# Infor SunSystems Installation Guide

Release 6.4.0

### Important Notices

The material contained in this publication (including any supplementary information) constitutes and contains confidential and proprietary information of Infor.

By gaining access to the attached, you acknowledge and agree that the material (including any modification, translation or adaptation of the material) and all copyright, trade secrets and all other right, title and interest therein, are the sole property of Infor and that you shall not gain right, title or interest in the material (including any modification, translation or adaptation of the material) by virtue of your review thereof other than the non-exclusive right to use the material solely in connection with and the furtherance of your license and use of software made available to your company from Infor pursuant to a separate agreement, the terms of which separate agreement shall govern your use of this material and all supplemental related materials ("Purpose").

In addition, by accessing the enclosed material, you acknowledge and agree that you are required to maintain such material in strict confidence and that your use of such material is limited to the Purpose described above. Although Infor has taken due care to ensure that the material included in this publication is accurate and complete, Infor cannot warrant that the information contained in this publication is complete, does not contain typographical or other errors, or will meet your specific requirements. As such, Infor does not assume and hereby disclaims all liability, consequential or otherwise, for any loss or damage to any person or entity which is caused by or relates to errors or omissions in this publication (including any supplementary information), whether such errors or omissions result from negligence, accident or any other cause.

Without limitation, U.S. export control laws and other applicable export and import laws govern your use of this material and you will neither export or re-export, directly or indirectly, this material nor any related materials or supplemental information in violation of such laws, or use such materials for any purpose prohibited by such laws.

### Trademark Acknowledgements



Publication Information

Release: Infor SunSystems 6.4.0
Publication Date: January 7, 2022
Document code: ss_6.4.0_install__en-us

# Contents

# About this guide

### Version 6.4A

This guide describes the steps to install SunSystems 6.4, where no previous SunSystems installation exists, or the previous installation has been removed. It provides details of mandatory pre-installation checks, the installation process, and post-installation tasks. It also provides supplementary reference information.

### Intended audience

This document is intended for system administrators, SunSystems consultants and channel partner consultants involved in deploying and maintaining SunSystems. Due to the numerous implementation options for SunSystems, only experienced installers should perform the installation process.

## Related documents

SunSystems documentation consists of user guides, such as the installation and upgrade guides, and online application help.

User guides are in PDF format and are available from the Infor Support Portal. To access documentation on the Infor Support Portal, select **Search > Browse Documentation**. We recommend that you check this portal periodically for updated documentation.

**Release Notes**
Details information relevant to this release that is not included elsewhere in the SunSystems documentation.

**What's New**
Highlights significant changes or enhancements in the release.

**Resolved Issues**
Describes issues resolved in the latest release.

**Infor SunSystems Architecture and Planning Guide**
Provides an architectural overview of the software. Refer to this guide when planning the deployment of SunSystems.

**Infor SunSystems Installation Guide**
Describes installing SunSystems in multiple deployment scenarios.
**Note:** Review the installation guides before making any changes to your SunSystems environment.

**Infor SunSystems Standalone Installation Guide**
Describes installing SunSystems on a single machine. No other environment is described.

**Infor SunSystems Upgrade Guide**
Describes upgrading SunSystems from an existing deployment.

**Guide to Migrating Data from SunSystems 4**
Describes migrating data from an existing SunSystems v4 installation, into SunSystems v6.

### SunSystems online help

Provides details of day-to-day operational tasks and is displayed while you are using SunSystems. The help files can be accessed from the cloud at https://docs.infor.com/en-us/sunsystems/6.4.x. See KB1859777 for instructions on how to download online help to a local server in your environment. See Configuration Manager in the online help for more information.

Read the Administrator Help after successful installation of SunSystems. There are specific tasks that must be carried out before the installation can be used and the Administrator Help provides details of setup and maintenance. The tasks are those that are normally expected of an application consultant or a systems administrator.

Tasks in the Administrator Help are broken into four areas:

- Tasks that are appropriate to SunSystems modules
- Generic tasks appropriate to all installations of SunSystems
- Financial tasks that are relevant only if the Financials modules are installed
- Order Fulfilment tasks that are relevant only if the Order Fulfilment modules are installed.

These topic modules are included in the online help.

- System Basics
- Modules
  - Financials
  - Order Fulfilment
  - SunSystems Connect
    - SSC Technical Reference
  - Transfer Desk
  - Transfer Desk Web
  - Enterprise Data Management
- Administration
  - Administrator Help
  - User Manager
  - Security Console
  - Configuration Manager
  - Integration Configuration
  - Financials Administration

- Order Fulfilment Administration
- Customization
  - User Group Menu Designer
  - Form Designer
  - Filter Designer
  - Formula Designer
  - Drill Association Designer
  - Data Description Editor
- Reporting
  - Report Designer
  - Report Manager.

# Contacting Infor

If you have questions about Infor products, go to Infor Concierge at https://concierge.infor.com/ and create a support incident.

The latest documentation is available from docs.infor.com or from the Infor Support Portal. To access documentation on the Infor Support Portal, select **Search > Browse Documentation**. We recommend that you check this portal periodically for updated documentation.

If you have comments about Infor documentation, contact documentation@infor.com.

# Chapter 1: Installing SunSystems in a multitier environment

This installation guide describes the installation of SunSystems 6.4 over multiple tiers.

Refer to the *Standalone Installation Guide for SunSystems v6.4* if you are running a simple installation of SunSystems.

Refer to the *SunSystems Upgrade Guide* if you are upgrading from SunSystems 6.2 or SunSystems 6.3.

**Note:** If you have an installation of SunSystems 6.4 and are updating it to the latest patch set, refer to the *SunSystems 6.4 Patch Set Installation Note* available with the patch set. The Installation Note contains important instructions which are not included in this Installation Guide.
**Note:** The SunSystems 6.4 installer is English language only. Language Deployer is used to add or remove languages from a SunSystems installation.

## Accessing SunSystems

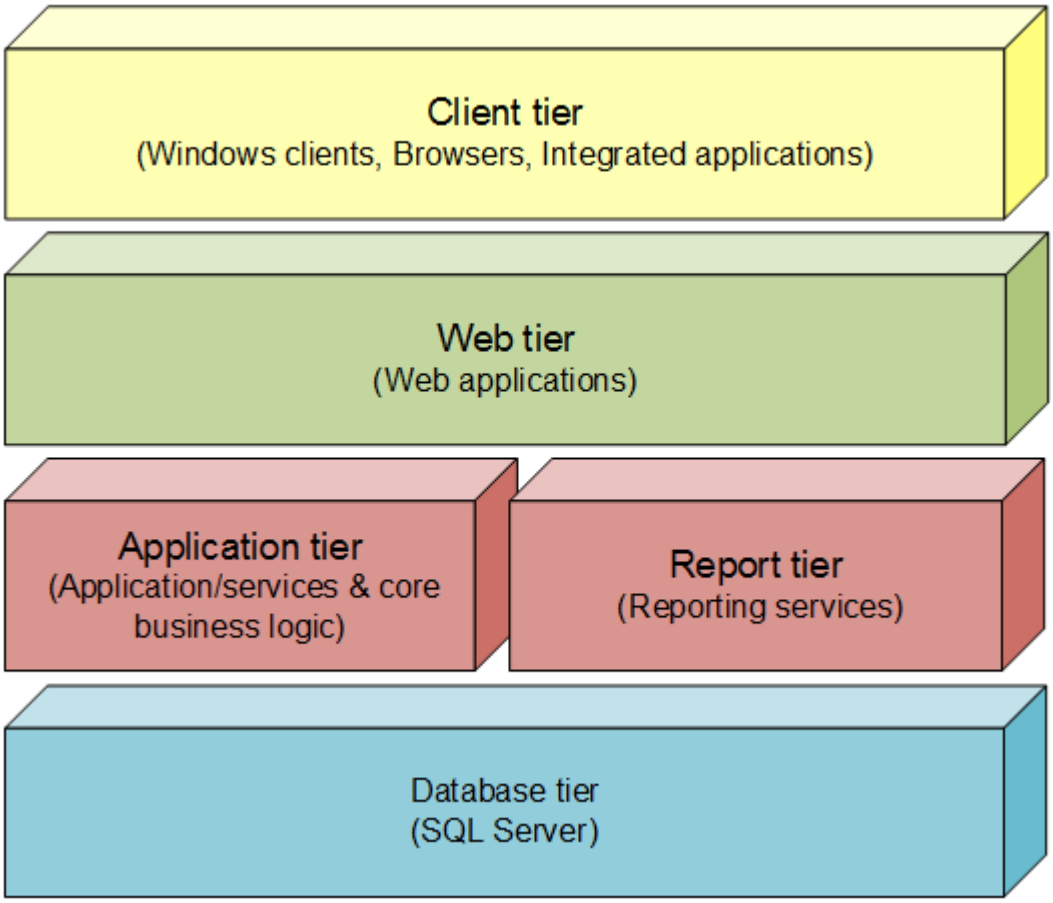
After a successful installation, SunSystems v6.4 can be accessed from an icon on the desktop, or from a URL:

`http://<FQDN>/sunsystems`

**Note:** The SunSystems URL is case sensitive.

## Architectural overview

A SunSystems implementation comprises software components that can be logically divided into distinct layers, or tiers, and is consistent with modern software design. Although the practical installation of the software can vary greatly, the logical tiers that define the software are always present.




This logical split is represented by the deployed components. It facilitates the differentiation between tiers that are publicly accessible, that is, exposed on the Internet, and private tiers that are only accessed internally.

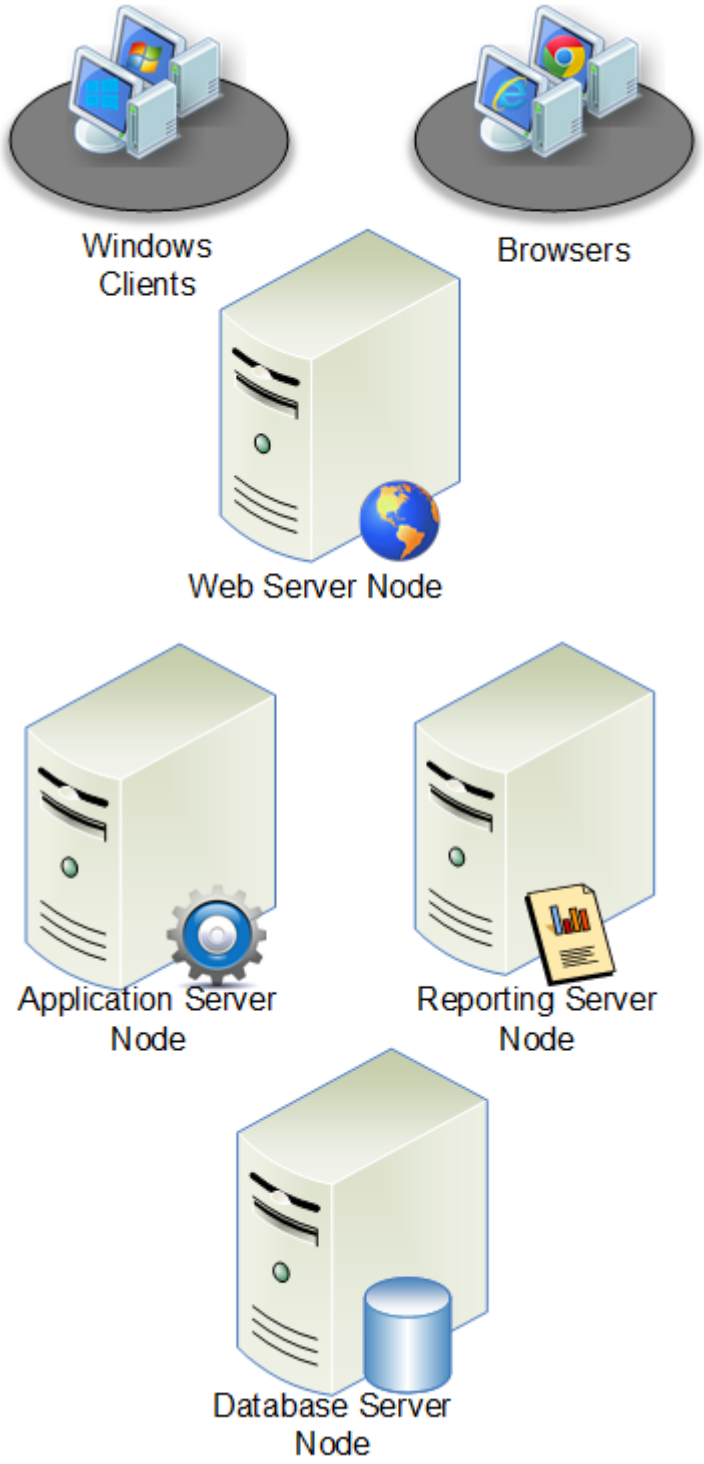
# Deployment nodes

The logical tiers in a SunSystems deployment consist of discrete node types. These map to a server instance that can be physical or virtual. The server instance corresponds to the installable components available from the SunSystems media. The exceptions to this are the Database and Reporting Server nodes; these correspond to the installable components available from Microsoft SQL Server media.

All software components can be deployed on a single server. More commonly, individual components are selected to build a customized, multitiered solution that meets deployment requirements, for example, for specific security or scalability needs.

This section describes each logical tier, its composition, scalability characteristics, and deployment considerations.

This diagram shows each logical tier with a brief description of its function.




**1** Web server node

Includes the software components with a browser interface/API. This makes public, or Internet, components easy to configure and, more importantly, to secure.

**2** Application server node

Includes the application services and APIs. These are required to support the web server node and the rich client components, and may include supporting web applications.

**3** Reporting server node

Includes Microsoft SQL Server Reporting Services (SSRS) and SSRS extensions. These extensions are required for SunSystems reporting. The node can be deployed with the database server or deployed separately depending on the scale of the solution. SSRS is installed using the Microsoft SQL Server installation media.

**4** Database server node

Microsoft SQL Server is used as the relational database management server for SunSystems. This node comprises all SunSystems databases and associated logins. Often the reporting server node and the database server node are the same, for simplicity and to reduce licensing costs.

# Installing SunSystems for the first time

If you are installing SunSystems for the first time, note that the servers on which Infor applications are installed should be member servers in a domain. They should be dedicated to the Infor applications. If not, then performance may be affected. The servers should not be:

- a primary or back-up domain controller, running Active Directory
- a mail server running Exchange or other mail
- a file or print server other than for SunSystems
- a virtualization host server running Hyper-V, VMware, ESXi, or Citrix XenServer
- an Intranet or Internet server, running Internet Information Server, Apache or similar, other than for SunSystems
- a Microsoft Small Business Server.
  **Note:** If deploying on Microsoft Small Business Server, Infor software must be installed in dedicated virtual images and not on the host operating system. This is subject to the supporting software environment meeting the minimum software requirements. If performance issues arise, separation onto dedicated hardware may be necessary.

If a SunSystems component is installed on a computer (physical or virtual) included in the list, the installation cannot be supported. If you are unsure, check with your local support region for further clarification before deploying the configuration.

**Caution:** Computer names should follow Microsoft naming conventions. In addition, you should not include the '_' underscore character in computer names as this causes problems for Tomcat and Java components.

# Windows service packs

The latest service pack should be applied to your Windows operating system before installing SunSystems components.

# Chapter 2: Installation prerequisites

To ensure a successful installation of SunSystems you must complete the prerequisites checklist for each node.

## Prerequisites checklist

The installation prerequisites are defined by node. Refer to the relevant prerequisites checklist when installing each node.

| ✓ | Task | References |
|---|---|---|
| | Design your implementation | *Architecture and Planning Guide for SunSystems* on Infor Support Portal |
| | In Active Directory, create SunSystemsServices and SunSystemsClients groups, and create the svc-SunSystems user and the SunSystemsReporting user | Creating users and groups in Active Directory on page 17 |
| | Complete the prerequisite checklist for the database and reporting server tiers | Prerequisites checklist for the database and reporting server tiers on page 18 |
| | Complete the prerequisite checklist for the application and web server tiers | Prerequisites checklist for the application and web server tiers on page 23 |
| | Complete the prerequisite checklist for the Windows client tier | Prerequisites checklist for the Windows client tier on page 27 |

## Creating users and groups in Active Directory

In Active Directory, you must create two domain Windows groups: one for the SunSystems services, for example, **`SunSystemsServices`**, and one for the SunSystems clients, for example, **`SunSystemsClients`**.

During installation, db_owner rights to the SunSystems databases is assigned to the **SunSystemsServices** group.

The Windows credentials of SunSystems users are added to the **SunSystemsClients** group. This is only required only for functions that make a direct connection to the database, for example, Bill of Materials Management (BOMM). You must set the AppRole.

You must create two domain service accounts, one for the SunSystems Reporting service and one for all other SunSystems services and app pools (in IIS), These service accounts must be added to the SunSystemsServices group.

For example, create the **SunSystemsReporting** service account for the SunSystems Reporting service, and the **svc-SunSystems** service account, for all other SunSystems services.

The SunSystems databases are accessed by Reporting Services.

You must give **Log on as a service** right to the **SunSystemsReporting** account for all web servers, application Servers and reporting servers. Give the **svc-SunSystems** domain user **Log on as a service** right on all application servers and all web servers.

Create users and groups in Active Directory:

1. Create the **SunSystemsServices** and **SunSystemsClients** groups.
2. Create the **SunSystemsReporting** and **svc-SunSystems** service accounts.
3. Add the users **SunSystemsReporting** and **svc-SunSystems** to the **SunSystemsServices** domain group
4. Run `secpol.msc` to launch Local Security Policy.
5. Select **Local Policies > User Rights Assignment**.
6. Select **Log on as a service** and right-click to open **Properties**.
7. Click **Add User or Group**.
8. Specify this information:

   **Enter the object names to select**
   Specify the **SunSystemsReporting** and **svc-SunSystems** service accounts. Click **Check Names** to ensure they are recognized.

9. Click **OK**.

# Prerequisites checklist for the database and reporting server tiers

Complete these tasks:

| ✓ | Server | Task | References |
|---|---|---|---|
| | • database server<br>• reporting server | Ensure the servers comply with the hardware requirements | Operating system requirements on page 19 |

| ✓ | Server | Task | References |
|---|---|---|---|
| | • database server<br>• reporting server | Install Microsoft .NET and add the Microsoft .NET features. Both are required on any tier where SunSystems software is installed. | Installing Microsoft .NET on page 24<br>Adding Microsoft .NET features on page 24 |
| | database server | Install and configure Microsoft SQL Server | Microsoft SQL Server and Reporting services on page 20<br>Microsoft SQL Server requirements on page 20<br>Installing Microsoft SQL Server on page 20 |
| | reporting server | Install and configure Microsoft Reporting Services and assign the **`SunSystemsReporting`** user as the reporting service account. | Installing Microsoft Reporting Services on page 21 |
| | | For SQL Server 2019 installations, additional file type extensions are required for SSRS | Adding file extensions to SQL Server Reporting Services on page 22 |
| | • database server<br>• reporting server | Check the firewall status | |

## Operating system requirements

| Operating systems (64-bit only) | Entry level recommendation |
|---|---|
| Windows 2022 Standard Edition and DataCenter Edition | Dual Core 3Ghz 8GB RAM |
| Windows 2019 Standard Edition or above | Dual Core 3Ghz 8GB RAM |
| Windows 2016 Standard Edition or above | Dual Core 3Ghz 8GB RAM |
| Windows 2012 R2 Standard Edition or above | Dual Core 3Ghz 8GB RAM |
| Windows 10 | Dual Core 3Ghz 8GB RAM |
| Windows 8.1 | (Client) |

# Microsoft SQL Server and Reporting services

If you are installing SQL Server 2016 then the option to install Reporting Services is included with Microsoft SQL Server. Do not select Reporting Services if you are installing the Report server on a separate tier because SQL Management Tools are included in a separate Report tier.

You must assign the SunSystemsReporting user as the reporting service account to enable access for Reporting Services to the SunSystems databases.

**Note:**

- If you are installing SunSystems in a multitier environment, and you are installing the database and reporting tiers on separate servers, then you must install Reporting Services on the reporting server.
- In a multitier environment, you must install the SQL Server Command-Line Utilities on the application server tier if you plan to install the SunSystems v63 Language Pack. This ensures that `bcp.exe` is available from the application server.
- Microsoft SQL Server does not give the sysadmin role to NT AUTHORITY\SYSTEM (Local System). No change to this is required on a multitier installation because all services will be run by domain service accounts.

## Microsoft SQL Server requirements

| Software | Notes |
|---|---|
| Microsoft SQL Server 2019 (Standard edition or above) | SQL Server Reporting Services and Management Tools are both separate installations<br>**Note:** Additional file type extensions are required for SSRS |
| Microsoft SQL Server 2017 (Standard edition or above) | SQL Server Reporting Services and Management Tools are both separate installations. |
| Microsoft SQL Server 2016 (Standard edition or above) | Features to include:<br>• Database Server<br>• Reporting Services (Native) (do not select if installing separately in a multitier environment)<br>• Management Tools (separate installer in SQL 2016) |

### Installing Microsoft SQL Server

**Note:** If you are installing SunSystems in a multitier environment, you must install Microsoft SQL Server on the database server tier.

1. Ensure you are using Microsoft SQL Server 2019, 2017 or 2016.
2. Run the Microsoft SQL Server installer.

3 Select **Installation > New SQL Server stand-alone installation or add features to an existing installation**
4 Select **Feature Selection** and select **Database Engine Services** as the installation feature.
5 Click **Install**.
6 Install the latest Service Pack and cumulative patch for SQL Server.
7 Install SQL Server Management Tools after the installation has completed:
   **a** Run the SQL Server Management installer.
   **b** Select **Installation > Install SQL Server Management Tools**.
   **c** Select the most recent version.

   **Note:** If a restart of the server is required, you are prompted by the installer.

## Installing Microsoft Reporting Services

Microsoft Reporting Services must be installed on the reporting tier:

1 Run the Microsoft SQL Server installer.
2 From the Installation menu, select **Install SQL Server Reporting Services**.
3 When the setup is complete, select **Configure Report Server**.
4 To create the Report Server database, select **Change Database > Create a new report server database** and click **Next > Next**.
5 Specify this information:

   **Service Account**
   Specify the **`<localmachine>\SunSystemsReportingService`** account as this user.

   **Password**
   Specify the password.

6 Backup the encryption key.
7 Specify the **Web Services URL** and **Web Portal URL**.
8 Check that the web browsers open without error:
   a Click the **Web Services URL** to ensure that the browser opens without error.
   b Click the **Web Portal URL** to ensure that the browser opens without error.

   You can also access this through Reporting Services Configuration Manager.

   **Note:** If the Web Services URL and Web Portal URL browsers open with error, you may need to delete encrypted content. Before doing so, you must make sure that SQL Server Reporting Services is not used by any other application that might use the encrypted content.
9 Check that TCP/IP is an enabled protocol for SQL Server Network Configuration. In SQL Server Configuration Manager, select the correct version of Configuration Manager to run:

| SQL Server version | Configuration Manager |
|---|---|
| SQL Server 2019 | `SQLServerManager15.msc` |
| SQL Server 2017 | `SQLServerManager14.msc` |

| SQL Server version | Configuration Manager |
|---|---|
| SQL Server 2016 | `SQLServerManager13.msc` |

a Open Microsoft SQL Server Configuration Manager.
b Expand the SQL Server Network Configuration.
c Click **Protocols for MSSQLSERVER** to ensure TCP/IP is enabled.

## Installing SQL Server Management Studio

Complete these steps to install Microsoft SQL Server Management Studio

1. Run the Microsoft SQL Server Installer.
2. Select **Installation > Install SQL Server Management Tools**.
3. Complete the installation.

   **Note:** You are prompted by the installer if you are required to restart.

## Adding file extensions to SQL Server Reporting Services

In Microsoft SQL Server 2019, specific file type extensions are required to import the example reports. These are included in the **AllowedResourceExtensionsForUpload** and **TrustedFileFormat** system properties in SSRS.

You must ensure that all necessary file type extensions are added before the example reports are imported.

**Note:** If the SSRS databases are recreated, then the file type extensions for both system properties revert to their default values.

Complete these steps:

1. Open SQL Server Management Studio.
2. In Object Explorer, select **Connect > Reporting Services**.
3. Right-click the report server name and select **Properties > Advanced**.

   **Note:** If the **Properties** option is unavailable, then you must add your SSMS login as a system administrator in SSRS.
4. Check that these file extensions are included in the list for **AllowedResourceExtensionsForUpload**:
   - `*.log`
   - `*.mhtml`
   - `*.csv`
   - `*.xlsx`

   If one of the values is missing then you must add it to the list.
5. Check that these file extensions are included in the list for **TrustedFileFormat**:
   - `txt`
   - `log`

- xsl
- doc
- docx
- tif
- tiff
- xml
- csv
- xlsx
- mhtml
- emf

If one of the values is missing then you must add it to the list.

6 Restart the SQL Server Reporting Services.

# Prerequisites checklist for the application and web server tiers

Complete these tasks:

| ✓ | Server | Task | References |
|---|---|---|---|
| | | Ensure the servers comply with the hardware requirements | Operating system requirements on page 19 |
| | application and web | Install Microsoft .NET and add the Microsoft .NET features. Both are required on any tier where SunSystems software is installed. | Installing Microsoft .NET on page 24<br>Adding Microsoft .NET features on page 24 |
| | application and web | Add Internet Information Services (IIS) roles | Adding the IIS role on page 25 |
| | application and web | Disable Default Website in IIS | Disabling Default Website in IIS on page 25 |
| | application and web | Install Oracle OpenJDK | Installing or updating Oracle OpenJDK on page 26 |
| | application and web | Install Apache Tomcat | Installing or updating Apache Tomcat on page 26 |
| | application only | Install SQL Server ODBC driver | Installing Microsoft SQL Server ODBC driver on page 27 |

| ✓ | Server | Task | References |
|---|---|---|---|
| | application and web | Install Application Request Routing (ARR) | Installing IIS Application Request Routing (ARR) on page 27 |
| | application and web | Check firewall status | |
| | application only | Ensure you have a valid SunSystems serialization file available. | |

## Installing Microsoft .NET

You must install Microsoft .NET by downloading it from the Microsoft website. Ensure you comply with the prerequisite Internet Security settings.

**Note:** You must install .NET 4.8 on all tiers.

To install Microsoft .NET:

1. Apply the required settings in Internet Security Settings:

   **Note:** This step must be completed before downloading .NET.

   a. Open Control Panel and select **Internet Options > Security > Custom Level**.
   b. Scroll to Downloads and select **Enable** in **File Download**.
   c. Select **Enable** in **Enable .NET Framework setup**.
2. Download and install .NET 4.8.
3. Restart the server.

## Adding Microsoft .NET features

These features must be added for Microsoft .NET:

1. Open Windows Control Panel and go to Programs and Features. Or, run `appwiz.cpl` from the Windows command prompt.
2. Select **Turn Windows features on or off**.
3. Select **`.NET Framework 4.8 Advanced Services`**.
4. Select these features:
   - **`ASP.NET 4.8`**
   - **`WCF Services`**
     - **`HTTP Activation`**
     - **`Message Queuing (MSMQ) Activation`**
     - **`Named Pipe Activation`**
     - **`TCP Port Sharing`**
5. Click **OK**.

## Adding the IIS role

**Note:** The IIS role is required on application and web tier servers.
**Note:** The IIS role is added first because the "Add Roles and Features Wizard" selects roles first.

Add these features to the IIS installation:

1. Open Server Manager and select **Add Roles and Features > Server Roles**.
2. Select **Web Server (IIS) > Web Server**.
3. Expand **Common HTTP Features** and select these features:
   - Default Document
   - Directory Browsing
   - HTTP Errors
   - Static Content
   - HTTP Redirection.
4. Expand **Health and Diagnostics** and select these features:
   - HTTP Logging
   - Custom Logging
   - Logging Tools
   - Request Monitor
   - Tracing.
5. Expand **Performance** and select these features:
   - Static Content Compression.
6. Expand **Security** and select these features:
   - Request Filtering
   - Basic Authentication
   - Digest Authentication
   - Windows Authentication.
7. Expand **Application Development** and select these features:
   - .NET Extensibility 3.8
   - ASP.NET 4.8
   - ISAPI Extensions
   - ISAPI Filters.
8. Go to **Web Server (IIS) > Management Tools** and select these features:
   - IIS Management Console.

## Disabling Default Website in IIS

**Note:** You may specify a different port for SunSystems during installation, if required.

Port 80 is used by SunSystems, by default. To enable this, you must disable the default website in IIS before installing SunSystems:

1. Open Default Website from Internet Information Services (IIS).
2. Select **Manage Website**.
3. Click **Stop**.

## Installing or updating Oracle OpenJDK

Oracle OpenJDK and Tomcat are prerequisites for SunSystems and must be maintained with the latest performance and security enhancements. Windows environment variables are used by SunSystems to establish the location of these local installations.

You must use the latest version to ensure your environment has the most recent security updates for Oracle Java Development Kit:

1. Download the `zip` file for Windows/x64 from https://jdk.java.net/17/
2. Unzip the file into `C:\JavaPlatform` or an equivalent folder and update the `SUNSYS_JAVA_HOME64` environment variable with this location.

   **Note:**

   - If you are updating Java on an existing installation, then you must run Restart Services after updating the Java environment variable.
   - If you are installing SunSystems, then `SUNSYS_JAVA_HOME64` is set during the installation process.

## Installing or updating Apache Tomcat

Use the latest version of Apache Tomcat 9 to ensure your environment has the most recent security updates.

**Note:** Apache Tomcat 10 is not supported.

To install or update Apache Tomcat, complete these steps:

1. If you are updating an existing SunSystems installation, all SunSystems users must be logged out and all SunSystems services must be stopped.
2. Open `https://tomcat.apache.org/download-90.cgi`.
3. Browse to **Core** under **Binary Distributions**, and click **zip**. This downloads the Apache Tomcat file, for example, `apache-tomcat-9.0.45.zip`.

   **Note:** You must use the core zip, not the Windows zip.
4. Unzip and save the files to `C:\JavaPlatform` or an equivalent folder.
5. If you are updating java on an existing SunSystems installation, then you must specify the installation directory in the `SUNSYS_TOMCAT_HOME` environment variable and run Restart Services. If you are installing a new version of SunSystems, then `SUNSYS_TOMCAT_HOME` is set during the installation process.
6. If required, run Restart Services.

## Installing Microsoft SQL Server ODBC driver

Download the latest version of Microsoft ODBC Driver for SQL Server for Windows x64. We recommend that you install this version or higher, if you want to ensure that security protocol TLS 1.2 is supported. SunSystems DeployAgent detects the highest version of ODBC driver installed and configures SunSystems to use it.

**Note:** TLS 1.2 is supported by SunSystems. For security reasons, it is your responsibility to disable security protocols TLS 1.0 and TLS 1.1 and earlier.

1. Open https://www.microsoft.com/en-us/download/details.aspx?id=53339
2. Select **`x64\msodbcsql.msi`** and click **Next**.
   The download should start automatically.
3. Run **`msodbcsql.msi`** on your application server.

## Installing IIS Application Request Routing (ARR)

Install IIS Application Request Routing 3.0 (x64) from the Microsoft website:

1. Open https://www.iis.net/downloads/microsoft/application-request-routing .
2. Click **Install this extension**.
3. Click **Products** on the **Web Platform Installer 5.0** dialog.
   Ensure that Application Request Routing 3.0 and URL Rewrite 2.0 are installed.
4. Close the **Web Platform Installer 5.0** dialog.

# Prerequisites checklist for the Windows client tier

Complete these tasks:

| ✓ | Task | References |
|---|---|---|
| | Ensure the Windows client complies with the hardware requirements | Operating system requirements on page 19 |
| | Ensure the SunSystems Administrator is a member of the Configuration Administrators group in User Manager. | |
| | Install Microsoft .NET and add the Microsoft .NET features. Both are required on any tier where SunSystems software is installed. | Installing Microsoft .NET on page 24<br>Adding Microsoft .NET features on page 24 |
| | Install Oracle Java JDK | Installing or updating Oracle OpenJDK on page 26 |

| ✓ | Task | References |
|---|---|---|
| | Download and install the latest version of Adobe Acrobat Reader from the Adobe website | |
| | Ensure you are using a supported web browser | Supported web browsers on page 28 |

## Supported web browsers

These web browsers are supported:

- Microsoft Chromium Edge
- Chrome
- Safari 13 or later.

**Note:** To access SunSystems online help using Safari, you must allow pop-up windows. Select **Safari > Preferences**, click **Security** and clear **Block pop-up windows**.

# Chapter 3: Installing SunSystems

Install SunSystems following the steps listed in the Installation Checklist.

To start the installation process, you must download the SunSystems ISO and run the installer.

The installation process is broken down into tiers:

- Installing the database tier
- Installing the application tier
- Installing the reporting tier
- Installing the web tier
- Installing the Windows client

This chapter also covers other aspects of the installation:

- Defining the deployment plan using DeployManager
- Applying a deployment plan using DeployAgent
- Running Switch Security
- Validating the deployment
- About multiple domain support
- Authentication in SunSystems
- Resetting a service account
- Resetting an application pool
- Configure a single server with an internal and external hostname.

## Installation checklist

Complete these tasks in the Installation Checklist:

| ✓ | Task | References |
|---|---|---|
| | Download the SunSystems ISO to a local folder and update Database Utilities.<br>Run the installer. | Updating Database Utilities from the Infor Support Portal on page 62The SunSystems ISO on page 30 |
| | Install the database tier | Installing the database tier on page 31 |
| | Install the application tier | Installing the application tier on page 33 |

| ✓ | Task | References |
|---|---|---|
| | Install the reporting tier | Installing the reporting tier on page 33 |
| | Install the web tier | Installing the web tier on page 34 |
| | Define a deployment plan using DeployManager | Defining the deployment plan using DeployManager on page 36 |
| | Apply the deployment plan using DeployAgent | Applying a deployment plan using DeployAgent on page 38 |
| | Run Switch Security to load balance SunSystems Security | Running Switch Security on page 38 |
| | Validate the deployment using DeployMonitor | Validating the deployment on page 38 |
| | Check port usage | Port usage on page 129 |
| | Apply firewall rules | Firewall rules on page 130 |
| | Check folder permissions | Folder permissions for services on page 130 |
| | Ensure the installation complies with multiple domain support | About multiple domain support on page 39 |
| | Conform with updates to authentication in SunSystems | Authentication in SunSystems on page 39<br>Resetting a service account on page 39<br>Resetting an application pool on page 40 |

# The SunSystems ISO

### Downloading the SunSystems installer and updating Database Utilities

The SunSystems 6.4 ISO can be downloaded from the Infor download centre: https://infor.subscribenet.com

**Note:** You can run a product search for Infor SunSystems 6.4.

Download the `SunSystems64.iso` to a local folder on your server.

Ensure you are using the latest version of Database Utilities. This is either the version included on the ISO, or the latest version from the Infor Support Portal. If required, you can browse to the location of the Database Utilities when you run the installer.

### Running the SunSystems installer

Run the SunSystems installer from a local folder.

To run the installer, right-click `SunSystems64.iso` then run the `setup.hta` file.

### New tools in SunSystems 6.4

New desktop tools are introduced in v6.4 which are designed to facilitate manual configuration:

- DeployManager
  Use to design your SunSystems implementation
- DeployAgent
  Use to deploy your design defined in DeployManager
- Switch Security
  Defines the location of the security server on the reporting tier, and most often used to load balance security
- Restart Services
  Stops and restarts all SunSystems services on the current server.

### Order of the installation steps

The order of the installation steps is important. For example, a reporting tier cannot be installed until an application tier has been installed.

In a two-tier environment that includes a combined database / SSRS server and a combined web / application server, a manual step is required. In this scenario, reports cannot be imported by the installer before Reporting Extensions are installed, and Reporting Extensions cannot be installed before the application tier is installed. To import the reports run `VisionImport.exe` from the command prompt. The instructions are in the troubleshooting section of this guide.

In a multitier deployment plan, DeployAgent should not be run until after the system has been configured with DeployManager.

# Installing the database tier

Creating the SunSystems databases is the first step when installing SunSystems. The SunSystems domain database, the business unit group and the security databases must be created.

## Installing the SunSystems domain and business unit group databases

1. Run the SunSystems installer.
2. Select **Install/Configure Database > A pre-configured SunSystems Business Unit Group**.

3 Select the SQL Server instance name, and the name of your domain database (SunSystemsDomain) that you want to create.
4 Specify the locations of your data file and log file.
5 Enter the details for your business unit group in **SunSystems Data Database Details**.
6 Specify the locations of your data file and log file.
7 Enter your Windows domain, SunSystemsServices and SunSystemsClients groups in **Group Account Settings**.

## Installing the SunSystems security database

1 From the SunSystems installer, select **Install/Configure Database > A new SunSystems Security database**.
2 Specify the database name, the database instance, the location of the data and log files and details of the domain groups.

## Installing additional business unit groups

Additional business unit groups can be added by selecting **A new Business Unit Group**. The *Architecture and Planning Guide* gives advice on how many business units (created in Business Unit Administration BUA) should be created in each business unit group.

A two way linked server is required when creating additional business unit groups on other Microsoft SQL Server instances. See Configuring the linked server connection on the database server on page 79

**Note:** Before installing additional business unit groups, you must ensure the linked server is specified using the fully qualified domain name (FQDN). In User Manager, select **Settings > SunSystems > Configure...** and specify the server using the FQDN.
**Note:** MSDTC is not needed because distributed transactions are no longer used.

## Recovery mode

In SQL Server Management Studio you should set the recovery mode for your SunSystems databases according to your back up policy.

The recovery mode for SunSystems databases is set in Microsoft SQL Server Management Studio and should be specified according to back policy.

# Installing the application tier

The SunSystems application tier must be installed after the SunSystems database tier has been installed.

**Note:**

- If the installer does not load, open **Task Manager**. If the process `mshta.exe` is running, close it.
- If you have installed SQL Server databases in a linked server environment then you must run this script in SQL Server:

  ```
  EXEC sp_serveroption 'YourServerNameGoesHere', 'DATA ACCESS', TRUE
  ```

1. Run the program `setup.hta`. This runs the SunSystems installer.
2. Click **Install SunSystems Software > Next**
3. Select **Setup Type**.
4. Select **Custom**.
5. Click **Next > Next > Install**.
6. Clear all features then select **SunSystems Application Tier** in the custom setup screen.
7. Clear **Install a SunSystems schema**.
8. Specify the database server instance and select the SunSystems security database.
9. Specify the database server instance and the name of the SunSystems domain database, in the **Domain Database** dialog.
10. Specify the administrator credentials that you use to login to User Manager.
11. Browse to the location of the Java JDK installation, for example, `C:\JavaPlatform\java\jdk-17\` in the **JDK Location** dialog.
12. Browse to the location of the Apache Tomcat installation, for example, `C:\JavaPlatform\apache-tomcat-9.0.45\`, in the **Apache Tomcat Location** dialog.
13. Specify a domain service account, for example, **`svc-SunSystems`**.
14. Specify the domain service account for reporting service account, for example, SunSystemsReporting.
15. Select the default settings for the SunSystems Application Tier Ports.
16. Specify the security group, for example, SunSystemsServices.
17. Create or overwrite any Virtual Host entries and select the default.
18. Click **Install** to complete the installation.

# Installing the reporting tier

The SunSystems reporting tier must be installed after the application tier, which includes the security server. Microsoft SQL Server Reporting Services Extensions must be installed on the server where SQL Server Reporting Services is located.

1. Run the installer.
2. Select **Install SunSystems software**.

3 Select **Custom**. Clear all features except Microsoft SQL Server Reporting Services Extensions.
4 Specify the SunSystems Application Server and specify the location of the security server.
5 Specify the Reporting service account, for example, SunSystemsReporting.
6 Select the SQL Server Report Server Instance.
7 Create or overwrite any virtual host entries and select the default value.
8 Click **Install** to complete the installation.

# Installing the web tier

The SunSystems web tier must be installed after the reporting tier, which includes the security server. Microsoft SQL Server Reporting Services Extensions must be installed on the server where SQL Server Reporting Services is located.

1 Run the installer.
2 Select **Install SunSystems software**.
3 Select **Custom**. Clear all features except SunSystems Web Tier.
4 Specify the location of the SunSystems application server, and the SunSystems security administrator credentials.
5 Specify the installation location of JDK and Apache Tomcat.
6 Specify the domain SunSystems service account, for example, svc-SunSystems, and the SunSystems reporting service account, for example, SunSystemsReporting.
7 Click **Next** to accept the default ports.
8 Click **Next** to import the example reports.

   **Note:** If the Web and Application tiers are installed on the same server but the Reporting tier is on a separate server, then example reports cannot be imported as part of the installation process. You must clear the option**Import example reports**. After the installation process is complete, use Report Manager to import the reports.
9 Create or overwrite any virtual host entries and select the default value.
10 Click **Install** to complete the installation.

# Running the SunSystems installer in silent mode

You can run the SunSystems installer in silent mode.

1 Copy the SunSystems v63 installation media to a local folder.
2 Navigate to the folder `\DVD\Application`
3 Copy the file `SQLExpressTemplate.xml` and rename as `SQLExpress.xml`
4 Open `SQLExpress.xml` in a file editor, for example, Notepad.
5 Follow the instructions in the file, using your implementation parameters.

6 Save your changes.
7 Open a command prompt and navigate to the `\DVD\Application` folder.
8 Specify the command:**`setup /v" /qn"`**
This runs the installer using the parameters defined in `SQLExpress.xml`

# Installing SunSystems Windows clients

Oracle OpenJDK is a prerequisite for each Windows client machine.

**Note:** To install SunSystems client, the Administrator must be a member of the Configuration Administrators group in User Manager.

1 Run the SunSystems installer.
2 Select **Install SunSystems software**.
3 Specify this information:

**Setup type**
Select **Custom**.

**Components**
Clear all components then select **SunSystems Client**.

**Application server name**
Specify the application server name.

**Security port number**
Specify port 40003 and http. If DeployAgent has been run on the application server or you are using an application server load balancer, then specify port 80.

**SunSystems Security Administrator**
Specify the SunSystems Security Administrator.

**SunSystems Java**
Browse to the local installation of Oracle OpenJDK.

4 Click **Next** to install SunSystems Client.
5 Browse to the location of Oracle Java JDK, and install it.

# Running a Windows client install in silent mode

1 Copy the SunSystems v63 installation media to a local folder.
2 Navigate to the folder `\DVD\Application`
3 Copy the file `SQLExpress-ExampleClientOnly.xml` and rename as `SQLExpress.xml`
4 Open `SQLExpress.xml` in Notepad.

5 Follow the instructions in the file, using your implementation parameters.
6 Save your changes.
7 Open a command prompt and navigate to the `\DVD\Application` folder.
8 Specify the command:**`setup /v" /qn"`**
This runs the installer using `SQLExpress.xml` for parameters.

# Defining the deployment plan using DeployManager

Define your deployment plan in a single step using DeployManager. After the design is complete, and has been saved, you do not need to run DeployManager again unless you wish to change the server deployment plan.

DeployManager is run on the application and web servers. You can use it to add or remove application and web nodes and configure load balancing SSL in SunSystems.

**Note:** Ensure DeployManager is closed after you have completed your deployment plan. While in use, it can create a large log file.
**Note:** If you add web, application and reporting servers then you must specify a load balancer name and port.

DeployManager is available from your desktop after the SunSystems installation has completed.

1 Run DeployManager from the desktop of an application or web server.
2 Log in using a SunSystems administrator user and password.
3 Select **Function > Deployment Builder** to open Deployment Builder. Use Deployment Builder to complete your deployment plan.
4 Add additional web servers to your deployment guide:
   a Click the **SunSystems Public Tiers** tab.
   b Select **Enable Load Balancing**.
   c Specify the **Encryption** method, depending on your requirement. Select from:
      - **`SSL/TLS certificate at Load Balancer`**
      - **`SSL/TLS certificate at IIS Server`**

      **Note:** You must select an SSL/TLS certificate if the web server is public.
   d Specify the URL/domain name of the load balancer in **Load Balancer Name**. For example, **`servername.domain.com`**
   e Specify the port for the load balancer in **Port**.
   f Click the **+** button in the Web Servers dialog to add a new server. A new line is added with default values for the IIS and Tomcat ports.
   g Double-click the **Server Name** on the new line to specify a new server name.
   h Optionally, amend the IIS port value by double-clicking the value. The default is **`80`**.
   i Optionally, amend the Tomcat port value by double-clicking the value. The default is **`40000`**.
5 Add additional application servers to your deployment plan:
   a Click the **SunSystems Private Tiers** tab.

b Select **Enable Load Balancing**.

c Specify the **Encryption** method, depending on your requirement. Select from:

- **`No transport encryption (HTTP Only)`**
- **`SSL/TLS certificate at Load Balancer`**
- **`SSL/TLS certificate at IIS Server`**

d Specify the URL/domain name of the load balancer in **Load Balancer Name**. For example, **`servername.domain.com`**

e Specify the port for the load balancer in **Port**.

f Click the **+** button in the Application Servers dialog to add a new server. A new line is added with default values for the IIS, Application, Security, Web Services and Tomcat ports.

g Double-click the **Server Name** on the new line to specify a new server name.

h Optionally, amend the IIS port value by double-clicking the value. The default is **`80`**.

i Optionally, amend the Application port value by double-clicking the value. The default is **`40001`**.

j Optionally, amend the Security port value by double-clicking the value. The default is **`40002`**.

k Optionally, amend the Web Services port value by double-clicking the value. The default is **`40003`**.

l Optionally, amend the Tomcat port value by double-clicking the value. The default is **`40004`**.

**6** Add additional reporting servers to your deployment plan:

**Note:** ARR Load Balancing is not automatically configured for this tier.

a Click the **SunSystems Private Tiers** tab.

b Select **Enable Load Balancing**.

c Specify the **Encryption** method, depending on your requirement. Select from:

- **`No transport encryption (HTTP Only)`**
- **`SSL/TLS certificate at Load Balancer`**
- **`SSL/TLS certificate at IIS Server`**

d Specify the URL/domain name of the load balancer in **Load Balancer Name**. For example, **`servername.domain.com`**

e Specify the port for the load balancer in **Port**.

f Click the **+** button in the Reporting Servers dialog to add a new server. A new line is added with default values for the Report Server Virtual Directory, Report Manager Virtual Directory and the Reporting Services.

g Double-click the **Server Name** on the new line to specify a new server name.

h Optionally, amend the Report Server Virtual Directory value by double-clicking the value. The default is **`ReportServer`**.

i Optionally, amend the Report Manager Virtual Directory value by double-clicking the value. The default is **`Reports`**.

j Optionally, amend the Reporting Services value by double-clicking the value. The default is **`80`**.

**7** Optionally amend the Desktop Services Tier values:

a Click the **SunSystems Public Tiers** tab.

b Specify the **Server Name**. The default is your desktop machine name.

c Specify the **Application Port**.

d Specify the **Security Port**.

8 Click the **Save** button to save your changes.

# Applying a deployment plan using DeployAgent

After creating a deployment plan, deploy it using DeployAgent.

DeployAgent must be run on each server in the application and web tiers.

**Note:** DeployAgent cannot be run on more than one server at a time.

1 Run DeployAgent on the application server.

   If an error occurs indicating that SunSystems application server will not start, then run DeployAgent on the next application server.

2 Repeat step 1 for the remaining servers in the application tier.

3 Rerun DeployAgent on any application server that failed in step 1.

4 Run DeployAgent on the web server.

5 Repeat step 4 for the remaining servers in the web tier.

# Running Switch Security

Any change to the way the Security Service is exposed, such as adding a load balancer, must also be made to the Security client, across all tiers. This change is made by DeployAgent, apart from the Reporting and Desktop tiers. DeployAgent is not present on these tiers so you must make this change using Switch Security.

Switch Security is a function available from the desktop.

**Note:** Microsoft SQL Server Reporting Server service must be restarted after changes are made in Switch Security.

# Validating the deployment

Use DeployManager to validate your SunSystems installation. It may be run on any server within the SunSystems installation.

You can observer the connections in your deployment plan being validated. It may not be possible for all connections to be validated, due to firewalls, the deployment plan and where DeployManager is being run.

1 Select a server on which to run DeployManager.

2 Select **Deploy Monitor** from the dropdown menu.

# About multiple domain support

SunSystems Windows clients can be installed on a different Active Directory Domain to the SunSystems server implementation. However, Active Directory Forest Trust must exist where the server domain trusts the client domain. Windows API is used by SunSystems to authenticate users across domains. This means if users on the other domain cannot be authenticated by Windows, they cannot be authenticated by SunSystems either.

# Authentication in SunSystems

Authentication in SunSystems 6.4 has improved from older versions of SunSystems.

### GetCredentials

Ensure all services and IIS application pools are run using a trusted user. These services and application pools must be run as a user who is defined as a member of the SunSystemsServices group:

Application pools

- SecurityConsole
- SunSystemsReportingServices.

Services

- SunSystemsConnectServer
- Microsoft SQL Server Reporting Services (SSRS).

### Password hash

SunSystems passwords must be reset after upgrading from an earlier version. This will also affect migrations from SunSystems 4.

# Resetting a service account

If the credentials for a service account are changed, then it must be updated. To change a service account, a new password must be applied for each service on each server. The services on each server must be restarted using Restart Services, which will restart the services in the correct order.

To change a service account, repeat these steps for each server in the SunSystems installation:

1. Open **Control Panel**.
2. Select **Administrative Tools > View Local Services**.
3. Select a SunSystems service.
4. open **Properties > Log on**

5 Enter a new password.
6 Add the service to a service group if it is not already a member.
7 Repeat steps 3 and 4 for the remaining SunSystems services.
8 Run the Restart Services application to restart all SunSystems services on the server, in the correct order.

# Resetting an application pool

If the credentials for an application pool are changed, then it must be updated.

To update an application pool, these Application Pools Identity must be updated:

- SunSystemsDefault
- SunSystemsReportingServices
- SunSystemsSecurity
- TransferDeskWebServer.

1 Open IIS.
2 Select **Host > Application Pools**.
3 Select **SunSystemsDefault**.
4 Select **Advanced Settings > Identity > Custom Account**.
5 Click **Set**.
6 Repeat steps 4 and 5 for SunSystemsReportingServices, SunSystemsSecurity and TransferDeskWebServer.
7 Restart IIS.

# Configure a single server with an internal and external hostname

Exposing a server using internal and external names is the logical equivalence of placing a load-balancing proxy in front of a single server. The internal and external server names must be provided to SunSystems. This is so that internal traffic between IIS and Tomcat remains linked to the internal server name, and external web traffic links to the external (load balancer) name.

**Note:** All SunSystems installations, including standalone installations, must be included in a public web tier, referred to as a SunSystems public tier. This means that the installation endpoints are visible to client machines. It does not mean that the installation is visible to the internet, or that it belongs to a DMZ. Nor is it as restricted as a private tier that uses firewalls to prevent access to everything apart from machines in the public tier.

1 Enable load balancing on the web tier.
2 Specify the load balancer name, for example, **`servera.cloud.company.com`**

3 Specify **443** as the load balancer port.

4 Add a single web server:

   a Specify the single web server, for example, **serverb.companybc.com** as the single web server.

   b Specify **443** as the IIS port.

   c Specify **40000** as the Tomcat port.

5 Save the deployment plan.

6 Run `DeployAgent.exe` on all tiers, starting with the application server tier.

# Chapter 4: Post-installation tasks

To complete a successful installation of SunSystems, you must complete the post-installation checklist.

## Post-installation checklist

| ✓ | Task | References |
|---|---|---|
| | Serialize SunSystems. Run the serialization file on all application servers. Ensure all business unit groups are selected. | |
| | Migrate users and groups | Migrating users and groups on page 44 |
| | Add services to the Trusted Service group | Adding services to the Trusted Service group on page 45 |
| | Add users to the SunSystems Reporting Services group | Adding users to the SunSystems Reporting Service group on page 45 |
| | Synchronize the business unit data models in Report Models | Synchronizing report models on page 46 |
| | Migrate reports | Migrating reports on page 46 |
| | Switch off compatibility view and restart your web browser. | |
| | Review log files for installation errors. Log files are found at `ProgramData\Infor\SunSystems\Logs`<br>If you cannot browse to this location, then in Windows Explorer, select **Organize > Folder and Search Options > View** and select **Show hidden files, folders, and drives**. | |
| | Restrict SecurityWeb permissions | Restricting SecurityWeb server permissions on page 47 |

| ✓ | Task | References |
|---|---|---|
| | Set the recommended memory allocation, where Microsoft SQL Server and SQL Server Reporting Services (SSRS) are on the same server | Allocating memory for Microsoft SQL Server and SSRS on page 47 |
| | Configure Microsoft SQL Server memory options | Configuring Microsoft SQL server memory options on page 48 |
| | Add load balancing | Adding load balancing on page 48<br>Adding a load balancer to the application tier on page 48<br>Adding a load balancer to the web tier on page 48 |
| | Add Secure Sockets | Adding Secure Sockets on page 49 |
| | Install SunSystems Windows clients | Installing SunSystems Windows clients on page 35 |
| | Open SunSystems in a web browser, for example, `http://<FQDN>/sunsystems`<br>If you have set up SSL in IIS and DeployManager, then use `https://<FQDN>/sunsystems`<br>**Note:** All URLs are accessible through the SunSystems URL. For example:<br>• Security Users SEU<br>`http://<FQDN>/sunsystems-security`<br>• Connect Portal SCP<br>`http://<FQDN>/sunsystems-connectportal` | |
| | Download and install additional languages | Installing languages on page 49<br>Language installation tasks on page 49<br>Installing a language pack on page 50<br>Amending the base language on page 50<br>Specifying a language for a user on page 51 |

| ✓ | Task | References |
|---|---|---|
| | For public facing web deployment you must secure the SunSystems web endpoint with a certificate. The public facing firewall must only be accessible through port 443.<br>We recommend that the Windows environment for the web server must be hardened to prevent https access by any connections using protocols lower that TLS 1.2.<br>See `https://www.cisecurity.org/` for details of how to security harden your system. | |
| | Configure SunSystems Help so it is accessible from Navigator | Configuring SunSystems help on page 51 |
| | If applicable, install the latest SunSystems patch sets. You can download the latest SunSystems 6.4 patch set from http://support.infor.com. | |
| | Investigate integrating SunSystems with the Infor OS platform. SunSystems integrates with the Infor OS Platform formally known as Infor Ming.le, ION, IFS, EAM. See *Infor OS* document, on http://support.infor.com. | |

# Serializing SunSystems

Serialize SunSystems. Run the serialization file on all application servers, ensuring that all business units groups are selected.

**Note:** You must include your SunSystems user as a member of the Trusted Service Group.

# Migrating users and groups

**Caution:** Do not switch off standard authentication in User Manager or Security Console unless you have a user with access to User Manager. The user must be a Windows authenticated user who has an administrator role.

If pre-configured data (PK1) has been installed, use SunSystems User Migration Wizard to import the pre-configured users and groups:

1. Open SunSystems.
2. Select **SunSystems Tools > Migration > SunSystems User Migration**.
3. Select **Operator ID** if you require a three digit SunSystems login.

   Alternatively, create your own Users and Groups. See the User Manager help in the online help.

# Adding services to the Trusted Service group

The SunSystemsServices group is used to grant access to the SunSystems database during installation. It is set as the default group for Trusted Service.

After installation has completed, SunSystems can use a separate Windows group for Trusted Service. This enhances the security of your system by separating the trusted services permissions from database access permissions. In order to use a separate group for Trusted Service, the group must be set up in Windows and configured with the appropriate permissions and Windows user accounts for each service.

**Note:** You do not have to have a separate Windows group configured specifically for Trusted Service; by default the system will use the same Windows group you selected for SunSystemsServices to obtain the required permissions.

Adding services to the Trusted Service group:

1. Open Active Directory.
2. Select **Users and Computers**.
3. Create the global group TrustedService.
4. Add the Windows accounts.
5. Open SunSystems navigator.
6. Select **Security Settings (SES) > Security Service**.
7. Specify this information:

   **Trusted Service Group**
   Specify the relevant Windows group name.

8. Alternatively, specify the Trusted Service Group in User Manager. Select **Settings > SunSystems > Trusted Service Group**.

# Adding users to the SunSystems Reporting Service group

Only users requiring administrative access to SRS need to be added to the SunSystems Reporting Administrators group.

**Note:** Preconfigured (PK1) data must be installed.
**Note:** You must make a note of which users have the SunSystems Reporting Model Managers role, and which users have the Reporting Administrator role. This information is required for subsequent steps in the post-installation checklist.

To add a user to the SunSystems Reporting Services group:

1. Log into User Manager as an administrator.
2. Select **Groups**.
3. Browse to the PK1 group and select **Edit > Edit Group...**.

4 Select **Function Permissions > Select All > Apply**.
5 Select **Action Permissions > Add**.
6 Specify PK1 and click **OK > OK > Apply > OK**.
7 Select **Users**.
8 Browse to a user that requires SRS group membership, for example, PK1, and select **Edit > Edit Users...**.
9 Click **Change...**.
10 Browse to SunSystems Reporting and select the functions required.
11 Click **OK > Apply**.
This applies the changed group membership.

# Synchronizing report models

You must create a report model for each business unit.

Synchronize the report models:

1 Log into SunSystems as a user who is a Report Model Manager..
2 Select **Report Models (RMD)**.
You can select multiple business units.
3 Select a business unit and click **Synchronize > Yes**.
On successful completion, the status is updated to `Synchronized`.

# Migrating reports

A migration report is generated after the report migration has completed. Reports that fail migration must be opened, corrected and redeployed in Report Designer.

To migrate a report:

1 Log into SunSystems as a user who is a SunSystems Reporting Administrator.
2 Select **Report Manager (RMA)**.
3 Select **Tools > Migrate Reports**.
4 Click **Yes**.

# Restricting SecurityWeb server permissions

During the installation, the access permissions to the SecurityWeb folder are full rights for Everyone. After the installation is complete, you should manually restrict access

**Note:** For Windows 2012, go directly to step 3.

1. Open IIS Security..
2. Switch the Anonymous User setting for the SecurityWeb website to the App Role account.
3. Restrict permissions to the SecurityWeb folder to Full control for the Security App role account.
4. Apply any other restrictions appropriate to your installation.
5. Grant Modify folder permissions to the SecurityWeb folder for local account IIS appool\SecurityWebServer.

# Allocating memory for Microsoft SQL Server and SSRS

If the Microsoft SQL Server databases and Microsoft SQL Server Reporting Services (SSRS) are installed on the same server, we recommend that minimum and maximum memory allocations for SSRS are specified. The settings are stored in the `RSReportServer.config` file.

The setting for WorkingSetMaximum must be appropriate for SSRS. This depends on the hardware RAM available. Sufficient RAM must be provided for the operating system and SQL Server database server. The memory for Microsoft SQL Server must never be expended; the minimum amount of memory reserved for SQL Server is 1GB. The setting for WorkingSetMinimum must also be set appropriately.

We recommend that the maximum memory for Microsoft SQL Server database server is specified. See Configuring Microsoft SQL server memory options on page 48.

1. Open the `RSReportServer.config` file.

   This is usually found at `Program Files\Microsoft SQL Server\MSRS13.MSSQLSERVER\Reporting Services\ReportServer`

2. Add or update these settings:

```
<Service>
<MemorySafetyMargin>80</MemorySafetyMargin>
<MemoryThreshold>90</MemoryThreshold>
<WorkingSetMaximum>4000000</WorkingSetMaximum>
<WorkingSetMinimum>2400000</WorkingSetMinimum>
```

3. Save your changes and close the file.

# Configuring Microsoft SQL server memory options

Use the two server memory options, **`min server memory`** and **`max server memory`**, to reconfigure the amount of memory (in megabytes) managed by the SQL Server Memory Manager for an instance of SQL Server. By default, SQL Server can change its memory requirements dynamically based on available system resources.

**Note:** Use the default settings to enable the memory requirements to be changed dynamically by SQL Server, based on the system resources available. The default setting for **min server memory** is 0, and the default setting for **max server memory** is 2147483647 megabytes (MB).

To specify a fixed amount of memory:

1. In Object Explorer, right-click a server and select **Properties**.
2. Click the **Memory** node.
3. Specify an amount for **Minimum server memory** and **Maximum server memory**, under **Server Memory Options**.

# Adding load balancing

If you have more than one server in the application tier, you must load balance the application tier. If you have more than one server in the web tier, you must load balance the web tier.

See the *SunSystems Architecture and Planning Guide* for information on scaling out SunSystems.

## Adding a load balancer to the application tier

To add load balancing to the application tier:

1. Open DeployManager.
2. Include the application load balancer in the deployment plan.
3. Save the configuration.
4. Run DeployAgent consecutively on each application server.
   **Note:** Do not run DeployAgent on multiple servers simultaneously.
5. Run SwitchSecurity on the reporting tier.
6. Specify the name of the application tier load balancer for the security service.

## Adding a load balancer to the web tier

To add a load balancer to the web tier:

1. Open DeployManager.
2. Include the web load balancer in the deployment plan.
3. Save the configuration.
4. Run DeployAgent consecutively on each web server.

**Caution:** Do not run DeployAgent on multiple servers simultaneously.

# Adding Secure Sockets

If SunSystems is outward facing, it must be secured with a certificate.

Secure Sockets (SSL) can be implemented in the load balancer, or in IIS.

See Appendix J for an example.

1. Create a certificate request in IIS, on the web server, and send it to the certificate provider.
2. Complete the certificate request in IIS, after you receive the certificate from the provider. This must be completed on the same server on which the certificate request was created.
3. Open IIS Manager.
4. Select **Sites > SunSystems Applications > Bindings**.
5. Add a site binding of type https on port 443. Select the SSL certificate you installed.
6. Open DeployManager.
7. Amend the deployment plan to use the new HTTPS site binding for SunSystems.
8. Save your changes.
9. Run DeployAgent consecutively on each server in your implementation. This applies the change to your system.

# Installing languages

The SunSystems installation sets the base language to 1, which means SunSystems is installed as English-only. Other languages must be installed using the Language Deployer after the installation has completed. Ensure the language required is available for deployment.

**Note:** SunSystems can support up to 99 language versions; the base language and 98 additional languages.

## Language installation tasks

Complete the tasks in the language installation checklist:

| Status | Task | References |
|---|---|---|
| | Install a language using the relevant Language Pack | Installing a language pack |
| | Amend the base language and update the base language descriptions | Amending the base language on page 50 |
| | Specify a language for each user in User Manager | Specifying a language for a user on page 51 |

## Installing a language pack

Language packs are available for download from the Infor Support Portal. Select a language pack relevant to your SunSystems v6.4 patch set.

A language pack contains instructions to add or remove additional languages to a SunSystems installation. Refer to the Installation note in the language pack for instructions on how to install your specific language. The language must be included in the serialization details.

Use Microsoft SQL Server Command Line Utilities to run the language deployer. This is normally found at `ENU\x64\MsSqlCmdLnUtils.msi`, or run `bcp.exe`. The utilities are included in Client Tools Connectivity/Client Tools SDK features in the Microsoft SQL Server Installer.

**Note:** If you have multiple versions of SQL Server installed, then the most recently installed version of `bcp.exe` must be listed first in the `PATH` environment variable. An incorrectly ordered variable may result in the error message `BCP.exe version is too low` while running Language Deployer. To check that the `PATH` variable is correctly ordered, run `bcp -v` from a command prompt.

## Amending the base language

1. Open SunSystems navigator.
2. Select **Business Unit Administration (BUA)**.
3. Select a business unit or business unit group to amend.

   **Note:** All business units in the business unit group must be offline.
4. Select **Actions > Advanced > Amend a Base Language**.
5. Complete this information:

   **Business Unit Group**
   Automatically populated with the selected business unit group.

   **Business Unit Code**
   Automatically populated with the selected business unit.

**Language Code**
Select a language from one of the installed languages.

**Update System Text**
Select **Yes** to update system text using the language defined for each Business Unit. Existing text will be overwritten. The default value is **No**.

6 Click **OK**.

7 Ensure these columns contain the correct language:

```
XXX_DRILL_ASSOCIATES(DRILL_DESCR)
XXX_ROLE(DESCR)
XXX_NUM_STREAM_HDR(DESCR)
XXX_NUM_STREAM(DESCR)
XXX_FIN_RPT_COL_HDGS(HEADING_1,HEADING_2,HEADING_3,HEADING_4)
XXX_BDGT_DEFN(DESCR)
XXX_ALLOCN_IND(NAME,S_HEAD)
XXX_TXN_REF_FMT(DESCR)
```

8 Repeat for each business unit group.

## Specifying a language for a user

1 Open SunSystems navigator.
2 Select **User Manager**.
3 Select **Edit User... > Operator**.
4 Click **Language** to select a language.
5 Click **OK**.

# Configuring SunSystems help

You can access SunSystems help from the cloud, or install it on a local server.

By default SunSystems links to cloud help. To access the help contents directly, open https://docs.infor.com and select **Enterprise Financial Management > Infor SunSystems**

**Note:** To access SunSystems online help, you must clear the **Block pop-up windows** option in the security settings of your browser.

To ensure context sensitivity works with cloud help, select **Configuration Manager (CGM) > SunSystems Help**, click **Edit** and select **Cloud** as the **Service Priority**. All SunSystems sessions must be closed and all users logged out before running Restart Services.

To install and configure local help files:

1. Log into SunSystems as a user who is a member of the Configuration Administrator's group in User Manager.
2. Select Configuration Manager (CGM).
3. Click **Online Help** and click **Edit**.
4. Specify this information:

   **Service Priority**
   Specify **Local**.

5. Save your change.
6. Ensure all user sessions are closed and all users are logged out.
7. Run Restart Services.
8. Download the SunSystems 6.4 help files zip from http://support.infor.com and open KB 1859777.
9. Copy the file to the SunSystems web tier.
   Unzip the file at `Program Files\Infor\SunSystems\HelpContent\`.

# Changing the configuration service account

You must run these `netsh` commands if you change the configuration service account after installing SunSystems:

1. Run the command to display the current configuration service account:
   ```
   netsh http show urlacl
   ```
2. Run the command to delete the current account. This must be done before you set the new service account.
   ```
   netsh http delete urlacl url=http://+:40003/sunsystems-configuration-api/
   ```
3. Run the command to set the new service account:
   ```
   netsh http add urlacl url=http://+:40003/sunsystems-configuration-api/
   user=DOMAIN\user
   ```
   where **`DOMAIN\user`** is the new service account.
4. Add the new service account to the **`SunSystemsServices`** domain group

# Managing users and sessions

Many administrative tasks, for example, restarting the SunSystems services, require you to log out all users and to close all sessions.

To log out all users and close all sessions:

1. Log into User Manager as the SunSystems Administrator
2. Select **Settings > SunSystems > Operator Activity**
3. Select an operator and click **Clear.**

The maximum number of sessions that a single user can open is nine. The maximum number of sessions that can be open at one time is 150. Setting a restriction prevents the limits of system resources being reached.

To view or maintain the total number of open sessions:

1. Log into SunSystems Web as a user who is a member of the SunSystems Administrators group.
2. Open the **Security User Activity (SEC)** function.

### Increasing the SunSystems Web connections limit

There is a default limit to the number of SunSystems Web connections that can be made to a SunSystems Web server. This limit is set per web server.

Log into SunSystems as a user who is member of the Configuration Administrators group. Choose function **Configuration Manager (CGM)**. Select **Application > Session Settings**, and click **Edit**.

**Note:** Due to an issue with IE11, you may not be able to see the Edit icon. However, it is there and can be clicked.

Set **Max Allowed Global Sessions** to `250`, which is the maximum setting.

The restriction in Tomcat of 200 sessions was removed by patch set 5. If this patch has not been applied, then the change can be applied manually:

1. Open `\Program Files\Infor\SunSystems\SunSystemsWeb\tomcat\conf\server.xml` using a file editor such as Notepad++.
2. Replace this text:`<Connector` with `<Connector maxThreads="550"`

This results in a Tomcat Connector configuration line similar to:

```
<Connector maxThreads=”550” port="9080" protocol="org.apache.coy
ote.http11.Http11NioProtocol" connectionTimeout="20000" redirectPort="9443"
compression="2048" compressableMimeType="text/html,text/xml,text/css,appli
cation/javascript"></Connector>
```

# Chapter 5: Requirements and planning

The hardware and software requirements for running SunSystems vary depending on the type of deployment that you choose, that is, stand-alone, two-tier installation, or three-tier installation.

See the *SunSystems Architecture and Planning Guide* for an overview of the architecture and planning considerations for the deployment of the software.

The requirements in this section should be regarded as the minimum for the type of deployment that you choose. If you are installing other software on the same computer(s) as SunSystems, you may need to increase the minimum requirements. Careful consideration must be given to your current requirements and hardware capacity. These are the main factors to consider:

- Transaction and event volume
- The number of primary system users
- The number of secondary users, that is, those who might find the information on the system useful as a source of information
- The location of the application users
- The volume of the local area network and whether it is related to the application.

If other applications share the network, any performance improvements to other application could affect the network.

Projections should be made to predict your future requirements. Expansion in any of the previously listed factors might have a detrimental effect on the performance of the system. For sizing advice, contact your regional office.

## Software requirements

These tables list the recommended operating systems to use:

### Standalone

| Layer | Windows version | Microsoft SQL Server version |
|---|---|---|
| All | Windows Server 2019, Windows Server 2016, Windows 10 | Microsoft SQL Server 2019, 2017 or 2016 Database Server, and Reporting Services.<br>(Standard Edition or above). |

### Two-tier

| Layer | Windows version | Microsoft SQL Server version |
|---|---|---|
| Client | Windows 10 | |
| Application and database | Windows Server 2019 or 2016 (Standard or Datacenter) | Microsoft SQL Server 2019, 2017 or 2016 Database Server, and Reporting Services.<br>(Standard Edition or above). |

### Three-tier

| Layer | Windows version | Microsoft SQL Server version |
|---|---|---|
| Client | Windows 10 | |
| Application | Windows Server 2019 or 2016 (Standard or Datacenter) | |
| Database | Windows Server 2019 or 2016 (Standard or Datacenter) | Microsoft SQL Server 2019, 2017 or 2016 Database Server, and Reporting Services.<br>(Standard Edition or above). |

# RDBMS support

SunSystems version 6.4 is supported with these relational databases:

- Microsoft SQL Server 2019
- Microsoft SQL Server 2017
- Microsoft SQL Server 2016.

Before upgrading to a new Microsoft SQL Server service pack, contact your regional support representative to check your support status.

**Note:** Binary sort order is mandatory.

### Clustered databases

If you intend to use database server clustering, check that the shared disk array installation, configuration and verification steps have been completed before you attempt to install SunSystems.

Check that Windows Cluster Services has been installed and configured on each database server or nodes.

**Note:** In the event of a failover, SunSystems automatically reconnects to SQL Server. This means that SunSystems services do not need to be restarted. Users do not need to log out and log back in but they must close then re-open any open menu functions.

# Chapter 6: Creating a secure installation

This chapter details the security requirements for configuring and running SunSystems, and describes the security issues in terms of database security and SunSystems application security. Recommendations are given on security settings for all Windows operating systems and database servers; issues such as file system and registry security are also covered.

## Requirements for a secure environment

To create a secure environment, you must review these requirements:

- Security model
- SunSystems Connect (SSC) security
- Microsoft SQL Server security
- Microsoft SQL Server service accounts
- Citrix XenApp
- Deployment
- Load Balancing.

## Security model

SunSystems can be configured to use two different authentication methods. The simplest requires the user to enter their credentials upon accessing SunSystems. If Windows authentication is required, with the correct configuration SunSystems obtains the Windows account credentials and uses these to log the user on to SunSystems. To define the ID of the user while using the application, mapping is required, but no further login requests are made.

## SunSystems Connect (SSC) security

SunSystems Connect provides web services that are accessible from anywhere using standard SOAP messaging. Historically, credentials were provided in the SOAP message itself, a relatively insecure way of submission because they could be intercepted.

To submit a SOAP request, the SunSystems security service issues vouchers to authenticated users. These vouchers are exchanged using industry standard public/private key exchange algorithms using the highest level of encryption available on the operating systems negotiating transfer. A client-side library is required to make these requests, and is provided for the Java programming environments and Microsoft programming environments.

See SunSystems Connect online help and the *SunSystems Connect Implementation Guide*.

## Microsoft SQL Server security

Microsoft SQL Server can operate in one of two security or authentication modes, depending on the chosen installation:

- Windows Authentication Mode (Windows Authentication)
- Mixed Mode (Windows Authentication and SQL Server Authentication).

Mixed Mode allows users to connect using Windows Authentication or SQL Server Authentication. Users who connect through a Windows user account can make use of trusted connections, that is, connections that are validated by Windows, in either Windows Authentication Mode or Mixed Mode. After successful connection to SQL Server, the security mechanism is the same for both modes.

Security systems that are based on SQL Server logins and passwords (SQL Server Authentication) might be easier to manage than security systems that are based on Windows user and group accounts. This is especially true for databases that are not mission-critical and applications without sensitive and confidential information.

For example, a single SQL Server login and password can be created for all users of an application, rather than creating all the necessary Windows user and group accounts. However, this removes the ability to track and control the activities of individual users and is therefore not recommended for SunSystems applications.

Windows Authentication has certain benefits over SQL Server Authentication, primarily because of its integration with the Windows security system. Windows security provides more features, such as secure validation and encryption of passwords, auditing, password expiration, minimum password length, and account lockout after multiple invalid login requests.

## Microsoft SQL Server service accounts

Depending on the Microsoft SQL Server components that you choose to install, SQL Server installs a variety of services. For the purpose of SunSystems security, the key service is the SQL Server database service called MSSQLSERVER, or MSSQL$<*instancename*> if it is a named instance.

Many server-to-server activities can be performed only with a domain user account. This means that you should use a domain user account on this service.

All domain user accounts must have permission to:

- Access and change the SQL Server directory (`\Mssql`)

- Access and change the `.mdf`, `.ndf`, and `.ldf` database files, regardless of location
- Log-on as a service right
- Read and write registry keys at and under these locations:
  - `HKEY_LOCAL_MACHINE\Software\Microsoft\MSSQLServer`
  - `HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\MSSQLServer`
  - `HKEY_LOCAL_MACHINE\Software\Microsoft\WindowsNT\CurrentVersion\Perflib`

For more information about other specific functionality, refer to your SQL Server documentation, in particular *Books Online*.

# Citrix XenApp

The SunSystems Windows services must not be set up to run under a local system account, because the system account performs network operations and has privileges that are not applicable for all users.

To secure the file system, use the SUBINACL utility. This is provided by Microsoft to secure the file system. Next, grant permissions to the SunSystems directories that are specified in the File Permissions and Ownership subsection.

In addition to using standard Windows security features and practices, access to Citrix servers can be restricted in several ways:

- SunSystems can be utilized as a published application. This implies that all users on a specific connection type can be restricted to running published applications. Published Application Manager allows you to restrict an application to specified users or groups of users (explicit user access only).
- Internet firewalls are supported by Citrix XenApp server to restrict Internet access to the XenApp server.
- Users are required to enter a user name and password to run an application (explicit user access only).
- It is recommended by Citrix that your website is disassociated from your production system, or you restrict external access. Any system accessible through the Internet facilitates unauthorized access to your production site and is a security risk. Therefore, your web server must be installed on a separate network loop outside the firewall, unless you plan to use it with a secure intranet.
- SunSystems does not support anonymous user access by Citrix. SunSystems allows only the domain users to log on to SunSystems who are members of the clients group, for example, SunSystemsClients.

## Citrix XenApp - Publishing applications

Anonymous user access is not supported by SunSystems. This ensures that access to SunSystems is restricted to domain users only.

To use SunSystems as a published application, domain users must be members of the SunSystemsClients group.

**Note:** Hot Keys are supported by SunSystems. For information about using the published application Hot Keys, refer to Citrix documentation.

## Citrix XenApp - Configuring folder and registry permissions

In SunSystems, all users are granted full control of the `ProgramData\Infor\SunSystems` folder.

If SunSystems online Citrix XenApp is published with domain user access, complete these steps:

1. Give 'write' access to the SunSystemsClients group where reports are located, if they are outside of SunSystems folder hierarchy.
2. Transfer desk creates files when running exports. The systems administrator must configure 'write' access to the SunSystemsClients group for this location.

# Deployment suggestions

Consider having a separate partition for user data. In the event of a full partition, storing user data, system files and print queues in the same partition prevents users from printing and may cause SunSystems to become unstable. Storing user data in a separate directory generates an 'out-of-space' error instead.

### Control access through groups

The administrator should create local applications groups or global applications groups, assign those groups the rights necessary to run the SunSystems application, and add global groups to them that contain the users who require access to the application.

The SunSystems administrator must create a local or global application group. These groups must be assigned the rights required to run SunSystems. Users that require access to SunSystems must belong to this group.

### Registry security

A security policy must be setup and assigned to the SunSystems Group. Audit the system to ensure that SunSystems users have the minimum access permissions required to run the software.

### CPU optimization and SunSystems

CPU optimization is recommended for a SunSystems deployment on Citrix XenApp. It normalizes the use of server resources by 'smoothing' out the peaks of CPU usage by each user. Approximately 20 percent of server CPU is reserved for automatic optimization by Citrix XenApp. This means that no single session controls the majority of CPU processing. When CPU power is borrowed from idle or inactive sessions, it can be reallocated when that session becomes active again. Invoking CPU optimization is beneficial, and should not have any noticeable negative effect.

CPU optimization is recommended for a SunSystems deployment on Citrix XenApp.

### Memory optimization and SunSystems

SpeedScreen technology is designed to optimize the graphics-based applications on Citrix, such as 3D graphics. However, this technology also optimizes the use of the network bandwidth. We recommend that the SpeedScreen setting is switched on in the SunSystems deployment on Citrix XenApp.

### Additional scalability recommendations

**Note:** If you are using XenApp 7.9, only web connection is supported. This means the ICA connection is not supported.

- Disable Virtual Channels in the Citrix ICA session
- Profile Considerations: Roaming profiles with folder redirection could lead to performance loss if not implemented with care
- Logically group servers and applications in the farm into two or more Load Managed Groups (LMG)
- Network Performance: Match speed and duplex settings for 10/100 Mbps connection. Autosense for 1000 Mbps connection.

### Citrix web client and SunSystems

Citrix XenApp 6.5 uses Citrix Web Interface to connect to published applications, so Citrix client is not required. SunSystems can be used with the Citrix Web Interface client. To do this, point your browser to the Web Interface URL of your Citrix server, specified as:

```
http(s)://<servername>:<port number>/Citrix/AccessPlatform/site/default.aspx
```

## About Load Balancing

### Active / Passive Arrangements

SunSystems 6.4 deployments are designed to be highly resilient in the event of both node and service level failure, whilst continuing to make the most of the remaining available resources under these scenarios. Any individual service of a SunSystems node should be able to fail independently while enabling remaining components to stay within the available deployment.

ARR-managed tiers for SunSystems, i.e. web and app tiers, only include active nodes. These nodes source traffic between each other, as well as from the tier entry point on the load balancer.

**Note:** All aspects of affinity and weighting are managed by the ARR deployment. This means that any active/passive arrangement cannot be controlled at the load balancer.

If 'reserve' hardware is required, then this should be included in the Deployment Manager model and all services, or even nodes, should be switched off to act as if under failure. When started, these resources are actively included into the available deployment.

### Traffic Encryption

TLS 1.2 encryption over all HTTP endpoints is supported by SunSystems. The support is provided at a 'between tiers' level. This means that all traffic crossing between client and web tiers, or web and app tiers will be encrypted.

Encryption 'within tiers' is not currently supported by SunSystems. Encryption 'within tiers' is defined as traffic between nodes of the same type and ensures service level resilience within the tier. This type of traffic uses a mix of HTTPS and HTTP for those services not directly hosted within IIS. A complete 'within tiers' level of encryption incurs a performance penalty from additional proxying and should not be required if a 'private subnetwork' model is used for each tier, as is the approach generally used.

All network tiers must be installed using a 'private subnetwork' model where nodes are installed alone in an IP subnetwork. The network switch should prevent any 'sniffing' from external clients. SunSystems may also be deployed using a VPN tunnel to create a virtual 'private subnetwork' to prevent any traffic snooping.

The Application server and Security Services for SunSystems utilize TCP endpoints which are not encrypted. In a web only deployment, these services are not externally exposed and where Desktop Clients are available, they should access the endpoints through the Desktop Services tier, using a VPN access. Third party encryption services, or a VPN, can be used with all SunSystems TCP endpoints to add additional security.

# Chapter 7: Database Utilities

SunSystems database administration is implemented through Database Utilities, which is a separate application.

A subset of the database administration functions is available from Business Unit Administration (BUA) in SunSystems.

The functions included in Database Utilities are grouped into sections:

| Function type | Description |
|---|---|
| Create | Use these functions to create a new domain database, security database, or new or pre-configured business unit group |
| Upgrade | Use these functions as part of the upgrade process including pre-upgrade system checks |
| Domain DB | Use these functions to maintain the domain database |
| SunSystems DB | Use these functions to maintain business unit groups |
| Security DB | Use these functions to maintain the security database |
| Form Actions | Use these functions to maintain forms |

## Updating Database Utilities from the Infor Support Portal

Database Utilities is provided with the SunSystems ISO or the DVD. However, you must download the latest version from Infor Support Portal before running the upgrade or performing any activity on a SunSystems database. Search for `KB2001312` in the Infor Support Portal.

# Accessing Database utilities from the ISO

You can access Database Utilities from the ISO. Run the SunSystems ISO by clicking `setup.hta` and select **Install/Configure Database**.

Alternatively, browse to the `\Sqlserver DatabaseUtilities\` folder and run `DBUTILITY.exe`.

# Accessing Database utilities from the DVD

You can access Database Utilities from the DVD. Browse the DVD to the `\SqlServer Database Utilities\` folder and run `DBUTILITY.exe`.

# Create

### A new SunSystems Domain database

Create a new domain SunSystems on the local machine.

Select **SunSystems Database Utilities > Create > A new SunSystems Domain database**.

You can use this utility to install the domain database on a different server to the one containing the SunSystems databases. Both servers must belong to the same domain.

All SunSystems databases must be registered in the domain database. For a new installation, this requires the domain database to be created before or simultaneously with other SunSystems databases.

This utility uses a subset of the steps for a full installation.

### A new SunSystems business unit group

Create a new business unit group on the local machine.

Select **SunSystems Database Utilities > Create > A new SunSystems Business Unit Group**.

Select this utility to create a live, store or archive business unit group.

You can also use this utility to create a business unit group on a server remote from the application servers. The servers must belong to the same SunSystems domain.

**Note:** To run this utility remotely, ensure that your local machine has Microsoft SQL Server Tools installed. This utility uses SQL Server client connectivity components, specifically `bcp.exe`, to connect to the SQL Server instance on the remote machine and it will fail if these have not been installed.

The business unit group is registered in the SunSystems domain database. If the domain database does not exist, then it is created on the local machine, after which the business unit group is registered.

Registering a second business unit group automatically converts the domain to a multiple database environment.

This option uses a subset of the steps used in a full installation.

### A new SunSystems Security database

Create a new SunSystems security database.

Select **SunSystems Database Utilities > Create > A new SunSystems Security database**.

This option uses a subset of the steps used in a full installation.

### A pre-configured SunSystems business unit group

Create the PK1 business unit group, containing multiple business units with the same data but different collations. See Migrating users and groups on page 44, and Adding users to the SunSystems Reporting Service group on page 45.

Select **SunSystems Database Utilities > Create > A pre-configured SunSystems Business Unit Group**.

**Note:** You can only create a pre-configured business unit group on the local machine. This utility will not create a database locally.

You can also use this utility to create a business unit group on the local server, if it is remote from the application servers. The servers must belong to the same SunSystems domain.

The business unit group is registered in the SunSystems domain database. If the domain database does not exist, then it is created on the local machine, after which the business unit group is registered. If the domain database already contains a PK1 business unit, then registration for the business unit group fails. Business units in a SunSystems domain must be unique.

Registering a second business unit group automatically converts the domain to a multiple database environment.

This option uses a subset of the steps used in a full installation.

# Upgrade

### Pre-upgrade check

Run on each SunSystems business unit group to identify outstanding transactions.

Select **SunSystems Database Utilities > Upgrade > Pre-Upgrade Check**.

This check must be run before performing an upgrade. If it returns outstanding transaction entries then the upgrade is prevented from progressing.

Included in the check are tests for:

- all help journals cleared down
- the Recover Failed Postings function (REP) is empty
- the ledger import queue is empty
- the data audit is empty.

### Remove work tables

Run on a business unit group to remove all work tables.

Select **SunSystems Database Utilities > Upgrade > Remove work tables**.

The stored procedure, **`SSP_DROP_WORK_TABLES`**Pre-upgrade is run, removing all temporary work tables from the database. This improves the performance of the upgrading business units during the process.

Work tables older than a month are deleted. You can amend the parameters so that all work tables are deleted.

### A SunSystems Security database

**Caution:** The automated database upgrade process affects standard SunSystems tables only. It does not affect any non-standard tables created separately to SunSystems.

Upgrades the security database.

Select **SunSystems Database Utilities > Upgrade > A SunSystems Security database**.

You must review and resolve any issues reported.

These automated tasks are run by the setup program:

- Security: Object existence checks
- Security: Add logins to SQL Server
- Security: Configure database access - SunSystemsSecurity
- Security: Upgrade schema SECUPGRADE621-630.INI
- Security: Update procedures
- Security: Update language metadata

**Caution:** Scroll through the upgrade screen to ensure that you identify any issues which do not stop the upgrade but produce a log file. If any issues are reported, you must restore the security database. The issues must be resolved and the upgrade process restarted from the beginning, including the prerequisites.

### A SunSystems Domain database

**Caution:** The automated database upgrade process affects standard SunSystems tables only. It does not affect any non-standard tables created separately to SunSystems.

Upgrades the domain database.

Select **SunSystems Database Utilities > Upgrade > A SunSystems Domain database**.

You must review and resolve any issues reported.

These automated tasks are run by the setup program:

- Domain: Add logins to SQL Server
- Domain: Prepare database access
- Domain: Object existence checks
- Domain: PreCheck DB integrity
- Domain: Upgrade schema DOMUPGRADE621-630.INI
- Domain: Data/Index file group check
- Domain: Update metadata
- Domain: Remove old dictionary tables
- Domain: Rename data dictionary tables
- Domain: Drop old constraints
- Domain: Create new dictionary tables
- Domain: Add data dictionary constraints
- Domain: Load data dictionary tables
- Domain: Install language metadata
- Domain: Update base language metadata
- Domain: Update language metadata
- Domain: Load data dictionary language tables
- Domain: Copy forward third party data
- Domain: Add data dictionary indexes
- Domain: Remove old dictionary tables
- Domain: Disable SSC hierarchy node
- Domain: Create generated data dictionary
- Domain: Generated menu
- Domain: Create DOMN_GEN_DATA triggers
- Domain: Remove data from difference tables
- Domain: Load data to difference tables
- Domain: Refresh difference tables' version
- Domain: Apply post upgrade scripts
- Domain: Filter FDD selection
- Domain: Finalise database
- Domain: Forms load
- Domain: Delete previous patch history
- Domain: Enable Broker
- Domain: Post upgrade DB integrity check

**Caution:** Scroll through the upgrade screen to ensure that you identify any issues which do not stop the upgrade but produce a log file. If any issues are reported, you must restore the security database. The issues must be resolved and the upgrade process restarted from the beginning, including the prerequisites.

### A SunSystems Domain database forcing all scripts to be reapplied

**Caution:** The automated database upgrade process affects standard SunSystems tables only. It does not affect any non-standard tables created separately to SunSystems.

Upgrades the domain database and forces all scripts to be applied to the database whether they have changed or not.

Select **SunSystems Database Utilities > Upgrade > A SunSystems Domain database forcing all scripts to be reapplied**.

This utility takes longer to complete than **A SunSystems Domain database** and must only be used by an experienced SunSystems installer, or under instruction from Infor Support.

### A SunSystems business unit group

**Caution:** The automated database upgrade process affects standard SunSystems tables only. It does not affect any non-standard tables created separately to SunSystems.

Upgrade one or more business unit groups.

To open this utility, select **SunSystems Database UtilitiesUpgradeA SunSystems Business Unit Group**.

These automated tasks are run by the setup program, for each business unit group:

- SunSystems: Object existence checks
- SunSystems: Create missing financial only BU table
- SunSystems: Pre-Upgrade checks
- Remove audit triggers
- Remove integration triggers
- Remove balance triggers
- SunSystems: Create GS views to domain tables
- SunSystems: Create SUN views to domain tables
- SunSystems: Upgrade database ‘SYSUPGRADE621-630.INI’
- SunSystems: Upgrade database ‘BUSUPGRADE621-630.INI’
- SunSystems: Update database, apply ‘SYSUPDATE.INI’
- SunSystems: Update database, apply ‘BUSUPDATE.INI’
- SunSystems: Load integration data
- SunSystems: Add ‘BUGROUP2’ to domain
- SunSystems: Update system base language
- SunSystems: Update business unit base language
- Post upgrade system tasks
- Post upgrade BU tasks
- Business rules check
- Drill to investigate
- SunSystems: Add logins to SQL Server
- SunSystems: Configure database access
- SunSystems: Create GS views to domain tables

- Post upgrade DB integrity check
- Add audit triggers
- Reapply integration triggers
- Reapply balance triggers
- SunSystems: Delete previous patch history
- SunSystems: Finalise database
- SunSystems: Configure database access
- SunSystems: Create GS views to domain tables
- Post upgrade DB integrity check
- Add audit triggers
- Reapply integration triggers
- Reapply balance triggers
- SunSystems: Delete previous patch history
- SunSystems: Finalise database
- SunSystems: Configure multi database flag

**Note:** During the upgrade of a SunSystems version older than v6.2.1, a section of the business unit upgrade script splits out data from one table, ZZZ_SSRFMSC, where ZZZ is the business unit code, to multiple new tables, for example, ZZZ_LDG_DEFN. On completion, the data from the ZZZ_SSRFMSC table will be retained in the ZZZ_SSRFMSC_SAVE table.

**Caution:** Scroll through the upgrade screen to ensure that you identify any issues which do not stop the upgrade but produce a log file. If any issues are reported, you must restore the security database. The issues must be resolved and the upgrade process restarted from the beginning, including the prerequisites.

### A SunSystems business unit group forcing all scripts to be reapplied

**Caution:** The automated database upgrade process affects standard SunSystems tables only. It does not affect any non-standard tables created separately to SunSystems.

Upgrades one or more business unit groups and forces all scripts to be applied to the database whether they have changed or not.

To open this utility, select **SunSystems Database Utilities > Upgrade > A SunSystems Business Unit Group forcing all scripts to be reapplied**.

This utility takes longer to complete than **A SunSystems Business Unit Group** and must only be used by an experienced SunSystems installer, or under instruction from Infor Support.

### Custom forms

Upgrade your custom forms after the database upgrade has completed.

Select **SunSystems Database Utilities > Upgrade > Custom forms**.

Prerequisites:

- SunSystems client is installed on the machine on which you are running the Upgrade Custom Forms process.

- If you are upgrading from SunSystems 6.1.1, then the pre-upgrade Custom forms are in the business unit group.

**Note:** The custom forms upgrade procedure selects the appropriate custom forms for upgrade. This means it does not upgrade filters and forms for functions removed from the new version.
**Note:** The manual amendment of forms should be completed by an application consultant, as each form must be checked out and amended in Form Designer.
**Note:** It is likely that forms will need to be redesigned in order to utilize the Infor SoHo user interface.

**Caution:** A form may not be fully upgraded if it contains a field associated with any of these functions:

- BCS Budget Check Setup
- CAA Corporate Allocation Calendar
- CAD Corporate Allocation Setup
- CAR Corporate Allocation Ratios
- CAS Corporate Allocation Sources
- CAT Corporate Allocation Target
- DYB Daybook Setup
- FDU Asset Timing Rules
- FNL Financial Analysis Layouts
- FRH Financial Column Headings
- FSL Financial Statement Layouts
- FSR Statement Line Contents
- FTC Financial Table Columns Record
- FTF Financial Table Format Record
- FTR Financial Table Row Record
- JNP Journal Presets
- LEQ Ledger Sequences
- LES Ledger Setup
- TXD Tax Details
- PYP Payment Profiles.

# Domain DB Utilities

These utilities perform functions on the domain database.

The options included are:

- Add a SunSystems business unit group to a SunSystems domain
- Remove a SunSystems business unit group from a SunSystems domain
- Recover business unit links
- Business unit groups parameter maintenance
- Query Database file groups
- Re-link all the SunSystems business unit groups to a SunSystems domain
- Load Difference tables
- Structural Integrity Check - Domain

- Data Integrity Check - Domain
- Database Health Check.

## Add a SunSystems business unit group to a SunSystems domain

This option enables you to add an existing business unit group to an existing domain.

To open this option, select **SunSystems Database Utilities > Domain DB Utilities > Add a SunSystems Business Unit Group to a SunSystems Domain**.

## Remove a SunSystems business unit group from a SunSystems domain

Use this option to remove a SunSystems business unit group from a SunSystems domain and optionally delete the database if it is held on the local machine.

To open this option, select **SunSystems Database Utilities > Domain DB Utilities > Remove a SunSystems Business Unit Group from a SunSystems Domain**.

**Caution:** Removing a SunSystems database from a SunSystems domain deletes the server files.

If removal from the domain leaves only one registered business unit group, the domain automatically reverts to a single database environment.

**Caution:** Removal of the only remaining business unit group in a SunSystems domain renders the domain incomplete and in an unsupported state.

After selecting this option you must:

- specify whether the business unit group should be removed from the domain, or removed and deleted.
- specify the location for log files.
- select the domain datasource name in which the business unit group to be removed is registered, and specify whether this uses integrated security.
- select the datasource name used for the business unit group to be removed and optionally deleted.
- confirm that the database and server instance details are correct.
- confirm that the domain and business unit group details are correct.

## Recover business unit links

This option runs the stored procedure `SSP_REFRESH_BULINKS`, which removes the existing business unit link entries and recreates them based on the current `DB_DEFN` entries on the SunSystems business unit group.

To use this option, select **SunSystems Database Utilities > Domain DB Utilities > Recover Business Unit Links**.

## Business unit groups parameter maintenance

This option provides facilities for the maintenance of parameters on existing SunSystems domain databases and SunSystems business unit groups.

To use this option, select **SunSystems Database Utilities > Domain DB Utilities > Business Unit groups parameter maintenance > .**

## Query Database file groups

This option lists the filegroups currently referenced in the SQL_OBJ_REGISTRY table.

To open this option, select **SunSystems Database Utilities > Domain DB Utilities > Query Database file groups**.

## Re-link all the SunSystems business unit groups to a SunSystems domain

This option re-links the existing SunSystems business unit groups to the existing SunSystems domain database. Use it to move the SunSystems domain database and SunSystems business unit groups from one server to another.

To open this option, select **SunSystems Database Utilities > Domain DB Utilities > Re-link all the SunSystems Business Unit Groups to a SunSystems Domain**.

## Load Difference tables

Use this option to reload the difference table in a specified SunSystems database with the data dictionary differences from a previous version of SunSystems.

To use this option, select **SunSystems Database Utilities > Domain DB Utilities > Load Difference tables**.

This utility is required for a custom upgrade. Use it to create a SunSystems database, either from scripts or by attaching a pre-configured database, and to upload the difference tables for the version that you are upgrading from. You must specify the log file folder location and the domain database information. A list of SunSystems databases that are in the domain database is displayed. Select the required database and the version of the data to be loaded in the difference tables.

You have the option to run further database utilities.

## Structural Integrity Check - Domain

This option performs a structural integrity check of all tables in the selected SunSystems domain database. This is the same check that is performed as part of the upgrade process.

To run this option, select **SunSystems Database Utilities > Domain DB Utilities > Structural Integrity Check – Domain**.

## Data Integrity Check - Domain

This option performs a data integrity check of all tables in the selected SunSystems domain database.

To run this option, select **SunSystems Database Utilities > Domain DB Utilities > Data Integrity Check – Domain**.

## Database Health Check

You can use the Database Health Check to check settings, performance, maintenance and housekeeping of the SunSystems databases and the instances that they reside on. See Database Health Check on page 144 for a table showing which items are checked.

To use this option, select **Database Utilities > Domain DB Utilities > Database Health Check**.

You must select a valid domain name and a database name.

**Note:** The version of the domain database must match the version of the SunSystems installation.

Two options are included with the Database Health Check:

- **`Include database performance testing`**

  Select this option to include performance testing. The results of the performance testing are retained for a specified number of months. For example, if you want to keep track of database performance over a period of time, specify **`Months to retain`** to indicate how many months the log files must be kept. The minimum value specified is **`0`**. The maximum value that can be specified is **`24`**. The default value is **`6`**. This means the log files are kept for 6 months.

- **`Exclude database performance testing`**

  The health check runs without any database performance testing.

The log file `DatabaseHealthCheck.log` is generated in the `ProgramData\Infor\SunSystems\Logs\Install` folder. The results are identified according to the type of observation made:

- **`Action`** - An action is required to resolve this status.
- **`Review`** - Further investigation is required to resolve this status.
- **`Information`** - Status information is provided but no action is required.

The generated log contains thorough and detailed information. It is expected to contain many rows.

| Name | Description | Type / Importance |
|---|---|---|
| Database Size | Total database size all data and log files | Information |
| Database Files | Lists all files for this database and their sizes | Information |
| Database Files Growth | Check all files have same file growth settings | Review |
| Database Owner | Lists the owner of each SunSystems database | Information |
| Collation Check | Best practice is the collation of the database to match the collation of the instance | Information |
| SunSystems version | Details the version of each of the SunSystems databases e.g. 6.03.00.1519 | Information |
| SunSystems Patch Set version | Details of the patch-set of each of the SunSystems databases e.g. S6 - PS - 01 | Information |
| Data Audit Rows | Number of rows in the SSDA_STORE table | Information |
| Data Audit Setup | Number of rows in the SSDA_DDR table where `AUDIT_ACTIVATED = 1` | Information |
| Database Recovery Model | Details the recovery model option, `FULL`, `BULK` or `SIMPLE` | Information |
| Page Verification | Page Verification Not Optimal for Database, SQL Server may have a harder time recognizing and recovering from storage corruption. Consider using `CHECKSUM` instead. `CHECKSUM` is the recommended setting | Action |

| Name | Description | Type / Importance |
|---|---|---|
| Database compatibility level | The database compatibility level must the highest supported by the server product version. Indicates that this is not the case and should be changed | Action |
| Database backups | Check backups are being done. Checks the date and time of the last backup and reports is one hasn't been done in the last 7 days | Action |
| Service Broker Enabled | Checks that the Service Broker is enabled for the Domain, Security and Landlord databases to enable SQL Query Notifications when changes are made in the database | Action |
| Database file growth | Percent grown is not best practice, fixed growth is better. Action if percent Review for fixed to ensure growth size is big enough so growth doesn't happen too often | Action / Review |
| DBCC CHECKDB last good run | This should be run on a weekly basis if not more frequently. Checks the date and time of the last `CHECKDB` and reports is one hasn't been done in the last 7 days | Action |
| Database option AUTO_CLOSE | Must always be set to `OFF`, must be amended if set `ON` | Action |
| Database option AUTO_CREATE_STATISTICS | Must always be set to `ON`, must be amended if set `OFF` | Action |
| Database option AUTO_SHRINK | Must always be set to `OFF`, must be amended if set `ON` | Action |
| Index fragmentation | Tells how many indexes have more than 100 pages and are more than 25% fragmented. Check your maintenance plans to ensure that a frequent process is run to keep the indexes defragmented. | Action |

| Name | Description | Type / Importance |
|---|---|---|
| Statistics review | Statistics that have more than 20,000 rows and less than 30% sampling. Check the statics and maybe rebuild them at a convenient time to ensure best performance. Tables with a large number of rows need a smaller sampling size | Action |
| SSP_DROP_WORK_TABLES | Date last run – should be run at least once a month. This procedure is a SunSystems one to keep the number of work tables to a minimum to improve performance | Action |
| SSP_DOMN_DROP_WORK_TABLES | Date last run – should be run at least once a month. This procedure is a SunSystems one to keep the number of work tables to a minimum | Action |
| SSP_HOUSEKEEPING | Date last run – should be run at least once a month This procedure is a SunSystems one to keep the number of rows in some interface tables to a minimum to improve performance | Action |
| Trusted Constraints - Foreign Keys | Identifies how many foreign keys that aren't currently set to trusted. Trusted constraints perform quicker than non-trusted ones. Can be enabled as an action in SunSystems function BUA | Action |
| Trusted Constraints - Check Constraints | Identifies how many check constraints that aren't currently set to trusted. Trusted constraints perform quicker than non-trusted ones. Can be enabled as an action in SunSystems function BUA | Action |
| Database users | List all users that have access to the database with the type of user | Review |

| Name | Description | Type / Importance |
|---|---|---|
| Recovery Mode full NO log backups | Details all SunSystems databases where the recovery mode is set to `Full` and no log backup have been done in the last 7 day | Action |
| Database Encrypted | Details whether transparent database encryption is enabled. If it is, you must ensure that certificate is backed up properly | Information |
| Database Change tracking | This is not a default setting, and it has some performance over-head. It tracks changes to rows in tables that have change tracking turned on | Action |
| Data Compression - table | Reports the number of tables where data compression is set | Information |
| Data Compression - index | Reports the number of indexes where data compression is set | Information |

# Database DB Utilities

### Structural integrity check

This utility checks the structural integrity of all tables in a specified business unit group.

To open this utility, select **SunSystems Database UtilitiesSunSystems DB UtilitiesStructural integrity check**.

This check is run on the domain database, and all business unit groups. It check is also run during the upgrade process.

**Note:** If the database integrity has been compromised, the **Structural Integrity Check** will fail. You must contact Infor Support or Infor Consulting Services in the event this occurs.
**Note:** All reported issues must be resolved before the upgrade can continue.

### Referential integrity check - SunSystems business unit group only

This utility checks the integrity of a SunSystems business unit group.

To open this utility, select **SunSystems Database UtilitiesSunSystems DB UtilitiesReferential Integrity Check – SunSystems Business Unit Group only**.

You must specify the SQL Server Instance Name and the SunSystems database. Errors or warnings generated by the check are listed in theR_ERR table and reports any issues found. The results should not stop an upgrade from running but should be addressed.

**Note:** The Referential Integrity Check should be run before a running a SunSystems upgrade, so that any errors can be resolved. The check may take longer to complete for larger databases.

### Query database file groups

List the filegroups referenced in the SQL_OBJ_REGISTRY table.

To open this utility, select **SunSystems Database UtilitiesSunSystems DB UtilitiesQuery database file groups**.

**Caution:** During an upgrade, you must ensure that all references to filegroups exist on the new machine, otherwise the upgrade will fail.

## Form actions

### Import forms into a SunSystems Domain

Imports forms into a SunSystems domain database.

### Force Import forms into a SunSystems Domain

Imports forms into a SunSystems domain database, even if they may have been previously imported.

### Export forms from a SunSystems Domain

Exports forms from a SunSystems domain database.

### Remove forms from a SunSystems Domain

Removes forms from a SunSystems domain database.

## Security DB

### Grant permission to Security DB

Grants the Windows Service Groups access to the Security database.

# Migrating databases

SunSystems databases can be migrated from one database server to another. Only database administrators can perform migrations, and the process requires downtime of SunSystems.

Before you can migrate a database, you must complete the prerequisites for migration:

- The version of the source and target Microsoft SQL Servers must be the same,
- The version of Windows, service pack level and operating system language must be the same.
- The user performing the migration must have Windows and database administrator rights.
- All SunSystems users must be logged off, and all SunSystems Windows services must be stopped.
- A SQL Server Login for the SunSystemsServices and SunSystemsClients groups must be created on the target database server. The Windows group names used must be the same for both servers.

See the *SunSystems Upgrade Guide* for the correct upgrade procedure for databases. It describes the steps to migrate a database from a source to a target server.

# Chapter 8: Microsoft SQL Server

In Microsoft SQL Server, performance and capacity can be increased by scaling up and scaling out. Scaleup means increasing the power of the database server. Scaleout is achieved through linked servers.

**Caution:**

- Before starting, you must ensure that you have administrator access to the SQL Server machines and Domain Controller machine to configure, or verify, the linked server environment.
- We do not recommend that you install SunSystems components on the Active Directory Domain Controller. Additionally, Microsoft advise against installing SQL Server on the Domain Controller.

**Note:**

- Standalone and 2-tier deployments of SunSystems are not supported in a linked server environment.
- When creating a new Linked Server, the fields RPC and RPC Out must be set to **`True`**, in Server Options. Otherwise, error messages are displayed when setting the Application Role in User Manager.
- To serialize SunSystems in a linked server environment, open the serialization file using Notepad and manually enter the details into SunSystems Serialisation (ZZS).
- SunSystems connects directly to the SQL Server default instance on port 1433. If a named SQL Server instance is being used, or a non-default port, the SQL Server Browser service is used to make the connection to the server.

## Configuring the linked server connection on the database server

**Note:** If you are using SQL Server 2019 or 2017 then you must create linked servers using the fully qualified domain name. You must also check that the server is specified in User Manager using the fully qualified domain name. In User Manager, select **Settings > SunSystems > Configure...** and specify the server using the fully qualified domain name.

1. Log in to Microsoft SQL Server Management Studio using an administrator account that includes sysadmin rights on SQL Server.
2. Expand the SQL Server instance node and select the **Server Objects** node.
3. Select **Linked Servers > New Linked Server > General**.
4. Specify **`Linked Server`** as the other database server name.
5. Select **SQL Server > Security**.

6 Select **Be made using the login's current security context**.

7 Select delegation for the domain service account.

**Note:** If your business unit groups and domain databases are on the same server, then NTLM Authentication is sufficient. This includes AlwaysOn Availability Groups where the Linked Server is configured for the listener name. Kerberos authentication is required with Linked Server when business unit groups and the SunSystems domain database are on different SQL Servers instances

8 In Active Directory, select delegation for the domain service account. Ensure that the relevant Service Principal Names exist.

9 Run the system stored procedure `sp_linkedservers` using the master database to verify the linked server configuration.

## Verifying the linked server connection for the SunSystems application

To verify the linked server connection fof SunSystems:

1 Open SunSystems navigator.

2 Select **Business Unit Administration** (BUA).

3 Create a business unit group in the linked server location.

4 Set the business unit group to be online.

5 Copy an existing business unit to the linked server business unit group.

# About Microsoft SQL Server clustering

Clustering refers to a group of two or more servers, or nodes that work together and are represented to a network as a single virtual server.

When a client machine connects to clustered SQL servers, the clustered SQL servers are recognised as a single SQL server. If one of the nodes fails, its responsibilities are taken over by another server in the cluster.

**Note:** SQL Server Reporting Services (SSRS) should not be installed on the SQL Server Cluster. It should be installed on its own server with the ReportServer database on the cluster. Should a SQL Server failover occur, SunSystems services will need to be restarted to reestablish connections to the databases. SunSystems users must be logged off and their activity cleared in **Operator Activity**, in **User Manager**. Users will need to log back into SunSystems.

When you install SunSystems for the first time use the SQL Server cluster address when creating the domain database, business unit group, and security database.

# Database replication

Database replication is not supported as a means of providing high availability or failover.

# Specifying a DNS CNAME record as a server alias

SunSystems 6.4 uses Microsoft JDBC driver for SQL Server. Microsoft SQL Server Alias is not supported by Microsoft JDBC driver for SQL Server. Instead, we recommend that you specify a DNS CNAME record to provide a server alias. In case of a server failover, you should set up a standby database server.

#### Prerequisites

Before specifying a DNS CNAME record, you must:

- SunSystems 6.4 is installed in a multitier environment
- You have domain administrator access
- A database with a named instance of SQL Server, for example, INSTANCE1, has been installed. You can also use a default SQL Server instance.

## Specifying the Domain Name System (DNS)

To specify a Domain Name System:

1. Open DNS Manager.
2. Expand the console tree.
3. Right-click the correct forward lookup zone and select **New Alias (CNAME)**.
4. Specify the CNAME, for example, **`DBSERVER`**.
5. Browse to select the target host.
6. Click **OK** to expand the CNAME to the fully qualified domain name (FQDN) of the server running SQL Server.
7. Specify **Time to live (TTL)** as `5` minutes.

## Specifying the database server setup

To specify the database server setup:

1. Create a Linked Server in Microsoft SQL Server Management Studio:
   a. Specify the name of the SQL Server instance, to which you are linking, on the General page, in the Linked server section. This is your CNAME, for example, **`DBSERVER\INSTANCE1`**.

   **b** Select SQL Server as the server type. This indicates that the linked server is another instance of SQL Server.
   **c** Select **Be made using the login's current security contex**t n the Security page.

**2** Specify database relinking details:
   **a** Open SunSystems Database Utilities.
   **b** Select **Security DB > Grant permission to Security DB**. Enter the SunSystemsServices domain group details.
   **c** Select **Domain database > Re-link all the SunSystems Business Unit Groups to a SunSystems Domain**. Specify a Datasource name that includes an Instance name, for example, **`DBSERVER\INSTANCE1`**.
   **d** Select **Relink Details**. Specify the Instance name, for example, **`DBSERVER\INSTANCE1`**, and the SunSystems Business Unit Group Database name.
   **e** Select **Group Account Settings**. Specify the details for the SunSystemsServices and SunSystemsClients Windows Domain groups. Select the languages. On the Progress Monitor page, click **Next** to finish.

**3** Open Windows Firewall. Ensure the port connection between the SunSystems application server and the SQL Server database server instance is not blocked.

# Using CNAME to refer to the database server during a new installation of SunSystems

You can use the CNAME to refer to the database server, at the time of SunSystems installation.

During SunSystems installation, you must enter **`CNAME\<Instance>`** to refer to the SQL Server database instance.

# Amending an existing SunSystems installation to use CNAME to refer to the database server

You can use the CNAME to refer to the database server in an existing installation. To do this, you must specify the application server setup, specify the SunSystems Reporting Services setup and update the standby database server.

## Specifying the application server setup

Update the application server with the DNS CNAME:

**1** Open DeployManager.
**2** Select the **SunSystems Private Tiers tab**.
**3** In the Application Servers section, click **Server Name** and specify **`DBSERVER\INSTANCE1`**.

4 If required, specify the ports for IIS, Application, Security, Web Services and Tomcat.
5 Log into User Manager using the SunSystems Administrator account.
6 Select **Settings > SunSystems > Configure**.
7 Specify **`DBSERVER\INSTANCE1`**.
8 Click **Test connection**.
9 Click **OK** to save your changes.
10 Restart the SunSystems Security service.
11 Restart IIS using IIS Manager, or by using the IISReset command-line utility.
12 Use Restart Services to restart all SunSystems services.

## Specifying the SunSystems Reporting Services setup

**Note:** You must specify CNAME in SunSystems Reporting Services if SunSystems has been set up with Microsoft SSRS on the database server.

Update the SunSystems Reporting Services with the CNAME DNS:

1 Update DeployManager:
   **a** Run DeployManager.
   **b** Log in as a SunSystems administrator.
   **c** Select **SunSystems Private Tiers > Reporting Servers**.
   **d** Replace server name with the CNAME for SQL Server Reporting Services. Save your changes.
   **e** Run DeployAgent on the application tier and the web tier after all changes have been made.
2 Use IIS Manager, or the IISReset command-line utility, to restart IIS on the application server.

### Specifying CNAME if SSRS is not installed on the database server

Specify CNAME in Microsoft SSRS if it is not installed on the database server:

1 On the SSRS server, open the Report Server Database Configuration Wizard.
2 Select **Database > Change Database > Choose an existing report server database**.
3 Click **Next**.
4 Select the Report Server database, for example, **`ReportServer$INSTANCE1`**.
5 Click **Next**.
6 Set **Service Credentials** to **`Authentication Type`**.
7 Click **Next**.
   **Note:** Deleting the encrypted content may affect other systems using Microsoft SSRS.
8 Select **Encryption Keys**.
9 Click **Delete** to Delete Encrypted Content.
10 Click **OK**.
11 Restart the Report Server.

## Updating the standby database server

**Note:** You must keep the standby database up to date by using log shipping or by restoring database backups.

Refer to the section Copying the databases from source to target installation on page 120.

# Responding to a failover

**Note:** You must test that failover works in your test environment, before moving to a live environment.

In the event of a failover:

1. Use IIS Manager, or the IISReset command-line utility, to restart IIS on all SunSystems servers.
2. Restart all SunSystems services on all SunSystems application and web tier servers using the Restart Services tool.

# Maintaining SunSystems using scheduled SQL jobs

This set of SQL jobs can be used to assist in maintaining SunSystems. They are accessed from Database Utilities.

### SunSystems Domain databases - dbo.SSP_DOMN_DROP_WORK_TABLES

This stored procedure removes work tables from the domain database. It uses these parameters:

| Parameter | Description |
|---|---|
| **drop_list_flag** | Distinguishes between 'delete' and 'list'<br>Specify **1** for 'delete' and **0** for 'list' |
| **intg_retention** | Days to retain INTG tables<br>default is 7 days |

An example procedure to remove work tables from the domain database:

```
exec dbo.SSP_DOMN_DROP_WORK_TABLES 1,7
```

### SunSystems business unit group databases - dbo.SSP_DROP_WORK_TABLES

This stored procedure removes work tables from a business unit group. It uses these parameters:

| Parameter | Description |
|---|---|
| **drop_list_flag** | Distinguishes between 'delete' and 'list'<br>Specify **1** for 'delete' and **0** for 'list' |

| Parameter | Description |
|---|---|
| **db_code** | Specify a single business unit or blank '' to indicate all |
| **tdesk_retention** | Transfer Desk work tables<br>recommendation is 60 days (2 months), minimum retention is 7 days with a default of 60 |
| **cdesk_retention** | Control Desk tables<br>recommendation is 7 days, minimum retention is 2 days with a default of 7 |
| **recon_mng_retention** | Recon manager<br>recommendation is 7 days, minimum retention is 2 days with a default of 7 |
| **cdesk_iface_retention_int** | Control Desk Interface<br>recommendation is 30 days (1 month), minimum retention is 7 days with a default of 30 |
| **other_tabs_retention** | Number of days additional tables ('%SALQ' '%SALQ_EX', '%SALQVCNLST', '%SACDLI', '%SMCDSO') are to be retained since creation, recommended 60 days (2 months), cannot drop tables created less than 7 days ago with a default of 60 |

Example procedure to remove work tables from a business unit group:

```
exec dbo.SSP_DROP_WORK_TABLES 1,'',60,7,7,30,60
```

### SunSystems Housekeeping - dbo.SSP_HOUSEKEEPING

This stored procedure completes basic housekeeping tasks. It removes rows from permanent work tables so it must be run on one business unit at a time. Depending on the amount of data in the ledger details, it may take a long time to complete when it is first run. You can test this by setting the @ldg_details parameter to a negative number to start with.

Here is a list of parameters and which tables are affected:

| Parameter | Description |
|---|---|
| **bu_code** | The business unit code |
| **ldg_details** | number of months to retain the data after the associated transaction is complete<br>For example, if you specify 6 then all data in the LDG_DETAIL table is cleared where the transaction has been complete for longer than 6 months |

| Parameter | Description |
|---|---|
| **iface_tables** | Number of weeks to retain the data in these tables<br>For example, **1**<br>• ACNT_PYMT_IFACE<br>• ASSET_DISPOSAL_IFACE<br>• ASSET_STATUS_IFACE<br>• ACNT_PYMT_IFACE<br>• CALC_DEP_IFACE<br>• CASH_SUMMARY_IFACE<br>• DAYBOOK_IFACE<br>• GEN_ALLOCN_IFACE<br>• GEN_PYMT_IFACE<br>• LDG_REVAL_IFACE<br>• PMD_RDS_IFACE<br>• PMD_RPTG_IFACE_TBL<br>• TAX_RPTG_IFACE_FIN<br>• TAX_RPTG_IFACE_POP<br>• TAX_RPTG_IFACE_SC<br>• TAX_RPTG_IFACE_SOP<br>• TREASURY_DEAL_IFACE<br>• TRIAL_BAL_IFACE<br>• TXN_MATCH_IFACE<br>• VOID_PYMT_IFACE<br>• ALLOCN_IFACE<br>• CTRL_DSK_IFACE<br>• PYMT_REJ_IFACE |
| **del_fin_rpt** | Number of weeks to retain the data in these tables<br>For example. **1**<br>• FIN_ANL_RPT<br>• FIN_STMNT_RPT<br>• FIN_TBL_RPT |
| **del_bu_temp_tbl** | clear down the temporary tables used in business unit copy<br>**1**=yes<br>**0**=no<br>• BUCPY_XFER_TBL_LIST<br>• BU_TEMPLATE_PARAMS |

| Parameter | Description |
|---|---|
| **del_bu_wrk_tbl** | Number of weeks to retain the data in these tables<br>For example, 1<br>• ZZZ_AUTHORISTN_SET_BANK<br>• ZZZ_AUTHORISTN_SET_PAY<br>• ZZZ_BILLING_LINK_ADJUST<br>• ZZZ_COSTING_ITEM_COSTS<br>• ZZZ_COSTING_UD_COSTS<br>• ZZZ_COSTING_WORK<br>• ZZZ_COSTING_KEY_INFO<br>• ZZZ_CURRENTLY_SELECTED<br>• ZZZ_DOC_FMT_HLD<br>• ZZZ_ERR<br>• ZZZ_GEN_INVY_CNT_WRK_1<br>• ZZZ_LINK_CHECK<br>• ZZZ_NOTE_DETAIL_TEMP<br>• ZZZ_NOTE_LDG_TEMP<br>• ZZZ_NOTE_TEMP<br>• ZZZ_PSTG_ERR<br>• ZZZ_PSTG_ERR_MSG<br>• ZZZ_PSTG_WRK_TBL<br>• ZZZ_PSTG_WRK_TBL_NOTE<br>• ZZZ_SAPYDDB<br>• ZZZ_SAPYPAY<br>• ZZZ_VCHR_WRK |
| **del_other_tbls** | Number of weeks to retain the data in these tables<br>For example, **1**<br>• DAG_TEMP<br>• DDE_USER_LABEL_WRK<br>• OFCD_WORK_FILE<br>• OPR_BU_PERD<br>• OPR_SESSION<br>• RECON_MGR_TEMP<br>• RECON_MGR_TEMP_LAD<br>• RI_ERR<br>• RWFNUM_STREAM<br>• SSLINKAGE |
| **return_err_no** | Returns a SQL error number (integer) if an error has occurred |
| **return_err_msg** | Returns the SQL error message (nvarchar(250)) if an error has occurred |

Example Housekeeping statement using business unit PK1:

```
Declare @return_err_no integer, @return_err_msg nvarchar(250)
exec dbo.SSP_HOUSEKEEPING 'PK1', 6, 1, 1, 1, 1, 1,
@return_err_no output, @return_err_msg output
```

Example Housekeeping statement to run for all business units in one business unit group:

```
declare @bu_code nchar(3)
declare @return_err_no integer
declare @return_err_msg nvarchar(250)

declare bu_cursor cursor fast_forward for
select DB_CODE from dbo.DB_DEFN with (NOLOCK) where DB_CODE <> '' order
by 1
open bu_cursor
fetch next from bu_cursor into @bu_code
while @@FETCH_STATUS = 0
begin
    exec dbo.SSP_HOUSEKEEPING @bu_code, 6, 1, 1, 1, 1, 1,
    @return_err_no output, @return_err_msg output
    fetch next from bu_cursor into @bu_code
end
close bu_cursor
deallocate bu_cursor
go
```

If you receive an error after executing the SSP_HOUSEKEEPING procedure, you can record the error and report in a way that is suitable for your business.

#### Resetting the operator information after a reboot only

This stored procedure clears all login information.

**Note:** This stored procedure may only be run immediately after the servers are rebooted. It is not permissible to run it at any other time.

This script must be run on a domain database:

```
Delete from dbo.DOMN_DB_OPR
go
update DOMN_OPR set LOGIN_IND = 0, CURRENT_DB_1 = '', CURRENT_DB_2 = '',
 CURRENT_DB_3 = '', CURRENT_DB_4 = '',
    CURRENT_DB_5 = '', CURRENT_DB_6 = '', CURRENT_DB_7 = '', CURRENT_DB_8
 = '', CURRENT_DB_9 = '',
    CURRENT_FUNCTION_1 = '', CURRENT_FUNCTION_2 = '', CURRENT_FUNCTION_3
 = '', CURRENT_FUNCTION_4 = '',
    CURRENT_FUNCTION_5 = '', CURRENT_FUNCTION_6 = '', CURRENT_FUNCTION_7
 = '', CURRENT_FUNCTION_8 = '', CURRENT_FUNCTION_9 = '',
    CURRENT_SYS_1 = '', CURRENT_SYS_2 = '', CURRENT_SYS_3 = '', CUR
RENT_SYS_4 = '',
    CURRENT_SYS_5 = '', CURRENT_SYS_6 = '', CURRENT_SYS_7 = '', CUR
RENT_SYS_8 = '', CURRENT_SYS_9 = '',
```

```
    PRESENT_BDGT = '', PRESENT_DB = '', SESSION_ID = '', CURRENT_NAV
MAN_PROP = NULL
go
```

# Revoking guest user access in a database

Microsoft SQL Server creates a guest user each time a database is created. The guest user exists to permit access to a database for logins that are not mapped to a specific database user. Any login can use the database through the guest user.

The SQL Server guest user is not required by SunSystems. Please consult Microsoft documentation if you wish to remove it.

It is common practice to revoke the access rights of the guest user as part of securing an environment. See the Microsoft website for more details.

# AlwaysOn Availability Groups requirements

**Note:** All databases within the same AlwaysOn Availability Group are supported. AlwaysOn Availability Groups with SQL Server standard edition are not supported because of the limitations imposed by this version.

During a new installation, SunSystems databases are created using Database Utilities then added to AlwaysOn Availability Groups. The Linked Server to the listener name must be set up.

**Note:** Before running the upgrade process, SunSystems databases must be removed from AlwaysOn Availability Groups, and added back after the upgrade has completed.

# Configuring Kerberos for Microsoft SQL Server

When setting up AlwaysOn Availability Groups, you must ensure that Linked Server works with Microsoft Kerberos.

**Note:** NTLM Authentication is sufficient if you have your business unit groups and domain database on the same server. This includes with AlwaysOn Availability Groups where Linked Server is configured for the listener name. Kerberos authentication is required with Linked Server when business unit groups and domain database are on different SQL Servers instances. For example, attempting to add an additional business unit group to an instance on another linked server will result in the error message `NT AUTHORITY\ANONYMOUS LOGON` if Kerberos has not been configured.

To configure Kerberos for both SQL nodes and your AAG listener:

1. Download the Microsoft Kerberos Configuration Manager for SQL Server.
2. Clear all GUIDs in the local administrator group.

3 Run Kerberos Configuration Manager for SQL Server and resolve any delegation or SPN issues.
4 Locate the database engine service account from an Active Directory domain controller.
5 Open the **Advanced** view.
6 Select **Attribute Editor > servicePrincipalName**.
7 Add a new entry, consisting of two SPNs, for the AAG listener.

   The new entry is in addition to the existing four entries. For the new entries, use the same format as the existing entries, but use the FQDN of your listener computer object.
8 Add a new entry that contains the port number.

   There should now be six SPNs, if you have two replicas in your availability group.
9 Open Database Utilities.
10 Select **Re-link all the SunSystems Business Unit Groups to a SunSystems Domain** and relink to a domain using the listener name.

If these steps are not completed, then the message `Could not find server <servername> in sys.servers` is displayed.

## Setting up AlwaysOn Availability Groups

Complete these steps to set up the AlwaysOn Availability groups:

1 Create the SunSystems databases.
2 Add the SunSystems databases to the AlwaysOn Availability Groups.
3 Create the linked server to an AlwaysOn Availability Group listener.
4 Use Database Utilities to run Relink to a domain using the listener name.
5 If you are updating a previously installed version of SunSystems, you must specify the listener name for the server where the domain database is installed:
   a Open User Manager.
   b Select **Settings > SunSystems > configure**
   c Specify the listener name.
6 Amend the security `global.config` file to include the listener name for accessing the security database.

## Connecting to the AlwaysOn Availability Group Listener using non-default ports

AlwaysOn Availability Groups (AOAG) is supported when all SunSystems databases are in the same availability group. If required, a non-default port can be used to set up the SQL Server connection.

**Note:** This feature is available from SunSystems 6.4 Patch Set 14.

1 Open User Manager and select **SettingsSunSystemsConfigure**. Amend the port value.

2 Open SQL Server Management Studio to connect to the primary SQL Server Replica.
   a Select **AlwaysOn High Availability > Availability Groups** and select the Availability Group.
   b Select **Availability Group Listeners**. Right-click the Listener Name and select **Properties**.
   c Specify the port number.

   **Note:** Do not append the port number to the listener name.

3 Add a new registration for the SQL Server startup account using the non-default port. Open a Command prompt and run these three commands in the order listed:

   **a** `setspn -L <servicename/serviceaccount>`

   For example, **`setspn -L sunsystemsdomain/sqladmin`** where the **`sqladmin`** user is a startup service account of the SQL Server instance on the **`sunsystemsdomain`** domain.

   **b** `setspn -D <serviceclass/host:portservicename>`

   For example, **`setspn -D MSSQLSvc/mylistener.sunsystemsdomain.com:1433`** where **`mylistener`** is an AOAG listener.

   **c** `setspn -S <serviceclass/host:portservicename>`

   For example, **`setspn -S MSSQLSvc/mylistener.sunsystemsdomain.com:56789`** where **`56789`** is a non-default port of **`mylistener`**.

4 Open SQL Server Management Studio to recreate the linked server object for the listener name.
   a Specify this information:

   **Server type**
   Select **`Other data source`**

   **Provider**
   Select **`Microsoft OLE DB Provider for SQL Server`**

   **Product name**
   Specify **`SQLServer`**
   **Note:** Do not include a space between **`SQL`** and **`Server`**.

   **Data source**
   Specify **`<listener name>,<port>`**

   b Click the **Security** tab and select **`Be made using the login's current security context.`**
   c Click the **Server Options** tab. Ensure that both **RPC** and **RPC Out** are set to **`True`**.
   d Create a second linked server for the FQDN of the listener name. You must repeat this step for all replicas.

   **Note:** You can check that the second linked server setup is correct by running this SQL query:
   `select * from sys.sysservers`

5 Remove all SunSystems databases from the Availability Group.
6 Run the latest version of Database Utilities (version 3 or later) to re-link your business unit groups.
   a Select **SunSystems Database Utilities > Domain DB Utilities > Re-link all the SunSystems Business Unit Groups to a SunSystems Domain**.
   b Specify this information:

**Instance Name**
Specify **<listener name>,<port>**

**Database Name**
Select the SunSystems domain database.

c Click **Next**. In the Relink Details window, select the business unit groups from the list.

**Note:** You must ensure that the Instance name is set to **<listener name>,<port>** for each business unit group.

d Click **Next**. Specify the Windows Domain Groups for SunSystems.

e Click **Next** to complete the remaining details then click **Next** to run the function.

**7** Set the port number for the connection to the SunSystems security database. Open the `\Program Data\Infor\SunSystems\Security\global.config` file on the SunSystems application server. Edit these lines to add the port element:

```
<database>SunSystemsSecurity</database>
<server>servername</server>
<port>nnnn</port>
```

**Note:** Do not append the port number to the database.

**8** Open User Manager and select **Settings > SunSystems > Configure**. Specify the port number in the port field.

**Note:** If you are unable to update the connection details using User Manager, then update the security port in the security database using this query:

```
UPDATE [<security-db-name>.{dbo].[SCTY_PROPERTIES] SET NUMPROP = <non-
default port> WHERE PROPNAME like 'db.port'
```

**9** Run Restart Services to restart the SunSystems services.

**10** Open SunSystems and select **Business Unit Administration (BUA)**. Bring all your business unit groups online.

**11** If there are report server databases in the AlwaysOn Availability Group, then these must be reconfigured in the SQL Server Reporting Services Configuration Manager.

# Chapter 9: SunSystems Connect

SunSystems Connect provides an Extensible Markup Language (XML) and Simple Object Access Protocol (SOAP) interface through which developers can access SunSystems data and core functionality. **Note:** SSC client applications must be run on the SSC application server. This includes Audit Viewer, Transaction Monitor and Component Manager.

## Software requirements

SunSystems Connect and Automation Desk require:

- Microsoft Windows Server 2016 (Standard or Enterprise)
- Microsoft Windows Server 2019 (Standard or Enterprise)

Third party applications that make SOAP calls to SSC, must be running on a machine with the required software.

## Installing SSC

When you install SunSystems Application Server, the Connect Server is automatically installed.

**Note:** Settings previously made in Property Editor are now specified in Configuration Manager (CGM). See the Configuration Manager help in the Online help for details.

### SSC layout

SSC is installed into the subdirectory ssc in the SunSystems program directory. The default folder structure and requirements for Write Permissions are listed in Appendix C.

### Changing the SSC TCP port value

The port value for SSC TCP is changed in DeployManager.

# Chapter 10: SunSystems Reporting Services (SRS)

You can manage Reporting properties using the Reporting module in Configuration Manager. In SunSystems, select **Configuration Manager (CGM) > Reporting**.

## Changing the SunSystemsReporting user and password

The installation process sets the **`SunSystemsReporting`** user as the identity for both Microsoft SQL Server Reporting Services and SunSystems Reporting Services.

**Note:** When moving from a domain account to a local account (or vice versa) you may need to add or remove RSWindowsNegotiate to the AuthenticationTypes in the `rsreportserver.config` in SSRS.
**Note:** Ensure that the new account has **`Read`** and **`Execute`** permissions to the SQL Server Reporting Services `RSTempFiles` folder, and all sub-folders. The path of the RSTempFiles folder is usually `ProgramFiles%\Microsoft SQL Server\MSRS13.MSSQLSERVER\Reporting Services\RSTempFiles`.

After installation, if you need to change the **`SunSystemsReporting`** user and password you must:

1. Add the new **`SunSystemsReporting`** user to the domain **`SunSystemsServices`** group.
2. Update the credentials used by Microsoft SQL Server Reporting Services:
   a. Run Reporting Services Configuration Manager from the **Start Menu** on the server hosting Microsoft SQL Server Reporting Services.
   b. Select the instance of Microsoft SQL Server Reporting Services used by SRS.
   c. Click **Connect**.
   d. Select **Service Account**.
   e. Select **Use another account**.
   f. Enter the domain and user account details and password for the new SunSystems reporting user.
   g. Click **Apply**.
   h. If required, back up your new encryption key to the local file system.
   i. Check for any errors in the **Results** panel.
3. Update the credentials used by the SunSystems Reporting Services web applications:
   a. Run Internet Information Services (IIS) Manager on the server hosting the SunSystems Reporting Services web applications.

b Expand the server node, in the tree. This is usually identified as the name of the server.
c Select **Application Pools**.
d Select the **SunSystemsReportingServices** Application Pool.
e Select **Actions > Advanced Settings**.
f Select the **Identity** property.
g Click the ellipses (**…**).
h Select **Custom account**.
i Specify the domain and user name of the new SunSystems reporting user.
j Click **OK**.
k Close IIS Manager.

**4** Update the credentials used by the SunSystems Reporting Services applications:
a Open the **Services** control panel applet.
b Select the **SunSystems Report Manager Service**
c Select **Action > Properties**.
d Select the **Log On** tab.
e Select **This account**.
f Specify the domain, user name and password of the new SunSystems Reporting user.
g Click **OK**.

**5** Run `ConfigureMSRS.exe` on the report server to add the domain user:
a Open a command prompt.
b Navigate to `\Program Files\Infor\SunSystems\`.
c Specify this command: `configuremsrs -install -instance [sql instance] -user [domain]\[user]`

**6** Check that `ConfigureMSRS.exe` has completed successfully:
a Open your browser as an administrator.
b Navigate to `http://localhost/Reports`.
c Select **Settings > Site Settings > Security**.
Ensure that domain\user has been added.

**7** Check that Service Broker is enabled for both the domain and security databases:
a Open Microsoft SQL Server Management Studio.
b Select **Databases > SunSystemsDomain > Properties > Options**.
c Select **Service Broker** and complete this information:

**Broker Enabled**
Select **`true`** to enable this setting.

# Managing and deploying reports

During installation, example reports are installed in a location that is accessible for demonstration purposes. This location is likely to be overwritten during an upgrade.

Operational reports must be deployed in a location more suitable to the requirements of the business. Path environment variables must be amended, and the appropriate folder level permissions set.

Reports may be renamed using the convention used by the example reports, or another appropriate convention.

# Configuring email support

Use Configuration Manager (CGM) in SunSystems navigator to configure SunSystems Reporting with the SMTP server.

Select **Configuration Manager (CGM) > Reporting > Common**.

See "Configuring the email settings for reporting" in the SunSystems online help.

# Chapter 11: SunSystems Web UI

The SunSystems Web user interface is customized in Configuration Manager (CGM). For example, you can change the font, colour, or how the session navigation menu is displayed in Infor Ming.le™.
**Note:** To use Configuration Manager, your user must be a member of the Configuration Administrators group.

Some properties in Configuration Manager require the SunSystems services to be restarted before changes are saved. Services are restarted using the Restart Services tool.

# Chapter 12: Troubleshooting

The information included in the Troubleshooting section will help system administrators resolve problems that are encountered during the installation process, or when attempting to start up SunSystems.

If the problem you are experiencing is not detailed below, you can contact technical support. Before calling for technical assistance, collate the information described in Contacting Technical Support.

You can search for known issues in the Support Knowledgebase on the Infor Support Portal. Often a solution can be found here before contacting Infor Support.

## Troubleshooting hints

There are several troubleshooting hints that will assist you when analyzing a problem:

- Take copies of error messages. They contain important information and technical support staff will require details.
- Do not assume too much about the possible cause of the problem, or you might overlook any evidence.
- Work carefully through the problem, ensure that you can duplicate the problem and assemble all the evidence, because you might need to pass it on to a member of the technical support staff.
- Confirm if the problem happens in other applications, on other user's machines, or only on one machine.
- Check security barriers (firewalls) because these can block communications between client and server machines.
- Do not overlook the obvious; check plugs, connections and cables.

## Support Knowledgebase on the Infor Support Portal

This knowledgebase is maintained by Infor Technical Support and contains helpful information regarding problems that may be encountered by customers implementing SunSystems. It is important to search by the SunSystems version number.

# General installation problems

An error message or unexpected software behaviour are indicators of an installation problem. These are the most likely causes of installation problems:

- Insufficient user credentials
- Prerequisites not complete or correctly installed
- Incorrect installation settings
- Incorrect access control such as network settings or folder permissions
- Incorrectly set IP address
- Changes made to registry settings used by SunSystems
- Insufficient account permissions for database access
- SunSystems Security or Configuration Services not started
- Insufficient service accounts where log on as a service role is not set.

### About the setup program

Background settings are specified by the user and validated by the setup program, during installation. If a setting is changed after installation, this will cause errors and unexpected behaviour in SunSystems.

The condition of an error condition, or unexpected response to a request, is described in an error message. To save the error message text to a file, click **Save**. A member of technical support can then analyze the contents of the file.

After saving an error message, you are given the option to continue working in SunSystems, or to abort. If you choose to continue, SunSystems operates normally as far as possible; if the error is too severe, it aborts automatically.

# Problems encountered during installation

Specific installation problems can be identified by a symptom, or error message. The most common installation problems are listed in this section and include a description of possible causes and solutions.

## Missing prerequisites

Where possible the SunSystems installer checks and notifies the user of any missing prerequisites. However, in the event of an installation problem, check that all the prerequisites have been correctly installed. Refer to the Prerequisites checklist on page 17.

## Tools for diagnosis

DeployManager and DeployAgent can be used as tools to help you validate your installation. In DeployManager you define your SunSystems Deployment. DeployAgent applies the deployment you defined in DeployManager.

Use the function Deployment Monitor, which is part of DeployManager, to validate all connections. Red indicates a firewall block or problem. When viewing results, consider that some connections may not be accessible due to firewall settings.

DeployAgent and DeployManager generate log files in `ProgramData\Infor\SunSystems\Logs\Deploy`.

Use the Restart Services tool to restart the SunSystems Services in the correct order:

1. Security and Configuration Services
2. SunSystems Connect Server
3. All other services.

## Configuration Service will not start

To diagnose problems starting the configuration service, check the `ConfigurationService.log` located in `ProgramData\Infor\SunSystems\Logs\Configuration`.

## 404 not found errors in browser

This error message means that the browser client can contact the server but the server cannot find what was requested. This could be caused by cached information that is held in the browser. Press **CTRL R** on the browser to clear the cache.

## Connection problems

### Possible cause(s)

The firewall settings may be blocking the connection.

The connection to the Microsoft SQL Server may be broken.

### Solution

Check the Windows firewall settings.

Check connection to SQL Server. Open SQL Server Configuration Manager and expand SQL Server Network Configuration. Click **Protocols for `<instancename>`**. Right-click the Protocol name, **`TCP/IP`** and click **`Enabled`**.

## DeployAgent displays error “cannot connect to configuration service…”

**Possible cause(s)**

This error can occur in a load balanced environment because the load balancer may direct to a server which has not yet been fully configured.

**Solution**

Run DeployAgent on all other servers in the same tier. On the server with the error message, run RestartServices then run DeployAgent. This problem can occur on the Application tier or the Web tier, in a load balanced environment.

## Report Manager URL not accessible

**Possible cause(s)**

The Report Manager may not be connected to a Windows domain.

**Solution**

Check that your machine is connected to a Windows domain.

## Service will not start

**Possible cause(s)**

If `Log on as a service right` has not been given to the service account, then installation will pause to display a message stating that the service will not start.

**Solution**

Specify the service account details in Services, restart the service manually, and specify `Log on as a service right`. After clicking **OK** the SunSystems installation process resumes.

## Server Error in Application: “SunSystems SECURITY/SECURITYWEBSERVER HTTP” Error 404.3 not found

**Possible cause(s)**

This error could indicate that ASP.NET is not registered.

**Solution**

Check that ASP.NET is registered. Run a command prompt as administrator. Change directory to `Windows\Microsoft.NET\Framework64\v4.0.30319`. Enter the command `aspnet_regiis -lv` to check if ASP.NET is already registered. If not already registered, specify **`aspnet_regiis -ir`** to register.

## Client installation fails to validate the configuration api

**Possible cause(s)**

This issue only occurs in a SunSystems environment where you have applied SSL. A connection cannot be made between the client and the security service unless you make a specific registry change on the machine on which you are installing SunSystems client.

**Note:** In addition to client installation, this issue can occur when adding any node to your SunSystems installation.

**Solution**

You must enable this registry key on the machine where you are running the SunSystems installer:

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319]

“SchUseStrongCrypto”=dword:00000001
```

## Installer rolls back after attempting the installation - No message is displayed

**Possible cause(s)**

Roll backs are usually caused by a problem communicating with the Security and Configuration services. The services must be started by the installer in order to complete the configuration of SunSystems.

The roll back may also be caused by a SunSystems application still included in IIS after it has been uninstalled.

The `.msi` log is usually found in the `%TEMP%` folder, or the folder above. This log is not easy to interpret but contains the reason for the rollback.

Relevant information is also logged in the `InstallLog.txt`, usually found in `ProgramData\Infor\SunSystems\logs\Install`.

You can also open IIS Manager to check that all SunSystems applications have been uninstalled correctly.

## SunSystems Reporting Installation does not complete or it hangs when loading reports

**Possible cause(s)**

The SunSystems Configuration Service may not be running.

**Solution**

If this occurs, check that the SunSystems Configuration Service is running. The service is located on the SunSystems application server.

## The security password cannot be validated by the SunSystems installer during a re-installation over existing databases

A re-installation may be required if you move the databases to a different database server.

**Possible cause(s)**

An incorrect security admin password is used during the re-installation of SunSystems over existing databases. This causes the installation to fail and locks the security admin user in the security database. As SunSystems is not installed, you are unable to unlock the admin user in Security Console / User Manager.

**Solution**

You must edit the SunSystems security database SCTY_USER table:

```
NAME=admin set PWD_DATA=NULL
```

Install SunSystems using a blank password for the admin user.

## The reports fail to load after applying a patch set

### Possible Cause(s)

After applying a patch set, an error message indicates that the reports failed to load and that they must be loaded manually.

This issue occurs in a two-tier environment that includes a combined database / SSRS server and a combined web / application server. The installation order is important. In this scenario, reports cannot be imported by the installer until after Reporting Extensions are installed, which cannot be before the application tier is installed. This means that a manual step is required as part of the installation process.

### Solution

To load the reports manually:

1. After the patch set installation has completed, open `InstallLog.log`
2. Find the VisionImport command, and take a copy.
3. Run the VisionImport command from an administrator command prompt, using your administrator password. For example:

   ```
   "C:\Program File\Infor\SunSystems\VisionImport.exe" /U:admin /P:"******"
   /T:"/" /D:"C:\ProgramData\Infor\SunSystems\Reporting\Example Reports"
   /V:1 /O:YES
   ```

   **Note:** You must replace "******" with your administrator password that you use to log into UserManager.

# Problems encountered during uninstallation

Specific uninstallation problems can be identified by a symptom, or error message. The most common uninstallation problems are listed in this section and include a description of possible causes and solutions.

## Message displayed: Locked file detected when trying to uninstall <file name>

### Possible cause(s)

SunSystems or a session is still active.

### Solution

Before you attempt to uninstall SunSystems, ensure that all SunSystems sessions have been closed.

# Problems encountered when running SunSystems

Specific problems when running SunSystems can be identified by a symptom, or error message. The most common problems are listed in this section and include a description of possible causes and solutions.

## Message displayed: Integrity Failure 001. Please contact your maintenance supplier

### Possible Cause(s)

Serialization has not been applied. SunSystems is licensed specifically for several users and language combinations. Only the components with valid serialization information are operable in the production environment.

### Solution

Run the serialization on all application tier servers for all business unit groups.

## Message displayed: Number of Licensed Users Exceeded

### Possible cause(s)

The supplied serialization details are configured to allow an explicit number of users to connect to the system at any one time. This does not prevent the definition of additional users in the system, but does inhibit the number of concurrent users from exceeding the licensed number.

### Solution

If this imposed limit does not enable all required users to connect to the system, contact your SunSystems supplier to arrange a new license.

## Serialization – nothing happens

### Possible cause(s)

Your SunSystems user is not part of the Trusted Service Group.

#### Solution

If you run a SunSystems serialization and nothing happens, check that the user you are logged in with is in the Trusted Service Group. Open User Manager and select **Settings > SunSystems > Trusted Service Group**. Use Task Manager to end task the process `Serialise (32 bit)` before you try to run the serialization again.

## Log into SunSystems but there is nothing on the menu

#### Possible cause(s)

The operator group is not set up in User Manager

#### Solution

Log into User Manager as administrator. Select **Group** and add **Function Permission** and **Action Permission** settings. If there are required functions not showing on the menu you can recreate the menu in **User Group Menu Designer (UGM)**.

## Accessing SunSystems when logged in to Windows as a local user

#### Possible cause(s)

Standard authentication has not been set up globally in User Manager.

#### Solution

If SunSystems is to be accessed from client machines when users are not logged on as Windows Domain users, you must set standard authentication globally in User Manager. Log into User Manager as an administrator. Select **SettingsSecurity Policy**and clear **Enable Windows Authentication**.

## To login as a different SunSystems user

#### Possible cause(s)

Your SunSystems user is authenticated using Windows authentication.

#### Solution

If you are set up in User Manager as a Windows authenticated user, you will automatically be logged into SunSystems. Contact your SunSystems administrator to change your user to standard authentication.

## "BCP.exe version is too low" while running Language Deployer

**Possible cause(s)**

The PATH environment variable may be incorrectly ordered. This can occur if you have multiple versions of SQL Server installed.

**Solution**

Check that your PATH variable is correct. The latest version of BCP.exe must be listed first.

You can check the contents of the PATH variable by running `bcp -v` from a command prompt.

## Language characters are not displayed correctly on reports

**Possible cause(s)**

SunSystems Reporting requires language-specific fonts to render a report to PDF. From Windows 2016, some fonts are no longer automatically included and are optional Windows features.

**Solution**

You must install the required font pack on the server where the reports are installed:

1. Find the required language pack from Microsoft Support.
2. Install the language pack on the server where the reports are installed.
3. In Windows, select **App and Features > Manage optional features > Add a feature** and select the required font.

   For example, if Hindi characters are not displayed correctly, you must install the language pack for **`Devanagari Supplemental Fonts`**. This will be listed under **Add a feature**.
4. Wait for the notification that the font has installed, then reboot your server.
5. Re-run the report to see the characters displayed correctly.

# About diagnostic tools

In certain circumstances, it is useful to determine the environment and programs that are running if SunSystems is functioning incorrectly. It might be necessary, under the direction of technical support, to use the internal tools available:

- Server Monitor
- SunDebug
- SSC logging
- Transfer Desk logging.

These tools display and log the SunSystems program behaviour. This facilitates the resolution of system failures that are not identifiable by the error message. They should be used only under the direction of a SunSystems administrator or technical support.

## Database test program

The database test program is intended as an investigative tool to diagnoses database connection problems.

The program is called `databasetest.exe` and is installed in the `<SunSystems>\ssc\bin folder`. You should run the program from the command prompt. The `databasetest.exe` program has two modes of operation, with or without a parameter.

If it is run with a single parameter that contains a JDBC URL, the program tests that connection. The format of the URL depends on the type of runtime driver that is being used.

If it is run without a parameter, the complete suite of database tests is run:

- Low level domain database connection test
- Low level locator service connection test
- Request domain database information for the locator service
- Request list of data sources from the domain database
- Request database information for each data source
- Low level database connection test for each data source.

# SunSystems disaster recovery

Infor Consulting Services (ICS) should be consulted for advice on your disaster recovery strategy.

## Database recovery and integrity

If any of the SunSystems databases require recovery, you must restore the security, domain and all SunSystems data databases from the same backup set. This must be done using the tools provided with the database server installation, by a Database Administrator (DBA).

After successfully recovering the databases, check the integrity of SunSystems databases. There are several integrity checks supplied with Database Utilities.

If the database machine has been replaced as part of the recovery process, you must use the new database server with the SunSystems application server:

- Restore SunSystems databases (SunSystems data database, domain database and security database) on the new machine.

- Run the SunSystems database utilities and choose the option to re-link the SunSystems data database and domain database.
- Check the database structural integrity of domain and business unit groups using the SunSystems database utilities.
- Run SunSystems function BUA to synchronize and bring business unit groups on-line.
- Use the Restart Services tool on each application tier server.
- Serialize SunSystems on each application tier server.

# Contacting Infor Technical Support

If you continue to experience problems, contact your designated Support Centre as outlined in your Software Maintenance Agreement. If you are supported by Infor, go to the Infor Support Portal at https://concierge.infor.com and create a support incident.

You can search for known issues in the Support Knowledgebase on Infor Support Portal. Often a solution can be found here before contacting Infor Support.

When contacting Infor Support, you must provide:

- the SunSystems serial number and version number, which are displayed in SunSystems Help
- the platform operating system version and service pack or patch level
- the database and version
- a brief description of the circumstances relating to the problem
- details of the steps to replicate the problem
- any saved error message files, as appropriate.

# Appendix A: Glossary of installation terms

### Glossary terms

| Term | Definition |
|---|---|
| application server component | A software element that is installed on an application server. That is, the application layer. |
| business unit group | A collection of SunSystems business units that are stored in a single SunSystems data database. That is, a business unit group is a SunSystems data database. Business units must be unique; for example, you cannot have business unit AAA present in more than one business unit group. |
| central logs repository | A directory on SunSystems application server and client machine containing log files generated by SunSystems. Files are created in relevant folders under the central logs repository. For example: `ProgramData\Infor\SunSystems\logs` |
| client component | A software element that is installed on the client machine. For example, Security Client, SunSystems Client, and Reporting Client are elements that are included in the SunSystems client installation. |
| collation | The character set, code page, and sort order used for languages. For example, Latin1_General_Bin is the Western European default. |
| database server component | The server hosting the RDBMS |
| domain database | A central repository containing information to connect to multiple SunSystems databases, of different code pages, through a single application server, or application server farm. |
| firewall | A protective channel between a secured network and an unsecured network, through which all traffic must pass. |

| Term | Definition |
| --- | --- |
| SunSystems security | The services, applications, and features controlling access to SunSystems programs and data. |
| SunSystems domain | The one-to-many application server and database installation accessible from a client installation and managed from a central repository. The central repository is also known as a domain database. For example, a SunSystems domain can describe a three-tier installation which includes an application server farm and access to multiple databases. |
| SunSystems session | An open SunSystems window. Up to nine sessions can be open simultaneously. |

# Appendix B: SunSystems URLs

Use a browser to access SunSystems:

| URL | Description |
|---|---|
| http://<FQDN>sunsystems | The SunSystems application |
| http://<FQDN>/sunsystems-security | Opens the function SEU Security Console |
| http://<FQDN>/sunsystems-connectportal | Opens the function SCP Connect Portal |
| http://support.infor.com | Infor Support website |
| http://docs.infor.com | SunSystems documentation website |

Use these URLs if you have SSL and IIS set up in DeployManager:

| URL | Description |
|---|---|
| https://<FQDN>sunsystems | The SunSystems application |
| https://<FQDN>/sunsystems-security | Opens the function SEU Security Console |
| https://<FQDN>/sunsystems-connectportal | Opens the function SCP Connect Portal |

# Appendix C: Default folder structure and write permission requirements

### SunSystems sub-folders in Program Files

Default location: `Program Files\Infor`

Read & Execute permission is required for this folder by the accounts running SunSystems services.

| Folder name | File types | Description |
|---|---|---|
| `SunSystems` | | The `sun5.ini` defines the location of work files. In the case of multiple application servers this can be set to a central location.<br>`[SunSystems] Sys-Work=C:\ProgramData\Infor\SunSystems\_work\`<br>User Manager/SecurityConsole enables you set the work folder at operator level within `\ProgramData\Infor\SunSystems\`. |
| `SunSystems\_sql` | `.sql`<br>`.ini` | Contains folders that are specific to the database environment, namely the steering files, which determine the sequence in which the SQL scripts are run. |
| `SunSystems\web\sunsystems-security` | `.dll`<br>`.xml`<br>`.js` | Folders containing SecurityConsole IIS application files. |
| `SunSystems\web\sunsystems-login-internal` | `.dll`<br>`.js` | Folders containing SecurityWebServer IIS application files. |
| `SunSystems\SSC` | `.xml`<br>`.jar`<br>`.dat`<br>`.slc`<br>`.bat`<br>`.dll` | Tomcat deployment of SSC. The binary, support, and help files for SunSystems Connect are located in this folder. Various subfolders under the SSC folder are written to by SunSystems Connect, Transfer Desk, Automation Desks, Component Manager, and Configuration Manager. |

| Folder name | File types | Description |
|---|---|---|
| SunSystems\SunSystems Web | .conf<br>.xml<br>.dtd<br>.jsp | Tomcat deployment files of SunSystems Web. |
| SunSystems\web\sunsystems-transferdeskruntime | .dll | SunSystems TransferDesk Web IIS application files. |
| SunSystems\web\sunsystems-reporting | .dll<br>.config<br>.exe | SunSystems Reporting Services IIS Website. ReportManager, ReportDesigner and SunSystemsReportServer application files. |
| SunSystems\web\sunsystems-reportingmodels | | |
| SunSystems\web\sunsystems-query-api | | |

### SunSystems sub-folders in ProgramData

Default location: \ProgramData\Infor

Read/Write permission is required by accounts running SunSystems Services.

| Folder name | File types | Description |
|---|---|---|
| SunSystems_data | | |
| SunSystems_work | | Default location for work files, for example, for Ledger Entry |

| Folder name | File types | Description |
|---|---|---|
| SunSystems\Checkout | .sfl<br>.dtd | This is the default client directory to hold Source Form Layout (SFL) files. Used by **Form Designer (FRD)**, **Filter Designer (FLD)** and Filter DD Regeneration to store local copies of SFL files. Form Designer stores checked out and newly created SFL files in this directory. When executing a local form compilation, the SFL file in this directory is compiled.<br>The directory location is established during installation to CheckOut\, in the SunSystems root directory.<br>The location can be changed for SFL files respectively through the registry settings HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\SunSystems\Form Designer\5.1\Settings\SFLDir<br>The directory location can be overridden for a single form checkout through FormDesigner in the **Check Out** dialog box, the **Open Form** dialog box, the **Local Compile** dialog box, the **Check In** dialog box, and the **Options** dialog box on the **General** tab. |
| SunSystems\ClientFile Directory | .dtd<br>.msg<br>.opx<br>.rfx | Cached message files, menu files, and form files are downloaded from the server into this folder on the client. The locations can be changed for the various file types using the registry settings.<br>Message files<br>HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\SunSystems\Navigation Manager\5.1\FileCache\MSG DIRECTORY<br>Form files<br>HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\SunSystems\Navigation Manager\5.1\FileCache\RFX DIRECTORY |
| SunSystems\DataAudit | | |
| SunSystems\Databases | .mdf<br>.ldf | Default location for SunSystems SQL Server Database files |

| Folder name | File types | Description |
|---|---|---|
| SunSystems\Integration | | |
| SunSystems\Logs\SunSystems\ | .log | SunSystems and SRS log files |
| SunSystems\MessageFiles | .msg | Message files |
| SunSystems\Output | | |
| SunSystems\Parameters | | |
| SunSystems\Reporting | .srdl | SRS Example Report files for importing into Report Store database. Patched example reports are inserted here by the Patch Set procedure. The transformed Output folder is the default location for transformed reports. |
| SunSystems\RPTParams | | Work folder for SRS |
| SunSystems\SaveConfig | | |
| SunSystems\Security | .config | Location of SunSystems Security Global.config. |
| SunSystems\ServerInfoCache | | Folder to hold the cached information that is obtained from the server by Common Services. Used by **Form Designer (FRD)** and **Filter Designer (FLD)**.<br>If ServerInformation caching is switched on through the Server tab of the Options dialog box, the directory is created and is set to ServerInfoCache\ by the installation procedure.<br>The location of this directory cannot be changed. |
| SunSystems\SSC | | |
| SunSystems\SunSystemsWeb | | |

IIS application SecurityWebServer requires read permissions to redirection.config.

In Windows 2019 and 2016:

1. Browse to \Windows\System32\inetsrv
2. Select **Properties** in the Config folder.
3. Select the **Security** tab.
4. Click **Advanced > Continue > Add > Select a Principal > Location**.
5. Select your local machine and click **OK**.

6 Specify the **IIS AppPool\SecurityWebServer** and select **Check Names**.
7 Click **OK**.
8 Select **Read & Execute** in Permissions.
9 Click **OK**.

# Appendix D: Moving databases to a new database server

These instructions describe moving SunSystems databases to a new database server. For example, you may wish to move databases from UAT to production, or from production to UAT.

To move databases successfully you must complete this checklist:

### Checklist for moving databases to a new installation

| ✓ | Task | References |
|---|---|---|
| | Ensure that the 6.4 target environment is on patch set 5 or later.<br>If the source environment is a version that is earlier than 6.4, then refer to the SunSystems Upgrade Guide for the steps to upgrade the source databases to 6.4.<br>The patch sets must also align with the target installation so you must apply outstanding patch sets to the source databases using the corresponding Patch Set DBDeployer tool. | |
| | Ensure that the version of Microsoft SQL Server installed in the target environment, including service packs, is the same or higher, than the version installed in the source environment.<br>**Note:** The version of SQL Server in the source environment must not be higher than the target environment. | |
| | Ensure that:<br>• SQL Server Reporting Services<br>• SunSystems Reporting Services including Microsoft SQL Server Reporting Services Extensions and the corresponding patch set<br>are installed in both the source and target environment. | Installing Microsoft Reporting Services on page 21Installing the reporting tier on page 33 |
| | Ensure that all test data is removed from the source environment. This is relevant if you are moving databases from a UAT environment, and you have completed testing. | |

| ✓ | Task | References |
|---|---|---|
| | Reports are not exported by DeployManager so must be migrated separately. To do this, you can either export the reports, or move the Report Server database:<br>• Reports can be exported from SunSystems Report Manager in the source environment and imported into Report Manager in the target environment. This does not require moving the Report Server database. See 'Migrating Reports' in *Chapter 4: Post-installation tasks*.<br>• If you prefer to move the Report Server database, refer to the Microsoft documentation on moving Report Server databases. | Migrating reports on page 46 |
| | You must save the target SunSystems configuration. This must be completed before you restore databases in the target installation.<br>Do this by using DeployManager to run a configuration export from any application or web node in the target installation. | Exporting a configuration using DeployManager on page 119 |
| | In the source installation, ensure all SunSystems users are logged out from SunSystems.<br>Clear any outstanding operator activity sessions. | |
| | Make a note of the SunSystems administrator user and password. This information is required when you log into User Manager or Security Console. | |
| | Move the databases from the source installation to the target installation. | Copying the databases from source to target installation on page 120 |
| | In the target installation, stop all SunSystems services and the Report server. Stop the SunSystems website on all applicable nodes. | |
| | Setup the restored databases in the target installation. | Setting up databases in the target installation on page 120 |

# Exporting a configuration using DeployManager

Configuration information, regarding the machines that compose a SunSystems installation, is stored in the databases. This makes the transfer of databases between two similar environments reasonably complex.

**Note:** You only need to run the export once.

To export a configuration:

1. Run DeployManager from any application or web node in your installation.
2. Select **Function > Environment Migration**.
3. In the Export Environment, click **Export** to save the target configuration.
4. Make a note of the location of the generated `Sunsystems-Environment.zip` file. The default location is the `Documents` folder.

# Copying the databases from source to target installation

**Note:** Report server database names must not be changed when the databases are moved from the source system to the target system.
**Note:** **`SunSystemsServices`** is an example name for the windows domain group

Complete these steps:

1. Backup existing SunSystems databases and Report server databases on the source server. This includes the SunSystems domain, security, data, report store, and report store temp databases.
2. Copy database backups to the target machine.

   **Note:** The mechanism used to move the databases, for example, using a centrally accessible share, is chosen by the user.
3. Backup the SSRS encryption key on the source machine.

   **Note:** Complete this step using the Reporting Services Configuration Manager tool or the command line tool `rskeymgmt.exe` provided by Microsoft.
4. Copy the encryption key to the target machine.

You must now setup the databases on the target machine.

# Setting up databases in the target installation

Complete these steps to setup the databases in the target installation:

1. Using Microsoft SQL Server, restore all databases that were copied from the source system, onto the target system.

   **Note:** Ensure that you overwrite any existing databases in the target installation, with the copied databases from the source installation.
2. Enable Service Broker for the two Report server databases. In SQL Server, select **Properties > Options** and select **`true`** for **Broker Enabled**.
3. Relink all business unit groups to a domain database:

**Note:**

- Ensure all references to the new database server are updated. You must use the SunSystemsServices Windows domain group.
- SunSystems Database Utilities is available from SunSystems media but we recommend that you check the Infor Support Portal for the latest version as important changes were made for patch set 7.

a In Database Utilities, select **SunSystems Database Utilities > Domain DB > Re-link all the SunSystems Business Unit Groups to a SunSystems Domain**.

b Specify the **Instance Name** as the new database server/instance name.

Scripts should run without any errors.

**4** Grant the Windows service groups access to the security database. In Database Utilities, select **Security DB > Grant permission to Security DB**.

**5** Start the SunSystems Security service.

**6** Import the saved configuration of the target installation:

**Note:** You only need to run the import once. It can be run from any application or web node in the target installation. Importing the saved configuration ensures that the underlying software and configuration remain consistent.

a Run DeployManager.

b Select **Function > Environment Manager**.

c Find the `SunSystems-Environment.zip` configuration file that you exported previously, and select it for import.

**7** Run DeployAgent on all servers except the database server.

**Note:** DeployAgent must be run on the application nodes first, and the web nodes second.

**8** Use Reporting Services Configuration Manager to import the encryption key into SSRS. Ensure the Reporting Services are running correctly with the new Report Server databases.

**9** Create the SunSystemsReporting account with the RSExecRole and db_owner role for both Report Server databases.

**Note:** Complete this step using the Reporting Services Configuration Manager tool or the command line tool `rskeymgmt.exe` provided by Microsoft.

**10** If the service account running SQL Server Reporting Services is different on the target machine to the source machine you must run `ConfigureMSRS.exe`.

**Note:** `ConfigureMSRS.exe` is only found on the tier on which SRS Extensions are installed. An example of the command line required to run `ConfigureMSRS.exe` is `C:\Program Files\Infor\SunSystems\ConfigureMSRS.exe -install -instance MSSQLSERVER -user DOMAIN\SunSystemsReporting`

The instance of the Reporting Service, and the account under which the Report Server is running, must both be supplied.

**11** Run Restart Services.

**12** Log into SunSystems and select **Business Unit Admin (BUA)** to restore the business unit groups online.

# Appendix E: Changing location of SunSystems components in multitier configurations

The installation of SunSystems components on a different server requires updating elements of the installation configuration.

## Changing location of Microsoft SQL Server Reporting Services (SSRS)

To change the location of Microsoft SQL Server Reporting Services (SSRS):

1. Run DeployManager.
2. Log in as a SunSystems administrator.
3. Select **SunSystems Private Tiers > Reporting Servers**.
4. Specify a new server name.
5. Run DeployAgent on all nodes.

## Security Server, SunSystems application server and Connect service

Use Switch Security to reconfigure links from SunSystems client to SunSystems security server, and the SunSystems application server.

# Appendix F: Application file types

The list of SunSystems file types:

| File suffix | File type | Usage | Application |
|---|---|---|---|
| .420 | file | used to upgrade from ssformat to ssreport | SunSystems |
| .cfg | file | configuration files | SunSystems |
| .dat | file | data files | SunSystems |
| .dll | file | Dynamic Linked Library Validation routines | SunSystems |
| .gnt | file | generated application code | SunSystems |
| .idx | file | index for .dat | |
| .ini | file | application initialization file | SunSystems |
| .lib | file | library files | SunSystems |
| .MSG | Program messages | System messages invoked by a program | SunSystems |
| .ocx | file | control files for ActiveX | SunSystems |
| .sql | file | set of stored procedures and database scripts that is supplied with SunSystems | SunSystems |
| .xml | file | XML data file | SunSystems |
| .cmd | file | command file, similar to a batch file but available only under Windows | Transfer Desk |

| File suffix | File type | Usage | Application |
|---|---|---|---|
| .css | file | Cascading style sheet that describes the formatting elements of a HTML page | Transfer Desk |
| .dat | file | encrypted data file | Transfer Desk |
| .dtd | file | document type definition that is used to describe and validate the structure of an XML document | Transfer Desk |
| .hs | file | Helpset file, which describes how help files are grouped together | Transfer Desk |
| .htm | file | Hyper-text Markup Language file, which contains help and other documentation | Transfer Desk |
| .jar | file | Java archive file, which contains compiled Java code and compressed Java code that is executed at run-time | Transfer Desk |
| .jhm | file | JavaHelp information file | Transfer Desk |
| .js | file | JavaScript file used in HTML files | Transfer Desk |
| .jsp | file | Java Server Page, used to generate web pages on a Java web server | Transfer Desk |
| .log | file | Text format log file | Transfer Desk |
| .properties | file | Configuration file, similar to a .ini file, that specifies parameters/settings, which are a applied at run-time | Transfer Desk |
| .srdl | file | Report layout | SunSystems Reporting |
| .xsd | file | XML Schema Definition, which describes the structure of an XML document | Transfer Desk |

| File suffix | File type | Usage | Application |
|---|---|---|---|
| .xsl | file | Extensible Style sheet Language file, which contains information that is used to trans-form the structure of an XML document | Transfer Desk |

# Appendix G: Infor Support Policy and installations running virtualization software

The Infor Support Policy regarding virtualization software such as Terminal Services, Citrix Xenapp and so on.

We will fully support SunSystems deployed in test and production environments, where the SunSystems implementation uses virtualization software and has been correctly sized to provide adequate system resources.

We will not directly support the virtualization technology used because that is the responsibility of the relevant vendor.

Reported support issues will be investigated in the normal way. However, we reserve the right to ask a customer to reproduce the issue outside of a virtual environment, if we believe that the issue may result from the failure of the abstraction layer, or its configuration, to provide a suitable application environment.

# Appendix H: Logging management

Log files are generated to assist you with troubleshooting and are stored in subfolders that are named according to function name.

The subfolders are located under the main SunSystems log folder, which, by default, is found at this location: `\ProgramData\Infor\SunSystems\Logs`.

## Database test program

The database test program diagnoses database connection issues. It is located at: `\ssc\bin\databasetest.exe`. Run the program from the command prompt.

There are two modes of operation:

- with a parameter that specifies the JDBC URL

  The JDBC URL connection is tested. The format of the URL depends on the type of runtime driver that is being used.
- with no parameters

  The program runs the complete suite of database tests, including:
  - Low level domain database connection test
  - Low level locator service connection test
  - Request domain database information for the locator service
  - Request list of data sources from the domain database
  - Request database information for each data source
  - Low level database connection test for each data source.

# Appendix I: Administrative access recovery

The Infor Support Policy regarding virtualization software such as Terminal Services, Citrix Xenapp and so on.

For example, Security Console and User Manager will be inaccessible if Windows authentication credentials are incorrectly mapped, or if the SunSystems administrator leaves the company without informing another user of the administrator login details.

To avoid such situations, these steps must be completed by a local administrator or the server where the security service is running:

**Note:** This feature should only be used when the administrator is unable to access the system to correct problems in the configuration.
**Note:** This feature is not available if User Manager is accessed remotely. The user must be on the specific server and be a local administrator in Windows.

1. Ensure all users have logged out of SunSystems.
2. Stop the SunSystems Security service.
3. Edit the `global.config` file.

   Usually this is located in `\ProgramData\Infor\SunSystems\Security\`.
4. Change the property entry `<serveradminaccess>0</serveradminaccess>` to `<serveradminaccess>1</serveradminaccess>`.
5. Restart the service.
6. Run Security Console or User Manager as an administrator:
   - If you are using Security Console, then right-click your browser icon and select **Run as Administrator**. Run the url **`http://<server>/sunsystems-security`**
   - If you are using User Manager, then right-click the User Manager executable and select **Run as Administrator**.
7. Correct the problem that was preventing the administrator from gaining access.
8. Reverse the above process, reverting the configured property in `global.config` back to **`0`**.
9. Save and close the file.

Users can log into SunSystems.

# Appendix J: Ports, security and authentication

## Port usage

Use this table to check the correct ports are being used:

**Note:** The application server and security service are not exposed through ARR.

| Port function | Default number | Affinity |
|---|---|---|
| All SunSystems web tier end-points | 443 (80 for http) | none |
| SunSystemsWeb | 40000 HTTP | none |
| Application server | 40001 TCP | none |
| Security server | 40003 HTTP | none |
| SunSystems Web Services | 40003 HTTP | none |
| SunSystems Connect | 40004 HTTP | none |
| k Connect RMI | 40005 TCP | none |

## Load Balancing configuration

Use these tables to check that the correct ports are being used.

### Web Tier Load Balancer listeners

| Balancer proto-col | Balancer ports | Instance proto-col | Instance port | Affinity |
|---|---|---|---|---|
| HTTP(S) | Default port 80(443) | HTTP(S) | Default port 80(443) | none |

**Application Tier Load Balancer Listeners**

| Balancer protocol | Balancer ports | Instance protocol | Instance port | Affinity |
|---|---|---|---|---|
| HTTP(S) | Default port 80(443) | HTTP(S) | Default port 80(443) | none |
| TCP | Default port 40001 | TCP | Default port 40001 | none |

# Firewall rules

Ensure that these firewall rules are applied:

- Communication enabled from the application nodes to the application tier load balancer over the http/s port
- Communication enabled from the application nodes to the application tier load balancer over ports 40001 and 40003
- Communication enabled from the application nodes to the application ports 40000 and 40003
- Direct access from the application nodes to Microsoft SQL Server
- Communication enabled from the web nodes to the application tier load balancer over the http/s port
- Communication enabled from the web nodes to the web tier load balancer over the http/s port
- Communication enabled from the web nodes to the application tier load balancer over ports 40001 and 40003
- Communication enabled from the reporting nodes to the application tier load balancer over the http/s port
- Communication enabled from the rich client to the application server tier over ports 80, 40001 and 40003
- Communication enabled from the rich client to the web server tier over port 80
- Communication enabled from the rich clients to the exposed Desktop Service tier on ports 40001 and 40003
- Direct access from the reporting nodes to Microsoft SQL Server, that is, port 1433 must be open by default

# Folder permissions for services

Ensure these service permissions have been applied on the application server:

- Full Control permission is applied to `ProgramData\Infor` for all service accounts
- Read & Execute permission is applied to `Program Files\Infor` for all service accounts

- Modify permission is applied, during SunSystems serialization, to `ProgramData\Infor\Sun Systems\_data\SSSystem.dat` for the SunSystems Connect service account

# Component ports

This table shows SunSystems components and their associated ports:

| Component | 6.3 internal ports | 6.3 external ports | 6.4 internal ports | 6.4 external ports |
|---|---|---|---|---|
| SunSystems Connect service | 40004 | 80 | 40004 | 80 |
| SunSystems Application Manager port range | n/a | n/a | n/a | n/a |
| SunSystems Application Manager listener port | n/a | n/a | n/a | n/a |
| Application Server service | 40001 | 40001 | 40001 | 40001 |
| RMI registry | 50001 | 50001 (we recommend local box access only) | 50001 | 50001 (we recommend local box access only) |
| Job execution | port removed, use RMI registry | port removed, use RMI registry | port removed, use RMI registry | port removed, use RMI registry |
| Locator service | port removed, use RMI registry | port removed, use RMI registry | port removed, use RMI registry | port removed, use RMI registry |
| Transfer execution | port removed, use RMI registry | port removed, use RMI registry | port removed, use RMI registry | port removed, use RMI registry |
| Transfer Monitor RMI port ranges | port removed, use RMI registry | port removed, use RMI registry | port removed, use RMI registry | port removed, use RMI registry |
| Configuration service | 40003 | 80 | 40003 | 80 |
| Secure job execution | port removed, use RMI registry | port removed, use RMI registry | port removed, use RMI registry | port removed, use RMI registry |
| SunSystems Web security | 80 | 80 | 80 | 80 |
| SunSystems Security | 40002 | 40002 | 40003 | 80 |

| Component | 6.3 internal ports | 6.3 external ports | 6.4 internal ports | 6.4 external ports |
|---|---|---|---|---|
| Microsoft SQL Server Reporting Services | 80 | 80 | 80 | 80 |
| SunSystems Report services | 80 | 80 | 80 | 80 |
| SunSystems Web | 40000 | 80 | 40000 | 80 |
| ASP NET State server | 42424 | 42424 | 42424 | 42424 |
| SunSystems API service | 40003 | 80 | 40003 | 80 |

# Application timeouts

Timeout values for SunSystems URLs are set by the installation and cannot be updated by a user.

- `#set( $defaultTimeout = "00:02:00")`
- `#set( $webSunSystemsTransferdeskDesignerTimeout = "00:10:00")`
- `#set( $webSunSystemsReportingTimeout = "00:20:00")`
- `#set( $webApplicationTierTimeout = "01:00:00")`
- `#set( $webApplicationConnectTierTimeout = "1.00:00:00")`
- `#set( $webReportingTierTimeout = "01:00:00")`
- `#set( $appSunSystemsQueryApiTimeout = "01:00:00")`
- `#set( $appSunSystemsReportingApiTimeout = "01:00:00")`
- `#set( $appSunSystemsConnectTimeout = "1.00:00:00")`

# Appendix K: Example deployment of Secure Sockets

This example uses HAProxy load balancer and shows the deployment created and saved in DeployManager, and applied consecutively to each node, starting with the application nodes, then the web nodes.

| HAProxy load balancer | SS63WEBLB.infor.com | SSL on load balancer, port 443 |
|---|---|---|
| web node | SS63W1.infor.com | |
| web node | SS63W2.infor.com | |

| HAProxy load balancer | SS63APPLB.infor.com | SSL on load balancer, port 443 |
|---|---|---|
| application node | SS63A1.infor.com | |
| application node | SS63A2.infor.com | |
| SQL/reporting node | SS63DB.infor.com | Reporting tier connects to security server through the application load balancer |

# Appendix L: SunSystems and Transparent Data Encryption (TDE)

TDE is an encryption technology within Microsoft SQL Server that offers encryption at file level; TDE protects data by encrypting the physical files of the database: both the data (`.mdf`) and log (`.ldf`) files.

The encryption and decryption process is completely transparent to the applications accessing the database. The file pages are encrypted before they are written to disk, and decrypted when read back into memory. The process uses either Advanced Encryption Standard (AES) or Triple DES encryption algorithms. Essentially, this is real-time I/O encryption and decryption and does not increase the size of the database.

The main purpose of implementing TDE is to prevent unauthorized access to the data by restoring the files to another server / SQL server instance. The backup files of databases that have TDE implemented are also automatically encrypted. This means that in the event that a database backup is lost or stolen, restoring the database will not be possible without the appropriate certificate and encryption keys.

## TDE software requirements

TDE is only available with Enterprise or Developer editions of Microsoft SQL Server. It is not available in the Standard or Business Intelligence editions. No additional software is required to implement TDE.

## TDE implementation and management

Implementing TDE is simple. The process requires creating encryption keys and certificates:

1. Create a master key
2. Create a certificate protected by the master key
3. Create a database encryption key protected by the certificate
4. Use SET / ALTER to enable encryption on the database.

In the event of a database restore, the certificate protecting the database encryption keys must be available. To prevent data loss, therefore, server certificate backups must be maintained in addition to database backups.

## Implications for SunSystems

To use TDE, no application changes are required, to either the code or the schema. TDE is transparent and works in the background, which means that the user experience is the same whether using TDE-encrypted databases or non-encrypted databases.

However, there is a performance overhead. The encryption and decryption process requires additional CPU cycles; Microsoft estimates the performance impact to range between 3 and 30 percent, depending on the type of CPU usage. SQL Server instances with low I/O and low CPU usage will have the least performance impact whereas servers with high CPU usage will have the most performance impact.

It is possible to have a mixed setup where some databases are TDE-enabled and others are not, because TDE is enabled at the database level.

Limited initial testing in SunSystems indicates that there is minimal impact on performance.

## Impact on SunSystems support

SunSystems support consultants are often required to backup and restore a customers database in order to resolve a support issue. The backup files of TDE-enabled databases are automatically encrypted, which means that encryption keys and certificates must also be provided by the customer. Before restoring a TDE-enabled database, a consultant will require the database backup files, the service master key backup file, the master database master key backup file and the master database certificate private key.

Alternatively, users could pack the business unit into a store business unit group (database) that is not TDE-enabled.

## Considerations when implementing TDE

TDE is designed to protect data at rest by encrypting the physical data files, not the data itself. In contrast, data in transit, that is, data transmitted to or from a client across the network, is not encrypted. If there is a requirement to encrypt data across the network, then an SSL connection must be implemented on the clients. Additionally, in a Replication setup, data is not automatically replicated in an encrypted form from a TDE-enabled database.

One consequence of implementing TDE is that the TempDB database will be automatically encrypted as part of maintaining full protection by TDE. This may have a performance impact on any unencrypted databases sharing the same SQL Server instance.

A disadvantage of implementing TDE is that any benefit gained from backup compression is rendered negligible because the backup files are only minimally compressed.

Further details about TDE can be found on the Microsoft website: https://docs.microsoft.com/en-us/sql/relational-databases/security/encryption/transparent-data-encryption-tde

# Appendix M: Order Fulfilment wizards

There are two Order Fulfilment wizards available:

- Order Fulfilment Business Unit Template wizard
- Order Fulfilment Copy Data wizard.

The wizards are delivered with SunSystems as SunSystems Tools and Wizards. They are intended for use by Infor consultants, and must be run from the command line.

## Using the Order Fulfilment Business Unit Template Wizard (WBD)

The Order Fulfilment Business Unit Template wizard, also known as the BUOFT wizard, is provided with SunSystems to assist you with implementing and configuring your system. Use it to optionally rename and create multiple copies of movement, purchase and sales types.

The wizard is included in the Ease of Implementation set of tools.

**Note:** In SunSystems, you must ensure you are currently in the business unit in which data is to be created.

1. Setup the environment before using the wizard:
   a. Run **Business Unit Setup** (BUS) to create the business unit and to specify the operating environment.
   b. Ensure the relevant users are groups have access to the business unit by using User Manager.
   c. Ensure an application role has been created in User Manager.
2. Run the wizard:
   a. Navigate to `\TechProducts\easeofimplementation\buoftwizard`
   b. Run `simplewizard.sln` from the command line.
   c. Follow the steps in the wizard which guide you through the process.
3. Generate customer specific data, for example, items, accounts, customers and suppliers.
4. Amend the data generated by the wizard to replace the dummy codes with the customer specific codes.

# Using the Order Fulfilment Copy Data wizard (WCD)

The Order Fulfilment Copy Data wizard, also known as the OFCD wizard, is provided with SunSystems to assist you with implementing and configuring your system. Use it to generate one or more copies of a specific static data entry within the same business unit. For example, purchase, sales and movement types, ledger interfaces, items, customers and suppliers.

The wizard is included in the Ease of Implementation set of tools.

**Note:** In SunSystems, you must ensure you are currently in the business unit in which data is to be created.

1. Run the Business Unit Order Fulfilment Template wizard.
2. Navigate to `\TechProducts\easeofimplementation\ofcdwizard`
3. Run `simplewizard.sln` from the command line.
4. Follow the steps in the wizard which guide you through the process.

# Appendix N: Deployment Tools

DeployAgent and DeployManager are deployment tools that are responsible for the setup and configuration of the SunSystems environment and various infrastructure-related security settings. In particular, these tools are responsible for the Application Request Routing (ARR) solution used by all SunSystems deployments.

The tasks performed by DeployAgent to configure a SunSystems node, include simple configurations of IIS, or changes to SunSystems configuration properties. Some tasks are complex and based on industry standards and are documented in this appendix.

## Environmental setup tasks for DeployAgent

**Note:** The environmental setup tasks for SunSystems occur at system level and therefore may impact other applications.

These tasks are required for the secure operation of SunSystems and are performed whenever DeployAgent is run:

| Task Name - DeployAgent UI | Description | Notes |
|---|---|---|
| Updating HTTP protocol versions | Disables support for HTTP/2 protocol<br>This feature is only supported by Windows Server 2016/Windows 10 and IIS 10.0 | Feature disabled due to issues with NTLM. HTTP/2 does not currently support NTLM and some browsers have issues with the failback procedure - especially as NTLM has a specific synchronous set of requests<br>For example, running Chrome 58+ in a Infor Ming.le iframe, the page fails to load and requires a manual refresh to enable failback to HTTP/1.1<br>For these reasons, HTTP/2 is currently disabled by the DeployAgent tool. |

# Microsoft IIS ARR setup

The ARR Farms and Rewrite Rules required to support the Deployment Topology setup in DeployManager are created by the Microsoft IIS ARR setup task. It is used to configure the security features within IIS that are specific to the SunSystems applications, and are based on the known Topology.

| Task name(s) (as in DeployAgent UI) | Detailed description | Notes |
|---|---|---|
| Reconfiguring 'SunSystemsDefault' AppPool | 'SunSystemsDefault' is the AppPool responsible for handling ARR proxied requests.<br>A number of AppPool settings for ARR, that are recommended by Microsoft, are applied here | cpu.resetInterval:"00:00:00"<br>processModal.idle.Timeout:"00:00:00"<br>queueLength:"4000"<br>recycling.periodicRestart.time:"00:00:00" |
| Reconfiguring 'Custom HTTP Headers' for 'SunSystems Applications' | Removes all additional Custom HTTP Headers configured within IIS | This is required to prevent the 'doubling up' of HTTP headers due to the looping SunSystems proxy configuration.<br>In particular, the 'Powered By' HTTP header, specified by IIS/ARR by default. However, this also means that any HTTP headers that should be added to HTTP Response, must be added using URL Rewrite Rules. |

<table>
<tr><th>Task name(s)<br>(as in DeployAgent UI)</th><th>Detailed description</th><th>Notes</th></tr>
<tr>
<td>
<ul>
<li>Rebuilding 'Allowed File Extensions' for 'SunSystems Applications'</li>
<li>Reconfiguring WEB 'Allowed File Extensions'</li>
<li>Reconfiguring APP 'Allowed File Extensions'</li>
</ul>
</td>
<td>Clears the list of all acceptable file extensions which may be served by the 'SunSystems Applications' site.<br>Adds back a white list of acceptable SunSystems file extensions. All other extensions are refused by IIS.</td>
<td>The list of acceptable extensions is:
<ul>
<li><code>.htm</code></li>
<li><code>.html</code></li>
<li><code>.jsp</code></li>
<li><code>.aspx</code></li>
<li><code>.svc</code></li>
<li><code>.js</code></li>
<li><code>.css</code></li>
<li><code>.svg</code></li>
<li><code>.png</code></li>
<li><code>.gif</code></li>
<li><code>.jpeg</code></li>
<li><code>.jpg</code></li>
<li><code>.ico</code></li>
<li><code>.axd</code></li>
</ul>
A file without an extension is also acceptable. This is required by the SunSystems reporting solution.</td>
</tr>
<tr>
<td>
<ul>
<li>Reconfiguring WEB application compression</li>
<li>Reconfiguring APP application compression</li>
</ul>
</td>
<td>Configures the IIS to provide GZip Compression for static content and dynamically generated content.<br>Ensures compression is specified as disabled for the appropriate SunSystems applications.</td>
<td>Compression configurations used are:
<table>
<tr><th>Application</th><th>Static</th><th>Dynamic</th></tr>
<tr><td>sunsystems-login</td><td>ENABLED</td><td>DISABLED</td></tr>
<tr><td>ALL OTHERS</td><td>ENABLED</td><td>ENABLED</td></tr>
</table>
</td>
</tr>
<tr>
<td>
<ul>
<li>Reconfiguring WEB application authentication</li>
<li>Reconfiguring APP application authentication</li>
</ul>
</td>
<td>Enforces the usage of "Require SSL" for Forms Authentication.</td>
<td>This option is only set to true when IIS is responsible for the SSL configuration (encryption at NODE level).<br>See https://technet.microsoft.com/en-us/library/cc771633(v=ws.10).aspx for details.</td>
</tr>
</table>

# Configuration service setup

The specification of the SunSystems Configuration service is checked by the "Configuration Service" setup task, inline with the Deployment Topology. This is completed before any further DeployAgent tasks. After changes to configuration the Configuration Service is restarted. The service must be restarted before proceeding with the remaining DeployAgent tasks.

# Virtual Host Table configuration

This task is used to configure the Virtual Host table, or source tier routing table, that contains source tier-based content. The table is used by SunSystems applications to communicate.

The related sub-tasks are based on the node configuration defined in the Deployment Topology.

# SunSystems service configuration

The SunSystems service task is responsible for any SunSystems component configuration that is related to the Deployment Topology. Many of these options specify the security features that relate to the deployed nodes and encryption.

These configuration options are held in the SunSystems Configuration service, but are not configurable through Configuration Manager:

**Table 1:**

| Task Name(s) (as in DeployAgent UI) | Detailed description | Notes |
|---|---|---|
| Configuring SunSystems Connect Server properties | SunSystems Connect configuration related to embedded Tomcat Server.<br>This task configures some of the basic service properties such as port number, in addition to further security configurations. | https://tomcat.apache.org/tomcat-9.0-doc/config/http.html<br>This task automatically sets these Tomcat HTTP Connector properties:<br>• tomcat.http_connector.port<br>• tomcat.http_connector_scheme<br>• tomcat.http_connector.secure |
| Configuring SunSystems Report Manager service properties | Configures the specified port number for the SunSystems Report Manager service. | |

| Task Name(s) (as in DeployAgent UI) | Detailed description | Notes |
|---|---|---|
| Configuring SunSystems Application server properties | Configures the specified port number configurations for the SunSystems Application server. | |

# Finalising SunSystems deployment

This task encompasses all other items not included in the previous tasks. It is used to complete any configuration not held in the Configuration service. It is also used to apply any patch set level fixes that cannot be completed during the normal patch set process. This generally relates to environmental changes such as changes to IIS.

**Table 2:**

| Task Name(s) (as in DeployAgent UI) | Detailed description | Notes |
|---|---|---|
| Updating SunSystems Web service server.xml settings | Configures the specified port number for SunSystems Web service. | |

# Restarting SunSystems

This task is the same as that provided for the `RestartServices.exe`. This process stops all SunSystems services and SunSystems specific IIS components then restarts them in reverse order.

A restart of all services and IIS marks a node as unavailable. After the restart, ARR detects if the system has returned to service within 30 seconds. The entry points stop returning `HTTP 502.4` errors and instead return the `HTTP 200` status.

# Appendix O: Database Health Check

Check and remove

You can use the Database Health Check to check settings, performance, maintenance and housekeeping of the SunSystems databases and the instances that they reside on.

The log file `DatabaseHealthCheck.log` is generated in the `ProgramData\Infor\SunSystems\Logs\Install` folder.

**Note:** The generated log contains thorough and detailed information. It is expected to contain many rows.

| Name | Description | Type |
|---|---|---|
| Server Name | Server name | Information |
| Server Instance Name | Server instance name | Information |
| Instance | SQL Server instance name | Information |
| Edition | SQL Server edition | Information |
| Product version | SQL Server product version number | Information |
| Version name | SQL Server product version name | Information |
| Full version name | SQL Server full version name | Information |
| Security - sysadmins | Which logins have sysadmin rights and can do whatever they want on SQL server | Information |
| Security - CONTROL SERVER | These logins can do what they want on SQL Server | Information |
| Number of databases on this instance | Shows how many databases are in this instance of SQL server. Useful to see the potential load on this instance | Information |

| Name | Description | Type |
|---|---|---|
| Default database configurations changed | Details any database configuration default that have been changed. Allow a focus on which default settings have been changed | Review |
| Parallelism settings | Reports current settings –Suggested settings for SunSystems is Max degree of parallelism = 2 and cost threshold for parallelism of 30. These are suggested settings and should be tested. | Review |
| SQL Server service account | SQL Server service account must not have the 'lock pages in memory' privilege on servers that host other mission-critical applications | Review |
| SQL Server Maximum Memory | SQL server should leave sufficient memory for OS - Calculate max. memory for SQL Server like this:<br>Total memory:<br>• 1 GB for OS<br>• 4 GB for OS the first 16 GB memory<br>• 1 GB for OS for every additional 8 GB memory. | Review |

| Name | Description | Type |
|---|---|---|
| Optimize for ad hoc workloads | This is used to improve the efficiency of the plan cache for workloads that contain many single use ad hoc batches.<br>When this option is set to 1, the Database Engine stores a small compiled plan stub in the plan cache when a batch is compiled for the first time, instead of the full compiled plan.<br>This helps to relieve memory pressure by not allowing the plan cache to become filled with compiled plans that are not reused.<br>To find the number of single-use cached plans, run the following query: -<br>`SELECT objtype, cacheobjtype, AVG(usecounts) AS Avg_UseCount,SUM(refcounts) AS AllRefObjects, SUM(CAST(size_in_bytes ASbigint))/1024/1024 AS Size_MBFROM sys.dm_exec_cached_plans`<br>`WHERE objtype = 'Adhoc' AND usecounts = 1`<br>`GROUP BY objtype, cacheobjtype;` | Review |
| Free space on disk | Details any disks where databases are located if the available free space is < 30%. If the figure is less than 30% it is suggested that you review the amount of free space to ensure that there is sufficient. | Review |

| Name | Description | Type |
|---|---|---|
| Check database files | This check the files in tempdb, master, msdb and model. Checks files, growth settings and location.<br>Tempdb should always have more than on data file and not more than the number of CPU cores. All tempdb datafiles should be the same size and grow by the same amount. | Review |
| Performance | This is to check the general performance of the disks – we would expect the total time to be less than 2 minutes.<br>This is running the Performance script that has been supplied by Infor. This is generally checking the read and write speeds. | Review |
| Long running queries | List the top 50 long running queries by average time. The details can be used to give an idea of heavily used tables and an idea of the function. Potentially index changes may assist. | Review |
| Long Running Queries by I/O | List the top 50 long running queries by I/O. The details can be used to give an idea of heavily used tables and an idea of the function. Potentially index changes may assist. | Review |
| Always On Enabled | Details whether AlwaysOn is enabled or not and if enabled details of Availability groups, Listener Name and Availability Replicas are provided. | Information |
| Linked Server Configuration | Provides details of Linked Servers if they have been configured - mainly used when a BU Group is on a server different to the server on which the Domain resides | Information |

The next section circulates through the SunSystems databases. These are identified by having the table SQL_OBJ_REGISTRY present in a database.

| Name | Description | Type / Importance |
|---|---|---|
| Database Size | Total database size all data and log files | Information |
| Database Files | Lists all files for this database and their sizes | Information |
| Database Files Growth | Check all files have same file growth settings | Review |
| Database Owner | Lists the owner of each SunSystems database | Information |
| Collation Check | Best practice is the collation of the database to match the collation of the instance | Information |
| SunSystems version | Details the version of each of the SunSystems databases e.g. 6.03.00.1519 | Information |
| SunSystems Patch Set version | Details of the patch-set of each of the SunSystems databases e.g. S6 - PS - 01 | Information |
| Data Audit Rows | Number of rows in the SSDA_STORE table | Information |
| Data Audit Setup | Number of rows in the SSDA_DDR table where `AUDIT_ACTIVATED = 1` | Information |
| Database Recovery Model | Details the recovery model option, `FULL`, `BULK` or `SIMPLE` | Information |
| Page Verification | Page Verification Not Optimal for Database, SQL Server may have a harder time recognizing and recovering from storage corruption. Consider using `CHECKSUM` instead. `CHECKSUM` is the recommended setting | Action |
| Database compatibility level | The database compatibility level must the highest supported by the server product version. Indicates that this is not the case and should be changed | Action |

| Name | Description | Type / Importance |
|---|---|---|
| Database backups | Check backups are being done. Checks the date and time of the last backup and reports is one hasn't been done in the last 7 days | Action |
| Service Broker Enabled | Checks that the Service Broker is enabled for the Domain, Security and Landlord databases to enable SQL Query Notifications when changes are made in the database | Action |
| Database file growth | Percent grown is not best practice, fixed growth is better. Action if percent Review for fixed to ensure growth size is big enough so growth doesn't happen too often | Action / Review |
| DBCC CHECKDB last good run | This should be run on a weekly basis if not more frequently. Checks the date and time of the last `CHECKDB` and reports is one hasn't been done in the last 7 days | Action |
| Database option AUTO_CLOSE | Must always be set to `OFF`, must be amended if set `ON` | Action |
| Database option AUTO_CREATE_STATISTICS | Must always be set to `ON`, must be amended if set `OFF` | Action |
| Database option AUTO_SHRINK | Must always be set to `OFF`, must be amended if set `ON` | Action |
| Index fragmentation | Tells how many indexes have more than 100 pages and are more than 25% fragmented. Check your maintenance plans to ensure that a frequent process is run to keep the indexes defragmented. | Action |

| Name | Description | Type / Importance |
|---|---|---|
| Statistics review | Statistics that have more than 20,000 rows and less than 30% sampling. Check the statics and maybe rebuild them at a convenient time to ensure best performance. Tables with a large number of rows need a smaller sampling size | Action |
| SSP_DROP_WORK_TABLES | Date last run – should be run at least once a month. This procedure is a SunSystems one to keep the number of work tables to a minimum to improve performance | Action |
| SSP_DOMN_DROP_WORK_TABLES | Date last run – should be run at least once a month. This procedure is a SunSystems one to keep the number of work tables to a minimum | Action |
| SSP_HOUSEKEEPING | Date last run – should be run at least once a month This procedure is a SunSystems one to keep the number of rows in some interface tables to a minimum to improve performance | Action |
| Trusted Constraints - Foreign Keys | Identifies how many foreign keys that aren't currently set to trusted. Trusted constraints perform quicker than non-trusted ones. Can be enabled as an action in SunSystems function BUA | Action |
| Trusted Constraints - Check Constraints | Identifies how many check constraints that aren't currently set to trusted. Trusted constraintsperform quicker than non-trusted ones. Can be enabled as an action in SunSystems function BUA | Action |
| Database users | List all users that have access to the database with the type of user | Review |

| Name | Description | Type / Importance |
|---|---|---|
| Recovery Mode full NO log backups | Details all SunSystems databases where the recovery mode is set to **`Full`** and no log backup have been done in the last 7 day | Action |
| Database Encrypted | Details whether transparent database encryption is enabled. If it is, you must ensure that certificate is backed up properly | Information |
| Database Change tracking | This is not a default setting, and it has some performance over-head. It tracks changes to rows in tables that have change tracking turned on | Action |
| Data Compression - table | Reports the number of tables where data compression is set | Information |
| Data Compression - index | Reports the number of indexes where data compression is set | Information |