. It should be another level deep at
least. Example of valid path is C:\MICROS\SIMPHONY\MYCAPSHOME -->
    <add key="CAPS_DIRECTORY_PATH" value="D:\MICROS\Simphony2\Simphony2\IISCAPS" />

    <!--CAPS Hosted path for db settings update, if CAPS not installed on IIS. This path also will be pre populated-->
    <!-- This path should not end with [DRIVE]:\MICROS or [DRIVE]:\MICROS\SIMPHONY. It should be another level deep at
least. Example of valid path is C:\MICROS\SIMPHONY\MYCAPSHOME -->
    <add key="CAPS_CONFIGURED_PATH" value="D:\MICROS\Simphony2\IISCAPS" />
  </appSettings>
</configuration>
```

Figure 5-6 CAPSConfigurator.exe.config IIS CAPS Directory Installation Folder Path

    b. Note that the default Simphony version 2.9 IIS CAPS folder location is: `[Drive]:\Simphony2\IISCAPS`. Rename the **IISCAPS** folder to **IISCAP_Backup**. This step ensures you maintain a backup of the old folder.

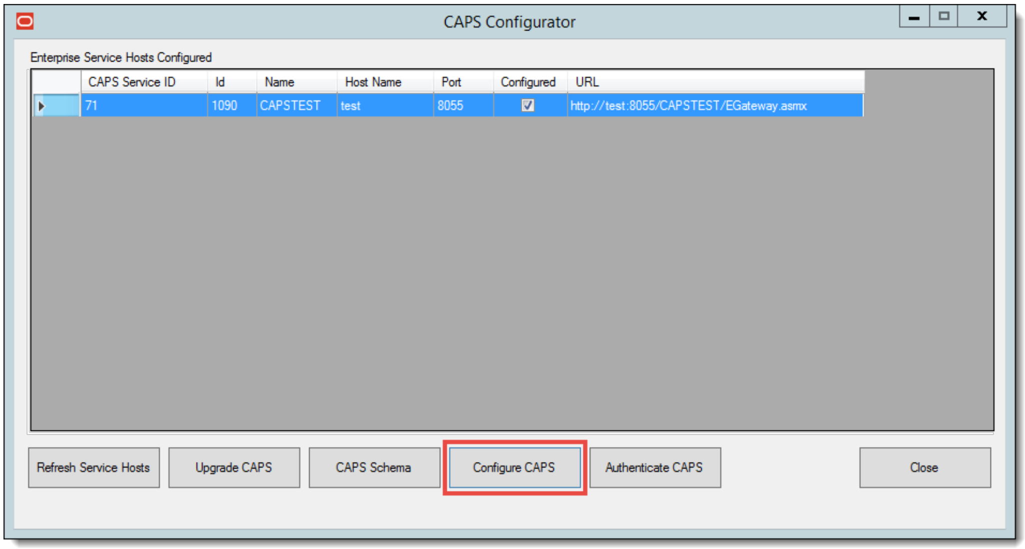


Name	Date modified	Type
DataRequestProcessingService	6/20/2018 4:27 PM	File folder
DataTransferService	6/20/2018 4:26 PM	File folder
DirectPostingService	6/20/2018 4:26 PM	File folder
EgatewayService	7/20/2018 11:18 AM	File folder
EmcClient	7/19/2018 6:17 AM	File folder
Engagement	2/14/2018 11:50 AM	File folder
IISCAPS	7/24/2018 6:51 AM	File folder
OpenSource	2/14/2018 11:48 AM	File folder
SequencerService	6/20/2018 4:26 PM	File folder
SimphonyImportExport	2/14/2018 11:50 AM	File folder
Tools	2/14/2018 11:49 AM	File folder

Figure 5-7 Default IIS CAPS Folder Installation Path

Step 4- Enable an Option and Configure CAPS

1. Access EMC and navigate to the Enterprise level, click the **Configuration** tab, and then click **Roles**.
2. Click on your assigned Role and toggle to **Form** view. Click on the **Operations** tab, and then click the **Miscellaneous** subtab. Under Miscellaneous Options, enable option **10065 - Download Software, Install and Authenticate Clients and Service Hosts Using CAL** and **Save**.
3. Logon to the **CAPS Configurator Tool** (using the CAPSConfigurator.exe**)** and freshly configure CAPS with the default configuration settings by clicking the **Configure CAPS** button. Upon successful installation, verify the new directory created under `[Drive]:\Simphony2\EgatewayService\IISCAPSServiceHost` path.



Enterprise Service Hosts Configured

	CAPS Service ID	Id	Name	Host Name	Port	Configured	URL
▶	71	1090	CAPSTEST	test	8055	☑	http://test:8055/CAPSTEST/EGateway.asmx

Figure 5-8 CAPS Configurator Tool

Step 5- Stop IIS

Stop IIS by:

1. Run the command window with administrator privileges.
2. Enter the `iisreset /stop` command and press **Enter**.

Step 6- Move the DbSettings.xml to the Newly Defined IIS CAPS Path

1. Copy the **DbSettings.xml** file from the old path (review Step 3- Rename the IIS Folder above, and verify the default CAPS IIS installation path), and then using Microsoft Windows Explorer, navigate to that path. For example, `[Drive]:\Simphony2\IISCAP_Backup\IISCAPS\DbSettings.xml`.
2. Paste the **DbSettings.xml** file to the new path: `[Drive]:\Simphony2\EgatewayService\IISCAPSServiceHost`
3. Edit the **DbSettings.xml** file to update the CAPS database password; this means to delete the previously existing password value on epw (encrypted format) and enter the password again with pwd (ClearText). For example:

```
<root>
    <db
        alias="CPServiceDb"
        dbType="sqlserver"
        dataSource="xxxx"
        catalog="xxxxxxx"
        uid="xxxxxxxxx"
        pwd=”CAPSDBPassword”
        port="1433" />
</root>
```

Step 7- Start IIS

Start IIS by:

1. Run the command window with administrator privileges.
2. Type the `iisreset /start` command and press **Enter**.

Step 8- Verify Log Creation, Database Tables, and Delete the Old Directory

1. Verify that logs are created here: `[Drive]:\Simphony2\EgatewayService\IISCAPSServiceHost\EgatewayLog.`
2. Verify that the tables are upgraded on the existing transaction database.
3. Delete the Simphony version 2.9 CAPS directory, for example the IISCAP_Backup directory (review Step 3- Rename the IIS Folder above).

6 Post-Installation Tasks

Update the Property EMC Client

The Enterprise Management Console (EMC) is the primary configuration application in Simphony. A shortcut for accessing EMC is installed on the application server during the installation.

Self-hosted customers also need to follow these steps to configure Remote EMC clients. Remote EMC clients allow users to access the EMC from other computers on the network.

1. Open a browser and navigate to `http://ApplicationServerName:PortNumber/egateway/download/EMCClient/`, and then click **EMCSetup.exe**.
2. If you see the Unknown Publisher warning, click **Run**.
3. On the **Welcome** screen, click **Next**.
4. Set the destination folder, and then click **Next**.
5. Enter the IP address or the name of the Simphony application server with the EGateway port number (for example, `http://192.168.220.224:8080`), and then click **Next**.
6. Click **Install**.
7. Click **Finish** to exit the installer.
8. Double-click the **AppLoader** icon on the desktop to launch the remote EMC.
   The AppLoader also updates the remote EMC with the same versions of files that are on the Simphony application server.

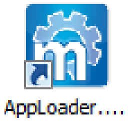


Figure 6-1 AppLoader Icon

Updating Simphony License Counts

To edit the system’s license counts:

1. In the EMC, select the Enterprise level, click **Setup**, and then click **Enterprise Parameters**.
2. Click the **License Configuration** tab.
3. Click **Configure** adjacent to **Workstations Client License Count**.
4. To add a new license count, select **I would like to set the license count to X, making the new license count X**.
5. To append licenses to an existing license count, select **I would like to add X to the current license count, making the new license count X**.
6. Enter the number of client licenses purchased.
7. (Optional) Enter additional details regarding the purchased license in the **Enter Reference Information for the License Count Change**, and then click **OK**.
8. Repeat Steps 3 through 7 for Engagement Client License Count, Transaction Service Client License Count, and KDS Client License Count.
9. Click **Save,** and then click **Yes** to agree to the license.

To perform a side by side comparison of the number of purchased licenses against the number of configured clients:
Click the **Licensing Configuration** tab, and then click **View** adjacent to the Properties, Revenue Centers, Concessions Terminals, Workstation Client License Count, Engagement Client License Count, Transaction Services Client License Count, or KDS Client License Count labels.

Updating Property Administrator and Database Logon Credentials

When logging in to the EMC for the first time after installing or upgrading to Simphony version 2.9 and later, a message indicates that the property credentials are not compliant with the Simphony standards. To keep the properties safe from security risks, you need to update the Admin and Database credentials, which Simphony uses to create and maintain the workstation databases. Simphony offers the options of configuring security credentials for each property separately or using the same credentials for all properties in the Enterprise. Simphony requires that you update the system and database administrator credentials every 90 days. If you do not update the credentials, EMC shows the Database Credentials Non-Compliance message each time you log in until you meet the compliance.

To configure credentials for each non-compliant property separately:

1. In the EMC, select the Enterprise level, click Setup, and then click Properties.
2. In table view, scroll to the right until you see the Admin Credentials and the Database Credentials columns. If a property is not compliant, the Admin Credentials and the Database Credentials columns are highlighted in red.
3. Click either the Admin Credentials or the Database Credentials column of the non-compliant property, and go to the Property Parameters module.
4. Click the Security tab.
5. Enter User Security Credentials. Simphony uses these credentials to authenticate the workstations.

   The Install User Security Username must have at least two characters and must not contain a company name, product name, common words, or Structured Query Language (SQL) keywords (for example, Micros, Oracle, abcd, 1234, and so on).

   The Install User Security Password must have a minimum of eight characters and adhere to the Oracle Database standards.
6. Enter the Current Password of the Admin User.
7. Enter a new strong password for the Admin User.

   See Database User Passwords for more information about password requirements.
8. Repeat Steps 6 and 7 for the Database User, and then click **Save**.
9. Repeat Steps 3 through 8 for all non-compliant properties.

To configure the same credentials for all non-compliant properties in the Enterprise:

1. In the EMC, select the Enterprise level, click **Setup**, and then click **Enterprise Parameters**.
2. Click the **Security** tab, and then select **Use Same Credentials for All Properties**.
3. Select the property whose credentials you want to use, and then enter the **New Install User Security Password**.
4. Re-enter the new security password in the **Confirm User Security Password** field, and then click **Save**.

Configuring IIS Application Pool Settings

Configure Recycle Settings for the IIS Application Pool

If you configure the application pool to recycle at a scheduled time using the IIS Manager, consider configuring the following recycle settings for the IIS Application Pools:

- Ensure that the Specific time(s) you define does not coincide with your Start-of-Day (SOD) or periods of peak sales activity
- Set the Memory Based Maximums to less than half of the available server memory
- Set the Simphony2 App Pool Pipeline mode to Classic
- Set the Disable Overlapped Recycle setting to True for the Simphony2 App Pool

In addition to the Simphony2 App Pool, the following IIS App Pools are also installed:

- ImportExportAPIPool - for the Import Export Service
- ImportExportAppPool - for the Import Export Service
- WCCPool - for the Engagement feature

These App Pool's Pipeline mode settings can remain on their default settings.

For instructions on configuring an application pool to recycle at a scheduled time, refer to the Microsoft TechNet Library at `https://technet.microsoft.com/en-us/`.

After the Simphony Installation

If You Installed the Blank Database

1. Open the **EMC** from the shortcut on the desktop or **Start** menu.
2. Enter the **Application Server Host Name**:
    a. If you are launching EMC locally from the server, enter localhost for the Application Server Host Name.
    b. If you are accessing the EMC remotely, enter the Server Host Name or IP address of the Simphony application server.
3. Enter the logon credentials for the Simphony super user that you created in Step 15 of Simphony Installation Tasks.
4. Click **Login**.
5. Click **OK** for the EMC Database Credentials Non-Compliance message.

If you can launch and see the EMC and the Simphony Gateway is up and running, Simphony is successfully installed.

If You Installed the Sample Database

1. Open the **EMC** from the shortcut on the desktop or **Start** menu.
2. Enter the **Application Server Host Name**:

   a. If you are launching EMC locally from the server, enter localhost for the application Server Host Name.
   b. If you are accessing the EMC remotely, enter the Server Host Name or IP address of the Simphony application server.
3. Log on to the EMC with:
   - Username = micros
   - Password = micros
4. Click **OK** when prompted to update the password.
5. Enter a new strong password (per PCI DSS 8.2.3 / PA-DSS 3.1.6 standards) for the Simphony super user, and then click **Accept.** If you are using an Oracle Database, refer to the *Oracle Database Security Guide* for more information about configuring password protection.
6. Click **OK** when prompted to update the username.
7. Enter a new username for the EMC super user, and then click **Accept**.
8. Click **Login**.
9. Click **OK** for the EMC Database Credentials Non-Compliance message.

If you can see the EMC dashboard, the Simphony gateway is up and Simphony is installed successfully.

Setting the Start-Of-Day Sequencer Machine and the App Server Time Zone

1. In the EMC, select the Enterprise level, click the Setup tab, and then click **Enterprise Parameters**.
2. Click the **Miscellaneous** tab.
3. Enter the Windows machine name for SOD Sequencer Machine Name.
4. Select the **App Server Time Zone**.
5. If you are deploying Simphony on multiple servers, the date, time, and the time zone settings of each app server and database server must correspond. Additionally, the servers' time zone must correspond with the App Server Time Zone setting in the EMC.
6. You can synchronize the time settings between the servers by configuring one of the servers to be a Network Time Protocol (NTP) server and then point the rest of the servers to the NTP server. For information on setting up a Network Time Protocol server, refer to the Microsoft TechNet Library at `https://technet.microsoft.com/en-us/` for more information.
7. Click **Save**.
8. If you installed Simphony on multiple application servers, disable the **Micros Sequencer Service** on all servers other than the SOD Sequencer Machine.
9. In the event the application server that is running the Micros Sequencer Service has performance issues, start the Micros Sequencer Service on another Simphony application server if the main application server is going to be down for multiple days.

Connecting Reporting and Analytics to Simphony

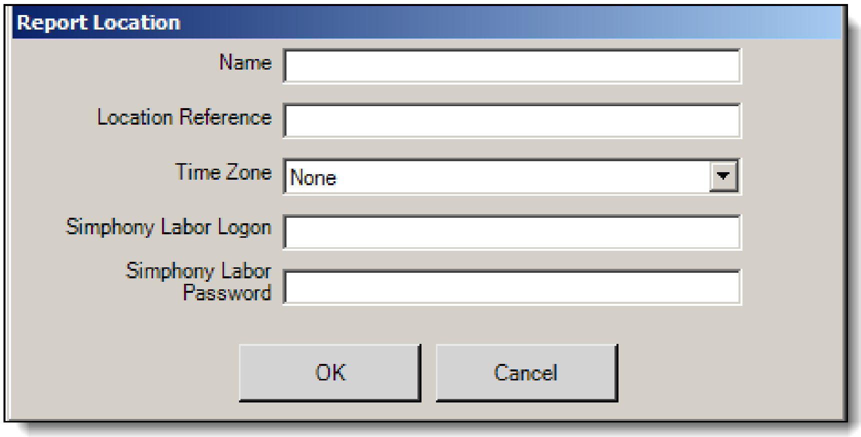
With the release of Simphony version 2.10 or later, if you utilize Reporting and Analytics (R&A) version 9.0 Patch 8, the steps outlined below are no longer required. Core Simphony reports are now available to set up by default from within the R&A application.

If you are utilizing R&A version 8.5.1, the following steps are still applicable. Before you connect to R&A, you need to have:

- At least one property in the Enterprise. The *Oracle Hospitality Simphony Configuration Guide* contains more information about adding properties to the Enterprise.
- Organizations and report locations created in R&A for your properties in the Enterprise. See the *Hospitality Enterprise Back Office Installation Guide* for more information about the prerequisite configurations that are required when creating Organizations and report locations.

To identify the location of Reporting and Analytics on the system, perform the following steps:

1. In the EMC, select the Enterprise level, click the **Setup** tab, click **Enterprise Parameters**, and then click the **mymicros.net** tab.
2. In the **mymicros.net Machine Name** field, enter the name of the computer that is running the MICROS Portal Service.
3. Select the Enterprise level**,** click the **Setup** tab, and then click **Properties**.
4. Double-click a property to open in form view.
5. Select the **Report Location** for the property. If the Report Location is not available in the drop-down, click **New**, and then create a Report Location.
6. Complete each field (required). Here are some recommendations:
    - Use the property name as the **Name**
    - Use the Property ID as the **Location Reference** (this must be unique)
    - Select the **Time Zone** from the drop down that matches the property's time zone
    - Enter a user name in the **Simphony Labor Logon** field (this must be unique)
    - Enter a password for **Simphony Labor Password** (this must be unique)
7. Click **OK,** and then click **Save**.



Report Location

Name

Location Reference

Time Zone: None

Simphony Labor Logon

Simphony Labor Password

Figure 6-2 Property Report Location

8. Repeat Steps 2 through 6 for all properties in the Enterprise.

Enabling Communication Between the Enterprise and Workstations

To allow the workstations in the property to communicate with the Enterprise, you must add Firewall exceptions for the following services on your Simphony application servers using either the default ports or the ports you assign when installing Simphony version 2.10:

- Internet Information Services (IIS): By default uses Transmission Control Protocol (TCP) port 8080
- Client Application Loader (CAL): By default uses TCP port 7300 and User Datagram Protocol (UDP) ports 7300 through 7302

  See Client Application Loader (CAL) in the *Simphony Configuration Guide* on the Oracle Help Center for more information about CAL Authentication for workstations.
- Oracle Hospitality Labor Management: By default uses TCP port 81

You may need to open extra ports for additional Simphony features. Contact your local support representative or Oracle Hospitality Support Services for assistance.

For instructions on opening a port in Windows Firewall, refer to the Microsoft TechNet Library at `https://technet.microsoft.com/en-us/library`.

Binding SSL Certificates to IIS

With the release of Simphony 2.9 or later, you must have a valid security Certificate installed on the Simphony application server. This is the same certificate that is identified and linked to IIS during the Simphony software installation process.

After a successful installation of the Simphony application, you must perform the following steps to Bind the SSL Certificate to the IIS website.

1. Click **Start**, and then click **Control Panel**.
2. If you are using Windows Server 2008 R2, click **System and Security**, and then click **Administrative Tools**.
3. In the Administrative Tools window, double-click **Internet Information Services (IIS) Manager**.
4. Under **Connections**, **Sites**, select the site to be secured with the SSL Certificate.
5. From the **Actions** menu (on the right), click on **Bindings...**
6. This opens the **Site Bindings** window.
7. In the Site Bindings window, click **Add...**
8. This opens the **Edit Site Binding** window.
9. From the **Type** drop-down list, select **https**.
10. Enter the IP address. It should be the IP address of the site or select **All Unassigned**.
11. From the Port field, enter the port number. The port over which traffic will be secured by SSL is usually 443. The SSL Certificate field should specify the installed certificate.
12. Click **OK**.

7 Uninstalling Simphony

Uninstalling only removes the Simphony application. To completely remove Simphony from the servers, you must manually delete the Simphony database components from the database after uninstalling the application.

1. Run the Simphony version 2.10 installation application, and click **Next**.
2. If you have the application and the database on separate servers, run the installation application on the application server.
3. Enter the credentials for a database administrator, and then click **OK**.
4. If you are using an Oracle Database, enter the credentials for the SYS user.
5. If you are using Microsoft SQL Server, enter the credentials for the SA.
6. Select **Uninstall Simphony,** and then click **Next**.
7. Click **Confirm**.

8 Troubleshooting

This section describes common problems you might encounter when installing Simphony version 2.10 and explains how to solve them.

Insufficient System Privileges

Insufficient System Privileges message appears when the prerequisite, Internet Information Services (IIS), has not been installed. See Installing Internet Information Services (IIS) for instructions on how to install IIS.

Cannot Connect to the Database Server During the Simphony Installation

The Simphony installation application may not connect to the database server due to the following reasons:

- Windows Firewall is running
- Simphony and SimphonyXDB instances are not running

Adding Simphony to the Windows Firewall Exceptions

The Windows Firewall, which is enabled by default on your operating system, could prevent the Simphony installation application from connecting to the database server. You must set up an exception rule on your firewall setting for the Simphony server and the database server to continue with the installation. For instructions on how to set up exception rules in Windows Firewall, refer to the Microsoft TechNet Library at `https://technet.microsoft.com/en-us/library`.

Installing Simphony on Separate Servers

If you are using a separate database server, you must set up an incoming rule to allow connections from Simphony depending on your database platform using either the default port or the port you assign while installing Simphony. By default, the Oracle Database server uses port 1521 and Microsoft SQL Server uses port 1443. For instructions on how to open a port in Windows Firewall, refer to the Microsoft TechNet Library at `https://technet.microsoft.com/en-us/library`.

Starting the Oracle Listener

If the Oracle Listener is not running, Simphony services cannot start. Make sure that the Oracle Listener is running:

- If you are using Oracle Linux, run the command $ lsnrctl status. If the listener is running, you should see the listener configuration settings and the services summary.
- If you are using Microsoft Windows, make sure that the Oracle TNS Listener service (for example, OracleOraDb11g_home1TNSListener) is set to **Started** in the Windows Services utility

If the Oracle Listener is not running, then you need to manually restart the listener using the Linux command = `lsnrctl start`. The *Platform Guide for Microsoft Windows* and the *Administrator's Reference for Linux and UNIX-Based Operating Systems* contain more information about manually starting Oracle services.

9 List of Simphony Components and Services

You can install the following components and services by running the Simphony installation application.

Table 9-1 - List of Application and Database Services

Component	Description
Data Transfer Service	Moves point of sale (POS) definitions and journal data to Reporting and Analytics. This is typically installed on each Simphony application server.
Direct Posting Service	Posts sales data to the Simphony Reports database. This is typically installed on each Simphony application server.
EMC Client	Contains all files necessary to run the Enterprise Management Console (EMC).
Open Source	This is typically installed on each Simphony application server.
Sequencer Service	Responsible for running the Start of Day Autosequences. This is typically installed on each Simphony application server, but is only enabled on one server.
Tools	Installs the tools required for import/export, encryption, etc. This is typically installed on each Simphony application server.
Import Export	Installs the Import Export Web API and the Web Application Data Request Processing Service. This is typically installed on each Simphony application server. The Web Application Data Request Processing Service processes Simphony Data Import/ Export requests and any scheduled Import/ Export requests.

10 List of Simphony Database Configuration Fields

The following table describes the fields that appear on the Simphony installation application when configuring the Simphony databases.

Table 10-1 - List of Database Configuration Fields

Field	Options
Service Name	If you are using an Oracle database, enter a service name on which to install the Simphony database.
Instance Name	If you have created a named instanced to install Simphony on Microsoft SQL Server, enter the instance name.
Username	Enter a strong username for the database.
Password	Enter a strong password for the user defined in the Username field to use to connect to the database.
Database Name	Enter a name for the database if you want to use a name other than the default. This field only appears if you select Microsoft SQL as your database type.
Database Port	Enter the port number to use to connect to the database if you want to use a port other than the default.

Appendix A

Sample Script for Creating Oracle Tablespaces

```
DECLARE

cursor mcrspos_tablespace_check is
    select tablespace_name
    from dba_tablespaces
    where tablespace_name = 'MCRSPOS';
v_tablespace varchar2(40);
v_path VARCHAR2(100);
sql_stmt VARCHAR2(10000);

BEGIN

open mcrspos_tablespace_check;
fetch mcrspos_tablespace_check into v_tablespace;
    if mcrspos_tablespace_check%NOTFOUND
    then
        SELECT substr(file_name, 1,((INSTR(file_name,'\', -1, 1))))
    into v_path
    from dba_data_files where rownum < 2;

    sql_stmt :=    'CREATE TABLESPACE MCRSPOS LOGGING DATAFILE '||''''||
v_path||'mcrspos01.dbf'||''''||' SIZE 512M AUTOEXTEND ON NEXT 128M
MAXSIZE UNLIMITED EXTENT MANAGEMENT LOCAL SEGMENT SPACE MANAGEMENT AUTO';


 execute immediate sql_stmt;

    end if;
close mcrspos_tablespace_check;
END;
/

DECLARE

cursor MCRSCACHE_tablespace_check is
    select tablespace_name
    from dba_tablespaces
    where tablespace_name = 'MCRSCACHE';
v_tablespace varchar2(40);
v_path VARCHAR2(100);
sql_stmt VARCHAR2(10000);

BEGIN

open MCRSCACHE_tablespace_check;
fetch MCRSCACHE_tablespace_check into v_tablespace;
    if MCRSCACHE_tablespace_check%NOTFOUND
    then
        SELECT substr(file_name, 1,((INSTR(file_name,'\', -1, 1))))
    into v_path
    from dba_data_files where rownum < 2;

    sql_stmt :=    'CREATE TABLESPACE MCRSCACHE LOGGING DATAFILE
'||''''|| v_path||'MCRSCACHE01.dbf'||''''||' SIZE 128M AUTOEXTEND ON NEXT
128M MAXSIZE UNLIMITED EXTENT MANAGEMENT LOCAL SEGMENT SPACE MANAGEMENT
AUTO';

 execute immediate sql_stmt;

    end if;
close MCRSCACHE_tablespace_check;
END;
/
```

Appendix B

Post-Installation Best Practices

Creating Database Backups

Create backups of the Simphony database periodically to ensure that you do not encounter potential data loss due to any unforeseen circumstances.

The *Database Backup and Recovery User Guide* contains more information about creating database backups using the Oracle Recovery Manager.

For instructions on creating database backups in Microsoft SQL Server, refer to the Microsoft TechNet Library at `https://technet.microsoft.com/en-us/` for more information.

Changing the Application Server's Name

If you change the Server Host Name of your Simphony application server, then make sure to carry out the following updates on the application server.

1. Find and replace the default *ServerName* in the following host files with the new *ServerName*. The default *ServerName* is associated with the IP address localhost.

Table 10-2 - Host Files

Path and filename	Variable
C:\Windows\System32\drivers\etc\hosts	*HostIPAddress ServerName* The *HostIPAddress* is typically set to `localhost`.
C:\Windows\System32\drivers\etc\lmhosts	*HostIPAddress ServerName* The *HostIPAddress* is typically set to `localhost`.

2. If you are using an Oracle database, find and replace the default *ServerName* in the following Oracle files with the new *ServerName*.

Table 10-3 - Oracle Database Files

Path and filename	Variable
Drive:\Oracle\product\version\dbhome_1\NETWORK\ADMIN\listener.ora	HOST=*ServerName*
Drive:\Oracle\product\version\dbhome_1\NETWORK\ADMIN\tnsnames.ora	HOST=*ServerName*

3. If the DNS is enabled on the network, find and replace the default *ServerName* in the following Simphony and mymicros files with the new *ServerName*. If DNS is not enabled, then the server's IP address must be entered.

Table 10-4 - Simphony Services and Reporting and Analytics Files

Path and filename	Variable
Drive:\Micros\Simphony2\EgatewayService\ DbSettings.xml	Set the *ServerName* for all `dataSource` entries.
Drive:\Micros\Simphony2\EgatewayService\ Web.config	Set the *ServerName* in the <appsettings> element for: • SimphonyCAL DiscoveryURL • BatchServiceURL • EGatewayURL • BatchServiceURL_1x • KdsCheckAndPosting • ServiceHost
Drive:\Micros\Simphony2\DirectPostingService\ DirectPostingService.exe.config	Set the *ServerName* on the EGatewayURL line.
Drive:\Micros\Simphony2\SequencerService\ SequencerService.exe.config	Set the *ServerName* on the EGatewayUrl line.
Drive:\Micros\Simphony2\DataTransferService\ mmserver\postingServer.properties	Set the ServerName on all URL lines.
Drive:\Micros\MyMicros\myPortal\ microsConfig.properties	Set the ServerName on all db.server* lines.
Drive:\Micros\MyMicros\infoDelivery\Db.xml	Set the ServerName on all db.server* lines.

4. Restart IIS and the MyMicros Portal service (or restart the computer for new installs).
5. If you are using Windows 32 (Win32) devices, follow the steps outlined below:
    a. Find and replace the default *ServerName* in the following file:

Table 10-5 - Simphony Install

Path and filename	Variable
Drive:\Micros\Install\SimphonyInstall.xml	Set the *ServerName* on all <ServerName>, <SvcHostName>

    b. Log onto the EMC and navigate to the Enterprise level and click the **Setup** tab, click **CAL Packages**, click the **Package Content** tab, and select the appropriate Service Host.
    c. Click **Win32** under the Platforms header.
    d. Click **Reload Package From Disk** to upload the Win32 CAL package to the database.

When prompted for the CAL package location, specify the *Drive*:\Micros\Simphony2\EgatewayService\CAL\Win32\Packages\ServiceHost2.0, and click **OK**.

Changing an Oracle Database Server’s Name

Refer to `http://docs.oracle.com` for more information about renaming your Oracle Database server.

Changing a Microsoft SQL Server’s Computer Name

Refer to `msdn.microsoft.com` for more information about renaming your Microsoft SQL Server computer.