

# Oracle<sup>®</sup> Hospitality Symphony

## Post-Installation or Upgrade Guide



Release 18.2

F12086-04

December 2019

The Oracle logo, consisting of the word "ORACLE" in white, uppercase, sans-serif font, centered within a solid red square.

ORACLE<sup>®</sup>

Copyright © Oracle and/or its affiliates. All rights reserved.

This software and related documentation are provided under a license agreement containing restrictions on use and disclosure and are protected by intellectual property laws. Except as expressly permitted in your license agreement or allowed by law, you may not use, copy, reproduce, translate, broadcast, modify, license, transmit, distribute, exhibit, perform, publish, or display any part, in any form, or by any means. Reverse engineering, disassembly, or decompilation of this software, unless required by law for interoperability, is prohibited.

The information contained herein is subject to change without notice and is not warranted to be error-free. If you find any errors, please report them to us in writing.

If this is software or related documentation that is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. Government, then the following notice is applicable:

U.S. GOVERNMENT END USERS: Oracle programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, delivered to U.S. Government end users are "commercial computer software" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, use, duplication, disclosure, modification, and adaptation of the programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, shall be subject to license terms and license restrictions applicable to the programs. No other rights are granted to the U.S. Government.

This software or hardware is developed for general use in a variety of information management applications. It is not developed or intended for use in any inherently dangerous applications, including applications that may create a risk of personal injury. If you use this software or hardware in dangerous applications, then you shall be responsible to take all appropriate fail-safe, backup, redundancy, and other measures to ensure its safe use. Oracle Corporation and its affiliates disclaim any liability for any damages caused by use of this software or hardware in dangerous applications.

Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Xeon are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. AMD, Opteron, the AMD logo, and the AMD Opteron logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group.

This software or hardware and documentation may provide access to or information about content, products, and services from third parties. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third-party content, products, and services unless otherwise set forth in an applicable agreement between you and Oracle. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services, except as set forth in an applicable agreement between you and Oracle.

# Contents

## Preface

---

## 1 Upgrading Symphony

---

Upgrading to Symphony Release 18.2	1-1
Symphony Upgrade Procedures	1-2
Upgrades When Adding a New Database Server	1-3
Upgrades without Separate Transaction and Security Database Servers	1-6
Upgrades with Existing Separated Transaction and Security Database Servers	1-8
Post-Upgrade Steps for CAPS on IIS for Symphony 2.9 Users	1-10
Step 1 - Close and Post All Transactions	1-10
Step 2 - Access the IIS Manager Console	1-10
Step 3 - Rename the IIS Folder	1-12
Step 4 - Enable an Option and Configure CAPS	1-13
Step 5 - Stop IIS	1-14
Step 6 - Move the DbSettings.xml to the Newly Defined IIS CAPS Path	1-14
Step 7- Start IIS	1-15
Step 8 - Verify Log Creation, Database Tables, and Delete the Old Directory	1-15

## 2 Post-Installation Tasks

---

Updating the Property EMC Client	2-1
Updating Check and Posting Service Clients	2-1
Updating CAL Packages	2-1
Enabling Communication Between the Enterprise and Workstations	2-1

## 3 EMC Access Security

---

Accessing the Symphony EMC Using Multi-Factor Authentication	3-1
Configuring the SMTP and Backup SMTP Servers in the EMC	3-1
Configuring and Resetting Email Addresses	3-3
Forgotten EMC Password Recovery	3-3
Configuring Access Privileges for Resetting a Password	3-5

Resetting Passwords from the Symphony Web Portal	3-6
Setting the Max Allowed Failed Logins for EMC Access	3-8

## 4 Updating Property Administrator and Database Logon Credentials

Configuring Different Credentials for Each Property	4-1
Configuring the Same Credentials for All Properties in the Enterprise	4-2

# Preface

This guide is for Symphony Cloud Services users and provides post-installation steps to perform after a fresh installation or upgrade to the Symphony 18.2 release. Beginning with the Symphony 2.9 release or later, users must install Reporting and Analytics (R&A) separately from Symphony using the Back Office R&A installation application. For upgrades from releases prior to Symphony 2.9, users must upgrade to Reporting and Analytics release 8.5.1 Patch 3 before installing or upgrading to Symphony release 2.9. Symphony release 18.2 is compatible with R&A releases 8.5.1 Patch 3 (for all-in-one installations), 9.0 Patch 8, and 9.1.

## Audience

This installation guide is intended for installers, programmers, technical support teams, product specialists, and others who are responsible for setting up Oracle Hospitality Symphony release 18.2.

## 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 all associated log files
- Screen shots of each step you take

## Documentation

The *Symphony Installation Guide* contains more information about performing installations and upgrades to Symphony.

Product documentation is available on the Oracle Help Center at <https://docs.oracle.com/en/industries/food-beverage/pos.html>.

## Revision History

---

Date	Description of Change
December 2018	Initial publication

---

---

Date	Description of Change
May 2019	<ul style="list-style-type: none"><li>• Removed the following sections from Chapter 2:<ul style="list-style-type: none"><li>– Updating Symphony License Counts</li><li>– Post Install Steps for Engagement on Load Balanced Symphony Servers</li></ul></li><li>• Added Chapter 3: EMC Access Security</li><li>• Updated the Upgrading to Symphony Release 18.2 topic.</li></ul>
December 2019	Updated the Upgrading to Symphony Release 18.2 topic by including the workaround to add the <code>SQLNET.INBOUND_CONNECT_TIMEOUT=120</code> parameter.

---

# 1

## Upgrading Symphony

The information on this page provides instructions on how to perform an upgrade to your Symphony system.

- [Upgrading to Symphony Release 18.2](#)
- [Symphony Upgrade Procedures](#)
- [Upgrades When Adding a New Database Server](#)
- [Upgrades without Separate Transaction and Security Database Servers](#)
- [Upgrades with Existing Separated Transaction and Security Database Servers](#)
- [Post-Upgrade Steps for CAPS on IIS for Symphony 2.9 Users](#)

### Upgrading to Symphony Release 18.2

Symphony version 18.2 performs an upgrade from Symphony version 2.9 or later. To enhance your system's security, during upgrades, the Symphony installation application enables you to physically separate the Transaction (MCRSPOS) database from the Security (MCRSCACHE) database (onto another database server), and then proceed with the upgrade. Oracle strongly recommends storing these databases on separate database servers. The following sections review three possible upgrade scenarios:

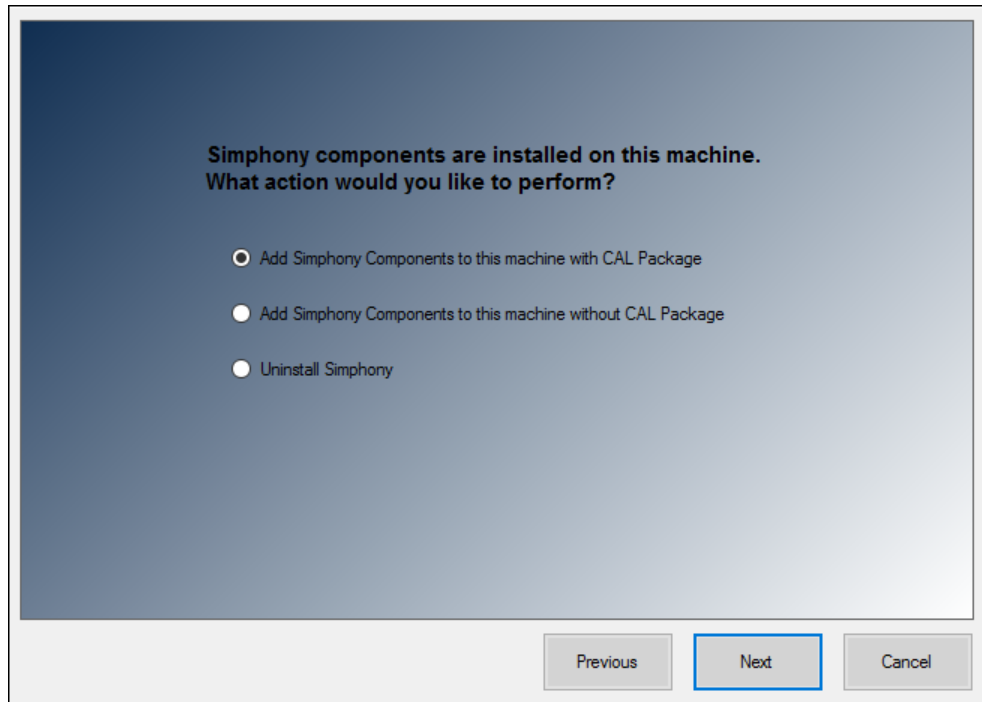
- [Upgrades When Adding a New Database Server](#)
- [Upgrades without Separate Transaction and Security Database Servers](#)
- [Upgrades with Existing Separated Transaction and Security Database Servers](#)

When upgrading in certain environments, you may experience the error ORA-25408, which is an Oracle Client related issue outside of Symphony. This condition is caused by environmental network timeouts being reached. To work around this issue, add the parameter `SQLNET.INBOUND_CONNECT_TIMEOUT=120` to the `Sqlnet.ora` file on the database server.

1. Ensure that the Symphony application and database servers meet the requirements listed in [Pre-Installation Tasks](#).
2. Log in and download the Symphony release 18.2 installation application from the Oracle Technology Network (OTN) website at <https://edelivery.oracle.com/>.
3. Run the **Setup**, and then click **Next**.  
If the application and the database are 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.

Beginning with the Simphony 2.10 release and later, you can upgrade application components on servers with or without downloading CAL Packages to the Simphony database. This flexibility can speed up the upgrade process on properties using multiple application servers.

**Figure 1-1 Simphony Components Installation Options**



## Simphony Upgrade Procedures

1. Ensure that the Simphony application and database servers meet the requirements listed in the *Oracle Hospitality Simphony Installation Guide*, specifically the *Pre-Installation Tasks* section.
2. Log in and download the Simphony 18.2 release installation application from the Oracle Technology Network (OTN) Web site 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 using 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 use an existing certificate, select **Existing**, and then select the installed certificate from the drop-down list.
  - 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. To add IIS Bindings, refer to [Binding Secure Server Certificates to IIS](#) and 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. Click **Next**, and then click **Confirm** to begin the upgrade.
10. Click **Yes** to restart the server.

## Upgrades When Adding a New Database Server

This section provides upgrade instructions to enhance your system security by adding a new database server to house the security database. If you are using multiple Symphony application servers, upgrade the initial application server to Symphony release 18.2. After upgrading subsequent application servers, ensure that on each application server 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 Symphony application server that was upgraded. For example:

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

To initiate this type of upgrade:

1. Perform Steps 1 through 5 in [Symphony Upgrade Procedures](#).
2. **Certificate Location:** Throughout the Symphony 18.2 upgrade process, the Symphony 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 use an existing certificate, select **Existing**, and then select the installed certificate from the drop-down list.

- d. If you are using a Load Balancer server and using the Import/Export Service or plan to use the Oracle Hospitality Symphony 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 Symphony 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 Symphony 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 match 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. Because 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, you must go to the secondary database server and manually create the folders specified in the **Remote Database Location** field. Alternatively, you 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.

**Figure 1-2 New Security Database Information**

The screenshot shows a dialog box with a dark blue header and a light gray body. The title is "Enter the information that will be used to create the New Security Database." Below the title are seven input fields, each with a label to its left. The labels and their corresponding values are: "Server Name:" (empty), "Instance Name:" (empty), "Username:" (empty), "Password:" (empty), "Confirm Password:" (empty), "Database Name:" (MCRSCACHE), and "Database Port:" (1433). The "Remote Database Location:" field contains "D:\MICROS\DATA\". At the bottom right of the dialog are three buttons: "Previous", "Next", and "Cancel".

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 then 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 sites 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 through 5 as in [Symphony Upgrade Procedures](#).
2. **Certificate Location:** Throughout the Symphony 18.2 upgrade process, the Symphony 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 use an existing certificate, select **Existing**, and then select the installed certificate from the drop-down list.
  - d. If you are using a Load Balancer server and using the Import/Export Service or plan to use the Oracle Hospitality Symphony 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.



- 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 sites 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 [Simphony Upgrade Procedures](#).
2. **Certificate Location** - Throughout the Simphony 18.2 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 list.
  - d. If you are using a Load Balancer server and using 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.



 **Note:**

If multiple Symphony application servers are utilized, upgrade the initial application server to Symphony release 18.2. After upgrading subsequent application servers, ensure that on each application server 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 Symphony application server that was upgraded. For example:

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

## Post-Upgrade Steps for CAPS on IIS for Symphony 2.9 Users

This section only applies if you are upgrading from the Symphony 2.9 General Release (GR) and are using either an Oracle or Microsoft SQL Server database platform, and are upgrading to Symphony releases 2.10, 18.1, or 18.2.

No additional post-upgrade steps are necessary for CAPS on Microsoft Internet Information Services (IIS) if you upgrade from Symphony releases later than Symphony 2.9 GR (for example, Symphony 2.10, 18.1, or 18.2).

- [Step 1 - Close and Post All Transactions](#)
- [Step 2 - Access the IIS Manager Console](#)
- [Step 3 - Rename the IIS Folder](#)
- [Step 4 - Enable an Option and Configure CAPS](#)
- [Step 5 - Stop IIS](#)
- [Step 6 - Move the DbSettings.xml to the Newly Defined IIS CAPS Path](#)
- [Step 7- Start IIS](#)
- [Step 8 - Verify Log Creation, Database Tables, and Delete the Old Directory](#)

### Step 1 - Close and Post All Transactions

Ensure that all transactions for the property are closed and posted to the Enterprise prior to performing the Symphony upgrade.

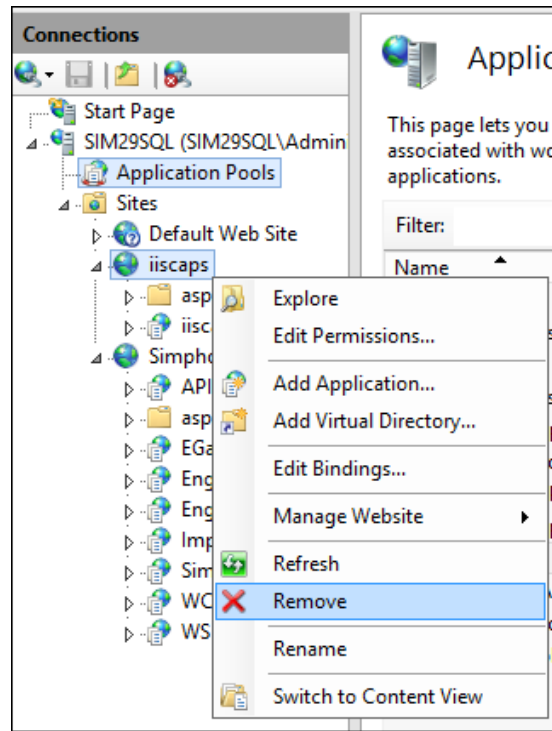
### Step 2 - Access the IIS Manager Console

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 the site created for IIS CAPS and select **Remove**. The name of the IIS CAPS site should



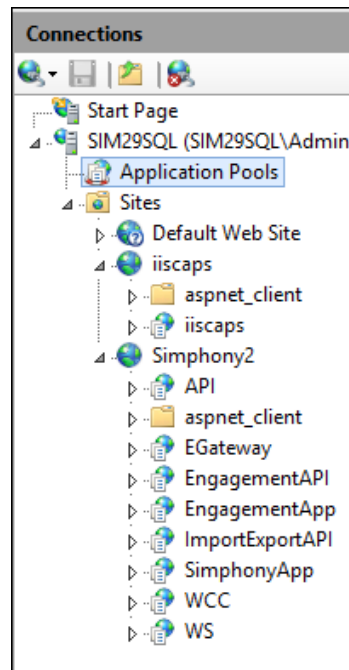
be the same as the *ServiceHostName*. For example, if your service host name is MyIISCapsSvcHost, your site name should be added using the exact same text.

**Figure 1-3 IIS CAPS Site**



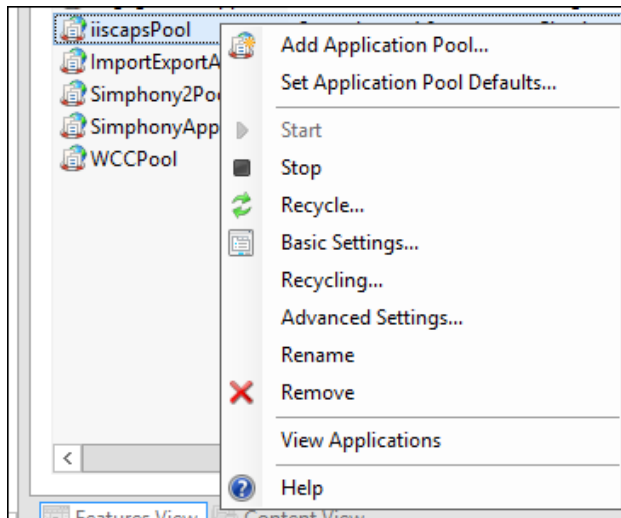
3. From the IIS Connections column, click **Application Pools**.

**Figure 1-4 Symphony Application Pools**



4. Right-click 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*.

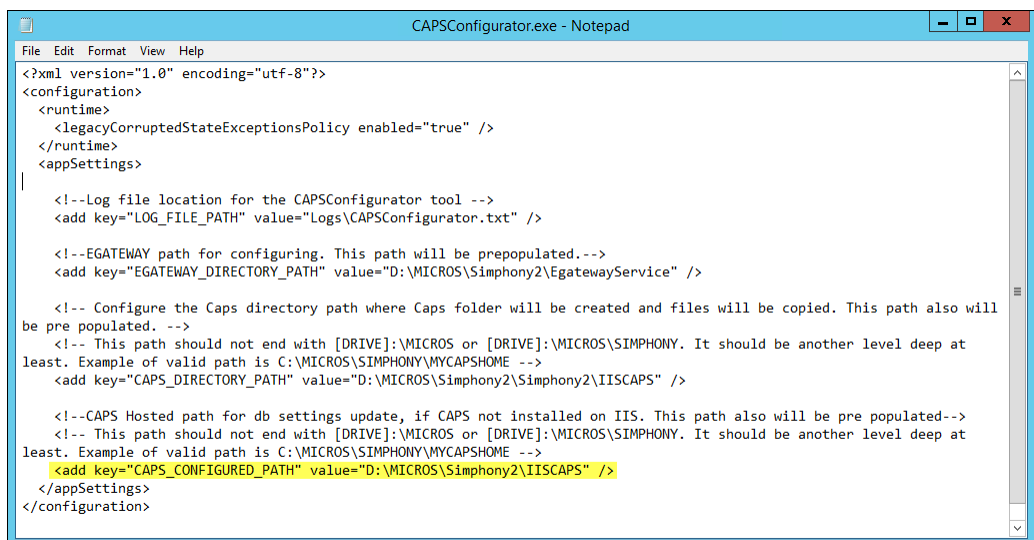
**Figure 1-5 IIS CAPS Application Pool**



## Step 3 - Rename the IIS Folder

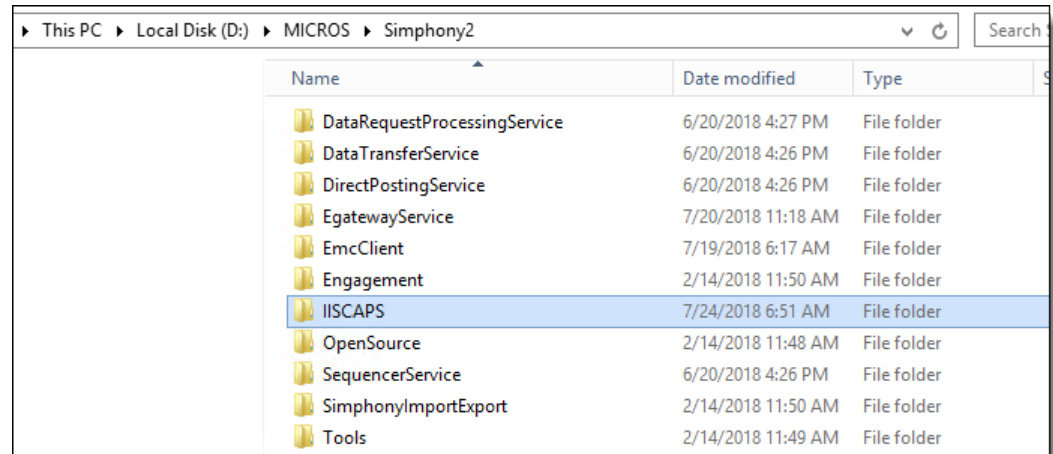
1. Rename the Symphony release 2.9 (or later) IIS CAPS folder.
2. Verify the installed folder path by navigating to the [Drive]:\MICROS\Symphony2\Tools\CAPSConfigurator\CAPSConfigurator.exe.config file and open it with a text editor such as Microsoft Notepad.

**Figure 1-6 CAPSConfigurator.exe.config IIS CAPS Directory Installation Folder Path**



3. Note that the default Symphony release 2.9 (or later) IIS CAPS folder location is: [Drive]:\Symphony2\IISCAPS. Rename the **IISCAPS** folder to **IISCAP\_Backup**. This step ensures that you maintain a backup of the old folder.

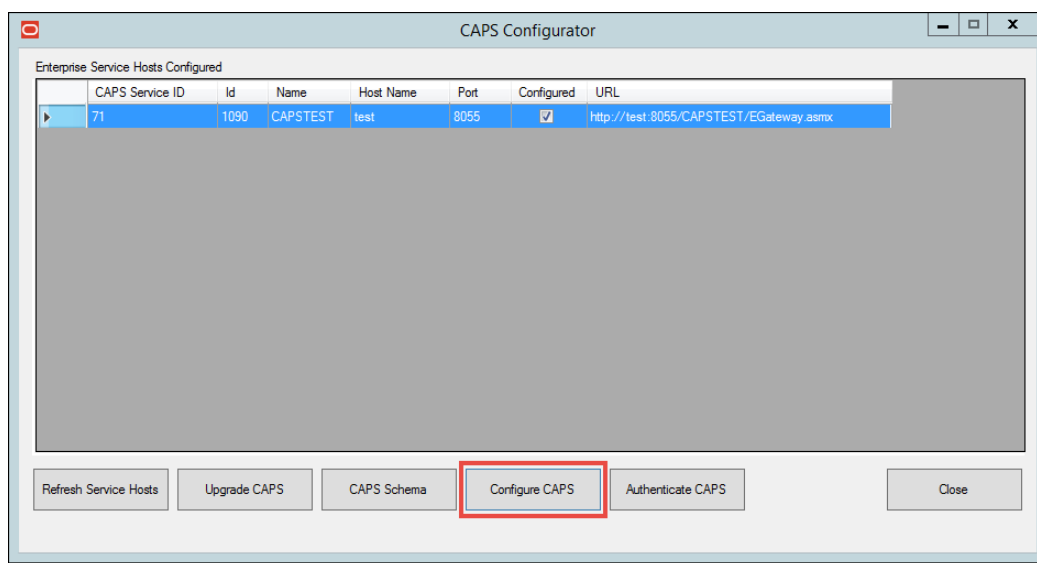
**Figure 1-7 Default IIS CAPS Folder Installation Path**



## 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 your assigned role and switch to Form view.
3. Click the **Operations** tab, and then click the **Miscellaneous** subtab.
4. In the Miscellaneous Options section, enable **10065 - Download Software, Install and Authenticate Clients and Service Hosts Using CAL**, and then click **Save**.
5. If you are configuring CAPS on IIS at the Symphony application server, you can access the CAPS Configurator Tool using this path: [Drive]:\MICROS\Symphony2\Tools\CAPSConfigurator\CAPSConfigurator.exe. If you are installing CAPS on IIS on a remote workstation or virtual machine, install CAL on that device, and through CAL, deploy a package called **CAPSONIIS** to the device. When the software is on the device, navigate to [Drive]:\MICROS\Symphony\CAPSONIIS\Tools\CAPSConfigurator\ and double-click the **CAPSConfigurator.exe** file.
6. Log on to the **CAPS Configurator Tool**, and freshly configure CAPS with the default configuration settings by clicking the **Configure CAPS** button.

**Figure 1-8 CAPS Configurator Tool**



7. Upon successful installation, verify that the new directory is created along the [Drive]:\Symphony2\EgatewayService\IISCAPSServiceHost path.

## Step 5 - Stop IIS

To stop IIS:

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](#), and verify the default CAPS IIS installation path), and then using Microsoft Windows Explorer, navigate to that path (for example, [Drive]:\Symphony2\IISCAP\_Backup\IISCAPS\DbSettings.xml).
2. Paste the **DbSettings.xml** file in the new path: [Drive]:\Symphony2\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

To start IIS:

1. Run the command window with administrator privileges.
2. Enter 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]:\Symphony2\EgatewayService\IISCAPSServiceHost\EgatewayLog`.
2. Verify that the tables are upgraded on the existing transaction database.
3. Delete the Symphony release 2.9 CAPS directory (for example, the `IISCAP_Backup` directory). See [Step 3 - Rename the IIS Folder](#) for details.

# 2

## Post-Installation Tasks

Perform all post-installation tasks to ensure that the application components and the databases are configured correctly.

- [Updating the Property EMC Client](#)
- [Updating Check and Posting Service Clients](#)
- [Updating CAL Packages](#)
- [Enabling Communication Between the Enterprise and Workstations](#)

### Updating the Property EMC Client

The Enterprise Management Console (EMC) is the primary configuration application in Symphony. 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 enable users to access the EMC from other computers on the network.

The *Oracle Hospitality Symphony Manager User Guide*, specifically the *Symphony Web Portal (SWP)* section contains instructions about accessing the SWP and updating your EMC Client for your property.

### Updating Check and Posting Service Clients

Update all Check and Posting Service (CAPS) clients prior to updating workstations with the latest CAL Packages. The *Symphony Client Deployment Guide* contains more information about configuring and deploying CAL Packages.

### Updating CAL Packages

Oracle Hospitality recommends that you consider updating your POS clients using the latest available CAL Packages. To accomplish this, verify the CAL Package contents and then configure and execute a CAL Package Deployment Schedule. The *Symphony Client Deployment Guide* contains more information about configuring and deploying CAL Packages.

### 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 Symphony application servers using either the default ports or the ports you assign when installing Symphony release 18.2:

- Internet Information Services (IIS): By default uses Transmission Control Protocol (TCP) port 8080 or port 443 for HTTPS connections.
- Oracle Hospitality Labor Management: By default uses TCP port 81.

You may need to open extra ports for additional Symphony 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>.

# 3

## EMC Access Security

Enterprise Management Console (EMC) access security has been enhanced with the support of Multi-Factor Authentication (MFA). This chapter reviews enabling configuring the system's EMC security settings including information about configuring employee passwords and email addresses.

- [Accessing the Symphony EMC Using Multi-Factor Authentication](#)
- [Configuring the SMTP and Backup SMTP Servers in the EMC](#)
- [Configuring and Resetting Email Addresses](#)
- [Forgotten EMC Password Recovery](#)
- [Setting the Max Allowed Failed Logins for EMC Access](#)

### Accessing the Symphony EMC Using Multi-Factor Authentication

To use Multi-Factor Authentication (MFA) on your Symphony system, you need to add and register your email address.

1. When first attempting to log in to the Symphony EMC, when prompted, enter your user name in the **User Name** field, and enter your email address in the **Email Address** field.
2. Re-enter your email address in the **Confirm Email Address** field, and then click **Register**.

This email address is used to send you a one-time password (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 then click **Enter**.

OTPs are only valid for five minutes, so enter your OTP password in a timely manner. If the five-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 in to the EMC at that time. After entering a valid OTP, the EMC opens.

### 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:



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.

**Figure 3-1 EMC Enterprise Parameters Login Tab**

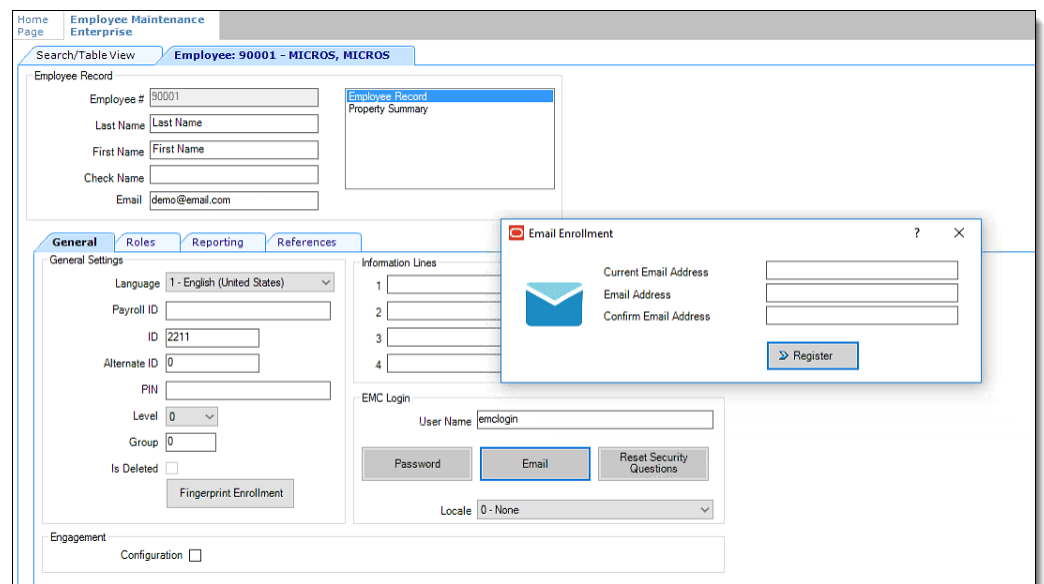
3. From the Email Configuration section, select the **Primary SMTP Server** subtab and enter the required settings in the fields listed below:
  - a. **Server**: Enter either the IP address (IPv4 Address) or the name of the Primary SMTP server. Click the **Select** button to choose an email provider, 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).
  - b. **Port**: Enter a port number or use the defaults.
  - c. **SSL**: Select to enable a secure connection using HTTPS.
  - d. **User Name**: Enter a user name for access to the Primary SMTP server.
  - e. **Password**: Enter a password for access to the Primary SMTP server and re-enter it in the **Confirm password** field for verification.
  - f. **Source Email**: Enter your source email address. This email address is used as the sender of all OTP emails.
  - g. (Optional) **Name**: Enter an alternate (alias) name for the **Source Email** sender.
4. Click the **Backup SMTP Server** subtab and enter the IP address or server name of the Backup SMTP server.
5. Enter information in the fields as listed above for the SMTP Backup server.
6. Click **Save**.
7. 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.

## Configuring and Resetting Email Addresses

After enabling Multi-Factor Authentication (MFA), each user that accesses the EMC or Symphony Web Portal (SWP) must register their email address. The system prompts each EMC user to do so. This enables users to receive the one-time password (OTP) via email to complete the EMC login process. 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**.

**Figure 3-2 Employee Email Address Configuration**



4. If a user's email address changes:
  - a. Click the **Email** button.
  - b. 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.
  - c. Click **Register**.
5. Depending on your Employee Role privilege settings in reference to accessing the Employee Maintenance module, you can also enter or edit the **Email** field for yourself or others.

## Forgotten EMC Password Recovery

Staff members occasionally forget their password to access the EMC or Symphony Web Portal (SWP). You can reset your password or, in some cases, assist others in

resetting their password (if you are privileged to do so). This is accomplished by receiving a temporary, One-Time Password (OTP) via email, which then allows you to log on and reset your password. To further enhance security, you are prompted by the system to choose three security questions from a drop-down list. You must then enter the answers (known only to you) to each of the security questions.

OTPs are valid for one single entry for the individual attempting to log on to the EMC at that time. One-Time Passwords are only valid for five minutes after they are generated by the system.

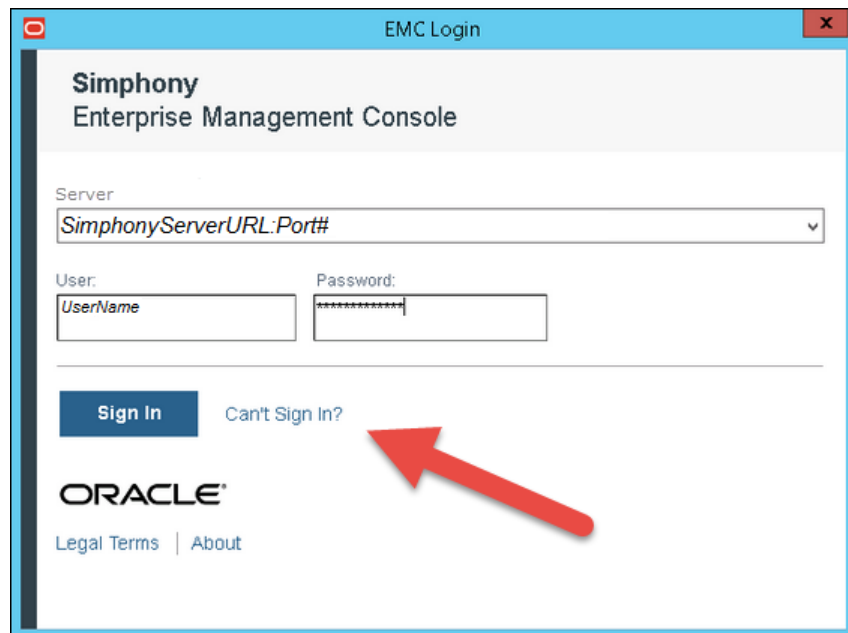
### Prerequisites

To use this functionality, the following requirements must be met:

- 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 is required so that One-Time Passwords can be emailed to employees as needed.
- To use the **Can't Sign In?** link, each employee using the EMC must have a valid email address configured in their employee record.

If you are locked out of the EMC, you can reset your own password (if you have the necessary access privileges assigned to your account).

Figure 3-3 EMC Login Can't Sign In?



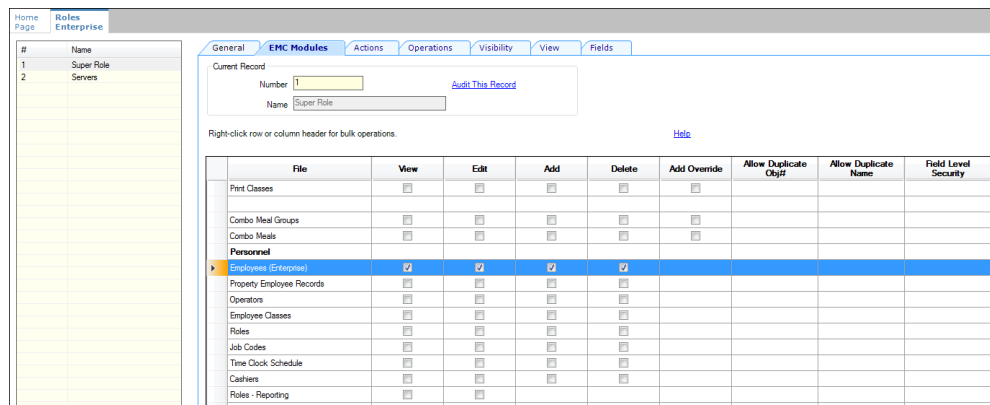
- [Configuring Access Privileges for Resetting a Password](#)
- [Resetting Passwords from the Simphony Web Portal](#)

## Configuring Access Privileges for Resetting a Password

To access and reset passwords for other users, you need to be assigned the appropriate privileges in the EMC.

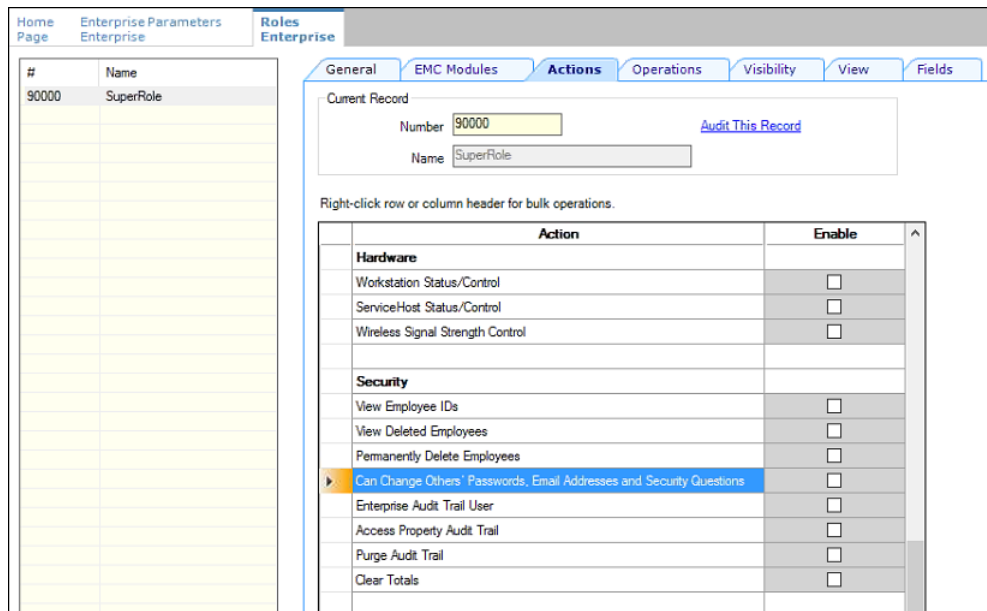
1. Select the **Enterprise level** , click **Configuration**, and then click **Roles**.
2. Click the **EMC Modules** tab and scroll to the **Personnel** section.
3. Select the options for the **Employees (Enterprise)** access privileges for each of the following columns:
  - **View**
  - **Edit**
  -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

**Figure 3-4 Roles for EMC Modules**



4. Click **Save**.
5. Click the **Actions** tab, and then scroll through the Action column until you reach the Security section.
6. Select the **Can Change Others' Passwords and Email Addresses and Security Questions** check box to enable the option, and then click **Save**.

**Figure 3-5 Roles Actions Security Settings**



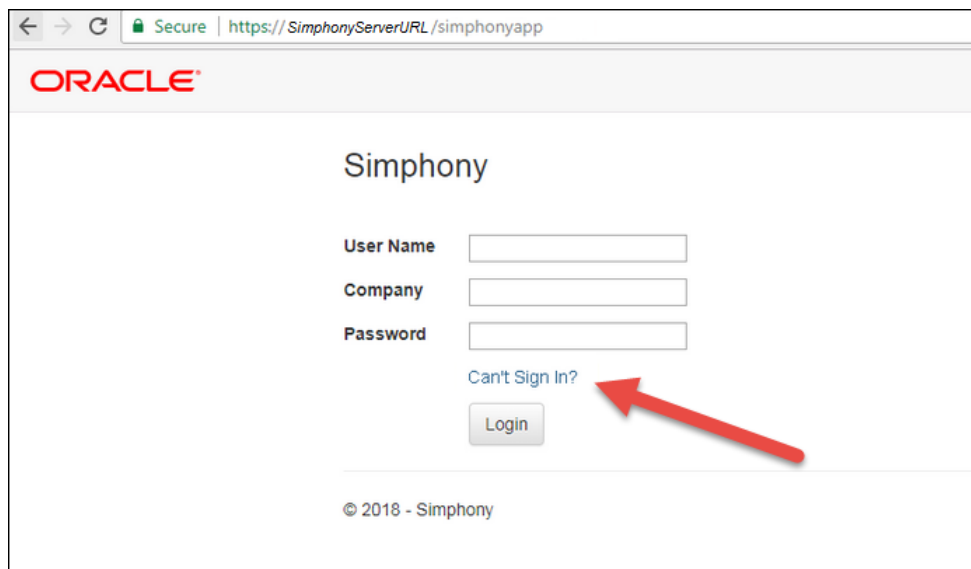
7. Ensure that all users requiring Multi-Factor Authentication (MFA) configuration permissions are assigned a role that have these access privileges enabled.

## Resetting Passwords from the Symphony Web Portal

You can reset passwords and configure your security questions from the Symphony Web Portal (SWP) page. To change your password:

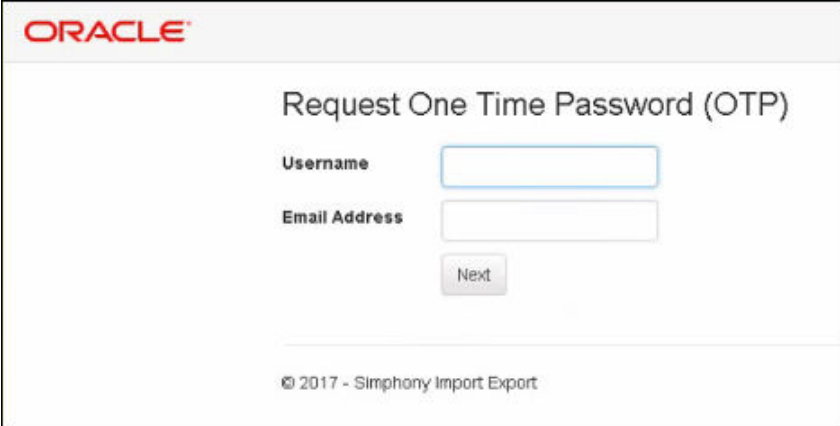
1. Open the Symphony Web Portal URL. When prompted, enter your **User Name**, and then click the **Can't Sign In?** link. You are provided with a One Time Password (OTP) via email.

**Figure 3-6 Symphony Web Portal Logon Screen's Can't Sign In? Link**



2. When prompted, enter your **User Name** and registered **Email Address**.

**Figure 3-7 Request One Time Password Screen**



ORACLE

Request One Time Password (OTP)

Username

Email Address

Next

© 2017 - Symphony Import Export

3. The system validates the information you entered, and shows a details page where you must correctly answer your security questions as configured in the system. Upon entering your validated logon and security question responses, an OTP token is sent to your email account, and you are redirected to the Forgot Password page. You are prompted to enter your OTP and your new password, and to confirm it by entering these credentials again.
4. When you click the **Can't Sign In?** link from the EMC Log in screen, the system redirects you to the **Request One Time Password (OTP)** page of the SWP in a browser. To log in, enter the following information, and then click **Next**:
  - **Username**
  - **Email Address**

From the SWP, you can change your password and update your security questions. The following image shows the default User Profile screen. You can access the User Profile screen from the SWP page by clicking the **User Profile** link on the toolbar.

**Figure 3-8 Simphony Web Portal (SWP) User Profile Screen**

The screenshot displays the Oracle Simphony Web Portal (SWP) User Profile screen. At the top, there is a navigation bar with links for Home, Import / Export, Status, Schedules, Help, and User Profile (highlighted with a red box and a red arrow). The page title is "User Profile".

**USER CONFIGURATION**

User Name: emclogin  
 Email: abc@email.com

**CHANGE PASSWORD**

\* Current Password:   
 \* New Password:   
 \* Confirm Password:

Change Password

**SECURITY QUESTIONS**

\* Question: - Select One -  
 \* Answer: Enter your answer here

\* Question: - Select One -  
 \* Answer: Enter your answer here

\* Question: - Select One -  
 \* Answer: Enter your answer here

Save Security Questions

**Password must**

- Start with a letter and contain numbers and special characters.
- Not be a restricted text as per organization's security policy.
- Be between 8 and 20 characters long.
- Be different from your last 4 passwords.
- Not be your current password.
- Contain at least one each of the following:
  - Lowercase letter
  - Uppercase letter
  - Number
  - Special Character

Build 2.1000.0.0.227 © 2017 - Simphony Import Export

If you do not meet the following prerequisites, you must request to have a privileged supervisor initiate recovery of your password:

- You do not have a valid email address configured within your employee record
- You have not configured your security questions and answers

## Setting the Max Allowed Failed Logins for EMC Access

MFA adheres to the EMC account lock out setting.

- Select the **Enterprise**, click **Setup**, and then click **Enterprise Parameters**.
- Click the **Login** tab.
- In the Options section, enter 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.

# 4

## Updating Property Administrator and Database Logon Credentials

When logging on to the EMC for the first time after installing or upgrading to Symphony release 18.2, a message indicates that the property credentials are not compliant with the Symphony standards. To keep the properties safe from security risks, you need to update the Admin and Database credentials, which Symphony uses to create and maintain the workstation databases. Symphony offers the options of configuring security credentials for each property separately or using the same credentials for all properties in the Enterprise. Symphony 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 on until you meet the compliance.

- To configure credentials for each non-compliant property separately, see [Configuring Different Credentials for Each Property](#).
- To configure the same credentials for all non-compliant properties in the Enterprise, see [Configuring the Same Credentials for All Properties in the Enterprise](#).
- [Configuring Different Credentials for Each Property](#)
- [Configuring the Same Credentials for All Properties in the Enterprise](#)

### Configuring Different Credentials for Each Property

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, and then enter the **User Security Credentials**. Symphony release 18.2 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.

5. Enter the **Current Password** of the Admin User.
6. Enter a new strong password for the Admin User.

Review the *Symphony Installation Guide* specifically, the **Database User Passwords** section which contains more information about password requirements.



7. Repeat Steps 5 and 6 for the **Database User**, and then click **Save**.
8. Repeat Steps 3 through 7 for all non-compliant properties.

If you are using Symphony release 2.9.1 or later (including the Symphony 18.2 release), the steps outlined above have changed in reference to allowing you to use your EMC logon credentials to perform downloads, upgrades, and authentications using the Client Application Loader (CAL) on service hosts and workstations.

See the *Oracle Hospitality Symphony Configuration Guide*, specifically, the Employees and Privileges chapter, for more information about configuring employees and their access privileges.

To allow users to use their EMC logon credentials to access and update service hosts and workstations:

- Access the EMC and select the Enterprise level, **Configuration** tab, and then click **Roles**.
- Select the **Operations** tab, click the **Miscellaneous** tab, and then within the Miscellaneous Options section, enable the **10065 – Download Software, Install and Authenticate Clients and Service Hosts Using CAL** option.
- Click **Save**.
- Repeat these steps for each employee role you wish to assign this privilege.

## Configuring the Same Credentials for All 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**.