Sysgem Enterprise Manager

Installation Guide

By Sysgem AG

Sysgem is a trademark of Sysgem AG. Other brands and products are registered trademarks of their respective holders. © 2000 Sysgem AG, Mühlebachstr. 84, CH-8008 Zürich, Switzerland, office@sysgem.com. All rights reserved.

Contents

Introduction 1

What's Inside 1
Available Product Guides 1
Contacting Us 1

Quick Start 3

Overview 3
Typical Configuration 3
Test System for Evaluation 4
Security Key 4
Installation and Configuration 4
Installing Windows 2000/NT Software 4
Installing Other Platform Agents 5
Entering an Evaluation License (First-Time Login) 5
Importing a Permanent SEM License 6
Installing Plug-In Application Modules 6
Installing Application Support Packages 6

Windows 2000/NT Software 7

Contents of Kit 7
SEM Components 7
System Hygiene 8
Prerequisites 8
Extras 8
Installing on Windows 2000/NT 8
SEM Windows 2000/NT Kit 9
Files Installed 11
Configuration Files 12
De-installation 13

AS400 15

Installing on AS400 15
Installing 15
Configure the software 17

OpenVMS Agent 19

Installing on OpenVMS 19
Example Installation 19
Files Installed 23

UNIX/Linux Agents 25

Introduction 25
Example 25
Files Installed 28
Root Directory 28

Agent Files ... 28
AutoStart ... 29
Stopping The Agent ... 30
Changing The Security Key ... 31

Configuration 33

Overview ... 33
Licenses ... 33
Editing an Evaluation License (First-Time Login) ... 33
Ordering a Permanent SEM License ... 34
Importing a Permanent SEM License ... 35
Installing Plug-In Application Modules ... 35
Installing Application Support Packages ... 35
License Manager ... 36
License Editor ... 37
Fields ... 37
Options ... 37
Security Keys ... 38
Setting Security Keys on NT ... 38
Setting Security Keys on OpenVMS ... 38
Setting Security Keys on UNIX/Linux ... 38
SEM Accounts ... 39
Mirrored Accounts ... 39
Option Settings ... 39
Account Passwords ... 39
Profiles ... 39
Tokens ... 40
Library Mappings ... 40
Agent Definitions ... 40
Archive ... 40
Templates ... 41

Problem Solving 43

Communications ... 43
PERL ... 43
Security Key ... 43
Common Socket Errors ... 44
Full List of Socket Errors ... 44

Annex: Security Keys 51

Introduction ... 51
Storage ... 51
Standard Security Keys ... 52
Simple ... 52
Advanced ... 52
Installation Keys ... 53
Domains ... 53
Advanced Example ... 54
Challenge / Response Authentication ... 55
Changing the Key ... 57
Management Console ... 57
Authorization Server ... 58
Obtaining Installation Keys ... 60
OpenVMS Server ... 59
Windows NT Server ... 59
Checking the Keys ... 60

Index 61

Introduction

What's Inside

This is the guide to installing and configuring the Sysgem Enterprise Manager (SEM) Base Framework on your systems.

For further information see also the other available product guides (shipped with SEM and available from the Downloads section of the Sysgem web site).

See also the *SEM Release Notes* for the latest features added to SEM.

Available Product Guides

1. SEM Installation Guide

   The guide to installing and configuring the Sysgem Enterprise Manager (SEM) Base Framework on your systems.

2. SEM User Guide

   The guide to using the Sysgem Enterprise Manager (SEM) Base Framework.

3. SSyM User Guide

   The guide to using the Sysgem System Manager (SSyM) Module.

4. SAcM User Guide

   The guide to using the Sysgem Account Manager (SAcM) Module.

5. SSeM User Guide

   The guide to using the Sysgem Security Manager (SSeM) Module.

6. SDeM User Guide

   The Guide to using the Sysgem Development Manager (SDeM) Module.

Contacting Us

Please contact your supplier or Sysgem AG at any time via Online Support on the Sysgem web page http://www.sysgem.com.

Quick Start

Overview

Typical Configuration

Sysgem Enterprise Manager (SEM) is a distributed application. In use, SEM is installed on one or more systems throughout an enterprise, allowing remote task-specific management of those systems and its layered applications.

A SEM installation consists of:

A. Three mandatory *SEM Base Framework Components:*

1. The SEM Management Console (the graphic user interface - GUI) is installed on a Windows 2000 or Windows NT system (usually a server and accessed from workstations).
2. The SEM Authorization Server. This stores logon information and user settings and is installed on a Windows 2000 or Windows NT system (usually a server).
3. One or more platform-specific SEM Agents (Novell NetWare[1], OpenVMS, OS/400, UNIX/Linux[2], Windows 2000/NT, etc.).

B. One or more task-specific *SEM Plug-In Application Modules:*

- Sysgem System Manager (SSyM) Module
- Sysgem Account Manager (SAcM) Module
- Sysgem Security Manager (SSeM) Module
- Sysgem Development Manager (SDeM) Module

C. Optional *SEM Application Support Packages:*

- SEM Lotus Notes Package
- SEM MS Exchange Package
- SEM Oracle Package
- SEM Pathworks Package
- SEM PMDF Package
- SEM SAP Package
- etc.

---

[1] Novell NetWare support is contained within the standard SEM Agent software running on Windows 2000/NT.

[2] The SEM Agent for UNIX/Linux currently supports: Compaq Tru64 (Digital UNIX), HP UNIX, SUN Solaris, IBM AIX, Linux on Intel Machines (Mandrake, Red Hat, SuSE).

Test System for Evaluation

If you are installing a test system for evaluation you can install the mandatory SEM Base Framework Components (the Management Console, the Authorization Server and a Windows 2000/ NT Agent) on a single Windows 2000/NT system (workstation or server).

All available SEM Plug-In Applications Modules and Application Support Packages are automatically loaded after you have entered an evaluation license.

Security Key

During installation you will be prompted to configure Security Keys. These are central to controlling which machines can use or be managed by your SEM installation.

New in version 2.1: Starting with version 2.1 of SEM, a security key can take two forms:

- Standard security keys are free-format, case-sensitive, alphanumeric phrases that are unique to your customer site.

  Each key is similar to a password, and you will need to decide on it and set it during the installation. It is essential that you remember it - it must be entered in exactly the same way for every component you install on your network.

- Installation keys add an additional layer of security to the system by requiring the administrator to generate keys using the authorization server before installation of components on other machines can proceed.

  A system using installation keys requires more planning and some administrative overhead when installing new software components, and also requires that your managed agents can communicate with the authorization server.

The two security key schemes are described in more detail in the annex to this document.

If you want components of SEM version 2.0 to interoperate with your new installation, you **must** have at least one standard security key configured.

Installation and Configuration

Installing Windows 2000/NT Software

Load the SEM CD and from the main AutoPlay menu choose “Install Kits…”.

- Select “Install Windows 2000/NT Software”.
- The InstallShield window will appear. Installation will be automatic. The default replies to questions are usually correct.
- You will be prompted for an installation password. Check with Sysgem’s Online Support (via the Sysgem web site) for the password to the current version.
- You will be asked to enter your security key (see above).

Installing Other Platform Agents

Load the SEM CD and from the main AutoPlay menu choose “Install Kits…”.

To install SEM on other platforms, select “Browse CD for other PlatformKits”. Pick the appropriate platform agent kit and copy (with ftp) to an appropriate directory on the target machine.

Novell NetWare

A separate Novell NetWare agent for managing the Novell server does not need to be installed, since it is contained within the standard SEM Agent software running on Windows 2000/NT. The Novell management scripts are distributed with the SEM Plug-In Application Modules and are transmitted from the SEM Management Console to the standard SEM Agent runnning on Windows 2000/NT. The Windows machine running the Agent requires the Novell Client to be installed.

OpenVMS

Unzip the kit on OpenVMS (see Xtras folder on the CD if you do not have UNZIP.EXE for OpenVMS). Then perform a standard installation using VMSINSTAL.

```
$ UNZIP :== $SYS$MANAGER:UNZIPAXP.EXE
$ UNZIP VMS_AGENT_021_A.ZIP
$ @SYS$UPDATE:VMSINSTAL VMSAGENT021 SYS$SYSROOT:[SYSMGR.SEMKIT]
```

UNIX/Linux

FTP the unixagent020.tar file from the SEM CD to an approriate directory on the UNIX/Linux machine.

```
# cd /kits/SEM_kit
# tar -xvf UNIX_agent_021.tar
# ./setup
```

Entering an Evaluation License (First-Time Login)

Log into SEM with the pre-installed SEM username and password:

Username:	**Demo**	(pre-configured demonstration environment)
	- or -	
	System	(full access to all features)
Password:	**sysgem**	

You will then be prompted for evaluation license information that you have to type in:

- Company/Organization name
- City
- Zip code
- Country

You are now licensed with full functionality for a limited period of 30 days. If you need to extend this evaluation period, contact Sysgem’s Online Support (via the Sysgem web site).

Importing a Permanent SEM License

Log into SEM and select:

File -> Import and Export -> Import License.

Pick the "SEM License PAK YYMMDDNN.txt" file from the "SEM_License" folder of your SEM CD.

Installing Plug-In Application Modules

All licensed SEM Plug-In Applications Modules are automatically available after you have installed a valid license.

Installing Application Support Packages

All licensed SEM Application Support Packages are automatically available after you have installed a valid license.

Windows 2000/NT Software

Contents of Kit

The Windows 2000/NT kit on the SEM CD contains:

- SEM Management Console
- SEM Authorization Server
- SEM Agent for Windows 2000/NT
- SEM Installation Guide
- VNC Remote Desktop Server

This kit contains all the SEM components you need for a full SEM installation on a Windows 2000/NT system.

If you are using NT 4.0 it is recommended that you install Service Pack3 (or higher). A copy is provided on the SEM CD.

SEM Components

The following components can be installed in any combination on Windows 2000 or Windows NT Workstations or Servers:

- SEM Management Console
- SEM Authorization Server
- SEM Agent for Windows 2000/NT

The SEM Management Console provides the Windows-based User Interface for the SEM user. It runs on the user's Windows 2000/NT workstation, but may be installed on a central Windows 2000/NT Server and accessed remotely.

The SEM Authorization Server controls the use of Sysgem Enterprise Manager on your network. The Authorization Server validates the login password whenever a user logs into SEM. There is normally a Primary Authorization Server installed on a Windows 2000/NT Server, and a backup installation for use if the Primary Authorization Server becomes unavailable. The Authorization Server runs as an NT Service. It uses an Access Control Profile granted to the user to control the privilege level allocated and to grant access to permitted product features. Archive databases and audit trails are normally stored on the same system as the Authorization Server.

The SEM Agent for Windows 2000/NT is installed on all Windows 2000/NT Servers being managed by SEM. It is normally installed, as a minimum, on the customer's Primary (NT) Domain Controller (PDC).

System Hygiene

SEM has been designed to install without modifying your existing files. All files installed on a Windows 2000/NT system reside in folders and sub-folders within a root directory called SYSGEM. You can select the location of this directory during the installation. All system and application extension files (.dlls) installed by SEM are installed in private directories within the “SYSGEM” root directory.

The interpretive command language “Perl” is used by all NT components of SEM, but a private installation of Perl is provided within the Sysgem root directory and used exclusively by SEM. This private installation does not affect any other version of Perl installed on the same system.

Prerequisites

Before you install the Sysgem Management Console you must first ensure that the following are installed:

- The ODBC Manager
- The ODBC Access driver

A warning message is displayed if either the ODBC Manager or ODBC Access driver is not installed (Windows 2000 always installs ODBC and ODBC Access drivers).

You will also need to establish a security key policy (see *Configuration* -> Security Keys as well as *Annex: Security Keys* of this installation guide for more details).

Extras

From the "Install Kits…" AutoPlay screen of your SEM CD you can also select an "Install Windows Extras…” menu. It allows you to install the following software components that are required to run SEM, and that are usually already present on most systems:

- Adobe Acrobat
- Depends (Dependency Walker)
- HTML Help
- NT 4.0 Service Pack 3
- ODBC
- Winzip

If your system does not already have these items, select them and they will be loaded for you.

Installing on Windows 2000/NT

Log in with local administrator privilege

Install the ODBC Manager and Access Driver (if not already installed).

You can then install the SEM Windows 2000/NT kit.

SEM Windows 2000/NT Kit

If you are installing from the SEM CD, select "Install Kits…" from the main AutoPlay menu screen and then select “Install Windows 2000/NT Software”. The install shield will appear and take you through the installation.

If you are installing from an Internet download, you will go straight to the install shield screen.

You will need a password from Sysgem AG to unpack the kit. Check with Sysgem’s Online Support (via the Sysgem web site) for the password to the current version.

The installation steps are:

Step / Window	Description
Welcome	Displays a dialog box that welcomes the end user.
Software License Agreement	Displays a dialog box containing a license agreement. You can scroll up and down to read the agreement, then must choose either the Yes, No, or Back button. If you select Yes, Setup will continue. If you select No, Setup will display the Exit Setup dialog.
Readme	A short information text.
User Information	Displays a dialog box that retrieves the user name and company name. Setup obtains the user name and company name from the registry. The Next button becomes enabled only when data exists in both edit fields. If Setup can locate default name and company values from the system, the Next button is automatically enabled.

Choose Destination Location	Displays a dialog box that allows you to select an alternate destination path. When you click the Browse button in that dialog box, the Choose Folder window is called to open a second dialog box that enables you to either select an existing folder or to enter a new folder name. If you enter the name of a folder that does not exist, a message box is displayed asking whether to create a folder with that name. If you select yes, the specified directory is created. If the default folder does not already exist on your system, it will not be created unless you press the Browse button and follow the steps to create it from the Choose Folder dialog box.
Select Components	Displays a dialog box containing a list of components in the current media that you can install. The components are: SEM Client - This is the user interface (client) that you install on a Windows 2000/NT workstation. SEM Authorization Server - The authorization server is installed on a central Windows 2000/NT system, it manages user logins and settings. SEM Windows Server - The Windows 2000/NT server, installed on the systems you will be managing with SEM. SEM Installation Guide - The installation guide that contains all the information you need for a successful installation of SEM. You will need the Adobe Acrobat Reader from www.adobe.com to read this file. VNC Remote Desktop Server - The VNC desktop server for Windows 2000/NT, requires the VNC viewer (installed with the SEM User Interface). This provides remote desktop management within SEM.
Select Program Folder	Displays Start menu program folders for selection. The default folder is SYSGEM. You can also enter a new folder name.
Start Copying Files	As summary of the selections you have made is displayed before the files are copied to their final destination. When you press Next: Any SEM services that you have selected are stopped. Setup transfers files associated with selected components in the kit to the destination folder. If errors occur it is usually because a file cannot be overwritten because it is locked by an SEM component such as the client (error -623). Make sure that you have closed all SEM windows and that nobody is accessing you current SEM installation from another computer over your network.

Post-Installation Configuration: TCP/IP Port Numbers	The SEM Authorization Server and SEM Windows Server require a port number. The default values are usually acceptable, but if you need to change these values then do so in this window. The defaults are 7250 for the SEM Authorization Server and 7251 for the SEM Windows Server. You are only prompted for port numbers for components that you have selected. You cannot use the same port number for the SEM Authorization Server and SEM Windows Server.
Post-Installation Configuration: Security Keys	The SEM components use a Security Key to protect the system from unauthorized components being introduced into the network.
Setup Complete	This is the final dialog box. If you have installed the SEM Client then you are given the option of starting the SEM Client. The default username is System and the password is Sysgem. When you use this combination you are prompted to change the password, as the initial System account is fully privileged.

Files Installed

The location of files stored on the Windows 2000/NT is selected during installation. By default, a SEM root directory is created as follows:

\Program Files\SYSGEM\

In this directory a number of sub-directories are created:

Directory	Description
SEM Authorization Server	This directory only exists on the machines where the SEM Authorization server has been installed. A number of other sub-directories are created within it. There is one sub-directory created for every SEM user who has logged into SEM by connecting to this Authorization Server. (It is created when the SEM user first logs into SEM – not when the SEM account is first created).There is a sub-directory for every module imported into SEM.
SEM Perl	All SEM scripts running on the Windows 2000/NT platform use the Perl interpreter installed under this directory.
SEM Server	This directory only exists on the machines where the SEM Server has been installed. It contains the Windows 2000/NT Agent executable image and any file on which that program depends.
SEM User Interface	This directory only exists on the machines where the SEM Management Console has been installed. It contains the Windows 2000/NT Agent executable image and any specific file on which that program depends.

SEM Utilities	Used to store miscellaneous executable images used in SEM scripts, for such actions as synchronizing the Windows 2000/NT user accounts from PDCs to BDCs after accounts have been updated, or for setting shares on files and folders.

Configuration Files

You will normally never change any of the values in the configuration files.

Management Console

The Management Console uses the configuration file configuration.cfg (located in the same directory as the executable) to control various aspects of the operation. With the configuration file you can set the tokens shown as follows:

Token	Value
#RESELLER	This gives information shown on the login screen and SEM desktop background.
#URL	The home page of the reseller. Also shown on the login screen and SEM desktop background.
#SUPPORT	Who to contact for technical support. Also shown on the login screen and SEM desktop background.
#PRODUCT	The formal product name
#SWISSFLAG	Whether the Swiss flag should be shown on the logon screen. The parameter values are either YES or NO.
#BITMAP	A refernce to a file containing the logo shown on the login screen, desktop background and various other places. By default the Sysgem logo is used in the file: Configuration.bmp.

Authorization Server

The Authorization Server uses the configuration file SEM AuthServer.cfg (located in the same directory as the executable) to control various aspects of the operation.

You do not normally need to view this file. You modify it only when you want to change the default settings for this component.

With the configuration file you can set any of the tokens shown as follows:

Token	Value
APPEND	If TRUE then the logfile entries are appended to SEM Authorization Logfile.txt. If FALSE then a new logfile is created each time the server is started (so long as LOGFILE is TRUE).
CONSOLE	If TRUE then lines written to the logfile are also written to the console (if running in an) MS-DOS window. Recommendation:

	FALSE.
DEBUG	Determines how much information is written to the logfile / console. The value must be in the range 0 to 9. Recommendation: 0.
LOGFILE	If FALSE then a logfile is not created. The recommendation is to set this TRUE.
PORT	The TCP/IP port used by the server to listen for connection requests. The default is 7250.

Agent for Windows 2000/NT

The Agent for Windows 2000/NT uses the configuration file SEM Server.cfg (located in the same directory as the executable) to control the operation.

You do not normally need to view this file. You modify it only when you want to change the default settings for this component.

With the configuration file you can set any of the tokens shown as follows:

Token	Value
APPEND	If TRUE then the logfile entries are appended to SEM Server Logfile.txt. If FALSE then a new logfile is created each time the server is started (so long as LOGFILE is TRUE).
CONSOLE	If TRUE then lines written to the logfile are also written to the console if running in an MS-DOS window. Recommendation: FALSE.
DEBUG	Determines how much information is written to the logfile / console. The value must be in the range 0 to 9. Recommendation: 0.
LOGFILE	If FALSE then a logfile is not created. The recommendation is to set this TRUE.
PORT	The TCP/IP port used by the server to listen for connection requests. The default is 7251.
TIMEOUT	The number of seconds to allow scripts to run before returning control to the client. The default in 10 minutes.

De-installation

If for any reason you need to de-install SEM, the InstallShield makes this a simple procedure. Select de-install from the control panel.

This process will not remove any new files generated by SEM. They should be manually deleted along with the SYSGEM directory after de-installation.

AS400

Installing on AS400

Installing

Sign on to the AS/400 as User=QSECOFR

If command entry is not displayed, then type and enter CALL QCMD - the command entry screen is displayed.

Check that system value QALWOBJRST is either *ALL or *ALWPGMADP - command DSPSYSVAL QALWOBJRST. If it isn't, then use CHGSYSVAL command to change the setting of QALWOBJRST to *ALL for the duration of the restore operation – record current setting of the QALWOBJRST system value first!

Create a Save File in a library (if you wish, create a library for this first - CRTLIB rstlib) - CRTSAVF rstlib/savf where "savf" is the name of the Save File and "rstlib" is the library it is created in.

Copy installation file into Save File:

- Use FTP on AS/400 to Get the save file from another system on to the AS/400:

  Type FTP other-system-name.

  Ensure options BINARY and NAMEFMT 0 (zero) are set.

  GET xxxxxx rstlib/savf (REPLACE (where xxxxxx is the path/file to download).

  Note: there is no close bracket ")" after "(REPLACE" QUIT.

- Use CPYFRMSTMF to copy the save from either the CD drive or an IFS file.

  Note: Client Access Express can be used, to copy the install file from a folder on a PC to a folder in the Integrated File System of the AS/400.

  CPYFRMSTMF FROMSTMF('/QOPT/../xxxxx') TOMBR('/QSYS.LIB/rstlib.LIB/savf.FILE') BROPT(*REPLACE)

  Note: replace "'QOPT/../xxx'" with the folder path/file in the IFS if copying from IFS !

Note: once this step is completed, you can verify the save file by running the following command:

DSPSAVF rstlib/savf

This will display a screen, the upper part of which will look like:

```
                        Display Saved Objects - Save File

Library saved  . . . :   SYSGEM_SEM            Release level  . . .
: V4R2M0
ASP  . . . . . . . . :   1                     Data compressed  . .
: No
Save file  . . . . . :   AS400B1290            Objects displayed  .
: 6
  Library  . . . . . :     SYSGEM_SAV          Objects saved  . . .
: 38
Records  . . . . . . :   6224                  Access paths . . . .
: 0
Save command . . . . :   SAVLIB
Save active  . . . . :   *NO
Save date/time . . . :   10/08/01   17:16:08

:::::::::::: :::::::::::: :::::::::::::: :::::::::::::
```

Notice the number of objects saved is: 38.

If installing for the first time, choose a *new* library name into which you will install and run SEM. If reinstalling then you should choose the current run library.

This library is referred to subsequently as {semlib}.

If reinstalling then:

- End the current Agent (if running) - ENDSBS semsbsd *IMMED (where semsbsd is the active SEM subsystem).
- Clear the SEM output queue - CLROUTQ semlib/SEMOUTQ (where semlib is the current SEM library).
- Clear the SEM library - CLRLIB semlib.

Restore the software to your chosen {semlib}

RSTLIB SAVLIB(SYSGEM_SEM) DEV(*SAVF) SAVF(library/savf) RSTLIB(semlib) where: "library/savf" is the save file (created in library "library" above) and "semlib" is your chosen software install library.

The message "38 objects restored from SYSGEM_SEM to {semlib}." indicates a successful restore to the library {semlib}.

Determine whether or not System Reply List will need updating. The SEM Agent needs a system reply list entry for message id. CPA3311: this will ensure that this message will be replied to automatically with the correct answer.

Run command WRKRPYLE: a screen like the following should be displayed:

```
                       Work with System Reply List Entries

System:
AS400
 Type options, press Enter.
   2=Change   4=Delete

      Sequence  Message
Compare
 Opt   Number   ID       Reply       Compare Value
Start
  _       10    CPA0700  D           *NONE
  _       20    RPG0000  D           *NONE
  _       30    CBE0000  D           *NONE
  _       40    PLI0000  D           *NONE
  _     1001    CPA3311  G           *NONE
```

Check for an entry for Message ID = CPA3311.

If this entry exists:

- Enter a 0 (zero) for the field "SYSRPYLE No. for CPA3311:" in the SEMINS program in the next step.
- If the reply value is not "G", then change it to "G" using option 2=Change against it in the work display shown.

If this entry does not exist:

- If sequence number 1001 is not in use (for another Message ID), then accept default for field "SYSRPYLE No. for CPA3311:", otherwise
- identify a sequence number currently not in use, and use that as the value for the field "SYSRPYLE No. for CPA3311@".

Press F3 to exit the WRKRPYLE work display and return to command entry screen

Configure the software

CHGCURLIB semlib

CALL SEMINS

Complete the screen presented, refer to online help text and the information in the Installing section..

Note: *POST* install configuration can be carried out as above, but with the final command being {CALL SEMCFG}, (instead of {CALL SEMINS}).

Note: the current build number of the installed SEM software can be determined by running the following command:

DSPDTAARA semlib/SEMBLDNBR

OpenVMS Agent

Installing on OpenVMS

The OpenVMS agent is installed using VMSINSTAL. The saveset containing the agents for both Alpha and VAX is VMSSVR021.A.

The saveset is saved as a zip file. You must unzip this file on an OpenVMS system to restore the original file attributes of the saveset.

If you do not have "Unzip" on OpenVMS, a copy of the Alpha and VAX unzip programs can be found under the "Extras" folder on the CD, or downloaded from the Sysgem website Download zone. Copy the appropriate one of these programs to your system, and define a "Foreign Command" to run the unzip program, e.g. after copying the file UNZIPAXP.EXE to SYS$MANAGER on an Alpha-VMS system, and the VMS_AGENT_021_A.ZIP zip archive file to a temporary directory, enter the following

```
$  UNZIP :== $SYS$MANAGER:UNZIPAXP.EXE
$  UNZIP  VMS_AGENT_021_A.ZIP
```

If you have received the saveset inside a zip file, then you must either unzip this file on an OpenVMS system to restore the original file attributes of the saveset, or invoke the command file ATTRIBUTES.COM.

The default OpenVMS agent port is 7251.

To override the default define the logical SEM-SERVER-PORT-NO before starting the agent.

To set the OpenVMS port to 7000 enter:

```
$ define SEM-SERVER-PORT-NO 7000
```

Example Installation

To install SEM, Log in the System account and type the following:

```
$ @sys$update:vmsinstal VMSAGENT021 products:[Sysgem.kits]
```

An OpenVMS v 7.3 installation logfile is shown below.

```
$ @sys$update:vmsinstal vmsagent021 products:[kits] options i


        OpenVMS AXP Software Product Installation Procedure V7.3


It is 3-FEB-2006 at 12:18.

Enter a question mark (?) at any time for help.

%VMSINSTAL-W-ACTIVE, The following processes are still active:
       TCPIP$FTP_1


The following products will be processed:

  VMSAGENT V2.1


        Beginning installation of VMSAGENT V2.1 at 12:18

%VMSINSTAL-I-RESTORE, Restoring product save set A ...

        ************************************
        *                                  *
        *    Installing agent for ALPHA    *
        *                                  *
        ************************************


  ************************************************************
  *                                                          *
  *  A directory will be created to store the agent files.  *
  *                                                          *
  ************************************************************

  -> If you are installing on a cluster then the directory
     must be created on a disk which is mounted cluster-wide.

  -> If you change this directory after you have installed this
     product you must also update:

       *  SYS$STARTUP:SEM-AGENT-STARTUP.COM

  -> See the User Guide for more information.

* Enter the device and directory [SYS$SYSROOT:[SYSGEM-SEM-AGENT]]:
%VMSINSTAL-I-SYSDIR, This product creates system disk directory
SYS$SYSROOT:[SYSGEM-SEM-AGENT].
%CREATE-I-EXISTS, SYS$SYSROOT:[SYSGEM-SEM-AGENT] already exists

    Installed Files
    ===============

    SEM-AGENT-AXP.EXE         will be created in
SYS$SYSROOT:[SYSGEM-SEM-AGENT]
    SSM-ACCESS-AXP.EXE        will be created in
SYS$SYSROOT:[SYSGEM-SEM-AGENT]
    SSM-ACCOUNTS-AXP.EXE      will be created in
SYS$SYSROOT:[SYSGEM-SEM-AGENT]
    SSM-AUDIT-EVENT-AXP.EXE   will be created in
SYS$SYSROOT:[SYSGEM-SEM-AGENT]
    SSM-AUDIT-TRAIL-AXP.EXE   will be created in
SYS$SYSROOT:[SYSGEM-SEM-AGENT]
    SSM-BLOWFISH-AXP.EXE      will be created in
SYS$SYSROOT:[SYSGEM-SEM-AGENT]
    SSM-PERF-INFO-AXP.EXE     will be created in
SYS$SYSROOT:[SYSGEM-SEM-AGENT]
    SSM-PROCESSES-AXP.EXE     will be created in
SYS$SYSROOT:[SYSGEM-SEM-AGENT]
    SSM-QUEUES-AXP.EXE        will be created in
SYS$SYSROOT:[SYSGEM-SEM-AGENT]
    SSM-SECURITY-AXP.EXE      will be created in
SYS$SYSROOT:[SYSGEM-SEM-AGENT]
```

```
    SSM-BLOWFISH-VAX.EXE      will be created in
SYS$SYSROOT:[SYSGEM-SEM-AGENT]
    SEM-AGENT-STARTUP.COM     will be created in SYS$STARTUP
    SEM-START-AGENT.COM       will be created in
SYS$SYSROOT:[SYSGEM-SEM-AGENT]
    SEM-STOP-AGENT.COM        will be created in
SYS$SYSROOT:[SYSGEM-SEM-AGENT]
    SEM-DEINSTALL.COM         will be created in
SYS$SYSROOT:[SYSGEM-SEM-AGENT]


  ***********************************************
  *                                             *
  *  SECURITY - Installation Key - SECURITY.    *
  *                                             *
  ***********************************************

  This product uses a powerful security model to
  guard against attack.

  If this is the first time that you have installed
  this agent on this host then you MUST enter a key.

  Starting with version 2.1 of Sysgem Enterprise Manager,
  keys can take two forms:

      [1] standard security keys - free format text
          strings (case sensitive) which are unique
          for your network and MUST be the same
          as that entered for other software components
          of this product on your network, and
      [2] an installation key - used by the agent to
          retrieve domain keys from the Authorization Server.

  For more information please read the user guide.

  Key configuration:

      [1] Standard security key
      [2] Installation key

      [9] Skip key configuration

* Please select a key type from the list above [1]: 1
* Enter the security key: FortKnox

    Installing Security Key...

Sysgem SEM Agent v2.1 build 2919
Copyright (c) 2002 by SYSGEM AG.

Initializing logfile
--------------------
Filename ...: ARNOLD$DKA100:[SYS0.][SYSGEM-SEM-AGENT.1-88]SysGem-
Agent-Logfile-Feb-06.txt;1
Status .....: %RMS-S-NORMAL, normal successful completion

Cluster nodename .....: ARNOLD
DECNET address .......: 1.88
OpenVMS version ......: V7.3
Hardware type ........: AlphaServer 1000A 5/400
Active CPUs ..........: 1
Username .............: SYSTEM
Process name .........: SYSTEM
Process id ...........: 000000B1
Base priority ........: 4
Working set extent ...: 65536
Paging file quota ....: 500000
Software version .....: Sysgem SEM Agent v2.1 build 2919
SCSA compliant .......: Yes
Build date ...........: Jan 25 2006 at 16:49:20

Installing SCSA Security Key
----------------------------
Index ......: 0
Value ......: FortKnox
```

```
Filename ...: ARNOLD$DKA100:[SYS0.][SYSGEM-SEM-AGENT.1-
88]security_key_0.arc;1
Status .....: OK


  The selected agent startup command files will be
  added to the SYSMAN startup database.

  Enter YES to add this file (recommended):
  $ MCR SYSMAN STARTUP ADD FILE SEM-AGENT-STARTUP.COM  /PHASE=END

  Enter NO to remove this file (if registered):
  $ MCR SYSMAN STARTUP REMOVE FILE SEM-AGENT-STARTUP.COM
/PHASE=END

* Enter YES or NO [YES]?
* Start the agent now ? [YES]?
!=================================================================
===========
!
!    Agent startup file
!    ------------------
!
!    Copyright (c) 1998-2000 SYSGEM AG.
!
!
!    P1 - port number
!
!    You can also override the default port numbers by defining a
logical name
!    before calling this file.
!
!        Logical name: SEM-AGENT-PORT-NO
!
!    Example: $ define /system SEM-AGENT-PORT-NO 7000
!
!=================================================================
===========

EXECUTABLE ...: SYS$SYSROOT:[SYSGEM-SEM-AGENT]SEM-AGENT-AXP.EXE

Current Process (will be stopped)
=================================

 3-FEB-2006 12:22:37.76   User: SYSTEM           Process ID:
00000096
                          Node: ARNOLD           Process name:
"SEM-AGENT-AXP"

Terminal:
User Identifier:    [SYSTEM]
Base priority:      5
Default file spec:  Not available
Number of Kthreads: 1

Devices allocated:  BG13:
                    BG14:

Soft CPU Affinity: off
Start New Process
=================
%RUN-S-PROC_ID, identification of created process is 000000C2

        ********************************************
        *                                          *
        *    Installation successfully completed   *
        *                                          *
        ********************************************


        Installation of VMSAGENT V2.1 completed at 12:22

    Adding history entry in VMI$ROOT:[SYSUPD]VMSINSTAL.HISTORY

    Creating installation data file:
VMI$ROOT:[SYSUPD]VMSAGENT021.VMI_DATA
```

```
VMSINSTAL procedure done at 12:23
```

Files Installed

SYS$STARTUP:

File	Description
SEM-AGENT-STARTUP.COM	Invokes the start-up file SEM-AGENT-AXP.COM located in the SEM Agent work directory.

SYS$SYSROOT:[SYSGEM-SEM-AGENT]:

File	Description
nn.nn.DIR	A subdirectory is created in the SEM root directory to provide a machine specific area into which temporary work files will be stored, or files that need to be machine specific for any reason, in a clustered OpenVMS environment. “nn.nn” is the DECnet executor node (area and number), and is system specific.
SEM-AGENT-AXP.COM	A command file to start the agent process (as a detached OpenVMS process).
SEM-AGENT-AXP.EXE	The SEM agent executable image.
SEM-AGENT-AXP.LIS	This gives a log file of the current Agent session. It begins a log of the start-up command file, giving information such as TCP/IP port in use, which security keys have been defined, TCP/IP address, etc.
SEM-DEINSTALL.COM	A command file for removing SEM from the system.
SEM-START-AGENT.COM SEM-STOP-AGENT.COM	Command files that may be used to manually stop and restart the agent process.
SSM-ACCESS-AXP.EXE SSM-ACCOUNTS-AXP.EXE SSM-PERF-INFO-AXP.EXE SSM-PROCESSES-AXP.EXE SSM-QUEUES-AXP.EXE SSM-SECURITY-AXP.EXE	SEM executable images to return data such as file access, user accounts, Audit Journal, performance, OpenVMS processes, queues, security. These images will be invoked from script files transmitted from the SEM client and will return data for display into the SEM display windows.
SSM-AUDIT-EVENT-AXP.EXE SSM-AUDIT-TRAIL-AXP.EXE	SEM executable images used for recording information into and extracting information from the OpenVMS audit journal files. This information gives details of the SEM user when transaction are conducted on this OpenVMS machine at the request of the SEM user logged into

	the SEM Management Console workstation.

(The default SYS$SYSROOT:[SYSGEM-SEM-AGENT] can be changed during installation).

UNIX/Linux Agents

Introduction

Sysgem provide a common installation procedure for all UNIX/Linux platforms supported by Sysgem Enterprise Manager.

First, to install the SEM Agent on Unix/Linux systems, you need to be logged into a privileged account, such as root.

You will then need to decompress the tar archive containing the installation kit. We suggest that a special directory is created for this purpose.

Invoke the installation procedure by running the "setup" program unpacked from the above tar file.

```
#./setup
```

The installation procedure prompts for the following information:

- The location to install the agent, is by default the following: /opt/Sysgem/SEM.
- The TCP/IP port number. By default this will be 7251. It should only need to be changed if 7251 clashes with one already in use.
- A security key or installation key. See Security Key for more information.
- Whether to start the Agent automatically on reboot.
- Whether to start the Agent auomatically on completion of the installation.

An example is given below showing a typical installion on a Sun Solaris machine.

To re-install the kit, perhaps as an upgrade for a later version, simply re-run the above procedure. There is no need to stop any daemons as these will be stopped and restarted automatically during the installation.

If you have any suggestions for improving the UNIX installation of Sysgem Enterprise Manager please contact our Online Support via http://www.Sysgem.com - your input is valuable.

Example

The following example shows the installation on Sun Solaris, having first unpacked the tar archive into a directory /kits/SEM_kit.

```
# ./setup
SEM Agent for UNIX
------------------

[8] Platform is SunOS
[7] Data file is _kit.6
[6] Creating /kits/SEM_kit/tmp
[5] Copying _kit.6 to /kits/SEM_kit/tmp
[4] Changing to /kits/SEM_kit/tmp
[3] Unpacking _kit.6
[2] Removing temporary files
[1] Launching SEMInstaller

Sysgem SEM Agent UNIX Installer

  Agent ......: Sysgem SEM Agent v2.1 build 2918
  Target .....: SunOS
  Hostname ...: rose
  Processor ..: sun4m

Step 1/6 - Checking Inventory

  Unpacking _data.0...

Step 2/6 - Directory

  Enter the directory where the agent is to be installed.
  The recommended default is /opt/Sysgem/SEM

Enter the directory [/opt/Sysgem/SEM]

Step 3/6 - Port Number

  Enter the TCP/IP port number. The default is 7251.

Enter the port number [7251]

Step 4/6 - Security Key

  This product uses a powerful security model to guard against
attack.

  As part of the installation you MUST enter a security key.

  ***********************************************
  *                                             *
  *  SECURITY - Installation Key - SECURITY.    *
  *                                             *
  ***********************************************

  This product uses a powerful security model to
  guard against attack.

  If this is the first time that you have installed
  this agent on this host then you MUST enter a key.

  Starting with version 2.1 of Sysgem Enterprise Manager,
  keys can take two forms:

      [1] standard security keys - free format text
          strings (case sensitive) which are unique
          for your network and MUST be the same
          as that entered for other software components
          of this product on your network, and
      [2] an installation key - used by the agent to
          retrieve domain keys from the Authorization Server.

  For more information please read the user guide.

Key Configuration:

      [1] Standard security key
      [2] Installation key

      [9] Skip key configuration
```

```
Please select a key type from the above list [1]
Enter the security key [] FortKnox
Confirmation ......... [] FortKnox
Step 5/6 - Autostart

  If you want the agent to start when you boot this system then
enter YES,
  otherwise NO.

  If you select NO then you must start the agent interactively each
time
  you boot this system.

Start the agent when the system boots? [Yes]

Step 6/6 - Start Agent

  If you want to use the agent now then it must be started after
the,
  installation is complete.

  If you do not start the agent now then you must start it by
either rebooting
  the system (if you have selected this option) or by starting it
interactively.

Start the agent after the installation? [Yes]

Confirmation
  Directory ...........: /opt/Sysgem/SEM
  Port number .........: 7251
  Security key ........: ########
  Autostart ...........: Yes
  Start agent .........: Yes

Is this correct? [Yes]

Start the installation now? [Yes]

Stopping Agent
  If the agent is running it will be stopped.
  Agent not found.

Creating Directory: /opt/Sysgem/SEM/library
  /opt... Exists
  /opt/Sysgem... Exists
  /opt/Sysgem/SEM... Exists
  /opt/Sysgem/SEM/library... Exists

Copying Files

Creating Directory: /usr/lib
  /usr... Exists
  /usr/lib... Exists

  SysgemSEMAgent...
  SysgemSEMAgent.cfg... Exists (not overwritten)
  SysgemSEMStart...
  SEMInstaller...
  ssm-accounts...
  ssm-blowfish...
  ssm-commander...
  ssm-perf...
  ssm-syslog...
  AddStartup...
  RemoveStartup...
  init.tcl...
  libstdc++.so.2.10.0... Exists (not overwritten)

Installing Security Key
  Installing SCSA Security Key
  ----------------------------
  Index ....: 0
  Value ....: ########
  File .....: /opt/Sysgem/SEM/Sun_security_key_0.arc
  Status ...: OK
```

```
  SCSA Security Keys
  ------------------
  Key 0 ...: Valid


Updating Autostart Tables
  Removing: /etc/rc3.d/S99Sysgem...
  Removing: /etc/init.d/SysgemSEMStart...
  Copying:  /etc/init.d/SysgemSEMStart...
  Linking:  /etc/rc3.d/S99Sysgem...

Starting The Agent
    PID     USER        TIME COMMAND
    434     root        0:00 /opt/Sysgem/SEM/SysgemSEMAgent

Installation completed.
#
```

The above example from an installation on Solaris is true for all variants of supported UNIX systems except IBM AIX. The Autostart procedures are different for AIX. The "Updating Autostart Tables" section of the AIX installation displays the following:

```
Updating Autostart Tables
  Inittab Entry
  -------------
  Sysgem_sem:2:wait:/opt/Sysgem/SEM/SysgemSEMStart
```

Files Installed

Root Directory

Platform	Directory
AIX	/opt/Sysgem/SEM
COMPAQ (Digital)	/opt/Sysgem/SEM
HP	/opt/Sysgem/SEM
LINUX Intel	/opt/Sysgem/SEM
SUN Solaris	/opt/Sysgem/SEM

Agent Files

File	Description
AddStartup	Adds the agent to the system's initialization tables.
RemoveStartup	Removes the agent from the system's initialization tables.
Sysgem-Agent-Logfile-Oct-00.txt	The agent logfile for October 2000.
SysgemSEMAgent	The agent executable image.
SysgemSEMAgent.cfg	The configuration file, contains entries which overwrites the default settings: Port number - the default is 7251. Debug level - the default is 0. Temporary directory for script files - the default is Sysgem_Script_<machine name>

SysgemSEMStart	The startup script that is invoked as part of the system initialization.
library/init.tcl	Required by ssm-commander (below).
ssm-accounts	A support module that lists the contents of the password and group files.
ssm-commander	A support module used to run UNIX commands that prompt the user for input.
ssm-perf	A support module that returns performance information - CPU loading, memory usage and list of processes.
ssm-syslog	A support module which returns entries from the syslog database.

AutoStart

So that the agent starts when the system is booted you must add entries to the initialization tables.

To make life easy, two files are provided in the root directory: AddStartup and RemoveStartup.

AddStartup is platform-dependent, as follows:

Platform	Method
AIX	Adds an entry to /etc/inittab (see inittab(4) for more information). An example of the /etc/inittab entry is shown below: *Sysgem_sem:2:wait:/usr/sbin/SYSGEM/SEM /SysgemSEMStart*
COMPAQ (Digital)	Copies *SysgemSEMStart* from the root directory to */sbin/init.d/SysgemSEMStart*, then creates a symbolic link */sbin/rc3.d/S99Sysgem* to *SysgemSEMStart*.
HP	Copies *SysgemSEMStart* from the root directory to */sbin/init.d/SysgemSEMStart*, then creates a symbolic link */sbin/rc3.d/S99Sysgem* to *SysgemSEMStart*.
LINUX Intel	Copies SysgemSEMStart from the root directory to /etc/init.d/SysgemSEMStart if possible, otherwise to /etc/rc.d/init.d/SysgemSEMStart, then creates a symbolic link /etc/rc.d/rc3.d/S99Sysgem to SysgemSEMStart.
SUN Solaris	Copies *SysgemSEMStart* from the root directory to */etc/init.d/SysgemSEMStart*, then creates a symbolic link */etc/rc3.d/S99Sysgem* to *SysgemSEMStart*.

Stopping The Agent

If the agent needs to be manually stopped:

Show the processes currently running:

Platform	Command
AIX	ps -ae
COMPAQ (Digital)	ps -ae
HP	ps -ae
LINUX Intel	ps x
SUN Solaris	ps -aef

Manually delete the process:

```
# kill <process_id>
```

Example on COMPAQ (Digital) UNIX:

```
 # ps -ae

  PID   TTY      S           TIME CMD
  4884  ttyp1    S        0:00.06
/usr/lbin/SYSGEM/SEM/SysgemSEMAgent
     .
     .
     .
# kill -9 4    884
```

Changing The Security Key

This example uses the installation on HP UNIX. The directory depends on the platform.

To change or add a security key FortKnox, enter:

```
/opt/Sysgem/SEM/SysgemSEMAgent -k FortKnox
```

The following is an example:

```
Falera> su
Password:
# cd /opt/Sysgem/SEM
# ./SysgemSEMAgent -k FortKnox
Sysgem SEM Agent v2.0 build 1124
Copyright (c) 2000 by SYSGEM AG.

Configuration File
------------------
Filename .....: ./SysgemSEMAgent.cfg
Entry ........: ##############################################################
Entry ........: #
Entry ........: #   Updated by System (Simon on WEATHERWAX)
Entry ........: #   Date: Sun Oct 10 12:59:17 WETDST 1999
Entry ........: #
Entry ........: #   Format: Token Value
Entry ........: #
Entry ........: #   Tokens are:
Entry ........: #     Debug level: DEBUG
Entry ........: #     Port no:     PORT_NO
Entry ........: #     Tmp dir:     TMP_DIR
Entry ........: #
Entry ........:
Entry ........: DEBUG 0
Entry ........: PORT_NO 7251
Entry ........: # TMP_DIR /tmp/Sysgem
Entry ........: PORT_NO 7251
Entry ........:
Entry ........: PORT_NO 7251

Installing SCSA Security Key
----------------------------
Index ....: 0
Value ....: FortKnox
File .....: ./Digital_security_key_0.arc
Status ...: OK

SCSA Security Keys
------------------
Key 0 ...: Valid

#
```

Configuration

Overview

The first installation of SEM requires very little configuration. It is intended to be as out-of the-box as is possible. A system can be installed for 'evaluation' simply by performing the installation procedure. It comes pre-configured with accounts and settings to allow you to log in and start using the product immediately.

When the system is deployed for live working, it is usually necessary to create SEM accounts for other users (Administrators and System Managers) with just enough features and privileges for their needs, and to expand the system to manage further multiple remote systems.

It is necessary to consider:

- Licenses
- Security Keys
- SEM Accounts
- Profiles
- Tokens
- Library Mappings
- Agent Definitions
- Templates

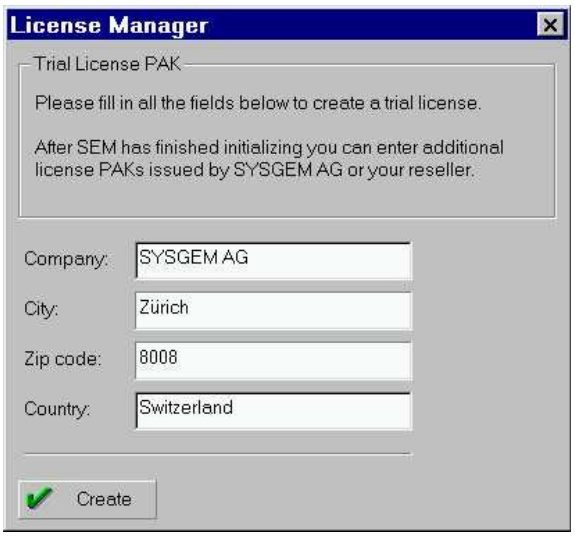
Licenses

Editing an Evaluation License (First-Time Login)

Log into SEM with the pre-installed SEM username and password:

Username:	**Demo**	(pre-configured demonstration environment)
	- or -	
	System	(full access to all features)
Password:	**sysgem**	

You will then be prompted for key fields so that an evaluation license can be created.



You must enter:

- Company Name
- City
- Zip code
- Country

You are now licensed with full functionality for a limited period of 30 days. If you need to extend this evaluation period, contact Sysgem's Online Support (via the Sysgem web site).

Ordering a Permanent SEM License

After the trial period has expired you require a permanent SEM License - a License PAK (Product Authorization Key) - from Sysgem AG.

The evaluation license is filled in by the customer. The contact details in the License PAK have to be identical to the evaluation license for customer specific settings to continue to apply after the License PAK has been installed.

This is because all internal files stored by SEM are security protected using the license as part of a checksum algorithm. Any SEM user account files, security profile files, etc. cannot be modified other than by SEM itself, and by the version of SEM installed on your customer site. Any configuration changes made during the evaluation period can therefore only be subsequently accessed if the License PAK details are the same as the evaluation license.

We therefore request that the customer's evaluation license is returned to Sysgem when ordering a License PAK:

1. Start the License Manager (**Tools -> License Manager**).
2. Select the **Base** pane.
3. Highlight your evaluation license.
4. Select the **Send License via Mail** option and send to support@Sysgem.com.

Importing a Permanent SEM License

Direct

The easiest way is to load the PAK (usually a base or group license) without starting the license manager:

1. Log into SEM and select **File -> Import and Export -> Import License**.
2. Pick the **SEM License PAK YYMMDDNN.txt** file from the **SEM_License** folder of your SEM CD.

License Manager

To load a base PAK:

1. Start the License Manager (**Tools -> License Manager**).
2. Select the **Base** pane.
3. Select the **Load Licenses File** option.
4. Pick the **SEM License PAK YYMMDDNN.txt** file from the **SEM_License** folder of your SEM CD.

To load a group PAK:

1. Start the License Manager (**Tools** -> **License Manager**).
2. Select the **Group** pane.
3. Select the **Load Licenses File** option.
4. Pick the **SEM License PAK YYMMDDNN.txt** file from the **SEM_License** folder of your SEM CD.

Installing Plug-In Application Modules

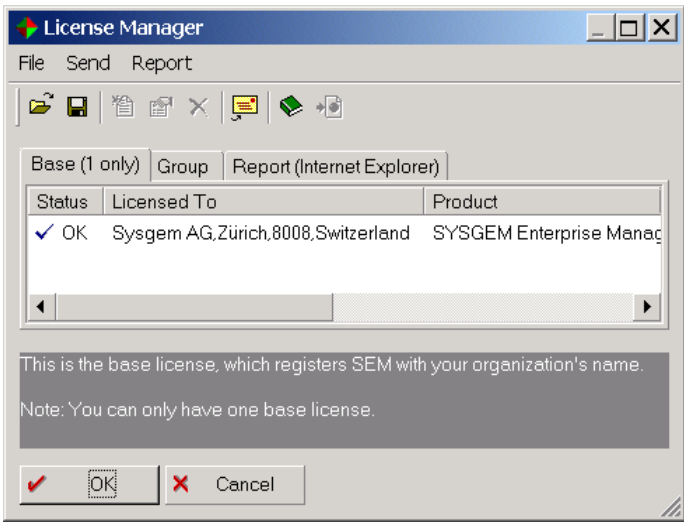
All licensed SEM Plug-In Applications Modules are automatically available after you have installed a valid license.

Installing Application Support Packages

All licensed SEM Application Support Packages are automatically available after you have installed a valid license.

License Manager

Start the License Manager (**Tools** -> **License Manager**).



There are three panes:

1. Base (Mandatory)

   This is a mandatory license. You will only have one base PAK. A Trial license is a base license with a termination date.

2. Group (Optional)

   The group license grants the company name in the base PAK the membership of a group. A company with a developer license can export definitions to any group of which the company is a member.

   For example, if Manchester, Liverpool and Bristol are members of the group Cities, and London has a developer license, then London can create definitions and export (distribute) them to the other members of the Cities group.

   A company can be a member of one or more groups. Each group license grants membership to one or more groups via the #GROUP_NAME token.

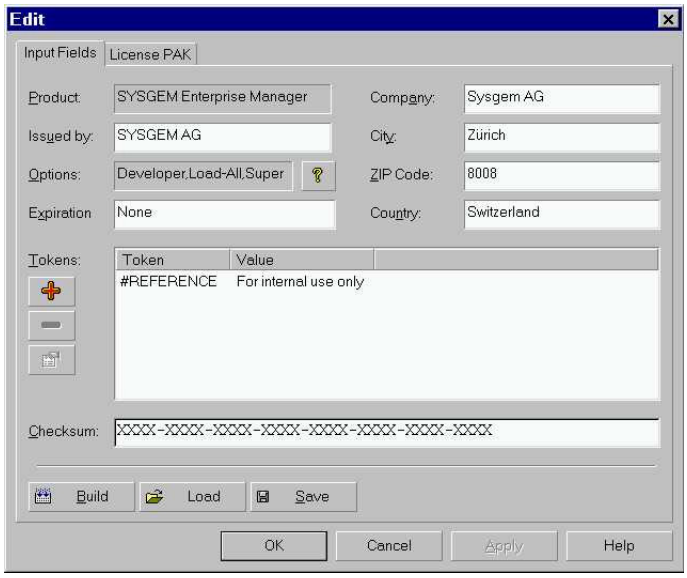
3. Report

   To display the status of your license(s) select the **Report** pane from the License Manager. This gives you a detailed description of your current license PAKs.

   Alternatively you can display the current status of your license by selecting **License Bar** from the **View** menu.

License Editor

Licenses are issued with the License Editor. Normally you will receive an already edited License PAK either electronically or it is provided in the SEM_License folder of the customer specific SEM CDs.



Fields

The License PAK fields are:

Field	Description
Product	The name of the product. For a base product PAK this overrides the title of Sysgem Enterprise Manager.
Issued by	The company issuing the PAK, usually Sysgem AG.
Options	The options enabled by the PAK.
Termination	The termination date of the PAK, this is a valid date (e.g. 01-JAN-2005) or None.
Company, City, Zip Code, Country	The name of the company or organization to which the PAK is issued.
Tokens	Optional tokens.
Checksum	Ensures that the PAK is valid.

Options

The Options are:

Option	Description
Build	When you click **Build** the fields are checked, the checksum validated, and the license PAK is written into the PAK field. Once the PAK has been successfully validated click **OK**.
Load	Click **Load**, select the file to load from the Open window. The PAK is loaded from the file. To validate the PAK click **Build**.
OK	Returns the current PAK to the License Manager.
Save	Click **Save** to save the current PAK to a file.

Security Keys

All SEM components (GUI, Agents, and Authorization Server) must be given a set of compatible Security Keys for the components to be able to work together. If the security keys do not match, then an error message: **Security key mismatch** will be displayed when one component tries to connect to another.

Multiple security keys may be defined for each component. For instance a Management Console (GUI) may have 2 keys (A, and B) and be able to connect to Agent machines that have either key A or B. A second GUI may just have key B, which could only connect to Agents with key B, and would be refused access by those Agents with key A.

A similar situation arises when multiple keys are defined on Agents. A network could be divided into two domains, one with key A and one with key B. An agent that had both keys A and B could be accessed by all Management Consoles with either A or B key, but agents with just one key would only be accessible from GUIs with that key.

Security keys may be set during the installation procedure, but may also be modified thereafter. To set a key in the Management Console, select the menu option :

Tools > Security Key Manager

To set a key on an NT Agent or on the Authorization Server, run the executable with a –kn qualifier followed by the text of the security key.

Setting Security Keys on NT

```
"SEM Server.exe" -k0 FortKnox
```

or

```
"SEM Server.exe" -i auth-svr:installation-key
```

(n in –kn is the numerical index of the required key. There may be up to 10 keys, 0-9. The index value is optional. If absent the key set will be key 0.)

Setting Security Keys on OpenVMS

To set a key on OpenVMS, first define a “foreign command” e.g.…

```
$ sem :== $SYS$SYSROOT:[SYSGEM-SEM-AGENT]SEM-AGENT-AXP.EXE
$ sem -k0 "FortKnox"
  or
$ sem -i auth-svr:installation-key
```

Setting Security Keys on UNIX/Linux

To set a key on a UNIX machine run the agent with the set security key parameter:

```
# ./SysgemSEMAgent -k0 FortKnox
```

or

```
# ./SysgemSEMAgent -i auth-svr:installation-key
```

SEM Accounts

A user has to be given a SEM account and has to log into that account with a username and password to be able to use the product.

SEM is installed with a pre-configured account called **System** that has a pre-set password of **Sysgem**. The System password should be changed during the first log in.

Two pre-configured demonstration accounts, called **Demo** and **Helpdesk**, are also provided in new installations. Both accounts have the password of **Sysgem**, which again should be changed during the first log in. These two accounts can safely be deleted if no demonstration environment is required.

Accounts are defined for other users of SEM using the **Managers > Users > Accounts** menu option. An account is given:

- a username,
- a password (which is case-sensitive)
- a profile (that grants privileges to the user).

Mirrored Accounts

An account can be mirrored to another user. It will then appear to be identical in all respects, including the profile granted, which module libraries have been mapped, preference settings, etc.

When creating a number of similar accounts, it is best to first create a generic account for that type of user. Then log into that account and make sure that the settings and privileges are as are required. Then to create the individual accounts and “Mirror” them to the generic account.

Option Settings

Each SEM user can set their own preference (option) settings by pressing the F8 function key (or by selecting the **Tools > Settings** menu option).

A user that is “Mirrored” to another user may not have the permission to edit their setting options. This control is invoked on the SEM User Account definition windows **(Managers > Users > Accounts).**

Account Passwords

Passwords can (and should) be changed by each SEM user. Passwords are made up of any alphanumeric character and are case sensitive. SEM passwords are stored using a one-way encryption algorithm.

Profiles

SEM has **Access Control Profiles** that control the level of privileges granted to SEM users. SEM ships with some pre-prepared profiles including one called **Full Access. Full Access** is pre-assigned to the **System** account, and allows full access to all SEM functionality. It should only be given to other SEM users with caution.

New profiles can be created and assigned to SEM users. Editing those profiles and checking the appropriate checkboxes controls the level of privileges granted.

A user may be given only one Profile.

Tokens

Access Control Tokens are an extension to the concept of Profiles. Whereas Profiles give privileges for the base SEM functionality – Tokens extend the scope to include privileges and features for individual Application modules. Each Application Module has its own set of Tokens.

Multiple Tokens are set into a Profile by editing the Profile using the **Managers > User > Profiles** menu option. Press the **Set** button (top right of the Profile form) to see a list of all Tokens that may be assigned to that Profile.

Edit Token privilege settings by using the menu option: **Managers> Users> Tokens**.

Library Mappings

Before a SEM user can make use of an application module (such as SAcM Account Manager) the library containing that module has to be mapped to the user. A user can select their own libraries mappings if they have sufficient privileges. Use **Tools > Library Mappings** to select which libraries are mapped to their account.

Libraries can be mapped for other users using **Managers > Users > Mappings.**

Agent Definitions

Define Remote Agents using the menu option: **Managers > Agents> New Agent.** Enter the following information for each remote Agent:

- Title (A name used by the GUI to reference the Agent)
- Address (either the I/P address or the name resolved by DNS)
- Port (Normally 7251)
- Description (A free format optional field)

It is good practice for a single SEM account (or a small number of SEM accounts) to define Agents and then to use that account to mirror the definitions from all other SEM user accounts. In this way, better control over Agent definitions can be maintained.

Archive

The SEM Archive is used for a number of archiving purposes. If a Custom Display Definition is modified, then the previous version is automatically stored in the SEM Archive. Historical items can be selected in the archive and restored if required.

The Archive database can record the results of each transaction from a Customer Display. Since some Applications (e.g. SAcM) have their own specific Audit Trail archiving, it is desirable (from a performance point of view) to suppress SEM archiving in favor of the Application Audit Trail archive.

The archiving of Custom Display transaction results can be switched off. Deselect the **Archive Script** icon from the top of the form. To ensure all archiving for all Display scripts is turned off, use the menu option: **Tools > System > Performance.**

Templates

Custom Display Forms such as **SAcM Account Manager > Enterprise Accounts > Create (Multi-Platform)** can have the content of fields saved into **Templates** and subsequently restored by selecting the appropriate template. This saves keying time and increases the consistency of data for frequently used entries in fields.

Templates are held in two locations. One is private to each user; the other is system wide and available to all users.

Use the following options to load or save template values into / from a form:

- Save to Template
- Load From Template

(See icons at the top left of an input form such as SAcM Account Manager> Enterprise Accounts > Create (Multi-Platform)).

A form can be pre-loaded with the content of a default template by using the following option:

- Template Options

The content of existing templates may be edited using the template editor. See Managers > Templates.

Problem Solving

Communications

Problem	Resolution
Connection refused	Check that the server is listening on the port you are trying to connect to. This error is usually returned when there is no program listening to the specific port.
Connection timed out	Check that the address you are using is valid - this error is usually returned when you try to connect to a system using an unreachable address.
No route to host	Check that TCP/IP is installed and running - select Network from the Control Panel. Use PING to make sure that IP is configured correctly.

For a full list of possible Windows Sockets errors see “Sockets Errors”.

PERL

Problem	Resolution
The SYSGEM PERL modules are out of date, or do not correspond to those originally installed.	The modules are always reinstalled when you install the SEM Windows 2000/NT kit. Check that you have the latest version of this kit.

Security Key

Problem	Resolution
The message “No Security Keys Defined” or “Security Key Mismatch” is displayed.	Check that the keys are installed correctly - keys are case-sensitive. If you have installed a new hardware adapter (or even just installed the driver software that enables the adapter) then you must re-enter the security keys, as the hardware address(es) is (are) used as part of the encryption algorithm. See “Security Keys” for more information.

Common Socket Errors

Problem	Resolution
Connection refused	The target system could be contacted, but there is no server listening on the port. The most probable cause of this error: 1. Server not started. 2. Wrong port number in the server definition.
Connection timed out	The target system could not be contacted - check the address specified in the server definition.

Full List of Socket Errors

The following is the latest list of all possible error codes returned by the Microsoft Sockets calls, along with their extended explanations. This information is ©1996-1998 Microsoft Corporation:

Error text	Description
Address already in use.	Only one usage of each socket address (protocol/IP address/port) is normally permitted. This error occurs if an application attempts to bind a socket to an IP address/port that has already been used for an existing socket, or a socket that wasn't closed properly, or one that is still in the process of closing. For server applications that need to bind multiple sockets to the same port number, consider using setsockopt (SO_REUSEADDR). Client applications usually need not call bind at all - connect will choose an unused port automatically. When bind is called with a wild-card address (involving ADDR_ANY), a WSAEADDRINUSE error could be delayed until the specific address is "committed." This could happen with a call to other function later, including connect, listen, WSAConnect or WSAJoinLeaf.
Address family not supported by protocol family.	An address incompatible with the requested protocol was used. All sockets are created with an associated "address family" (i.e. AF_INET for Internet Protocols) and a generic protocol type (i.e. SOCK_STREAM). This error will be returned if an incorrect protocol is explicitly requested in the socket call, or if an address of the wrong family is used for a socket, e.g. in sendto.

Bad address.	The system detected an invalid pointer address in attempting to use a pointer argument of a call. This error occurs if an application passes an invalid pointer value, or if the length of the buffer is too small. For instance, if the length of an argument which is a struct sockaddr is smaller than sizeof(struct sockaddr).
Bad protocol option.	An unknown, invalid or unsupported option or level was specified in a getsockopt or setsockopt call.
Cannot assign requested address.	The requested address is not valid in its context. Normally results from an attempt to bind to an address that is not valid for the local machine. This can also result from connect, sendto, WSAConnect, WSAJoinLeaf, or WSASendTo when the remote address or port is not valid for a remote machine (e.g. address or port 0).
Cannot send after socket shutdown.	A request to send or receive data was disallowed because the socket had already been shut down in that direction with a previous shutdown call. By calling shutdown a partial close of a socket is requested, which is a signal that sending or receiving or both has been discontinued.
Class type not found.	The specified class was not found.
Connection refused.	No connection could be made because the target machine actively refused it. This usually results from trying to connect to a service that is inactive on the foreign host - i.e. one with no server application running.
Connection reset by peer.	The remote host forcibly closed an existing connection. This normally results if the peer application on the remote host is suddenly stopped, the host is rebooted, or the remote host used a "hard close" (see setsockopt for more information on the SO_LINGER option on the remote socket.) This error may also result if a connection was broken due to "keep-alive" activity detecting a failure while one or more operations are in progress. Operations that were in progress fail with WSAENETRESET. Subsequent operations fail with WSAECONNRESET.
Connection timed out.	A connection attempt failed because the connected party did not properly respond after a period of time, or established connection failed because connected host has failed to respond.
Destination address required.	A required address was omitted from an operation on a socket. For example, this error will be returned if sendto is called with the remote address of ADDR_ANY.
Graceful shutdown in progress.	Returned by WSARecv and WSARecvFrom to indicate the remote party has initiated a graceful shutdown sequence.

Host is down.	A socket operation failed because the destination host was down. A socket operation encountered a dead host. Networking activity on the local host has not been initiated. These conditions are more likely to be indicated by the error WSAETIMEDOUT.
Host not found.	No such host is known. The name is not an official hostname or alias, or it cannot be found in the database(s) being queried. This error may also be returned for protocol and service queries, and means the specified name could not be found in the relevant database.
Insufficient memory available.	An application used a Windows Sockets function that directly maps to a Win32 function. The Win32 function is indicating a lack of required memory resources.
Interrupted function call.	A blocking operation was interrupted by a call to WSACancelBlockingCall.
Invalid argument.	Some invalid argument was supplied (for example, specifying an invalid level to the setsockopt function). In some instances, it also refers to the current state of the socket - for instance, calling accept on a socket that is not listening.
Invalid procedure table from service provider.	A service provider returned a bogus proc table to WS2_32.DLL. (Usually caused by one or more of the function pointers being NULL.)
Invalid service provider version number.	A service provider returned a version number other than 2.0.
Message too long.	A message sent on a datagram socket was larger than the internal message buffer or some other network limit, or the buffer used to receive a datagram into was smaller than the datagram itself.
Network dropped connection on reset.	The connection has been broken due to "keep-alive" activity detecting a failure while the operation was in progress. It can also be returned by setsockopt if an attempt is made to set SO_KEEPALIVE on a connection that has already failed.
Network is down.	A socket operation encountered a dead network. This could indicate a serious failure of the network system (i.e. the protocol stack that the WinSock DLL runs over), the network interface, or the local network itself.
Network is unreachable.	A socket operation was attempted to an unreachable network. This usually means the local software knows no route to reach the remote host.

Network subsystem is unavailable.	WSAStartup returns this error if the Windows Sockets implementation cannot function at this time because the underlying system it uses to provide network services is currently unavailable. Users should check: (1) That the appropriate Windows Sockets DLL file is in the current path, (2) That they are not trying to use more than one Windows Sockets implementation simultaneously. If there is more than one WINSOCK DLL on your system, be sure the first one in the path is appropriate for the network subsystem currently loaded. (3) The Windows Sockets implementation documentation to be sure all necessary components are currently installed and configured correctly.
No buffer space available.	An operation on a socket could not be performed because the system lacked sufficient buffer space or because a queue was full.
No route to host.	A socket operation was attempted to an unreachable host. See WSAENETUNREACH
Non-authoritative host not found.	This is usually a temporary error during hostname resolution and means that the local server did not receive a response from an authoritative server. A retry at some time later may be successful.
One or more parameters are invalid.	An application used a Windows Sockets function, which directly maps to a Win32 function. The Win32 function is indicating a problem with one or more parameters.
Operation already in progress.	An operation was attempted on a non-blocking socket that already had an operation in progress - i.e. calling connect a second time on a non-blocking socket that is already connecting, or canceling an asynchronous request (WSAAsyncGetXbyY) that has already been canceled or completed.
Operation not supported.	The attempted operation is not supported for the type of object referenced. Usually this occurs when a socket descriptor to a socket that cannot support this operation, for example, trying to accept a connection on a datagram socket.
Operation now in progress.	A blocking operation is currently executing. Windows Sockets only allows a single blocking operation to be outstanding per task (or thread), and if any other function call is made (whether or not it references that or any other socket) the function fails with the WSAEINPROGRESS error.
Overlapped I/O event object not in signaled state.	The application has tried to determine the status of an overlapped operation which is not yet completed. Applications that use WSAGetOverlappedResult (with the fWait flag set to false) in a polling mode to determine when an overlapped operation has completed will get this error code until the operation is complete.

Overlapped operation aborted.	An overlapped operation was canceled due to the closure of the socket, or the execution of the SIO_FLUSH command in WSAIoctl.
Overlapped operations will complete later.	The application has initiated an overlapped operation which cannot be completed immediately. A completion indication will be given at a later time when the operation has been completed.
Permission denied.	An attempt was made to access a socket in a way forbidden by its access permissions. An example is using a broadcast address for sendto without broadcast permission being set using setsockopt (SO_BROADCAST).
Protocol family not supported.	The protocol family has not been configured into the system or no implementation for it exists. Has a slightly different meaning to WSAEAFNOSUPPORT, but is interchangeable in most cases, and all Windows Sockets functions that return one of these specify WSAEAFNOSUPPORT.
Protocol not supported.	The requested protocol has not been configured into the system, or no implementation for it exists. For example, a socket call requests a SOCK_DGRAM socket, but specifies a stream protocol.
Protocol wrong type for socket.	A protocol was specified in the socket function call that does not support the semantics of the socket type requested. For example, the ARPA Internet UDP protocol cannot be specified with a socket type of SOCK_STREAM.
Resource temporarily unavailable.	This error is returned from operations on non-blocking sockets that cannot be completed immediately, for example recv when no data is queued to be read from the socket. It is a non-fatal error, and the operation should be retried later. It is normal for WSAEWOULDBLOCK to be reported as the result from calling connect on a non-blocking SOCK_STREAM socket, since some time must elapse for the connection to be established.
Socket is already connected.	A connect request was made on an already connected socket. Some implementations also return this error if sendto is called on a connected SOCK_DGRAM socket (For SOCK_STREAM sockets, the to parameter in sendto is ignored), although other implementations treat this as a legal occurrence.
Socket is not connected.	A request to send or receive data was disallowed because the socket is not connected and (when sending on a datagram socket using sendto) no address was supplied. Any other type of operation might also return this error - for example, setsockopt setting SO_KEEPALIVE if the connection has been reset.

Socket operation on non-socket.	An operation was attempted on something that is not a socket. Either the socket handle parameter did not reference a valid socket, or for select, a member of an fd_set was not valid.
Socket type not supported.	The support for the specified socket type does not exist in this address family. For example, the optional type SOCK_RAW might be selected in a socket call, and the implementation does not support SOCK_RAW sockets at all.
Software caused connection abort.	The software in your host machine aborted an established connection, possibly due to a data transmission timeout or protocol error.
Specified event object handle is invalid.	An application attempts to use an event object, but the specified handle is not valid.
Successful WSAStartup not yet performed.	Either the application hasn't called WSAStartup or WSAStartup failed. The application may be accessing a socket which the current active task does not own (i.e. trying to share a socket between tasks), or WSACleanup has been called too many times.
System call failure.	Returned when a system call that should never fail does. For example, if a call to WaitForMultipleObjects fails or one of the registry functions fails trying to manipulate the protocol/namespace catalogs.
This is a non-recoverable error.	This indicates some sort of non-recoverable error occurred during a database lookup. This may be because the database files (e.g. BSD-compatible HOSTS, SERVICES or PROTOCOLS files) could not be found, or a DNS request was returned by the server with a severe error.
Too many open files.	Too many open sockets. Each implementation may have a maximum number of socket handles available, either globally, per process or per thread.
Too many processes.	A Windows Sockets implementation may have a limit on the number of applications that may use it simultaneously. WSAStartup may fail with this error if the limit has been reached.
Unable to initialize a service provider.	Either a service provider's DLL could not be loaded (LoadLibrary failed) or the provider's WSPStartup/NSPStartup function failed.
Valid name, no data record of requested type.	The requested name is valid and was found in the database, but it does not have the correct associated data being resolved for. The usual example for this is a hostname -> address translation attempt (using gethostbyname or WSAAsyncGetHostByName) which uses the DNS (Domain Name Server), and an MX record is returned but no A record - indicating the host itself exists, but is not directly reachable.

WINSOCK.DLL version out of range.	The current Windows Sockets implementation does not support the Windows Sockets specification version requested by the application. Check that no old Windows Sockets DLL files are being accessed.

Annex: Security Keys

Introduction

Security is built into the Sysgem Enterprise Manager.

Every component of the Sysgem Enterprise Manager requires a security key to be configured as it is installed. The security key protects the system from unauthorized components being introduced into the network. Agents will only communicate with a legitimate user interface, and will reject a user interface masquerading as a genuine component. This prevents attempts to gain fraudulent access to the user-account management services provided by Sysgem Enterprise Manager.

When the security key is configured, it is encoded and stored on the machine where the Sysgem Enterprise Manager component has been installed. When the system is used to connect from the user interface to the servers, a check is made to ensure that the security keys match. If the security key on a server system does not match the client key, then the server will not co-operate with that user interface, and the requested connection will fail.

Storage

Security keys are always stored in an encrypted form on the local system, and are independent of the Sysgem Enterprise Manager user. Part of the encryption algorithm includes the hardware address of the communications boards on that machine

An encrypted key may not be copied between hardware devices - for instance an image backup of the software on one system cannot be introduced on another machine without the key being reentered on the new machine. Similarly, if a new Ethernet board has been introduced on a machine, then the security key will have to be configured again. System privileges are required to be able to re-configure a security key, and the relevant security key must be known (exactly) if this component is going to continue to cooperate with the rest of the domain after the key has been reentered.

Since it is the Authorization Server which controls the access control database, it is the Authorization Server which needs to be protected, and it is this software which holds the Installation Key for the User Interface component. If the Authorization Server is moved between machines, or if a new Ethernet board is inserted on this machine, then the Installation Key must be reset for the Authorization Server.

Providing the same Authorization Server is being used, as many User Interfaces as desired may be installed, without having to redefine the Installation Key.

Standard Security Keys

When using standard security keys, the key is a free format alpha/numeric case-sensitive character string defined by you for your network, and MUST be entered in exactly the same format for the installation of each component in the Sysgem Enterprise Manager domain. It is this key, and this key alone, which defines whether a component is included in this particular Sysgem Enterprise Manager domain.

Simple

If you are installing a simple system - for example to test Sysgem Enterprise Manager - then you only need a single security key. This must be the same on all Sysgem Enterprise Manager components.

Suggestion: **FortKnox**

The key is entered when you install the Sysgem Enterprise Manager components. To change the key after you have installed a component see Section, “Changing The Key”

Advanced

In an advanced (or more complex) environment you may decide to group your agents and restrict access to these groups by assigning different keys to each group.

You make use of the multi-key storage interface to define more than one key for the Sysgem Enterprise Manager components.

To access these servers a User Interface must have at least one key definition that corresponds to at least one key definition for each server group.

Component	Security Key(s)
Authorization Server NT Server: CETAGANDA	TOPSECRET
Server Group 1 NT Servers: BILBO, FRODO, ELROND	GANDALF
Server Group 2 UNIX Servers: RED, GREEN, BLUE	BLACK
Server Group 3 OpenVMS Servers: FORTY2, MARVIN	ZAPHOD
User Interface 1 NT Workstation: WEATHERWAX	TOPSECRET, GANDALF, BLACK
User Interface 2 NT Workstation: RINCEWIND	TOPSECRET, BLACK, ZAPHOD

In the above example users of Sysgem Enterprise Manager on WEATHERWAX can logon via the Authorization Server on CETAGANDA and access Server Group 1 and Server Group 2.

Similarly users of Sysgem Enterprise Manager on RINCEWIND can logon via the Authorization Server on CETAGANDA and access Server Group 2 and Server Group 3.

Installation Keys

New in version 2.1:

Installation keys extend the standard security keys by not revealing the actual security key at any point. During installation, the Authorization Server is configured with a set of security keys, as before. However, instead of entering the same keys when installing servers and User Interfaces, an Installation Key obtained from the Authorization Server is entered. This Installation Key can optionally be restricted to control which components can be installed.

The security keys configured on the Authorization Server bear no relation to the actual keys used by Sysgem Enterprise Manager to authenticate components – the security key is only used to confirm that the user requesting an Installation Key from the Authorization Server is authorized to do so. However, the sets of keys behave in the same way as standard security keys, in that multiple keys can be used to restrict the access of individual workstations to servers.

Each Installation Key can optionally be restricted in any combination of the following details:

- Component type

  A key can be valid for installing servers, user interfaces, or both.

- Number of installations

  Each key can be used a certain number of times, after which further installations with it will be impossible.

- Time of installation

  Each key can be used up until a certain time and date, after which further installations with it will be impossible.

To accomplish this, the installation procedure for each component will communicate with the Authorization Server that issued the key. If the installation key is still valid, the Authorization Server provides the new component with the actual key being used on the network.

See the section Obtaining Installation Keys for details of generating Installation Keys.

Domains

The Installation Key system also introduces an optional domain system which can be used to tie each set of security keys to a given Authorization Server. When this is in use, only those keys belonging to the domain are considered when attempting to connect to servers – so a workstation that has security keys set for several domains will only be able to connect to servers that have keys for the Authorization Server the User Interface logged on to.

Advanced Example

Using the set of groups described above for an advanced installation using standard security keys, we might set the system up as follows:

Component	Key(s)
Authorization Server	Security Keys: 1: GANDALF 2: BLACK 3: ZAPHOD Installation Keys: Restrictions: 1: EB22-PSC4-D6WB-ZFVY-8DKQ-Y45U-NYHH (2 uses) 2: LU3H-T4R2-WS4E-ARCM-SLC3-GRT4-S8MZ (3 uses) 3: 6BQR-7NHY-3XGB-DWXY-GJPX-VD7Y-ZA43 (2 uses)
Server Group 1 NT Servers	EB22-PSC4-D6WB-ZFVY-8DKQ-Y45U-NYHH
Server Group 2 UNIX Servers	LU3H-T4R2-WS4E-ARCM-SLC3-GRT4-S8MZ
Server Group 3 OpenVMS Servers	6BQR-7NHY-3XGB-DWXY-GJPX-VD7Y-ZA43
User Interface 1 NT Workstation	EB22-PSC4-D6WB-ZFVY-8DKQ-Y45U-NYHH LU3H-T4R2-WS4E-ARCM-SLC3-GRT4-S8MZ
User Interface 2 NT Workstation	LU3H-T4R2-WS4E-ARCM-SLC3-GRT4-S8MZ 6BQR-7NHY-3XGB-DWXY-GJPX-VD7Y-ZA43

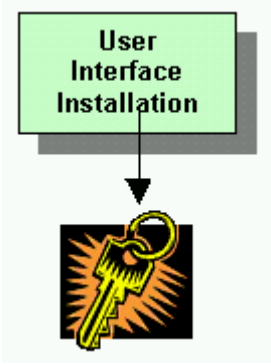
Should an unauthorized user now attempt to configure another machine on the network, they would find that specifying GANDALF, BLACK or ZAPHOD as a standard security key will not allow them to connect to the authorization server, and trying to use any of the three Installation Keys will also fail as they are no longer valid. To successfully install another machine, they would need to gain access to the Authorization Server, provide one of the three security keys, and request a new Installation Key.

Challenge / Response Authentication

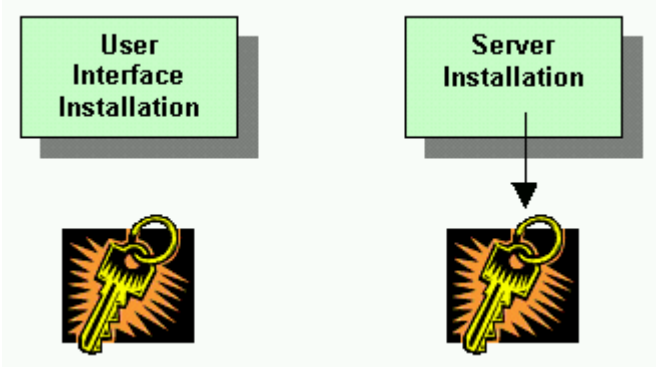
The following shows the sequence of events during the challenge/response dialogue of the security authentication between the co-operating components in a Sysgem Enterprise Manager domain:

In this description the Server is either the Authorization Server or a Platform Server.

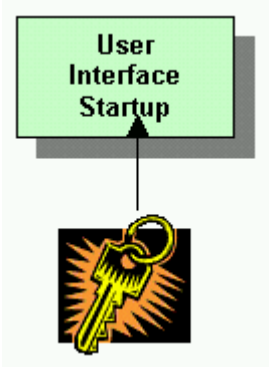
1. Install User Interface and configure security keys.



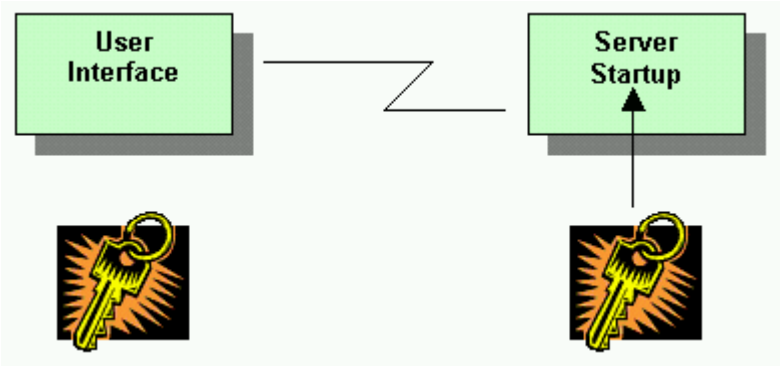
2. Install Server and configure security keys.



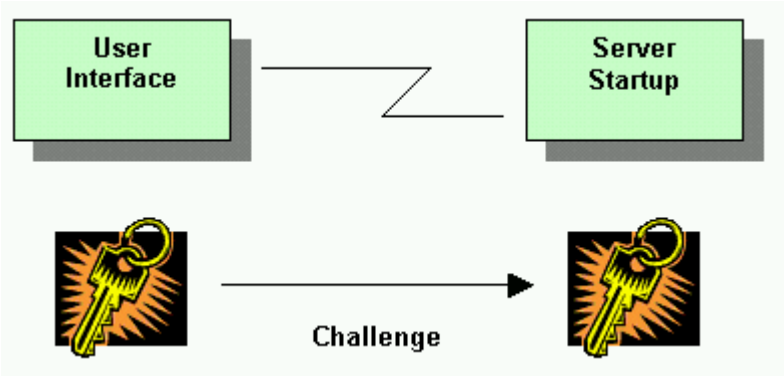
3. Start User Interface (read encrypted key - is it valid for this hardware?).



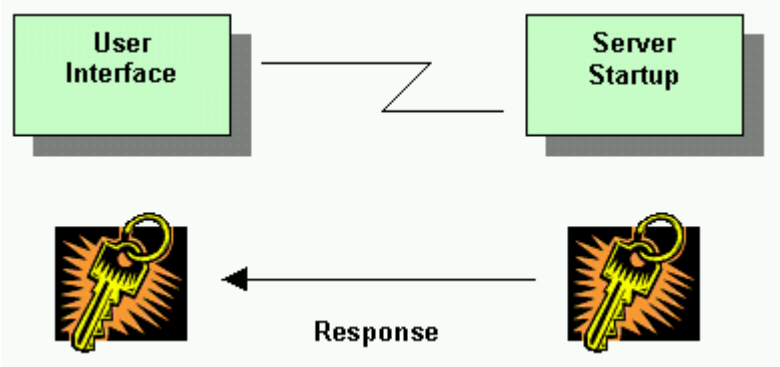
4. User Interface sends connect request to Server (read encrypted key - is it valid for this hardware?).



5. User Interface issues 'Challenge' to Server (the challenge includes a timestamp, and is never the same as any previously generated challenge).



6. Server computes a 'Response' using the values of the Challenge and the Installation Key to generate the response.



7. User Interface validates the response ensuring that this is a valid response to this challenge, and that the keys in the client and the server match.

Steps 5 to 7 are repeated, this time with the server issuing the challenge, and the User Interface responding.

Changing the Key

Each Sysgem Enterprise Manager component supports ten standard security keys, and ten security keys for each configured Sysgem domain if installation keys are in use. The Authorization Server can only be a member of one Sysgem domain, but can still use both standard security keys and Installation Keys simultaneously.

Management Console

You either start the Security Key Manager from Security Key Manager option on the Tools menu, or from the command line.

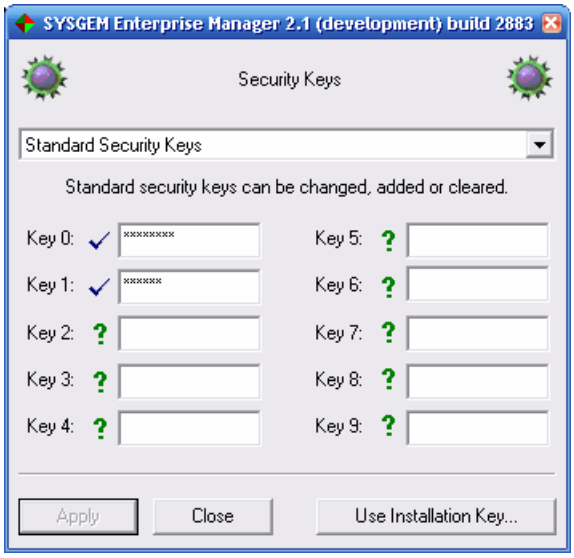
To change the Management Console key(s) from the command line you must start the executable with the -k argument. The executable is usually found in

```
C:\Program Files\SYSGEM\SEM User Interface\SEM Client
```

So you enter (at a command prompt or the Start menu's Run option):

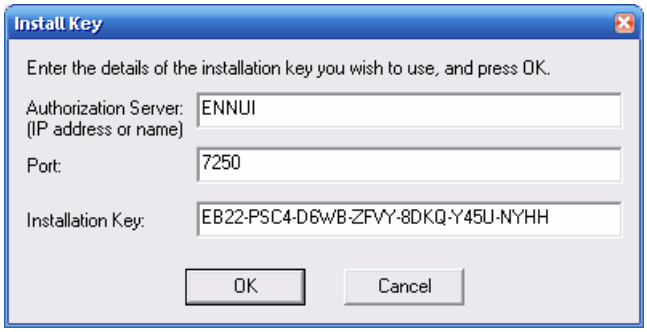
```
C:\Program Files\SYSGEM\SEM User Interface\SEM Client.exe -k
```

The following dialog box is displayed:

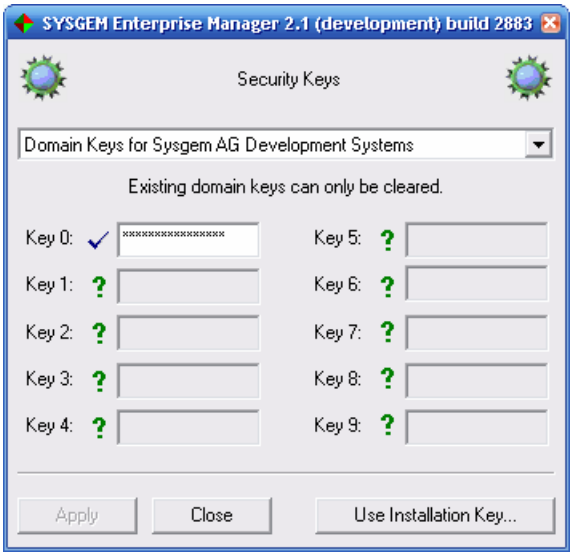


To alter the standard security keys, enter or change values in the fields, then click Apply. Fields which are not modified are left unchanged.

To install a new key using using an Installation Key, click the Use Installation Key… button and enter the details of your Authorization Server and Installation Key:



To remove security keys set using an Installation Key, select the domain from the drop-down list and clear the relevant key field:



Authorization Server

To change the Authorization Server key after installation change to the Authorization Server directory - usually:

C:\Program Files\SYSGEM\SEM Authorization Server

and start the *SEM AuthServer* executable with one of the following arguments:

Argument	Description
-Kn	Set key (0 to 9), 0 is the default. To set key 3 to FortKnox enter: "SEM AuthServer" -K3 FortKnox
-Rn	Remove key (0 to 9), 0 is the default. To remove key 7 enter: "SEM AuthServer" -R7
-RA	Removes all security keys. To remove all keys enter: "SEM AuthServer" –RA
-SD	Set domain name; use name “0” to reset to a domain common to all installations: "SEM AuthServer" –SD "Sysgem AG"
-SKn	Set domain key (0 to 9), 0 is the default. To set key 0 to FortKnox enter: "SEM AuthServer" –SK0 FortKnox
-SRn	Remove domain key (0 to 9), 0 is the default.
-SRA	Removes all domain keys.
-SSn	Generate single-use Installation Key for domain key 0 to 9 (0 is the default). To generate an Installation Key for key 0 enter: "SEM AuthServer" –SS0 FortKnox
-SIn	Generate Installation Key for domain key 0 to 9 (0 is the default), prompting for parameters. "SEM AuthServer" –SI0 FortKnox

OpenVMS Server

To change the VMS Server key after installation use a foreign command:

```
$ SEM == $dev:[dir]sem-agent-axp
```

where dev:[dir] is usually sys$sysroot:[Sysgem-sem-agent], so the foreign command definition becomes:

```
$ SEM == $sys$sysroot:[Sysgem-sem-agent]ssm-agent-
axp
```

and enter:

```
$ SEM -K "FortKnox"
```

for a standard security key, or

```
$ SEM -I authsvr:6BQR-7NHY-3XGB-DWXY-GJPX-VD7Y-ZA43
```

for an installation key, where authsvr is the name or address of your Authorization Server.

Unix Server

To change the security key or use an installation key on a Unix server after installation, run the agent with the –k or –i arguments respectively:

```
# /opt/Sysgem/SysgemSEMAgent -k0 FortKnox
```

or

```
# /opt/Sysgem /SysgemSEMAgent -i authsvr:installation-
key
```

Windows NT Server

Changing the Windows NT security key is similar to changing the Authorization Server key, except that you change to the Windows NT Server directory - usually:

C:\Program Files\SYSGEM\SEM Server

Start the *SEM Server* executable with one of the following parameters:

Argument	Description
-Kn	Set key (0 to 9), 0 is the default. To set key 3 to FortKnox enter: "SEM Server" -K3 FortKnox
-Rn	Remove key (0 to 9), 0 is the default. To remove key 7 enter: "SEM Server" -R7
-RA	Removes all security keys. To remove all keys enter: "SEM Server" –RA
-I	Use Installation Key. To use a key issued by the machine AuthServer enter: "SEM Server" –I AuthServer:installationkey

Checking the Keys

To check the keys:

1. Start the User Interface.
2. Connect to the Authorization Server - if you get this far then the User Interface and Authorization Server keys are the same.
3. Select Servers from the Managers menu.
4. The Server Definitions window is displayed. You can test the status of the server installations by select one or more entries, the pressing the Test button (top right).
5. A connection is established with each selected server (this checks the IP connection) and the security handshake is performed (this checks the security keys).
6. The result is displayed in the IP Connection Status colum.

Obtaining Installation Keys

New in version 2.1:

An Installation Key can be obtained by running the Authorization Server with the –SS or –SI options and providing the correct security key. The Authorization Server is typically installed in C:\Program Files\Sysgem\SEM Authorization Server, and can be started either from the Run… option on the Start menu or from a command prompt.

The –SS option generates an Installation Key that can be used to install either agenrs or GUIs, but can only be used once before expiring.

The –SI option provides the ability to restrict the key in other ways; an example of generating an Installation Key through this method is shown below. Text entered by the user is shown in **bold**:

```
C:\> CD "\Program Files\Sysgem\SEM Authorization Server"
C:\Program[...]Server> "SEM AuthServer" -si0 FortKnox

SCSA Installation Key Generation
================================

This routine generates an installation key for installing other
Sysgem Enterprise Manager components.  Please see your User Guide
for more information on the installation key system.

Default responses to questions are shown in brackets.
Enter 'q' at any time to quit without generating a key.

Generate a key for cloning this Authorization Server? [No] n
Allow key to be used for installing Management Consoles? [Yes] y
Allow key to be used for installing Agents? [Yes] n
Allow key to be used how many times (U = unlimited)? [Unlimited] 2
Allow key to be until (N = no expiry)? [No expiry] January 25

Key Validity:

   Valid components .........: Management Consoles
   Maximum number of uses ...: 2
   Expires ..................: Wed Jan 25 00:00:00 2006

Is this correct? [Yes] <CR>

New installation key generated: AETJ-UU4T-JYNH-M7EC-JTWQ-PGMU-7CLZ
```

Index

A

Access Control Profiles 33
Access Control Tokens 34
Account Passwords 33
Address already in use 38
Address family not supported by protocol family 38
AddStartup 23
Adobe Acrobat 8
Advanced 46
Agent Definitions 27
Agent Files 16, 24
Agent for Windows 2000/NT 7
AIX 3, 24
Alpha 15, 22, 45
Annex
  Security Keys 45
Append 12
APPEND 12
Application Support Packages 3, 4, 29
Archive 7, 15, 21, 34
Archive Script 34
Authentication 46
Authorization Server 3, 7, 32, 46
AutoPlay 4, 8
AutoStart 22
Available Product Guides 1

B

Bad address 39
Bad protocol option 39
Base 1
base PAK 29
Base pane 28
BITMAP 12
Build 16, 22, 31

C

Cannot assign requested address 39
Cannot send after socket shutdown 39
Challenge / Response Authentication 46
Changing The Key 45
Changing the Security Key 26
Checking The Keys 50
Checksum 28
Choose Destination Location 10
Class type not found 39
Common Socket Errors 38
Communications 37, 45
Company, City, Zip Code, Country 31
COMPAQ (Digital) UNIX 25
Compaq Tru64 21
Component 4, 10, 32, 45
Configuration 3, 8, 24, 27
Configuration Files 12
Connection refused 37
Connection reset by peer 39
Connection timed out 37
CONSOLE 3, 7, 19, 32, 49
Contacting Us 1
Contents of Kit 7

D

DEBUG 13, 24
De-installation 13
Description 9, 18, 24, 30, 38, 46
Destination address required 39
Directory 4, 8, 15, 21, 49
Downloads section 1

E

Enterprise Accounts 35
Error text 38
Evaluation License 4, 27
Example Installation 15
Extras 8, 15

F

Fields 9, 27, 49
File 5, 10, 15, 21, 29, 41
Files Installed 8, 18, 24
First-Time Login 5, 27
Full Access 33
Full List of Socket Errors 38

G

Graceful shutdown in progress 39
Group 24, 29, 46
group PAK 29

H

Host is down 40
Host not found 40
HP 3, 24
HP UNIX 26
Html Help 8

I

IBM AIX 3, 24
Importing a Permanent SEM License 5, 29
Install Kits 4, 8
Install Windows 2000/NT Software 4, 9
Installation and Configuration 4
Installation Key 17, 45
installation logfile 15
Installing Application Support Packages 5, 29
Installing on OpenVMS 15
Installing on Windows 2000/NT 8
Installing Other Platform Agents 4
Installing Plug-In Application Modules 5, 29
Installing Windows 2000/NT Software 4
Insufficient memory available 40
Interrupted function call 40
Introduction 1, 21, 45
Invalid argument 40
Invalid procedure table from service provider 40
Invalid service provider version number 40
Issued by 31

L

Library Mappings 27
library/init.tcl 24
License Bar 30
License Editor 31
License Manager 28
License PAK 5, 28
Licenses 27
LINUX i386 24
LINUX Intel 24
Load 4, 29
LOGFILE 12, 15, 24

M

Management Console 3, 7, 19, 32, 49
Managers 27, 50
Message too long 40
Method 25
Mirrored Accounts 33

N

Network dropped connection on reset 40
Network is down 40
Network is unreachable 40
Network subsystem is unavailable 41
No buffer space available 41
No route to host 37
No Security Keys Defined 37
Non-authoritative host not found 41
Novell NetWare 3
NT 4.0 7
NT 4.0 Service Pack 3 8
NT Service 7

O

ODBC 8
ODBC Access driver 8
ODBC Manager 8
OK 17, 23, 31
One or more parameters are invalid 41
Online Support 1, 4, 9, 21, 28
OpenVMS Agent 15
Operation already in progress 41
Operation not supported 41
Operation now in progress 41
Option 11, 22, 28, 39, 49
Option Settings 33
Options 16, 31, 50
Ordering a Permanent SEM License 28
Overlapped I/O event object not in signaled state 41
Overlapped operation aborted 42
Overlapped operations will complete later 42
Overview 3, 27

P

password 4, 7, 21, 27
Performance 19, 24, 34
Perl 8, 37
Permanent SEM License 5, 28
Permission denied 42
Platform 3, 11, 22, 35, 46
Plug-In Application Modules 3, 29
PORT 11, 15, 21, 34, 37
Post-Installation Configuration
  Security Keys 11
pre-installed SEM username and password 5, 27
Prerequisites 8
Problem 37
Problem Solving 37
PRODUCT 1, 7, 16, 22, 27
profile 7, 28
Protocol family not supported 42
Protocol not supported 42
Protocol wrong type for socket 42

Q

Quick Start 3

R

Readme 9
RemoveStartup 23
Report 30
RESELLER 12
Resolution 37
Resource temporarily unavailable 42
Root Directory 8, 19, 24

S

SAcM Account Manager 34
SAcM User Guide 1

Save 16, 31
SDeM User Guide 1
Security 1, 3, 8, 17, 21, 27, 37, 45
Security Key 4, 11, 17, 22, 32, 37, 45
Security key mismatch 32, 37
Security Keys 8, 11, 19, 23, 32, 37, 45
Select Components 10
Select Program Folder 10
SEM Accounts 27
SEM Agent for Windows 2000/NT 7
SEM Agents 3
SEM Application Support Packages 3, 5, 29
SEM Authorization Server 3, 7, 49
SEM AuthServer.cfg 12
SEM Base Framework Components 3
SEM Installation Guide 1, 7
SEM License 5, 28
SEM Lotus Notes Package 3
SEM Management Console 3, 7, 19
SEM MS Exchange Package 3
SEM Oracle Package 3
SEM Pathworks Package 3
SEM Plug-In Application Modules 3
SEM PMDF Package 3
SEM Release Notes 1
SEM SAP Package 3
SEM User guide 1
SEM Windows 2000/NT Kit 8, 37
Send License via Mail 28
Service Pack3 7
Setting Security Keys on NT 32
Setting Security Keys on OpenVMS 32
Setup Complete 11
Simple 13, 45
Socket is already connected 42
Socket is not connected 42
Socket operation on non-socket 43
Socket type not supported 43
Sockets Errors 37
Software caused connection abort 43
Software License Agreement 9
Specified event object handle is invalid 43
SSeM User Guide 1
ssm-accounts 16, 23
ssm-commander 23
ssm-perf 16, 23
ssm-syslog 23
SSyM User Guide 1
Start Copying Files 10
Stopping The Agent 25
Storage 45
Successful WSAStartup not yet performed 43
SUN Solaris 3, 24
SUPPORT 3, 9, 21, 28, 41
SWISSFLAG 12
Sysgem Account Manager (SAcM) Module 1, 3
Sysgem Development Manager (SDeM) Module 3
SYSGEM root directory 8
Sysgem Security Manager (SSeM) Module 3
Sysgem System Manager (SSyM) Module 1, 3
Sysgem web page 1
SysGem-Agent-Logfile-Oct-00.txt 24
SysgemSEMAgent 23, 32
SysgemSEMAgent.cfg 23
SysgemSEMStart 23
System account 11, 15, 33
System call failure 43
System Hygiene 8

T

tar archive 21
Templates 27
Termination 30
Test System for Evaluation 4
This is a non-recoverable error 43
Token 12, 26, 30
Tokens 12
Too many open files 43
Too many processes 43
Typical Configuration 3

U

Unable to initialize a service provider 43
UNIX 3, 21, 32, 46
UNIX/Linux Agents 21
UNIX/Linux platforms 21
unixagent020.tar file 5
unzip 4, 15
URL 12
User Information 9
username 5, 11, 17, 27

V

Valid name, no data record of requested type 43
VAX 15
View menu 30
VMSINSTAL 4, 15
VMSSVR020.A 15
VNC Remote Desktop Server 7

W

Welcome 9
What's Inside 1
Windows 2000/NT 3, 7, 37
Windows 2000/NT Software 4, 7
WINSOCK.DLL version out of range 44
Winzip 8

X

Xtras folder 4