Infor SunSystems Installation Guide

Version 6.2.1

Publication Information

Release: Infor SunSystems v6.2.1

Publication date: October 13, 2016

Document code: v621H

Contents

About this guide

This installation guide describes the process to install SunSystems 6.2.1, where no previous SunSystems installation exists, or the previous installation has been removed. It provides details of all mandatory pre-installation checks, the installation process itself, and post-installation tasks.

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 consultants should perform the installation process.

Related documents

You can find the documents in the product documentation section of the Infor Xtreme Support portal, as described in “Contacting Infor".

What’s New (New functions and features)

Infor SunSystems Architecture and Planning Guide

Infor SunSystems 6.2.1 Upgrade Guide

Infor Ming.le™ documentation on the Infor Xtreme Support portal

Contacting Infor

If you have questions about Infor products, go to the Infor Xtreme Support portal at www.infor.com/inforxtreme.

If we update this document after the product release, we will post the new version on this website. We recommend that you check this website periodically for updated documentation.

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

Part 1 Installing SunSystems

Chapter 1 SunSystems 6.2.1 installation

1

Introduction

If you are upgrading from SunSystems 5.4.1 or SunSystems 6.1.0, you must refer to the SunSystems Upgrade Guide.

If you already have an installation of SunSystems 6.2.1 and are updating it to the latest Patch Set, refer to the SunSystems 6.2.1 Patch Set Installation Note available with the Patch Set. The Installation Note contains important instructions for updating, which are not documented in this Installation Guide.

Installing SunSystems 6.2.1 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, and dedicated to Infor applications. If not, the performance may be affected detrimentally. In particular, the servers should not be:

- a primary or back-up domain controller, running Active Directory
- a mail server running Exchange, Lotus cc:Mail 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, Lotus Notes, Apache or similar, other than for SunSystems
- a Small Business Server.

Note: When 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 above 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 in SunSystems Report Manager.

Windows service packs

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

Chapter 2 Prerequisites for installing SunSystems in a standalone environment

2

Introduction

Ensure you have uninstalled any previous installation of SunSystems and SunSystems Reporting Services.

Prerequisites check list

Prior to running a standalone installation of SunSystems, complete the prerequisite check list below. Details for each prerequisite item follow the check list:

Prerequisites for standalone installations	✓
Windows 10, Windows 8, Windows 8.1, Windows 7, Windows Server 2012, Windows Server 2012 R2 or Windows Server 2008 R2 – Dual Core 3Ghz 6GB RAM minimum.	
SunSystemsServices and SunSystemsClients local Windows groups Create the local Windows user SunSystemsReporting. For the Express installation, you must use the default password **Infortemp01**	
Local Security Policy (run secpol.msc), Local Policies, User Rights Assignment, Log on as a service	
Add the SunSystemsReporting user to the SunSystemsServices group	
Microsoft .NET Framework 3.5.1 (in Turn Windows features on or off)	
Microsoft .NET Framework 4.5 Advanced Services. Include WCF Services: all components including HTTP Activation and Microsoft Message Queue (MSMQ). For Windows 2008 R2, you must download .NET Framework 4.5 installer. For Windows 10, use .NET 4.6 which is an in situ upgrade of .NET 4.5	
Internet Information Services 7+ (IIS). Select the components listed in 'Turn Windows Features on or off'.	
Microsoft Message Queue (MSMQ) Server (it is included in WCF Services in Windows 8.1)	

Prerequisites for standalone installations	✓
Microsoft SQL Server 2008 R2, 2012, 2014 or Microsoft SQL Server 2016 Database Server, Standard Edition or above Include features: Database Server, Reporting Services (Native), and Management Tools	
SQL Server Management Studio, Security, Logins, NT AUTHORITY\SYSTEM, Properties, Server Roles, add sysadmin role	
In SQL Server Configuration Manager, check that TCP/IP is an enabled protocol.	
SQL Server Reporting Services Configuration Manager, Service Account, Use another account, and add <localmachinename>\SunSystemsReporting and password **Infortemp01** and click apply.	
Microsoft System CLR Types	
Microsoft Report Viewer 2012	
Adobe Acrobat Reader 10+	
Internet Explorer 11, Edge, Mozilla Firefox, or Google Chrome IE 8,9 and 10 are supported by SunSystems, but are no longer receiving security updates from Microsoft	
Download the latest SunSystems 6.2.1 Patch Set from **www.inforxtreme.com**	
SunSystems serialization file	

Users and groups

Two Windows groups must be created: SunSystemsServices and SunSystemsClients. The SunSystemsServices Windows group is assigned db_owner rights to the SunSystems databases by the installer. The Windows credentials of SunSystems users are only added to the SunSystemsClients Windows group for functions that make a direct connection to the database i.e. Bill of Materials Management (BOMM). A SunSystemsReporting service account must also be created and added to the SunSystemsServices group.

Note: SunSystemsServices, SunSystemsClients and SunSystemsReporting are example names.

Create SunSystemsServices and SunSystemsClients groups, and the SunSystemsReporting user:

Log into your standalone computer as a user that is a member of the local Windows Administrator group.

Go to: Control Panel > Administrative Tools > Computer Management > Local Users and Groups > Groups.

Create the group SunSystemsServices.

Create the group SunSystemsClients.

Create the user SunSystemsReporting.

Add the password **Infortemp01** if you are intending to run the express installation. Avoid using a semi colon ; character in the password.

Select Password never expires.

Add the SunSystemsReporting user to the SunSystemsServices group.

Ensure the SunSystemsReporting user has the local security policy Log on as a service right:

a. Run **secpol.msc** to launch Local Security Policy.

b. Go to: Local Policies > User Rights Assignment.

c. Right-click Log on as a service, and select Properties.

d. Click: Add User or Group > Locations, and specify your local computer.

e. Click OK, and specify SunSystemsReporting in Enter the object names to select.

Turn Windows features on or off

IIS is required to host SecurityWebServer, SecurityConsole and TransferDeskWebServer. The following features must be added to the IIS installation.

Go to: Control Panel > Programs > Programs and Features > Turn Windows features on or off, and click '+' to expand the individual features:

- Features >.NET Framework 3.5 Features
  - .NET Framework 3.5 (includes .NET 2.0 and 3.0)
- Features > .NET Framework 4.5 Features
  - .NET Framework 4.5
  - ASP.NET 4.5
- Features > .NET Framework 4.5 Features > WCF Services:
  - HTTP Activation
  - Message Queuing (MSMQ) Activation
  - Named Pipe Activation
  - TCP Port Sharing
- Internet Information Services > Web Management Tools:
  - IIS Management Console
- Internet Information Services >World Wide Web Services > Application Development Features:
  - .NET Extensibility 3.5
  - .NET Extensibility 4.5
  - ASP .NET 3.5
  - ASP .NET 4.5
  - ISAPI Extensions

    - ISAPI Filters.
- Internet Information Services > World Wide Web Services > Common HTTP Features:
    - Default Document
    - Directory Browsing
    - HTTP Errors
    - HTTP Redirection
    - Static Content.
- Internet Information Services > World Wide Web Services > Health and Diagnostics:
    - Custom Logging
    - HTTP Logging
    - Logging Tools
    - Request Monitor
    - Tracing.
- Internet Information Services > World Wide Web Services > Performance:
    - Static Content Compression.
- Internet Information Services > World Wide Web Services > Security:
    - Basic Authentication
    - Digest Authentication
    - Request Filtering
    - Windows Authentication.
- Microsoft Message Queue (MSMQ) Server
    - Microsoft Message Queue (MSMQ) Server Core.

Microsoft SQL Server and Configuring Reporting Services

Install Microsoft SQL Server, and configure Reporting Services:

1. Install a default instance of Microsoft SQL Server and include:
    - Database Engine Services
    - Management Tools
    - Reporting Services - Native.
    - Reporting Services Configuration dialog - choose Install and Configure.
2. Following on from the SQL Server installation, run Reporting Services Configuration Manager, click the Web Service URL and the Report Manager URL to check they do not display errors in the browser.
3. Click the Database tab to ensure the ReportServer database has been created.
4. Go to: Reporting Services Configuration Manager > Service Account, and select Use another account.

5. Enter the user **<localmachine>\SunSystemsReporting** and the password **Infortemp01** to enable access for Reporting Services to the SunSystems Data databases.

Note: Ensure that a filename for a backup encryption key has been specified.

Microsoft SQL Server 2012, 2014 and 2016

Microsoft SQL Server 2012, 2014 and 2016 do not give the sysadmin role to NT AUTHORITY\SYSTEM (Local System). Therefore, you must add this role to the SYSTEM login in Microsoft SQL Server for a standalone SunSystems installation:

1. Launch Microsoft SQL Server Management Studio and connect to your server.
2. Go to: Security > Logins > NT Authority\SYSTEM > Properties > Server Roles.
3. Select sysadmin and click OK.

On a live installation, a named service account should be used for the SunSystems installation instead of local system. In this case you would not give sysadmin role to local system.

Microsoft System CLR Types

If you have not installed SQL Server 2012, this is required.

If you are using Microsoft SQL Server 2008 R2, SQL Server 2014, or SQL Server 2016:

If your Windows operating system is 32-bit, install CLR Types (x86):

http://go.microsoft.com/fwlink/?linkid=239644&clcid=0x409

If your Windows operating system is 64-bit, install CLR Types (x64):

http://go.microsoft.com/fwlink/?LinkID=239643&clcid=0x409

Microsoft Report Viewer 2012

Recommended even if you have SQL Server 2012 installed.

The Microsoft Report Viewer 2012 redistributable is available from:

http://www.microsoft.com/en-us/download/details.aspx?id=35747

Adobe Acrobat Reader 10+

Adobe Acrobat Reader 10+ is available from the Adobe website.

Compatible internet browsers

Internet Explorer 11 or Edge are available from the Microsoft website.

Note: Internet Explorer 8, 9 and 10 are supported by SunSystems but no longer receiving security updates from Microsoft.

Mozilla Firefox is available from the Mozilla website.

Google Chrome is available from the Google website.

Safari (OSX / IOS only) is only supported on mobile devices.

Chapter 3 Installing SunSystems in a standalone environment

3

Downloading SunSystems 6.2.1 ISO

Download the SunSystems 6.2.1 DVD ISO available from the Infor download centre:

https://infor.subscribenet.com

Run a Product Search for SunSystems 6.2.1 and download InforSunSystems62_1.iso.

Installing SunSystems

The standalone installation is a two-step process:

1. Install server and client components
   - **a** Run the Infor SunSystems installer
   - **b** Select: New Installation > Server & Client Components
   - **c** Select: Express

Caution: Do not apply SunSystems patch sets until SunSystems Reporting Services has been installed.

   - **d** Return to the Install Products menu.
   - **e** In Services, check that SunSystems Configuration Service is running. This is required for installing SunSystems Reporting Services (SRS).

Install Reporting Services

   - **f** Go to: Install Products menu
   - **g** Select Reporting Services
   - **h** Select Express installation.

Caution: It is possible to install SunSystems in a standalone environment using Local System as the service account. However, this is not a recommended configuration for normal deployments and should only be used to quickly test an installation, or for demonstration purposes. We recommend that a single tier should be configured using local or domain accounts for secure access.

As there are limitations as to how Local System can be added to groups, it is necessary to disable the checking of trusted group membership by specifying the special **UNPROTECTED** string, in place of a group name. This allows any process to act as if it were a trusted SunSystems service and exposes the possibility that a user with network access could change data using the identity and permissions of another user. For this reason, production systems must never be deployed this way.

Installing SunSystems Web Help

By default, SunSystems Web Help is not included as part of the Express installation. You must install the web help in order to have online help for the SunSystems applications that are web-based, including Report Manager, Data Access Manager, Transfer Desk Web and Security Console.

If you wish to include SunSystems Web Help as part of an Express installation, then from the installation DVD, edit **Application\SQLExpress.xml**:

Change **<SunSystemsWeb><Option Enable="Y" Help="N" />**

to **<SunSystemsWeb><Option Enable="Y" Help="Y" />**

Manually installing SunSystems Web Help

If you did not include SunSystems Web Help in the Express installation, you may subsequently install the web help by going to the **Application/Packages/SunSystemsWebHelp** folder on the installation DVD, and running **SunSystemsWebHelp.msi**. After completion, you must restart the SunSystems Web service.

Note: The SunSystems Web Help is a sizeable component, and may take significant time to install.

Post-installation steps

SunSystems patch sets

SunSystems patch sets are available from http://www.inforxtreme.com. Here is the specific link for SunSystems 6.2.1 Patch Sets: https://www.inforxtreme.com/espublic/EN/AnswerLinkDotNet/solutions/ViewSolution.aspx?SolutionID=1489656

1. Download the latest patch set available for SunSystems 6.2.1.
2. Read the instructions in the patch set installation note, included in the zip file.
3. Install the latest patch set.
4. Check which patch sets have been installed successfully. Go to: Control Panel > Programs > Programs and Features > View Installed Updates.

5. Restart the SunSystems services, or shut down and restart your computer.

Serialization

To serialize SunSystems, go to Windows File Explorer and run your serialization file.

Add SunSystems Reporting Service Group membership to SunSystems users

Only SunSystems Reporting Service Administrators require SRS group membership. Normal SunSystems users do not require this membership to run ordinary reports:

1. Sign in to User Manager as admin.
2. Select the Groups tab and edit group PK1. Select Function Permissions, then click Select All twice and click Apply.
3. Select Action Permissions. Add PK1 and click Apply.
4. Select the Users tab. Right-click a user that requires SRS group membership (for example, PK1) and select Edit User.
5. Click Change (next to Group Membership). Expand SunSystems Reporting Users and select the SunSystems Reporting functions required for this user.
6. Click OK to submit the amended group membership.

Note: Make a note of which users have been given the SunSystems Data Access Managers role and the Report Manager role, because these roles are required later.

Configuring SunSystems Data Models in Data Access Manager

You must use Data Access Manager to configure data models prior to using any reporting functions:

1. Log into SunSystems as user ZZZ and click OK to create a menu.
2. Select the function Data Access Manager (DAR).
3. From the task tree, select SunSystems > Configure Business Units and click Run.
4. In Configure Business Units, select the PK1 business unit and click OK. Wait until the configuration completes.

Click Save before exiting Data Access Manager.

Windows 10

Chinese language users may experience corrupt Chinese characters when exporting a report to pdf. To resolve this issue for Chinese Traditional:

1. Go to **Start** > **Search programs and files**, and search for **Manage Optional Features**.
2. Select **Add a feature**.
3. Select **Chinese (Traditional) Supplemental Fonts** and any other relevant fonts.

4. Click **Install**.

You may need to add other fonts depending on the target language.

Uninstalling SunSystems on Windows 10

To uninstall SunSystems:

1. Go to **Control Panel** > **Programs and Features**, or **Uninstall a Program**.
2. Select for SunSystems 6.2.1
3. Click **Uninstall**.

Note: Do not use **Applications and Features** to uninstall SunSystems because linked applications like SunSystems Help will rollback the uninstallation of SunSystems.

Chapter 4 Prerequisites for installing SunSystems in a multi-tier environment

4

Introduction

Ensure you have uninstalled any previous installation of SunSystems and SunSystems Reporting Services.

Hardware and Software Requirements

Database Server

Operating Systems	SQL Server versions required	Entry level recommendation
Windows 2008 R2 Standard edition or above	SQL Server 2008 R2 SQL Server 2012 SQL Server 2014 SQL Server 2016	Dual Core 3Ghz 6GB RAM
Windows 2012 (inc R2) Standard edition or above	SQL Server 2008 R2 SQL Server 2012 SQL Server 2014 SQL Server 2016	Dual Core 3Ghz 6GB RAM

SunSystems Application Server

Operating Systems	Entry level recommendation
Windows 2008 R2 Standard edition or above	Dual Core 3Ghz 4GB RAM
Windows 2012 (inc R2) Standard edition or above	Dual Core 3Ghz 4GB RAM

SunSystems Report Server

Operating Systems	Entry level recommendation
Windows 2008 R2 Standard edition or above	Dual Core 3Ghz 4GB RAM
Windows 2012 (inc R2) Standard edition or above	Dual Core 3Ghz 4GB RAM

SunSystems Report Manager

Operating Systems	Entry level recommendation
Windows 2008 R2 Standard edition or above	Dual Core 3Ghz 4GB RAM
Windows 2012 (inc R2) Standard edition or above	Dual Core 3Ghz 4GB RAM

SunSystems Web Server

Operating Systems	Entry level recommendation	Other
Windows 2008 R2 Standard edition or above	Dual Core 3Ghz 4GB RAM	IIS 7 or above
Windows 2012 (inc R2) Standard edition or above	Dual Core 3Ghz 4GB RAM	IIS 7 or above

SunSystems Security Server

Operating Systems	SQL Server versions required	Entry level recommendation
Windows 2008 R2 Standard edition or above	SQL Server 2008 R2 SQL Server 2012 SQL Server 2014 SQL Server 2016	Dual Core 3Ghz 3GB RAM

Operating Systems	SQL Server versions required	Entry level recommendation
Windows 2012 (inc R2) Standard edition or above	SQL Server 2008 R2 SQL Server 2012 SQL Server 2014 SQL Server 2016	Dual Core 3Ghz 3GB RAM

Prerequisites check list

Prior to running a multi-tier installation of SunSystems, complete the prerequisite check list below. Details for each prerequisite item follow the check list:

Prerequisite	Components	✓
SharePoint Installation	Hosting Infor Ming.le™ and SunSystems plug-in. Must not be on the same server as SunSystems.	
Database server	SunSystemsServices and SunSystemsClient global Windows groups	
SunSystems Security server	.NET Framework 3.5.1. Features .NET Framework 4.5 .NET Framework 4.6	
SunSystems Security server	Internet Information Services (IIS) 7 or above	
SunSystems Application server	.NET Framework 3.5.1 Features.NET Framework 4.5 Features including WCF Services (all components including HTTP Activation)	
SunSystems Application server	Internet Information Services (IIS) 7 or above – if Security Server is to be installed	
SunSystems Application server	Microsoft SQL Server Command Line Utilities SqlCmdLnUtils.msi (bcp is required for SunSystems patch sets)	
Microsoft SQL Server Reporting Services server	Windows Server 2012 or Windows 2008 R2	
Microsoft SQL Server Reporting Services server	.NET Framework 3.5.1 Features .NET Framework 4.5 Features including WCF Services (all components including HTTP Activation)	

Prerequisite	Components	✓
Microsoft SQL Server Reporting Services server	Microsoft SQL Server 2008 R2, Microsoft SQL Server 2012, Microsoft SQL Server 2014, or Microsoft SQL Server 2016 Database Server, and Reporting Services. Standard Edition or above. Choose Install and Configure during installation process.	
SRS Report Server	.NET Framework 3.5.1 Features .NET Framework 4.5 Features including WCF Services (all components including HTTP Activation) .NET Framework 4.6	
SRS Report Server	Microsoft System CLR Types if you are using Microsoft SQL Server 2008 R2, 2014 or 2016	
SRS Report Server	SunSystemsReporting Windows domain user	
SRS Report Server	Internet Information Services (IIS) 7 or above	
SRS Report Server	Microsoft Message Queue (MSMQ)	
SRS Report Server	Microsoft Report Viewer 2012	
SRS Report Manager	.NET Framework 3.5.1 Features .NET Framework 4.5 Features including WCF Services (all components including HTTP Activation) .NET Framework 4.6	
SRS Report Manager	Microsoft System CLR Types if you are using SQL Server 2008 R2	
SRS Report Manager	SunSystemsReporting Windows domain user	
SRS Report Manager	Internet Information Services (IIS) 7 or above	
SRS Report Manager	Microsoft Message Queue (MSMQ)	
SRS Report Manager	Microsoft Report Viewer 2012	
SunSystems Web server	.NET Framework 3.5.1 Features .NET Framework 4.5 Features including WCF Services (all components including HTTP Activation) .NET Framework 4.6	
SunSystems Web server	Internet Information Services (IIS) 7 or above	
Client computers	.NET Framework 3.5.1. Features	
Client computers	Adobe Acrobat Reader 10+	
Web clients	Internet Explorer (11, 10, 9 or 8), Edge, Mozilla Firefox, Google Chrome or Safari (OSX/IOS only)	

Windows 64-bit operating system

When installing SunSystems on a 64-bit operating system, you must ensure that ASP.NET has been correctly registered, otherwise the installation will fail:

1. Run a command prompt as Administrator.
2. Change the directory to **Windows\Microsoft.NET\Framework64\v2.0.50727**
3. Check if ASP.NET is already registered, by entering the command **aspnet_regiis –lv**

If not already registered, you must register it by entering **aspnet_regiis–ir**

Infor Ming.le™ with SunSystems plug-in and Infor ION

SunSystems must not be installed on the same server as ION or Infor Ming.le™.

Installation documentation for Infor Ming.le™ and ION can be found on InforXtreme:
http://www.inforxtreme.com

Port usage

Port function	Default number/range	Affinity
SSC web services and application Transfer Desk Web services	8080	Required [1]
SunSystemsWeb	80	[3]
Security Console and Authentication web applications	81	Required [1]
SunSystemsWeb	9080	[3]
Transfer Desk Web application	9090	Required [1]
SunSystems Report Manager Service	9000	Required [4]
Reporting applications (RMA, DAR)	94	Required [1]
Configuration Service	40003-40004	None
ASP.NET state server	42424	None

Port function	Default number/range	Affinity
Session Control	50000	None
RMI Registry	50001	Required
Locator Service	50005-50006	Required
Transfer Execution	50008	Required
Secure Job Execution	55001	Required
Transaction Monitor RMI	50050-50099	None
Security APIs	55000	None
Session Interfaces	40100-40999	None [2]

Note:

1. Where Affinity is required, this refers to Client affinity in a hardware load balanced environment
2. Session interfaces must either connect directly to the physical machine (bypassing the load balancer) or separate port ranges must be defined for each physical machine and the balancer configured to route to the correct one.
3. SunSystems Web should only be load balanced through IIS. See Web Server Scalability.
4. You cannot combine load balancing of SunSystems Report Manager Service and https SRS Report Server.

Users and Groups

In a multi-tier environment, the user running the installation must logon to the appropriate server with a Windows domain account that has been added to the local Windows administrator group:

1. Go to Active Directory > Users and Computers.
2. Create the global groups SunSystemsServices and SunSystemsClients.
3. Create the global user account SunSystemsReporting.
4. Create one or more accounts to run the SunSystems services.
5. In Active Directory, add these accounts to the global SunSystemsServices group.

Ensure the SunSystemsReporting user has the local security policy Log on as a service right:

a. Run **secpol.msc** to launch Local Security Policy.

b. Go to: Local Policies > User Rights Assignment.

c Right-click Log on as a service, and select Properties.

d Click: Add User or Group > Locations, and specify your local computer.

e Click OK, and specify SunSystemsReporting in Enter the object names to select.

Alternatively, global service accounts can be used with local windows groups.

Note: SunSystemsServices, SunSystemsClients and SunSystemsReporting are example names.

Repeat step 6 for each Example User Name in the following Services table:

Service	Example User Name	Service Required for Access to
SunSystems Security Server	**<dom>\svc-sssec**	Security database; Domain database
IIS AppPool Security WebService	**<dom>\svc-sssecweb**	Modify permissions for **Program Files (x86)\Infor\SunSystems\SecurityWeb** Read permissions for **Windows\System32\inetsrv\config**
SunSystems Service Account (SunSystems Session Manager service)	**<dom>\svc-sssessionman**	Domain database; SunSystems databases via Windows Authentication
SunSystems Connect	**<dom>\svc-ssconnect**	
SunSystems Web Service	**<dom>\svc-ssweb**	
SRS Reporting Print Service	**<dom>\svc-srsprint**	
SRS Report Server AppPool	**<dom>\svc-srsapppool**	Domain database; SunSystems database and ReportServer databases
SRS Report Manager AppPool	**<dom>\svc-srsapppool**	
SQL Server Reporting	**<dom>\SunSystemsReporting**	Domain database, SunSystems databases and ReportServer databases
SQL Server Database instance	**<dom>\svc-ssdatabase**	

The SunSystemsServices group must be added to SQL Server security with public role.

Manually add the SunSystems service accounts and the SunSystemsReporting user to the SunystemsServices domain group in Active Directory Users and Computers.

Note: The SunSystemsReporting user must always be a domain account, except when created as part of a standalone installation.

Caution: Before initiating the installation on any tier with a SunSystems Windows service, you must ensure that the domain service account has local security policy log on as a service rights in Local Policies > User Rights Assignment.

Folder Permissions

On the SunSystems Application server:

- All service accounts have Full control permission on folder **ProgramData\Infor**
- All service accounts have Read & Execute permission on folder **Program Files (x86)\Infor**

  The SunSystems Connect service account (for example, svc-ssconnect) has Modify permission on folder **ProgramData\Infor\SunSystems_data\SSSystem.dat** during SunSystems serialization.

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. SunSystems uses the Windows API to authenticate users across domains. So if Windows cannot authenticate users on the other domain, SunSystems will not be able to do this either.

Security Improvements

GetCredentials

SunSystems now includes an improvement to security to protect the GetCredentials command. The consequence will be that the following services and application pools will need to be run by a trusted user:

Application Pools

- SecurityConsole
- SunSystemsReportingServices

Services

- SunSystemsConnectServer
- Microsoft SQL Server Reporting Services (SSRS)

These services and application pools can be run as a user which is defined as a member of the SunSystemsServices group. This is a permanent change to the requirements for configuring SunSystems.

Password Hash

SunSystems passwords will need to be reset when customers upgrade from any earlier version. (The fix will also affect migrations from version 4).

Service account password expiry

When you are using domain service accounts and the password needs to be updated, this must be done for all SunSystems Windows Services. On each server select Control Panel, Administrative Tools, View Local Services, select each SunSystems service, Properties, Log on, and enter the new password. You will need to restart the service.

Application Pools also need to be updated. In IIS, Application Pools, SecurityWebServer, right-click Advanced Settings, Identity, Custom Account, Set. Repeat for SecurityConsole, TransferDeskWebServer, and SunSystemsReportingServices. You will need to restart IIS.

In Reporting Services Configuration Manager update Service Account with the new password.

Microsoft Internet Information Services (IIS)

IIS is required to host SecurityWebServer, SecurityConsole and TransferDeskWebServer. The following features must be added to the IIS installation.

Go to: Control Panel > Programs > Programs and Features > Turn Windows features on or off, and click '+' to expand the individual features:

Add Roles and Features for Windows Server 2012

Go to: Server Manager > Dashboard > Add Roles and Features. Ensure the following features are selected:

- Features > .NET Framework 3.5 Features
  - .NET Framework 3.5 (includes .NET 2.0 and 3.0)
- Features > .NET Framework 4.5 Features
  - .NET Framework 4.5
  - ASP.NET 4.5
- Features > .NET Framework 4.5 Features > WCF Services:
  - HTTP Activation
  - Message Queuing (MSMQ) Activation
  - Named Pipe Activation
  - TCP Port Sharing
- Features > Message Queuing
  - Message Queuing Services
- Server Roles > Web Server (IIS) > Web Server > Common HTTP Features
  - Default Document
  - Directory Browsing
  - HTTP Errors

    - Static Content
    - HTTP Redirection
- Server Roles > Web Server (IIS) > Web Server > Health and Diagnostics
    - HTTP Logging
    - Custom Logging
    - Logging Tools
    - Request Monitor
    - Tracing
- Server Roles > Web Server (IIS) > Web Server > Performance
    - Static Content Compression
- Server Roles > Web Server (IIS) > Web Server > Security
    - Request Filtering
    - Basic Authentication
    - Digest Authentication
    - Windows Authentication
- Server Roles > Web Server (IIS) > Web Server > Application Development
    - .NET Extensibility 3.5
    - .NET Extensibility 4.5
    - ASP.NET 3.5
    - ASP.NET 4.5
    - ISAPI Extensions
    - ISAPI Filters
- Server Roles > Web Server (IIS) > Management Tools
    - IIS Management Console

Note: During this process you must specify an alternative path to the installation, as the features are not installed as part of the Windows Server 2012 installation or upgrade. After mounting the Windows Server 2012 installation media, specify the alternative path as **d:\sources\SxS** where **d:** is the mounted drive.

Add Roles and Features for Windows Server 2008 / 2008 R2

Go to: Server Manager > Add Role > Web Server (IIS). Check the following Role Services are added to the IIS install:

- Features > .NET Framework 3.5 Features
    - .NET Framework 3.5.1 (includes .NET 2.0 and 3.0)
- .NET Framework 4.5: You have to download .NET Framework 4.5 from Microsoft and install. When installed, it will appear in Programs and Features. You do not have to activate the individual components within .NET 4.5.
- Common HTTP Features
    - Static Content

    - Default Document
    - Directory Browsing
    - HTTP Errors
    - HTTP Redirection
- Application Development
    - ASP.NET
    - .NET Extensibility
    - ISAPI Extensions
    - ISAPI Filters
- Health and Diagnostics
    - HTTP Logging
    - Logging Tools
    - Request Monitor
    - Tracing
    - Custom Logging
- Security
    - Basic Authentication
    - Windows Authentication
    - Digest Authentication
    - Request Filtering
- Performance
    - Static Content Compression
- Management Tools
    - IIS Management Console
    - IIS 6 Management Compatibility
        - IIS 6 Management Console
        - IIS 6 Metabase Compatibility
        - IIS 6 WMI Compatibility
        - IIS 6 Scripting Tools

Microsoft Message Queue (MSMQ)

Ensure that MSMQ has been installed.

In Windows Server 2008 R2, go to: Server Manager > Features > Add Features and select Message Queuing Server.

In Windows 7, go to: Control Panel > Programs and Features > Turn Windows features on or off > Microsoft Message Queue (MSMQ) Server > Microsoft Message Queue (MSMQ) Server Core.

Note: For Windows Server 2012, MSMQ is part of the IIS installation. See the section Add Roles and Features > On Windows Server 2012, in this guide.

Installing Microsoft SQL Server

SunSystems 6.2.1 is compliant with Microsoft SQL Server 2008 R2, Microsoft SQL Server 2012, Microsoft SQL Server 2014, or Microsoft SQL Server 2016 Database Server, and Reporting Services.

Caution: SunSystems 6.2 data is stored in Unicode. When planning your installation, be aware that the SunSystems data will require up to double the disk space compared with previous SunSystems versions.

Microsoft SQL Server 2012 does not support the restoring of database backups made on versions of SQL Server prior to SQL Server 2005. To do this, you must take the intermediate step of restoring to SQL Server 2005/2008, before SQL Server 2012.

Microsoft SQL Server can be installed with mixed mode, or Windows authentication. SunSystems always uses Windows authentication when connecting to the database.

ION requires mixed mode and SQL Server on port 1433.

If a SQL Server named instance is used, the SQL Server Browser Service must be started as it is required to make a connection to the server. If using a default SQL Server instance you must use the default port 1433, as the browser service cannot be used to connect to a default instance.

Note: The SQL Server Aliases feature is not supported with this SunSystems release.

If installing a named instance, the 'data access' option is disabled by default. In this case it is important to enable the data access option by executing the following SQL query:

USE master;

EXEC sp_serveroption ‘<server-name>\<instancename>’, 'data access', ‘true';

Note: If you are manually creating your own SunSystems Data database (Business Unit Group), note that Binary Sort Order is mandatory.

If you are installing a fresh installation of Microsoft SQL Server, you must install Database Engine Services and Management Tools as a minimum. You must install and configure Reporting Services – Native on the server to be the SQL Server Reporting Services (SSRS) server.

If you are installing Microsoft SQL Server 2016, you must install Database Engine Services, Management Tools, Reporting Services – Native and Reporting Services Configuration dialog - choose Install and Configure.

If Microsoft SQL Server is already installed, select Microsoft SQL Server > Configuration Tools > SQL Server Installation Center, and add to your existing instance of Reporting Services.

In SQL Server Configuration Manager, go to: SQL Server Network Configuration > Protocols for MSSQLSERVER and ensure that TCP/IP is enabled. Check that TCP/IP is also enabled for SQL Native Client 10.0 Configuration > Client Protocols.

Click the Web Service URL and the Report Manager URL to check they do not display errors in the browser.

Click the Database tab to ensure the ReportServer database has been created.

Go to Reporting Services Confiiguration Manager > Service Account, and select User another account. Enter the domain account and password for the SunSystemsReporting user to enable access for Reporting Services to the SunSystems Data database.

Microsoft SQL Server 2012, 2014 and 2016 and the sysadmin role

For security reasons, Microsoft SQL Server 2012, Microsoft SQL Server 2014 and Microsoft SQL Server 2016 do not give sysadmin role to NT AUTHORITY\SYSTEM (Local System). You must create a Windows service account and use this account to run your SunSystems services. Make sure the account has the security policy Log on as a service right in Local Security Policy > Local Policies > User Rights Assignment.

Reporting prerequisites

SunSystems Configuration Service

This service is new for SunSystems 6.2. It stores some configuration settings for SRS. The service is installed at the same time as the SunSystems application server. Check that this service is running before attempting to install SRS.

The SRS installer finds the server location by querying the DOMN_VRTL_HOST table.

The Configuration service is deployed on the SunSystems application server as a windows service. Its function is to store properties (typically configuration settings) used by SunSystems in the database and to expose a set of APIs to allow SunSystems components to access these in a consistent and secure way.

Currently not all configuration is held this way, with only SunSystems reporting making extensive use of this service. However, over time, additional SunSystems components will use the service to persist configuration changes making management and control simpler for an administrator.

ConfigEditor.exe enables configuration settings held in the database to be hanged. ConfigEditor.exe can be run from the SunSystems program directory. SunSystems credentials will be required to launch ConfigEditor.exe. Give your SunSystems user, membership of the Configuration Administrators group. You do this in User Manager, Users, Group Membership, and Change.

Installing Microsoft SQL Server Reporting Services

If you already have SQL Server installed and need to add Reporting Services, run the SQL Server installer and go to: SQL Server Feature Installation > Instance Features. Select Reporting Services (Native) and click Next to proceed with install and configure Reporting Services.

On completion of the installation of SQL Server Reporting Services, further steps are required to be completed in Microsoft SQL Server Reporting Services. The details are below.

Microsoft Report Viewer 2012

Recommended even if you already have SQL Server 2012 installed.

Microsoft Report Viewer 2012 is a prerequisite for the installation of SunSystems Reporting. The redistributable must be installed on the machine hosting the SunSystems Report Manager. A warning message is displayed if this has not been installed.

As a prerequisite to installing Microsoft Report Viewer 2012, some classes from Microsoft CLR Types for Microsoft SQL Server 2012 are required:

- CLR Types (x86): **http://go.microsoft.com/fwlink/?linkid=239643&clcid=0x409**
- CLR Types (x64): **http://go.microsoft.com/fwlink/?linkid=239644&clcid=0x409**

The Microsoft Report Viewer 2012 redistributable can be downloaded from:

http://www.microsoft.com/en-us/download/details.aspx?id=35747

A set of language packs is also available from the Microsoft website. See the section Setting up SunSystems Report Viewer with Different Languages.

If the SunSystems Report Manager Web application has already been installed, then it must be restarted after installing ReportViewer 2012. If you install ReportViewer 2012 before installing Reporting, then no restart is required.

Configuring Microsoft SQL Server Reporting Services using Reporting Services Configuration Manager

Ensure the SunSystemsReporting Windows user (local or domain) is given appropriate permissions to the ReportServer and ReportServerTempDB databases.

Ensure you are logged on as a user with the sysadmin role for the database server to enable these permissions to be set.

1. Run SQL Server Reporting Services Configuration Manager.
2. Enter the Server Name and Report Server Instance and click Connect.
3. Select Service Account. For the Report Server Service Account, select Use another account.
4. Enter account details and password for the SunSystems Reporting Services Windows user, for example, SunSystemsReporting. Click Apply. You may be required to enter a backup encryption key filename and password, so make a note of this filename and location.
5. The SQL Server Connection dialog box is displayed. For Credentials Type, select Current User – Integration Security (ensure you have sysadmin role or db_owner access to the ReportServer and ReportServerTempDB databases). Click OK. Alternatively, the SQL Server sa account may be used.
6. Check the Results panel does not contain any errors. If Apply is disabled, click Enter.

In the Database tab, ensure the ReportServer database has been created.

Memory allocation for SSRS

Where SQL Server databases and SQL Server Reporting Services (SSRS) are on the same machine, you are advised to set the maximum and minimum meory allocation for SSRS. Edit the RSReportServer.config file, typically found at

\Program Files\Microsoft SQL Server\MSRS11.MSSQLSERVER\Reporting Services\ReportServer

and add the following configuration settings:

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

The WorkingSetMaximum should be appropriate for SSRS depending on hardware RAM available, leaving enough RAM remaining for the operating system and SQL Server database server. You must ensure that SQL Server is never starved of memory; the minimum amount for SQL Server should be at least 1GB. The WorkingSetMinimum for SSRS should also be set appropriately.

Checklist for Reporting	✓
Microsoft SQL Server ReportServer and ReportServerTempDB databases have been created	
In Reporting Services Configuration Manager, check Report Manager URL link is working	
In Reporting Services Configuration Manager, check Web Manager URL link is working	
SunSystems Configuration Service must be running on SunSystems application server.	

Adobe Acrobat Reader 10+

This is available from the Adobe website.

Windows Identity Foundation

There is now an option in SunSystems Security User Manager to authenticate using Infor Federation Services (IFS). If this option is required, then you must install Windows Identity Foundation. Download the x86 or x64 runtime package appropriate for the Server, where SunSystems Security Web application is running in IIS:

- For Windows 7 and Windows Server 2008 R2, select the msu file with name starting Windows6.1.

http://www.microsoft.com/downloads/en/details.aspx?FamilyID=eb9c345f-e830-40b8-a5fe-ae7a864c4d76

SunSystems installer features

The SunSystems installer is based on Microsoft Installer (MSI) technology, which supports multiple installation options. The following options are supported with SunSystems installer:

- **Silent Installation**

  The SunSystems installer supports express installation, which runs as silent installation. All required parameters are saved in a parameter file created by the installer, and are not used during the installation. For example, at a command prompt, enter: **setup /v“ /qn”**. This uses SQLExpress.xml for parameters. See SQLTemplate.xml for an explanation of parameters.

- **Administrative Installation**

  Using this feature, SunSystems installation files can be ‘unzipped‘ to a shared location. All the installation parameters that are given during the administrative install will be used as defaults for subsequent installations on client computers. During this unzip process, a new MSI installer file will be generated, which should be passed to client computers for further installation. The newly created MSI will take all the defaults from the network location, and software will be installed on demand.

  When creating the install point for the SunSystems installation files, you must ensure you also copy the “Packages” and “SqlServerDatabaseUtilities” folders from the original media to the correct location. The SqlServerDatabaseUtilities folder must be at the same level as the root of the install point, and the Packages folder must be at the same level as the SunSystems ClientApp MSI.msi file.

  <sharename>

  <sharename>\SqlServerDatabaseUtilities

  <sharename>\<SunSystems application>\SunSystems ClientApp MSI.msi

  <sharename>\<SunSystems application>\Packages

  If you wish to use the Express or Silent Installation option from the install point, then SQLExpress.xml must also be present in the **~\<share folder>\<SunSystems application>** folder.

Note: When considering the use of Administrative Installs, you should be aware of Microsoft’s Best Practices and the potential limitations of Administrative Installs. Refer to Microsoft documentation for more details.

- **Installation through command prompt**

  This feature enables SunSystems installation through a command prompt, which enables the installer to work with scripts or as a scheduled job.

- **Product Advertisement and Installation through group policy**

  Using this option, SunSystems can be installed on multiple computers on the network.

- **Installation using management application, such as Microsoft SMS**

  SunSystems installer supports installation through Microsoft Systems Management Server (SMS).

When installing SunSystems 6.2.1, you are presented with two options:

- New Installations & SunSystems v5 or v6.1 upgrades.
- Updates for existing SunSystems installations – for updating v6.2.1. Selecting this option uses the Database Utilities to update the databases. Features that were selected during the v6.2.1 installation will be carried forward, together with user settings, where possible. The sequence which follows will be mainly pre-populated with the correct carried forward values.

If you select the second option to update your existing v6.2.1 installation, you must ensure all of the relevant prerequisites are fulfilled.

Chapter 5 Installing SunSystems in a two-tier environment

5

Introduction

This configuration is for a system with a small number of SunSystems users. A single combined application and database server is installed. SunSystems client installations connect to this server.

Before you start, ensure that you have all of the prerequisite software installed, and you are logged in as a user who is a member of the local Windows administrator group.

If a Microsoft SQL Server default instance is installed and pre-configured SunSystems data is required, you may run an express installation in place of a complete install.

Installing the SunSystems application server

1. From the installer menu, select Server & Client Components, then Complete installation. If preconfigured SunSystems PK1 data is required, select the check box to install a SunSystems schema in the next dialog box.

SunSystems Security

2. Select the local database instance where the security database will be created, and tick to select new Security Database. Accept the default database name and location of database files.

SunSystems Domain

3. Enter Domain Datasource name, for example, DOMAINDSN, and accept local SQL Server instance and default domain database name. Accept the option to create a new Domain Database.
4. Accept the location of the database files and accept database collation Latin1_General_BIN.

SunSystems Database Business Group name details

5. Accept default settings BUGROUP, local SQL server instance, and database name SunSystemsData.

SunSystems security settings

6. Enter a security admin password and accept default English language and port 55000.
    a. Security Server account: As database and application is on the same machine, you can use local system account.

b SunSystems Service Account: As database and application is on the same machine, you can use local system account.

c Security Groups: Ensure that you have created SunSystemsServices and SunSystemsClients local groups in Windows on the database server as described in prerequisites.

Security database server language selection

7. Select any additional languages you require.

Do not apply SunSystems Patch Sets before you have installed SunSystems Reporting Services.

Select Reporting Services

8. Specify your local machine for SunSystems Report Server name and the SunSystems Report Manager.
9. To start the installation, click the Install button.

SRS Installation

10. Select Reporting Services.
11. Select complete installation.

SunSystems domain type

12. Select the local SQL Server instance.

Domain database

13. Enter the name of the domain database.

SunSystems Reporting Services

14. Enter user ID password and other details.

Report server instance

15. Select the Microsoft SQL Server Reporting Services instance.

Security server details

16. Enter security admin password.

Report Manager SMTP Server:

SMTP Server: **mail.<web domain>**

Port: **25** (for example)

Sender address: **<e-mail address for report distribution>**

Note: You must enter a port number to continue, even if you do not want emailed reports.

17. Complete the installation.

Installing SunSystems client

1. Select SunSystems Application Client (SQL Server). Choose Custom installation.
2. Selecting Components: From the installation component tree select SunSystems Client by de-selecting application server and security server. (SunSystems Client automatically includes Security client and SRS client).
3. Enter the server name where you have installed the SunSystems Application for Security and for the SunSystems Application Server.
4. Specify the SunSystems Report Server name and the SunSystems Report Manager name.
5. Proceed with the installation until completed.

Now refer to the Post-Installation Configuration section.

Chapter 6 Installing SunSystems in a multi-tier environment

6

Introduction

This section documents the installation of SunSystems in an environment where multiple servers are required for various SunSystems components, in order to serve a larger number of SunSystems users.

Installing the database and security servers

Refer to the SunSystems Architecture and Planning Guide to plan which servers you require. Specific prerequisites are required for each machine. If you are deploying a multi-tier installation, you must create the SunSystems Domain database first, followed by Security server. Subsequent components do not require installation in a strict order.

Multi-Tier Server	Example Name
Database and Security Server	ServerDBSEC
SunSystems Application Server	ServerAPP
SunSystems Web Server	ServerWEB
SQL Server Reporting Services Server	ServerSSRS
SunSystems Report Manager	ServerRS
SunSystems Report Manager	ServerRM
Infor Ming.le™ hosted in SharePoint	SharePointServer
SunSystems Client computer	Client1

Note: After you finish an installer option, you may have to wait a few seconds before selecting another option. The installer is tidying up temporary files in the background.

Application Role

The Application Role is an optional feature that allows certain client applications to connect directly to the database in a controlled fashion. The encryption method used to secure this information is not compatible with multiple security servers. If the application role is required, an installation must only have a single security server.

The minimum requirement for the user performing the installation is Create Database, Add login, and Create **sysviews** in master database. The first stage is to create the Domain database, then the SunSystems Security Database, then the SunSystems Data database (Business Unit Group). Then install SunSystems Security Server, which contains a Windows Service component and an IIS component. Detailed instructions are as follows:

Create a new SunSystems Domain database

1. On your Database Server (ServerDBSEC), launch the installer and select Database Utilities (SQL Server).
2. Select Create > a new SunSystems Domain database.
3. Specify a domain datasource name, for example, DOMAINDSN, local database server/instance, and domain database name, for example, SunSystemsDomain.
4. Select the location for data and log files.
5. Enter Administration and Client Groups: for example, SunSystemsServices and SunSystemsClients.
6. Select a base language, for example, 01English.
7. Proceed with the installation, and when processing is complete return to the database utilities menu.

Create a new SunSystems Security database

1. From the installer in the Database Utilities menu, select Create > a new SunSystems Security database.
2. Enter the database server\instance and database name, for example, SunSystemsSecurity
3. Select the location for data and log files.
4. Specify the data and index file groups.
5. Enter Administration and Client Groups: for example, SunSystemsServices and SunSystemsClients.
6. Proceed with the installation, and when processing is complete, exit to the main installer menu.

Create a new SunSystems Business Unit Group

This option will create a SunSystems Business Unit Group from scripts containing only default system data. After creation, no Business Units will be present.

1. If pre-configured data (PK1) is required, select Database Utilities > Create > a pre-configured SunSystems Business Unit Group. If pre-configured data is not required, then select Create > a new SunSystems Business Unit Group.
2. Specify the domain data source details created in the domain database installation.
3. Enter the Business Unit Group name, for example, BUGROUP, the local database instance name, and the database name, for example, SunSystemsData.

4. Select the data and log file locations.
5. Enter Administration and Client Groups: for example, SunSystemsServices and SunSystemsClients.
6. Select base language and additional languages to be used with this Business Unit Group.
7. Proceed with the installation, and when processing is complete return to the installer main menu.

Installing SunSystems Security

When installing SunSystems Security Web on a 64-bit Operating System without Microsoft SQL Server already installed, check ASP.NET is registered. If it is not already registered, you must register it. For details see the section 64-bit Operating System Prerequisite within this guide.

Note: SunSystems Security Web is a prerequisite of SunSystems 6.2.1 and is required for all browser-based access, including Reporting, SunSystems Web, Transfer Desk Web and the SSC demonstration website.

1. From the installation menu select Server & Client Components, Custom install.
2. From the features tree select Security Service and Security Web Server only.
3. Accept the local database server/instance.
4. Select the existing database created in the previous step.
5. Specify the security administrator name (admin) password, language, and listening port.
6. Enter the security service account, which must be a Windows domain account. This user must be part of the SunSystemsServices group. Ensure this account has Modify permissions for the **Program Files (x86)\Infor\SunSystems\SecurityWeb** folder, and Read permissions for the **\Windows\System32\inetsrv\config** folder.
7. Enter security groups.
8. Proceed with the installation until complete.
9. Alternatively, there is the option to independently install SunSystems Security Service and Security Web Server on different servers. In this case SunSystems Security Service must be the first to be installed.
10. IIS application SecurityWebServer requires modify permissions to web.config.
    a. In File Explorer, navigate to **Program Files (x86)\Infor\SunSystems**.
    b. Select SecurityWeb folder > Properties > Security tab.
    c. Click Edit > Add > Locations.
    d. Select your local machine and click OK.
    e. Enter IIS AppPool\SecurityWebServer > Check Names and click OK.
    f. In Permissions, select Modify and click OK.
11. IIS application SecurityWebServer requires read permissions to redirection.config.
    a. In File Explorer, navigate to **\Windows\System32\inetsrv**.

b Go to: Config folder > Properties > Security tab.

c Click Edit > Add > Locations.

d Select your local machine and click OK.

e Enter IIS AppPool\SecurityWebServer > Check Names and click OK. In Permissions, select Read & Execute and click OK.

Post-Installation Checklist for Database/Security Server

Check the following:	✓
In IIS Manager, check SecurityWebServer is running: **http://localhost:81/SecurityWebServer**	
Check Windows SunSystems Security Service is running.	
Add domain service accounts to SunSystemsServices Group.	

Installing the SunSystems application server

1. Ensure the Domain Service Accounts you intend to use have local security policy Log on as a service rights. Run **secpol.msc** to launch Local Security Policy. In Local Policies > User Rights Assignment, right-click Log on as a service and select Properties. Click Add User or Group > Locations and specify your Windows domain. Click OK, and specify the service accounts in the Enter the object names to select box.
2. On the application server (ServerAPP), select Server & Client Components and then Custom install.
3. From features, select SunSystems Application (and SunSystems Client) only.
4. Enter Database/Security server (ServerDBSEC) for SunSystems security.
5. Do not install a SunSystems schema.
6. Enter domain datasource details for SunSystems Domain.
7. Enter a Windows domain account for SunSystems services.
8. Specify Report Server (ServerRS), Report Manager (ServerRM) and SQL Server Reporting Services Server (ServerRS).

Complete the installation.

Caution: Do not apply SunSystems patch sets before you have installed SunSystems Reporting Services.

Add SunSystems Reporting Service Group Membership to SunSystems Users

Only SunSystems Reporting Service Administrators require SRS group membership. Normal SunSystems users do not require this membership to run ordinary reports.

1. If preconfigured data (PK1) has been installed, sign into User Manager as admin. Select Groups tab.
2. Edit Group PK1.
3. Select SunSystems Function Permission. Click Select all. Click Apply.
4. Select SunSystems Action Permissions. Add PK1. Click Apply. Click OK.
5. Go to the Users tab.
6. Right-click a user that requires SRS group membership (PK1 for example), and select Edit User.
7. Click Change (next to Group Membership).
8. Expand SunSystems Reporting, and select SunSystems Reporting functions required for this user.
9. Click OK to submit the changed group membership.

Serialization

At this stage of the installation, SunSystems can be serialized.

Note: If you serialize from within SunSystems using Serialization (ZZS), the SessionManager service login user must be a member of the Administrator group.

Post-Installation Checklist for SunSystems Application Server

Check the following:	✓
Check Windows Service SunSystems Session Manager is running:	
Check Windows service SunSystems Connect is running.	
You can access the SSC website at **http://localhost:8080/ssc**	

Installing SunSystems Reporting server

SunSystems Reporting can be installed on a single server together with SQL Server Reporting Services. To install on a single server, select Installations for a SQL environment > Reporting Services > Complete.

Alternatively, it can be split into three reporting components, each installed on a separate server. In this case, you must install in the following order:

1. Install Microsoft SQL Server Reporting Services Extensions on Server A

2. Install SunSystems Report Server on Server B
3. Install SunSystems Report Manager on Server C.

Prerequisites for installing Microsoft SQL Server Reporting Services

1. Prior to commencing installation, check that you have installed the appropriate prerequisites for the Microsoft SQL Server Reporting Services (ServerSSRS).
2. For each server, ensure you are a domain user with local administrator rights.

Installing Microsoft SQL Server Reporting Services Extensions on Server A

1. Run the installer. From the installation menu, select Installations for a SQL environment > Reporting Services > Custom Installation.
2. Select SQL Server Reporting Services extensions only. Deselect all other components.
3. Enter the following server details:
   - SunSystems Security server (ServerDBSEC)
   - Report Server (ServerRS)
   - Report Manager (ServerRM).
4. Ensure you have the correct URL. Go to Reporting Services Configuration Manager and check the following URL links are working:
   - Report Manager URL
   - Web Manager URL.
5. Enter the following user details:
   - Domain SunSystems Reporting user account
   - SunSystemsReporting account Password
   - SunSystemsServices group.
6. Select the local SQL Server instance where Reporting Services is installed.
7. Click Install.

Note: If you have any problems with the installation, check ConfigureReporting.log, which is found in **ProgramData\infor\SunSystems\Logs**.

Installing SunSystems Report Server on Server B

1. Run the installer. Select **Installations for a SQL environment** > **Reporting Services** > **Custom Installation**.
2. Select Report Server only. Deselect all other components.
3. Enter the following server details:
   - SunSystems Security server (ServerDBSEC)
   - Report Manager (ServerRM).

4. Ensure you have the correct URL by checking SQL Server, Reporting Services Configuration Manager, Web Service URL and Report Server Web Service URL.
5. Enter the following database details:
   - Domain database **<server\instance>**
   - Domain database name.
6. Enter the following SunSystemsReporting details:
   - Domain SunSystemsReporting account (to run the Report Server service)
   - Domain SunSystemsReporting account password
   - SunSystemsServices group.
7. Ensure the SunSystemsReporting user has local security policy Log on as a service right:
   - Run **secpol.msc** to launch Local Security Policy.
   - In Local Policies > User Rights Assignment, right-click Log on as a service and select Properties.
   - Click Add User or Group > Locations.
   - Specify your local machine and click OK.
   - Specify SunSystemsReporting in 'Enter the object names to select'.
8. Select the local SQL Server instance where Reporting Services is installed.
9. Click Install.

Post-Installation Checks for Server A and Server B

Check the following:	✓
In IIS Manager, check Application Pool SunSystemsReportingServices has started.	
Check the Windows Service SunSytemsReportingPrintService has started.	

Installing SunSystems Report Manager on Server C

1. Run the installer. Select Installations for a SQL environment > Reporting Services > Custom Installation.
2. Select Report Manager only. Deselect all other components.
3. Enter the following server details:
   - SunSystems Security server (ServerDBSEC)
   - Report Server (ServerRS).
4. Ensure you have the correct URL by checking SQL Server, Reporting Services Configuration Manager, Web Service URL and Report Server Web Service URL.
5. Enter the following database details:
   - Domain database **<server\instance>**

- Domain database name.

6. Enter the following SunSystemsReporting details:
   - Domain SunSystemsReporting account (to run the Report Server service)
   - Password
   - SunSystemsServices group.
7. Ensure the SunSystemsReporting user has local security policy Log on as a service right:
   - Run **secpol.msc** to launch Local Security Policy.
   - In Local Policies > User Rights Assignment, right-click Log on as a service and select Properties.
   - Click Add User or Group > Locations.
   - Specify your local machine and click OK.
   - SpecifySunSystemsReporting in 'Enter the object names to select'.
8. Enter the following Report Manager SMTP Server details:
   - SMTP Server: **mail.<web domain>**
   - Port:**25** (for example)
   - Sender address: **<e-mail address for report distribution>**

Note: You must enter a port number to continue, even if you do not want emailed reports.

9. Click Install.

Note: Loading sample reports may take up to 30 minutes.

Installing SunSystems Web

Caution: Prior to installing SunSystems Web, ASP.NET must be registered. If not already registered, you must register it. For details, see "Windows 64-bit operating system" in "Prerequisites for installing SunSystems in a multi-tier environment".

SunSystems Web runs within Apache tomcat. For this installation it is essential to install SunSystems Client:

1. Run the installer on the web server (ServerWEB).
2. Select Server & Client Components and then Custom installation.
3. From the feature tree, select SunSystems Client and SunSystems Web, SunSystems Web Help and Transfer Desk Web.
4. Enter server locations of SunSystems Security, SunSystems Application, Report Server and Report Manager.
5. Enter a Windows Domain Service Account for SunSystems Web. For example, svc-ssweb.

6. Enter the server location of the SSC Server (usually the same as the SunSystems application server) and SSC port number – 8080 by default.
7. SunSystems Domain: For SQL Server, give the Server, Instance and SunSystems Domain Database name.
8. Enter the Transfer Desk Web port number, or accept the default of 9090.

Ensure SunSystems Web Service Account has local security policy 'log on as a service' rights

1. Run **secpol.msc** to launch Local Security Policy.
2. Right-click Log on as a service and select Properties in Local Policies > User Rights Assignment.
3. Click Add User or Group > Locations and specify your Windows Domain.
4. Click OK.
5. Specify your Windows Domain Service account in Enter the object names to select.

Proceed with the installation until it is complete.

Internet Explorer 8 settings

To access SunSystems Web in Internet Explorer 8:

1. Go to: Tools > Compatibility View Settings.
2. Remove the check from Display intranet sites in compatibility view.

To display SunSystems reports in a new tab, change the default setting in Internet Explorer:

3. From the menu bar, select Tools > Internet Options > General > Tabs > Settings.
4. When a pop-up is encountered, click Always open pop-ups in a new tab.

Override user logged in

For SunSystems Web Users, you can set the override user logged in feature.

1. Login to User Manager as administrator.
2. Go to Groups > SunSystems Users Group > Operator Group.
3. Select Enable Clear Operator at login.

SunSystems Web Default Menus

To prevent the creation of a default menu where none exists when a user first logs in to SunSystems Web, you must modify an option in the **server-custom.properties** file. Set **client.defaultMenuCreation=false**.

By default, **client.defaultMenuCreation=true**. If set to false, then when a user logs into SunSystems web for the first time as a member of a group that does not have a menu, a message will be displayed indicating that a default menu has not been created.

Post-Installation Check for SunSystems Web

Check the following:	✓
Ensure the Windows service SunSystems Web Service has started.	
http://localhost:9080/SunSystems gives you access to a browser-based SunSystems interface	
Go to Internet Information Services (IIS) Manager > Application Pools, and check that TransferDeskWebServer has started.	

Post-Installation Steps

Adding Functions

The Transfer Desk Web installation creates three new SunSystems functions. Add these to the SunSystems menu:

1. Go to User Manager > Groups and select a user group from SunSystems Users. Click Edit > Function Permissions. Select SFM Server File Management, TRH Transfer History Viewer and TRP Transfer Profiles.
2. To run these functions, you must add them to your SunSystems menu. Log in to the SunSystems Windows client as administrator, and run the function User Group Menu Designer (UGM).
3. Select the user group for the SunSystems Web users, or PK1 for demonstration.
4. From the list of Function Names, search for Server File Management and click Add.
5. Add Transfer History Viewer and Transfer Profiles in the same way.
6. Click Save.

If any of these functions cannot be found, verify that they are selected in User manager for the same User Group. To test that these functions have been added to the menu, log out of SunSystems and log back in with the relevant user.

Defining the SSC Root Shared Folder

Before using Transfer Desk Web, a network shared folder, referred to as the Root Directory, must be created and Transfer Desk configured to use it.

We recommend that this is created on the machine hosting the SunSystems Connect Server Service, and in the **\ProgramData\Infor\Sunsystems** folder:

1. In Windows Explorer, create the folder, for example, C:\ProgramData\Infor\TransferDeskWeb**SSC Shared**.

2. Create the network share as follows: Open the folder Properties. In the Security tab, add the service account running your SunSystems Connect Server service, and grant Read and Write permissions. In the Sharing tab, select Share, and grant Read and Write permissions to this account. Click Share > Done > Close to complete this step. Make a note of the share name, for example, **<servername>\SSC Shared**.
3. Log in to a SunSystems Windows client as a user who is a member of the SunSystems Connect Administrators Group.
4. Select Transfer Desk > File > Server Folder Management > File > Change Root Directory.
5. Specify the Root Folder Name. For example, enter TransferDesk.
6. Specify the Root Folder Directory. Enter the full share name, for example, **<servername>\SSC Shared**.
7. Create subfolders for User Groups using File > Create Folder and assign the appropriate SunSystems User Groups to each subfolder.
8. Save your changes.

We recommend that subfolders are named so that you can easily identify which User Groups are assigned, for example, PK1 User Group.

Note: You must set the “File basis” to “server” in order for the profile to be displayed in Transfer Desk Web.

Installing SunSystems Client

1. Go to Server & Client Components > Custom installation on the client computer, for example, Client1.
2. Deselect all components n the component tree apart from SunSystems Client. SunSystems client includes Security client and SRS client.
3. Specify the Security server name and port number.
4. Select the SunSystems Application server name and port number.
5. Enter the server where SunSystems Report Server is installed and the server where SunSystems Report Manager is installed.
6. Proceed with the installation until it is complete.

Accessing SunSystems when Logged in to Windows as a Local User

If SunSystems is to be accessed from client computers when users are not logged on as Windows Domain users, you must set standard authentication globally in User Manager:

1. Log into User Manager as administrator.
2. Go to Settings > Security Policy
3. Deselect Enable Windows Authentication.

Chapter 7 Post-installation configuration for SunSystems in a multi-tier environment

7

SunSystems patch sets

SunSystems Patch Sets are available from **http://www.inforxtreme.com**. Here is the link to the latest SunSystems 6.2 Patch Set:
https://www.inforxtreme.com/espublic/EN/AnswerLinkDotNet/solutions/ViewSolution.aspx?SolutionID=1489656

The latest Patch Set must be applied to all tiers in a multi-tier installation. Read the Patch Set installation note included in the zip file for instructions.

You can check which Patch Sets are installed in **Control Panel** > **Programs** > **Programs and Features** > **View Installed Updates**.

After applying Patch Sets either restart the SunSystems services or shut down and restart your computer.

Serialization

At this this stage of the installation, SunSystems should be serialized.

Note: If you serialize from within SunSystems using Serialization (ZZS), the SessionManager service login user must be a member of the Administrator group.

Post-installation tasks

Migrating SunSystems Users and User Manager permissions

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

1. Go to: **Start** > **Infor SunSystems** > **SunSystems tools** > **Migration** > **SunSystems User Migration**.
2. Select Operator ID if a three digit SunSystems login is required. Alternatively, refer to the User Manager Help to create your own Users and Groups.

Add services to the Trusted Service group

During installation, the SunSystemsServices group is used to grant access to the SunSystems database. It is also set as the default group for trusted services.

After installation has completed, SunSystems can be implemented to use a separate Windows group for trusted services. This can enhance the security of your system by separating the trusted services permissions from database access permissions. In order to use a separate group for trusted services, 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 services; the system will, by default, use the same Windows group you selected for SunSystemsServices to obtain the required permissions.

Create the Windows TrustedServices group and add accounts

In Active Directory > Users and Computers, create the global group TrustedServices. Add the appropriate Windows accounts.

Configure the TrustedServices group in Security Console or User Manager

To configure in Security Console, select Security Settings (SES) > Security Service, and specify the relevant Windows group name in the Trusted Service Group field. Alternatively, in User Manager, go to Settings > SunSystems > Trusted Services Group.

If you do not correctly configure the Trusted Service Group SunSystems serialization will not run.

Add SunSystems Reporting Service group membership to SunSystems users

Only SunSystems Reporting Service Administrators require SRS group membership. Normal SunSystems users do not require this membership to run ordinary reports.

If preconfigured data (PK1) has been installed, sign into User Manager as admin:

1. Select Groups tab and edit Group PK1.
2. Select Function Permissions.
3. Click Select All > Apply.
4. Select Action Permissions > Add PK1 > Apply.
5. Select Users tab.
6. Right-click a user that requires SRS group membership, for example, PK1, and select Edit User.
7. Click Change.
8. Expand SunSystems Reporting Users, and select the SunSystems Reporting functions required for this user.
9. Click OK to submit the changed group membership.

Note: Note which users you have given SunSystems Data Access Managers role, and Report Manager role because these are required for the following steps.

Configuring Business Unit Data Models in Data Access Manager

1. From SunSystems, select Data Access Manager (DAR).
2. Select Configure Business Units and click the run icon.
3. Select the business units you would like to create a reporting data model for. Then click OK.
4. Save the changes before you exit Data Access Manager.

Note: You must use Data Access Manager to configure data models first before using any reporting functions such as Report Manager.

Note: If you create new business units you must add these to Configure Business Unit Data Models in Data Access Manager. Should you make any changes to an existing business unit, for example, modify languages, you must uncheck the Business Unit, click OK > Save, then redo the configuration.

Migrating reports

To run reports in Report Manager (RMA), the reports must be migrated to the latest schema version. You must be a member of the Reporting Administrator group to run this function.

1. From Report Manager (RMA), select Tools > Migrate Reports.
2. Click Yes to migrate all reports.

A Migration Report is generated on completion of the migration. Any reports that fail migration must be opened, corrected and redeployed in Report Designer.

Internet Explorer compatibility mode

To access SunSystems Web in Internet Explorer 8 go to: Tools > Compatibility View Settings, and deselect display intranet sites in compatibility view.

Log file locations

Log files can be found in standard location **ProgramData\Infor\Logs\SunSystems**. If you cannot see this location in Windows explorer, select in Folder Options > View and select Show hidden files, folders, and drives. Installer msi log files are found in the `%TEMP%` folder, or the folder above this location.

Security Web 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 as follows:

Note: For Windows Server 2012, bypass step 1 and step 2 and go to step 3.

1. In IIS Security, switch the Anonymous User setting for the SecurityWeb website to the App Role account.
2. Restrict the permissions to the SecurityWeb folder to Full control for the Security App Role account, and apply any other restrictions appropriate to your installation. In a typical Windows 7 installation, this folder is located in **Program Files\Infor\SunSystems\SecurityWeb.**
3. Grant Modify folder permissions to the SecurityWeb folder for local account **IIS apppool\SecurityWebServer**.

Changing the Configuration Service account logon

After installation, when you change the Configuration Service logon you must also run the following **netsh** command:

http add urlacl url=http://+:40004/Configuration user=DOMAIN\user

The Configuration user is the <DOMAIN\username> where username is the new service account.

To see which account is currently set as the Configuration Service account:

netsh http show urlacl url=http://+:40004/Configuration

To delete the current account prior to setting the new service account:

netsh http delete urlacl url=http://+:40004/Configuration

Modifying languages in your system.

SunSystems Database Utilities > Database Languages

Modifying languages on a domain and SunSystems Business Unit Group databases

From SunSystems Database Utilities, select Database Languages > Modify languages on Domain and SunSystems Business Unit Group databases.

This option applies and removes Language Packs to and from SunSystems business unit group databases. It must be run on a machine that provides a SunSystems Domain database DSN connection and a SQL Server installation, such as the SunSystems database server, and must be

rerun for each of the SunSystems business unit groups in the SunSystems domain that require the adjustment.

To modify a language on a SunSystems business unit group:

1. Uninstall the database Patch Sets using the DB Deployer tool.
2. From Database Utilities, select Database Languages and complete the Modify Languages on Domain and SunSystems Business Unit Group databases option.
3. Restart the SunSystems Security service.
4. Regenerate your menus:
   a. Log in to SunSystems as a user with access to the User Group Menu Designer (UGM).
   b. Select Change Language, and specify the language you wish to regenerate your menus for.
   c. Select Synchronise to Permissions.
   d. Click Save to save your changes, then exit User Group Menu Designer.
5. Reapply the database Patch Sets using the DB Deployer tool.

Note: If you make changes to existing business units you must update Configure Business Unit Data Models in Data Access Manager. Clear the Business Unit box, click OK, Save, and redo the configuration.

Note: Client and Application Server installations now include all standard SunSystems languages by default. It is only necessary to add languages to each SunSystems business unit group.

Installing a non-core language

Refer to the Language Pack Installation Note for instructions on how to install your specific language.

Hindic Numerals

Hindic numerals, also known as Arabic numerals, are now supported through your Windows Region and Language settings.

You must ensure that the correct country region for the appropriate number format has been switched on. Also ensure that the correct Native Digit setting has been selected. Go to Region and Language settings > Customize Format > Numbers > Use native digits. Select from:

- Context

  The digit shape depends on the previous text in the same output. European digits follow Latin scripts; Arabic-Indic digits follow Arabic text and Thai digits follow Thai text.
- None

  The digit shape is not changed. Full Unicode compatibility is maintained.
- National

The digit shape is the native equivalent of the digits from 0 through 9. ASCII digits from 0 through 9 are replaced by equivalent national digits.

Caution: If you have logged into SunSystems prior to installing another SunSystems language, then you need to go into function UGM and run ‘synchronise with permissions’ for each user group.

Chapter 8 Infor Ming.le™, ION and Configuring SunSystems with them

8

Prerequisites

SunSystems must not be installed on the same server as ION or Infor Ming.le™. This section outlines what you have to do to configure SunSystems with Infor Ming.le™ and optionally IFS and ION.

Infor Ming.le™

Instructions are found in Infor Ming.le™ Installation and Configuration Guide on Infor Xtreme

http://www.inforxtreme.com

SunSystems

Refer to SunSystems Installation section of SunSystems Installation guide.

ION

Refer to the latest ION installation and configuration documentation on Infor Xtreme.

Infor Federation Services

There are 8 scenarios to install IFS, ION and Infor Ming.le™, IFS with Infor Ming.le™ installed together is just one of them. It is not mandatory to link SunSystems security to IFS.

Configuration

Installing the Infor Ming.le™ Plug-in for SunSystems

See Infor Ming.le™ Installation and Configuration Guide. You should be logged in as the domain spinstall account.

From the Start menu, run Infor Ming.le™ Configuration Wizard.

Select your web application: Infor Ming.le™ SharePoint, and the site collection you created, for example, https://Mingle.infor.com. Select Infor Ming.le™ and SunSystems plug-in, and other features you require, then click Configure. There are several features that require a licence key. On the next dialog check that the SunSystems details are complete:

Title:

SunSystems

Site:

Select from dropdown `https://MingleServer.infor.com/sunsystems`

Site Collection:

`https://MingleServer/sites/<site collection>/sunsystems`

Logical ID:

`lid://infor.sunsystems.1` (This needs to be the unique universal id of one SunSystems installation, which must be consistent in SunSystems PPE, ION Desk, Workflow drill back, Infor Ming.le™ everywhere).

Application Version:

`6.2`

Hostname:

`SUNserver.infor.com`

Port:

`9080` (or 9443 if you have set up SunSystems Web as https)

Context:

`SunSystems`

Use HTTPS:

`No` (or Yes if you have set up SunSystems Web as https)

Infor Federation Services

Enabling IFS in User Manager

SunSystems Security must be configured for SSL before this step.

In User Manager, Settings menu > Security Policy, select the Authentication tab, Configure. Enter the IFS Server FQDN name, for example, MingleServer.domain.com, and the HTTP Port number. (You can check this port number in IIS Manager on the IFS Server). Click Apply to confirm the connection, and then click OK. Now check the Use an IFS server for Single Sign-On Authentication check box, and click OK.

Enabling SunSystems in IFS

Open the Infor Federation Services application from the desktop, click the refresh icon and select the Configure dropdown > Applications. Select SunSystems, and click the “Activate and add to ADFS” button. You must enter your local administrator user and password. Check all the Security Roles check boxes, and click the Submit button to save. Now go to Manage > Users. If you click on a user, you can see Authorized Applications list IFS and SunSystems in the right hand window.

On your SunSystems server, restart the SunSystems security website in IIS Manager.

In Internet Explorer, go to:

```
https://SUNserver.infor.com:82/SecurityWebServer
```

You will then be notified that the security policy has been changed. Close the browser and retry.

Check SunSystems Security Web Server secure port after enabling IFS	
`https://SUNserver.domain.com:82/SecurityWebServer`	

ION Configuration

- See Workflow Configuration Guide.

Contextual applications

- See Context Sensitive Links and Drillbacks appendixes in this guide.

Q&A

- See Q&A Installation Guide on the Q&A media.

Logical Ids

The logical ID identifies the instances of the SunSystems environment and is set in a few places, It ties together the BODs SunSystems publishes to the ION connection point and to how Infor Ming.le™ has SunSystems instances installed.

Here is an example description of where logical IDs can be set and must be the same.

A logical ID can look like 'Infor.SunSystems.SunLive'

1. SunSystems web-nav – used to send out in web UI
   The file can be found at:-
   C:\ProgramFiles (x86)\Infor\SunSystems\SunSystemsWeb\tomcat\webapps\SunSystems\WEB-INF\server-custom.properties

   Change the property:-
   client.logicalId=lid:// Infor.SunSystems.SunLiv

2. SunSystems deployment in Infor Ming.le™ – used for Infor Ming.le™ to send correct LID to SunSystems in messages and linking:

- Lid in Infor Ming.le™-SunSystems Plug-in in 'Infor Application Deployments' in Infor Ming.le™ site content, for example 'lid://infor.sunsystems.SunLive'
- Lid Prefix in 3 latest SunSystems drill back views, e.g. has to be 'lid://infor.sunsystems', in 'Infor Application Views' of Mingle site content.
- Lid prefix in Infor Application Information of SunSystems in Infor Ming.le™ site content, for example. must be 'lid://infor.sunsystems'

3. PPE – used to set in outgoing BODs
   Lid of SunSystems ION integration setting in Property Editor (PPE) under note 'integration ->from queue', must be 'lid://infor.sunsystems.SunLive'

4. ION connection point – used to route the BODs
   See ION guides for how to configure a connection point.

Context Sensitive Links to Context Apps

The following table shows the SunSystems functions and fields that have context sensitive links to context apps:

SunSystems Function	Function ID	Scenario	SunSystems Field - Field ID/Subset	Infor 'Address' Context Attributes - SunSystems Fields	Infor 'contactContext' Attributes - SunSystems Fields	Business Search Context Attributes - SunSystems Fields	Search Request Context - SunSystems Fields	Package Information - SunSystems fields
		Contextual Application:		*Bing Maps*	*Twitter*	*Yelp*	*WolframAlpha*	*Package Tracker*
Addresses	**VW5138**	From a customer or supplier record, click the 'Addresses' drill button (which uses data from the 'Company Address Code') and display the full address information	Address Code - 10/0 Address Line 1 - 20/0 Address Line 2 - 30/0 Address Line 3 - 40/0 Address Line 4 - 50/0 Address Line 5 - 60/0 Town/City - 250/0 State - 170/0 Postal Code - 160/0 Country - 100/0 E-mail Address - 252/0 Address Misc Description 1 - 254/0 Address Misc Description 2 - 256/0	street - Address Lines 1-5 city - Town/City state - State zipCode - Postal Code country - Country	contactName - Address Code companyName - Address Line 1 emailsAddresses - E-mail Address twitterIds - Address Misc Description 1 facebookIds - skypeIds - Address Misc Description 2 yahooIds - msnIds - aimIds -	businessName - Address Line 1 businessCategory- businessLocation - Town/City, State	searchEngine- wolfram searchExpression - Address Line 1	N/A
Analysis Codes	**VW5270**	Create or view an analysis code	Analysis Dimension - 10/0 Analysis Code - 20/0 Name - 90/0	N/A	N/A	N/A	searchEngine- wolfram searchExpression - Analysis Code, Name, Dimension	N/A
Analysis Dimensions	**VW5269**	Create or view an analysis dimension	Analysis Dimension - 10/0 Description 90/0	N/A	N/A	N/A	searchEngine- wolfram searchExpression - Dimension, Description	N/A
Bank Details Setup	**VW5147**	Create or view a bank account	Bank Name - 110/0 Bank Branch - 100/0	Street - Bank Name, Bank Branch	companyName - Bank Name twitterID - Bank Name	businessName - Bank Name businessCategory- 'Bank'	searchEngine- wolfram searchExpression - Bank Name, Bank Branch	N/A

SunSystems Function	Function ID	Scenario	SunSystems Field - Field ID/Subset	Infor 'Address' Context Attributes - SunSystems Fields	Infor 'contactContext' Attributes - SunSystems Fields	Business Search Context Attributes - SunSystems Fields	Search Request Context - SunSystems Fields	Package Information - SunSystems fields
Business Unit Name	**VW5151**	Create or amend business unit information	Description - 30/0 Email Address - 100/0 Web Page Address - 90/0	N/A	contactName - Description companyName - Description emailsAddresses - E-mail Address twitterIds - Description	businessName - description	searchEngine- wolfram searchExpression - Description	N/A
Chart of accounts	**VW5152**	Create or view an account record. Fits well when the customer is using account records as customer/supplier records	Description - 20/0	N/A	companyName - Description	businessName - Description	searchExpression - Description	N/A
Contact	**VW5810**	Enter a contact code, browse the contact record	Name - 20/0 E-mail Address - 110/0 Contact Misc Reference 1 - 280/0 Contact Misc Reference 2 - 290/0	N/A	contactName - Name companyName - emailsAddresses - E-mail Address twitterIds - Contact Misc Reference 1 facebookIds - skypeIds - Contact Misc Reference 2 yahooIds - msnIds - aimIds -	businessName - Name businessCategory- businessLocation -	searchEngine- wolfram searchExpression - Name	N/A
Customer	**VW5150**	Enter a customer code, browse the customer record, link through to an address	Name - 120/0 E-Mail Address - 90/0 Web Page Address - 100/0 Customer Misc Reference 1 - 2410/0 Customer Misc Reference 1 - 2420/0	N/A	contactName - Name companyName - emailsAddresses - E-Mail Address twitterIds - Customer Misc reference 1 facebookIds - skypeIds - Customer Misc reference 2 yahooIds - msnIds -	businessName - Name businessCategory- businessLocation -	searchEngine- wolfram searchExpression - Name	N/A
Employee	**VW5132**	Enter an employee code, browse record, link through to an address	Family Name - 130/0 First Name - 60/0 Telephone No - 115/0 Mobile Phone Number - 710/0 E-mail Address - 720/0	N/A	contactName - First Name + Family Name companyName - emailsAddresses - E-Mail Address twitterIds - facebookIds - skypeIds - yahooIds - msnIds -	N/A	searchEngine- wolfram searchExpression - First Name + Family Name	N/A

SunSystems Function	Function ID	Scenario	SunSystems Field - Field ID/Subset	Infor 'Address' Context Attributes - SunSystems Fields	Infor 'contactContext' Attributes - SunSystems Fields	Business Search Context Attributes - SunSystems Fields	Search Request Context - SunSystems Fields	Package Information - SunSystems fields
Fixed Asset Record	**VW5204**	Create or view a fixed asset record - can send twitter id values based on asset code or desc	Asset Code - 10/0 Description - 90/0	N/A	twitterIds - Asset Code, Description	N/A	searchEngine- wolfram searchExpression - Description	N/A
Fixed Asset Class	**VW5257**	Create or view a fixed asset class - can send twitter id values based on asset class code or desc	Asset Class Code - 10/0 Description - 90/0	N/A	N/A	N/A	N/A	N/A
Inventory Locations	**VW5080**	Enter location code, use the warehouse code to do some BI, use description for wolfram search	Location Code - 10/0 Description - 80/0 Warehouse Code - 20/0 Warehouse code name - 230/0	Street - Warehouse Code, Warehouse code name	twitterIds - Warehouse code, warehouse name	businessName - Warehouse code businessLocation - Warehouse code		
Item Master	**VW5001**	Create or view an item	Item Code - 10/0 Description - 380/0	N/A	twitterID - Item Code, Description	N/A	searchEngine- wolfram searchExpression - Item Code, Description	N/A
Purchase Invoice Entry	**PIE**	Create or view a purchase invoice	Supplier Code - 42/0 Invoice Address Line 1 - 582/0 Invoice address line 2 - 584/0 Invoice address Country - 598/0 Invoice address Postal Code - 614/0	street - Invoice address Line 1 & 2 country - invoice address country zipCode - invoice address postal code	contactName - Supplier Code companyName - Supplier Code twitterID - Supplier Code	businessName - Supplier Code businessLocation - invoice address Postcode		N/A

SunSystems Function	Function ID	Scenario	SunSystems Field - Field ID/Subset	Infor 'Address' Context Attributes - SunSystems Fields	Infor 'contactContext' Attributes - SunSystems Fields	Business Search Context Attributes - SunSystems Fields	Search Request Context - SunSystems Fields	Package Information - SunSystems fields
Purchase Order Entry	**POE**	Enter a purchase order, select supplier code - see form ALLPOES3	Supplier - 106/0 Supplier order address Line 1 - 724/0 Supplier order address Line 2 - 726/0 Supplier order address Line 3 - 728/0 Supplier order address Line 4 - 730/0 Supplier order address Line 5 - 732/0 Supplier order town/city - 772/0 Supplier order country - 740/0 Supplier order postcode - 756/0	street - Line 1 & Line 2 city - Supplier order town/city zipCode - supplier order postcode country - supplier order country	contactName - Supplier companyName - Supplier twitterID - Supplier	businessName - Supplier businessLocation - supplier order Postcode	searchEngine- wolfram searchExpression - Supplier	N/A
Sales Order Entry	**SOE**	Enter a sales order reference and browse the record. View tracking information by adding a tracking number to the 'Line 5' field	Customer Name - 128/0 Line 1 - 731/1 Line 2 - 732/1 Line 3 - 733/1 Line 4 - 734/1 Line 5 - 735/1 Carrier - 361/1	street - Line 1 & Line 2 city - Line 3 state - Line 4 zipCode - country -	contactName - Customer Name companyName - Customer Name emailsAddresses - twitterIds - facebookIds - skypeIds - yahooIds - msnIds -	businessName - Customer Name businessCategory- businessLocation -	searchEngine- wolfram searchExpression - Customer Name	carrier - Carrier trackingNumber - Line 5
Supplier	**VW5148**	Enter a supplier code, browse the customer record, link through to an address	Supplier Name - 60/0 E-mail Address - 130/0 Web Page Address - 140/0 Supplier Misc Reference 1 - 9140/0 Supplier Misc reference 2 - 9145/0	N/A	contactName - Supplier Name companyName - emailsAddresses - E-Mail Address twitterIds - Supplier Misc Reference 1 facebookIds - skypeIds - Supplier Misc Reference 2 yahooIds - msnIds -	businessName - Supplier Name businessCategory- businessLocation -	searchEngine- wolfram searchExpression - Supplier Name	N/A

SunSystems Function	Function ID	Scenario	SunSystems Field - Field ID/Subset	Infor 'Address' Context Attributes - SunSystems Fields	Infor 'contactContext' Attributes - SunSystems Fields	Business Search Context Attributes - SunSystems Fields	Search Request Context - SunSystems Fields	Package Information - SunSystems fields
Warehouse Groups	**VW5036**	Enter warehosue group codes and display the area on a map	Warehouse group code - 10/0 Description - 60/0	City - Warehouse group code	twitterIds - Description	businessName - businessCategory- 'Warehouse' businessLocation - Warehouse group code'	searchEngine- wolfram searchExpression - Description	N/A
Warehouse Setup	**VW5122**	Enter a warehouse code and use it to display a map. Linked address goes to the detailed address detail	Warehouse Code- 10/0 Description - 130/0 Default Carrier - 170/0	City - Warehouse code	twitterIds - Warehouse Code	businessName - Warehouse code businessCategory- 'Warehouse' businessLocation - Description	searchEngine- wolfram searchExpression - Description	carrier - Default Carrier

Drillback Views

The following table shows the available drillback views.

Key

- Drillback View ID – The Drillback View definition
- SunSystems Function (Function ID) – The SunSystems function and function ID, and where the drillback / IBC publication will occur
- Filter Type ID – The filter type code used to invoke the IBC and drillback handling
- ID (+SunSystems value name) – The field on the function form that receives the values from a drillback URL. The value of the ID1 parameter sent in a drillback URL.
- Further IDs and SunSystems Reference (Unique ID) – Additional values that SunSystems supports in a drillback URL.
- Infor Business Context Support (Entity Type) – The 'Infor Standard Entity Type' associated to a SunSystems object. IBC messages switch on contextual applications, shortcuts and sharing in Infor Ming.le™..
- Infor Business Context BOD (Noun) – The BOD associated with the function. If set, it will emit a BOD Reference message within IBC. Denotes which SunSystems objects publish a BOD so the system can emit the BOD reference information within an IBC message. This switches on things like the 'follow' feature in Paparazzi.
- Secondary Entities – Indicates entities related to the function that can also go out as separate messages
- Drillback Type
  - BOD: BOD-based Infor Ming.le™ produced drillback – which SunSystems objects can support an automatic drillback, where the link is generated by Infor Ming.le™.
  - BOD_COMPONENT
  - OTHER
  - Drillback not supported

The following URL can be executed in order to generate a views.xml file which details the drillback views which SunSystems supports. Just paste this URL (replacing localhost with the machine name if applicable) into an internet browser.

http://localhost:9080/SunSystems/unsecured_pages/mingle/Views.jsp

Drillback View ID	SunSystems Function (Function ID)	Filter Type ID	ID1 (+SunSystems value name)	Further IDs and SunSystems Reference (Unique ID)	Infor Business Context Support (EntityType)	Infor Business Context BOD (Noun)	Secondary Entities	Drillback Type
AccoutingEntityView	Business Unit Setup (VW5286)		BusinessUnitCode (Business Unit Code)		InforAccountingEntity	AccountingEntity	n/a	BOD
AccountingJournalView	Journal Type (VW5354)		JournalType (Journal Type)		InforAccountingJournal	AccountingJournal	[InforJournalClass, InforPaymentProfile]	BOD_COMPONENT
AdditionalFieldView	Additional Fields Setup (VW5802)		ColumnType(Column Type)	ID2=ColumnNumber	InforAdditionalFields	n/a	n/a	OTHER
AddressView	Addresses (VW5138)		AddressCode (Address Code)		InforAddress	n/a	n/a	OTHER
AllocationCodeView	Allocation Codes Setup (VW5554)		AllocationActionCode (Allocation Action Code)		InforAllocationCodes	n/a	n/a	OTHER
AllocationRatioView	Corporate Allocation Ratios (VW5631)		AllocationRatioCode (Allocation Ratio Code)		InforAllocationRatio	n/a	[InforAnalysisDimension]	OTHER
AllocationSetupView	Corporate Allocation Setup (VW5627)		AllocationSetupCode (Allocation Setup Code)		InforAllocationSetup	n/a	[InforAccountingJournal, InforChartOfAccount]	OTHER
AnalysisCodeView	Analysis Codes (VW5270)		Code (Analysis Code)	ID2= Dimension (Analysis Dimension)	InforAnalysisCode	CodeDefinition	n/a	BOD_COMPONENT
AnalysisDimensionView	Analysis Dimensions (VW5269)		AnalysisDimension (Analysis Dimension)		InforAnalysisDimension	CodeDefinition	n/a	BOD_COMPONENT
AnalysisHierarchyView	Analysis Hierarchy (VW5310)		AnalysisDimension (Analysis Dimension)	ID2=AnalysisHierarchyLabel (Analysis Hierarchy Label)	InforAnalysisHierarchy	n/a	n/a	OTHER
AnalysisLayoutView	Financial Analysis Layouts (VW5654)		LayoutCode (Layout Code)		InforAnalysisLayout	n/a	n/a	OTHER
AssetClassView	Fixed Asset Class (VW5257)		AssetID (Asset Class Code)		InforAssetClass	n/a	[InforChartOfAccount]	OTHER
AssetMasterView	Fixed Asset Class (VW5257)/Asset Records (VW5204)		AssetID (Asset Class Code)		InforAssetMaster	n/a	[InforAssetClass]	BOD
AuthJournalView	Authorizations (SAAQ)	SAAUTHDR	AuthorisationSetReference (Authorisation Set Ref)		InforAuthJournal	n/a	n/a	OTHER

Drillback View ID	SunSystems Function (Function ID)	Filter Type ID	ID1 (+SunSystems value name)	Further IDs and SunSystems Reference (Unique ID)	Infor Business Context Support (EntityType)	Infor Business Context BOD (Noun)	Secondary Entities	Drillback Type
AuthPaymentView	Payment Journal		PaymentAuthorisationSetReference (Payment Authorisation Set Ref)		n/a	n/a	n/a	OTHER
BankDetailsView	Bank Details Setup (VW5147)		BankDetailsCode (Bank Details Code)	ID2 = BankSubCode (SunSystems)	InforBankDetails	n/a	[InforChartOfAccount, InforCustomerPartyMaster, InforSupplierPartyMaster]	OTHER
BatchView	Batch References Setup (VW5029)		ItemCode (Item Code)	ID2 = BatchReference (Batch Reference)	InforBatch	n/a	n/a	OTHER
BudgetCheckSetupView	Budget Check Setup (VW5565)		AccountCodeFrom (Account Code From)	ID2 = AccountCodeTo (Account Code To)	InforBudgetCheckSetup	n/a	n/a	OTHER
BusinessAccountCodeView	Business Account Codes (INTGBAC)		AccountRecognitionCode (Account Recognition Code)		InforBusinessAccountCode	n/a	[InforAnalysisDimension, InforChartOfAccounts]	OTHER
ChargeIndexView	Charge Index (VW5261)		ChargeIndexCode (Charge Index Code)		InforChargeIndex	n/a	[InforAnalysisDimension]	OTHER
ChargeRuleView	Charge Rules (VW5074)		ChargeRuleCode (ChargeRuleCode)		InforChargeRules	n/a	[InforChargeIndex]	OTHER
ChartOfAccountsView	Chart of accounts (VW5152)		Accounting Chart ID (Business unit code)	ID2=Natural Account (Account Code)	InforChartOfAccounts	ChartofAccounts	[InforCurrency]	BOD_COMPONENT
ConsolidationGroupView	Consolidation Groups (VW5522)		ConsolidationGroupName (Consolidation Group Name)		InforConsolidationGroup	n/a	n/a	OTHER
ContactsMasterView	Contacts (VW5810)		ContactCode (Contact Code)		InforContact	ContactMaster	n/a	BOD
CurrencyDailyRateView	Currency Exchange Rates		Currency Code From (Currency Code From)	ID2 = Currency Code To ID3 = From Date ID4 = To Date ID5 = Account From	InforCurrencyDailyRate	CurrencyExchangeRateMaster	n/a	BOD_COMPONENT
CurrencyExchangeMasterDailyRateView	Currency Daily Rates (VW5057)				InforCurrencyDailyRate	CurrencyExchangeRateMaster	[InforChartOfAccounts, InforCurrency]	BOD_COMPONENT
CurrencyExchangeMasterPeriodRateView	Currency Period Rates (VW5058)				InforCurrencyPeriodRate	CurrencyExchangeRateMaster	[InforChartOfAccounts, InforCurrency]	BOD_COMPONENT
CurrencyPeriodRateView	Currency Period Rates (VW5058)		Currency Code From (Currency Code From)	ID2 = Currency Code To ID3 = From Period ID4 = To Period ID5 = AccountFrom	InforCurrencyPeriodRate	n/a	n/a	BOD_COMPONENT
CurrencyView	Currency Codes (VW5285)		CurrencyCode (Currency Code)		InforCurrency	n/a	[InforChartOfAccounts]	OTHER

Drillback View ID	SunSystems Function (Function ID)	Filter Type ID	ID1 (+SunSystems value name)	Further IDs and SunSystems Reference (Unique ID)	Infor Business Context Support (EntityType)	Infor Business Context BOD (Noun)	Secondary Entities	Drillback Type
CustomerReturnView	Sales Return Note (SOE)		TransactionReference (Transaction Reference)		InforCustomerReturn	n/a	n/a	OTHER
CustomerView	Customers (VW5150)		CustomerId (Customer Code)		InforCustomerPartyMaster	CustomerPartyMaster	[InforChartOfAccounts, InforCurrency, InforEmployee, InforWarehouse]	BOD
DocumentFormatView	Document Format (VW5159)		DocumentFormatCode (Document Format Code)		InforDocumentFormat	n/a	[InforAccountingEntity]	OTHER
EmployeeView	Employees (VW5132)		EmployeeId (Employee Code)		InforEmployee	Person	n/a	BOD
EventProfileView	Event Profiles (SSEP)		EventCode (Event Code)		InforEventProfile	n/a	n/a	OTHER
FinancialTableFormatView	Financial Table Formats (VW5647)				InforFinancialTableFormat	n/a	n/a	OTHER
GLMovementView	Balances (SALQ)		PostingKey (Not supported)	ID2=Natural Account (Account Code) ID3=PeriodID (Accounting Period MMM) ID4=Year (Accounting Period YYYY)	n/a	n/a	n/a	BOD_COMPONENT
HeldJournalView	Ledger Inquiry – Held Journals (SAJH)		JournalHeldReference (Journal Held Reference)		InforHeldJournal	n/a	[InforAccountingJournal]	OTHER
InspectionCodeView	Inspection Codes (VW5089)		InspectionCode (Inspection Code)		InforInspecationCode	n/a	[InforEmployee]	OTHER
IntegrationConfigView	Integration Configuration (INTGMAIN)		ConfigurationName (Configuration Name)		InforIntegrationConfig	n/a	n/a	OTHER
InventoryCostTypeView	Inventory Cost Types (VW5205)		CostTypeCode (Cost Type Code)		InforInventoryCostTypes	n/a	n/a	OTHER
InventoryCostView	Inventory Costing Inquiry (ICOCD)	IMCDITCO	ItemCode (Item Code)		InforInventoryCost	n/a	n/a	Drillback not supported
InventoryCountView	Inventory Count Entry (ICLE)		InventoryCountDefinitionCode (Inventory Count Definition Code)		InforInventoryCount	n/a	n/a	BOD
InventoryLocationView	Inventory Locations (VW5080)		LocationCode (Location Code)		InforInventoryLocation	n/a	[InforInventoryZone, InforWarehouse]	OTHER

Drillback View ID	SunSystems Function (Function ID)	Filter Type ID	ID1 (+SunSystems value name)	Further IDs and SunSystems Reference (Unique ID)	Infor Business Context Support (EntityType)	Infor Business Context BOD (Noun)	Secondary Entities	Drillback Type
InventoryReceiptNoteEntryView	Inventory Receipt Note Entry (RNE)		ReceiptNoteReference (Receipt Note Reference)		InforInventoryReceiptNoteEntry	n/a	[InforItemMaster]	OTHER
InventoryRevaluationView	Inventory Revaluation Profile (VW5458)		ProfileCode (Profile Code)		InforInventoryRevaluationView	n/a	n/a	OTHER
InventoryView	Inventory Inquiry (INVINQ)		Item (Item Code)	ID2=Warehouse (Warehouse Code) ID3= CurrentDate (Projected From To dates)	InforInventory	n/a	n/a	OTHER
InventoryZoneView	Inventory Zones (VW5206)		ZoneCode (Zone Code)		InforInventoryZone	n/a	n/a	OTHER
InvoiceLineView	Sales Invoice Control Desk (SMCDSI)		InvoiceNumber (Sales Invoice Id)	ID2= InvoiceLineNumber (Line Number)	n/a	n/a	n/a	BOD_COMPONENT
InvoiceView	Sales Invoicing (SCD)	SMCDSI	InvoiceNumber (Sales Invoice Id)		InforSalesInvoice / InforInvoice	n/a	[InforCustomerPartyMaster, InforItemMaster, InforSalesOrder, InforSalesType]	BOD
ItemCharacteristicView	Item Characteristics (VW5247)		CharacteristicCode (Characteristic Code)		InforItemCharacteristic	n/a	n/a	OTHER
ItemView	Item Master (VW5001)		Item (Item Code)		InforItemMaster	ItemMaster	[InforSupplierPartyMaster, InforUnitOfMeasure, InforWarehouse]	BOD
JournalClassView	Journal Class Setup (VW5541)		JournalClassCode (Journal Class Code)		InforJournalClass	n/a	n/a	OTHER
JournalPresetView	Journal Presets (VW5600)		PresetCode (Preset Code)	ID2 = LineNumber (Line Number)	InforJournalPreset	n/a	[InforChartOfAccount]`	OTHER
JournalView	Ledger Inquiry (SALQ)	SALQ	JournalNumber (Journal Number)		InforSourceSystemJournalEntry	SourceSystemJournalEntry	[InforAccountingJournal, InforChartOfAccount]	BOD
LedgerInterfaceView	Ledger Interface (VW5145)		InterfaceCode (Interface Code)		InforLedgerInterface	n/a	[InforAccountingJournal, InforChartOfAccounts]	OTHER
LedgerSetupView	Ledger Setup (VW5588)		BusinessUnitCode (Business Unit Code)		InforLedgerSetup	n/a	n/a	OTHER
MovementOrderPresetView	Movement Order Presets (VW5538)		PresetCode (Preset Code)		InforMovementOrderPreset	n/a	n/a	OTHER
MovementOrderView	Movement Inquiry (MCD)	IMCDMO	MovementOrderReference (Movement Order Reference)		InforMovementOrder	n/a	[InforItemMaster]	OTHER

Drillback View ID	SunSystems Function (Function ID)	Filter Type ID	ID1 (+SunSystems value name)	Further IDs and SunSystems Reference (Unique ID)	Infor Business Context Support (EntityType)	Infor Business Context BOD (Noun)	Secondary Entities	Drillback Type
MovementTypeView	Movement Types (VW5157)		TypeCode (Type Code)		InforMovementType	n/a	n/a	OTHER
PayableView	Payment Selection and Review (SALQ)		PayableDocumentId (Journal Number)		n/a	n/a	n/a	BOD
PaymentProfileView	Payment Run (SAGP)		PaymentProfileCode (Payment Profile Code)		InforPaymentProfile	n/a	[InforBankDetails, InforChartOfAccounts]	OTHER
PaymentTermsView	Payment Terms (VW5208)		PaymentTermCode (Payment Term Code)		InforPaymentTerms	n/a	n/a	OTHER
PurchaseInvoiceLineView	Purchase Inquiry (PCD)	PMCDPI	InvoiceNumber (Purchase Invoice reference)	ID2= InvoiceLineNumber (Line Number)	InforPurchaseInvoiceLine	n/a	[InforChartOfAccounts, InforItemMaster, InforSupplierPartyMaster]	BOD_COMPONENT
PurchaseInvoiceView	Purchase Invoice Entry (PIE)		InvoiceNumber (Purchase Invoice reference)		InforPurchaseInvoice	n/a	[InforChartOfAccounts, InforItemMaster, InforPaymentTerms, InforSupplierPartyMaster]	BOD
PurchaseOrderLineView	Purchase Inquiry (PCD)	PMCDPO	PurchaseOrder (Purchase Order Reference)	ID2= PurchaseOrderLineNumber (Line Number)	InforPurchaseOrderLine	PurchaseOrder	[InforChartOfAccounts, InforItemMaster, InforSupplierPartyMaster]	BOD_COMPONENT
PurchaseOrderView	Purchase Order Entry (POE)		PurchaseOrder (Purchase Order reference)		InforPurchaseOrder	PurchaseOrder		BOD
PurchasePriceBookView	Purchase Price Book (VW5498)		DefinitionCode (Definition Code)		InforPurchasePriceBook	n/a	n/a	OTHER
PurchaseTypeView	Purchase Types (VW5182)		PurchaseTransactionType (Purchase Transaction Type)		InforPurchaseType	n/a	n/a	OTHER
ReceivableView	Ledger Inquiry (INVINQ)		ReceivableDocumentId (Journal Number)		n/a	n/a	n/a	BOD
ReconciliationProfileView	Reconciliation Accounts (VW5917)		ProfileCode (Profile Code)		InforReconciliationProfile	n/a	[InforChartOfAccounts]	OTHER
RejectionCodeView	Financial Rejection Code Setup (VW5926)		RejectionCode (Rejection Code)		InforRejectionCode	n/a	n/a	OTHER
RevaluationProfileView	Ledger Revaluation (SALR)		ProfileCode (Profile Code)		InforRevaluationProfile	n/a	n/a	OTHER
RuleSetView	Rule Sets (INZRS)		EventCode (Event Code)	ID2 = RuleCode (Rule Code)	InforRuleSet	n/a	n/a	OTHER

Drillback View ID	SunSystems Function (Function ID)	Filter Type ID	ID1 (+SunSystems value name)	Further IDs and SunSystems Reference (Unique ID)	Infor Business Context Support (EntityType)	Infor Business Context BOD (Noun)	Secondary Entities	Drillback Type
SalesContractView	Sales Blanket Contract (VW5484)		Heading (Heading)		InforSalesBlanketContract	n/a	[InforCustomerPartyMaster, InforItemMaster]	OTHER
SalesOrderLineView	Sales Order Entry (SOE)		SalesOrder (Sales Order Transaction Ref)	ID2= SalesOrderLineNumber (Line Number)	InforSalesOrderLine	SalesOrder	[InforCustomerPartyMaster, InforItemMaster]	BOD_COMPONENT
SalesOrderPresetView	Sales Order Preset (VW5196)		PresetCode (Preset Code)		InforSalesOrderPreset	n/a	n/a	OTHER
SalesOrderView	Sales Order Entry (SOE)		SalesOrder (Sales Order Transaction Ref)		InforSalesOrder	SalesOrder	[InforChartOfAccounts, InforCustomerPartyMaster, InforItemMaster]	BOD
SalesPriceBookView	Sales Price Book (VW5498)		BookCode (Book Code)		InforSalesPriceBook	n/a	n/a	OTHER
SalesTypeView	Sales Types (VW5186)		TypeCode (Type Code)		InforSalesType	n/a	n/a	OTHER
ScheduledPaymentSetupView	Scheduled Payment Setup (VW5011)		SetupCode (Setup Code)		InforScheduledPaymentSetup	n/a	n/a	OTHER
SourceSystemJournalEntryView	Journal Inquiry (SALQ)	SALQ	JournalNumber (Journal Number)		n/a	n/a	n/a	BOD_COMPONENT
StatementLayoutView	Financial Statement Layouts (VW5653)		LayoutCode (Layout Code)		InforStatementLayout	n/a	n/a	OTHER
SupplierView	Supplier (VW5148)		Supplier (Supplier Code)		InforSupplierPartyMaster	SupplierPartyMaster	[InforChartOfAccounts, InforPurchaseType, InforWarehouse]	BOD
TaxCodeView	Tax Details (VW5640)		Code (Code)		InforTaxCode	n/a	n/a	OTHER
UnitOfMeasureView	Unit of Measure Labels (VW5175)		LabelCode (Label Code)		InforUnitOfMeasure	n/a	n/a	OTHER
ValueBookView	Value Book (VW5498)		ValueCode (Value Code)		InforValueBook	n/a	n/a	OTHER
WarehouseView	Warehouse Setup (VW5122)		WarehouseCode (Warehouse Code)		InforWarehouse	n/a	[InforAddress]	OTHER

Part 2 Installation Reference

Chapter 9 Requirements and planning

9

Introduction

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.

For an overview of the architecture and planning considerations for the deployment of the software, refer to the SunSystems Architecture and Planning Guide.

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 might need to increase the minimum requirements. Careful consideration must be given to your current requirements and hardware capacity. The following factors are key areas 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 number of computers currently on the network
- 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

The following tables show the recommended operating systems to use:

Installation Type	Layers	Recommended version of Windows
Stand-alone	All	Microsoft SQL Server 2008 R2, Microsoft SQL Server 2012, Microsoft SQL Server 2014, or Microsoft SQL Server 2016 Database Server, and Reporting Services. Standard Edition or above.
Two-Tier	Client	Windows 10, Windows 8.1, Windows 7.
	Application and Database	Windows Server 2012 (Standard or Datacenter), Windows 2008 Server R2 (Standard or Enterprise), MS-SQL Server 2008 R2, MS-SQL Server 2012, MS-SQL Server 2014 or Microsoft SQL Server 2016 Database Server, and Reporting Services. Standard Edition or above.
Three-Tier	Client	Windows 10, Windows 8.1, Windows 7.
	Application	Windows Server 2012 (Standard or Datacenter), Windows 2008 Server R2 (Standard or Enterprise)
	Database	Windows Server 2012 (Standard or Datacenter), Windows 2008 Server R2 (Standard or Enterprise), MS-SQL Server 2008 R2, MS-SQL Server 2012, MS-SQL Server 2014 or Microsoft SQL Server 2016 Database Server, and Reporting Services. Standard Edition or above.

RDBMS support

SunSystems version 6.2 is supported with the following relational database systems:

- Microsoft SQL Server 2016.
- Microsoft SQL Server 2014.
- Microsoft SQL Server 2012.
- Microsoft SQL Server 2008 R2 (Standard, Enterprise and Workgroup editions), 32-bit and 64-bit versions.

Before you upgrade to a new Microsoft SQL Server service pack, contact your regional support representative to ascertain the support status.

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: Although SunSystems can be configured to operate against a clustered database server configuration, the application is not cluster-aware. In the event of a fail-over, application services should be restarted, and clients should be logged out and then logged back in.

Networking

Microsoft TCP/IP is the recommended protocol for use with SunSystems. Appropriate IP addressing and name resolution must be in place for SunSystems to function correctly.

If the SunSystems application is behind a firewall, refer to the rest of this guide about how you can configure the SunSystems settings.

All ODBC components and MDAC components that are required by SunSystems are installed and configured as part of the installation process.

Chapter 10 Creating a secure SunSystems installation

10

Introduction

This section 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

Security model

SunSystems can be configured to use two different authentication methods. The simplest requires the user to enter their credentials upon accessing SunSystems, which are held encrypted in the database and validated to authenticate the user. 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.

For more information, refer to the SunSystems Connect Help and the SunSystems Integration Group.

Permissions and ownership

Users must have 'read' permissions and 'execute' permissions on the SunSystems program folder, and full permissions on the following folders:

Folders	Usage
C:\Temp	Temporary folder used for server context information and by Reporting
_back	Used by SunSystems at runtime
_print	Used by SunSystems at runtime
_work	Temporary working directory
ssc	Used by SunSystems Connect
%ALLUSERSPROFILE%\Infor\ (Including all subfolders)	Used by SunSystems at runtime, logging and storing temporary files

With regards to the operating system, the following permissions should be set: 'Read' and 'execute' to the SunSystems service accounts in **\Winnt\System32**.

Microsoft SQL Server

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.

Because many server-to-server activities can be performed only with a domain user account, you should use a domain user account on this service.

All domain user accounts must have permission to do the following:

- 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 the following 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 should 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 every user.

To secure the file system, use the SUBINACL utility, which is provided by Microsoft, to ‘lock down’ the file system. You can then 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 is supported to work 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).
- Citrix XenApp supports Internet firewalls that can be used to restrict Internet access to the Citrix XenApp server.
- Users can be required to enter a user name and password to run an application (explicit user access only).
- Citrix and most web professionals recommend that you either disassociate your website from your production system, or rigorously restrict external access. Any system accessible through the Internet is by definition a security risk and might give anyone unauthorized access to your production site through the web. Therefore, unless you have robust security and plan to use this

with an Intranet, you should keep your web server on a separate network loop outside the firewall, if you have one.

- 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.

Publishing applications

SunSystems does not support anonymous user access. This ensures that access to SunSystems is restricted to domain users only.

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

Note: SunSystems supports different Hot Keys. For information about using the published application Hot Keys, refer to Citrix documentation.

Configuring folder and registry permissions

SunSystems downloads forms on a per user basis in the **multipleclientfile** folder. It is important that the users who download these forms have the correct privileges in the **multipleclientfile** folder.

In SunSystems, everyone has full control of the following folders:

- In Windows 2008, and Windows 7: **ProgramData\Infor\SunSystems.**

If SunSystems on Citrix XenApp is published with domain user access, complete the following steps:

1. Give write access to SunSystemsClients group on the location where reports are located, if they are outside of SunSystems folder hierarchy.
2. Transfer desk creates files when running export. Systems administrator should configure write access to SunSystemsClients group for this location.

Deployment suggestions

Consider having a separate partition for user data. If users are allowed to store data in the same partition as the system files and print queues, when the partition is full, they lose the ability to print, and the SunSystems application might become unstable. By keeping the data in a separate directory, an out-of-space error is generated 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.

Registry security

You should set up a policy to be 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 normalizes the usage of server resources by each user by smoothing out the normal CPU peaks that most applications have. CPU optimization is based on Citrix XenAppreserving approximately 20 percent of the CPUs for automatic optimization. Therefore, no single session controls the majority of CPU processing. When CPU power is borrowed from idle sessions or inactive sessions, it can be reallocated when that session becomes active again. Invoking CPU optimization is typically beneficial, and should not have any noticeable negative effect.

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

Memory optimization and SunSystems

Application memory is not a primary bottleneck in SunSystems, but on a different hardware platform with more processing power, the bottleneck could shift from CPU to application memory.

Memory optimization is recommended to turn on in SunSystems deployment on Citrix XenApp.

SpeedScreen and SunSystems

SpeedScreen technology is designed to optimise the graphics-based applications on Citrix, such as 3D graphics. However, this technology also helps to use the network bandwidth in a better way. We recommend that you turn on the SpeedScreen setting on the SunSystems deployment on Citrix XenApp.

Additional scalability recommendations

1. 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.

Hardware and Configuration Recommendations

1. Dual processor computers provide the best results. For 32-bit systems, more than two processors provide diminished returns.

At least 4 GB of RAM are required. Memory extension with /PAE option may help, but too much memory with /PAE option might cause performance loss.

Set Static page file size. To prevent resizing, minimum and maximum settings should be constant.

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, for example:

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

Chapter 11 Database administration

11

Introduction

Business Unit Administration (BUA) makes some of the Database Administration functions available from the SunSystems Navigator. The SunSystems Installation DVD allows you to carry out additional database administration tasks on an existing installation.

The database processing procedure should start when the SunSystems Database Server link is invoked from the SunSystems installation screen. The SunSystems installation screen is displayed automatically when the DVD is inserted into the machine. If the SunSystems installation screen does not start automatically, either locate the DVD drive in Windows Explorer and double-click **Setup.hta** or run **D:\Setup.hta** from a command prompt, where **D:** is your DVD drive.

After you start the database installation, you must select the database operation required.

SunSystems Database Utilities

SunSystems Database Utilities > Create

Creating a new SunSystems domain database

From SunSystems Database Utilities, select Create > a new SunSystems Domain database to create a new SunSystems domain database on the local machine.

All SunSystems databases must be registered in a SunSystems domain. Therefore, the SunSystems Domain database must be created together with, or before, SunSystems databases in the same SunSystems domain.

This option is used if the SunSystems Domain database is to be on a separate database server to the database that is used for the SunSystems database(s) in the same SunSystems domain.

A subset of the steps for a full installation is used for this operation. Although a subset of steps is required, the layout of dialog boxes that are displayed and the information that is required in each dialog box is the same as for a full installation. For instructions about the full installation procedure, refer to the ‘Installing SunSystems in a multi-tier environment’ section of this installation guide.

Creating a new SunSystems Business Unit Group

Note: If you need to run this utility remotely, first ensure that your local machine has the Microsoft SQL Server Tools installed. The utility uses SQL Server client connectivity components (specifically `bcp.exe`) to connect to the SQL Server instance on the remote machine, and will fail if these have not been installed.

From SunSystems Database Utilities, select Create > a new SunSystems Business Unit Group. This option uses scripts to create a SunSystems business unit group on the local machine, which is then registered:

- In a new SunSystems domain, by creating a new SunSystems domain database on the local machine. This happens if the domain database does not already exist.
- In an existing SunSystems domain through an existing SunSystems domain database.

This option is used, as an alternative to creation during an Application Server installation, if the SunSystems Business Unit Group is to be created as follows:

- On a server remote from the Application Servers in the SunSystems domain.

As an addition to those that were created/attached during Application Server installations for the SunSystems Domain.

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

A subset of the steps for a full installation is used for this operation. Although a subset of steps is required, the layout of dialog boxes that are displayed and the information that is required in each dialog box is the same as for a full installation. For instructions about the full installation procedure, refer to the ‘Installing SunSystems in a multi-tier environment’ section of this installation guide.

Creating a new SunSystems Security database

From SunSystems Database Utilities, select Create > a new SunSystems Security database to create a new SunSystems domain database on the local machine.

A subset of the steps for a full installation is used for this operation. Although a subset of steps is required, the layout of dialog boxes that are displayed and the information that is required in each dialog box is the same as for a full installation. For instructions about the full installation procedure, refer to the ‘Installing SunSystems in a multi-tier environment’ section of this installation guide.

Importing a pre-configured SunSystems Business Unit Group

From SunSystems Database Utilities, select Create > a pre-configured SunSystems Business Unit Group.

Do not attempt to run this function to create a database on a remote machine. Importing a pre-configured SunSystems business unit group only works on the local machine and is registered as follows:

- In a new SunSystems domain by creating a new SunSystems domain database on the local machine.
- In an existing SunSystems domain through an existing SunSystems domain database.

This option is used, as an alternative to attaching during an Application Server installation, if the preconfigured SunSystems business unit group is to be attached/installed as one of the following:

- On a server remote from the Application Servers in the SunSystems domain.
- As an addition to those created/attached during Application Server installations for the domain.

Registration of a SunSystems business unit group is prevented if the database contains a business unit that is already registered in the SunSystems domain. Business units in a SunSystems domain must be unique.

Registering a second SunSystems database automatically converts the SunSystems domain to a multiple SunSystems database environment.

A subset of the steps for a full installation is used for this operation. Although a subset of steps is required, the layout of dialog boxes that are displayed and the information that is required in each dialog box is the same as for a full installation. For instructions about the full installation procedure, refer to the Installing SunSystems section of this installation guide.

SunSystems Database Utilities > Upgrade

Pre-Upgrade Outstanding Transaction Check

This check should be run before you perform an upgrade. This check runs as part of the upgrade process and prevents the upgrade from progressing if it returns existing entries of outstanding transactions.

The checks performed are as follows:

- Checks for the existence of any Held Journals
- Checks for the existence of any entries in the Recover Failed Postings function (RFP)
- Checks for any entries in the ledger import queue
- Checks for the existence of any entries in the data audit.

Remove work tables

This option will run the stored procedure, SSP_DROP_WORK_TABLES, against your selected business unit group. This will remove temporary work tables and views from the database which can greatly improve the performance of the Upgrade Business Unit section of the upgrade process.

See the SunSystems Upgrade Guide for more details.

A SunSystems Security database

This option will upgrade the security database. See the SunSystems Upgrade Guide for more details.

A SunSystems domain database

This option will upgrade the domain database. See the SunSystems Upgrade Guide for more details.

A SunSystems Domain database forcing all scripts to be reapplied

This option is to upgrade the domain database and force all scripts to be applied to the database whether they have changed or not. This is slower than selecting ‘a SunSystems domain database’ and should only be used under instruction from Infor Support or your channel partner. See the SunSystems Upgrade Guide for more details.

A SunSystems Business Unit Group

This option upgrades the business unit group database, and only upgrades one business unit group so will need to be run for each business unit group in your domain. See the SunSystems Upgrade Guide for more details.

A SunSystems Business Unit Group forcing all scripts to be reapplied

This option is to upgrade the business unit group database and force all scripts to be applied to the database whether they have changed or not. This is slower than selecting ‘a SunSystems Business Unit’ and should only be used under instruction from Infor Support or your channel partner. See the SunSystems Upgrade Guide for more details.

Custom Forms

This option enables you to upgrade your custom forms. See the SunSystems Upgrade Guide for more details.

SunSystems Database Utilities > Domain DB Utilities

The SunSystems Database Utilities > Domain DB Utilities gives access to the utilities that are available for use against a SunSystems domain database. After you select this option, you can choose from the following options.

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.

Remove a SunSystems Business Unit Group from a SunSystems Domain

The Remove a SunSystems Business Unit Group option removes a SunSystems business unit group from a SunSystems domain and optionally deletes the database if it is held on the local machine.

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

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

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

After you select the Remove a SunSystems Database option, carry out the following:

- Specify whether the business unit group should be removed from the SunSystems domain, or removed and deleted.
- Specify the location for log files.
- Select the datasource name used for the SunSystems Domain database for the SunSystems domain 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 SunSystems business unit group to be removed and optionally deleted.
- Confirm that the database and server instance details are correct.
- Confirm that the SunSystems domain and SunSystems 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.

Business Unit groups parameter maintenance

The Business Unit Group Parameter Maintenance option provides facilities for the maintenance of parameters on existing SunSystems Domain databases and SunSystems business unit groups.

The following options are then available.

Query database file groups

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

Re-link all the SunSystems Business Unit Groups to a SunSystems Domain

The Re-Link SunSystems Database option re-links the existing SunSystems business unit groups to the existing SunSystems domain database. This utility allows you to move the SunSystems domain database and SunSystems business unit groups from one server to another.

Load difference tables

This option reloads the difference table in a specified SunSystems database with the data dictionary differences from a previous version of SunSystems. This information is required for a Custom Upgrade and allows you to create a SunSystems database, either from scripts or by attaching a preconfigured 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 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.

SunSystems Database Utilities > SunSystems DB Utilities

The SunSystems DB Utilities menu gives access to the utilities that are available for use against a SunSystems database. After you select this option, you can choose from the following options:

Structural integrity check

This option checks the structural integrity of the SunSystems business unit group against a master template for that database version.

You have the option to run further database utilities.

Referential Integrity Check - SunSystems Business Unit Group only

This option checks the integrity of a SunSystems business unit group against a master template for that database version. You must specify the SQL Server Instance Name and the SunSystems business unit group.

The integrity check is run and any errors or warnings are displayed.

Note: The Referential Integrity Check should be run before you upgrade so that any errors can be identified before a full upgrade.

You have the option to run further database utilities.

Referential Integrity Check - SunSystems Business Unit Group referenced to domain

This option carries out a referential integrity check of a SunSystems business unit group. You must specify the SQL Server Instance Name and the SunSystems database.

The integrity check is run and any errors or warnings are recorded in the RI_ERR table.

You have the option to run further database utilities.

Query database file groups

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

SunSystems Database Utilities > Form Actions

Import forms into a SunSystems Domain

This option imports forms into a SunSystems domain database.

Export forms form a SunSystems Domain

This option exports forms from a SunSystems domain database.

Remove forms from a SunSystems Domain

This option removes forms from a SunSystems domain database.

SunSystems database migration

SunSystems databases can be migrated from one database server to another. This process requires database administrator privileges and there are some prerequisites as well. The database migration process requires downtime of SunSystems.

The prerequisites are as follows:

- Source and destination SQL Server version should be same.
- Source and destination Windows version, service pack level and operating system language should be same.
- The user performing the database migration should have Windows and database administrator privileges.
- All the SunSystems users should log off and all the SunSystems windows services should be stopped.
- Create SQL Server Login for SunSystemsServices and SunSystemsClients groups on the target database server. The windows group names should be same as used in the source SQL Server.

Follow the database upgrade procedure detailed in the SunSystems Upgrade Guide. This procedure provides the detailed steps required to migrate the database from one server to another.

Changing the Port Number

If TCP port in SQL Server has been changed, for example, from 1443 to 8030:

1. Open the **Global.config** file in **ProgramData\Infor\SunSystems\Security**.
2. Change the **<port>** number in the **<sql-store>** section to **8030**. Save and close the file.
3. Change the database port to **8030** in **DOMN_DSRCE_CONFIG**.
4. Ensure that the **ODBC SUNDOMAIN DSN** is using port **8030**.
5. Restart the SunSystems Security service.
6. Run Property Editor (PPE).
7. Change the **system/jdbc/** url from

   `jdbc:sqlserver://{0}/{1};appName=Connect`

   to

```
jdbc:sqlserver://ACSUN:8030/{1};appName=Connect
```

Note: The argument {1} should stay as it is.

8. Restart the SunSystems Connect Server service.
9. Login to SunSystems and check that Transfer Desk (TRD) is working.

Chapter 12 Microsoft SQL Server

12

Introduction

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

Caution: Before you start, you should ensure that you have administrator access to the SQL Server machines and Domain Controller machine to configure, or to verify, the linked server environment.

Caution: We do not recommend installing SunSystems components on the Active Directory Domain Controller. In addition, Microsoft advise against on the Domain Controller.

Note: SunSystems does not support stand-alone or 2-tier setup in a linked server environment.

Note: When you create a new Linked Server, in the Server Options, set RPC=True and RPC Out=True; otherwise error messages are displayed when you set the Application Role in User Manager.

Note: To serialize SunSystems in a linked server environment, open the serialization file using Notepad and manually enter the details into SunSystems Serialization (ZZS).

Note: If a SQL Server named instance is used, SQL Server Browser Service is required to connect to the server.

Reconfiguring SQL Server properties

Microsoft SQL Server must be reconfigured to allow distributed transactions to run:

1. From the Windows Start menu click Programs > Microsoft SQL Server > SQL Server Management Studio.
2. Expand the SQL Servers node, and right-click the SQL Server instance that either already holds the SunSystems Domain database, or, if not yet installed, the one that you intend to use.
3. Click Properties and then click the Connections panel.
4. Select the Allow remote connections to this server check box and the Require distributed transactions for server-to-server communication check box.

If not already selected, select Configured values.

Configuring the linked server connections

To allow SunSystems to correctly run distributed transactions, such as the SunSystems applications software Installer, SunSystems Business Unit Create, Setup, and Copy, a linked server connection must be created on the database servers.

The Configuring the Distributed Transaction Coordinator Service section describes the diagnostic tests that should be run, and the actions to be carried out to verify that the initial configuration is correctly working. A later section describes the diagnostic tests and actions that should be run to verify the linked server connection in SunSystems applications.

Configuring the linked server connection on the database server

1. Log on to SQL Server Management Studio using an administrator account (sysadmin rights on SQL Server)
2. Expand the SQL Server instance node and click the **Server Objects** node.
3. Right-click **Linked Servers** > **New Linked Server > General**.
4. Specify **Linked Server** as the other database server name.
5. Click **SQL Server** > **Security**.
6. Select **Be made using the login's current security context**.
7. Ensure that delegation is selected for the servers involved, and the relevant Service Principal Names are present, in Active Directory. The connection relies on Kerberos authentication.
8. Verify the linked server configuration by running the system stored procedure **sp_linkedservers** using the master database. Two rows will be returned: one for the local server and the other for the remote server.

Configuring the Distributed Transaction Coordinator service

To allow distributed transactions to run, the Distributed Transaction Coordinator service must be configured on both database servers.

Note: If the operating system on database servers is restored from a single image, DTC will require reinstallation on all database servers involved in linked servers. To do so, follow Microsoft Windows online Help. If the operating system on database servers was installed from installation media, DTC reinstallation is not required.

On the database server, complete the following steps:

1. From the Windows Start menu, click **Control Panel > AdministrativeTools > Component Services**.
2. In Component Services, expand **Component Services** and double-click **Computers**.
3. Right-click **My Computer,** and from the resultant shortcut menu, click **Properties**.
4. Click the **MSDTC** tab. Verify that Use local coordinator is selected.

5. Click the **Default Protocols** tab and set DCOM Protocols to Connection-orientated TCP/IP.
6. Click **My Computer**, expand Distributed Transaction Coordinator. **Local DTC**, Properties.
7. Select Security. Ensure that the following check boxes are selected:
    - Network DTC Access
    - Allow Remote Clients
    - Allow Inbound
    - Allow Outbound
    - No Authentication Required
    - Enable Transaction Internet Protocol (TIP) XA and SNA LU 6.2 Transactions.
8. Ensure that DTC Logon Account is set to **NT Authority\NetworkService** and click OK.
9. In the MSDTC service message box, if displayed, click Yes to restart the service.
10. Click OK in the DTC Console Message dialog.
11. Click OK in the System Properties dialog.

Note: Sometimes you must start the DTC service before you start the Microsoft SQL Server service so that the linked server distributed queries work.

12. Repeat these steps for the other database server.

Verifying the linked server connection

The linked server connection verification for SunSystems consists of running the following SunSystems functions:

- Business Unit Administratrion (BUA). Create a new Business Unit Group in the linked server location. Put online.
- Business Unit Administration copy an existing Business Unit to the linked server Business Unit Group.

Microsoft SQL Server clustering installation

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

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 and in User Manager, Operator Activity, users will need to be cleared, and these users will have to log into SunSystems again.

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 by SunSystems with SQL Server.

Specifying a DNS CNAME record as a server alias

SQL Server Alias is not supported by Microsoft JDBC driver for SQL Server, which is used by SunSystems 6.2.1.

We recommend that you specify a DNS CNAME record to provide a server alias, and set up a standby database server, in case of a server failover.

Prerequisites

Prior to specifying a DNS CNAME record, you must ensure:

- SunSystems 6.2.1 is installed in a multi-tier 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.

Domain controller setup

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

Database server setup

1. Create a Linked Server in SQL Server Management Studio:
    a. On the General page, in the Linked server section, specify the name of the instance of SQL Server that you are linking to. 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. On the Security page, select **Be made using the login's current security context**.

2. Open SunSystems Database Utilities:

    a. 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.

    b. Select **Relink Details**. Specify the Instance name, for example, `DBSERVER\INSTANCE1`, and the SunSystems Business Unit Group Database name.

    c. 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 SQL Server Configuration Manager. Select **SQL Server Network Configuration** > **Protocols** for `INSTANCE1` > **TCP/IP**. In TCP/IP Properties, click **IP Addresses**. TCP Dynamic Ports in IPAll specifies the SQL Server listening port. Make a note of the port number. By default, the port is 1433.

4. 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.

Note: If you are installing SunSystems with Microsoft SSRS on the same database instance, then you must specify CNAME\<Instance> in SunSystems Reporting Services.

Altering an existing SunSystems Installation to use CNAME to refer to the database server

Application server setup

1. Open File Explorer and browse to **\ProgramData\Infor\SunSystems\Security**. Open **Global.Config** and specify:

    <sql-store>`DBSERVER\INSTANCE1`**</sql-store>**.

    Restart the SunSystems Security service.

2. Log into User Manager using the SunSystems Administrator account. Open **Settings** > **SunSystems** > **Configure**. Specify `DBSERVER\INSTANCE1` and click **Test connection**. Click **OK** to save your changes.

3. Run `\Windows\SysWOW64\Odbcad32.exe`. Configure the SunSystems System DSN Server to include the new database server instance, for example, `STANDBYDBSERVER\INSTANCE1`. Do not specify your CNAME. Click **Finish** to save your changes.

4. Restart IIS using IIS Manager, or by using the IISReset command-line utility.

5. Restart all SunSystems services.

SunSystems Reporting Services

Note: If SunSystems has been set up with Microsoft SSRS on the database server, then you must specify CNAME in SunSystems Reporting Services.

1. Edit the `DOMN_VRTL_HOST` table. Specify CNAME as the `ACTUAL_HOST_NAME` value, where `VRTL_HOST_NAME = ms-app-ssrs` and `ms-app-ssrs-rm`.
2. Use IIS Manager or the IISReset command-line utility to restart IIS on the Application Server.
3. Specify CNAME in Microsoft SSRS if it is not installed on the database server:
    a. Open the Report Server Database Configuration Wizard. Select **Database** > **Change Database** > **Choose an existing report server database**. Click **Next**.
    b. Specify the Database Name, for example, `DBSERVER\INSTANCE1`. Select **Current User – Integrated Security** as the Authentication Type. Click **Test Connection**. Click **Next**.
    c. Select the Report Server Database, for example, `ReportServer$INSTANCE1` and click **Next**.
    d. Select **Service Credentials** as the Authentication Type and click **Next** to finish.
4. Select **Encryption Keys**. Click **Delete** to Delete Encrypted Content. Click **OK**. Restart the Report server.

Note: Deleting the encrypted content may affect other systems using Microsoft SSRS.

Set up the standby database server

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

1. Open SQL Server Management Studio. Open **Database Properties** for the SunSystems Security database and select **Options**. Select **True** for Broker Enabled. Click **OK** to save your changes.
2. Open SunSystems Database Utilities.
3. Select **Database Server** > **Re-line all the SunSystems Business Unit Groups to a SunSystems Domain**. Specify a datasource name that includes an instance name, for example, `DBSERVER\INSTANCE1`. Click **OK**.
4. Select **Relink Details**. Specify the instance name, for example, `DBSERVER\INSTANCE1`. Specify the SunSystems Business Unit Group Database name.
5. 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.

In the event of a failover

1. Update CNAME in DNS as the new database server/instance.
2. Run `\Windows\SysWOW64\Odbcad32.exe` to specify the new database server instance, for example, `STANDBYDBSERVER\INSTANCE1`, in the SunSystems system DNS server. Do not use the CNAME.

   Note: This step must be completed manually after a failover because the ODBC data source cannot be set to the DNS CNAME.

   Note: The Application server retains the CNAME\INSTANCE1 server entry, for example, `DBSERVER\INSTANCE1`.
3. Use IIS Manager or the IISReset command-line utility to restart IIS on all SunSystems servers.
4. Restart all SunSystems services on all SunSystems servers.

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

Chapter 13 SunSystems Connect

13

Introduction

SunSystems Connect (SSC) provides an Extensible Markup Language (XML) and Simple Object Access Protocol (SOAP) interface through which developers can access SunSystems data and core functionality.

Software requirements

Microsoft Windows 2008 R2 or 2012 (Standard or Enterprise) is required for the SunSystems Connect and Automation Desk installation. Where a third party application is written that makes a SOAP call to SSC, the machines on which it is run must have the correct version of all the necessary supporting software installed, for example, the correct Microsoft SOAP Toolkit.

Installing SSC

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

Note: SunSystems Connect functionality consists of Property Editor (PED) and Component Manager (CM). Component Manager can be run only on a server with the client installed on it. Therefore, Component Manager (CM) cannot be run on the client machine, in a client-only installation. Property Editor can be run on a client machine; however, several properties are not applicable.

Note: The SSC service account must be a valid domain user account and should be the same as that nominated for the SunSystems Session Manager service. A valid set of print drivers should be installed and must be the printer that is set in Document Format Setup.

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 B.

Changing SSC TCP port value

By default, SSC is configured on TCP port 8080. To change this value, use Property Editor (PPE) function. Select tomcat, http_connector, port, and Modify the port value. Restart Sunsystems Connect Server. As this property is held locally, you have to change it on application servers and all client machines.

The following registry setting also needs to be changed on application servers and all client machines:

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\SunSystems\Core\5.1\Comms\ConnectServicesListenerPort

Chapter 14 Scalability: Application servers and SunSystems Connect

14

Introduction

SunSystems can be implemented in several configurations and therefore offers the flexibility to plan and deploy the product in a variety of scenarios that are tailored to meet specific requirements. For the more complex or demanding implementations of SunSystems, several options are available to allow further growth of the infrastructure.

This section outlines some of these options, by introducing the concept of multiple application servers. However, this is not to be confused with clustering for failover that is limited to the database server tier and is supported for SQL Server by Microsoft. Clustering for failover is documented at the end of this section.

Note: Planning a scalable infrastructure for SunSystems is a task suited to experienced consultants who understand the dynamics of the software. SunSystems is a sophisticated application and the way it is used can affect the way it should be deployed. You should consult your SunSystems software provider for such implementations.

Static load balancing

The simplest way to achieve scalability is the addition of another server to act as an application server. In this scenario, an additional server is installed with the SunSystems application software and a selected number of clients moved from pointing to their original server to the new server.

The benefits of static load balancing are as follows:

- It is easy to set up
- No additional hardware or software required.

However, you should be aware of the following before you begin with this type of implementation:

- It takes no account of comparative server load
- If a server fails, client must be manually redirected to an active server.

Hardware-based dynamic load balancing

This uses dedicated hardware, such as a router, that can be configured to share IP traffic between servers. Hardware capabilities will vary, but the key requirement is the ability to set server affinity for the duration of session activity.

The benefits of hardware-based dynamic load balancing are as follows:

- It shares the requests between servers
- You can add and remove servers with no server configuration
- No client reconfiguration is required
- Offers more sophisticated load distribution models to choose from.

You should be aware that additional hardware is required.

Caution: Due to the complexity of this configuration, seek advice from your SunSystems software provider before you start to implement hardware load balancing.

Software-based dynamic load balancing

This uses third party software, such as the Windows Network Load Balancing (NLB) available with the Microsoft SQL Server 2008 Enterprise Server products. Using such software, you can configure multiple servers to be seen as a single IP address by the rest of the network. Clients must only point to this 'virtual' IP address and the NLB decides which server processes the request.

The benefits of software-based dynamic load balancing are as follows:

- No additional hardware is required.
- It shares the requests between servers.
- You can add and remove servers with minimal effect on service.
- No client reconfiguration is required.

However, you should be aware of the following:

- Licensing costs can be expensive.
- A basic load distribution algorithm is used.
- It can be difficult to set up.

Two Network cards (NICs) are required for each server.

Prerequisites for application server load balancing

Before you start load balancing configuration on SunSystems application server, check the following prerequisites:

- The application machines are running Windows 2012 or Windows 2008 R2.
- Windows Network Load Balancing component is installed on every application server that will be part of the cluster.

- If you are configuring load balancing using Unicast, then every application server machine must have 2 Network Interface Cards (NIC).
- Static IP addresses are available for each machine, as given in the following section.
- There is a DNS server available on the network.
- Each application server name can be resolved by DNS.
- The client machines are running Windows 7 or Windows 8.

Configuring software-based load balancing with Windows Server 2008, Windows Server 2008 R2 or Windows Server 2012

This section provides details for configuring SunSystems with load balancing. For the steps involved in Network Load Balancing Manager configuration, refer to relevant Microsoft Windows documentation.

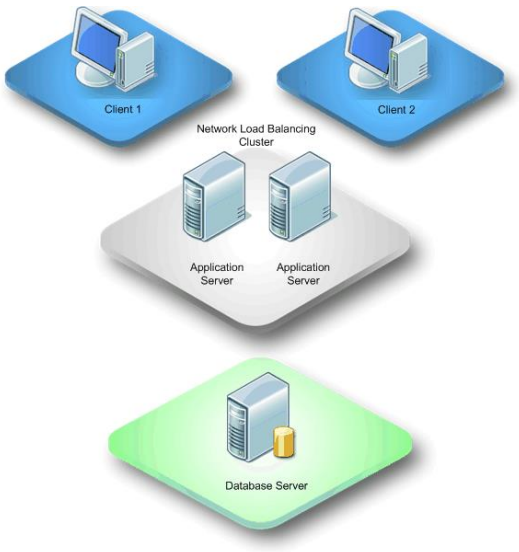
Note: Microsoft has advised that although the Network Load Balancing (NLB) functionality in Windows Server 2012 is mostly the same as Windows Server 2008 R2, some task details have been changed in Windows Server 2012.

For network load balancing configuration, refer to the “Port Rules Tab for Application Load Balancing” section.

Setup environment

The environment is shown below and in more detail in the table.

Note: For brevity, in this scenario only two clients and two servers are used.



Test environment	Operating system	Computer name	IP address	
DATABASE SERVER	Windows 2008 R2 Server	DB	10.10.10.30	
APPLICATION SERVER 1 Windows 2008 R2 Server		AD1	1st NIC	10.10.10.31
			2nd NIC	10.10.10.40
			Load Balance IP	10.10.10.36
APPLICATION SERVER 2 Windows 2008 R2 Server		AD2	1st NIC	10.10.10.32
			2nd NIC	10.10.10.41
			Load Balance IP	10.10.10.36
CLIENT 1	Windows 7	CL1	10.10.10.33	
CLIENT 2	Windows 7	CL2	10.10.10.34	

The dedicated IP address for the machines and the Load Balanced IP addresses must be static IP addresses, not DHCP addresses. TCP/IP is the only network protocol that should be present on the cluster adapter. Do not add any other protocols, such as IPX, to this adapter.

Each of the two Application Server NICs is defined with a unique IP address. The NIC dedicated for Load Balancing is defined with two IP addresses: one for the card, such as 10.10.10.40; and one for the Load Balance Cluster, such as 10.10.10.36. This Cluster IP address exists on both Application Servers.

Installing network load balancing if it was previously uninstalled

Cluster parameters tab

- Primary IP address

  This is a virtual IP address and must be set identically for all hosts in the cluster. This IP address is used to address the cluster as a whole, such as 10.10.10.36.

- Subnet mask

  This denotes the subnet mask for the IP address specified, such as 255.0.0.0.

- Full Internet name

  This specifies a full Internet name for the Network Load Balancing cluster. The name should be resolvable to the cluster's primary IP address through the DNS server or Hosts file; for example, **cluster.rddomain.rd.com**.

- Network address

This specifies the network address (MAC address) for the network adapter to be used for handling client-to-cluster traffic. Network Load Balancing automatically generates the network address based on the cluster's primary IP address.

- Multicast support

  This check box should be selected if you are using a single net adapter. However, because this topic covers the use of two network adapters, this check box must not be selected.

- Remote password

  This specifies a password to be used for restricting access to the cluster from remote, networked computers running Windows 2008 using the `Wlbs.exe` cluster control program.

- Remote control

  This specifies whether remote control operations are enabled. This check box must remain cleared.

Host parameters tab

- Priority (Unique host ID)

  This ID is for handling default network traffic that is not otherwise specified on the **Port Rules** tab. The ID is used in case a host in the cluster goes offline, and determines which host in the cluster takes over handling this traffic, if required. On each application server, this number should be unique, such as AD=1, AD2=2.

- Initial cluster state

  This check box should be selected so that Network Load Balancing can start and join the cluster when the Advance Server is started.

- Dedicated IP address

  This is the unique IP address for the application server used for network traffic that is not associated with the cluster. This IP address is the original IP address assigned to the Application Server, such as 10.10.10.40 or 10.10.10.41.

- Subnet mask

This denotes the subnet mask for the IP address specified, such as 255.0.0.0.

Port rules tab

Note: The following setting should be identical on all Application Servers in the Load Balancing Cluster. If you are implementing Application Load Balancing in a Citrix environment, skip this section and refer to the Port Rules Tab for Citrix section.

- Port range

  This specifies the TCP/UDP port range that a port rule should cover. Port numbers in a range of 0 to 65,535 are currently supported. This can be left as the default.

- Protocols

This allows you to choose the specific TCP/IP protocol that a port rule should cover: TCP, UDP, or both. The default is Both.

- Filtering mode

  Select Multiple hosts for both Application Servers to handle SunSystems traffic. This specifies that multiple hosts in the cluster handle network traffic for the associated port rule.

- Affinity

  Select Single. This option specifies that Network Load Balancing directs multiple requests from the same client IP address to the same cluster host. This is the default setting for affinity.

- Load weight

  Set the load weight to Equal so that both Application Servers equally distribute SunSystems traffic.

- Handling priority

This option is not used when the Filtering mode is set to Multiple hosts.

Network load balancing configuration test in Windows Server 2008, Windows Server 2008 R2 and Windows Server 2012

1. To check whether the Load Balancing Cluster IP address is accessible by the network, a `ping` test can be performed from within a command prompt screen. On a client machine, do the following:

   a. Click the Windows Start button and click the Run icon.

   b. Type **CMD** in the Run dialog box and click OK.

   c. When the screen is loaded, type **PING** followed by the cluster IP address. For example, **PING 10.10.10.36**. One of the following messages is displayed:

6. Successful Reply from 10.10.10.36
7. Unsuccessful Request Time Out.

If communication is unsuccessful, recheck Load Balancing Setup and try the test again.

Repeat the Network Load Balancing configuration steps on each Application Server to be used in the Network Load Balancing cluster.

You can check that each Application Server joins the Load Balance cluster:

   d. On an Application Server, open Event Viewer. This is located in the Control Panel >> Administrative Tools.

   e. An entry should exist where the Source tab indicates WLBS (2008 / 2008 R2) or NLB (2012). Double-click the entry. Any errors produced by Load Balancing are shown. If the Application Server has joined the Load Balance group, it shows that server 1 has converged with server 2.

f If the convergence entry does not exist and only one server is mentioned, recheck Load Balancing Setup and recheck Event Viewer.

To resolve the Load Balancing Cluster name, such as `cluster.rddomain.rd.com`, to the cluster IP address, such as 10.10.10.36, a DNS entry must be manually created on the DNS Server by a Server Administrator. This creation allows IP and name resolution.

After this DNS entry has been created, perform a `ping` test from within a command prompt screen. On a client machine, do the following:

g Click the Windows Start button and click the Run icon.

h Type `CMD` in the Run dialog box and click OK.

i When the screen is loaded, type `PING` and the cluster DNS name. For example, `PING` cluster. One of the following messages is displayed:

8. Successful Reply from 10.10.10.36
9. Unsuccessful Request Time Out.

j If communication is unsuccessful, recheck Load Balancing Setup and try the test again.

SunSystems configuration in a load balancing environment

Note: The following sections are applicable to all Implementation Methods: Static Load Balancing, Hardware-Based Dynamic Load Balancing, and Software-Based Dynamic Load Balancing.

To remove affinity from a single Citrix/application server, the following port rules are recommended to enhance load balancing ratios.

Note: The following table is a guide that covers modifying port rules for four load balanced application servers. The same scenario exists for fewer or more application servers, although the port ranges vary depending on customer requirements.

By using the following port range, each server in the cluster reflects the same port ranges, but the servers are configured with a cascading port range, and varied load priority. Each server must have the following port rules:

Listener port (50000) specified as Affinity = None.

Example Port Ranges set up for 4 servers

The following example port ranges are specified as Single server and Equal distribution and here is an example of the set up for 4 application servers.

Example AppSrv1

Start	End	Mode	Load/Priority	Affinity
8080	8080	Multiple	Equal	Required
40003	40004	Multiple	Equal	None
50000	50000	Multiple	Equal	None
50001	50002	Multiple	Equal	Required
50005	50006	Multiple	Equal	Required
50008	50008	Multiple	Equal	Required
55001	55001	Multiple	Equal	Required
55000	55000	Multiple	Equal	None
40100	40199	Single	1	Not Applicable
40200	40299	Single	32	Not Applicable
40300	40399	Single	32	Not Applicable
40400	40499	Single	32	Not Applicable

Example AppSrv2

Start	End	Mode	Load/Priority	Affinity
8080	8080	Multiple	Equal	Required
40003	40004	Multiple	Equal	None
50000	50000	Multiple	Equal	None
50001	50002	Multiple	Equal	Required
50005	50006	Multiple	Equal	Required
50008	50008	Multiple	Equal	Required
55001	55001	Multiple	Equal	Required
55000	55000	Multiple	Equal	None
40100	40199	Single	32	Not Applicable
40200	40299	Single	1	Not Applicable
40300	40399	Single	32	Not Applicable
40400	40499	Single	32	Not Applicable

Example AppSrv3

Start	End	Mode	Load/Priority	Affinity
8080	8080	Multiple	Equal	Required
40003	40004	Multiple	Equal	None
50000	50000	Multiple	Equal	None
50001	50002	Multiple	Equal	Required
50005	50006	Multiple	Equal	Required
50008	50008	Multiple	Equal	Required
55001	55001	Multiple	Equal	Required
55000	55000	Multiple	Equal	None
40100	40199	Single	32	Not Applicable
40200	40299	Single	32	Not Applicable
40300	40399	Single	1	Not Applicable
40400	40499	Single	32	Not Applicable

Example AppSrv4

Start	End	Mode	Load/Priority	Affinity
8080	8080	Multiple	Equal	Required
40003	40004	Multiple	Equal	None
50000	50000	Multiple	Equal	None
50001	50002	Multiple	Equal	Required
50005	50006	Multiple	Equal	Required
50008	50008	Multiple	Equal	Required
55001	55001	Multiple	Equal	Required
55000	55000	Multiple	Equal	None
40100	40199	Single	32	Not Applicable
40200	40299	Single	32	Not Applicable
40300	40399	Single	32	Not Applicable
40400	40499	Single	1	Not Applicable

Caution: The following section contains information about modifying the registry. Before you modify the registry, you must create a backup of the registry and ensure that you understand how to restore the registry if a problem occurs.

After the changes have been made on the Load Balanced network card, you must modify the port range in the registry on each application server as follows. You must also remember to reset these changes to the registry after reinstalling SunSystems:

1. Run **Regedit**
2. Find the following registry location: **HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\SunSystems\Core\5.1\SessionManager**
3. Within this registry key, make the following changes to the **PortRange1_Max** and **PortRange1_Min** to reflect the changes in the table for each Application Server:

10. **AppSrv 1 Max = 40199 Min = 40100**
11. **AppSrv 2 Max = 40299 Min = 40200**
12. **AppSrv 3 Max = 40399 Min = 40300**
13. **AppSrv 4 Max = 40499 Min = 40400**

4. Restart SunSystems Session Manager Service on all SunSystems application servers.
5. The SunSystems Configuration service is located on the application servers. The load balanced address should be used. In the SunSystems Domain database, edit table **DOMN_VRTL_HOST**:
   a. Find **infor-cfg-tcp** in the column VRTL_HOST_NAME.

      In the same record, find the ACTUAL_HOST_NAME. Change the value to the load balanced application server name.

   b. Find **infor-cfg-http** in the column VRTL_HOST_NAME.

      In the same record, find the ACTUAL_HOST_NAME. Change the value to the load balanced application server name.

   c. Find **infor-cfg-named_pipes** in the column VRTL_HOST_NAME.

      In the same record, find the ACTUAL_HOST_NAME. Change the value to the load balanced application server name.
6. Restart the SunSystems Security service.
7. Stop and then restart IIS services.

Load balancing SunSystems Connect (SSC)

By default, SSC refers to the local host when running. To enable SSC to function in a load balanced environment, you must make the following changes on each Load Balanced Application Server:

1. Run Property Editor (PPE).

2. Select Tomcat.
3. Select **additional_hosts** and enter the Load Balanced name or IP address. Save the changes and log out.
4. For the change to take effect, stop and start the SunSystems Connect Service.
5. Repeat steps 1-4 for each remaining application server.

You can now run SSC.

Specifying a DNS CNAME record as a server alias for the Application server

Update CNAME in DNS to identify the SunSystems Application server. This will simplify the process of switching to a different server in the case of server failure.

Specify a DNS CNAME for a new SunSystems installation

1. In Active Directory, specify your CNAME, for example, **V62APPSERVER**.
2. Set this to the fully qualified domain name (FQDN) of the application server, i.e. **<Server name e>.<domain.com>**
3. Install SunSystems client and ensure it points to the new CNAME.

Database server

4. In Microsoft SQL Server, open the SunSystems Domain database.
5. Update the DOMN_VRTL_HOST table so ACTUAL_HOST_NAME = **<CNAME value>** where VRTL_HOST_NAME = **infor-cfg-tcp.**
6. Update the DOMN_VRTL_HOST table so ACTUAL_HOST_NAME = **<CNAME value>** where VRTL_HOST_NAME = **infor-cfg-http.**
7. Update the DOMN_VRTL_HOST table so ACTUAL_HOST_NAME = **<CNAME value>** where VRTL_HOST_NAME = **infor-cfg-named-pipes.**

Specify a DNS CNAME for an existing SunSystems installation

Database server

1. In Microsoft SQL Server, open the SunSystems Domain database.
2. Update the DOMN_VRTL_HOST table so ACTUAL_HOST_NAME = **<CNAME value>** where VRTL_HOST_NAME = **infor-cfg-tcp.**
3. Update the DOMN_VRTL_HOST table so ACTUAL_HOST_NAME = **<CNAME value>** where VRTL_HOST_NAME = **infor-cfg-http.**
4. Update the DOMN_VRTL_HOST table so ACTUAL_HOST_NAME = **<CNAME value>** where VRTL_HOST_NAME = **infor-cfg-named-pipes.**

SunSystems web servers and client machines

5. Flush the DNS cache on all web servers and client machines.
6. Run the Switch Server application.
7. Specify the CNAME value as the Default server name.
8. Go to **Search all programs and files** and enter **regedit**.
9. Go to HKEY_LOCAL_MACHINE > SOFTWARE > Wow6432Node > SunSystems > Install > SSCServer.
10. Enter the CNAME, for example, **V62APPSERVER**.

Sunsystems web servers and application servers

11. Flush the DNS cache on all web servers and application servers.
12. Restart all SunSystems services.

Chapter 15 SunSystems Reporting Services (SRS)

15

IIS and SunSystems reporting

Reporting uses a specifically configured website, rather than the default website; the SRS website must be configured to use a port number other than the default port number.

During installation you are asked to specify two port numbers because on complex multi-tier installations, where Report Manager and Report Server are installed on different machines, a different port number may be used on each machine.

Changing the SunSystemsReporting user and password

The installation process sets the SunSystems Reporting user as the user for both the SSRS and IIS. If after installation it is necessary to change the user or the password you must follow these steps.

Step 1: Update the credentials used by Microsoft SQL Server Reporting Services

1. On the server hosting SQL Server Reporting Services, run Reporting Services Configuration Manager from the Start Menu.
2. Select the instance of SQL Server Reporting Services used by SRS.
3. Select Service Account.
4. Select Use another account.
5. Enter the account name and password for the new SunSystems Reporting user.
6. Click Apply.
7. If required, back up your new encryption key to the local file system.
8. Check for any errors in the Results panel.

Step 2: Update the credentials used by the SRS web applications

Caution: For x86 machines, substitute all occurrences of **%ProgramFiles(x86)%** with **%ProgramFiles%**.

1. From an Administrator command prompt on the SRS Server, run the following commands:

   cd C:\windows\Microsoft.Net\Framework\v2.0.50727

aspnet_regiis.exe –pdf

"system.web/identity" "%ProgramFiles(x86)%\Infor\SunSystems Reporting Services\web\SunSystemsReportServer"

aspnet_regiis.exe –pdf

"system.web/identity" "%ProgramFiles(x86)%\Infor\SunSystems Reporting Services\web\SunSystemsReportManager"

2. Using Notepad, open **web.config** in **%ProgramFiles(x86)\Infor\SunSystems Reporting Services\web\SunSystemsReportServer**.
3. Change the userName and password values of the identity element in the file, to the new SunSystems Reporting user:

   <identity impersonate="true" userName="domain\newuserid" password="password@123456" />
4. Using Notepad, open **web.config** in **%ProgramFiles(x86)%\Infor\SunSystems Reporting Services\web\SunSystemsReportManager**.
5. Change the userName and password values of the identity element in the file, to the new SunSystems Reporting user:

   <identity impersonate="true" userName="domain\newuserid" password="password@123456" />
6. Update IIS to use the new SunSystems Reporting user.

Step 3: Update IIS to use the new SunSystems Reporting user

1. Logon to the SRS server and open the SRS installation log file **SRS_Install.log**. Typically this is **C:\ProgramData\Infor\Logs\SunSystems\Install**.
2. Find the first log entry for **ConfigureReporting.exe** and copy the line into Notepad.
3. Delete all text before “ConfigureReporting.exe”. Delete the closing bracket at the end of the line. Change the user and password parameter values.
4. From an Administrator command prompt on the SRS server, run the following command:

   cd %ProgramFiles(x86)%\Infor\SunSystems

Note: If you are running a dedicated SRS server, you must run this command instead:
cd %ProgramFiles%\Infor\SunSystems Reporting Services\apps

5. Copy and paste the command line text from Notepad into the command prompt and run the command.
6. Any other services that use the Reporting Services User are required to be changed such as the SunSystemsReportingPrintService.
7. When moving from a domain account to a local account (or vice versa) you may need to add/remove **RSWindowsNegotiate** to the **AuthenticationTypes** in the **rsreportserver.config** of SSRS.

```
<Authentication>
      <AuthenticationTypes>
      <RSWindowsNegotiate />
      <RSWindowsNTLM />
      </AuthenticationTypes>
      <RSWindowsExtendedProtectionLevel>Off</RSWindowsExtendedProtectionLevel>
      <RSWindowsExtendedProtectionScenario>Proxy</RSWindowsExtendedProtectionS
      cenario>
      <EnableAuthPersistence>true</EnableAuthPersistence>
</Authentication>
```

8. Ensure that the new account has Read and Execute permissions to the Microsoft Reporting Services RSTempFiles folder, and all sub-folders. The path of the RSTempFiles folder is typically **%ProgramFiles%\Microsoft SQL Server\<instance name>\Reporting Services\RSTempFiles**.

E-mail support

The support for emailing reports has been improved and no longer uses the inbuilt Microsoft Reporting Services E-mail facility. The administrator now defines the e-mail server and default 'from' address when installing this version. In addition, a log is now written to the report server detailing the recipients emailed and the attachments sent.

Load balancing SunSystems Reporting services

You can load balance the SRS Report Manager and SRS Report Server:

1. While installing the SunSystems Reporting components, specify the load balanced server address for Report Manager and SunSystems Report Server.
2. In the SunSystems Domain database, edit the **DOMN_VRTL_HOST** table.
3. Select the row where **DFLT_PATH='SunSystemsReportManager'**.
4. Update **ACTUAL_HOST_NAME** to the load balanced server name for SRS Report Manager.
5. Repeat for SunSystems Report Server.
6. Stop and then restart IIS services.

Managing and deploying reports

The example reports must not be used operationally in their initially installed location, which is primarily for demonstration purposes and liable to be overwritten on upgrade. Even if not customized from the issued examples, operational reports must be deployed to a folder structure appropriate to the requirements of the business and Path Variables amended and folder level access permissions set accordingly. Reports may be renamed using an appropriate convention, or one based on that used for the example reports, if preferred.

Chapter 16 Publishing SunSystems through Secure Sockets Layer (SSL)

16

Introduction

The instructions below assume that you have SunSystems Security Web, SunSystems Web and SunSystems Reporting Services on the same server.

For SunSystems Web, be careful of case sensitivity when editing **server.xml**. For example, the case sensitivity of **keystorePass=** must be correct. It is also important to avoid pasting a trailing space when copying text to configuration files.

The following table shows suggested ports and certificate names. We recommend you update the table with the details of your installation.

	http	https	Certificate and path	Certificate password
Security Web	81	82	IIS: SunWeb Certificate	
SunSystems Web	9080	9443	SunWeb.jks	
SunSystems Reporting	94	83	IIS: SunWeb Certificate	
Transfer Desk Web	9090	9091	IIS: SunWeb Certificate	
SSC	8080	8443	SunWeb.jks	

Note: If you are intending to use isapi_redirect.dll to publish SunSystems Web through IIS, you do not need to install java, convert the certificate to java format, or amend SunSystems Web running in tomcat to use a certificate. See the section SunSystems Web Load Balancing.

Prerequisites

For the following steps you must install the latest version of java jre. Then in Advanced System Settings set the environment variable (set as a system variable): **JAVA_HOME** `to for example C:\Program Files\Java\jre7\bin`

Next, add **;%JAVA_HOME%** to the end of your **PATH** environment variable.

Obtaining and exporting a certificate from your organisation's Certificate Authority

1. Create a 'Certificate Signing Request'.

Choose a server with IIS role on the same domain you want to install the certificate. Launch IIS, Select the Server, Server Certificates, Action - Create Certificate Request. Common name - enter the wildcard address for the domain e.g. *.infor.com Enter your company details and click next. Select Microsoft RSA SChannel and Bit Length 2048. Save as certnew.txt. Make a note of the folder you save this to. The bit length must be a minimum of 2048. Certnew.txt is the CSR.

2. Send the CSR to the certificate authority.

This might be via a web browser, but equally it could be emailed, or done manually for a self sign using something like the openssl toolkit. Use Firefox or Chrome to access your organisation's certificate issuer and request a Certificate, Advanced Certificate Request, and paste your certificate request including all the readable text at the beginning and end. Certificate Template - Web Server. Submit.Two files are created. Download both.

3. Add the certificate to IIS.

Look in your download directory and you find certnew.cer. and certnew.p7b. Copy them both back to to your IIS machine. On IIS machine, Right click and install certnew.cer for local machine (not user).

In IIS Manager, Server Certificates. Complete Certificate Request, browsing to certnew.cer. Messages may be displayed. Press F5 to see the installed certificate.

7. Export the PFX archive.

If you wish to reuse the certificate in tomcat, you can export the certificate from IIS to create the file **SunWeb.pfx**. Make a note of the destination folder and the password you entered.

Converting your Certificate from IIS format to Java format using Jetty

1. To convert your certificate to Java format you will need the file **jetty-6.1.1.jar**. Copy **jetty-6.1.1.jar** from the Jetty folder in the SunSystems Installation DVD into a folder, for example, **\ProgramData\Infor\SunSystems\Jetty**. If you do not have access to the SunSystems Installation DVD, Jetty can be downloaded from **http://dist.codehaus.org/jetty/jetty-6.1.x/jetty-1.1.0.zip** and extracted into a folder, as above.
2. Extract this zip file into a folder. For example: **\ProgramData\Infor\SunSystems\Jetty**. The only file required is **jetty-6.1.1.jar**.
3. In a command prompt, go to the folder containing **jetty-6.1.1.jar.** Run the following command to check java environment variables are set up correctly:

   java -classpath jetty-6.1.1.jar org.mortbay.jetty.security.PKCS12Import

   A message is displayed: **usage: java PKCS12Import {pkcs12file} [newjksfile]**
4. Place your **SunWeb.pfx** file in this working directory and run the following command to create java format keystore:

   java -cp jetty-6.1.1.jar org.mortbay.jetty.security.PKCS12Import SunWeb.pfx SunWeb.jks

You must enter the password that was set for the .pfx file, and provide a new password for the Java keystore.

Configuring SSL for SunSystems Security Web

1. In IIS Manager, open Sites > SunSystems Security, and in the Actions panel click Bindings. Ensure you change the port number when you add the site binding, as follows:

   Type: **https**

   IP Address: All unassigned

   Port: **82**

Select your SSL certificate from the dropdown list.

Edit **server-custom.properties**, which can be found in

Program Files(x86)\Infor\SunSystems\SunSystemsWeb\tomcat\webapps\SunSystems\WEB-INF. Add the following URLs under Server Configuration, exactly as they are shown here:

security.loginserver.url=https://sunsystems-security/Login.aspx

security.logoutserver.url=https://sunsystems-security/Logout.aspx

In the SunSystems Domain database, edit table **DOMN_VRTL_HOST**:

a. Find **sunsystems-security** in the column VRTL_HOST_NAME.

b. In the same record, find the ACTUAL_HOST_NAME for **sunsystems-security**. Change the value to the FQDN.

c. In the same record, set the SECURE_PORT_NUM to 82.

d. In the same record, set **PORT_NUM** to 0.

e. Find **sunsystems-securityconsole** in the column VRTL_HOST_NAME.

f. In the same record, find the ACTUAL_HOST_NAME for **sunsystems-securityconsole**. Change the value to the FQDN.

g. In the same record, set the SECURE_PORT_NUM to 82.

h. In the same record, set **PORT_NUM** to 0.

In IIS Manager, restart SecurityWebServer. In Services, restart SunSystems Web Service.

Check SecurityWebServer and SunSystems Web

Check the following:	✓
Check the authentication for SunSystems Web: **http://<servername.domain.com>:9080/SunSystems**	
Check SecurityWebServer: **https://<servername.domain.com>:82/SecurityWebServer**	

Configuring SSL for SunSystems Web

1. Right-click Notepad, select 'run as administrator' and edit server.xml to use this keystore. Open **server.xml**, which can be found in **Program Files (x86)\Infor\SunSystems\SunSystemsWeb\tomcat\conf**

   You will need to open **server.xml** using Notepad. Right-click Notepad, select 'run as administrator' and edit the file.

2. Specify the keystore location and password for HTTPS port 9443:

   a Remove comment markers if required '<!–' from the start, and '–>' from the end, of this block of text.

   <Connector port="9443" protocol="org.apache.coyote.http11.Http11NioProtocol" compression="2048" compressableMimeType="text/html, text/xml, text/css, application/javascript" SSLEnabled="true" maxThreads="150" scheme="https" secure="true" clientAuth="false" sslProtocol="TLS" keystoreFile="" keystorePass="" />

   b Amend the line starting with keystoreFile for your certificate .jks file name and location:

   keystoreFile="C:/ProgramData/Infor/jetty/SunWeb.jks" keystorePass="[change]"/>

   The value used for keystore File must be the location where you saved SubWeb.jks in the section 'Obtaining and exporting a domain certificate from Certificate Authority through IIS'. The value above is an example.

Caution: Take care to enter the text correctly. The syntax is case sensitive, for example, keystorePass.

3. Restart SunSystems Web service and log in to SunSystems using **https://<servername.domain.com>:9443/SunSystems.**

You are redirected to the secure port for security and maintain a secure connection accessing SunSystems. In the case of problems, check the log files in **ProgramData\Infor\SunSystems\Logs.**

Check secure connection login

Check the following:	✓
https://<servername.domain.com>:9443/SunSystems	
In browser: Check your Certification Path from the lock symbol.	

External access to SunSystems Web

If users access SunSystems Web from a machine that is not a member of the same Windows domain as the SunSystems installation, you will need to edit the table DOMN_VRTL_HOST in the SunSystems Domain database. Replace the value in ACTUAL_HOST_NAME with the FQDN of the correct server hosting the application, in the following records where:

- **VRTL_HOST_NAME = sunsystems-securityconsole**
- **VRTL_HOST_NAME = sunsystems-security**
- **VRTL_HOST_NAME = sunsystems-transferdesk**
- **VRTL_HOST_NAME = sunsystems-help**
- **VRTL_HOST_NAME = infor-app-srs**
- **VRTL_HOST_NAME = infor-app-dar**

You must restart all SunSystems services after making these changes. Stop and restart IIS services.

Configuring SSL for SunSystems Reporting

Note: Restricted access to the https port is only required for SRS Report Manager and Data Access Manager, as the SunSystems Web user will not access SRS Report Server and other SRS applications directly.

1. In IIS Manager, open Sites > SunSystems Reporting, and in the Actions panel click Bindings. Add a site binding as follows:

   Type: **https**

   IP Address: All unassigned

   Port: **83**

2. Select the SunWeb certificate from the dropdown menu, and click View to check your certificate is valid.
3. In the SunSystems Domain database, edit the table DOMN_VRTL_HOST:

   a Find the record where VRTL_HOST_NAME = **infor-app-srs:**

   i) In the same record, change the value of ACTUAL_HOST_NAME to the FQDN of the SunSystems Report Manager server.

   ii) In the same record, set the SECURE_PORT_NUM to 83.

iii) In the same record, set the PORT_NUM to 0.

b Find the record where VRTL_HOST_NAME = **infor-app-dar**:

i) In the same record, change the value of ACTUAL_HOST_NAME to the FQDN of the SunSystems Report Server server (where Data Access Manager is hosted).

ii) In the same record, set the SECURE_PORT_NUM to 83.

c In the same record, set the PORT_NUM to 0. Find the record where VRTL_HOST_NAME = **infor-app-rs**:

i) In the same record, change the value of ACTUAL_HOST_NAME to the FQDN of the SunSystems Report Server server (where Data Access Manager is hosted).

ii) In the same record, set the SECURE_PORT_NUM to 83.

iii) In the same record, set the PORT_NUM to 0.

The Web.config file must be edited for ReportManager, changing the value of the endpoint **bindingConfiguration** from **HttpSunSystemsReportingBinding** to **HttpsSunSystemsReportingBinding** for all endpoints. The Web.config file can be found in: \Program Files (x86)\Infor\SunSystems Reporting Services\web\ReportManager.

Do **not** change the elements under customBinding in web.config, as these two configurations define the correct settings for http and https.

If only https is enabled for SunSystemsReportServer, the Web.config file must also be edited for SunSystemsReportServer, changing the value of the endpoint **bindingConfiguration** from **HttpSunSystemsReportingBinding** to **HttpsSunSystemsReportingBinding** for all endpoints. The Web.config file can be found in: \Program Files (x86)\Infor\SunSystems Reporting Services\web\SunSystemsReportServer.

Restart IIS, SunSystems Security Service, and SunSystems Report Manager Service.

Check the SunSystems Reporting Services websites are accessible.

The following links should result in the relevant web page:	✓
https://<servername.domain.com>:83/ReportManager	
https://<servername.domain.com>:83/DataAccessManager	
In SunSystems Windows client, run RMA and Trial Balance (TBL) to check reporting is working from the Windows client.	
In the case of problems, check the log files in **ProgramData\Infor\SunSystems\Logs**	

Configuring SSL for Transfer Desk Web

1. In IIS Manager, open Sites > SunSystems Transfer Desk, and in the Actions panel click Bindings. Add a site binding as follows:

   Type: **https**

   IP Address: All unassigned

   Port: **9091**

2. Select the SunWeb certificate from the dropdown menu, and click View to check your certificate is valid.
3. In the SunSystems Domain database, edit the table DOMN_VRTL_HOST:
   a. Find **sunsystems-transferdesk** in the column VRTL_HOST_NAME
   b. In the same record, find the ACTUAL_HOST_NAME for **sunsystems-transferdesk**. Change the value to the FQDN of the SunSystems Transfer Desk Web server.
   c. In the same record, set the SECURE_PORT_NUM to 9091.
   d. In the same record, set the PORT_NUM to 0.
4. Restart TransferDeskWebServer

Check the URL for Transfer Desk Web

Check the following:	✓
https://<servername.domain.com>:9091/TransferDeskWebServer	

Configuring SSL for SSC

Earlier in this section, using jetty, you created **SunWeb.jks**. This certificate file can also be used for SSC.

1. In Services, stop the 'SunSystems Connect Server' Windows service.
2. Copy the 'SunWeb.jks' file into the '<install location>/SunSystems/SSC' folder.

3. Run Property Editor from within SunSystems (shortcut 'PPE') and Navigate to 'tomcat' -> 'https_connector'.
4. Select 'keystore' and modify the value to be '$(system.install_dir)/SunWeb.jks'.

5. Select 'password' and modify the value to be the password you used when creating the SunWeb.jks file.

6. Save the changes, and close Property Editor.

7. Exit SunSystems.
6. In Services, start ‘SunSystems Connect Server’ Windows service.

7. If you have used the alternative method of renaming SunWeb.jks as tomcat.keystore, applying 6.2.1 to an existing v620 installation will overwrite tomcat.keystore. You will need to copy ‘SunWeb.jks’ and rename to ‘tomcat.keystore’ again after applying 6.2.1.

Check the connection for SSC demo page and SOAP connnection

Check the following:	✓
https://<servername.domain.com>:8443/ssc	
https://<servername.domain.com>:8443/connect/wsdl/ComponentExecutor	

Configuring SSL for SunSystems Web Help

In the SunSystems Domain database, edit the table DOMN_VRTL_HOST:

a. Find **sunsystems-help** in the column VRTL_HOST_NAME

b. In the same record, find the ACTUAL_HOST_NAME for **sunsystems-help.** Change the value to the FQDN of the SunSystems Web server.

c. In the same record, set the SECURE_PORT_NUM to 9443.

d. In the same record, set the PORT_NUM to 0.

e. Restart IIS

Transport Layer Security (TLS)

The concept of “Transport Layer Security” is to wrap communications traffic in a content agnostic manner, providing a low cost, yet reliable layer of security in transit. This layer of security was originally provided by SSL (Secure Sockets Layer), but is now being steadily replaced by TLS (Transport Layer Security) protocols.

There are three versions of SSL (SSL 1.0, 2.0 and 3.0) and presently three versions of TLS (1.0, 1.1, and 1.2) – supporting applications (such as web servers) typically attempt to negotiate the most secure protocol between both client (browser) and server. However attackers will often attempt to take advantage of this negotiation phase to deliberately request less secure protocols (and encryption ciphers) to expose previously discovered (and exploitable) flaws. It is therefore recommended that software installers disable ALL SSL protocols, and any weaker TLS protocols – relying solely upon TLS 1.2.

Exposed IIS servers publishing (any or all of) SunSystems Web Security (Login Application), SecurityConsole, TransferDeskWeb, SRS Report Manager or SunSystemsWeb (setup for load

balancing) should be amended. See the following Microsoft knowledge base article to disable the SSL protocols through the Windows Registry.

http://support.microsoft.com/kb/187498

SunSystems Connect application (SSC) specifies TLSv1.2 in props.xml from SunSystems v6.2.1 PS13 onwards.

Browser support: Please note that IE9 and IE10 require the support for TLS v1.2 to be enabled.

Verification: it is easy to verify these settings for external websites. For example, see https://www.ssllabs.com/ssltest/

Chapter 17 SunSystems Web

17

SunSystems Web user interface customisation

The SunSystems Web user interface can be customized by adding settings to the file **server-custom.properties**. For example, you can change the font, colour, or how the session navigation menu is displayed in Infor Ming.le™.

1. Using notepad, open **server-custom.properties** in **Program Files (x86)\Infor\SunSystems\SunSystemsWeb\tomcat\webapps\SunSystems\WEB-INF**.
2. Add the new settings to the file, and save. No setting is mandatory, and they can be applied in any order.
3. Allow user option to create default menu where none exists. VALUES (true, false) DEFAULT (true)
   client.defaultMenuCreation=true
4. Restart the SunSystems Web Service then restart the browser. This ensures that any temporary cookies are removed.

SunSystems Web display properties

The following table shows the complete list of properties that can be used:

Property	Description	Values
client.rendermode	Sets default values for specific properties from this table	**client.rendermode=standalone** **client.rendermode=workspace** **client.rendermode=mobile**
client.menuStyle	Controls the main menu navigation style. If Infor Ming.le™ is selected, the SunSystems tabbed menu is switched off.	**client.menuStyle=legacy** **client.menuStyle=workspace** **client.menuStyle=mobile**
client.showAppHeader	Show the top level Infor Application Header.	**client.showAppHeader=true** **client.showAppHeader=false**

Property	Description	Values
client.showAppNavBar	Show the session navigation menu and dropdown navigation menu.	**client.showAppNavBar=true** **client.showAppNavBar=false**
client.showAppNavBarMenu	Show the dropdown navigation menu.	**client.showAppNavBarMenu=true** **client.showAppNavBarMenu=false**
client.showVsgFontsOnly	Show the Visual Style Guide fonts only (font-family only), ignoring Form Designer.	**client.showVsgFontsOnly=true** **client.showVsgFontsOnly=false**
client.showVsgColoursOnly	Show the Visual Style Guide colours only (background / foreground) ignoring Form Designer.	**client.showVsgColoursOnly=true** **client.showVsgColoursOnly=false**
ui.forceVsgVersion	Controls the UX version used. 2 presents the default Blue 2.0 style and 3 presents the new UX 3.0 style. This is a system wide setting regardless of the render mode selected.	**ui.forceVsgVersion=2** **ui.forceVsgVersion=3**
client.logicalId	Non UI-specific. Used for IBC and drillback messaging in Infor Ming.le™ / ION. Replacement for **hostPage.logicalId**	**client.menuStyle=infor.sunsystems.1**
client.embeddedSessionLimit	Non UI-specific. Defines how many embedded sessions can run in web mode. Default is 4. Replacement for **hostpage.embeddedSssionLimit**	**client.embeddedSessionLimit=5**

These properties use the format **client.<property name>=value** which sets the same value for all rendering modes. For example, **client.menuStyle=workspace**displays SunSystems Web using Infor Ming.le™-style menus, whether it is run from within Infor Ming.le™, Infor Motion SunSystems iOS or in Standalone mode.

User interface visual style

By default, SunSystems Web is presented using a blue user interface. To display the new, white user interface, add the setting **ui.forceVsgVersion=3** to **server-custom.properties**.

Render modes

SunSystems Web is presented using one of three display configurations, or ‘render modes’, that define the navigation options displayed in each environment:

- standalone: running SunSystems Web outside of any application
- workspace: running SunSystems Web from within Infor Ming.le™
- mobile: running SunSystems Web from within Infor Motion SunSystems iOS.

Specifying a render mode automatically sets default values for a group of properties:

Render mode	Default values
client.rendermode=standalone	**client.standalone.menuStyle=standalone** **client.standalone.showAppHeader=true** **client.standalone.showAppNavBar=true** **client.standalone.showAppNavBarMenu=false**
client.rendermode=workspace	**client.workspace.menuStyle=workspace** **client.workspace.showAppHeader=false** **client.workspace.showAppNavBar=true** **client.workspace.showAppNavBarMenu=true**
client.rendermode=mobile	**client.mobile.menuStyle=mobile** **client.mobile.showAppHeader=false** **client.mobile.showAppNavBar=false** **client.mobile.showAppNavBarMenu=false**

These properties use the format **client.<render mode>.<property name>**, which you can use to set a property value for a specific render mode. For example, you can specify these settings to display the SunSystems tabbed menu, whether running SunSystems Web from within Infor Ming.le™ , or in Standalone mode:

client.workspace.menuStyle=legacy

client.standalone.menuStyle=legacy

You can also use this format to override the default values for the render modes. For example, **client.rendermode=workspace** automatically sets **showAppHeader** to **false**, but if you follow it with **client.workspace.showAppHeader=true**, then the Infor Ming.le™ render mode will display the Infor Application Header.

Setting up SunSystems Report Viewer with different languages

To enable additional language users to see the report viewer header in their own language, individual Microsoft Report Viewer language packs must be installed. Prior to installing Report Viewer, ensure you have installed the prerequisite classes from Microsoft System CLR Types if you are using Microsoft SQL Server 2012. For more information, refer to the Prerequisites section.

1. From the Microsoft website, download Report Viewer Redistributable 2012 and install on your SSRS Server.
2. Download and install the Microsoft Report Viewer 2012 Language Pack for each required language.
3. After installation, check each has been installed successfully in Control Panel > Programs and Features.
4. In IIS Manager restart application pool SunSystemsReportingServices.

Web Server Scalability

Introduction

SunSystems Web provides a unique feature called ‘Session Restoration’ which allows a web user to return to their ‘running’ sessions through a later login. As this returning user may be on a new web browser environment (or even a different browser session on the same machine), existing Session affinity techniques such as Session Cookies, or Browser IP affinity are not suitable to re-establish this connection. Each SunSystems Web server maintains a direct socket connection to the running Application process, which can only be restored by guiding the returning web sessions back to the same web server which holds this connection (all application sessions for a single user will therefore be routed through a single web server), this creates a ‘SunSystems User’ affinity model.

This affinity model is implemented by SunSystems through load balancing with IIS, using the ISAPI_REDIRECT module, and therefore mandates the usage of this deployment model.

Prerequisites

- SunSystems Web is installed on each WebServer machine.
- IIS is installed on each WebServer machine.
- For the following steps you must install the latest version of java jre. Then in Advanced System Settings set the environment variable (set as a system variable): **JAVA_HOME** `to for example C:\Program Files\Java\jre7\bin`

  Add **;%JAVA_HOME%** to the end of your **PATH** environment variable.

Check SunSystems Web (in tomcat) is working on all web server machines

Check the following:	✓
http://WebServer1.9080/SunSystems	
http://WebServer2.9080/SunSystems	

SunSystems Web Load Balancing

Prerequisites

- The SunSystems Web machines are all running the same version and edition of Windows 2012 (or Windows 2008 R2).

- Windows Network Load Balancing component is installed on every application server that will be part of the cluster.
- If you are configuring load balancing using Unicast, then every application server machine must have two Network Interface Cards (NIC).
- Static IP addresses are available for each machine.
- A DNS server is available on the network.
- Each SunSystems Web server name can be resolved by DNS.
- Plan to install the components SunSystemsWeb, SecurityWebServer/SecurityConsole, and TransferDeskWeb on all of the SunSystems Web servers.

Setting up Windows network load balancing

1. You need to make these changes to all Servers where SunSystems Web has been installed. These Servers need to be the identical version and edition of Windows.
2. In Server Manager, Features, add Network Load Balancing.
3. Control Panel, Network and Sharing Center, Change Adapter settings, Ethernet Properties, Internet Protocol Version 4 (TCP/IPv4) set static IP Subnet mask and Default gateway. Do not tick Network Load Balancing (NLB) – this will automatically be set by Network Load Balancing Manager.
4. In Active Directory, Users and Computers, add the load balanced server.
5. In DNS, in Forward Lookup Zones for your domain, add the load balanced server with a static IP. All static IP addresses should also be registered on your DHCP server.
6. On one Web Server, run Network Load Balancing Manager. Create a cluster for the load balanced server and add all SunSystems Web servers to this cluster. Define port rules for 80 (SunSystems), 81 (Security), and 9090 (Transfer Desk Web). What port rules you define depends on which SunSystems components are installed on the SunSystems Web servers. Port rules are set up for each host in the cluster.

Example WebSrv1

Start	End	Mode	Load/Priority	Affinity
80	80	Multiple	Equal	None
81	81	Multiple	Equal	Required
9090	9090	Multiple	Equal	Required
94	94	Multiple	Equal	Required

Apache Tomcat configuration

Carry out the following steps on each web server machine:

1. Stop the SunSystems Web service.
2. Open the **server.xml** configuration file of the Apache Tomcat SunSystems Web is running within. This is usually found in:

   Program Files (x86)\Infor\SunSystems\SunSystemsWeb\tomcat\conf
3. Make the following modifications: should be made to each Tomcat Node to uniquely identify them and ensure that AJP ports are open:

   a. Modify the tomcat engine definition to include the jvmRoute name chosen for that node. Note that the jvmRoute should be set to the host name of the web server machine.

   b. Change **<Engine name="Catalina" defaultHost="localhost">**to **<Engine name="Catalina" defaultHost="localhost" jvmRoute="WebServer1">**
4. Ensure the AJP/1.3 connector is enabled (not commented out) and note the port number (default 9009):

   <Connector port="9009" protocol="org.apache.coyote.ajp.AjpNioProtocol" redirectPort="9443" />
5. Ensure the AJP port is open.

IIS configuration

A load balancing configuration tool is supplied on the SunSystems 6.2.1 DVD in the LoadBalancing folder. Right click ssweb-loadbalancer.jar, and Open with, Java. Select the location where your configuration files will be generated. Use the + button to add SunSystems web servers to the load balanced array, and click the generate configuration button. This process can be repeated if you want to add more servers for example. The following load balancing configuration files will be generated so you will not have to manually create or edit these files:

Isapi_redirect.dll

Isapi_redirect.properties

Uriworkermap.properties

Web.config

Workers.properties

1. Open IIS Manager, select the root node (the server), and select option ISAPI and CGI Restrictions. From the Actions, select Add. Select the path to the DLL, that is, in this example **<IIS-tomcat_connector-conf>\isapi-redirect.dll**, enter a description of ISAPI_REDIRECT and check the Allow extension path to execute check box.
2. Open the Default website where you want to activate the redirect and open the option 'ISAPI Filters'.
3. From the 'Actions', select 'Add'.

4. Enter a filter name SunSystems, and select the path to the DLL for the executable, that is,

   <IIS-tomcat_connector-conf>\isapi-redirect.dll.

5. Right-click the default website selected in step 8 and select 'Add Virtual Directory...'. You must enter **sunsystems** for the alias, and select the path to the DLL for the physical path, that is **<IIS-tomcat_connector-conf>\isapi-redirect.dll**.
6. Select the virtual directory just created SunSystems and open the option 'Handler Mappings'.
7. In the disabled list select the mapping 'ISAPI-dll' and from the 'Actions' select 'Remove'.
8. From the 'Actions', select 'Add Module Mapping...'.
9. Enter the following, but do not click OK:

   Request Path: *.dll

   Module: IsapiModule (this can be selected from the drop down list)

   Executable: <IIS-tomcat_connector-conf>\isapi-redirect.dll

   Name: ISAPI_REDIRECT-dll

10. Click 'Request Restrictions' button.
    a. Select the 'Mapping' tab and check the 'Invoke handler only if request is mapped to' check box, and select 'File'.
    b. Select 'Verbs' tab and select 'All verbs'.
    c. Select 'Access' tab and select 'Execute'.
    d. Click OK to close the 'Request Restrictions' dialog box.
11. Click OK to close the 'Edit Module Mapping' dialog box.
12. Message is displayed. Do you want to allow this ISAPI extension? Yes.
13. From the 'Actions', select 'Edit Feature Permissions'.
14. Check the 'Execute' check box.
15. Locate the**<IIS-tomcat_connector-conf>** directory and open the **web.config** file in a text editor such as notepad.
16. Add the following attribute to the end of the ISAPI_REDIRECT-dll entry: **responseBufferLimit="0"**
17. Save and close the file.
18. Restart IIS.

Setting values for Java memory

Initial and maximum heap sizes should not be specified, as this enables default values, specific to your computer, to be set automatically. In most cases, an initial value of 16Mb and a maximum value of 256Mb are set. To remove the preconfigured values for initial and maximum heap sizes:

1. Type **CMD** in the Run dialog box and click OK.
2. Navigate to **Program Files(x86)\Infor\SunSystems\SunSystemsWeb\tomcat\bin**
3. Run **SunSystemsWebw //ES//SunSystemsWeb**
4. Select the Java tab in the SunSystems Web Service Properties dialog box.
5. Specify Initial memory pool as **Nothing**.
6. Specify Maximum memory pool as **Nothing**.
7. Click OK to save the changes.

SunSystems Web WAR Configuration

The SunSystems web application must be configured to operate in a Load Balanced environment. In this state it provides assistance to the load balancing infrastructure to redirect initial requests to the correct web server.

The following steps should be carried out on each web server machine.

1. Open the **server-custom.properties** file located in the war of SunSystems Web. This is usually found under:

   Program Files (x86)\Infor\SunSystems\SunSystemsWeb\tomcat\webapps\SunSystems

   \WEB-INF

2. Remove the # from the following line:

   #loadbalancer.enableLoadBalancer=true

Restart the SunSystems Web service.

Check SunSystems Web redirection through IIS is working on all Web Server machines

Check the following:	✓
http://WebServer1/SunSystems	
http://WebServer2/SunSystems	
http://WebServer1/jkmanager `(debugging tool)`	
User Manager, Settings, SunSystems, Operator Activity. For each user logged into a SunSystems function you can scroll right to see application server name and web server name.	

Load balancing the Security Web server

You can load balance the Security Web server, by entering the load balanced server name in the SunSystems Domain database:

1. Edit the DOMN_VRTL_HOST table.
2. Select the row where DFLT_PATH='SecurityWebServer'.
3. Update ACTUAL_HOST_NAME to the load balanced server name for Security Web Server.
4. Restart IIS.

Load balancing Transfer Desk Web

If you have installed Transfer Desk Web (separate installer), you can load balance TransferDeskWebServer, by entering the load balanced server name in the SunSystems Domain database:

1. Edit the DOMN_VRTL_HOST table.
2. Select the row where **DFLT_PATH='TransferDeskWebServer'**.
3. Update ACTUAL_HOST_NAME to the load balanced server name for Transfer Desk Web Server.
4. Restart IIS.

Switch off jkmanager

When the debugging tool is no longer required it is advised to deactivate for security reasons. For all Web Servers edit the**uriworkermap.properties** file to deactivate the jkmanager debugging tool. Type # preceding line **/jkmanager|/*=jkstatus**

Pop-up windows

If you have blocked pop-up windows in your web browser, you must add the SunSystems web server host as an exception to run reports correctly.

SunSystems host names

Host names in your SunSystems deployment must not contain '_' underscore, which is widely accepted to be an invalid character for host names, even though Windows allows it. Use of an underscore in a host name will cause SunSystems Web to fail. Host names must consist of alphanumeric characters (a-z, 0-9) and can include a '-' hyphen, as long as the hyphen is not the first or last character of the name.

SunSystems multiple virtual host deployment

Multiple virtual host deployments are not supported. Deployments must be either:

- Internal only
- Fully, externally visible, on a single virtual host.

Internal browser clients must access the system on the external address when required. If you require separate internal and external addresses for deployment, this must be considered by your IT department, with particular regard towards DNS mapping within your network systems.

Chapter 18 Troubleshooting

18

Introduction

The information in this section is to 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, refer to the subsection Before Contacting Technical Support, which details the information you must collate, before you call for technical assistance.

Troubleshooting hints

Listed below are some troubleshooting hints that might assist you when trying to analyze a problem:

- Pay attention to error messages. Error messages contain important information to solve a problem and are required by the technical support staff.
- Do not assume too much about the possible cause of the problem, or you might overlook any evidence presented.
- 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.
- Affirm whether the problem happens in other applications on other user's machines, or only on one machine.
- Be aware of security barriers (firewalls) because these can block communications between client and server machines
- Do not overlook the obvious; check plugs, connections and cables.

General installation problems

Problems can be in the form of an error message or unanticipated behaviour of the software. The problems described here are those that are most likely to occur because of the following:

- Incorrect installation settings.
- Incompatible data for installation settings and serialization.
- Access control – network settings, folder permissions.

- Incorrectly set IP addresses.
- Network Library not set to TCP/IP.
- Changes made to registry settings used by SunSystems.
- Database Access – Account Permissions.
- Services – Account Permissions.

The setup program configures all of the background settings that are required for your chosen installation type using the information you supply during installation. The setup program also validates the data that you enter; if the details that you enter are incompatible, an error message is displayed.

However, certain settings are inadvertently changed during or after the installation process, which renders them to be invalid and causes errors to be displayed.

If an unexpected event occurs in SunSystems, a SunSystems error message is displayed, which describes the error condition or unexpected response to a request. To save the error text, click the **Save** button to save the details to a file and location of your choice. A member of technical support can then analyze the contents of the file. You are given an option to either continue or abort SunSystems. If you choose to continue, SunSystems operates normally as far as possible; if the error is too severe, it automatically aborts.

Specific installation problems

Refer to the subsections below to resolve issues that can be encountered during the installation process and when running a new installation of SunSystems. Each problem is presented as a Symptom, usually as a message. The message text is presented here in bold. Possible causes and solutions then follow this.

Problems encountered during installation

The installation process fails

Possible Cause(s)

The SQL Server Autoshrink process is switched on (likely on a stand-alone installation).

Solution(s)

Before you start your SunSystems installation, ensure that the SQL Server Autoshrink process is switched off; failure to do so might cause contention that will make the installation process fail. You should switch off the Autoshrink facility for running SunSystems because it can affect performance.

Message displayed: [Microsoft][ODBC SQL Server Driver][Named Pipes] Specified SQL Server not found

Possible Cause(s)

The target machine that is selected to be used as the Database Server has not been located and therefore might not be connected to the network.

Solution(s)

Minimise the setup program dialog box and ensure that all machines that are designated to be included in either a two-tier installation or three-tier installation can communicate through the network.

Message displayed: [Microsoft][ODBC SQL Server Driver][Named Pipes] Unable to validate the login – error: A required privilege is not held by the client.

[Microsoft][ODBC SQL Server Driver][Named Pipes] Do you want to continue with this set toLocal Account?

Note: The account under which SessionManager runs must have permissions to access the ServerFiles folder. Depending on your configuration, the Local System Account might not have such permissions; if so, after the installation is complete, you must change the account that SessionManager is running under.

Possible Cause(s)

The target machine that is selected as the Database Server has been located, but the user on the client machine has not been set up as a user on the server.

Solution(s)

Minimise the setup program dialog box and ensure that the client machine has the correct access rights to the server.

Message displayed: [Microsoft][ODBC SQL Server Driver][Named Pipes] Access denied

Possible Cause(s)

The target machine that is selected as the Database Server has been located, but the user on the client machine has not been set up as a user on the server.

Solution(s)

Minimise the setup program dialog box and ensure that the client machine has the correct access rights to the server.

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

Possible Cause

ASP.NET is not registered.

Solution

Check ASP.NET is registered. Run a command prompt as administrator. Change directory to Windows\Microsoft.NET\Framework64\v2.0.50727. Enter the command aspnet_regiis –lv to ascertain if ASP.NET is already registered. If not already registered, enter: aspnet_regiis –ir to register.

Message displayed: Cannot start the Server-side process. Check the server is switched on

Possible Cause(s)

There is a problem with the connection from the client machine to the server that is running the Application Layer.

Solution(s)

This particular problem could be caused by numerous oversights; check the following:

- The client is connected to the network.
- The SunSystems Session Manager service is running.
- SQL Server is running on the database server.
- The client machine can **ping** the computer name used in the set up. Run **SwitchServer.exe** to check what this is.
- The IP address that is returned to the server by the client **ping** is the IP address displayed when IPCONFIG is run on the server. Windows 2003 allocates more than one IP address.
- Stop and restart the SunSystems Session Manager service on the application server.
- The name of the server is correct in the client registry:

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\SunSystems\Core\5.1\Comms\SessionManagerServerLocation

Note: The server location/name might be overridden with the server location/name in **HKEY_CURRENT_USER\Software\SunSystems\Core\5.1\Comms\SessionManagerServerLocation**. When you are troubleshooting client/server connections, check that the server name is correct.

- The Listener port set up on the applications server matches the port set up on the client. On the server, this is held in the registry setting:

  HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\SunSystems\Core\5.1\SessionManager\ListenerPort

- On the client, this is held in the registry setting:

  HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\SunSystems\Core\5.1\Comms\Session ManagerListenerPort

Note: The listener port might be overridden with the listener port in **HKEY_CURRENT_USER\SOFTWARE\SunSystems\Core\5.1\Comms\SessionManagerListenerPort**. When you are troubleshooting client/server connections, check that the listener port is correct.

- Ensure the Session Manager ports are excluded from the range of ephemeral ports:

  The following command shows the excluded port range:

  netsh int ipv4 show excludedportrange tcp

  Set the excluded port range with this command:

  netsh int ipv4 Add excludedportrange tcp 40100 900

  For more details, go to **http://support.microsoft.com/kb/2665809/en-us**

Message displayed: Unable to create the environment to view report instances. Please contact your environment administrator

Possible Cause(s)

This issue is caused by the changed path not being picked up by the application until reboot occurs.

Solution(s)

Reboot

Installer rolls back after attempting the installation. No message is displayed.

Look in **%TEMP%** or the folder above this for the msi log. This log is not easy to interpret but contains the reason for the rollback.

Also check **InstallLog.txt** in **ProgramData\Infor\Logs\SunSystems\Install**

Causes could include SunSystems applications still existing in IIS after uninstalling them. Check in IIS Manager.

SunSystems Reporting Installation will not complete / hangs – Loading Reports

Check that the SunSystems Configuration Service is running (it is located on the SunSystems application server).

Problems encountered when uninstalling SunSystems

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

Possible Cause(s)

SunSystems or a session is still active.

Solution(s)

Before you attempt to uninstall SunSystems, ensure that SunSystems has been closed.

Problems encountered when running SunSystems

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

Possible Cause(s)

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

Solution(s)

To input the supplied license details, run System Serialization (ZZS).

Note: If you serialize from within SunSystems using Serialization (ZZS), the SessionManager service login user must be a member of the Administrator group.

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(s)

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

Message displayed after completing the serialization form: System Parameters Amendment Failure

Possible Cause(s)

The serialization details that you entered do not match those for the required software component. Either the supplied license values have been typed incorrectly in the serialization form (missed digits result in invalid licenses), or the zero prefix has been omitted.

Solution(s)

Recreate serialization information with the relevant options:

- Initiate SunSystems
- Run System Serialization (ZZS)
- Reinsert the values again as supplied on your SunSystems serialization document
- Restart SunSystems.

Serialisation – nothing happens

If you run a SunSystems serialisation **and nothing happens, check that the user you are logged in with is in the Trusted Service Group. User Manager, SunSystems, Trusted Service Group. Use Task Manager to kill the Serialisation.exe process before you try to run the serialisation again.**

Users experience missing installation options

Possible Cause(s)

For example, documentation is now required but was not initially selected during the installation.

Solution(s)

Run the setup program from the SunSystems installation media. Select the documentation option, or any other options to install the required components.

Selections of ranges may be subject to abnormal truncation and apparently miss or lose data if the binary sort order is not used.

Possible Cause(s)

During database installation/creation, there are specific data storage options that must be selected. Binary Sort Order is mandatory. Binary Sort Order sets the database selection criteria to match the ASCII sort order A-Z a-z etc. which is compatible with the SunSystems program logic. SunSystems internal COBOL programming and business logic demands that dictionary sorts such as Aaâäàå, should not be used.

Database Transport (ODBC drivers).

Solution(s)

Select Binary Sort Order during database installation/creation.

SunSystems fails to connect to a remote server that is located on the secure side of a firewall mechanism.

Possible Cause(s)

The specific port numbers that are available to the software to successfully traverse the security zone of a firewall system must be programmed into the file `sun5.ini` as follows:

Port numbers that are specified by a default install do not match the configuration of the security firewall. The default behaviour of the system is to randomly allocate a transmission port through negotiation between the client and the server components. This method is rejected by firewall security mechanisms, and attempts to use the software through such a secure system, without modification, will fail.

Solution(s)

`Change the direct connection port settings in Sun5.ini, as follows:`

sun5.ini setting **– Direct-Connect-Port, Direct-Connect-Port-Range**.

For more information about configuring firewall enabled SunSystems configuration, refer to technical support.

For more information about SunSystems port settings, refer to Appendix A – TCP/IP Ports Used by SunSystems.

Note: Microsoft domain logins are case sensitive; caching is done at server level and this cache occasionally deletes its contents. For example, if a user name is created using mixed cases as UserName, users must log in as ‘UserName’ and not ‘username’. Failure to do so causes an error when the user attempts to log in to SunSystems. The workaround involves the SQL Server database administrator (DBA) installing SQL Server 2008 in a different collation order to Latin1_General_BIN, which is case sensitive. If the master database is not case sensitive, this problem is not encountered.

Apologies - but your browser isn’t currently supported

Possible Cause(s)

Browser is displaying in compatibility view mode.

Solution(s)

Internet Explorer 8 > Tools > Compatibility View Settings. Uncheck Display intranet sites in Compatibility View.

Log into SunSystems but there is nothing on the menu

Possible Cause(s)

Operator Group not set up in User Manager

Solution(s)

Log into User Manager as administrator, edit Group, 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

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 administrator, select Settings > Security Policy and clear Enable Windows Authentication.

Cannot find SunSystems Data Source in ODBC Data Source Administrator

On a 64 bit OS, to access the dialog box you must run **odbcad32.exe** in **C:\Windows\SysWOW64**

To login as a different SunSystems User

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.

If you are a standard authenticated user, check the SunSystems user icon in the sys tray, right-click and select Exit Login Monitor to enable you to log in each time you open SunSystems.

Unable to load client print control

This message displayed when clicking the printer icon in a viewed report on a machine with SunSystems client installed.

On the server containing SQL Server Reporting Services (SSRS):

Install the prerequisite classes from Microsoft System CLR Types for if you are using Microsoft SQL Server 2008 R2. Next, install Microsoft Report Viewer Redistributable 2012 (Full Installation), and restart Windows.

On the client machine upon clicking the printer icon in a viewed report you will be prompted to install a SQL Server Reporting Services component. This component will enable you to print from the viewed report.

Cannot create a connection to data source 'EvoReportDataSource'

Check that you have run Data Access Manager for all Business Units and ensure that WCF Services have been installed on the SQL Server Reporting Services Server.

The SunSystems connection is invalid (reason: Login failed. The login is from an untrusted domain)

Ensure the account running SunSystems reporting service has been added to the SunSystemsServices group on the database server if using local groups on a multi-tier configuration.

Message displayed: Operation failed with 0x8007000B

Check that all the correct IIS role services have been installed, and ASP.NET has been registered.

Refer to the Prerequisites section for details.

Service Temporary Unavailable/Server not found

In a load balanced SunSystems application server environment check that the registry settings have been correctly applied corresponding to the network load balancing port rules. After reinstalling SunSystems you need to reset these registry changes.

Connect Service will not start after applying 6.2.1

This will be an issue if you have SSC configured for SSL, and you apply 6.2.1 to a 6.2.0 installation. Tomcat.keystore will be overwritten. You will need to copy 'SunWeb.jks' and rename to 'tomcat.keystore' after applying 6.2.1.

Troubleshooting SunSystems Transfer Desk Web

Not displaying properly in the browser?

Switch off Compatibility View.

In Internet Explorer > Tools > Compatibility View Settings, remove transfer desk website from list and untick Display intranet sites in Compatibility view and Display all websites in Compatibility view.

Transfer Desk profiles not visible

Check in the SunSystems Windows Client that the server based Transfer Desk Profiles exist.

The following URL lists the transfer profiles available:

http://<servername>:9090/TransferDeskWebServer/TransferProfiles

Note: This link is for troubleshooting purposes only. To use the Transfer Desk Web functions, log in to SunSystems Web then run Transfer Profiles (TRP), Transfer History Viewer (TRH), or Server File Management (SFM) as required. For more information refer to the Transfer Desk online help.

Service Unavailable HTTP Error 503. The service is unavailable.

Go to Internet Information Services (IIS) Manager > Application Pools and check that TransferDeskWebServer has started. Also check that SecurityWebServer has started. This is installed as part of the SunSystems installation, so may be on a different server.

Error caused by an unexpected exception on server side.

Transfer Desk Web creates a system file called dummy_profile.xml in the root folder. Should this file be accidently deleted, profiles will not run in Transfer Desk Web. To recreate this file go to Transfer Desk, Server Folder Management, Change Root Directory, and create a new Root Directory using a network shared folder. Now you can revert to your original root directory and dummy_profile.xml will be generated.

Troubleshooting SSC

Unable to display the SSC demonstration website

Cause

The SunSystems Connect Server service might not be running. To check this on your server, open the Services folder (In Windows 2008, this is in Control Panel > Administrative Tools). There should be a SunSystems Connect Server service marked as Started.

Solution

If the service is marked as Started, try stopping and restarting.

If the service is not marked as Started, click the **Start** button to manually start it.

If the service does not exist, try reinstalling it as follows:

From a command prompt, run the following:

"SunSystems root directory\ssc\bin\connect server.exe" -i "SunSystems Connect Server"

"SunSystems root directory\ssc\bin\connect_start.txt" "SunSystems root directory\ssc\bin\connect_stop.txt"

Where**SunSystems root directory** is the location of SunSystems, such as**c:\Program Files\SunSystems**.

If the problem persists, contact Technical Support.

Attempting to start Transfer Desk fails with the error message ‘Cannot contact Transfer Desk server’

Cause

The SunSystems Connect server might not be running. To check this on your server, open the Services folder (this is in Control Panel > Administrative Tools). There should be a SunSystems Connect server, marked as Started.

Solution

If the service is marked as Started, try stopping and restarting it.

If the service is not marked as Started, click the Start button to manually start it.

If the service does not exist, try reinstalling it as follows:

From a command prompt, run the following:

"<SunSystems root directory>\ssc\bin\connect server.exe" -i "SunSystems Connect Server"

"<SunSystems root directory>\ssc\bin\connect_start.txt" "SunSystems root directory\ssc\bin\connect_stop.txt"

Where **SunSystems root directory** is the location of SunSystems, such as **c:\Program Files\SunSystems**.

If the problem persists, restart your machine or uninstall and reinstall the SunSystems Connect server as follows:

From the Windows 2000 Control Panel, launch the services option and stop the SunSystems Connect server.

From a command prompt, run the following:

"<SunSystems root directory>\ssc\bin\connect server.exe" -u "SunSystems Connect Server"

"<SunSystems root directory>\ssc\bin\connect server.exe" -i "SunSystems Connect Server"

"<SunSystems root directory>\ssc\bin\connect_start.txt" "SunSystems root directory\ssc\bin\connect_stop.txt"

Where **SunSystems root directory** is the location of SunSystems, such as **c:\Program Files\SunSystems**.

When trying to perform an SSC export the following message is displayed:

Invalid SQL is generated.

The SQL statement can be found in the Message Log (if the Log Server is running).

There is insufficient system memory to run this query.

Possible Causes

Microsoft SQL Server is running out of memory whilst executing a SQL Query.

Solution

Increase the memory available to Microsoft SQL Server by increasing the physical memory that is installed on the server machine, or adjust SQL Server's memory configuration, or both. Memory configuration can be modified through the SQL Server Properties dialog box.

If you still experience memory problems, reduce the number of selected table columns in your SSC export. To do this, from Component Manager click the Definitions tab and then edit the payload definition. For more information, refer to the SSC online documentation.

The SSC installation may not deploy successfully on a two-tiered or three-tiered environment

Solution(s)

Reinstall SSC. If further assistance is required, contact your local support help desk.

Troubleshooting SunSystems Reporting Services (SRS)

Print Icon not available / working from within Report Viewer

First make sure you have the latest version of Report Viewer 2012 installed on the server hosting SRS.

1. Login to your SRS Server as a user with administrative rights.
2. Install Report Viewer 2012
   (from http://www.microsoft.com/en-us/download/details.aspx?id=35747) making sure any specified pre-requisites are installed e.g.:
   a. The latest version of .NET 4.5.1 which can be downloaded from http://www.microsoft.com/en-us/download/confirmation.aspx?id=40773.
   b. Microsoft System CLR Types for SQL Server 2012, if you are not using SQL Server 2012, which can be downloaded from http://www.microsoft.com/en-us/download/details.aspx?id=29065.
3. Once these steps are done, the server must be rebooted.

The second step is to install the Print Client on each SunSystems client requiring client side printing:

1. Run SRS in Internet Explorer, navigating to http://ssrsserver:94/ReportManager and then run a standalone report, such as ARAB1.
2. On the Report Viewer, select the "print icon", this should install the print client (the first time you do this you may get an error but subsequent attempts should work).

You must do this in Internet Explorer, as SunSystems Windows Client does not have the privileges to install Active X components.

Schema Version Unmatched

The database version of SRS() is inconsistent with the SunSystems database (168.03) - please ensure all SRS tiers have been updated.

This message is displayed after upgrading to 6.2.1.

The solution is to run Data Access Manager DAR.

Method not found:'Void System.ServiceModel.Channels.SecurityBindingElement.set_AllowInsecureTransport(Boolean)'.

If your database server is running Windows 2008 R2, check that you have the hotfix for Windows Communication Foundation (WCF) in the Microsoft .NET Framework 3.5 Service Pack 1 (SP1) http://support.microsoft.com/kb/976462/en-us

The requested service, 'http://servername:94/SunSystemsQuery/Dictionary.svc' could not be activated. See the server's diagnostic trace logs for more information.

The first time you access a WC service it won't activate if there is less than 5% memory available. This is by design. You need to make sure the server you are running on has the minimum specification for a standalone box, i.e. 6GB.

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, namely: Server Monitor, SunDebug, SSC logging or Transfer Desk logging, or all of them. These tools are designed to display and log the SunSystems program behaviour and allow quick resolution of any system failures that are not identifiable by just the error messages alone. This feature 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 that diagnoses database connection problems. The program is called **databasetest.exe** and is installed in the **<sun5>\ssc\bin** folder. You should run the program from the command prompt. The **databasetest.exe** program has two modes of operation:

If it is run with no parameters, the program runs the complete suite of database tests, as follows:

- 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.

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.

SunSystems disaster recovery

SunSystems is a client/server application which is designed to run on multiple tiers. In case of disaster recovery, all the tiers should be checked for possible error. To resolve common issues, refer to the Troubleshooting section.

Database recovery and integrity

If any of the SunSystems databases require recovery, you must restore Security, Domain and all SunSystems Data databases from the same backup set. This should be done using the tools provided with the database, by a Database Administrator (DBA).

After successfully recovering the database, check the integrity of SunSystems database. The utilities provided with database setup include a database integrity check.

During the recovery process, if the database machine has been replaced, follow the steps below to use the new database server machine with SunSystems application server.

- Restore SunSystems databases (SunSystems data database, domain database and security database) on the new machine.
- Run the SunSystems database setup and choose the option to re-link the SunSystems data database and domain database. Check the database integrity using the database installer option.
- Update the **DOMN_DSRCE_CONFIG** table in the SunSystems domain database, to reflect the new database server details.

If the database server is also the SunSystems security server, install the SunSystems Security server by using the previous SunSystems security database. Refer to the SunSystems Security Server Recovery section for details.

If the SunSystems Security server is installed on the database server machine and SunSystems Security requires recovery, reinstall SunSystems Security server again after uninstall. Select the already existing SunSystems security database.

After following the above steps, the SunSystems database is ready to be used with application server.

SunSystems application server recovery

There may be three situations that may arise with the application server:

1. Case 1: The SunSystems application server is working. Database server machine has been replaced and the previous database recovered on the new machine.

Case 2: The SunSystems application server has crashed. Database is working without problem.

Case 3: Application server has crashed and needs to be replaced with another application server machine.

Case 1

If the database server has been replaced, update the SunSystems domain database details in User Manager > Settings > SunSystems > Configure.

Case 2

If the application server requires recovery, restore the server backup from the backup media. If the database server has been replaced, the application server must be updated to point to the new database server as follows:

1. Run User Manager and update the SunSystems domain database details.

If the SunSystems Security database was also installed on the replaced database server, update the SunSystems Security **Global.config** file, in **ProgramData\Infor\Sunsystems\Security**.

Update the server name according to the new security server name.

Case 3

If the application server machine crashes and needs to be replaced:

2. Re-install all the SunSystems application components. That is, application server, security client/server, etc. as on the previous application server.

During the installation, provide the existing SunSystems database server details.

Start the SunSystems Services on application server. These services are:

14. SunSystems Security Service
15. SunSystems Session Manager service
16. SunSystems Connect Server service.

After you start these services, check the central log repository for any possible error in the log files, for these services. Report any errors to SunSystems Technical Support.

Security server recovery

If the machine hosting the Security Server has been replaced, you must edit the **global.config** file used by SunSystems Reporting to reference the new machine. On the machine hosting the SunSystems Reporting Service, edit **global.config** found in **ProgramData\Infor\SunSystems\Security** and change the value of the **<host>** parameter to the new security server machine name.

Check the SunSystems client connectivity

When all the SunSystems services are running smoothly, try to log in to the SunSystems client. Any problems will be logged in the log files in the central log repository on the client machine. Check whether the SSC website is working.

If the issues persist in SunSystems Client, contact SunSystems Technical Support.

Contacting Technical Support

If you still experience problems, contact your designated Support Centre as outlined in your Software Maintenance Agreement. If you are supported directly by Infor, please log an incident at **http://www.InforXtreme.com**.

There is also a facility in InforXtreme to search the knowledgebase solutions for known issues. You could do this before logging an incident, as a known solution may provide the answer.

Please have ready the following details:

- SunSystems serial number and version number, which are displayed in SunSystems Help
- Platform operating system version and service pack or patch level
- Database and version
- Briefly define circumstances that relate to the error or problem
- Detail steps taken, which are required to replicate the problem
- Saved error message files as appropriate.

Glossary

19

Term	Definition
Application server component	Consists of all software elements that are installed on the designated application server, namely the application layer.
Business Unit Group	A collection of SunSystems Business Units that are stored in a single SunSystems data database. In other words, a SunSystems data database is a Business Unit Group. However, 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, which contains all the log files that are generated by SunSystems. Files are created in relevant folders under the central logs repository. For example: ProgramData\Infor\SunSystems\logs
Client component	Consists of all software elements that are installed on the client PC. Security Client, SunSystems Client, and Reporting Client are included in the SunSystems Client install.
Collation	A collective term for 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	An independent database in the SunSystems Domain; a central repository that contains information to facilitate connections to multiple SunSystems databases of different code pages through a single application server or application server farm.
Firewall	A protective channel through which all traffic between a secured network and an unsecured network must pass.
SunSystems Security	A blanket term that covers the services, applications, and features that control access to SunSystems programs and data.
SunSystems domain	A collective term for the one-to-many application server and SunSystems database installations, accessible through a client installation and managed through a central repository (Domain database). For example, a three-tier installation, or variations including an application server farm and access to multiple SunSystems databases.
SunSystems session	An open SunSystems window. You can open up to nine sessions at a time.

Appendix A TCP/IP Ports

A

SunSystems application server inbound ports

Component description	Port	location and configuration	Other information
SunSystems Connect Service	8080	Property Editor: tomcat, http_connector, port HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432 Node\SunSystems\Core\5.1\Comms\ConnectServicesListenerPort	SOAP interface and HTTP port
Session Manager Port Range	40100 to 40999	HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432 Node\SunSystems\Core\5.1\SessionManager\PORTRANGE1_MIN and PORTRANGE1_MAX Multiple ranges can be added, for example, PORTRANGE2_MIN and PORTRANGE2_MAX	MDMServices uses second port in range
Session Manager Listener Port	50000	HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432 Node\SunSystems\Core\5.1\Comms\SessionManagerListenerPort SUN5.ini SESSION-MANAGER-PORT=50000	
RMI Registry	50001	Property Editor: rmi, registry_port	SSC
Job Execution	50002	Property Editor job, server_port	SSC
Locator Service	50006	HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432\ SunSystems\Core\5.1\Comms\LocatorServiceListenerPort	
Transfer Execution	50008	HKEY_LOCAL_MACHINE\SOFTWARE\Wpw6432 Node\SunSystems\Core\5.1\Comms\TransferExecutionListenerPort	Transfer Desk
Transaction Monitor RMI Port Ranges	50050 to 50099	Property Editor: rmi, ports	SSC

Component description	Port	location and configuration	Other information
Configuration Service	40003 40004		Report Manager, Data Access Manager, SunSystems Report Server connect to Configuration Service
Secure Job Execution	55001	Property Editor: job, secure_server_port	SSC

SunSystems security server inbound ports

Component Description	Port	Location and Configuration	Other Information
SunSystems Web Security	81	IIS	SunSystems Security Web authentication
SunSystems Security	55000	`global.config` file located in: `ProgramData\Infor\SunSystems\Security`	

SunSystems Reporting (SRS) inbound ports

Component Description	Port	Location and Configuration	Other Information
SQL Server Reporting Services	80	SQL Server Reporting Services	
SRS	94	IIS	SunSystems Report Manager, Data Access Manager, and Report Server
SunSystems Report Manager Service	9000		
ASP.NET State Server	42424		Relevant to Multiple Report Server configurations with server to hold state

External firewall inbound ports - when deploying SunSystems Web based solution

Component Description	http port	https port	Other Information
SunSystems Web Security	81	82	
SunSystems Reporting Services	94	83	
SSC	8080	8443	
SunSystems Web	9080	9433	
SunSystems Web (proxied through IIS)	80	443	
Transfer Desk Web	9090	9091	

Appendix B Default folder structure and write permission requirements

B

SunSystems subfolders in Program Files(x86)

Default location \Program Files(x86)\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. [SunSystems] Sys-Work=C:\ProgramData\Infor\SunSystems_work\ User Manager/SecurityConsole enables you set the work folder at operator level within \ProgramData\Infor\SunSystems\ .
SunSystems_sql	.sql .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\Docs	.pdf .chm	SunSystems documentation in the form of guides (.pdf), and the documentation start menu (SSDocumentation.chm) are located in this folder. The application Help (.chm) and auxiliary files (.js and .png) are located in the <installation folder>.
SunSystems\Security Console	.dll .xml .js	Folders containing SecurityConsole IIS application files.

Folder name	File types	Description
SunSystems\ Security Web	.dll .js	Folders containing SecurityWebServer IIS application files.
SunSystems\ SSC	.xml .jar .dat .slc .bat .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 Property Editor.
SunSystems\ SunSystems Web	.conf .xml .dtd .jsp	Tomcat deployment files of SunSystemsWeb.
SunSystems\ TransferDesk Web	.dll	SunSystems TransferDeskWeb IIS application files.
SunSystems Reporting Services	.dll .config .exe	SunSystems Reporting Services IIS Website. DataAccessManager, ReportManager, and SunSystemsReportServer application files.

SunSystems subfolders in ProgramData

Default location \ProgramData\Infor

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

Folder name	File types	Description
SunSystems_work		Default location for work files e.g. for Ledger Entry
Logs\SunSystems\	.log	SunSystems and SRS log files
SunSystems\SunSystemsReporting	.srdl	SRS Example Report files for importing into Report Store database. Patched example reports are inserted here by the Patch Set procedure. The ransformed Output folder is the default location for transformed reports.
SunSystems\CheckOut	.sfl .dtd	This is the default client directory to hold Source Form Layout (SFL) files. Used by Form Designer, Filter Designer 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. The directory location is established during installation to \CheckOut\, in the SunSystems root directory. 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 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.

Folder name	File types	Description
SunSystems\ ClientFileDirectory	.dtd .msg .opx .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. Message files HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\SunSystems\Navigation Manager\5.1\FileCache\MSG DIRECTORY Form files HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\SunSystems\Navigation Manager\5.1\FileCache\RFX DIRECTORY
SunSystems\ RPTParams		Work folder for SRS
SunSystems\ ServerInfoCache		Folder to hold the cached information that is obtained from the server by Common Services. Used by Form Designer and Filter Designer. 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. The location of this directory cannot be changed.
SunSystems\ Security	.config	Location of SunSystems Security Global.config.
SunSystems\ MessageFiles	.msg	Message files.
SunSystems\ Databases	.mdf .ldf	Default location for SunSystems SQL Server Database files

IIS application SecurityWebServer requires read permissions to redirection.config. In File Explorer, navigate to **\Windows\System32\inetsrv**. Go to: Config folder > Properties > Security tab. Click Edit > Add > Locations. Select your local machine and click OK. Enter IIS AppPool\SecurityWebServer > Check Names and click OK. In Permissions, select Read & Execute and click OK.

Appendix C Changing location of SunSystems components in multi-tier configurations

C

Reconfiguring SunSystems client connections

Security Server, SunSystems application server and Connect service

Switch Server enables you to reconfigure SunSystems Client links to Security Server, and SunSystems Application Server.

Changing location of Microsoft SQL Server Reporting Services (SSRS)

Edit the DOMN_VRTL_HOST table and change the ACTUAL_HOST_NAME to the name of the SSRS server where VRTL-HOST-NAME = ms-app-ssrs and ms-app-ssrs-rm. When load balancing SSRS you may need to use the IP address.

Restart all SunSystems services and IIS.

Changing location of SunSystemsReportServer

Edit the DOMN_VRTL_HOST table and change the ACTUAL_HOST_NAME to the name of the SRS-RS Report Server server where VRTL-HOST-NAME = infor-app-rs. Restart all SunSystems services and IIS.

Changing location of SunSystems Report Manager

The SunSystems Domain database holds the location of SunSystems Report Manager. Edit DOMN_VRTL_HOST table. Select the row where DFLT_PATH = ‘ReportManager’ and update ACTUAL_HOST_NAME to the new name of the SunSystems Report Manager server. Restart all SunSystems services and IIS.

Moving SunSystems databases to a new database server

Note: These instructions assume your server has SQL Server database engine, SQL Server Reporting Services, and SunSystems Reporting Services - SQL Server Reporting Services extensions with the corresponding Patch Set installed.

1. Get all SunSystems users to log out. Check in User Manager, Operator Activity. Stop all SunSystems services. Backup your existing SunSystems Domain, SunSystems Security, and SunSystems Data, Report Store, and Report Store Temp databases on the source server.
2. Copy these back up files onto the new database server.
3. Stop SunSystems Services and SSRS.
4. Restore these databases into the new database instance.
5. In SQL Server Management Studio, go to the SunSystems Security database > Properties > Options > Service Broker > Broker Enabled and set to True.
6. Ensure that the SunSystemsServices group has db_owner role for the SunSystemsSecurity database. In SQL Server Management Studio, Logins, SunSystemsServices, Properties, User Mapping, select SunSystemsSecurity, select db_owner role, OK.
7. Re-check ODBC Data Source 32 bit connection and the setting in global.config located at ProgramData\infor\SunSystems\Security is correctly configured with the new server name.
8. Start SunSystems Security Service.
9. User Manager, Settings, SunSystems, Configuration, enter the new location of the domain database.
10. User Manager, Settings, SunSystems Activity, Clear all users.
11. Run Relink. Using the SunSystems installation DVD, Database Utilities, SunSystems Domain Utility menu, re-link SunSystems Data to SunSystems Domain. On the Relink Details dialog, make sure to overtype Instance Name with the new database server/instance name. Scripts should run without any errors.
12. Confirm database name is correct in the Domain Database table DOMN_DSRCE_CONFIG.

13. Start SunSystems Connect, Session Manager, and Configuration services.
14. Log into SunSystems and a message will be displayed saying a synchronization is required.
15. BUA, Explode All. Click on a Business Unit and from Actions synchronize. Synchronization completed successfully should be displayed. Repeat for each business unit.
16. Select the business unit, Actions, Put Online. Repeat for each business unit.
17. SunSystems Reporting: You have a choice. You can export out, and import in, the reports from Report Manager RMA, Action Menu. Alternatively, move the ReportServer databases as follows:
18. In Reporting Services Configuration Manager, stop Report Server.
19. Restore ReportServer and ReportServerTemp databases. Make sure that the SunSystemsReporting user has db_owner, public, and RSExecRole for these databases.
20. In Reporting Services Configuration Manager delete encrypted content, and start Report Server. (If SSRS is not used solely for SunSystems Reporting, deleting encrypted content may have implications on other systems using SSRS).
21. Edit DOMN_VRTL_HOST table to ensure that all SunSystems components have the correct ACTUAL_HOST_NAME.
22. Restart SQL Server Reporting Services Service, SunSystems services, and IIS.
23. Run DAR to re-create the data models.

Appendix D Application files

D

The following table shows the list of file types that constitute SunSystems:

File Suffix	File Type	Usage	
.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
.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

File Suffix	File Type	Usage	
.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 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
.xsl	File	Extensible Style sheet Language file, which contains information that is used to transform the structure of an XML document	Transfer Desk

Appendix E Infor Support Policy and installations running virtualization software / Terminal Services / Citrix Xenapp / other

Because an implementation using virtualization software has been correctly sized to provide adequate system resources, we will fully support SunSystems deployed in this environment for test environments and production environments.

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, but we reserve the right to ask a customer to reproduce the issue outside of a virtual environment if we believe that the issue might result from a failure of the abstraction layer, or its configuration, to provide a suitable application environment.

Appendix F Logging management

F

Diagnostics: Changing logging level

SunSystems application log

SunSystems COBOL application logging is controlled by **SUN5.ini** located in **Program Files (x86)\Infor\SunSystems**. There is a setting for Sun5 log as **Sun5-Log=1**. To produce detailed log files set this flag as **Sun5-Log=5**

After setting this flag, save the Sun5.ini file and restart SunSystems Windows services (Security, Connect, and Session Manager). Log files will be generated in **ProgramData\Infor\logs\SunSystems\Cobol**

The Log level 5 in Sun5.ini will generate detailed COBOL log. Please use this setting for diagnostic/testing purpose only and revert this level to 1 after the diagnosis/testing is over.

Java applications

SunSystems Connect

SSC server side log file Server.log is located in **ProgramData\Infor\logs\SunSystems\SSC** folder. In SunSystems, Property Editor, go to Logging > Simple > Server > Enabled. Click Modify and specify true/false.

To increase logging level, Select the Logging > Simple > Server > Level and click Modify. Select ALL from the popup dialog box and click OK. Save the changes in Property Editor and click Exit. To make these settings work, SunSystems Connect service must be restarted. Please revert after diagnostics/testing.

.NET applications

User Manager

.NET application. The User Manager log file is produced in the **ProgramData\Infor\Logs\SunSystems\User Manager** folder on the SunSystems Security Server. The logging level of this file can be changed on the Security Server by setting the log level in **UserManager.adv.su.Config.xml**, in **Program Files (x86)\Infor\SunSystems**. Open this file in Notepad (run as administrator), set the value as follows, and save:

```
<application name="UserManager" level="DEBUG"
```

```
advfilename="UserManager.adv.SU.Config.xml" />
```

Level=ALL is the most detailed setting. Beware the log files become very large. Please revert the logging level to INFO after you complete testing.

Transfer Desk Web

Activate .NET log4net DEBUG by amending `TransferDeskWebServer.Adv.SU.Config.xml`

`Program Files (x86)\Infor\SunSystems\TransferDeskWeb\TransferDeskWebServer.SU.Config`

For diagnostic purposes the logging level can be changed to `DEBUG` in the following line:

```
<level value="INFO" />
```

You must restart the SunSystems Transfer Desk Web Service.

The log file is produced `\ProgramData\Infor\Logs\SunSystems\TransferDeskWebServer\TransferDeskWebServer.log`

Change back to `INFO` after you have completed testing.

SRS Report Server/Report Manager

The same method for altering logging applies to SunSystems Reporting Services as it is a .NET application.

Security Server

Folder	Application	Controllable Yes/No	How/Where
C:\ProgramData\Infor\Logs\SunSystems\DBDeployer	Patch Set Deployer Tool	No	Automatically reports when the program …V6.2_PS20 for Database Tier\DBDeployer\SunSystems.Patches.DBDeployer.exe is used to apply patches to the Database.
C:\ProgramData\Infor\Logs\SunSystems\FilterDDRegeneration	Filter Regeneration (FLR)	No	Is populated when the function FLR is run within SunSystems.
C:\ProgramData\Infor\Logs\SunSystems\FormCompiler	Form Compilation (FRC)	No	Is populated when the function FRC is run within SunSystems.
C:\ProgramData\Infor\Logs\SunSystems\Install	Installations, Upgrades any functions from the Database Utilities folder.	No	Is populated mostly when the Database Utilities program is executed - InforSunSystems621\SqlServerDatabase Utilities\setup.exe.
C:\ProgramData\Infor\Logs\SunSystems\ReportAdministrator	SunSystems Report Administrator	No	Automatically reports when the program is used.
C:\ProgramData\Infor\Logs\SunSystems\Security	Used by SunSystems User Manager function and the SunSystems Security Service modules.	No	Automatically logs when the program is used and records user activity.

C:\ProgramData\Infor\Logs\SunSystems\SunSystems.V5	Records activities around the actual issues involved while logged into SunSystems and calling the various functions.	No	Via the file C:\Program Files (x86)\Infor\SunSystems\SUN5.ini

Application Server

Folder	Application	Controllable Yes/No	How/Where
C:\ProgramData\Infor\Logs\SunSystems\Cobol	SunSystems	No	Automatically reports messages when the COBOL aspects of the underlying functions have issues.
C:\ProgramData\Infor\Logs\SunSystems\DataAccessManager	Data Access Manager (DAR)	No	Automatically reports when the function DAR is used.
C:\ProgramData\Infor\Logs\SunSystems\DBDeployer	Patch Set Deployer Tool	No	Automatically reports when the program …V6.2_PS20 for Database Tier\DBDeployer\SunSystems.Patches.DBDeployer.exe is used to apply patches to the Database.
C:\ProgramData\Infor\Logs\SunSystems\FilterDDRegeneration	Filter Regeneration (FLR)	No	Is populated when the function FLR is run within SunSystems.
C:\ProgramData\Infor\Logs\SunSystems\FormCompiler	Form Compilation (FRC)	No	Is populated when the function FRC is run within SunSystems.
C:\ProgramData\Infor\Logs\SunSystems\Install	Installations, Upgrades any functions from the Database Utilities folder.	No	Is populated mostly when the Database Utilities program is executed - InforSunSystems621\SqlServerDatabase Utilities\setup.exe
C:\ProgramData\Infor\Logs\SunSystems\Navigator	The SunSystems interface when users log into the SunSystems application.	No	Most action within the SunSystems application.
C:\ProgramData\Infor\Logs\SunSystems\ReportDesigner	SunSystems Report Designer	No	Automatically reports when the program is used.
C:\ProgramData\Infor\Logs\SunSystems\ReportAdministrator	SunSystems Report Administrator	No	Automatically reports when the program is used.
C:\ProgramData\Infor\Logs\SunSystems\Dataload	Used by SunSystems Internal Functions – DB Utilities.	No	Automatically reports when Database Utilities tries to load Demo Data.
C:\ProgramData\Infor\Logs\SunSystems\MenuImportExport.V5	Used by SunSystems Menu Import/Export function.	No	Automatically reports when the program is used.
C:\ProgramData\Infor\Logs\SunSystems\Security	Used by SunSystems User Manager function.	No	Automatically logs when the program is used and records user activity.
C:\ProgramData\Infor\Logs\SunSystems\SqlInstaller	Collects information relating to data movements in and out of SunSystems using the SSC (SunSystems	No	Automatically logs when modules are used which involves requesting and/or modifying data.

	Connect program modules.		
C:\ProgramData\Infor\Logs\SunSystems\SSC	Collects information relating to data related communications with the Database.	Yes	The levels of logging can be modified via the file D:\Program Files (x86)\Infor\SunSystems\SSC\bin\PropertyEditor.exe. This program allows users to decide.
C:\ProgramData\Infor\Logs\SunSystems\SunSystems.V5	Records activities around the actual issues involved while logged into SunSystems and calling the various functions.	Yes	Via the file C:\Program Files (x86)\Infor\SunSystems\SUN5.ini

Web Server

Folder	Application	Controllable Yes/No	How/Where
C:\ProgramData\Infor\Logs\SunSystems\FilterDDRegeneration	Filter Regeneration (FLR)	No	Is populated when the function FLR is run within SunSystems.
C:\ProgramData\Infor\Logs\SunSystems\FormCompiler	Form Compilation (FRC)	No	Is populated when the function FRC is run within SunSystems.
C:\ProgramData\Infor\Logs\SunSystems\Install	Installations, Upgrades any functions from Database Utilities folder.	No	Is populated mostly when the Database Utilities program is executed - InforSunSystems621\SqlServerDatabase Utilities\setup.exe
C:\ProgramData\Infor\Logs\SunSystems\Security	Used by SunSystems User Manager function.	No	Automatically logs when the program is used and records user activity.
C:\ProgramData\Infor\Logs\SunSystems\SunSystems.V5	Records activities around the actual issues involved while logged into SunSystems and calling the various functions.	Yes	Via the file C:\Program Files (x86)\Infor\SunSystems\SUN5.ini
C:\ProgramData\Infor\Logs\SunSystems\SunSystemsWeb	Logs a combination of modules which govern using all aspects of SunSystems Web.	No	Automatically logs when the Web Interface program modules are used.
C:\ProgramData\Infor\Logs\SunSystems\TransferDeskWebServer	Logs the modules which relate to invoking SSC within the web interface.	No	Automatically logs when the TransferDesk web interface program modules are used.

Reporting Server

Folder	Application	Controllable Yes/No	How/Where
C:\ProgramData\Infor\Logs\SunSystems\DataAccessManager	Data Access Manager (DAR)	No	Automatically logs when the DAR module is invoked to perform the functions relating to the management of Business Unit Models for Reporting.
C:\ProgramData\Infor\Logs\SunSystems\Install			
C:\ProgramData\Infor\Logs\SunSystems\ReportServer			
C:\ProgramData\Infor\Logs\SunSystems\ReportDesigner	This program is used to design reports.	No	Automatically logs when the Report Designer program is used.

C:\ProgramData\Infor\Logs\SunSystems\ReportAdministrator			
C:\ProgramData\Infor\Logs\SunSystems\ReportStoreMigrate	Keeps track of issues relating to migration of reports between Patch Set levels.	No	Automatically generates the logs when the Report Migration module is used.
C:\ProgramData\Infor\Logs\SunSystems\SunSystemsReportingPrintService	Logs issues relating to the backend processes involved in rendering reports to the screen and other output format required.	No	Automatically generates the logs when the service is used.
C:\ProgramData\Infor\Logs\SunSystems\SunSystemsReportManager	Logs the internal processes relating to presenting the Reports for users.	No	
C:\ProgramData\Infor\Logs\SunSystems\SunSystemsReportServer	Logs the internal processes relating to communications with SQL Reporting Services.	No	
C:\ProgramData\Infor\Logs\SunSystems\VisionImport		No	

Reporting Servers – Houses SQL Server Reporting Services and SunSystems Reporting Services Extensions

Folder	Application	Controllable Yes/No	How/Where
C:\ProgramData\Infor\Logs\SunSystems\DataAccessManager	Data Access Manager (DAR)	No	Automatically logs when the DAR module is invoked to perform the functions relating to the management of Business Unit Models for Reporting.
C:\ProgramData\Infor\Logs\SunSystems\Install			
C:\ProgramData\Infor\Logs\SunSystems\ReportServer	Logs connectivity to SQL Reporting Services Via SunSystems Reporting Extensions	No	Automatically logs how connection requests are made to SSRS.

Appendix G Administrative access recovery

G

There are several scenarios when the administrator may be unable to access User Manager. For example, User Manager may be inaccessible due to incorrectly mapped Windows authentication credentials or the designated administrator leaving the company without handing over access to another user.

To overcome this, the following steps must be carried out by a local administrator of the server where the Security Service is running:

1. Ensure all users are logged out of the system.
2. Stop the SunSystems Security Service.
3. Edit the global.config file. Normally 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. 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 back to `0`.
9. Allow users to log in to the system.

Note: This feature should only be used when the administrator is unable to access the system to correct problems in the configuration.

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.