INSTALLATION GUIDE – ORACLE

Infor10 Financials Business (SunSystems)

Infor10 Financials Business (SunSystems) – Installation Guide – Oracle
Based on software version 6.1.1 – document version D, February 2012

Infor
1 Lakeside Road
Aerospace Centre
Farnborough
Hampshire
GU14 6XP
United Kingdom
Phone: +44 (0) 1252 556000

Contents

Part 1 – Installation

What's New in SunSystems

This new version of SunSystems integrates with Microsoft SharePoint through Infor10 Workspace and is web browser enabled for most SunSystems functions. SQL Server Reporting based SunSystems Reporting Services (SRS) replaces the SunSystems v5 reporting solution. SunSystems Security installation is now integrated into the SunSystems application installer. Full details of SunSystems enhancements are described in the SunSystems Upgrade Guide.

> **Note:** The Oracle version of SunSystems requires Microsoft SQL Server Reporting Services and Database.

Installing SunSystems

If you are upgrading from an earlier version of SunSystems, you must refer to the SunSystems Upgrade Guide.

> **Note:** Following the installation, you must install SunSystems v6.1 Patch Set 5 or later, because it contains critical fixes and functionality without which SunSystems may not function correctly.

Prerequisites

Installation on 64-bit Operating Systems

SunSystems is a 32-bit application, but it can be used on 64-bit operating system in emulate mode. Therefore, the application can access only 32-bit resources of a 64-bit operating system. SunSystems can use only the 32-bit Oracle client to access a 64-bit Oracle database. SQL Server Reporting Services (64 bit) requires 64 bit Oracle client.

If installing 32 bit and 64 bit Oracle clients on the same machine, ensure the second client installation gets a different oracle home name by launching the oracle client installer from the command prompt using SETUP.EXE with the argument ORACLE_HOME_NAME='Oracle Home Name', for example, SETUP.EXE ORACLE_HOME_NAME=Ora_Client_32.

> **Note:** 64-bit Oracle comes with the 64-bit Oracle Client only. To use SunSystems with 64-bit Oracle, a separate installation of 32-bit Oracle Client is necessary on all tiers.

SharePoint Installation to host Infor10 Workspace and SunSystems Plug-in

Refer to the following documentation available on InforXtreme Support:

- Infor10 Workspace documentation
- Infor10 Financials Business (SunSystems) Quick Start Guide: SunSystems / Workspace / ION. The Quick Start guide describes a demonstration installation procedure for SunSystems v6.1 with Workspace using an SQL Server database. The instructions for the SunSystems Plug-in are also consistent with an Oracle database platform.

Stand-alone Installation

- Windows 7, Windows 2008 R2, or Windows 2008
- .NET Framework 3.5.1 Features
- SunSystemsReporting local Windows user (a user name of your choice can be used)
- SunSystemsServices and SunSystemsClients local Windows groups (alternative names can be used)
- Internet Information Services 7 (IIS) or above
- Web Services Enhancements 3.0 (WSE)
- Microsoft Message Queue (MSMQ)
- Adobe Reader
- Oracle Server Edition 11gR1 or 11gR2 (Standard or Enterprise) must be installed

- Oracle 32 bit Client Edition 11gR1 or 11gR2 if 64 bit database is used (Administrator or Custom, installed to a different home directory)
- SQL Server 2008 R2 Reporting Services, and configure using Reporting Services Configuration Manager
- Microsoft Report Viewer 2010 SP1.

Database Server

- Oracle Server Edition 11gR1 or 11gR2 (Standard or Enterprise) must be installed, the minimum supported versions of Oracle 11gR1 and 11gR2 are 11.1.0.6 and 11.2.0.1 respectively
- The database can be hosted on any of the supported platforms specified by Oracle for the Oracle Database 11gR1 or 11gR2 editions
- Oracle 32 bit Client Edition 11gR1 or 11gR2 if 64 bit database is used (Administrator or Custom, installed with a different home name and to a different home directory to any other existing Oracle client installation)
- You must create an appropriate Oracle Database Instance to hold each language variant that you require
- You must know the passwords for Oracle users 'SYS' and 'SYSTEM', which are a mandatory requirement for the SunSystems Installer
- The Windows Registry key NLS_LANG in the relevant Oracle Home entry to be set to match the character set of the underlying database
- The Windows Registry key NLS_SORT in the relevant Oracle Home set to 'BINARY'
- The global_names database parameter must be set to 'False'
- The remote_os_authent parameter must be set to 'True' for Unix/Linux installations. Although this parameter is deprecated in Oracle 11gR2, SunSystems makes reference to it
- The SQLNET.AUTHENTICATION_SERVICES parameter in file SQLNET.ORA (located in the OracleHome\network\admin folder) should be set to include 'NTS'
- Ensure that the tnsnames.ora entries for the database instances are the same across all tiers
- Ensure that the database parameters for sessions, processes, and transactions are set to a sufficiently high level for the number of concurrent SunSystems v5 users and processes that will run

Note: In a multi user environment, this number should be raised to a higher value to accommodate all users.

- Ensure that the Oracle recyclebin feature is turned off
- The hidden parameter "_optimizer_join_elimination_enabled" should be set to false. This is to workaround Oracle Bug#9050716.
- If you intend to import the preconfigured SunSystems Dump file, you must ensure that you have created a tablespace called 'USERS', and that the schema that you intend to import into has been granted an unlimited quota on 'USERS'.

SunSystems Security Server

- Windows 2008 R2, or Windows 2008
- .NET Framework 3.5.1 Features
- Oracle 32 bit Client Edition 11gR1 or 11gR2 ('Administrator' level).

SunSystems Security Web Service

- Windows 2008 R2, or Windows 2008
- .NET Framework 3.5.1 Features
- Internet Information Services 7 (IIS) or above
- Web Services Enhancements 3.0 (WSE).

SunSystems Application Server

- Windows 2008 R2, or Windows 2008
- .NET Framework 3.5.1 Features
- Internet Information Services 7 (IIS) if Security Server is to be installed.
- Oracle 32 bit Client Edition 11gR1 or 11gR2 ('Administrator' level) must be installed.
- You must know the passwords for Oracle users 'SYS' and 'SYSTEM', which are a mandatory requirement for the SunSystems Installer.
- The Windows Registry key NLS_LANG in the relevant Oracle Home entry to be set to match the character set of the underlying database.
- The Windows Registry key NLS_SORT in the relevant Oracle Home set to 'BINARY'.
- The SQLNET.AUTHENTICATION_SERVICES parameter in file SQLNET.ORA (located in the OracleHome\network\admin folder) should be set to include 'NTS'.
- Ensure that the tnsnames.ora entries for the database instances are the same across all tiers.

SQL Server Reporting Services

- Windows 2008 R2, or Windows 2008
- SQL Server 2008 R2 Reporting Services and Database and configure using Reporting Services Configuration Manager
- Web Services Enhancements 3.0 (WSE)
- Microsoft Report Viewer Redistributable 2010 SP1 (Full Installation)
- Oracle 64 bit Client Edition 11gR1 or 11gR2 (Administrator level) for 64 bit SQL Server
- Oracle 32 bit Client Edition 11gR1 or 11gR2 (Administrator level) for 32 bit SQL Server.

SRS Report Server

- Windows 2008 R2, or Windows 2008
- .NET Framework 3.5.1 Features
- SunSystemsReporting (or alternative) Windows Domain user
- Internet Information Services 7 (IIS) or above
- Web Services Enhancements 3.0 (WSE)
- Oracle 32 bit Client Edition 11gR1 or 11gR2 ('Administrator' level).

SRS Report Manager

- Windows 2008 R2, or Windows 2008
- .NET Framework 3.5.1 Features
- SunSystemsReporting Windows Domain user
- Internet Information Services 7 (IIS) or above
- Web Services Enhancements 3.0 (WSE)
- Microsoft Message Queue (MSMQ)
- Oracle 32 bit Client Edition 11gR1 or 11gR2 ('Administrator' level)
- Microsoft Report Viewer 2010 SP1.

SunSystems Web Server

- Windows 2008 R2, or Windows 2008.
- .NET Framework 3.5.1 Features.

Client Machines

- Windows 7, or Windows XP
- .NET Framework 3.5.1 Features.
- Adobe Reader
- Oracle 32 bit Client Edition 11gR1 or 11gR2 ('Administrator' or 'Custom' level) must be installed.
- The Windows Registry key NLS_LANG in the relevant Oracle Home entry to be set to match the character set of the underlying database.
- The Windows Registry key NLS_SORT in the relevant Oracle Home set to 'BINARY'.
- The SQLNET.AUTHENTICATION_SERVICES parameter in file SQLNET.ORA (located in the OracleHome\network\admin folder) should be set to include 'NTS'.
- Ensure that the tnsnames.ora entries for the database instances are the same across all tiers.

Browser Clients

- Adobe Reader web application
- Internet Explorer 8.

Installing the Prerequisites

- Ensure that you have uninstalled any previous installation of SunSystems and SunSystems Reporting Services.
- Ensure that each server is able to be resolved through the name resolution method being used, such as DNS or WINS.
- Ensure that no other applications are currently running. Ensure that you have sufficient disk space on the target machine(s) and that you have installed all of the required prerequisite software (refer to the section Hardware and Software Requirements).
- If you are reinstalling SunSystems in order to change the initial installation type, such as from a stand-alone installation to a two-tier thin installation, ensure that you have taken a copy of your Domain schema and your SunSystems schema(s) and forms. If you recreate the Domain schema and add the SunSystems schemas back into it, a new set of ServerFiles is created.

Users and Services

Log in as a user that is member of the local Windows Administrator group. Create local Windows user SunSystemsReporting with password never expires. Make a note of the password entered. (Alternative names can be used).

SunSystems services can be run under local system account. However, SunSystems Security requires a domain account; the local system account is not supported.

> **Important Note:** Before you start the installation on each tier with a SunSystems Windows service, you should ensure that the domain service account has local security policy log on as a service rights in Local Policies, User Rights Assignment.

Folder Permissions

Minimum requirements for the service accounts are Full control for `ProgramData\Infor\` and Read & execute permission for `Program Files(x86)\Infor\`.

The SunSystems Connect service account, for example, svc-ssconnect requires Modify permission for `Program Files(x86)\Infor\SunSystems\SSSystem.dat` during SunSystems Serialization.

IIS Application Pool Identity SecurityWebService requires modify permission for `C:\Program Files (x86)\Infor\SunSystems\SecurityWeb` folder, and through Properties, Security, Advanced, read permission for `C:\Windows\System32\inetsrv\config` folder.

Installing Microsoft Internet Information Services 7 (IIS)

If you are installing on **Windows Server 2008 R2**, in Server Manager, Add Role, Web Server (IIS). Check the following Role Services are added to the IIS install.

- 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 Metabase Compatibility, IIS 6 WMI Compatibility, IIS 6 Scripting Tools, IIS 6 Management Console

If you are installing on **Windows 7**, in Control Panel, Programs and Features, Turn Windows Features on or off. Check that the following Features (click '+' plus to expand to individual features) are added to the Internet Information Services installation.

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

Installing Microsoft Message Queue (MSMQ)

This is a Microsoft feature and can be installed as follows:

- Windows Server 2008 R2: Server Manager, Features, Add Features, Select Message Queuing Server
- Windows 7: Turn Windows Features On or Off, Microsoft Message Queue (MSMQ) Server Core

Installing Web Services Enhancements 3.0 (WSE)

Download from the Microsoft web site and install in the following mode:

Setup Type: Install Runtime

Installing Oracle

As described in Prerequisites section, Oracle 11g or higher is supported for SunSystems v6.1.

Locate and copy the file `ORASQL11.DLL` (located in the OracleHome `\BIN` folder) to the same location. Rename the copied file as `ORASQL10.DLL`. Repeat this on each SunSystems Application Server machine.

Installing SQL Server (for Reporting Services server)

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

If a SQL Server named instance or alias is used, the SQL Server Browser Service must be started as it is required in order 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.

If installing a named instance ' 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>', 'data access', 'true';
```

If installing a fresh installation of SQL Server you must install Database Engine Services, and Management Tools, and as a minimum, and Reporting Services on the machine you are running SSRS.

If SQL Server is already installed you will need to select Microsoft SQL Server 2008, Configuration Tools, SQL Server Installation Center and add to your existing instance Reporting Services.

In SQL Server Configuration Manager, SQL Server Network Configuration, Protocols for MSSQLSERVER, make sure that TCP/IP is enabled. Now check SQL Native Client 10.0 Configuration, Client Protocols, that TCP/IP is also enabled here.

Installing SQL Server 2008 R2 Reporting Services

If you already have SQL Server installed and need to add Reporting Services, run the SQL Server 2008 R2 installer, SQL Server Feature Installation.

Instance Features, select Reporting Services and Next to proceed with the installation of Reporting Services.

On completion of the installation of SQL Server Reporting Services, it is essential for this to be configured in the next step.

Microsoft ReportViewer 2010 SP1

SunSystems Reporting Services has been adapted to use the latest version of ReportViewer control, specifically ReportViewer 2010 SP1. As a prerequisite for the installation of this release, the redistributable must be installed on the machine hosting the SunSystems Report Manager. A warning message is displayed if this has not been installed.

The redistributable and set of language packs are available from the following links:

http://www.microsoft.com/downloads/en/details.aspx?FamilyID=3eb83c28-a79e-45ee-96d0-41bc42c70d5d

http://www.microsoft.com/downloads/en/details.aspx?FamilyID=CC14EFF2-D47B-43A5-A139-FBB01E5F2836&displaylang=en

If the SunSystems Report Manager web application has already been installed, then it must be restarted after installing ReportViewer 2010 SP1. If you install ReportViewer 2010 SP1 before installing Reporting, then no restart is required.

Configuring SQL Server 2008 R2 Reporting Services using Reporting Services Configuration Manager

1. SunSystemsReporting (local or domain) Windows user will be given appropriate permissions to ReportServer and ReportServerTempDB databases. Make sure you are logged on as a user with sysadmin role for the database server to enable these permissions to be set.
2. From the Start menu run SQL Server 2008 R2 >> Configuration Tools >> Reporting Services Configuration Manager. Select the reporting services server and instance name.
3. Enter Server Name and Report Server Instance and click Connect.
4. Select Service Account. Report Server Service Account select Use another account. Enter account details for the SunSystems Reporting Services Windows user, for example, SunSystemsReporting, and password. Click Apply. You may be required to enter a backup encryption key file name and password; make a note of this file name and location.
5. SQL Server Connection Dialog is displayed. For Credentials Type select Current User – Integrated Security (ensure that 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, and if apply button is disabled, click enter.
7. In the Database tab, ensure that the ReportServer database has been created.

Checklist for SQL Server Reporting	✓
SQL Server ReportServer and ReportServerTempDB databases have been created	
Reporting Services Configuration Manager check Report Manager URL link is working	
Reporting Services Configuration Manager check Web Manager URL link is working	

Adobe Reader

This is available from the Adobe website.

SunSystems Installer Features

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

- Silent Installation: SunSystems installer supports express installation, which runs as silent installation. This is possible through a parameter file created by Installer. All the required parameters will be saved in the parameter file and the installer will not ask for them during installation. For example, at a command prompt, enter: `setup /v "qn"`. This uses `OracleExpress.xml` for parameters. For an explanation of parameters, see `OracleTemplate.xml`.
- Administrative Installation: Using this feature, SunSystems installation files can be 'unzipped' on a shared location. All the installation parameters that are given during the administrative install will be used as defaults for subsequent installations on client machines. During this unzip process, a new MSI installer file will be generated, which should be passed to client machines for further installation. The newly created MSI will take all the defaults from the network location, and software will be installed on demand.
- Installation through command prompt: This feature enables SunSystems installation through 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 machines on the network at the same time.
- Installation using management application, such as Microsoft SMS: SunSystems installer supports installation through Microsoft Systems Management Server (SMS).

Installing Stand-Alone

Before you start, ensure that you have installed the prerequisites required for a standalone installation and you are logged in as a user member of the local Windows administrator group. If you have default instance of Oracle, you can use the Express installation option. The OracleExpress.xml file must be modified first; see SunSystems Installer Features section above for more information.

The installation is a two-step process:

1. Server and Client components
2. Reporting Services.

Insert the DVD and if "Install Products" dialog is not displayed, run `setup.hta` from the `Oracle\DatabaseUtilties` folder on the installation media. Select Server & Client Components. At the "Setup type" dialog select Express, which installs a full stand-alone installation with default settings.

Upon completion of the SunSystems installation, return to the Install Products dialog and select "Reporting Services" and select the Complete installation option.

Alternatively, you can follow the instructions for Installing Two-Tier server using the Complete installation option.

> **Note:** After you finish using an installer option you may have to wait a few seconds before selecting another option.

Now go to the Post-Installation Configuration section.

Installing Two-Tier

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, make sure 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 an Oracle default instance is installed and pre-configured SunSystems data is required, an express installation can be done instead of a complete install.

1. From the installer menu, Installations for an Oracle environment, select Server & Client Components then Complete installation.

2. If a new or preconfigured SunSystems schema is required, check the check box to install a SunSystems schema on the next dialog.
3. Select 32 bit Oracle home.
4. SunSystems Security Schema Connection: Select the local database instance where the security schema will be created, enter 'system' dba user and password.
5. SunSystems Security Oracle Tablespace: Select Create New User, and accept the default Schema Owner and tablespace names.
6. SunSystems Domain Schema: Enter TNS name, 'system' dba user and password, 'sys' sysdba user name and password, and accept local Oracle domain schema name and enter domain schema password. You must confirm you want to create the domain schema.
7. Tablespaces for SunSystems Domain Schema: Select the tablespace name to assign tables to, the tablespace name to assign table indexes to, and the tablespace name for use during temporary database operations.
8. Create/Import SunSystems Schema: Select 'Import a pre-configured schema' or 'Create a Sunsystems Schema'.
9. SunSystems Schema Business Unit Group Name: Accept default name BUGROUP
10. Pre-configured Schema Variants: Use this option to select a pre-configured business unit in the desired language.
11. SunSystems Schema: Enter SunSystems Data Schema Account password.
12. Tablespaces for SunSystems Schema: Select the tablespace name to assign tables to and the tablespace name for use during temporary database operations.
13. SunSystems Security Settings: Enter a security admin password and accept default English language and default ports 55000 and 81 for SunSystems Service and SunSystems WEB IIS respectively. The password is blank by default.
14. Security Service Account: Enter user name, password and domain information. A domain account is mandatory.
15. SunSystems Service Account: As the database and application are on the same machine, you can use local system account.
16. SunSystems Web Service Account: As the database and application are on the same machine, you can use local system account.
17. SunSystems Reporting Services:
18. Installation Type: select complete. Specify your local machine for Security Server, SunSystems Report Server name and the SunSystems Report Manager. Accept default ports for both.
19. Select Oracle home for the local 64 bit Oracle database,
20. SunSystems Domain connection: enter the DOM schema password.
21. For the security schema, enter DBA User and Password e.g. system manager
22. Enter the password for SunSystemsReporting user.
23. Select the SQL Server Reporting Services instance.
24. Enter the SMTP Server details – you must enter a port number at least e.g.25
25. Complete the installation.

Infor10 Workspace

A server hosting Microsoft SharePoint 2010 can be added to this configuration to host SunSystems in Workspace. See the Installing the Infor10 Workspace SunSystems Plug-in section within this guide.

Installing SunSystems Client in a Two-Tier Installation

1. Installations for an Oracle environment >> Server and Client Components >> Custom installation.
2. Selecting Features: From the software components feature tree, select SunSystems Client only by de-selecting application server and security server features. (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 go to the Post-Installation Configuration section.

Installing a Multi-Tier Configuration

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, it is important to start by creating the SunSystems Domain schema first, followed by Security server. Subsequent components do not require installation in a strict order.

Multi-tier server example names (given in brackets)

ServerDB	Database Server
ServerAPP	SunSystems Application Server
ServerWEB	SunSystems Web Server
ServerSSRS	SQL Server Reporting Services Server
ServerRS	SunSystems Report Server
ServerRM	SunSystems Report Manager
SharePointServer	Infor10 Workspace hosted in SharePoint
Client1	SunSystems Client machine

Note: After you finish using 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.

Database Server

The first stage is to create the Domain schema, then the SunSystems Security schema, then the SunSystems Data schema (Business Unit Group).

Create a New SunSystems Domain Schema

1. On your Database Server (ServerDB) launch the installer and select Database Utilities (Oracle).
2. Select Create a new SunSystems Domain Database Schema.
3. Select 32 bit client Oracle home.
4. The user enters TNS name – domain schema name, for example DOM, domain password, system dba user name and password, sys dba user name and password.
5. Select the tablespace name for tables, indexes and temporary use.
6. Proceed with the installation, and when processing is complete return to the database utilities menu.

Create a new Security Schema

1. From the installer Database Utilities (Oracle) menu select Create a new Security schema.
2. Select Oracle home.
3. Enter TNS name, SunSystems security schema name e.g SunSystemsSecurity, system dba user name and password, sys dba user name and password.
4. Select the tablespace name for tables, indexes and temporary use.
5. Enter the service account name, password, domain information to create OPS account.
6. Proceed with the installation, and when processing is complete exit to main installer menu.

Create a new SunSystems Data Schema (Business Unit Group)

1. If preconfigured data (PK1) is required, choose from Database Utilities (Oracle) - Import a pre-configured SunSystems Data Schema, otherwise select Create a new SunSystems Data Schema.
2. Select 32 bit Oracle home.
3. Accept the domain schema details created in the domain schema installation.
4. Enter the Business Unit Group name e.g. BUGROUP
5. Enter TNS name, SunSystems schema name e.g. SUN, and password, system dba user name and password, sys dba user name and password.
6. Select the tablespace name for tables, indexes and temporary use.
7. Select base language and additional languages to be used with this Business Unit Group.
8. Proceed with the installation, and when processing is complete return to the installer main menu.

Installing SunSystems Application Server (Including Security)

1. On the application server (ServerAPP) the user selects Installations for an Oracle environment, Server & Client Components and then Complete install if you also want to install SunSystems Web.
2. Do not install a SunSystems schema.
3. Choose 32 bit Oracle client.
4. In Security dialog select TNS name, Oracle DBA user and password.
5. Select TNS name, SunSystems Domain schema name, system user and password, sys dba user and password.
6. Enter a Windows domain account (an OPS$ account) for SunSystems services. Make sure this account has Modify permissions for the `C:\Program Files (x86)\Infor\SunSystems\SecurityWeb` folder, and Read permissions for the `C:\Windows\System32\inetsrv\config folder`.
7. Specify Report Server (ServerRS) and Report Manager (ServerRM) and SQL Server Reporting Services Server (ServerRS).
8. Ready to install the program.
9. SunSystems installation completes.

Add SunSystems Reporting Service Group Membership to SunSystems Users

1. If preconfigured data (PK1) has been installed, and User Migration has been run, 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 on 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 – Application Server

	✓
Check Windows Service SunSystems Session Manager is running.	
Check Windows Service SunSystems Connect is running.	
You should be able to access the SSC web page `http://localhost:8080/ssc`	

Installing SunSystems Web

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

1. On the web server machine (ServerWEB) run the installer.
2. Select Installations for an Oracle environment, Server & Client Components, and then Custom installation.
3. From the feature tree, select SunSystems Client and SunSystems Web only.
4. Enter server locations of SunSystems Security, SunSystems Application, Report Server and Report Manager.
5. Proceed with the installation until it is complete.

Internet Explorer 8 Settings

To access SunSystems Web in Internet Explorer 8 go to Tools >> Compatibility View Settings, and remove the check from Display intranet sites in compatibility view.

If you want SunSystems reports to appear in a new tab: change the default setting in Internet Explorer From the menu bar, select Tools >> Internet Options >> General >> Tabs >> Settings >> 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. Log in to User Manager as administrator, select Groups tab, edit SunSystems Users Group, Select Operator Group and tick Enable Clear Operator at login.

Silverlight 4

When first accessing SunSystems Web you may be prompted to follow instructions to install Silverlight 4.

Post-Installation Checklist – SunSystems Web

	✓
Ensure SunSystemsWebService Windows Service is started	
http://localhost:9080/SunSystems gives you access to browser based SunSystems interface. This is running in Apache Tomcat.	
http://localhost:81/SecurityWebServer to check that security web service is running in IIS	

Infor10 Workspace

A server hosting Microsoft SharePoint 2010 can be added to this configuration to host SunSystems in Workspace. See the Installing the Infor10 Workspace SunSystems Plug-in section within this guide.

Installing SunSystems Client in a Multi-Tier Installation

1. On the client machine, for example, Client1, Installations for an Oracle environment, Server & Client Components, choose custom installation.
2. In the component tree, deselect the other components leaving SunSystems Client only. (SunSystems client includes Security client and SunSystems Reporting Services 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 machines when users are not logged on as Windows Domain users, you will need to set standard authentication globally in User Manager. Log into User Manager as administrator, select Settings >> Security Policy, and remove the check from Enable Windows Authentication.

Installing SunSystems Reporting Server

SunSystems Reporting can be installed all on one server together with SQL Server Reporting Services. In this case, select Complete to install all three SunSystems Reporting Services components at the same time. Alternatively, it can be split up to 3 reporting components installed on separate servers. In this case you must install in the following order: SQL Server Reporting Services extension first, SunSystems Report Server next, and then SunSystems Report Manager.

SQL Server Reporting Services Extensions

1. Check that you have installed the appropriate prerequisites for the SQL Server Reporting Services Server (ServerSSRS).
2. Run installer as a domain user with local administrator rights, and from the installation menu select Installations for an Oracle environment, Reporting Services, and then Custom installation.
3. Choose only SQL Server Reporting Services extensions by deselecting the other components on the tree.
4. Enter the name of the SunSystems Security server (ServerDBSEC) and then Report Server (ServerRS) and Report Manager (ServerRM).
5. Enter the domain SunSystemsReporting user account, password and SunSystemsServices group.
6. Next select the local SQL Server instance where Reporting Services is installed.
7. Click install.
8. If you have any problems with the installation check `ConfigureReporting.log` found in `C:\ProgramData\infor\SunSystems\Logs`.

Perform these checks if not completed at a previous step	✓
Reporting Services Configuration Manager, check Report Manager URL link is working.	
Reporting Services Configuration Manager, check Web Manager URL link is working.	

SunSystems Report Server

1. Run installer as a domain user with local administrator rights, and from the installation menu select Installations for an Oracle environment, Reporting Services, and then Custom installation.
2. Choose only Report Server by deselecting the other components on the tree.
3. Enter the name of the SunSystems Security server (ServerDBSEC) and then Report Manager (ServerRM).
4. Select from the dropdown the Oracle Home for your 32 bit Oracle Client installation.
5. Enter TNS name, SunSystems Domain schema name (DOM) and password.
6. Security Schema Details: enter Oracle DBA account (SYSTEM) and password.
7. Enter the domain SunSystemsReporting account (this OPS$ account must not be greater than 30 characters) to run the Report Server service, password and SunSystemsServices group.
8. Next select the local SQL Server instance where Reporting Services is installed.
9. Complete the installation.

	✓
In IIS Manager, check Application Pool SunSystemReportingServices is started.	
Check SunSystemsReportingPrintService Windows Service is started	

SunSystems Report Manager

1. Run installer as a domain user with local administrator rights, and from the installation menu select Installations for an Oracle environment, Reporting Services, and then Custom installation.
2. Choose only Report Manager and Sample Reports by deselecting the other components on the tree.
3. Select from the dropdown the Oracle Home for your 32 bit Oracle Client installation.
4. Enter TNS name, SunSystems Domain schema name (DOM) and password.
5. Security Schema Details: enter Oracle DBA account (SYSTEM) and password.
6. Enter the domain SunSystemsReporting account (this OPS$ account must not be greater than 30 characters), password and SunSystemsServices group.
7. Report Manager SMTP Server: enter SMTP Server, port (25) and sender email address. You must enter at least a port number to proceed.
8. Proceed with the installation. Loading sample reports may take up to 30 minutes.

Installing the Infor10 Workspace SunSystems Plug-in

SunSystems Web

For the SunSystems deployment in Workspace, it is recommended that SharePoint be installed on a separate machine to SunSystems Web.

Installing Infor10 Workspace and SunSystems Plug-in

The SunSystems plug-in is now included in the Workspace 10.1 installer, so it is now a one-step installation. Obtain the Infor10 Workspace 10.1 installer DVD image from the Infor and Lawson Product Download Center (In www.inforxtreme.com, select Downloads >> Products).

Ensure SharePoint Foundation 2010 is installed and configured. Please refer to the Infor10 Workspace Installation Guide on InforXtreme.

Ensure the SharePoint 2010 Timer Service is running, otherwise components will be listed as deploying. Log in to SharePoint Foundation 2010 with the SPInstall account.

If you have an existing SharePoint default site we recommend that you create a new Infor site collection to house the SunSystems and other Infor products, preventing any conflict with your default site.

1. Run as Administrator Infor10 Workspace 10.1 setup.exe to install Workspace.
2. Select Features: Tick Infor10 Workspace Core. Expand Plug-ins, and tick Generic Product Plug-in, and SunSystems. Start the SharePoint 2010 Administration Windows Service if required.
3. Complete installation.
4. It may take up to five minutes for the installed solutions to be deployed in SharePoint.

Verifying the Infor10 Workspace Deployment

If you use standalone mode, in order to deploy you will need to carry out the following:-

1. Open a command prompt run in administrator mode.
2. Change directory to:
   ```
   Program Files\Common Files\Microsoft Shared\Web Server Extensions\14\bin
   ```
3. Run this command:
   ```
   stsadm -o execadmsvcjobs
   ```
4. Wait two minutes.
5. In SharePoint 2010 Central Administration, select System Settings >> Manage Farm Solutions >> Solutions Management page verify that both Workspace and SunSystems plug-in are listed as deployed.

Infor10 Workspace Configuration Tool is available from the start menu and enables the user to add plug-ins. Detailed documentation is available: refer to the Infor10 Workspace Installation and Configuration Guide (for version 10.1) on InforXtreme.

Post-Installation Configuration

Serialization

At 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.

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. Select this from Start, Infor10 Financials SunSystems, SunSystems tools, Migration, SunSystems User Migration. If a three digit SunSystems login is required select Operator Id.

Alternatively, refer to the User Manager Help to create your own Users and Groups.

Add SunSystems Reporting Service Group Membership to SunSystems Users

If preconfigured data (PK1) has been installed, sign into User Manager as admin. Select Groups tab. Edit Group PK1. Select Function Permissions, click Select All, Apply. Select Action Permissions, Add PK1, Apply.

Now go to Users tab. Right click on a user that requires SRS group membership (PK1 for example), and select Edit User. Click Change (next to Group Membership). Expand SunSystems Reporting Users, and select SunSystems Reporting functions required for this user. Click OK to submit the changed group membership. Note which users you have given SunSystems Data Access Managers role, and Report Administrator role because these are needed for the following steps.

Configuring SunSystems Reporting Service in Data Access Manager

From start menu, sign into Infor10 Financials SunSystems, Reporting, Data Access Manager. If you have difficulties use alt-tab to check that a hidden dialog is not being displayed. Select Define SunSystems Connection in the task tree, then right click, Run Task. Enter connection details to the Oracle instance SunSystems Domain schema name and click OK. Select Configure business unit data models in the task tree, then right click, Run Task. Check the Business Unit(s) that will be reported against and click OK. Save the changes before you exit Data Access Manager.

Please note that if you create new business units you will need to 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.

Internet Explorer Compatibility Mode

To access SunSystems Web in Internet Explorer 8 go to Tools, Compatibility View Settings, and un-tick display intranet sites in compatibility view.

Log File Locations

Log files can be found in standard location `ProgramData\Infor\SunSystems\logging`. 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.

Part 2 – Installation Reference

Requirements and Planning

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 Versions of Windows and Database
Stand-alone	All	Windows 7, Vista, MS-SQL Server 2008 R2 Oracle 11g R1 or 11g R2
Two-Tier	Client	Windows 7, Vista, Windows XP
	Application and Database	Windows 2008 Server R2 (Standard or Enterprise), MS-SQL Server 2008 R2 Oracle 11g R1 or 11g R2 or any of the supported operating systems listed by Oracle for this edition of the database
Multiple Tier	Client	Windows 7, Vista, Windows XP
	Application	Windows 2008 Server R2 (Standard or Enterprise) R2
	Database	Any of the supported operating systems listed by Oracle for Oracle 11gR1 or 11gR2 (Standard or Enterprise)
	Reporting	Windows 2008 Server R2 (Standard or Enterprise), MS-SQL Server 2008 R2

Note: Physical databases must be in the collation of the data that is being stored.

RDBMS Support

SunSystems – Oracle is supported only with the following relational database systems:

- Oracle 11g R1 (11.1.0.6) Standard Edition, Enterprise Edition, or greater
- Oracle 11g R2 (11.2.0.1) Standard Edition, Enterprise Edition, or greater

Note: Check with Oracle, and with SunSystems Support, for the supported versions of Oracle 11g R1 and R2 on your platform.

SunSystems Reporting Services (SRS) requires Microsoft SQL Server 2008 R2 (Standard, Enterprise, and Workgroup editions) - 32-bit version or 64-bit version.

Note: For information on SQL Server support, see the separate SunSystems – SQL Server Installation Guide.

Database Collation

When you create your SunSystems database, you must select the appropriate collation for the language version you use, for example:

- Use JA16SJIS with Japanese versions of SunSystems
- Use ZHS16GBK with Simplified Chinese versions of SunSystems
- Use ZHT16BIG5 with Traditional Chinese versions of SunSystems
- Use CL8MSWIN1251 with Russian versions of SunSystems.

Note: You cannot store code page X data in a code page Y Oracle database; for example, you cannot store code page 932 data (Japanese) in a code page 1252 database (Western European). Although this was possible in some circumstances with previous versions of SQL Server and Oracle, it has always been unsupported. To a 1252 Oracle database, anything but a 1252 character is not a valid character data.

Note: SunSystems Oracle implementations on a UNIX platform require the same character set specification as SunSystems Oracle on Windows. For example, a Western European SunSystems database on UNIX should still be created as 'WE8MSWIN1252'.

To install SunSystems in a specific language, note the following:

- It is not necessary to have a language-specific operating system for the database server, application server, or the client, but the desired language locale must be installed using Control Panel.
- Oracle can support any language. The oracle database should be created in the appropriate codepage for the language(s) being used; this is done through the National Language Support (NLS) settings. When you create the SunSystems schema, you must select the appropriate codepage for the language(s) that you want to support; for example, French is supported in the European codepage but is not supported in the Chinese codepage.

If required, set the Oracle `NLS_LANG` variable value on the client server and on the application server to the desired language to be used. `NLS_LANG` is in the HKLM Software >> Oracle >> Key_ORACLE_HOME_NAME registry setting.

Binary Sort Order is mandatory, And sets the database selection criteria to match A-Z a-z ASCII values, and so on, which are compatible with the SunSystems program logic. SunSystems internal COBOL programming and business logic, which demands that dictionary sorts Aaåääå and so on, must *not* be used.

For Oracle, ensure that the `NLS_SORT` registry string in the relevant Oracle Home is set to `BINARY`.

Oracle Software Installation

For Oracle, install Oracle Database Enterprise or Standard Edition on the nominated database server. If you intend to use multiple database servers, install on each server; if you intend to use Oracle Real Application Clusters (RAC), install on the nominated cluster server.

Install Oracle Client Edition ('Administrator' level) on the nominated Application server. If you intend to use multiple Application servers, install on the nominated cluster server.

Install Oracle Client Edition ('Administrator' or 'Custom' level with minimum components of Oracle Net, Oracle Windows Interfaces and Oracle JDBC/THIN Interfaces) on each Client machine.

After Oracle is installed, create a Listener on the nominated database server. If multiple servers are in use, create a Listener on each server. If you intend to use Oracle Real Application Clusters (RAC), configure a Listener for each node in the cluster.

SunSystems and Oracle Real Application Clusters (RAC)

Before you install SunSystems, you must create an Oracle database Instance to hold the SunSystems database objects. As part of your preinstallation tasks, it is recommended that you take complete backups of

all existing databases in case database creation affects the existing databases. Backups should include parameter files, database files, redo log files, control files and network configuration files.

To enable Transparent Application Failover (TAF), configure the `tnsnames.ora` file for TAF on all Application servers and Client machines.

Load Balancing

If you intend to use Windows Network Load Balancing (NLB), check that NLB has been installed on each application/report server. For more information about configuring these, refer to the Scalability section of this installation guide.

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.

Creating a Secure SunSystems Installation

Introduction

This section details the security requirements for configuring and running SunSystems, and also 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.

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 right 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 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.

In SunSystems, the security service issues vouchers to authenticated users who want to submit an SOAP request. 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`.

Oracle

Introduction

SunSystems Security makes use of Oracle ‘OS Authentication’ to run the Service Account. As long as an Oracle Database User exists with the same name as the Windows workgroup or domain user id running the SunSystems Security Windows Service, the service can connect without authentication. For more information, refer to the Oracle online documentation.

Oracle Service Account

During the installation of SunSystems and SunSystems Security, you will be asked for details of a Windows workgroup or a Domain account under which the SunSystems Security service will run. The SunSystems installer will create an account(OPS$ account) on the database using the credentials supplied. If the account under which the SunSytems Global Security service runs is changed after the installation has been completed then a corresponding database account will also need to be created in the database, refer to Appendix H – Creating a New Oracle Service Account for details on how to do this.

Oracle profiles

There is a new Oracle 11g feature that expires User accounts after 6 months, therefore, all SunSystems-related Oracle Schemas are assigned to a new profile called 'SUNPROFILE', which does not expire. This profile is created on Oracle 11g installations of SunSystems 5.4.1. For more information, refer to the SunSystems 5.4.1 Upgrade Guide.

Oracle 'Advanced Security'

Oracle's Advanced Security features and security options (such as custom password complexity) are not supported.

Microsoft SQL Server – for SunSystems Reporting Services (SRS)

Introduction

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.

SQL Server Services 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 (Presentation Server)

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, which implies that all users on a specific connection type can be restricted to running published applications only. Published Application Manager allows you to restrict an application to specified users or groups of users (explicit user access only).
- Citrix XenApp (Presentation Server) supports Internet firewalls that can be used to restrict Internet access to the XenApp (Presentation Server).
- Users can be required to enter a user name and password to execute an application (explicit user access only).
- Citrix and most web professionals recommend that you either disassociate your web site 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 very 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 via Citrix. SunSystems allows only the domain users to log on to SunSystems who are members of clients group e.g. 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 will download forms on a per user basis in the `multipleclientfile` folder. It is very 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, Vista, and Windows 7: `C:\ProgramData\Infor\SunSystems`.

If SunSystems on Citrix XenApp (Presentation Server) 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 need 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 XenApp (Presentation Server) reserving 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 (Presentation Server).

Memory Optimization and SunSystems

Application memory is not a primary bottleneck in SunSystems; however, 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 (Presentation Server).

SpeedScreen and SunSystems

SpeedScreen technology is designed to optimise the graphics-based applications on Citrix, such as 3D graphics. However, this technology will also help to use the network bandwidth in better a way. It is recommended to turn on the SpeedScreen setting on the SunSystems deployment on Citrix XenApp (Presentation Server).

Additional Scalability Recommendations

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

Hardware and Configuration Recommendations

1. Dual processor machines provide the best results. For 32-bit systems, more than two processors provide diminished returns.
2. 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.
3. Set Static page file size. To prevent resizing, minimum and maximum settings should be constant.

Citrix Web Client and SunSystems

Citrix XenApp (Presentation Server) 4.5 provides a way to connect to published applications without having Citrix client preinstalled. Citrix Web Interface is part of Citrix XenApp (Presentation Server) 4.5.

SunSystems can be used with Citrix Web 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.`

Database Administration

Introduction

SunSystems Installation DVD allows you to carry out 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 execute `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.

Using a 64-bit DBMS

SunSystems is a 32-bit application, but it can be used on 64-bit operating system in emulate mode. Therefore, the application can access only 32-bit resources of a 64-bit operating system. SunSystems can use only the 32-bit Oracle client to access a 64-bit Oracle database.

> **Note:** 64-bit Oracle comes with the 64-bit Oracle Client only. To use SunSystems with 64-bit Oracle, a separate installation of 32-bit Oracle Client is necessary on all tiers.

Creating a New SunSystems Domain Schema

Use the Create a SunSystems Domain Schema option to create a SunSystems Domain schema on the local machine or on the specified Oracle Database Server.

All SunSystems schemas must be registered in a SunSystems domain. Therefore, the SunSystems Domain schema must be created at the same time as, or in advance of, creating SunSystems schemas in the same SunSystems domain.

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

> **Note**:
>
> - All servers that host the SunSystems Domain schema and SunSystems schemas must reside in the same Windows domain. Cross-domain environments are not supported in this release.
> - All SunSystems Data Schemas must reside in the same Oracle Database Instance as the SunSystems Domain Schema.

A subset of the steps for a full installation is used for this operation. Although only 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.

> **Note:** The GLOBAL_NAMES parameter on all Oracle database instances must be set to 'False'. Edit the `init<sid>.ora` file (where SID denotes the system identifier) then restart the Oracle instance and specify the `init<sid>.ora` file at startup.

Creating a New SunSystems Data Schema

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

The Create a SunSystems Schema option uses scripts to create a SunSystems schema on the local machine or the specified Oracle Database server and registers this as follows:

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

This option is used, as an alternative to creation during an Application Server installation, if the SunSystems schema 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.

Note:

- All servers that host the SunSystems Domain schema and SunSystems schemas must reside in the same Windows domain. Cross-domain environments are not supported in this release.
- All SunSystems Data schemas must reside within the same Oracle Database Instance as the SunSystems Domain schema.

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

A subset of the steps for a full installation is used for this operation. Although only 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.

Import a Preconfigured SunSystems Data Schema

Import a preconfigured SunSystems Data schema is registered as either:

- In a new SunSystems domain by creating a new SunSystems Domain schema.
- In an existing SunSystems domain through an existing SunSystems Domain schema.

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

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

Note:

- All servers that host the SunSystems Domain schema and SunSystems schemas must reside in the same Windows domain. Cross-domain environments are not supported in this release.
- All SunSystems Data schemas must reside within the same Oracle Database Instance as the SunSystems Domain schema.

Registration of a SunSystems schema is prevented if the schema 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 schema automatically converts the SunSystems domain to a multiple SunSystems schema environment.

A subset of the steps for a full installation is used for this operation. Although only 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.

Modifying Languages on a SunSystems Data Schema

The **Modify Languages on a SunSystems Data Schema** option applies/removes Language Packs to/from SunSystems schemas. This option must be run on a machine that has an Oracle Installation with a TNS connection to the Domain schema and all SunSystems schemas. For example, on an Application Server it must be rerun for each of the SunSystems schemas in the SunSystems domain that require the adjustment.

Note:

- If you make changes to existing business units you will need to update Configure Business Unit Data Models in Data Access Manager. Uncheck the Business Unit, click OK, Save, then redo the configuration.
- Client and Application Server installations now include all standard SunSystems languages by default. It is only necessary to add languages to each SunSystems Data schema.

Database Utilities

The **Database Utilities** option 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 SunSystems schema against a master template for that schema version. You must specify the TNS name and the SunSystems Schema name.

You have the option to run further database utilities.

Referential Integrity Check, SunSystems Data Only

This option checks the integrity of a SunSystems schema against a master template for that schema version. You must specify the TNS name and the SunSystems Schema name.

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

> **Note**: Database 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 Data Referenced to Domain Schema

This option carries out a referential integrity check of a SunSystems schema. You must specify the TNS name and the SunSystems Schema name.

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.

Load Differential Tables

This option reloads the difference table in a specified SunSystems schema 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 schema, either from scripts or by attaching a preconfigured schema, 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 schema information. A list of SunSystems schemas that are in the domain schema is displayed. Select the required schema and the version of the data to be loaded in the difference tables.

You have the option to run further database utilities.

Pre-Upgrade Outstanding Transactions Check

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

The checks that it performs are as follows:

- Checks for the existence of any Held Journals
- Checks for the existence on 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.

SunSystems Domain Schema Utilities

Removing a SunSystems Data Schema from a SunSystems Domain

The Remove a SunSystems Schema option removes a SunSystems schema from a SunSystems domain and optionally deletes the schema if it is held on the local machine or on a specified Oracle Database server.

> **Note**: For SunSystems versions before v6.1.0, removing a SunSystems schema from a SunSystems domain deleted the server files.
>
> For SunSystems v6.1.0 and above, the server files are in the SunSystems schema; this option will remove a SunSystems schema from a SunSystems domain.

If removal from the SunSystems domain leaves only one registered SunSystems schema, the domain automatically reverts to a single SunSystems schema environment.

Note: Removal of the only remaining SunSystems schema in a SunSystems domain renders the domain incomplete and in an unsupported state.

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

1. Specify whether the schema should be removed from the SunSystems domain, or removed and deleted.
2. Specify the location for log files.
3. Select the TNS name used for the SunSystems Domain schema for the SunSystems domain in which the schema to be removed is registered, and specify whether or not this uses integrated security.
4. Select the TNS name used for the SunSystems schema to be removed and optionally deleted.
5. Confirm that the schema and server instance details are correct.
6. Confirm that the SunSystems domain and SunSystems schema details are correct.

Complete the following steps:

1. Specify the TNS name for the Domain schema.
2. Specify the Domain User credentials.
3. Specify the Oracle 'system' user DBA credentials.
4. Specify the Oracle 'sys' user SYSDBA credentials.

Re-link SunSystems Data Schema to SunSystems Domain

The Re-Link SunSystems Schema option re-links the existing SunSystems schema to existing SunSystems Domain schema. This utility allows you to move SunSystems domain schema and SunSystems data schema from one server to another.

Recovering BU links

This option executes 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 schema.

Business Unit Group Parameter Maintenance

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

The following options are then available.

Changing the Business Unit Group Name

The Change Business Unit Group Name option is used to change the business unit group name that is used for the SunSystems schema previously selected.

Enter a new Business Unit Group name.

Changing Double Byte Processing

This setting is used on Double Byte Character Set (DBCS) operating systems or emulators, to validate your data for truncated or split characters during data entry, data importing, and posting.

Note: Null is used to signify that Single Byte Character Set (SBCS) processing is required.

Administering SunSystems on Oracle Real Application Clusters

Following a reboot of any of the database servers in the RAC environment, the nodes must be restarted. To restart the nodes, you are recommended to create a script.

Depending on your server hardware configuration, the Oracle services may take some time to restart. Following installation, you are recommended to review the initialisation parameter values for the following.

Parameter	Recommended Value
Processes	600
Sessions	processes * 1.1 + 8

Typically, the Oracle installation default values are considerably below these recommended values and this might result in errors being displayed when you submit SunSystems reports, or connection errors when you attempt to use the SunSystems database. Each report request requires 4 processes to execute.

Note: If the processes count is exceeded, all subsequent connection requests are refused.

SunSystems Database Migration

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

The prerequisites are as follows:

- Source and destination Oracle 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 (SYS and SYSTEM) privileges
- All the SunSystems users should log out and all the SunSystems windows services should be stopped.

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

SunSystems Connect (SSC)

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 2008 (Standard or Enterprise) is required for the SunSystems Connect and Automation Desk installation.

Where a third party application is written that makes an 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 installed automatically.

> **Note**: SunSystems Connect functionality comprises 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.

Securing SSC

Additional security measures are the responsibility of the web site developers or the integration developers. The four areas of security that must be addressed when you set up SSC are described below.

The Tomcat Keystore File

The Tomcat keystore file holds the X.509 certificate that defines the encryption keys for secure sockets. By default, it is called `SUNSYSTEMS5\ssc\tomcat.keystore`, where `SUNSYSTEMS5` is the name of your SunSystems program root directory.

The file that is included with SSC is password protected and has a default password of 'changeit'. However, the password protection is of limited use in that, because the application must gain access to the password, the password is specified in clear text within the property files. In this instance, you should improve the protection of this file using Windows Access Control.

The certificate within the tomcat keystore is self-signed by SunSystems. Therefore, the first time Windows Internet Explorer opens a secure page using the certificate, a message indicates that the certificate is not known to be trusted and that the certificate organization does not match the web site name.

You might want to replace the certificate with one of your own, particularly if the web server is exposed to external users. For more information, refer to your Tomcat documentation and the Java keytool application.

Enabling Secure Web Pages

By default, the Tomcat server has secure sockets enabled. To use a secure connection, use the following URL:

```
https://localhost:8443/ssc/
```

The padlock icon on the browser status bar indicates secure connections.

The Tomcat secure connection is configured in the property editor under the `tomcat.https_connector` section.

Enabling Secure SOAP

Secure web pages imply secure SOAP, because SOAP messages pass over normal http/s type connections. To access secure SOAP, you must change the SOAP server URL in your client code to the following:

```
https://<server>:8443/connect/soap/...
```

Changing SSC TCP port value

By default, SSC is configured on TCP port 8080. To change this value, use the Switch server utility that is provided with SunSystems.

Scalability – Application Servers and SunSystems Connect

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.

> **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 needed
- Offers more sophisticated load distribution models to choose from.

You should be aware that additional hardware is required.

> **Important Note**: Because of the complexity of this configuration, before you start to implement hardware load balancing, seek advice from your SunSystems software provider.

Software-Based Dynamic Load Balancing

This uses third party software, such as the Windows Network Load Balancing (NLB) available with the 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 affect on service.
- No client reconfiguration is needed.

However, you should be aware of the following:

- Licensing costs can be expensive.
- Only 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 2008 or Windows 2008 R2.
- Windows Network Load Balancing component is installed on every application server that will be part of the cluster.
- Every application server machine has 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.

Configuring Software-Based Load Balancing with Windows 2008

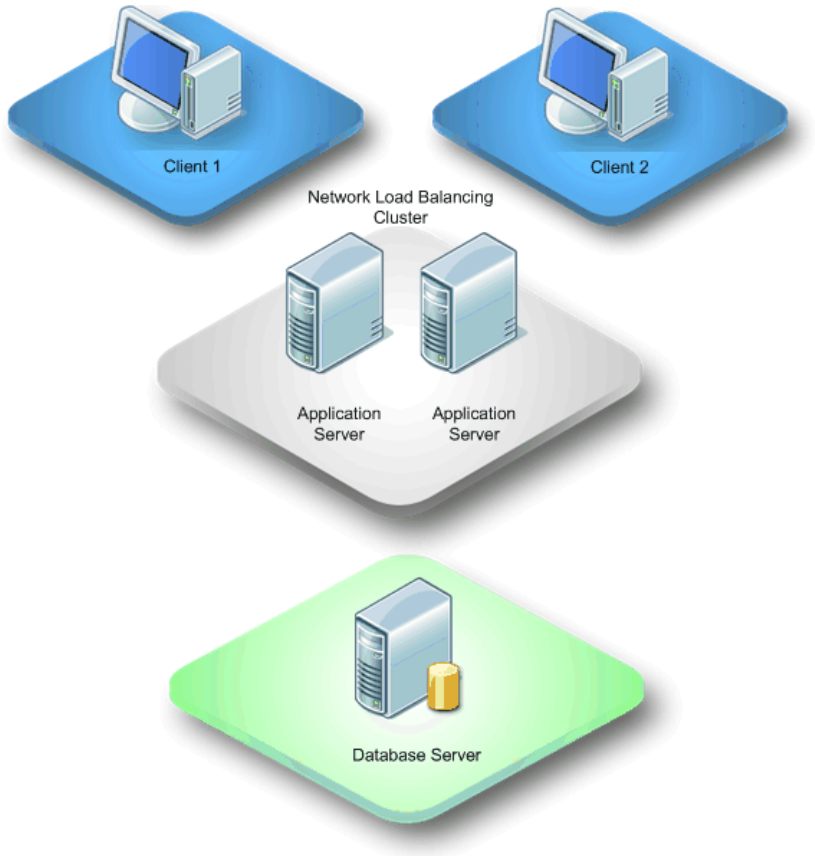
This section provides details for configuring SunSystems with load balancing. For the steps involved in Network Load Balancing Manager configuration, refer to relevant Microsoft Windows documentation.

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	
REPORTING SERVER	Windows 2008 R2 Server/ SQL Server 2008 R2	RS		
DATABASE SERVER	Windows 2008 R2 Server/ Oracle 11g R1 or 11g R2	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. You must 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 in order 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 2008

After you complete the Network Load Balancing Manager configuration, complete the following steps to verify the configuration:

1. To check if 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:

- Successful Reply from 10.10.10.36
- Unsuccessful Request Time Out.

2. If communication is unsuccessful, recheck Load Balancing Setup and try the test again.
3. Repeat the Network Load Balancing configuration steps on each Application Server to be used in the Network Load Balancing cluster.
4. You can check that each Application Server joins the Load Balance cluster:
   a) On an Application Server, open Event Viewer. This is located in the **Control Panel >> Administrative Tools**.
   b) An entry should exist where the **Source** tab indicates WLBS. 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.
   c) If the convergence entry does not exist and only one server is mentioned, recheck Load Balancing Setup and recheck Event Viewer.
5. 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.
6. After this DNS entry has been created, perform a `ping` test 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` and the cluster DNS name. For example, `PING` cluster. One of the following messages is displayed:
      - Successful Reply from 10.10.10.36
      - Unsuccessful Request Time Out.
   d) 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.

If SunSystems software is installed on multiple Application Servers, the data elements not held in the database, such as the report parameters (RptParams) directory, are duplicated and can cause version inconsistencies. To prevent this, a shared and centralized location for this directory is required, which can be achieved by the following manual configuration.

> **Note**: In a load balancing environment, the server that holds the installation of the SunSystems application files is referred to as the Application Server; a potential server or workstation that will contain the RptParams directory is referred to as the Central Data Server – you should use the database server for this task.

Port Rules Tab for Application 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 only a guide that covers modifying port rules for four load balanced application servers. The same scenario would exist for fewer or more application servers, although the port ranges would 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.
```

The following port ranges are specified as Single server and Equal distribution.

Example AppSrv1

Start	End	Mode	Load/Priority	Affinity
8080	8080	Multiple	Equal	None
50000	50000	Multiple	Equal	None
50001	50002	Multiple	Equal	Single
50005	50006	Multiple	Equal	Single
50008	50008	Multiple	Equal	Single
55001	55001	Multiple	Equal	Single
55000	55000	Multiple	Equal	Single
40100	40199	Single	1	Not Applicable
40200	40299	Single	2	Not Applicable
40300	40399	Single	3	Not Applicable
40400	40499	Single	4	Not Applicable

Example AppSrv2

Start	End	Mode	Load/Priority	Affinity
8080	8080	Multiple	Equal	None
50000	50000	Multiple	Equal	None
50001	50002	Multiple	Equal	Single
50005	50006	Multiple	Equal	Single
50008	50008	Multiple	Equal	Single
55001	55001	Multiple	Equal	Single
55000	55000	Multiple	Equal	Single
40100	40199	Single	4	Not Applicable
40200	40299	Single	1	Not Applicable
40300	40399	Single	2	Not Applicable
40400	40499	Single	3	Not Applicable

Example AppSrv3

Start	End	Mode	Load/Priority	Affinity
8080	8080	Multiple	Equal	None
50000	50000	Multiple	Equal	None
50001	50002	Multiple	Equal	Single
50005	50006	Multiple	Equal	Single
50008	50008	Multiple	Equal	Single
55001	55001	Multiple	Equal	Single
55000	55000	Multiple	Equal	Single
40100	40199	Single	3	Not Applicable
40200	40299	Single	4	Not Applicable
40300	40399	Single	1	Not Applicable
40400	40499	Single	2	Not Applicable

Example AppSrv4

Start	End	Mode	Load/Priority	Affinity
8080	8080	Multiple	Equal	None
50000	50000	Multiple	Equal	None
50001	50002	Multiple	Equal	Single
50005	50006	Multiple	Equal	Single
50008	50008	Multiple	Equal	Single
55001	55001	Multiple	Equal	Single
55000	55000	Multiple	Equal	Single
40100	40199	Single	2	Not Applicable
40200	40299	Single	3	Not Applicable
40300	40399	Single	4	Not Applicable
40400	40499	Single	1	Not Applicable

Warning: 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:

1. Run `Regedit`.
2. Find the following registry location:
   `HKEY_LOCAL_MACHINE\Software\SunSystems\Core\5.1\Session Manager`.
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:
   - `AppSrv 1 Max = 50199 Min = 50100`
   - `AppSrv 2 Max = 50299 Min = 50200`
   - `AppSrv 3 Max = 50399 Min = 50300`
   - `AppSrv 4 Max = 50499 Min = 50400`.

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 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.

SunSystems Reporting Services (SRS)

Setting up Email Distribution of SunSystems Reports

To configure SQL Server Reporting Services for sending e-mails using a simple SMTP server:

> **Note:** More complex scenarios, such as SSL access to the SMTP server, require more complex configuration.

1. Run Reporting Services Configuration Manager.
2. Select E-mail Settings.
3. Enter Sender Address and SMTP Server.
4. Edit rsreportserver.config found in the Reporting Services\Report Server\ folder in your SQL Server Reporting Services installation.

   <UrlRoot>http://SERVERNAME:80/ReportServer_INSTANCENAME</UrlRoot>

   <SendEmailToUserAlias>False</SendEmailToUserAlias>.

   For non-standard smtp configurations you may also need to update tags:

   <SMTPServerPort>

   <SMTPUseSSL>

   <SMTPAuthenticate>

   These are documented at http://msdn.microsoft.com/en-us/library/ms157273.aspx.
5. Add Generate events to the System Administrator's System Roles.
6. Run SQL Server Management Studio
7. Connect to Reporting Services and login in as SunSystemsReporting user (or a user with SSRS administrators rights)
8. Expand Security -> System Roles -> System Administrator.
9. Right click and select Properties.
10. Make sure Generate events is selected
11. You should now be able to run an email report in SunSystems by entering the email recipient on the report output tab before you run the report.

Changing SunSystemsReporting User and Password

The installation process sets the SunSystemsReporting user as the service user both in Windows services and IIS. It may be necessary to change the password and/or the user.

Modify the **Service Account** in **Reporting Services Configuration Manager.**

From Administrator mode command prompt (change directory to Program Files (x86)\Infor\SunSystems Reporting Services\apps) run **ConfigureReporting.exe** on relevant machines, using the argument string substituting with the new User Name and/or Password. You will find the installation specific argument string in `SRS_Install.log` in `ProgramData\Infor\Logs\SunSystems\Install`. An example is:

```
ConfigureReporting.exe -user infor\SunSystemsReporting -password Infor123
-sun5Groups "infor\SunSystemsServices" -log -logFile
"C:\ProgramData\Infor\Logs\SunSystems\Install\ConfigureReporting.log" -errorFile
"C:\ProgramData\Infor\Logs\SunSystems\Install\ConfigureReporting.error" -
categories fwk -install -path "C:\Program Files (x86)\Infor\SunSystems Reporting
Services"
```

This will:

- Modify the **Identity** of the **SunSystemsReportingServices** Application Pools.
- Change the impersonation in the appropriate **web.config** files.
- Add the new user to the **SunSystemsServices** group.
- Give the user access to **SSRS** web applications (both **Site Settings** and **Folder Settings**).

Any other services that use SRS User will also need to be changed such as the Print service.

When moving from a domain account to a local account (or vice versa) you may need to add/remove **RSWindowsNegotiate** to **AuthenticationTypes** in the **rsreportserver.config** of **SSRS**.

```
<Authentication>
   <AuthenticationTypes>
      <RSWindowsNegotiate />
      <RSWindowsNTLM />
   </AuthenticationTypes>
   <RSWindowsExtendedProtectionLevel>Off</RSWindowsExtendedProtectionLevel>
   <RSWindowsExtendedProtectionScenario>Proxy</RSWindowsExtendedProtectionSce
  nario>
   <EnableAuthPersistence>true</EnableAuthPersistence>
</Authentication>
```

Email Support

The support for emailing reports has been improved and no longer uses the inbuilt Microsoft Reporting Services Email facility. The administrator now defines the email 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.

SunSystems Web

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. From the Microsoft website, download Report Viewer Redistributable 2010 SP1 and install on your SSRS Server and SRS Report Manager. Afterwards download and install the Microsoft Report Viewer 2010 Language Pack for each required language. Following installation check each has been installed successfully in Control Panel, Programs and Features. In IIS Manager restart SunSystemsReporting Services application pool.

Configuring https SunSystems Security with SunSystems Web

1. Generate a machine level self signed certificate for IIS. This is done in IIS Manager, left hand panel: click server machine; middle panel: Server Certificates; Action panel: create self-signed certificate.
2. Enable https port on IIS using the certificate from step above. In IIS Manager, Sites, SunSystems Security, in Actions panel- click Bindings, edit site bindings, add binding:
   - Type: https,
   - IP Address: All unassigned,
   - Port: 82,
   - select your SSL certificate from dropdown.
3. SunSystems Domain schema, edit table DOMN_VRTL_HOST, add secure_port value (82) for SunSystems-security.
4. Restart SunSystems Web Windows service.
5. Test SunSystems Security on port 82. When you login to SunSystems on `http://localhost:9080/SunSystems` you are redirected to `https://localhost:82/SecurityWebServer/Login.aspx` which is the secure SunSystems security port. After signing into SunSystems you will be returned to an http: connection when accessing SunSystems Web application.

Configuring https SunSystems Web

1. Edit the `server-custom.properties` file located in:

   ```
   Program Files (x86)
          \Infor\SunSystems\SunSystemsWeb\tomcat\webapps\SunSystems\WEB-INF
   ```

   Add the following URLs:
   - `security.loginserver.url=https://sunsystems-security/Login.aspx`
   - `security.logoutserver.url=https://sunsystems-security/Logout.aspx`
2. Enable SunSystems Web tomcat for HTTPS, using the keytool on Tomcat JRE to generate a .keystore file. By default, the keytool is stored in:

   `Program Files (x86)\SunSystems\SunSystemsWeb\jre\bin\keytool.exe`.

   Open a command prompt in this location and run:

   `keytool –genkey –alias tomcat –keyalg RSA`

   You must enter a password, for example, changeit, and a string of personal questions. Browse for the location you want to put the .keystore file generated by the keytool.
3. Edit `server.xml` (`Program Files (x86)\Infor\SunSystems\SunSystemsWeb\tomcat\conf`) and specify the keystore location and password for HTTPS port 9443.

   Remove comment markers `<!--` and `->` from around this block of text, and amend the text to exactly correspond to the following:

   ```
   <Connector port="9443" SSLEnabled="true"
         protocol="org.apache.coyote.http11.Http11Protocol"
         maxThreads="200" scheme="https" secure="true"
         clientAuth="false" sslProtocol="TLS"
        keystoreFile="C:\Users\<userId>\.keystore" keystorePass="changeit" />
   ```

   where `<userId>` should be substituted as appropriate.

Again, remove the comment markers <!-- and -->, and check the text exactly corresponds to the following:

```
<Connector executor="tomcatThreadPool"
      port="9080" protocol="HTTP/1.1"
      connectionTimeout="20000"
      redirectPort="9443" />
```

4. Restart SunSystems Web and log in to SunSystems using https://localhost:9443/SunSystems. You should now be redirected to the secure port for security and maintain a secure connection accessing SunSystems. In the case of problems check log files in ProgramData\Infor\SunSystems\Logs.

Configuring https Secure Connection for SunSystems Reporting

1. On the server hosting SunSystems Report server generate a machine level self signed certificate for IIS. This is done in IIS Manager, left hand panel-click server machine, in middle panel-Server Certificates, in Action panel-create self-signed certificate.
2. Enable https port on IIS using the certificate from step above. In IIS Manager, Sites, SunSystems Security, in Actions panel- click Bindings, edit site bindings, add binding:
   - Type: https
   - IP Address: All unassigned
   - Port: 83
   - select your SSL certificate from the dropdown.
3. SunSystems Domain schema, edit table DOMN_VRTL_HOST; in the row for infor-app-srs, set Port Number = 0, and Secure Port Number = 83.
4. Restart SunSystems Reporting Service in IIS, and SunSystems Reporting Print Service in Windows local services.

Note: Port number 83 is given as an example; alternative port numbers can be used.

Web Server Scalability

This appendix documents the configuration steps required to set up web server scalability.

These steps assume that the SunSystems Web is being installed on a 32-bit Windows Server machine under the C:\Program files\Infor\SunSystems\ installation folder; however your installation may be different.

Prerequisites

- SunSystems Web is installed on each web server machine.
- IIS is installed on each web server machine.

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 under C:\Program Files\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.

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

   Replace hostName with the host name of the web server machine.

   ```
   <Engine name="Catalina" defaultHost="localhost">
   ```

   to

   ```
   <Engine name="Catalina" defaultHost="localhost" jvmRoute="hostName">
   ```
4. Ensure the AJP/1.3 connector is enabled (not commented out) and note the port number (default 8009).

```
<Connector port="8009" protocol="AJP/1.3" redirectPort="8443" />
```

5. Ensure the AJP port is open.

IIS Configuration

The steps below outline the configuration that is required to get IIS communicating with Apache Tomcat using the Apache Tomcat Connector. These steps must be carried out on each web server machine. For further information see http://tomcat.apache.org/connectors-doc/index.html.

There is a known issue with IIS 7 that may result in incomplete log messages. More information on this issue can be found at https://issues.apache.org/bugzilla/show_bug.cgi?id=45769. A patch for this issue can be obtained from http://support.microsoft.com/kb/956120.

1. Create a directory to hold the configuration files. From this point forward this directory will be referred to as <IIS-tomcat_connector-conf>.
2. Download the latest ISAPI redirector IIS server plugin from the distribution page, rename as isapi_redirect.dll and save to the <IIS-tomcat_connector-conf> directory. The 32-bit dll can be obtained from http://www.apache.org/dist/tomcat/tomcat-connectors/jk/binaries/win32/. The 64-bit version of the dll can be downloaded from http://www.apache.org/dist/tomcat/tomcat-connectors/jk/binaries/win64/.
3. Create a file under the <IIS-tomcat_connector-conf> called workers.properties. The file should contain information for each web server machine. This file will be the same across all the web server machines as long as the <IIS-tomcat_connector-conf> directory on each machine has the same structure. The contents will be similiar to below:

workers.properties

```
# Define list of workers
worker.list=loadbalancer,jkstatus
# Status worker
worker.jkstatus.type=status
# AJP13 worker for web server 1
worker.jvmRouteWebServer1.type=ajp13
worker.jvmRouteWebServer1.host=hostNameWebServer1
worker.jvmRouteWebServer1.port=ajpPortWebServer1
worker.jvmRouteWebServer1.lbfactor=1
# AJP13 worker for web server 2
worker.jvmRouteWebServer2.type=ajp13
worker.jvmRouteWebServer2.host=hostNameWebServer2
worker.jvmRouteWebServer2.port=ajpPortWebServer2
worker.jvmRouteWebServer2.lbfactor=1
.
.
# AJP13 worker for web server N
worker.jvmRouteWebServerN.type=ajp13
worker.jvmRouteWebServerN.host=hostNameWebServerN
worker.jvmRouteWebServerN.port=ajpPortWebServerN
worker.jvmRouteWebServerN.lbfactor=1
# Define the LB worker
worker.loadbalancer.type=lb
worker.loadbalancer.sticky_session=1
worker.loadbalancer.session_cookie=SUNSYSTEMS_LB
 worker.loadbalancer.balance_workers=jvmRouteWebServer1,jvmRouteWebServer2,...
                                                    ,jvmRouteWebServerN
```

4. Create a file under the <IIS-tomcat_connector-conf> directory called uriworkermap.properties. This file will be the same across all the web server machines as long as the <IIS-tomcat_connector-conf> directory on each machine has the same structure. The contents as a minimum should be:

uriworkermap.properties

```
# Mapping the URI /jkmanager and everything under /jkmanager/:

# This is optional for production but if enabled in production it is highly recommended that you secure access to the /jkmanager offset

/jkmanager|/*=jkstatus

# Mapping the URI /SunSystems and everything under /SunSystems/:

/SunSystems|/*=loadbalancer
```

5. Create a properties file under the <IIS-tomcat_connector-conf> directory with the same name as the DLL file but with the .properties extension. This file will be the same across all the web server machines as long as the <IIS-tomcat_connector-conf> directory on each machine has the same structure. The contents as a minimum should be:

isapi_redirect.properties

```
# The path to the ISAPI Redirector Extension, relative to the website

# This must be in a virtual directory with execute privileges

extension_uri=/sunsystems/isapi_redirect.dll

# Full path to the log file for the ISAPI Redirector

log_file=<IIS-tomcat_connector-conf>\logs\isapi.log

# Log level (debug, info, warn, error or trace)

log_level=info

# Full path to the workers.properties file

worker_file=<IIS-tomcat_connector-conf>\workers.properties

# Full path to the uriworkermap.properties file

worker_mount_file=<IIS-tomcat_connector-conf>\uriworkermap.properties

# Log file size in megabytes.

# The value can have an optional M suffix, i.e. both 5 and 5M will rotate the log file when it grows to 5MB

log_filesize=100
```

6. Open IIS Manager, select the root node (the server), and select option ISAPI and CGI Restrictions.
7. 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 suitable description and check the 'Allow extension path to execute' check box.
8. Open the website where you want to activate the redirect and open the option 'ISAPI Filters'.
9. From the 'Actions', select 'Add'. Enter a filter name, and select the path to the DLL for the executable, that is,
   <IIS-tomcat_connector-conf>\isapi-redirect.dll.
10. Right click the website selected in step 8 and select 'Add Virtual Directory...'. Enter 'sunsystems' for the alias, and select the path to the DLL for the physical path, i.e. <IIS-tomcat_connector-conf>\isapi-redirect.dll.
11. Select the virtual directory just created and open the option 'Handler Mappings'.
12. In the disabled list select the mapping 'ISAPI-dll' and from the 'Actions' select 'Remove'.
13. From the 'Actions', select 'Add Module Mapping...'.
14. 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
```

15. 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.
16. Click OK to close the 'Edit Module Mapping' dialog.
17. From the 'Actions', select 'Edit Feature Permissions'.
18. Check the 'Execute' check box.
19. Locate the <IIS-tomcat_connector-conf> directory and open the '`web.config`' file in a text editor such as notepad.
20. Add the following attribute to the end of the ISAPI_REDIRECT-dll entry: `responseBufferLimit="0"`
21. Save and close the file.
22. Restart IIS.

SunSystems Web WAR Configuration

The SunSystmes 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:
   `<SunSystems_intall_folder>\SunSystemsWeb\tomcat\webapps\SunSystems\WEB-INF`
2. Remove the # from the following line
   `#loadbalancer.enableLoadBalancer=true`
3. Restart the SunSystems Web service.

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 in order 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 comprise 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.

Windows Server 2008 – Internet Explorer 8 (IE8)

IE8 on Windows Server 2008 contains a security mechanism that prevents the computer from downloading an ActiveX plug-in that is necessary for the SunSystems Web client. Therefore, to run the SunSystems Web client on a Windows Server 2008 machine, you must initially lower the security setting in IE8 to enable the required plug-in to download. Once the plug-in has been downloaded, IE8 security can be reset back to its normal setting.

To lower the security setting on Windows Server 2008 to enable the plug-in to download:

1. On the Windows Server 2008 computer, open IE8.
2. Select Tools >> Internet options.
3. Select the Security tab.
4. Click the Custom level button.
5. Locate the options for ActiveX controls and plug-ins.
6. Set the option 'Download signed ActiveX controls' to enable.
7. Set the option 'Download unsigned ActiveX controls' to enable.
8. Click OK to close the Security Settings, then click OK to close the Internet Options.

After the SunSystems Web client is run and the ActiveX plug-in is downloaded, follow the above instructions but set the options in steps 6 and 7 to the security level you require, for example 'disable'.

Post Installation Tasks

Apply SunSystems v6.1 Patch Set 5 or later to ensure you have the most up-to-date fixes and functionality.

Troubleshooting

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 occurs 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 as a result of the following:

- Incorrect installation settings.
- Incompatible data for installation settings and serialization.
- Access control – network settings and permissions.
- Incorrectly set IP addresses.
- Network Library not set to TCP/IP.
- Changes made to registry settings used by SunSystems.
- Database Access – 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

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\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\SunSystems\Core\5.1\SessionManager\ListenerPort`

- On the client, this is held in the registry setting:

`HKEY_LOCAL_MACHINE\SOFTWARE\SunSystems\Core\5.1\Comms\SessionManagerListenerPort`

> **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.

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 amended 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% for the msi log. This log is not easy to interpret but contains the reason for the rollback. Also check InstallLog.txt in C:\ProgramData\Infor\Logs\SunSystems\Install

Causes could include SunSystems applications still existing in IIS after deinstallation. Check in IIS Manager.

Problems Encountered when Uninstalling

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.

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 A-Z a-z ASCII values, and so on, which are compatible with the SunSystems program logic. SunSystems internal COBOL programming and business logic demands that dictionary sorts Aaâäàå, and so on, 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 follow.`

`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.

SunSystems Web is only supported on Internet Explorer 8.

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 appearing on the menu you may need to 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 will need to set standard authentication globally in User Manager. Log into User Manager as administrator, Settings, Security Policy, un-tick Enable Windows Authentication.

I want 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.

Cannot create a connection to data source 'EvoReportDataSource'

Check that you have run Data Access Manager for all Business Units and ensure that WSE 3.0 has 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.

Troubleshooting SSC

The SSC demonstration web page does not appear

Cause

The SunSystems Connect Server service might not be running. To check this on your server, open the Services folder (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, execute 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.

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, execute 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, execute 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/Oracle is running out of memory whilst executing an SQL Query.

Solution

Increase the memory available to Microsoft SQL Server/Oracle by increasing the physical memory that is installed on the server machine, and/or adjust SQL Server/Oracle's memory configuration. 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.

Diagnostic Tools

In certain circumstances, it is useful to be able 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 and/or SunDebug and/or SSC logging and/or Transfer Desk logging. These tools are designed to display and log the SunSystems program behaviour and allow quick resolution of any system failures that are not easily 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 schema connection test.
- Low level locator service connection test.
- Request domain schema information for the locator service.
- Request list of data sources from the domain schema.
- Request schema information for each data source.
- Low level schema 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 the SunSystems database requires recovery, it is necessary to restore Security, Domain and all

SunSystems Data schemas 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 schema. 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 schemas (SunSystems data schema, domain schema and security schema) on the new machine.
- Run the SunSystems schema setup and choose the option to re-link the SunSystems data schema and domain schema. Check the schema integrity using the database installer option.
- Update the SunSystems domain schema table `DOMN_DSRCE_CONFIG` 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 schema.

If SunSystems security server is installed on the database server machine and SunSystems Security needs recovery, reinstall SunSystems Security server again after uninstall. Select the already existing SunSystems security schema.

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. The SunSystems application server is working. Database server machine has been replaced and the previous database recovered on the new machine.
2. The SunSystems application server has crashed. Database is working without problem.
3. Application server has crashed and needs to be replaced with another application server machine.

In case 1, if the database server has been replaced, update the SunSystems domain schema details in User Manager >> Settings >> SunSystems >> Configure.

In case 2, if the application server needs recovery, restore the server backup from the backup media. If the database server has been replaced, the application server needs to be updated to point to the new database server as follow:

- Run User Manager and update the SunSystems domain.schema details.
- If the SunSystems Security schema was also installed on the replaced database server, update the SunSystems Security Global.config in `C:\ProgramData\infor\security` Update the server name according to the new security server name.

In case 3, if the application server machine crashed and needs to be replaced:

- 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:
- SunSystems Security
  - SunSystems Session Manager
  - SunSystems Connect

After you start these services, check the central log repository for any possible error in log files for the services given here. Report any errors to SunSystems Technical Support.

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 Web site 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 www.inforxtreme.com. There is also the facility to search the knowledgebase solutions in Infor Xtreme

Support for known issues prior to logging as an incident, 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 needed to replicate the problem
- Saved error message files as appropriate.

Glossary

Term	Definition
Application server component	Consists of all software elements and data elements that are installed on the designated application server, namely the application layer and database layers.
Business Unit Group	A collection of SunSystems Business Units that are stored in a single SunSystems data schema. In other words, a SunSystems data schema 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: C:\ProgramData\Infor\SunSystems\logs
Client component	Consists of all software elements that are installed on the client PC. Includes Security Client, SunSystems Client, and Reporting Client.
Collation	A collective term for the character set, code page, and sort order used for languages. For example, `WE8MSWIN1252` is the Western European default for Oracle.
Database server component	For relational versions, the server hosting the RDBMS.
Domain schema	An independent schema in the SunSystems Domain; a central repository that contains information to facilitate connections to multiple SunSystems schemas 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 schema). For example, a three-tier installation, or variations including an application server farm and/or access to multiple SunSystems schemas.
SunSystems session	An open SunSystems window. You can open up to nine sessions at a time.

Appendix A – TCP/IP Ports

The following tables detail the TCP/IP ports that are used by SunSystems products as of version Enterprise.

This table is of particular significance to installations where security is strictly enforced and ports are closely managed, typically through one or more firewalls.

This table provides default settings and details how they can be changed. The Enterprise upgrade process does not override existing port settings unless the port settings are in an unsafe range that is known to cause issues.

Application Server (Session Management)

The following tables apply to each application server that is configured. Where multiple servers are present, they should share the listening port but have different port ranges for each server.

Component Description	Configured Default Port	Location and Configuration	Other Information

Session Manager Service Listening Port	50000	Registry entries:
		`HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Sunsystems\Core\5.1\Comms\SessionManagerListenerPort`
		`SUN5.ini`
		`SESSION-MANAGER-PORT=50000`
			Proprietary interface

Session Manager
Port allocation Range(s)
	40100 to 40999	Registry entries:
		`HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Sunsystems\Core\5.1\SessionManager\PORTRANGE1_MIN`
		`HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\SunSystems\Core\5.1\SessionManager\PORTRANGE1_MAX`
			40101 is the first available port
			Can have multiple ranges, for example, `RANGE2_MIN` etc.

CDR (Common Data Retrieval Service)	40100	Automatically configured	Derived from first entry in session manager port range
MDBServices	40101	Automatically configured	Derived from second entry in session manager port range
ASP.NET State Server	42424	Configurable	
CDR (Listener)	50005	Registry entries: `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\SunSystems\Core\5.1\Comms\CDRListenerPort`	
Locator Service (listener)	50006	Registry entries: `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\SunSystems\Core\5.1\Comms\LocatorServiceListenerPort`	
Transfer Execution (listener)	50008	Registry entries: `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\SunSystems\Core\5.1\Comms\TransferExecutionListenerPort`	

Note: Ephemeral port range for Windows is 1024-5000. SunSystems Client creates random TCP ports on the client machine to connect to SunSystems application server in ephemeral port range. Adjust your firewall outbound ports accordingly (if necessary). In default configuration, firewalls do not restrict outbound ports.

Authentication Service

Component Description	Configured Default Port	Location and Configuration	Other Information
SunSystems Security	55000	global.config file located in: `C:\ProgramData\Infor\SunSystems\Security`	

Secure Job Execution	55001	props.xml file located in:
		`C:\ProgramData\Infor\SunSystems SSC\props.xml`
		`"secure_server_port" value="55001"`	

SunSystems Web Security	81		SunSystems Web authentication, hosted in IIS

Transfer Desk and SunSystems Connect

Component Description		Configured Default Port	Location and Configuration	Other Information

Transfer Desk Service	Listening port	50001	props.xml file located in:
			`C:\ProgramData\Infor\SunSystems SSC\`
			`"SERVER_PORT" value="50001"`
			`"secure_server-port" value="50001"`
			`"registry_port" value ="50001"`
				RMI interface

	RMI objects	50050 to
		50099
			props.xml file located in:
			`C:\ProgramData\Infor\SunSystems SSC\`
			`"ports.first" value="50050"`
			`"ports.last" value="50099"`
				RMI interface

	Job execution port	50002	props.xml file located in:
			`C:\ProgramData\Infor\SunSystems SSC\`
			`"job.server_port" value="50002"`
				Proprietary interface

SunSystems Connect Service		8080
		8443
			Server.xml located in:
			`C:\Program Files x86)\Infor\SunSystems\ssc\tomcat\conf\`
			`"Connector port" value="8080"`
				(SOAP interface)
				HTTP port
				HTTPS port

Note: Ephemeral port range for Windows is 1024-5000. Transfer Desk uses these ephemeral ports when it deals with certain SunSystems requests. These ephemeral ports must be configured to comply with local security policies. For access through the SunSystems Connect Service interface, this is not an issue.

SunSystems Reporting (SRS)

Component Description	Configured Default Port	Location and Configuration	Other Information
SRS	80	IIS Manager	Running in IIS

SunSystems Web

Component Description	Configured Default Port	Location and Configuration	Other Information
SunSystems Web	9080		Running in Tomcat

Database Settings (Informational)

Component Description	Configured Default Port	Location and Configuration	Other Information
Microsoft SQL Server default instance	1433	Enterprise Manager User Interface	
SQL Browser Service	1434		
Oracle	1521	Database Listener	

Appendix B – Default Folder Structure and Write Permission Requirements

After successful installation, Setup creates subfolders in the SunSystems program folder, and Program data folder.

Program folder location in Windows 2008/Windows 7: `C:\Program Files (x86)\Infor\SunSystems`.

Program data folder location in Windows 2008/Windows 7: `C:\ProgramData\Infor\SunSystems`.

SunSystems Program Folder Structure

Folder Name	Client Layer	Application Layer	File Types	Description	Write Permission Required

<installation folder>		✓		The Filter DD Regenerator function writes a log file to the SunSystems installation folder. The location of this log file cannot be changed.
				The installation folder is the default location for Financials-based work files, such as Ledger Entry.
				The `sun5.ini` configuration file can be used to change this default through the following entry:
				`[SunSystems]`
				`Sys-Work=`
				For example, change this to `Sys-Work=_work\` to redirect work files to the `_work` folder.
				On an individual SunSystems operator basis, the work folder can be set with the Operator Setup function. However, this has some limitations: a maximum of eight characters, and the inability to specify subfolders.
				Write access to the installation folder is required for the Serialization function as part of implementation or addition of new modules.
					✓

`_sql\procs`		✓	`.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.	
`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>.	

Folder Name	Client Layer	Application Layer	File Types	Description	Write Permission Required
ssc \bin \components \docs \help \jre \lib \localisation \tomcat	✓		.xml .txt .dat .slc .bat .dll .jar	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 Desks, Automation Desks, Component Manager, and Property Editor.	✓
ssc\tomcat \conf \webapps		✓	.conf .xml .dtd .jsp	The SSC server application. Subfolders contain Tomcat configuration and server application files.	
ssc\lib\client	✓			Deployment of SunSystems Connect and deployment of new SSC components causes files to be written to various folders under the ssc\lib\client root folder. This location cannot be changed.	✓

SunSystems Subfolders in Program Data

Windows 7 and Windows 2008: C:\ProgramData\Infor\SunSystems.

Folder Name	Client Layer	Application Layer	File Types	Description	Write Permission Required
_back	✓	✓	.bak	Written to by various functions such as Business Unit Copy, Business Unit Delete, Ledger Conversion, and Data Migration. Location is not configurable, that is, it must be underneath the SunSystems installation folder. Default backup folder for default Business Unit. Files are restored from here.	✓
_Data	✓	✓	.idx .dat	Data dictionary files and tables and schemata required when a database is created using scripts.	✓

Folder Name	Client Layer	Application Layer	File Types	Description	Write Permission Required
_Data\01		✓	.ctl .idx .dat	Written to by various functions such as Business Unit Copy, Business Unit Delete, Ledger Conversion, and Data Migration. Location is not configurable, that is, it must be underneath the SunSystems installation folder. Holds tables that are specific to the language that is selected during the installation process, that is, 01 is the folder for English.	✓
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\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.	✓
ClientFileDirectory	✓	✓	.dtd .msg .opx .rfx	Cached report executables, message files, menu files, and form files are downloaded from the server into this folder on the client. If reports are instigated from clients but configured to run on a Report Server machine, any parameters are stored here in an XML file. The locations can be changed for the various file types using the registry settings. Message files HKEY_LOCAL_MACHINE\SOFTWARE\SunSystems\Navigation Manager\5.1\FileCache\MSG DIRECTORY Form files HKEY_LOCAL_MACHINE\SOFTWARE\SunSystems\Navigation Manager\5.1\FileCache\RFX DIRECTORY The locations in the above two registry entries can be controlled using the FRREGEDIT function in its full mode, under the Client Settings\Client files directory entry. Report executables and XML parameter file passed from client to Report Server HKEY_LOCAL_MACHINE\SOFTWARE\SunSystems\ReportManager\5.1\Settings\CacheDirectory Also FormRunner writes out an OPXDTD.DTD file to the ClientFileDirectory folder, which is an XML document type definition file used to verify the integrity of the OPX (menu) files. Whenever the menu file is accessed, this file is written out.	✓

Folder Name	Client Layer	Application Layer	File Types	Description	Write Permission Required
ClientFileDirectory\LocalCompile	✓	✓	.msg	The client directory holds run-time form (RFX) files for locally compiled SFL forms. Used by Form Designer to write the locally compiled RFX file to. Also writes *.rfx.log and *.sfl.log files in this directory if the local compilation fails. It is set during installation to \ClientFileDirectory\LocalCompile\, in the SunSystems root directory. The location can be changed using the registry setting: HKEY_LOCAL_MACHINE\SOFTWARE\SunSystems\Navigation Manager\5.1\FileCache\Local Compile Directory The location in this registry entry can be controlled using the FRREGEDIT function in full mode, under the Client Settings\Client files directory entry.	✓
ServerFiles		✓	.rfx .sfl .opr .dat .idx .msg	The ServerFiles folder stores SFL (source form layout) files, RFX (run time forms) files, RFD (form definition) files (.dat and .idx) and menu files. Used by Form Designer, Filter Designer, Filter DD Regeneration, and Form Compiler. Form Designer receives the server copy of SFL files from this directory and writes SFL files to it when checking them in. When Form Designer creates a new filter function, it also writes RFD .dat and .idx files to this directory. Form Compiler writes RFX files to this directory. If the form compilation fails, Form Compiler writes *.rfx.log and *.sfl.log files in this directory. The folder location is set during installation to \ServerFiles, in the SunSystems root directory. This location can be changed by using the Database Processing options on the installation media. For more information, refer to the Database Administration section of this installation guide. If the ServerFiles location is on a different machine to the application server, the full path must be specified. **Note**: Server file names must not contain spaces. FormRunner writes out an OPXDTD.DTD file to the ServerFiles folder, which is an XML document type definition file that is used to verify the integrity of the OPX (menu) files. Whenever the menu file is accessed, this file is written here.	✓
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, the directory is created and is set to ServerInfoCache\ by the installation procedure. The location of this directory cannot be changed.	✓
Sstm\transferlogs		✓		This folder is written to by Transfer Desks and is used to store log files that detail transfer results. The location of this directory cannot be changed.	

Folder Name	Client Layer	Application Layer	File Types	Description	Write Permission Required
Ssts \adm		✓	.adm	The layouts for the import files.	
Upgrade \UpgradeTo51 x \CustomPost		✓		The upgrade routine to upgrade SFL (form source) files and SRD (data source) files writes the upgraded files to this directory. The upgrade routine to upgrade OPX (menu) files writes the upgraded files to this directory. The SFL conversion routine to convert SFL files writes the converted files to this directory. The location is set by the installation routine. It is used when upgrading SunSystems from one version to another. The location of this directory cannot be changed.	✓
Upgrade \UpgradeTo51 x \log		✓		The upgrade routine to upgrade SFL files and SRD files writes log files to this directory. The upgrade routine to upgrade OPX files writes log files to this directory. The SFL conversion routine to convert SFL files writes log files to this directory. The location is set by the installation routine. It is used when upgrading SunSystems from one version to another. The location of this directory cannot be changed.	✓
C:\Temp	✓			By default, the server context information (from RptParams) is downloaded to this folder. A temporary subfolder is created and the ROX file is copied there (from ClientFileDirectory), from where it is run. This is to avoid contention problems with multiple ReportManagers accessing the same file at the same time. The location can be changed using a registry setting: (HKEY_CURRENT_USER\SOFTWARE\SunSystems\ReportManager\5.1\Settings\WorkDirectory). Report Designer also writes temporary files to this location.	✓
Temp		✓		Certain processes write temporary files to the location pointed to by the TEMP environment variable. Therefore, write permissions are required for this folder.	✓
ssc \bin \components \docs \help \jre \lib \localisation \tomcat	✓		.xml .txt .dat .slc .bat .dll .jar	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 Desks, Automation Desks, Component Manager, and Property Editor. SunSystems Connect and Transfer Desks require write permissions to ssc\lib\drivers\sasi\classes and ssc\lib\drivers\sasi\java as they compile classes at run-time in these locations. Property Editor maintains numerous files in ssc\lib\properties.	✓

Folder Name	Client Layer	Application Layer	File Types	Description	Write Permission Required
SunSystems	✓	✓		All the installer log files, such as InstallLog.log, InstalldatabaseLog.log go here.	✓
SunSystems\FormCompiler	✓	✓			✓
SunSystems\Navigator	✓	✓		All the log files that correspond to SunSystems user interface navigation go here.	✓
SunSystems\Cobol		✓			✓
SunSystems\DataLoad		✓			✓
SunSystems\FormCompiler		✓			✓
SunSystems\SqlInstaller		✓		SQL Installer log files	✓
SunSystems\SSC		✓		All the SSC-related log files go here.	✓

Note: Order Fulfilment modules do not write temporary files.

SunSystems Logs Folder

Windows 2008, Windows 7: `C:\ProgramData\Infor\Logs`.

SunSystems Connect Logs Folder

The folder used for SunSystems Connect logging depends on your operating system, as follows:

Windows 7 and Windows 2008: `C:\ProgramData\Infor\Logs\ssc\transferlogs`

Appendix C – Changing Location of SunSystems Components in Multi-Tier Configurations

Reconfiguring SunSystems Client Connections

Security Server, SunSystems Application Server and Connect Service

From Start, Infor10 Financials SunSystems, Tools, Switch Server dialog enables you to reconfigure SunSystems Client links to Security Server, SunSystems Application Server and Connect Service.

SunSystems Reporting Services Client Applications (installed via SunSystems Client or SRS Client)

Using an editor in administrator mode, amend the following config files substituting <SERVERNAME> with the name of your SRS Server.

DataAccessManager [Program Files (x86)\Infor\SunSystems\DataAccessManager.exe.config]

```
 <appSettings>
  <add key="SystemsUnion.Tools.SunSystemsStudio.StudioWebServiceURL" value="http://<SERVERNAME>/SunSystemsReportServer/SunSystemsStudio.asmx" />
 </appSettings>
<applicationSettings>
  <Properties.Settings>
   <setting name="DataAccessManager_SystemsUnion_Tools_SunSystemsStudio_SunSystemsStudio" serializeAs="String">
            <value>http://< SERVERNAME >/SunSystemsReportServer/SunSystemsStudio.asmx</value>
   </setting>
  </Properties.Settings>
 </applicationSettings>
```

Report Administrator [Program Files (x86)\Infor\SunSystems\ReportAdministrator.exe.config]

```
<appSettings>
  <add key="SystemsUnion.Core.Configuration.ConfigurationWebServiceURL" value="http://< SERVERNAME >/SunSystemsReportServer/Configuration.asmx" />
  <add key="SystemsUnion.Core.DataSource.Factory.DataSourceWebServiceURL" value="http://< SERVERNAME >/SunSystemsReportServer/DataSource.asmx" />
  <add key="SystemsUnion.Core.SunSystems5.SunSystemsInformationWebServiceURL" value="http://< SERVERNAME >/SunSystemsReportServer/SunSystems.asmx" />
  <add key="SystemsUnion.Services.Data.Dictionary.Service.ReportingDictionaryServiceURL" value="http://< SERVERNAME >/SunSystemsReportServer/Dictionary.asmx" />
  <add key="SystemsUnion.Services.Data.SpecialFields.Service.SpecialFieldsWebServiceURL" value="http://< SERVERNAME >/SunSystemsReportServer/SpecialFields.asmx" />
  <add key="SystemsUnion.Services.Data.Dictionary.Service.MetaDataDetailsWebServiceURL" value="http://< SERVERNAME >/SunSystemsReportServer/MetaDataDetails.asmx" />
  <add key="SystemsUnion.Services.Data.MetaData.Service.ReportingMetaDataWebServiceURL" value="http://< SERVERNAME >/SunSystemsReportServer/MetaData.asmx" />
  <add key="SystemsUnion.Services.Data.MetaData.Service.PanApplicationReportingMetaDataWebServiceURL" value="http://< SERVERNAME >/SunSystemsReportServer/PanApplicationMetaData.asmx" />
```

```
</appSettings>
<VisionReportingClient>
  <add key="WS_ENDPOINT_URL_REPORT_MANAGEMENT_SERVICE" value="http://<SERVERNAME>/SunSystemsReportManager/ReportManagementService.asmx" />
  <add key="WS_ENDPOINT_URL_RENDER_SERVICE" value="http://<SERVERNAME>/SunSystemsReportManager/RenderQueueService.asmx" />
  <add key="WS_ENDPOINT_URL_LOOKUP_SERVICE" value="http://<SERVERNAME>/SunSystemsReportManager/LookupService.asmx" />
</VisionReportingClient>
```

Report Designer [Program Files (x86)\Infor\SunSystems\ReportDesigner.exe.config]

```
<add key="SystemsUnion.Core.DataSource.Factory.DataSourceWebServiceURL" value="http://<SERVERNAME>/SunSystemsReportServer/DataSource.asmx"/>
<add key="SystemsUnion.Core.SunSystems5.SunSystemsInformationWebServiceURL" value="http://<SERVERNAME>/SunSystemsReportServer/SunSystems.asmx"/>
<add key="SystemsUnion.Core.AppDictionary.Client.LocalisedObjectServiceURL" value="http://<SERVERNAME>/SunSystemsReportServer/LocalisedObjectWebService.asmx"/>
<add key="SystemsUnion.Services.Data.Dictionary.Service.ReportingDictionaryServiceURL" value="http://<SERVERNAME>/SunSystemsReportServer/Dictionary.asmx"/>
<add key="SystemsUnion.Services.Data.SpecialFields.Service.SpecialFieldsWebServiceURL" value="http://<SERVERNAME>/SunSystemsReportServer/SpecialFields.asmx"/>
<add key="SystemsUnion.Services.Data.Dictionary.Service.MetaDataDetailsWebServiceURL" value="http://<SERVERNAME>/SunSystemsReportServer/MetaDataDetails.asmx"/>
<add key="SystemsUnion.Services.Data.MetaData.Service.ReportingMetaDataWebServiceURL" value="http://<SERVERNAME>/SunSystemsReportServer/MetaData.asmx"/>
<add key="SystemsUnion.Services.Data.MetaData.Service.PanApplicationReportingMetaDataWebServiceURL" value="http://<SERVERNAME>/SunSystemsReportServer/PanApplicationMetaData.asmx"/>
<add key="PrintPreviewParameterEntryPage" value="http:// <SERVERNAME>//SunSystemsReportManager/secure/ParameterEntryForm.aspx?reportExecutable={0}&amp;printPreviewParameters=1&amp;
postId={1}"/>
<add key="PrintPreviewRenderPage" value="http:// <SERVERNAME>//SunSystemsReportManager/secure/PreviewReportRender.aspx?reportExecutable={0}&amp;printPreviewRender=1&amp;postId={1}"/>
<add key="WS_ENDPOINT_URL_REPORT_MANAGEMENT_SERVICE" value="http://<SERVERNAME>/SunSystemsReportManager/ReportManagementService.asmx"/>
<add key="WS_ENDPOINT_URL_RENDER_SERVICE" value="http://<SERVERNAME>/SunSystemsReportManager/RenderQueueService.asmx"/>
<add key="WS_ENDPOINT_URL_LOOKUP_SERVICE" value="http://<SERVERNAME>/SunSystemsReportManager/LookupService.asmx"/>
```

Changing Location of SQL Server Reporting Services (SSRS)

On the SunSystems Report Manager Server, edit web.config in administrator mode, and substitute <SERVERNAME> with the name of the SSRS server.

SunSystemsReportManager [Infor\SunSystemsReportingServices\web\SunSystemsReportManager\web.config]

```
<VisionReportManager>
  <add key="MSRS_REPORT_SERVER_SERVICE" value="http://<SERVERNAME>/ReportServer /ReportService2010.asmx"/>
  <add key="SSRS_REPORT_EXECUTION_SERVICE" value="http://< SERVERNAME >/ReportServer /ReportExecution2005.asmx"/>
```

</VisionReportManager>

If you have multiple SunSystemsReportManager installations you must change all of them.

Changing Location of SunSystemsReportServer

On the SunSystems Report Manager Server, edit web.config in administrator mode, and substitute <SERVERNAME> with the name of the SunSystems Report Server.

SunSystemsReportManager [Infor\SunSystemsReportingServices\web\SunSystemsReportManager\web.config]

If you have multiple SunSystemsReportManager installations you must change all of them.

<add key="SystemsUnion.Core.Configuration.ConfigurationWebServiceURL" value="http://< SERVERNAME >/SunSystemsReportServer/Configuration.asmx"/>
<add key="SystemsUnion.Core.Repository.Manager.RepositoryWebServiceURL" value="http://< SERVERNAME >/SunSystemsReportServer/Repository.asmx"/>
<add key="SystemsUnion.Core.DataSource.Factory.DataSourceWebServiceURL" value="http://< SERVERNAME >/SunSystemsReportServer/DataSource.asmx"/>
<add key="SystemsUnion.Core.AppDictionary.Client.DictionaryServiceURL" value="http://< SERVERNAME >/SunSystemsReportServer/DictionaryService.asmx"/>
<add key="SystemsUnion.Core.SunSystems5.SunSystemsInformationWebServiceURL" value="http://< SERVERNAME >/SunSystemsReportServer/SunSystems.asmx"/>
<add key="SystemsUnion.Core.AppDictionary.Client.LocalisedObjectServiceURL" value="http://< SERVERNAME >/SunSystemsReportServer/LocalisedObjectWebService.asmx"/>
<add key="SystemsUnion.Services.Data.MetaData.Service.PanApplicationReportingMetaDataWebServiceURL" value="http://< SERVERNAME >/SunSystemsReportServer/PanApplicationReportingQueryService.asmx"/>
<add key="SystemsUnion.Services.Data.MetaData.Service.ReportingMetaDataWebServiceURL" value="http://< SERVERNAME >/SunSystemsReportServer/MetaData.asmx"/>
<add key="SystemsUnion.Services.Data.Dictionary.Service.SpecialReportingDictionaryServiceURL" value="http://< SERVERNAME >/SunSystemsReportServer/Dictionary.asmx"/>
<add key="SystemsUnion.Services.Data.Execution.Service.ExecutionWebServiceURL" value="http://< SERVERNAME >/SunSystemsReportServer/Execution.asmx"/>
<add key="SystemsUnion.Services.Data.Dictionary.Service.ReportingDictionaryServiceURL" value="http://< SERVERNAME >/SunSystemsReportServer/Dictionary.asmx"/>
<add key="SystemsUnion.Services.Data.SpecialFields.Service.SpecialFieldsWebServiceURL" value="http://< SERVERNAME >/SunSystemsReportServer/SpecialFields.asmx"/>
<add key="SystemsUnion.Services.Data.MetaData.Service.PanApplicationReportingMetaDataWebServiceURL" value="http://< SERVERNAME >/SunSystemsReportServer/PanApplicationMetaData.asmx"/>

On the SSRS server, edit web.config in administrator mode, and substitute <SERVERNAME> with the name of the SunSystems Report Server.

[Program Files\Microsoft SQL Server\MSRS10_50.MSSQLSERVER\Reporting Services\ReportServer\web.config]

<add key="SystemsUnion.Core.UserInfo.Service.UserInfoWebServiceURL" value="http://< SERVERNAME>/SunSystemsReportServer/UserInfo.asmx" />
<add key="SystemsUnion.Core.Repository.Manager.RepositoryWebServiceURL" value="http://< SERVERNAME>/SunSystemsReportServer/Repository.asmx" />
<add key="SystemsUnion.Core.Configuration.ConfigurationWebServiceURL" value="http://< SERVERNAME>/SunSystemsReportServer/Configuration.asmx" />
<add key="SystemsUnion.Core.DataSource.Factory.DataSourceWebServiceURL" value="http://< SERVERNAME>/SunSystemsReportServer/DataSource.asmx" />
<add key="SystemsUnion.Core.AppDictionary.Client.DictionaryServiceURL" value="http://< SERVERNAME>/SunSystemsReportServer/DictionaryService.asmx" />
<add key="SystemsUnion.Core.SunSystems5.SunSystemsInformationWebServiceURL" value="http://< SERVERNAME>/SunSystemsReportServer/SunSystems.asmx" />
<add key="SystemsUnion.Services.Data.MetaData.Service.ReportingMetaDataWebServiceURL" value="http://< SERVERNAME>/SunSystemsReportServer/MetaData.asmx" />

<add key="SystemsUnion.Services.Data.Execution.Service.ExecutionWebServiceURL" value="http://< SERVERNAME>/SunSystemsReportServer/Execution.asmx" />

<add key="SystemsUnion.Services.Data.Dictionary.Service.ReportingDictionaryServiceURL" value="http://< SERVERNAME>/SunSystemsReportServer/Dictionary.asmx" />

<add key="SystemsUnion.Services.Data.SpecialFields.Service.SpecialFieldsWebServiceURL" value="http://< SERVERNAME>/SunSystemsReportServer/SpecialFields.asmx" />

<add key="SystemsUnion.Services.Data.MetaData.Service.PanApplicationReportingMetaDataWebServiceURL" value="http://< SERVERNAME>/SunSystemsReportServer/PanApplicationMetaData.asmx" />

Changing Location of SunSystems Report Manager

The SunSystems Domain schema holds the location of SunSystems Report Manager. Edit DOMN_VRTL_HOST table. Select the row where DFLT_PATH = 'SunSystemsReportManager' and update ACTUAL_HOST_NAME to the new name of the SunSystems Report Manager server.

Appendix D – Application Files

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
.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

File Suffix	File type	Usage	
.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 on Virtualization Software/Terminal Services/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

SunSystems can also centralize all the log files into a single location, which facilitates finding and analyzing the log file. The following table contains all the log files and their control mechanism.

The location of these files is as follows:

Windows 2008/Windows 7: `C:\ProgramData\Infor\Logs\SunSystems\logs`

Log File Name	Description
`InstallLog.txt`	Installation log file
`InstallDatabaseLog.log`	Database Installation log
`Navigator \ MenuImportexport.log`	
`Navigator \ MenuMigrationV5.log`	
`SunSystems.log`	
`SunSystems.v5.log`	
`SqlInstaller \ SQLxx_xxxx_xxxx.log`	SQL execution logs
`SSC\memory-monitor.log`	
`SSC\logging\`	
`FormCompiler\`	Form compilation log
`DataLoad\Domain`	Domain Database uploading error log
`Cobol\`	Cobol application log files

Appendix G – SunSystems Security

Standard Single Sign On

When using Windows authentication, mapped users are not prompted to log in to SunSystems because the security client automatically identifies them as a valid user. This single sign on behaviour can also be achieved when using standard authentication, that is, user name and password, by utilising the login monitor tool.

This program displays a small icon in the system notification area, normally at the right or bottom of the Windows Task Bar. The Login Monitor controls access to the saved user credentials and gives them to any SunSystems Security-enabled application that requests authentication.

The Login Monitor program is automatically started when a Windows session begins; under normal circumstances, the program continues to be active until the user logs out of Windows or closes the application by right-clicking the icon and clicking Exit on the shortcut menu. The administrator can also opt to remove the program from start-up so it never appears to the end user, or right click the icon and select Exit Login Monitor to switch it off.

Logging Out

To open a status dialog box that displays the user name of the SunSystems user currently cached, double-click Login Monitor. To discard the saved user credentials, click Log Out so that the next SunSystems application that is started displays a new login dialog box, which allows the user to log in as a different SunSystems user. Any applications that are already running continue to run in the context of the original user.

If all applications are closed down, the login monitor will retain the last credentials used. As far as SunSystems is concerned, the user is not logged in to SunSystems, but the credentials are cached on the client so that the next login attempt does not need to prompt for a user name and password.

When you use this feature, note the following points:

- Closing an application logs you out of the application, but the login monitor still shows the current cached user.
- Logging out of the Single Sign On session neither logs you out of any applications that are currently running, nor does it close those applications.
- If you are in a high-security environment, you should log out of the Single Sign On session when away from your desk for extended periods. This minimizes the risk of an unauthorised person using your machine in your absence.

Note: Single Sign On functionality is limited when deploying applications on Citrix as published applications. Credentials are not shared between publications and there is no Login Monitor. However, it is fully functional through a Citrix published desktop.

Appendix H – Administrative Access Recovery

There are a number of scenarios when the Administrator may be unable to access User Manager. For example, because of 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. Depending on operating system, this may be located under `\Documents and Settings\All Users\Application Data\Infor\SunSystems\Security`, or `\Users\All Users\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 in order 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.

Appendix I – Sample Oracle INIT.ORA File

The following list gives an example of an INIT.ORA file which is compatible with SunSystems 6.1.0 using Oracle 11gR1 against a codepage 1252 (Western European) database.

> **Note**: Before you use this example, first review whether the memory and process limits are scaled for your implementation of SunSystems, and also check that the Locale is correct. Failure to do so will lead to an invalid implementation of SunSystems.

```
sundb.__db_cache_size=205520896
sundb.__java_pool_size=4194304
sundb.__large_pool_size=4194304
sundb.__oracle_base='C:\oracle'#ORACLE_BASE set from environment
sundb.__pga_aggregate_target=306184192
sundb.__sga_target=532676608
sundb.__shared_io_pool_size=0
sundb.__shared_pool_size=314572800
sundb.__streams_pool_size=0
background_dump_dest='C:\oracle\admin\sundb\bdump'
compatible='11.1.0'
control_files='C:\oracle\oradata\sundb\control01.ctl','C:\oracle\oradata\sundb\c
ontrol02.ctl','C:\oracle\oradata\sundb\control03.ctl'
core_dump_dest='C:\oracle\admin\sundb\cdump'
db_block_checksum='TYPICAL'
db_block_size=8192
db_cache_advice='ON'
db_cache_size=0
db_create_file_dest='C:\oracle\oradata\sundb'
db_domain=''
db_file_multiblock_read_count=8
db_files=256
db_name='sundb'
db_recycle_cache_size=0
db_securefile='NEVER'
diagnostic_dest='C:\ORACLE'
fast_start_mttr_target=0
global_names=FALSE
instance_name='sundb'
java_max_sessionspace_size=0
java_pool_size=0
java_soft_sessionspace_limit=0
job_queue_processes=2
large_pool_size=0
log_archive_start=TRUE
log_buffer=524288
```

```
log_checkpoints_to_alert=TRUE
memory_max_target=800M
memory_target=800M
nls_language='ENGLISH'
nls_sort='BINARY'
nls_territory='UNITED KINGDOM'
open_cursors=512
optimizer_features_enable='11.1.0.6'
optimizer_mode='ALL_ROWS'
pga_aggregate_target=0
processes=500
recyclebin='OFF'
remote_login_passwordfile='EXCLUSIVE'
session_cached_cursors=32
sessions=550
sga_max_size=512M
shared_pool_reserved_size=16M
shared_pool_size=0
sort_area_retained_size=0
sort_area_size=8388608
star_transformation_enabled='FALSE'
timed_statistics=TRUE
transactions=610
undo_management='AUTO'
undo_retention=900
undo_tablespace='UNDOTBS'
user_dump_dest='C:\oracle\admin\sundb\udump'
workarea_size_policy='AUTO'
“_optimizer_join_elimination_enabled"=false
remote_os_authent=TRUE
```

Appendix J – Creating a New Oracle Service Account

If a change to the account under which the SunSytems Global Security service runs is changed, a corresponding database account/user must be created in the database as follows:

```
CREATE USER "OPS$<Domain/Workgroup>\<Domain/Workgroup Account>"
IDENTIFIED EXTERNALLY
DEFAULT TABLESPACE <Tablespace Name>
TEMPORARY TABLESPACE <Temporary Tablespace Name>
PROFILE DEFAULT
ACCOUNT UNLOCK;
```

where:

<Domain/Workgroup> is the name of the domain or workgroup.

<Domain/Workgroup Account>" is the account name.

<Tablespace Name> is the name of the tablespace to be assigned as the default tablespace for the user.

<Temporary Tablespace Name> is the name of the temporary tablespace to be assigned to the user.

Once the user has been successfully created, the following system privileges must be granted to the user:

```
GRANT CREATE SESSION TO "OPS$<Domain/Workgroup>\<Domain/Workgroup Account>";
GRANT CREATE USER TO "OPS$<Domain/Workgroup>\<Domain/Workgroup Account>";
```

Grant the following object priveleges to the user:

```
GRANT ALTER, DELETE, INDEX, INSERT, REFERENCES, SELECT, UPDATE, ON COMMIT
REFRESH, QUERY REWRITE, DEBUG, FLASHBACK ON <SECURITY SCHEMA NAME>.DOMN_GS_AUDIT
TO "OPS$<Domain/Workgroup>\<Domain/Workgroup Account>";

GRANT ALTER, DELETE, INDEX, INSERT, REFERENCES, SELECT, UPDATE, ON COMMIT
REFRESH, QUERY REWRITE, DEBUG, FLASHBACK ON <SECURITY SCHEMA
NAME>.DOMN_GS_AUDIT_ARCHIVE TO "OPS$<Domain/Workgroup>\<Domain/Workgroup
Account>";

GRANT ALTER, DELETE, INDEX, INSERT, REFERENCES, SELECT, UPDATE, ON COMMIT
REFRESH, QUERY REWRITE, DEBUG, FLASHBACK ON <SECURITY SCHEMA
NAME>.LANGUAGE_MAPPING TO "OPS$<Domain/Workgroup>\<Domain/Workgroup Account>";

GRANT ALTER, DELETE, INDEX, INSERT, REFERENCES, SELECT, UPDATE, ON COMMIT
REFRESH, QUERY REWRITE, DEBUG, FLASHBACK ON <SECURITY SCHEMA
NAME>.SECURITY_PROPERTIES TO "OPS$<Domain/Workgroup>\<Domain/Workgroup
Account>";

GRANT ALTER, DELETE, INDEX, INSERT, REFERENCES, SELECT, UPDATE, ON COMMIT
REFRESH, QUERY REWRITE, DEBUG, FLASHBACK ON <SECURITY SCHEMA
NAME>.SUNSYSTEMS_LANGUAGE TO "OPS$<Domain/Workgroup>\<Domain/Workgroup
Account>";
```

where:

<SECURITY SCHEMA NAME> is the name of the schema that was provided during the installation.

Note: If the database is hosted on a UNIX server, the database account must be created without the <Domain/Workgroup> and privileges granted accordingly, because Windows Operating Systems do not send the Windows domain/workgroup name with the Windows domain/workgroup acccount when connecting to databases on UNIX.