Oracle® MICROS Simphony

Post-Installation or Upgrade Guide

Release 19.3
F47306-01
September 2021

ORACLE

Oracle MICROS Simphony Post-Installation or Upgrade Guide, Release 19.3

F47306-01

Contents

Preface

This guide is for Simphony Cloud Services users and provides post-installation steps to perform after a fresh installation or upgrade to the latest Simphony release. You install Reporting and Analytics separately from Simphony using the Back Office Reporting and Analytics installation application.

Audience

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

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

The *Simphony Installation Guide* contains information about performing new installations.

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
September 2021	Initial publication.

1

Upgrading Simphony

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

Upgrading to Simphony Release 19.2 or Later

To enhance your system's security during upgrades, the Simphony 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

1. Ensure that the Simphony application and database servers meet the requirements listed in Pre-Installation Tasks.
2. Log in and download the Simphony release 19.1 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 program on the application server.
4. Enter the logon credentials for a database administrator, and then click **OK**.

   For an Oracle database, enter the credentials for the SYS user.

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

Upgrade Procedures

1. Ensure that the Simphony application and database servers meet the requirements listed in the *Oracle Food and Beverage Compatibility Matrix* and *Oracle MICROS Simphony Release Notes*.
2. Log in and download the Simphony software from the Oracle Technology Network (OTN) Web site at https://edelivery.oracle.com.

> **Important:**
>
> To improve overall system performance on database servers, if you are performing an upgrade or importing a database after a fresh installation, **prior** to performing the upgrade, or immediately after importing a database after a fresh installation, you should:
>
> - Access the downloaded software, right-click on the ISO, and then click **Mount**.
> - Browse the ISO and navigate to the **INSTALL** folder, and then open the **DBScripts** folder.
> - The DBScripts folder contains a text document named **README_Oracle_String_Update.txt**.
> - Open the README_Oracle_String_Update.txt, carefully read the content, and then perform the steps as outlined there.
> - Once completed, continue to step 3 (below).

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**. Enter the credentials for the sys 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. Enter the **Security Database Server Name**, the **DB Service Name**, and the **Security DB Schema Name** and **Password**.
9. Click **Next** to enter the Reporting and Analytics information.
10. If you are connected to Reporting and Analytics, enter the passwords for the MMSQL and CEDB database users, and then click **Next**.

11. Click **Next**, and then click **Confirm** to begin the upgrade.
12. 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 Simphony application servers, upgrade the initial application server. 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 Simphony 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 Simphony Upgrade Procedures.
2. **Certificate Location**: Throughout the 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 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 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**.

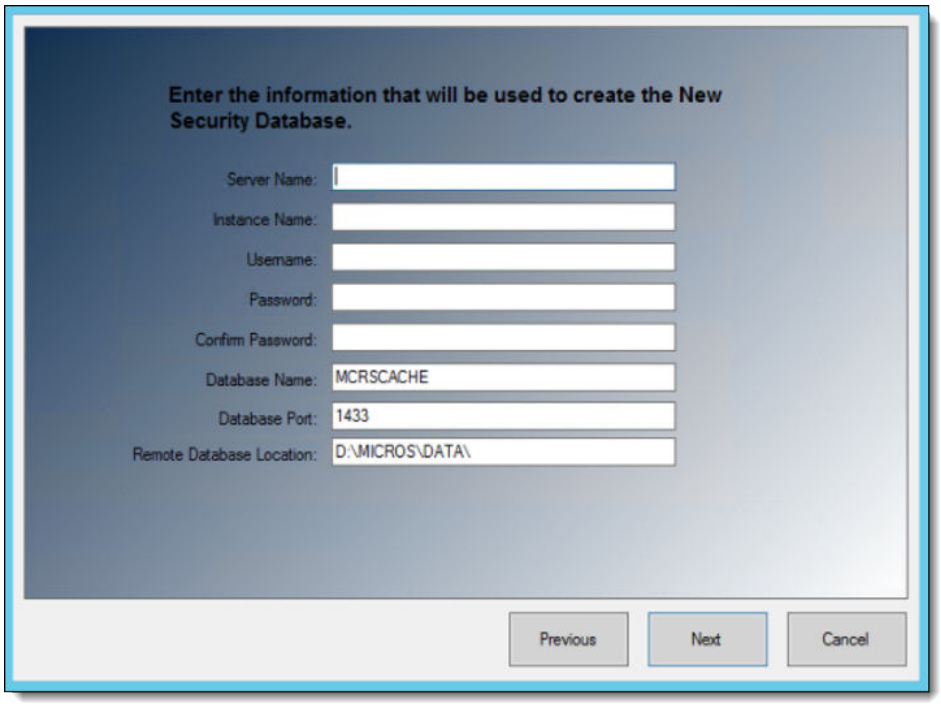
4. When using **LoadBalancer**, enter (or verify) the **Service Host Name** (for the Simphony application server). If the Service Host Name does not match the FQDN of your computer, a warning message dialog appears.
    a. Do not ignore the message; select **No**, and then correct the invalid Service 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. **Username**: Enter your security database access user name.
    d. **Password**: Enter your security database access password.
    e. **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. **Username**: Enter your security database access user name.
    d. **Password**: Enter your security database access password.
    e. **Confirm Password**: Re-enter your security database access password.
    f. **Database Name**: Enter the name of the security database.
    g. **Database Port**: Enter the port number used to access the security database.
    h. **Remote Database Location**: Enter the path and folder names where the Security database is to be created.

Figure 1-1 New Security Database Information



8. Enter the logon credentials for a database administrator (sys user), and then click **OK**.
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. **Username**: Enter (or verify) your reporting database access user name.
    d. **Password**: Enter your reporting database access password.
    e. **Database Port**: Enter the port number used to access the reporting database.
    f. **Username**: Enter (or verify) your reporting database access user name.
    g. **Password**: Enter your reporting database access password, and then click **Next**.
10. Enter a database administrator's logon credentials for the sys user, click **OK**, and then click **Next**.
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 Upgrade Procedures.

2. **Certificate Location**: Throughout the 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 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 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 security database server.
   b. **Service Name**: (Oracle Database users) Enter the name of the service (TNS alias).
   c. **Username**: Enter your security database access user name.
   d. **Password**: Enter your security database access password.
   e. **Database Port**: Enter the port number used to access the security database server, and then 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. **Username**: Enter (or verify) your reporting database access user name.
    d. **Password**: Enter your reporting database access password.
    e. **Database Port**: Enter the port number used to access the reporting database.
    f. **Username**: Enter (or verify) your reporting database access user name.
    g. **Password**: Enter your reporting database access password, and click **Next**.
8. Enter a database administrator's logon credentials, click **OK**, and then click **Next**. For an Oracle Database, enter the credentials for the sys 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 Upgrade Procedures.
2. **Certificate Location** - Throughout the 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.
   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 security database server.
   b. **Service Name** - Oracle Database users - Enter the name of the service (TNS alias).
   c. **Username** - Enter your security database access user name.
   d. **Password** - Enter your security database access password.
   e. **Database Port** - Enter the port number used to access the security database server, and then 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. **Username** - Enter (or verify) your reporting database access user name.
   d. **Password** - Enter your reporting database access password.
   e. **Database Port** - Enter the port number used to access the reporting database.
   f. **Username** - Enter (or verify) your reporting database access user name.
   g. **Password** - Enter your reporting database access password, and click **Next**.
8. Enter a database administrator's logon credentials, click **OK**, and then click **Next**. For an Oracle Database, enter the credentials for the sys 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**.

> **Note:**
>
> If multiple Simphony application servers are utilized, upgrade the initial application server to Simphony release 19.1. 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 Simphony application server that was upgraded. For example:

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

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

This section applies only if you are upgrading from the Simphony 2.9 General Release (GR) to a higher release. Review the *Oracle Food and Beverage Compatibility Matrix* and *Oracle MICROS Simphony Release Notes* for information about system requirements.

> **Note:**
>
> Beginning with the Simphony 19.1 release, Microsoft SQL Server is no longer supported as a database platform.

No additional post-upgrade steps are necessary for CAPS on Microsoft Internet Information Services (IIS) if you upgrade from Simphony releases later than Simphony 2.9 GR.

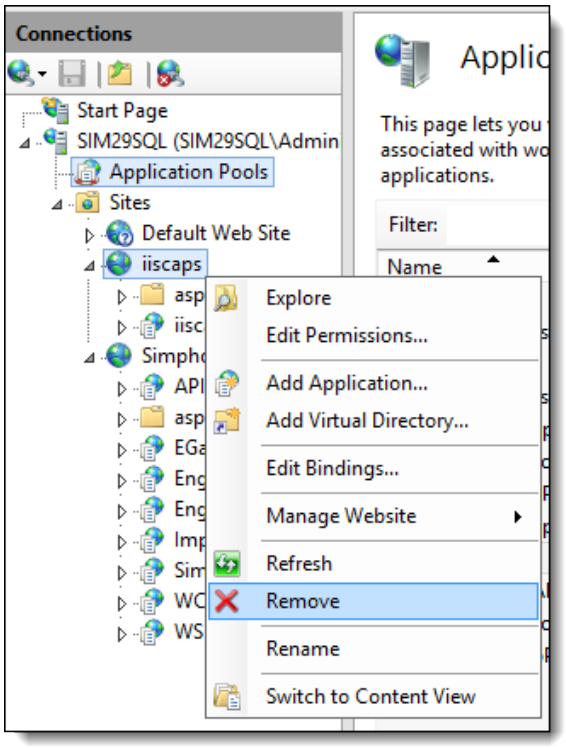
Step 1 - Close and Post All Transactions

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

Step 2 - Access the IIS Manager Console

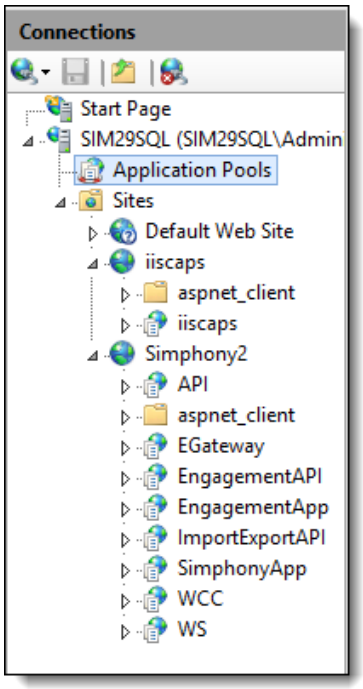
1. From the desktop of each server running CAPS on IIS, select **Start**, **Control Panel**, **Administrative Tools**, and then select **Internet Information Services (IIS) Manager**.
2. From the IIS Connections column, expand the **Sites** folder and right-click the site created for IIS CAPS and select **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 1-2 IIS CAPS Site



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

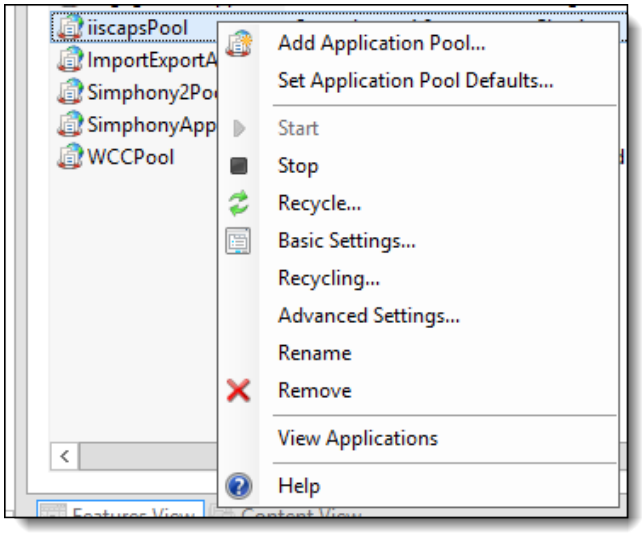
Figure 1-3 Simphony Application Pools



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 1-4 IIS CAPS Application Pool

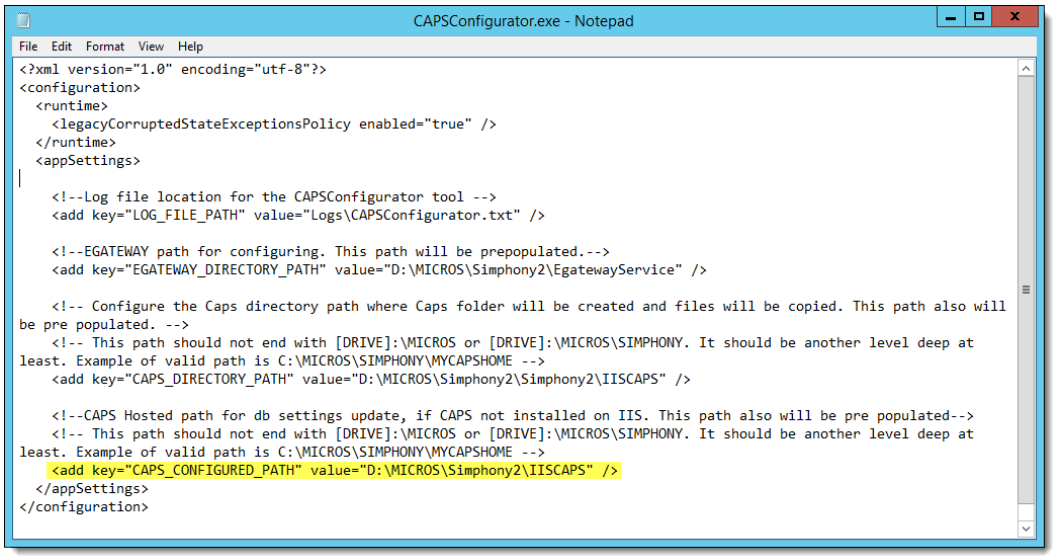


(Optional) Step 3 - Rename the IIS Folder

This step is not required if you are performing an upgrade.

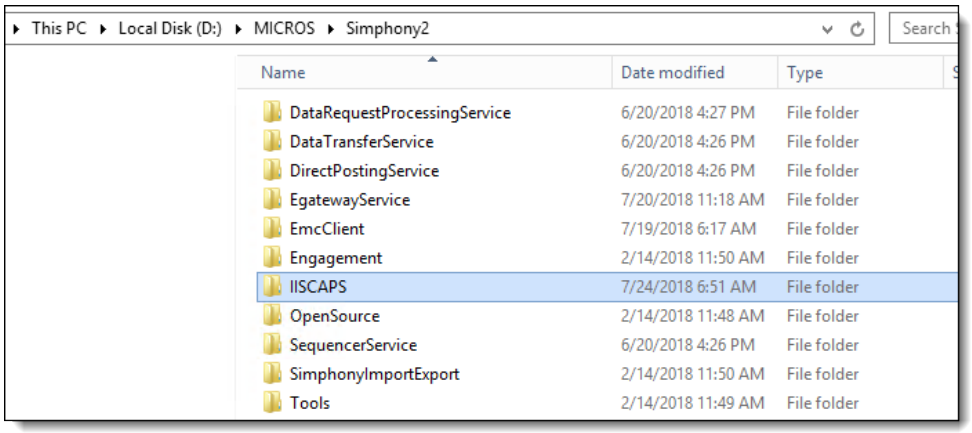
1. Rename the Simphony release 2.9 (or later) IIS CAPS folder.
2. Verify the installed folder path by navigating to the `[Drive]:\MICROS\Simphony2\Tools\CAPSConfigurator\CAPSConfigurator.exe.config` file and open it with a text editor such as Microsoft Notepad.

Figure 1-5 CAPSConfigurator.exe.config IIS CAPS Directory Installation Folder Path



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

Figure 1-6 Default IIS CAPS Folder Installation Path

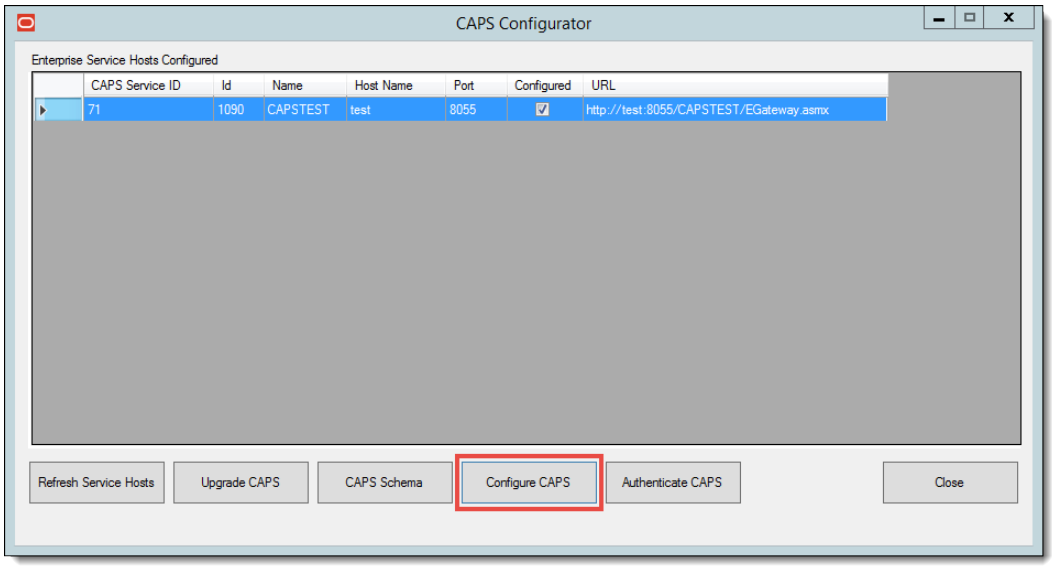


(Optional) Step 4 - Enable an Option and Configure CAPS

This step is not required if you are performing an upgrade.

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 Simphony application server, you can access the CAPS Configurator Tool using this path: `[Drive]:\MICROS\Simphony2\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\Simphony\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 1-7 CAPS Configurator Tool



7. Upon successful installation, verify that the new directory is created along the `[Drive]:\Simphony2\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**.

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

This step is not required if you are performing an upgrade.

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]:\Simphony2\IISCAP_Backup\IISCAPS\DbSettings.xml`).
2. Paste the **DbSettings.xml** file in 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

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]:\Simphony2\EgatewayService\IISCAPSServiceHost\EgatewayLog`.
2. Verify that the tables are upgraded on the existing transaction database.
3. Delete the Simphony release 2.9 CAPS directory (for example, the IISCAP_Backup directory). See Step 3 - Rename the IIS Folder for details.

2

Post-Installation/Upgrade Tasks

Perform all post-installation or upgrade tasks to ensure that the application components and the databases are configured correctly. Provide privileged users with their EMC logon credentials (including the Company Name from the Reporting and Analytics Short Org name). This also applies to the SWP and workstation logon screens.

Updating 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 enable users to access the EMC from other computers on the network.

The *Oracle Hospitality Simphony Manager User Guide*, specifically the **Simphony 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 *Simphony 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 *Simphony Client Deployment Guide* contains more information about configuring and deploying CAL Packages.

Database Size Reduction and System Performance Improvement

To reduce the data footprint of the Simphony Transaction database and to improve overall system performance, you can change the Data Transfer Service (DTS) and data Purging job settings. For brand-new installations, default DTS and Purge job settings have been assigned to assist in controlling the amount of data that is getting stored.

After performing an upgrade, you are required to enable a new employee Roles option to grant permissions for those employees deemed responsible for editing these job settings going forward.

See the *Configuring Access Privileges for Data Transfer Service (DTS) and Data Purge Job Settings* section for instructions for configuring the access privilege.

Listed in the tables below, are the default DTS and data purge job settings.

Table 2-1 Default DTS Job Settings

Default DTS Job Name	Job Settings - Number of Days
Authorizations	2
Definitions	15
Journals	2
Simphony Database Purge	30
Command Module Maintenance	60
Mymicros.net Daily Aggregation	15
Time Zones	30
Labor Definitions	15

Table 2-2 Default Data Purge Job Settings

Default Purge Job Name	Job Settings - Number of Days
Activity Log	30
Audit Trail	90
Authorization Log	30
Checks	7
Client Event Log	30
CM Transaction Detail	7
Import Export	30
Journals	7
KDS Details	7
Queued Checks History	7
Signature Capture	7
Time Cards	60
Totals	7
Transaction Log	90

Configuring Access Privileges for Data Transfer Service (DTS) and Data Purge Job Settings

The option named **10066 – Enable Access to edit Job/Purge Settings**, allows you to control who has access to changing the Data Transfer Service (DTS) and data Purge job settings. For Simphony version 19.1 fresh installations, default DTS and Purge job settings have been assigned to assist in controlling the amount of data that is getting stored. After performing an upgrade, you are required to enable this employee Roles option to grant permissions for those employees deemed responsible for editing these job settings going forward.

To locate and enable the option:

1. Select the Enterprise level, click **Configuration**, and then click **Roles**.
2. Click the **Operations** tab and scroll down to the **Miscellaneous Options** section.
3. Enable the **10066 – Enable Access to edit Job/Purge Settings** option and **Save**.

Enabling Communication Between the Enterprise and Workstations

To allow the workstations in the property to communicate with the Enterprise, 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:

- 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 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.

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 Simphony EMC Using Multi-Factor Authentication

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

1. When first attempting to log in to the Simphony 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**.

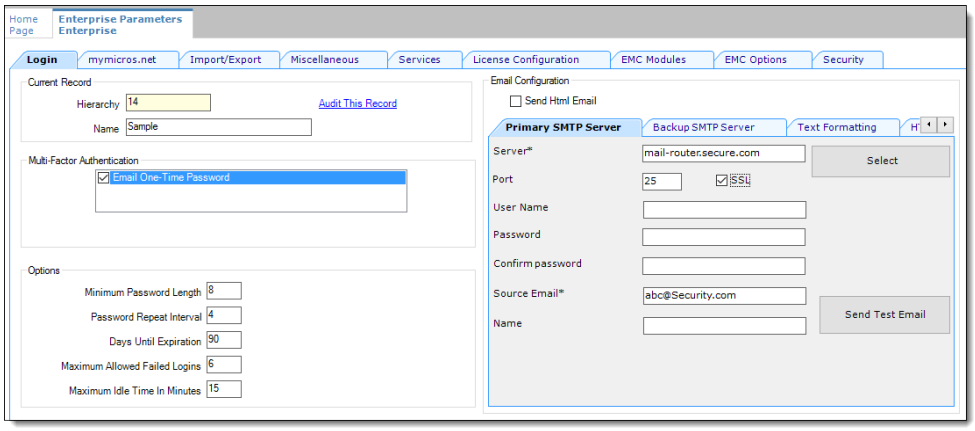
   OTPs are only valid for five minutes, so enter your OTP password in a timely manner. If the five-minute threshold is exceeded, you are required to re-login to the EMC to generate another OTP. OTPs are valid for one single entry for the individual attempting to log in to the EMC at that time. After entering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



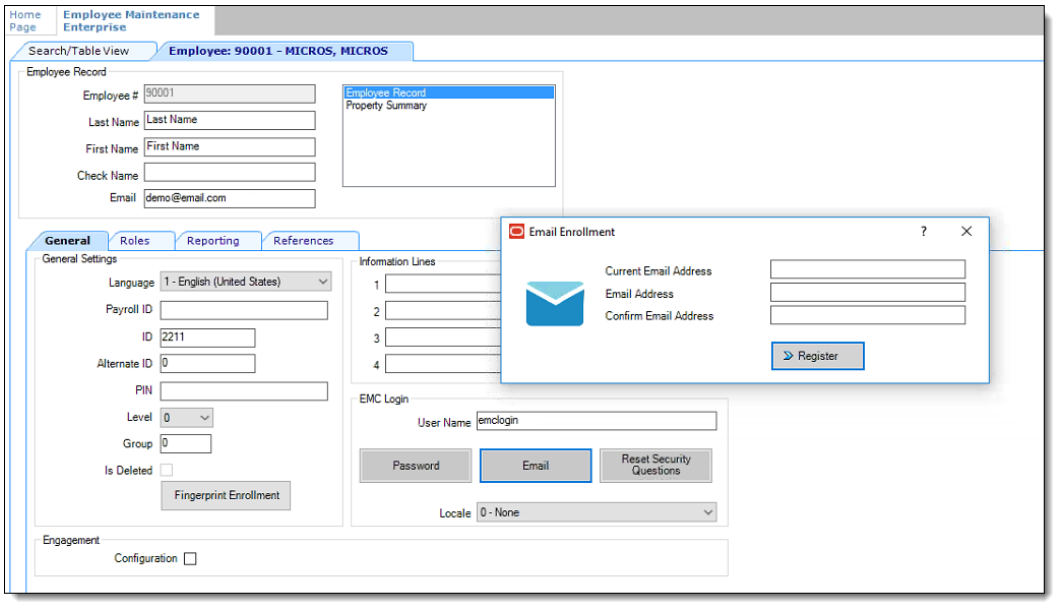
3. From the Email Configuration section, select the **Primary SMTP Server** subtab and enter the required settings in the fields listed below:
   a. **Server**: Enter either the IP address (IPv4 Address) or the name of the Primary SMTP server. Click the **Select** button to choose an email provider, 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 Simphony 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 Simphony 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.

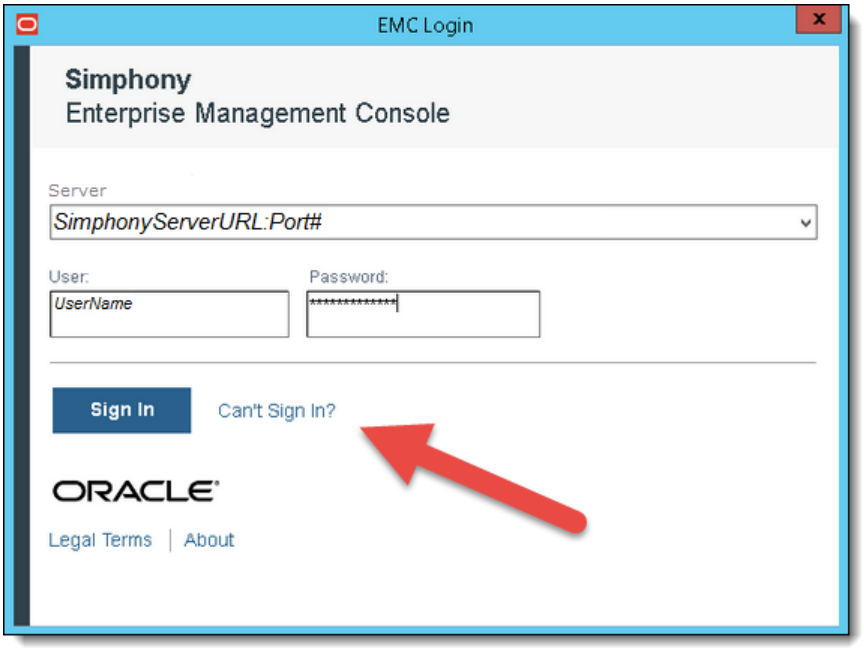
Prerequisites

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?

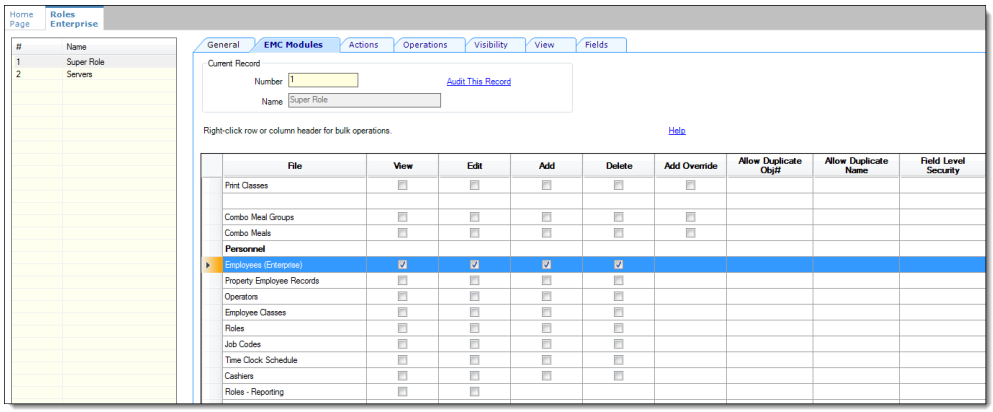


Configuring Access Privileges for Resetting a Password

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

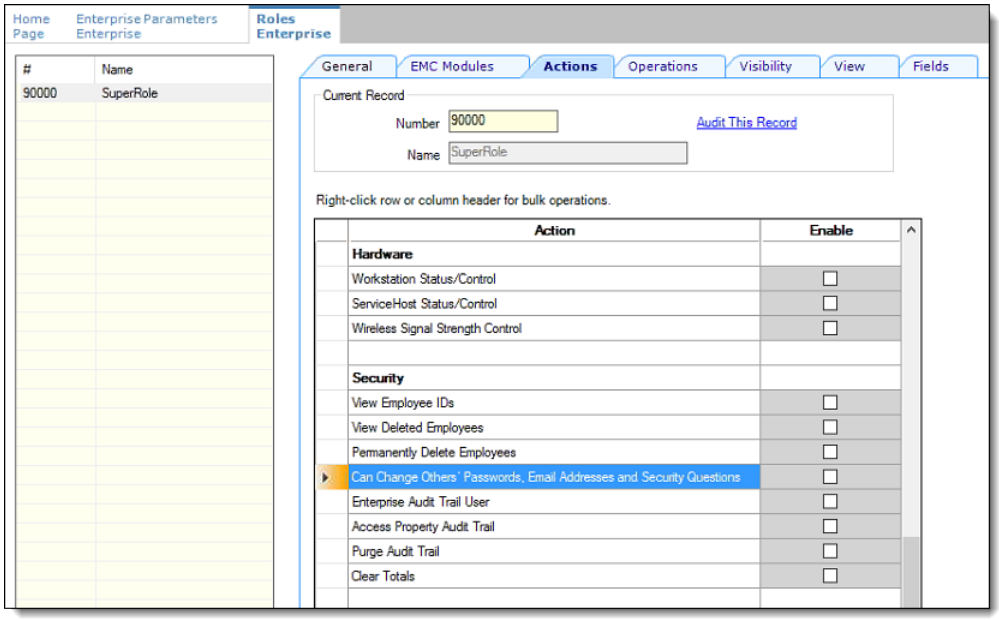
1. Select the **Enterprise level** , click **Configuration**, and then click **Roles**.
2. Click the **EMC Modules** tab and scroll to the **Personnel** section.
3. Select the options for the **Employees (Enterprise)** access privileges for each of the following columns:
   - **View**
   - **Edit**
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



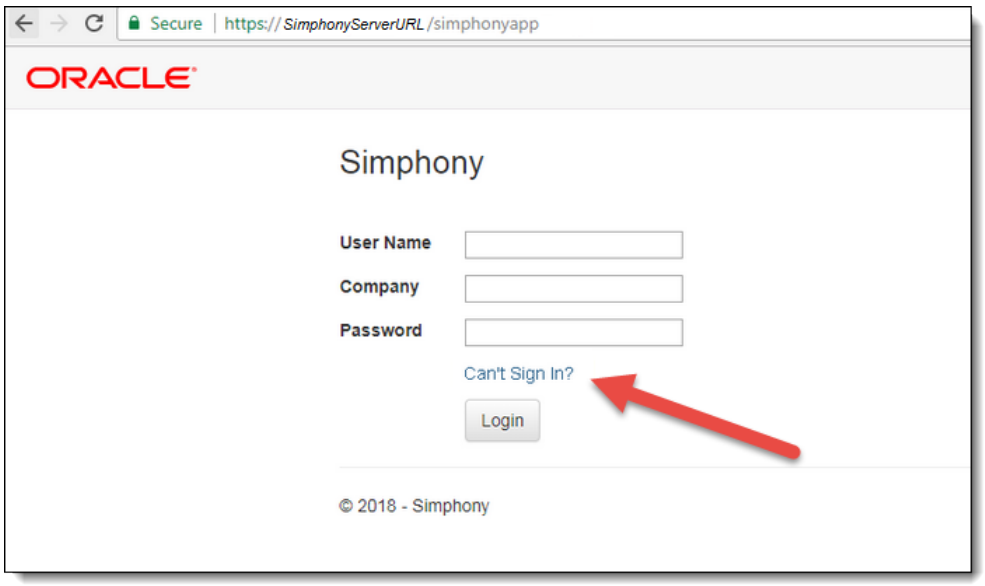
7. Ensure that all users requiring Multi-Factor Authentication (MFA) configuration permissions are assigned a role that have these access privileges enabled.

Resetting Passwords from the Simphony Web Portal

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

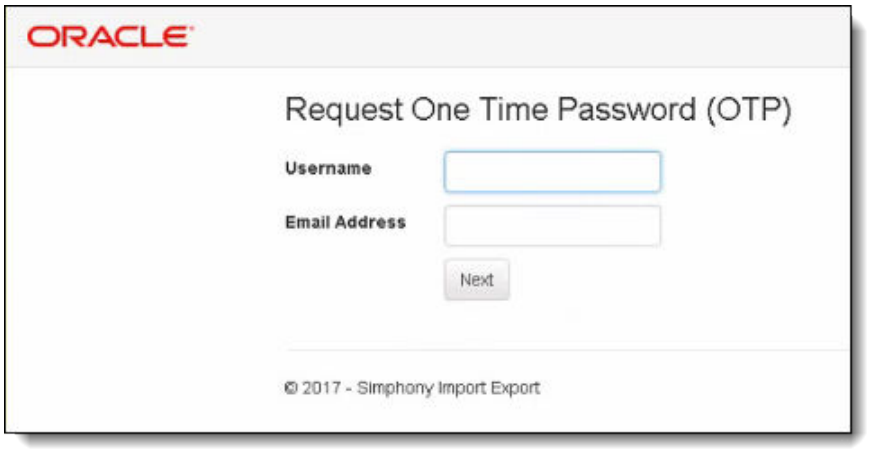
1. Open the Simphony Web Portal URL. When prompted, enter your **User Name**, and then click the **Can't Sign In?** link. You are provided with a One Time Password (OTP) via email.

Figure 3-6 Simphony 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

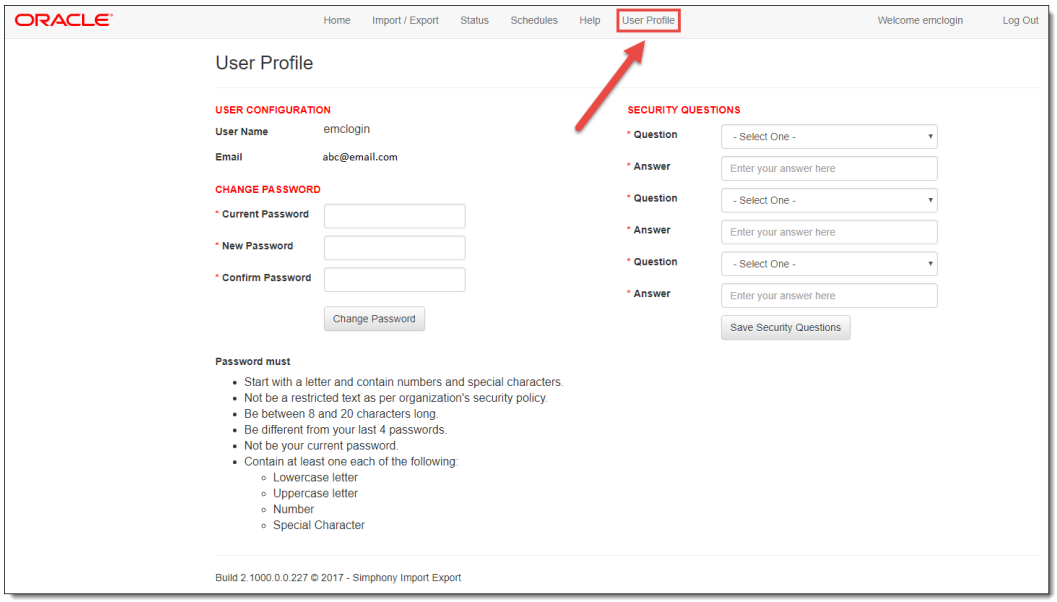


3. The system validates the information you entered, and shows a details page where you must correctly answer your security questions as configured in the system. Upon entering your validated logon and security question responses, an OTP token is sent to your email account, and you are redirected to 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



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.

1. Select the **Enterprise**, click **Setup**, and then click **Enterprise Parameters**.
2. Click the **Login** tab.
3. 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 Simphony, 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 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

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**. Simphony release 19.1 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 *Simphony 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 Simphony release 2.9.1 or later, 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 Simphony 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**.