SCALIX™

Installation Guide

Version 10.0.1

Installation Guide

Published by Scalix Corporation
1400 Fashion Island Blvd., Suite 602
San Mateo, CA 94404-2061
USA

Product Version: 10.0.1

E: 3.30.2006/b

Notices

The information contained in this document is subject to change without notice.

Scalix Corporation makes no warranty of any kind with regard to this material, including, but not limited to, the implied warranties of merchantibility and fitness for a particular purpose. Scalix Corporation shall not be liable for errors contained herein or for incidental or consequential damages in connection with the furnishing, performance, or use of this material.

Unix is used here as a generic term covering all versions of the UNIX operating system. UNIX is a registered trademark in the United States and other countries, licensed exclusively through X/Open Company Limited.

Linux is a registered trademark of Linus Torvalds.

Red Hat, and Fedora are registered trademarks of Red Hat Software Inc. rpm is a trademark of Red Hat Software Inc.

SUSE is a registered trademark of Novell Inc.

Java is a registered trademark of Sun Microsystems Inc.

Microsoft, Windows XP, Windows 2000, Windows NT, Exchange, Outlook, Active Directory, and Internet Explorer are either registered trademarks or trademarks of Microsoft Corporation in the United States and other countries.

Restricted Rights Legend

Use, duplication, or disclosure is subject to restrictions as set forth in contract subdivision (c)(1)(ii) of the Rights in Technical Data and Computer Software clause 52.227-FAR14.

Introduction

This user guide covers the setup and installation of the Scalix messaging system—Enterprise Edition, Small Business Edition or Community Edition—on qualified Linux systems. This guide also describes how to install and configure Scalix Connect for Microsoft Outlook on Windows 2000 and XP client computers.

Contents of this Guide

Included in this guide are the following topics:

PLUS... This guide also provides a separate chapter on the installation and configuration of Scalix Connect for Microsoft Outlook, on Windows 2000 and XP systems—from both administrator and end-user perspectives. Various client-setup methods are detailed, including installations done remotely without end-user participation, and full end-user involvement in installation. Lastly, the uninstallation of Scalix Connect from client PC's is also detailed. For complete information, see "Installing and Managing Scalix Connect" on page 135

About Scalix Product Editions

Scalix offers three editions of its powerful email and calendaring platform based on Linux and open systems: Scalix *Enterprise Edition, Small Business Edition* and Scalix *Community Edition*.

Scalix Enterprise Edition is the company's flagship product and is ideal for organizations that demand the full range of functionality in a commercial email and calendaring system. It includes multi-server support, unlimited number of *Standard* users, any number of *Premium*

users, the full complement of Scalix advanced capabilities, and a wide variety of technical support options.

Scalix Small Business Edition targets organizations getting started with a commercial version of Scalix that do not have the higher end requirements of Enterprise Edition. It is functionally equivalent to Enterprise Edition except that it allows only single-server installations instead of multi-server, and does not include the capabilities for high availability and multi-instance support.

Scalix Community Edition is the free, single-server, unlimited-use version of the Scalix product and is great for cost-conscious organizations that desire a modern email and calendaring system but do not require advanced groupware and collaboration functionality for their entire user population. It includes unlimited Standard users, twenty-five free Premium users, a subset of Scalix functionality, and fee-based, incident-based technical support.

The following table compares the Scalix product editions in greater detail:

Product Feature	Community Edition	Small Business Edition	Enterprise Edition
User Types			
Standard Users	Free, unlimited	Free, unlimited	Free, unlimited
Premium Users	Maximum 25 premium users (free)	Any number of licensed premium users	Any number of licensed premium users
Core Functionality			
Email & calendaring Server	Single-server	Single-server	Multi-server
Internal user directory	[X]	[X]	[X]
GUI-based installation	[X]	[X]	[X]
GUI & command line administration	[X]	[X]	[X]
Complete documentation	[X]	[X]	[X]
POP/IMAP email client access	Unlimited	Unlimited	Unlimited
Native MS Outlook support (via MAPI)	Premium users only (max 25)	Premium users only	Premium users only
Fully functional AJAX web client (Scalix Web Access)	[X] (group scheduling in calendar for 25 premium users only)	[X] (group scheduling in calendar for all premium users)	[X] (group scheduling in calendar for all premium users)
Native Novell Evolution support	[X] (group scheduling in calendar for 25 premium users only)	X] (group scheduling in calendar for all premium users)	X] (group scheduling in calendar for all premium users)
Public folders	Premium users only (max 25)	Premium users only	Premium users only

High availability	Not available	Not available	[X]
Multiple instances per server	Not available	Not available	[X]
Migration tools	Not available	[X]	[X]
Upgrade To Enterprise Edition	Via license key. Re-installation not required	Via license key. Re-installation not required	Not applicable
Ecosystem Support			
Meta-directory support via LDAP	[X]	[X]	[X]
iCal support	[X]	[X]	[X]
Native Exchange Interoperability (via TNEF)	Not available	[X]	[X]
Active Directory integration with MMC plug-in	Not available	[X]	[X]
Anti-virus	Via flexible 3rd party interface	Via flexible 3rd party interface	Via flexible 3rd party interface
Anti-spam	Via flexible 3rd party interface	Via flexible 3rd party interface	Via flexible 3rd party interface
Archiving	Via flexible 3rd party interface	Via flexible 3rd party interface	Via flexible 3rd party interface
Wireless email & PIM	Email-only via POP/IMAP	Email & PIM via Notify	Email & PIM via Notify
Technical Support			
Community Forum	Free	Free	Free
Knowledgebase, Tech notes	Free	Free	Free
Incident-based Support	Fee-based	Fee-based	Fee-based
Software subscription	Not available	[X]	[X]
Premium 7x24 Support	Not available	[X]	[X]
Cost			
Licensing	Free, unlimited use	Cost based on number of premium users, no cost for Scalix server(s)	Cost based on number of premium users, no cost for Scalix server(s)

Scalix User Types

Scalix users can be defined as *Standard* or *Premium* users, as defined in the following:

Standard Users

Standard users gain access to a subset of Scalix functionality including email, personal calendar and contacts through Scalix Web Access and Novell Evolution as well as email access using POP/IMAP clients. The ability to deploy standard users is ideal for cost-conscious organizations with users who do not have high-end groupware and collaboration requirements. An unlimited number of standard users may be deployed with any Scalix edition for free.

Premium Users

Premium users have access to the full benefits and functionality of the Scalix email and calendaring system. The following Scalix product capabilities are available only to premium users:

- Native MS Outlook support (via MAPI)
- Group scheduling functionality including free/busy lookup in Outlook, Scalix Web Access and Evolution clients
- Access to public folders
- Wireless email and PIM

Any number of licensed premium users may be deployed with Scalix Enterprise Edition. Scalix Community Edition is limited to a maximum of twenty-five (25) free premium users, who enjoy many of the features available to Enterprise Edition premium users.

Flexible, Cost-Effective Email For Everyone

The distinction between standard and premium users provides organizations with the flexibility to cost-effectively provide email for all users. For example, manufacturers and retailers may desire headquarters staff to be designated as premium users as they require advanced groupware capabilities, while less demanding users, such as shop floor or store personnel, would be satisfied as standard users with only email and personal calendaring capabilities. Similarly, educational institutions may decide that faculty and staff are premium users that need advanced collaboration capabilities while students are standard users that just need email and personal calendaring. There is no cost for deploying standard users with either Scalix Community Edition or Scalix Enterprise Edition.

Required Licenses

Scalix *Community Edition, Small Business Edition* and *Enterprise Edition* use the same installer. The main difference is that Small Business Edition and Enterprise Edition require a license key while Community Edition does not. Additionally, if you are a Scalix Community Edition customer, you can only perform the “typical” installation, in which all the Scalix components are stored on a single host computer.

To activate your Scalix system as either a Small Business or Enterprise Edition system, you must enter a license key at a strategic point in the installation process. Please obtain your Scalix license key and have it ready for use before installing Scalix 10.0 or 10.0.1.

You may proceed with the installation without a license key, however, your system is treated as a Community Edition system and your users as Standard users until the correct license key is entered by means of the *Scalix Administration Console*.

Additionally, you can install Scalix Enterprise Edition onto a single host, or distribute the primary components onto separate hosts—both of which are detailed fully in this guide.

Identifying the Instance Home Directory

Throughout the installation procedure, there are repeated references to the instance's home directory, known as "~". The location of this directory varies depending on how you ran your initial setup. For example, if you named the instance when you created it, the home directory becomes /var/opt/om.[name]. But if your instance is unnamed, the home directory becomes /var/opt/scalix.

To determine the home directory for a particular instance, look in /opt/scalix/global/config.

Contents

Pre-Installation Requirements

This chapter describes, in complete detail, all of the pre-installation requirements that should precede your setting up of a Scalix Enterprise Edition messaging system on any qualified Linux OS host computers. As of this edition, the only "qualified" OS packages that are supported by Scalix include specific Red Hat and SUSE Linux packages, as detailed in this chapter

The following sections detail the complete range of hardware and software requirements for a Scalix email system (both *Community Edition* and *Enterprise Edition*), both general requirements and OS- or manufacturer-specific requirements.

Setting up a successful Scalix system requires that the packages and software listed in the following table rows be installed on the host computer. We have grouped the requirements by computer and Linux version/distribution.

And please note that (1) JSDK is no longer required, except on IBM Z-series computers, and (2) Java Runtime Environment and Tomcat (along with the JK Tomcat/Apache connector) are installed automatically as part of the Scalix system, even if pre-existing installations are present on the host.

Contents

This chapter includes the following pre-installation information:

Required Hardware/Network Setup

Unlike previous versions of Scalix, you do not need to install any Java Software Development Kit packages (JSDK); instead, Scalix has bundled the *Java Runtime Environment* (JRE) version 1.5 to install on the host computer, if it is not already present.

Components	Requirements
Hardware / host computers	Any Intel x86 or x86_64 host computer that supports Linux Any AMD or AMD64 host computer that supports Linux An IBM Z-series host computer (Z-VM mode) **IMPORTANT:** Scalix software can be installed on a 64-bit Intel or IBM computers, and in 64-bit Linux environments (as 32-bit applications).
Operating systems (Linux)	You can install and run Scalix in any of the following versions of Linux: • Red Hat Enterprise Linux 3, 4 • Red Hat Enterprise Linux 3, 4 • SUSE Linux Enterprise Server 9 Scalix can be installed on the following Linux OS's (on Intel or AMD hosts), but should be done only for evaluation purposes: • Fedora Core 4 • SUSE Linux Open Source Software (OSS), v10.0
RAM	512 MB (minimum)
Available disk space	100 + MB of free disk space (not anticipating any needed installation of Java Runtime Environment, Tomcat or JK Connector) The space should be apportioned as noted here: • opt/scalix: 125 MB. • /var/opt/scalix: 70 MB, if doing the basic installation. • /var/opt: If doing a high availability system, be sure to apportion this directory enough memory as this is where failover is directed. See "A Survey of Linux Installation Qualifications" on page 17 for more information about creating a separate partition for the Message Store. **NOTE:** To check the amount of free disk space on the host computer, log in and run the df –h command.
DNS	IMPORTANT: You must configure a Reverse DNS Lookup entry (on the DNS server) for all the Scalix servers in the network. Make sure that a DNS alias exists for scalix-default-mail and that the fully qualified domain name for the target host (for the scalix-default-mail alias) is set to any Scalix Server.

Required Software for Intel or AMD Systems

Any Intel-based or AMD64-based host computer has unique Linux installation requirements, as detailed in the following tables.

Components	Requirements
Intel x86— **Any installation of Linux**	All Intel x86-based hosts (running any Linux variation) require the following: • glibc • bash • ncurses • libstdc++ • coreutils • grep • diffutils • gawk • sed • util-linux • openssl • which • tcl • tk • cyrus-sasl (32-bit libs) • sendmail (v8.12 and above) • Python v2.2 through 2.4 INCLUDED WITH SCALIX INSTALLATION • JRE v1.5 • Tomcat 5.0.28 (tar.gz file) • JK Apache/Tomcat Connector • libical rpms
Intel x86— **Red Hat / Fedora Linux**	All Red Hat and Fedora Linux hosts require the following: *Only needed for an x86_64 platform • compat-libstdc++ • procps • elinks • krb5-libs • httpd • cyrus-sasl-md5 (32-bit libs) • cyrus-sasl-plain (32-bit libs) • libstdc++ (32-bit libs)* • libxm12 (32-bit libs)* • ncurses (32-bit libs)*
Intel x86— **SUSE Linux**	All SuSe Linux hosts require the following: • lynx-2.8.5-27.i586.rpm (included with Scalix) • ps • compat • heimdal-lib • apache • cyrus-sasl-plain (32-bit libs) • python-gtk-2.0.0-215.3

Alert Tomcat 5.5 is not supported in Scalix.

Required Software for IBM Z-Series Systems

The IBM Z-series of host computers has different requirements from other systems, as detailed in the following tables.

Components	Requirements
IBM s390/390x computers— **Required Red Hat 31-bit (s390) or 64-bit (s390x) packages**	Both Red Hat Linux installations require the following: • bash • coreutils • grep • diffutils • gawk • sed • util-linux • tcl • tk • procps • elinks • krb5-libs • httpd
IBM s390/390x computers— **Required SLES 31-bit or 64-bit packages**	SLES 9.0 Linux installations require the following: • bash • coreutils • grep • diffutils • gawk • sed • util-linux • tcl • tk • ps • compat • apache • cyrus-sasl-digestmd5 (32-bit libs) • cyrus-sasl-crammd5

Components	Requirements
IBMs390/390x computers— **Required Red Hat 31-bit packages**	The packages listed below must be the 31-bit (s390) versions of the package as they contain shared libraries which Scalix uses, and Scalix Server is compiled as a 31-bit application. However, if the 64-bit (s390x) version of a package is already installed on the server, you do not have to remove the package. The 31-bit (s390) and 64-bit (s390x) version can co-exist on the server. Red Hat linux hosts require the following: • compat-libstdc++ • krb5-libs • libstdc++ • libxml2 • ncurses • openldap • openssl • glibc • which • XFree86-libs (RH3) • libgcc (RH4) • xorg-x11-libs (RH4) • sendmail (8.12 and above) • Python 2.2 through 2.4 • cyrus-sasl One or more of the following, depending on the required authentication: • cyrus-sasl-plain (32-bit libs) • cyrus-sasl-gssapi (32-bit libs) • cyrus-sasl-md5 (32-bit libs) INCLUDED WITH SCALIX— • JRE v1.5 • Tomcat 5.0.28 • JK Tomcat/Apache connector
IBM s390/390x computers— **Required SLES 31-bit packages**	IMPORTANT: The packages listed below must be the 31-bit (s390) versions of the package, because they contain shared libraries which Scalix uses, and Scalix Server is compiled as a 31-bit application. SLES 9.0 platforms require the following: • glibc • heimdal-lib • openldap2-client • openssl • libstdc++ • XFree86-libs • libxml2 • lynx-2.8.5-27.s390.rpm (included with Scalix) • which • sendmail (8.12 and above) • Python 2.2 through 2.4 • apache 2 • J2SE 1.4.2_03 SDK or later, or JRE 1.4.2 • cyrus-sasl One or more of the following depending on the required authentication: • cyrus-sasl-plain (32-bit libs) • cyrus-sasl-gssapi (32-bit libs) • cyrus-sasl-md5 (32-bit libs) INCLUDED WITH SCALIX— • JRE v1.5 • Tomcat 5.0.28 • JK Tomcat/Apache connector

Components	Requirements
Possible 31-bit software dependencies affecting IBM Z-series s390 systems	**Red Hat 3 Linux:** zlib, db4, gdbm, XFree86-libs-data, XFree86-Mesa-libGL, libgnat, gpm, cracklib, pam, fontconfig, laus-libs, freetype, libgcc, gcc-gnat, glib, expat. **Red Hat 4 Linux:** zlib, gdbm, xorg-x11-Mesa-libGL, cracklib, cracklib-dicts, pam, fontconfig, freetype, glib2, expat, e2fsprogs, libselinux. **SLES 9.0 Linux:** e2fsprogs, db, gdbm, readline, pam, libgcc, expat, fontconfig, freetype2, ncurses, zlib, cracklib.

Approved Web Browsers and Email Clients

Components	Requirements
Approved web client software (Scalix Web Access client browsers)	• Internet Explorer 5.5 or 6.0 • Mozilla 1.7 or higher • Firefox 1.0 and later
Approved e-mail client software	• Microsoft Outlook versions 2000, XP, and 2003 and later (versions 9, 10, 11) • Novell Evolution, versions 2.4.2 and later
Approved Windows OS versions (for client workstations)	• Windows 2000 • Windows XP (All earlier versions of Windows are not supported, irrespective of which version of Outlook you have installed.)

Helpful Debugging Resources for Scalix

It is strongly recommended that you install the following binaries on your Scalix host(s), to assist you if you need to work with Scalix Support in resolving any problems.

- tcpdump
- ethereal
- lsof
- strace
- gdb

Important—About the Scalix License Key

During the installation/upgrade process, you are asked to provide a Scalix license key. This is true whether you are installing Community Edition or Enterprise Edition. If you are installing Community Edition, you can "click through" this step, and proceed without importing a license. It is required only if you are installing Enterprise Edition.

What is on your Scalix system

To list all of the .rpm packages that are installed on the system, run this command:

```
rpm -qa
```

Use this to determine whether you have satisfied the Scalix package dependencies that are detailed later in this chapter. You can also determine the version number for a specific package (for example, diffutils) by adding the -q extension to this command, as shown here:

```
rpm -q diffutils
```

A Survey of Linux Installation Qualifications

If you are planning to install and run a Linux host as the Scalix Server, be aware of the following:

- Scalix Corporation recommends assigning a *static* IP address to the host. This minimizes problems with DNS.
- Performance of the Scalix Server can be modestly increased by operating the system in runlevel 3 (command line mode) instead of runlevel 5 (GUI mode).

Pre-installation qualifications

Be sure to review the following before installing Linux on the host computer, if you are starting with a new computer and performing a clean installation.

- Scalix Corporation recommends installing Linux on a host computer that does not already have an operating system installed. This includes operating systems stored in separate partitions on a single host.
- If you are performing a clean installation of Linux on the host computer, you must choose the disk partitioning option during the installation. Partitioning the main drive ensures that Scalix Server operates properly.

The following section provides the needed partition specifics.

Partitioning a Linux host

For more help with planning and setting up *Logical Volume Manager* (LVM) and partitioning the host hard drive, browse the Tech Notes in the Scalix Support Knowledgebase.

- Partitioning of the host can be accomplished during the installation of the Linux operating system, or can be retroactively applied by means of a disk partitioning utility.
- Required Linux-specific partitions include root (/), /boot, and /swap. See the following subsections for relevant instructions.
- A /var partition must be created, for use as the destination directory for Scalix Server.

Note For step-by-step assistance with installing of a Linux operating system, see the appropriate installation documentation for the version of Linux you've acquired.

Setting up a root (/) partition

This is a required partition that must be assigned to a native Linux disk partition. Scalix Corporation recommends a root partition of approximately 6 GB. This enables you to install all of the required packages and software needed by the Linux server.

Setting up a /boot partition

The /boot partition stores the operating system kernel (which allows the system to load the Linux operating system), along with support files used during the bootstrap process. Because of the limitations inherent in the BIOS of most host computers, Scalix Corporation recommends creating a boot partition no larger than 75 MB to store these files.

Setting up a /swap Partition

This partition must have a capacity at least equal to twice the amount of physical RAM on the host.

Swap partitions are used to support virtual memory. Data is written to a swap partition when there is not enough physical RAM to store the data the system is processing. For example, if you have 1 GB of physical RAM, the swap partition must have at least 2 GB capacity.

Setting up the /var partition

The Scalix Message Store, the configuration files, and any language files are installed in the /var partition, in the /var/opt/scalix directories created during the installation process. This partition must be large enough to accommodate the future requirements of the Scalix Message Store. For example, 100 users using an average of 100 MB for every mailbox requires setting the size of the /var partition to approximately 10 GB.

Tip Some versions of Linux include a *Logical Volume Manager* (LVM). Scalix Corporation recommends using a LVM volume for the /var partition. This enables you to increase the size of the /var partition as needed, or to back up the Scalix Server, without having to shut down the system.

Red Hat Linux-specific Qualifications

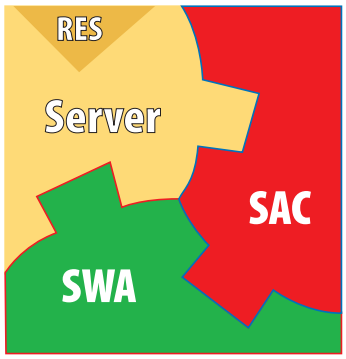
The system onto which you are installing Scalix Server is a dedicated messaging server. As a result, selecting **Everything** in the Package Group Selection window during the installation

of Red Hat Linux can severely reduce overall system performance. Installing a large number of packages causes excessive use of disk space and results in a number of unnecessary processes running on the system that can interfere with the efficiency, security, and scalability of the e-mail server. Scalix Corporation recommends installing only the package groups listed below. With the exception of Tomcat and JRE, these package groups contain all the required packages (RPMs) along with their respective software dependencies.

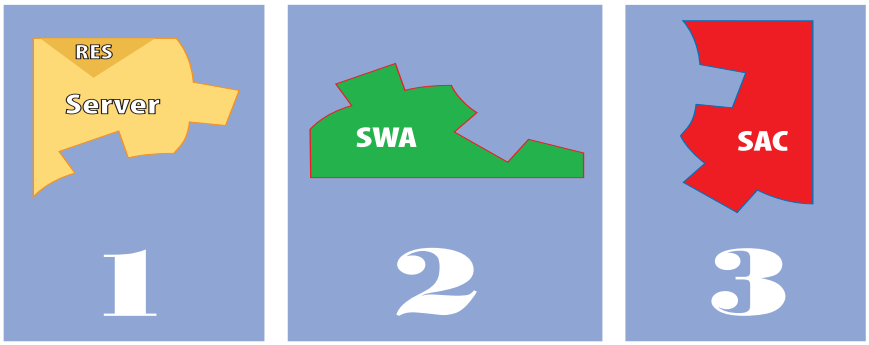
1. During the installation of Red Hat Linux, select *Customize selection of packages to be installed* and click **Next**.
2. When the *Package Group Selection* pane appears, select only the following package groups:
   - X Window System
   - KDE Desktop Environment or GNOME Desktop Environment (or both)
   - Graphical Internet
   - Text-based Internet
   - Server Configurations Tools
   - Network Servers (also, select Details, then select krb5-server)
   - Web Server
   - Development Tools
   - Kernel Development
   - Legacy Software Tools
   - Administration Tools
   - System Tools
3. You can now complete the installation.

Planning Your Scalix Component Deployment

Before you start the actual Scalix installation, you should plan the Scalix software deployment. Scalix utilizes up to three distinct components: the *Server* (and *Remote Execution Service*), the *Administration Console*, and *Scalix Web Access*. The following illustration shows your installation options: all Scalix components on a single host—



Or Scalix components on separate hosts.



You can install and configure the Scalix components in one of two arrangements:

- **Single-host mode:** In which all components are installed on a single host computer
- **Multi-host mode:** In which the separate components are on separate hosts

Both installation options are fully detailed in this guide. Whichever mode you pick, you can only have one instance (installation) of the Administration Console.

You should also determine the security requirements for your deployment, as the Scalix Installer enables you to configure Kerberos for secure communication between the Remote Execution Service and the Administration Console—if these components are installed on separate hosts.

Additional notes about a single-server installation

If you install all of the Scalix system components onto the same host computer, (single-host mode) you will need to install and configure the *Remote Execution Service*. However, because there is no data transmitted between the Scalix Administration Console and a Remote Execution Service instance over the network, you do not need to activate and configure Kerberos authentication.

Additional notes about a multi-host installation

In a multiple or remote Scalix server system, Scalix Corporation recommends that you configure Kerberos authentication so that data transmitted between the Administration Console and instances of the Remote Execution Service is encrypted. Before doing this, make sure you create a keytab file for the Administration Console Service and all instances of the Remote Execution Service. If necessary, securely copy the keytabs onto the respective systems hosting these services.

To enable and use a multi-host installation of Scalix, do the following:

- install the Scalix Administration Console separately, as described later in this guide.
- On each Scalix Server host in your network (not the Scalix Administration Console system), make sure you install the Remote Execution Service.
- If not already created, create a Kerberos keytab for the Remote Execution Service.

- Also, verify Scalix Server Directory Synchronization Agreements to ensure timely data synchronization between the servers in your environment. The default is 24 minutes.

See the *Scalix Administration Guide* for more information about Directory Synchronization Agreements, including Kerberos authentication.

What's Next

Having partitioned the host computer, installed Linux (and needed utilities), you can now install the Scalix software, as detailed in the following chapters. Each chapter covers a different mode, single host and multi-host, using either a GUI-based wizard or CLI.

Using the installer wizard

- "Installing Scalix on a Single Host" on page 23
- "Installing Scalix Components on Separate Hosts" on page 37

Using Command Line Interface

- "Installing, Upgrading and Uninstalling Scalix with CLI" on page 71

Installing Scalix on a Single Host

This chapter describes, in step-by-step detail, how to install the complete package of Scalix components onto a single host computer. This process is for both Scalix Community Edition and Scalix Enterprise Edition. (If you are installing Community Edition, you need to use this wizard or use CLI to install all the components onto a single host.)

If you are installing Scalix Enterprise Edition, you can follow this procedure, and you also have the option of installing Scalix components onto separate host computers, as detailed in the next chapter.

To verify that you've completed a successful installation, take advantage of the procedure detailed later in this chapter, "Confirming the Success of Your Scalix Installation" on page 33

Note	Make sure you read the Scalix Release Notes (on the CD ROM or tar.gz file) before you begin installing Scalix. There may be late changes, cautions, tips or qualifications you should know about.

Contents

This chapter includes the following information:

Installing the Scalix Software on a Single Host

To install Scalix components onto a prepared Linux host computer, start the Scalix Installer program and work through the Installation Wizard, as described in the following steps.

Tip You will have an opportunity to install JRE, Tomcat, and mod_jk during the Scalix installation as the installers are bundled with the Scalix package.

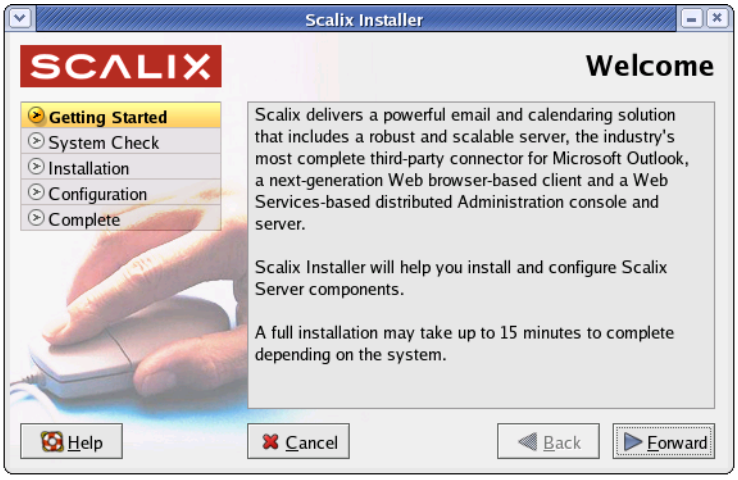
1. Log in to the target host computer as root.
2. Insert the Scalix Installation CD into the CD ROM drive.
   - Alternate: Change to the shared directory that contains Scalix installation files. If you downloaded a copy of the Scalix .tar file, you can copy it to a convenient directory on the host, then untar the archive and start the process.
3. If required, mount the CD ROM drive by entering this command:

   ```
   mount /mnt/cdrom
   ```

   ```
   cd /mnt/cdrom/
   ```
4. Enter this command:

   ```
   sh scalix-installer
   ```

   This starts the Scalix Installer Wizard, which (after a brief setup) displays the *Welcome* screen.



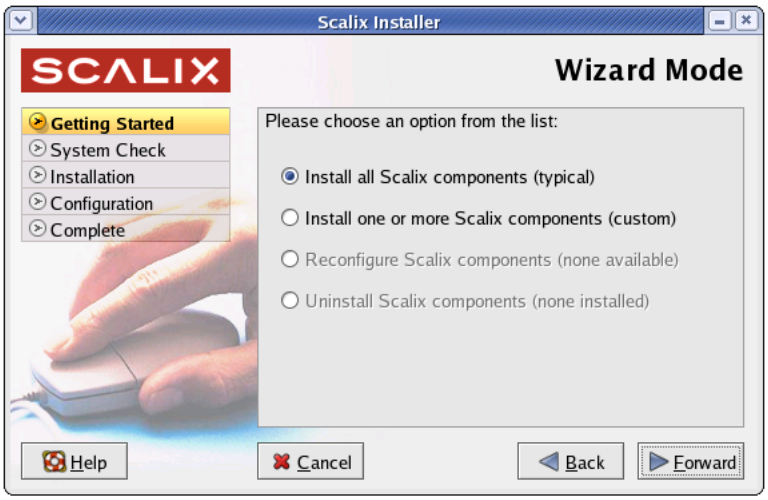
5. After reading the “Welcome” text, click **Forward**.

The *License Agreement* screen appears.

- Read through the license agreement.
- If you accept the conditions of installation and use, click the checkbox by "I have read and accept the above License Agreement"

6 Click the now-active **Forward** to proceed.

The *Wizard Mode* screen appears.

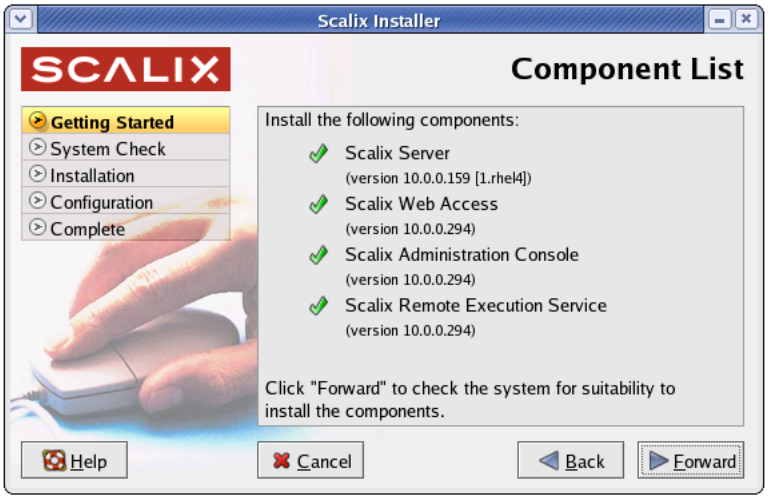


7 To initiate a single-server installation, select **Install all Scalix components**.

As a result, the four principal components—Scalix Server, Scalix Web Access, the Scalix Administration Console, and the Remote Execution Service (RES)— will all be installed on the target host computer.

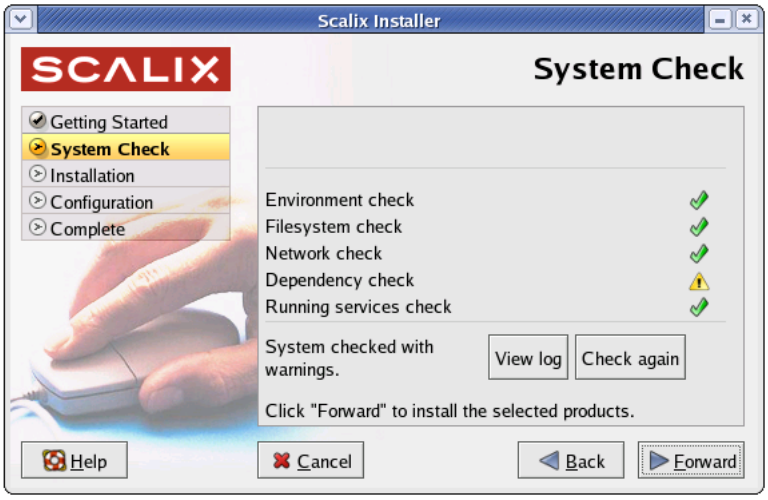
8 Click **Forward** to continue.

After a brief pause, the *Component List* screen appears.



9 Click **Forward** to proceed.

The *System Check* screen appears as the installer assesses the current software resources on this host to ensure that it can successfully complete the installation.



This task may require several minutes for completion.

10 Green checkmarks indicate a ready system, and you can click **Forward** to proceed.

If the system check fails to locate specific software applications or resources, one of two possible symbols will appear:

- A “stop sign” symbol indicates the absence of critical software. You cannot proceed with installation in this state.

- A “caution” symbol appears if critical software is missing that the installer will automatically add. This includes Java Runtime Environment and two related Tomcat packages.

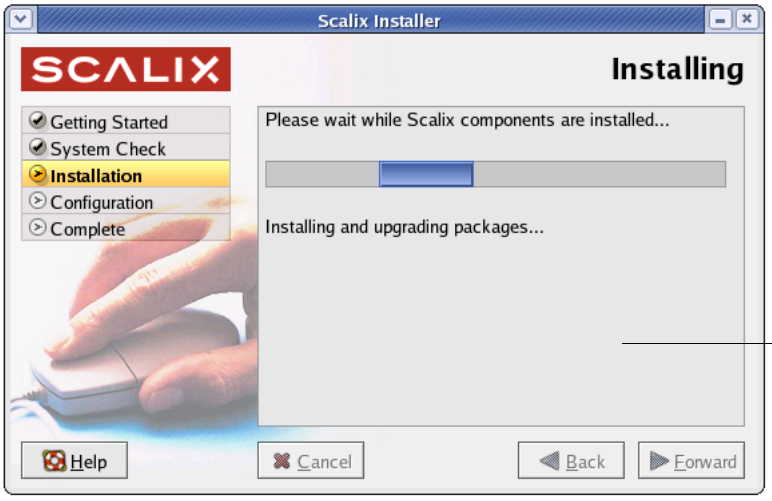
Alert	If the stop sign appears and the system check fails, you can review the log file to determine the cause, then make the needed adjustments. Once this is complete, you should be able to start and complete the Scalix installation.

11 If a system or dependency check results in an alert, click **View Log**. A dialog box reports on which system components are missing.

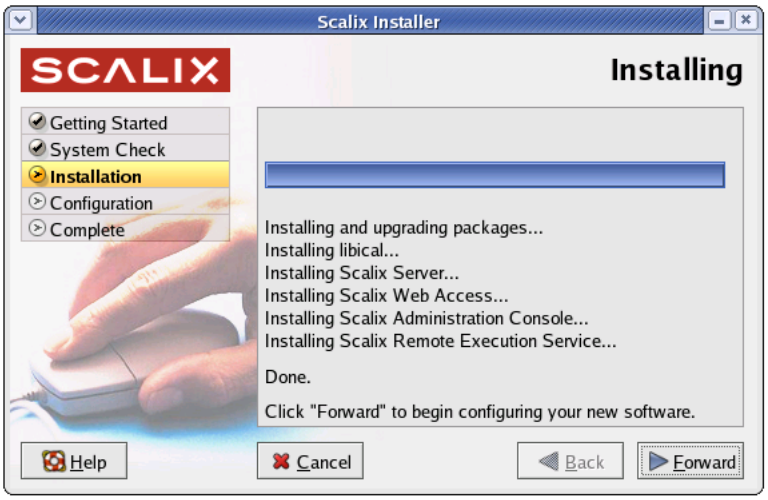
12 If the “cautions” report JRE or Tomcat as missing, you can proceed with installation, as the installer will install the missing packages in most cases.

13 Click **Forward** to continue.

The Scalix Installer begins installing the selected components (and any missing packages) and displays an *Installing (status)* screen.



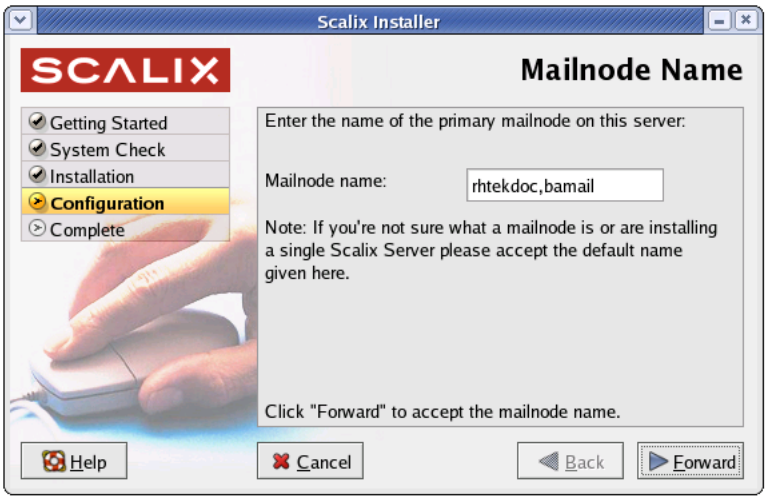
This process takes several minutes to complete. The wizard reports on which package is currently being installed. (If the previous system check did not find JRE or Tomcat, they also are installed at this time.)



When the installation is complete, a “Done” message appears in the status list, and the **Forward** button becomes active.

14 Click **Forward** to proceed.

The *Mailnode Name* screen appears.



15 If you are setting up a single-server system, Scalix recommends that you accept the default entries (hostname, domain of the host) and click **Forward**.

The *Email Address Format* screen appears.

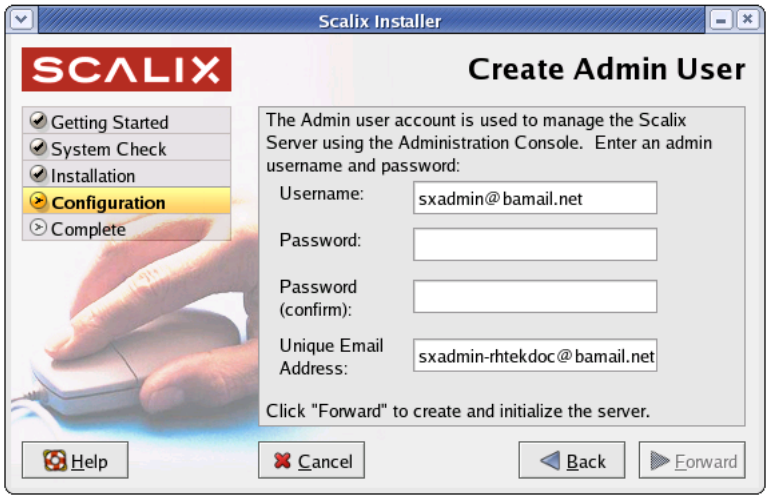
16 Use this screen to customize the following:

- **Domain name** of this server
- **Display name format** of all Scalix mail accounts
- **Internet address format** of all Scalix accounts

Examples of the Display Name and the Internet Address format are displayed in this window, depending on the selections you make in the pull-down menus.

17 Click **Forward** when you are finished.

The *Create Admin User* screen appears.



18 Make sure the default **Username** is correct, and edit it if it's not. (You can use almost any character or number in a user name.)

19 Enter the system administrator **Password** used to manage the Scalix Server.

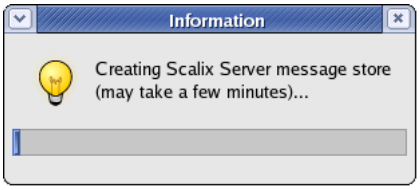
20 Confirm the new password text.

21 Either accept the default email address for this user in the **Unique Email Address** field, or change it accordingly.

Tip	Additional administrator accounts can be configured in Scalix after the installation process is complete. You can use Scalix administration resources (Console or CLI) to accomplish this.

22 Click **Forward**.

The Scalix Installer begins creating the message store. A separate Information dialog box appears (as shown below) and stays on-screen for the duration of the message store creation process.

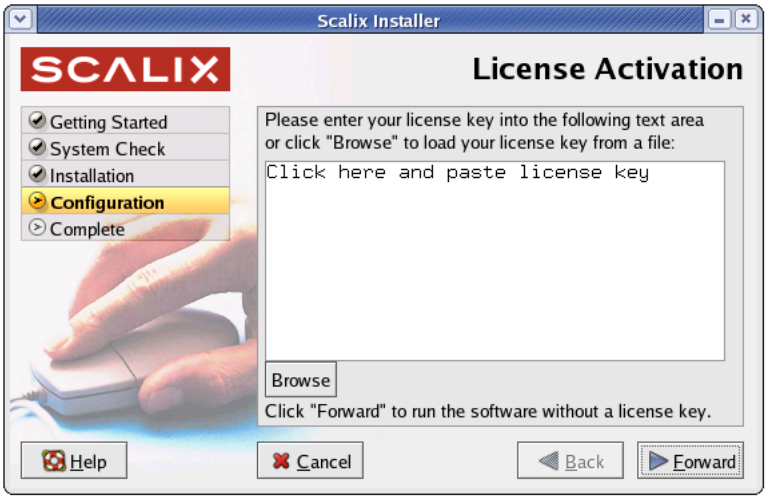


The message store setup may take several minutes or more.

Alert	Do not close the “Information: Creating Scalix Message Store” status dialog box (or any other active dialog boxes) by clicking the “X” button in the top-right corner of the dialog box. This causes the installation process to fail, and you will have to uninstall Scalix (using the Scalix Installer) before attempting to install Scalix again.

23 When this step is complete, click **Forward**.

The *License Activation* screen appears.



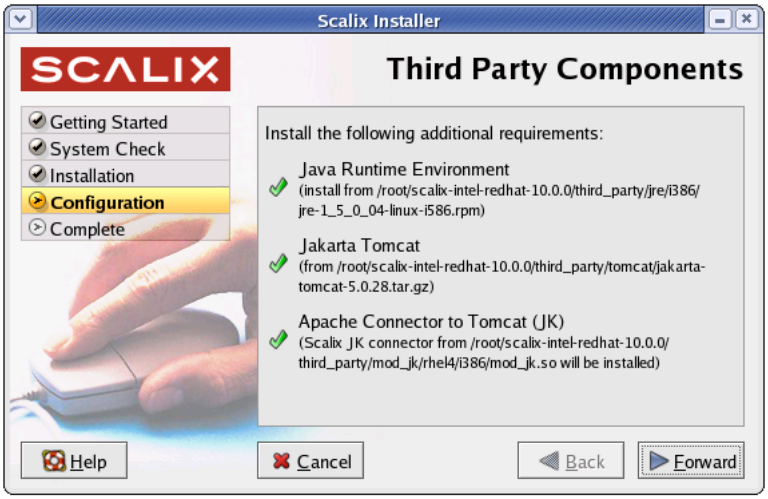
24 If you have a license to run Scalix as an Enterprise Edition system, you have two options for entering the license at this time:

- Use a text editor to cut-and-paste the text from any text file containing the exact license text.
- Click **Browse** to locate, open and import the contents of the file.
- After you enter a license, click **Forward** to continue.

25 If you want to run Scalix as a *Community Edition* system, you do not need a license. You can click **Forward.**

- When a warning dialog box asks you to confirm that “no license was entered”, click **OK**.

The *Third Party Components* screen now appears.



This confirms that Java Runtime Environment, Tomcat and the JK Tomcat/Apache connector are about to be installed in Scalix-related directories.

Information/Status dialog boxes may appear during installation of these components, and automatically close when finished.

26 When the third-party component installation is complete, click **Forward**.

The *Secure Communication* screen appears.

27 Enter a password that the Scalix Administration Console will use to authenticate against the LDAP server. This is a non-expiring password and is for a different account than the administrative login. Keep the password on file because you will need to enter it on each server if you upgrade to a multi-server setup at some point. If you lose the password, it is stored in /etc/opt/scalix/caa/scalix.res/config/psdata.

28 When the Secure Communication step is complete, click **Forward**.

The Scalix Installer displays the *Done* screen. Your installation was successful.

Click **OK** to exit the installation wizard.

Confirming the Success of Your Scalix Installation

After successfully installing Scalix on the host computer, you can perform the following tasks to ensure that Scalix Server and other components installed correctly.

1: Verify that Apache has started

To verify that the Apache server has started, do the following:

1. Log in to the Scalix host as root.
2. If this host runs Red Hat Linux, enter this command:

   ```
   ps –ef | grep httpd
   ```

3. If this host runs SUSE Linux, enter this command:

   ```
   ps –ef | grep apache
   ```

   If Apache is running on the host, a list of Apache processes appears.
4. Open a web browser and connect to http://localhost/

   The Apache Test Page should appear, confirming your Apache server is working.

2: Verifying network connections

To verify that network protocol access and connectivity is sufficient for the Scalix Server, do the following:

1. Log in to the Scalix host as root.
2. Open a command line window.
3. Ping any address outside the corporate firewall that returns ping requests.
4. Ping other messaging servers inside the corporate firewall.
5. From inside the firewall, ping the Scalix Server using the hostname.
6. From outside the firewall, ping the Scalix Server using the hostname.
7. Depending on the usage requirements for the Scalix Server, make sure the following ports (with port number) are open:
   - Scalix UAL (5729)
   - LDAP (389)
   - HTTP (80)
   - HTTPS (443)
   - SMTP (25)
   - POP (110)
   - IMAP (143)
   - UDP (5757)

- Kerberos - Single Sign-on only (88 and 749)

3: Testing Scalix Web Access installation

To ensure that Scalix Web Access is installed correctly, follow these steps:

1. Log in to the Scalix host as root.
2. Make sure the Tomcat service is started, by entering this command:

   ```
   ps –ef | grep tomcat
   ```

3. In your web browser, enter this URL in the Location field:

   ```
   http://[server-name]/webmail/
   ```

   The Scalix Login page should appear in the browser window.
4. If the Login page does not appear, open this Tomcat log file:

   ```
   $TOMCAT_HOME/logs/scalix-swa_log.<date>.txt
   ```

5. Review this log file for any recorded errors.
6. Log in to Scalix Web Access using the administrator username and password you previously configured during installation.
7. Once these tests are successfully complete, you can proceed.

4: Testing the Administration Console installation

To ensure that the Administration Console is installed correctly, follow these steps:

1. Log in to the Scalix host as root.
2. Make sure the Tomcat service is started, by entering this command:

   ```
   ps –ef | grep tomcat
   ```

3. In your web browser, enter this URL in the Location field:

   ```
   http://[server-name]/sac/
   ```

   The Scalix SAC Login page should appear.
4. If the Login page does not appear, open this log file:

   ```
   $TOMCAT_HOME/logs/caa.log file
   ```

5. Review this log file for any recorded errors.
6. Log in to the Administration Console using admin_username@server.domain.ext as the username.

   The Administration Console requires the Authentication ID value for the username field. The default Authentication ID for the administrator account is automatically created by the Scalix Installer during the installation of Scalix Server and is in this format:

   ```
   admin_username@server.domain.ext
   ```

   The administrator_username is the name you specified during installation.

7 To view the Authentication ID for the administrator account, enter:

```
omshowu -n admin_username
```

8 An additional option: You can modify the authentication ID for the administrator account and all other users using the Scalix Administration Console or by executing the ommodu command on the Scalix Server as follows:

```
ommodu -o username --authid new_authid
```

Getting Started with Scalix

Now that you've successfully installed and started up your new Scalix mail system, you can proceed to put it to work. This can be done with both of the following toolsets:

Scalix Administrative Console

1 Open a web browser and log in to this URL—

http://[localhost.domain.com]/sac

Alert Do not try to log in as the user sxqueryadmin or change its settings in any way. It is a system user and should not be changed.

2 When the Scalix Administrative Console (SAC) appears, you can complete a wide range of tasks that fall into these categories:

- Scalix user account management
- Group (public distribution list) management
- Starting and stopping server services and daemons
- Monitoring queues
- Changing a limited set of server configuration settings.

You can also perform some level of system monitoring, to assess the current state of processes and resources as well as any load being made on Scalix queues.

The Scalix Administration Console can be used for most day-to-day system administration tasks.

See the separate publication, *Scalix Administrative Console Guide*, for more information.

Scalix CLI

Open a terminal window and use the complete set of CLI commands and extensions to configure and customize your system. For server setup tasks, or for high-end, advanced maintenance, you should use the extensive Linux-based command line interface. The CLI provides a full set of commands, or you can use the CLI to set up and run all needed administrative scripts.

See the separate publication, *Scalix Administration Guide*, for more information.

Installing Scalix Components on Separate Hosts

This chapter provides complete instructions for separate installations of the primary components of Scalix, as part of an *Enterprise Edition* system:

- *Scalix Server* (and *Remote Execution Service* [RES])
- *Scalix Administration Console*
- *Scalix Web Access* components.

A reminder—installing Scalix components on separate hosts is not an option for Community Edition systems. Only Enterprise Edition system components can be distributed across several hosts.

Note Make sure you read the Scalix Release Notes (on the CD ROM or tar.gz file) before you begin installing Scalix Server. There may be late cautions, tips or qualifications you should know about.

Contents

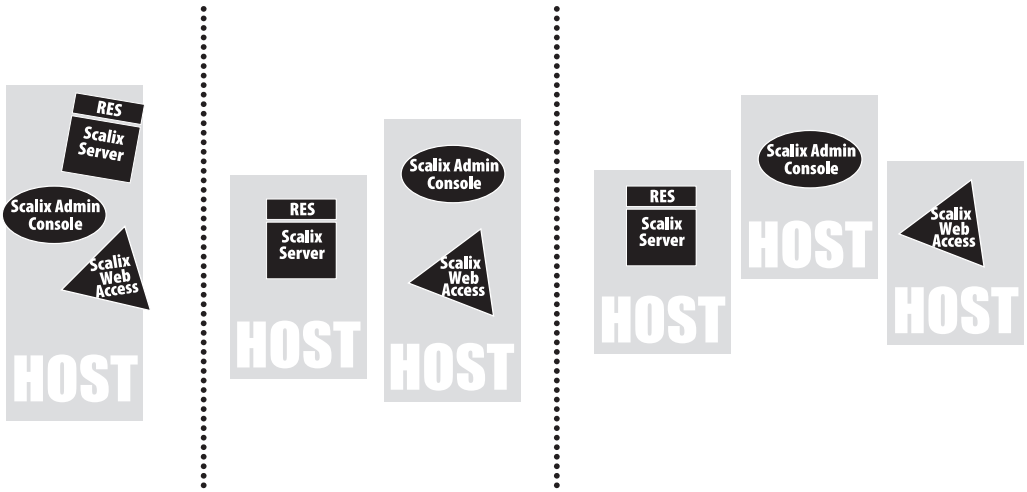
This chapter includes the following information:

Distributing Scalix Software Components to Separate Hosts

The Scalix software comes in three distinct “packages” that you can install on a single host or on separate hosts, if you prefer. Your options include combinations of the following components:

- Scalix Server (along with RES, a required server component)
- Scalix Administration Console
- Scalix Web Access server

As this illustration shows, you can distribute the components in several ways.



As the illustration shows, Scalix Server and RES, though discreet components, must be installed on the same host computer.

Depending on your preferences, you’ll need to run the installer on each computer, to distribute the components to the appropriate host computers. As each components’ installation involves variations in the installation process, we’ve detailed each installation separately, as listed here:

- “Installing the Scalix Server and RES Software” on page 39
- “Installing the Scalix Administration Console” on page 46
- “Installing the Scalix Web Access Server Software” on page 51

As noted previously, to get the most out of a multi-host installation of Scalix, install the Scalix Administration Console on its own host.

Notes Tomcat should be installed on the same hosts as each Scalix component, in whatever arrangement you choose.

Installing the Scalix Server and RES Software

We strongly recommend that you verify the existence of all required software resources on the host computer before starting this installation. The complete list is printed in “Pre-Installation Requirements” on page 11.

As noted previously, Scalix Server and RES, though discreet components, must be installed on the same host computer.

1. Log in to the target host computer as root.
2. Insert the Scalix Installation CD into the CD ROM drive.
   - Alternate: Change to the shared directory that contains Scalix installation files. If you downloaded a copy of the Scalix .tar file, you can copy it to a convenient directory on the host, then untar the archive and start the process.
3. If required, mount the CD ROM drive by entering this command:

   ```
   mount /mnt/cdrom
   ```

   ```
   cd /mnt/cdrom/
   ```
4. Enter this command:

   ```
   sh scalix-installer
   ```

   This starts the Installation Wizard, which displays the *Welcome* screen after a brief setup.
5. Read the introductory “Welcome” text, then click **Forward**.

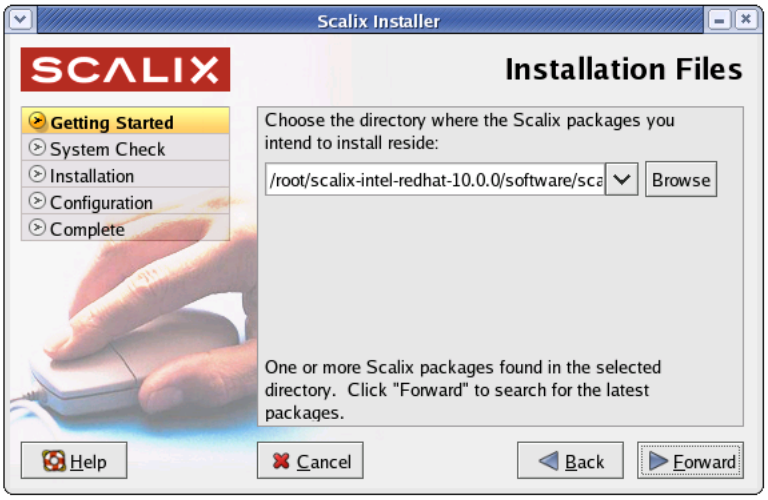
   The *License Agreement* screen appears.
   - Read through the license agreement.
   - If you accept the conditions of installation and use, click the checkbox by “I have read and accept the above License Agreement”
6. Click the now-active **Forward** to proceed.

   The *Wizard Mode* screen appears.

Tip For an illustration of this screen and other screens not shown in this procedure, turn to the corresponding step in “Installing Scalix on a Single Host” on page 23.

7. Select this option: **Install one or more Scalix components (custom)**
8. Click **Forward**.

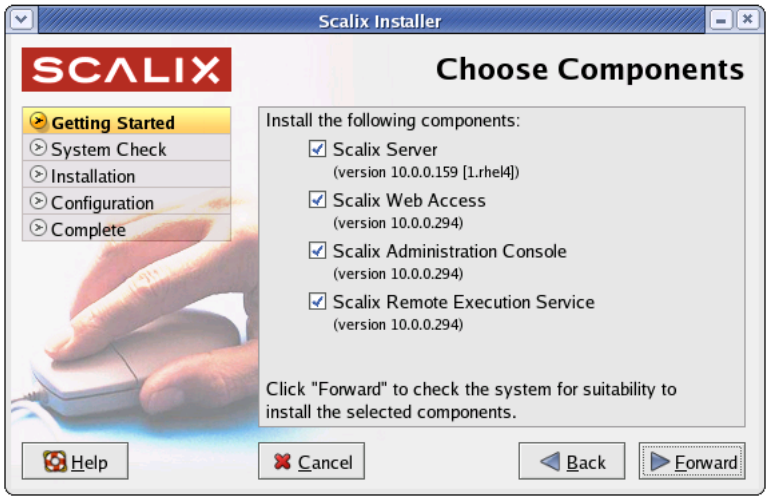
The *Installation Files* screen appears.



This screen confirms that the installation package has been located.

9 Click **Forward**.

The *Choose Components* screen appears showing all four components as ready to install.



10 Make sure that only the checkboxes by these two components are checked:

- Scalix Server
- Scalix Remote Execution Service (RES)

Alert	Do **not** install these components (Server and RES) on separate host computers.

11 Click **Forward** to continue.

The *System Check* screen appears, while the Scalix Installer assesses the current software resources on this host.

12 Green checkmarks indicate a ready system, at which time you can click **Forward** to proceed.

If the system check fails to locate specific software applications or resources, one of two possible symbols will appear:

- A “stop sign” symbol indicates the absence of critical software. You cannot proceed with installation in this state.
- A “caution” symbol appears if critical software is missing that the installer will automatically add. This includes Java Runtime Environment and two related Tomcat packages.

13 If a system or dependency check results in an alert, click **View Log**. A dialog box reports on which system components are missing.

14 If the “cautions” report JRE or Tomcat as missing, you can proceed with installation, as the installer will install the missing packages in most cases.

15 Click **Forward** to continue.

The Scalix Installer begins installing the selected components (and any missing packages) and displays an *Installing (status)* screen.

A series of Information/Status dialog boxes will appear, and auto-close when finished.

16 When installation is complete, click the now-active **Forward**.

The *Mailnode Name* screen appears.

17 Scalix recommends that you accept the default value (hostname, domain of the host) and click **Forward**.

Alert Changing the name of a mailnode requires several key changes to configuration files, and if this is done incorrectly, can cause severe problems with the Scalix Server.

The *Email Address Format* screen appears.

18 Use this screen to customize the following:

- **Domain name**
- **Display name format** of Scalix mail accounts
- The **Internet address format** of Scalix accounts.

Examples of a typical display name and Internet address formats are displayed in this window, depending on the selections you make in the pull-down menus.

19 Click **Forward** when you are finished.

The *Create Admin User* screen appears.

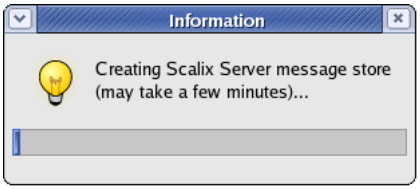
20 Enter the primary administrator **Username** and **Password** used to manage the Scalix Server.

21 Enter an email address for this user in the **Unique Email Address** field.

Tip	Additional administrator accounts can be configured in Scalix after the installation process is complete. You can use Scalix Administration Console or CLI to accomplish this.

22 Click **Forward**.

The Scalix Installer begins creating the message store. A separate *Information* dialog box appears and stays on-screen for the duration of the setup process.



Alert	The message store setup may take several minutes. Do not close the "Creating Scalix Message Store" status dialog box (or any other dialog box) by clicking the "X" button in the top-right corner of the dialog box. This causes the installation process to fail, and you will have to uninstall Scalix (using the Scalix Installer) before attempting to install Scalix again.

When the message store is complete, the *License Activation* screen appears.

23 If you have a license to run Scalix as an Enterprise Edition system, you have two options for inputting the license at this time:

- Use a text editor to cut-and-paste the text from any text file containing the exact license text.
- Click **Browse** to locate, open and import the contents of the file.
- After you enter a license, click **Forward** to continue.

24 If you want to run Scalix as a *Community Edition* system, you do not need a license. You can click **Forward.**

- When a warning dialog box asks you to confirm that "no license was entered", click **OK**.

The *JRE (Java Runtime Environment) Configuration* screen appears. You have two options:

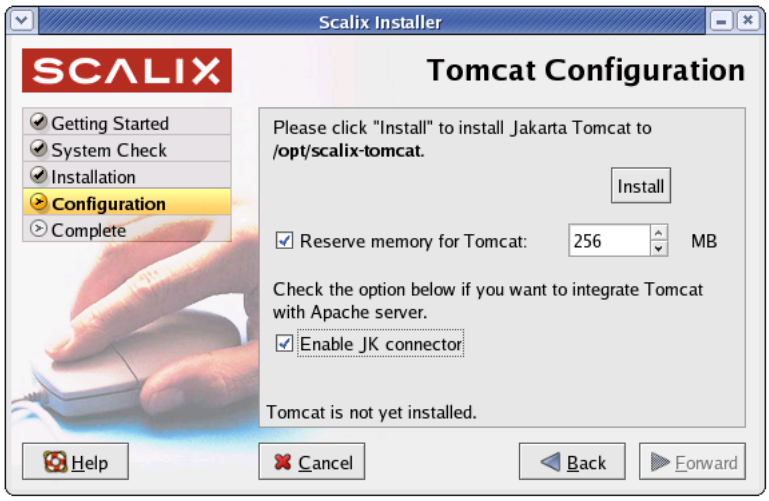
- Confirm the existence and directory pathway to the current installation, and skip this task.
- If not present on this host, install JRE at this time.

25 To install JRE using the Scalix Installer, look for the **Install** button in the JRE Configuration screen and click it.

- A dialog box appears listing the default installer package. Click **Install**, and when installation is complete, click **OK** to close this dialog box.

26 When JRE is confirmed as installed, click **Forward**.

The *Tomcat Configuration* screen appears.



You have two options:

- Confirm the existence and directory pathway to the current installation, and skip this task.
- If not present on this host, install Tomcat (and JK Connector) at this time.

27 To install Tomcat and the JK Connector using the Scalix Installer, click the check-box by **Enable JK Connector**.

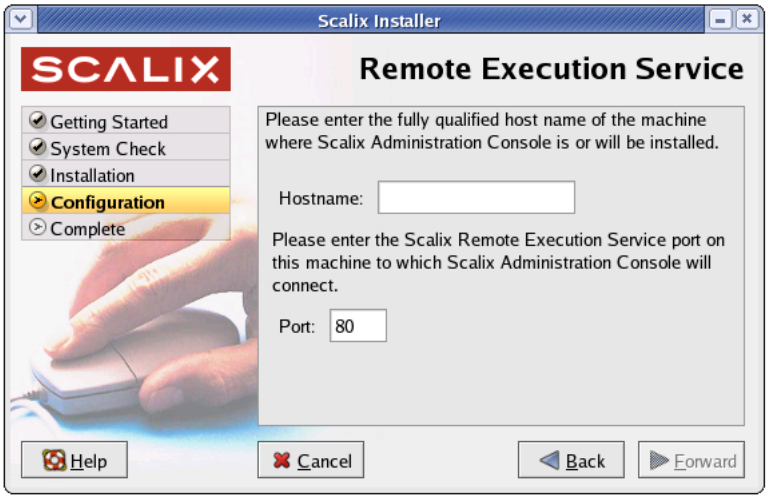
- You can modify the reserve memory settings, if needed.

28 Locate the **Install** button in the Tomcat Configuration screen and click it.

- A dialog box appears listing the default installer package. Click **Install**, and when installation is complete, click **OK** to close this dialog box.

29 When Tomcat is confirmed as installed, click **Forward**.

The *Remote Execution Service Configuration* screen appears.



30 Click in the Hostname field and type the name of the computer where the Scalix Administration Console (SAC) is to be installed.

31 Confirm the **Port** used for communication to the Scalix Administration Console.

32 Click **Forward**.

The first of two *Secure Communication* screens appear.

33 Enter a password that the Scalix Administration Console will use to authenticate against the LDAP server. This is a non-expiring password and is for a different account than the administrative login. Keep this password on file because you must enter the same exact same password on each server. If you lose the password, it is stored in /etc/opt/scalix/caa/scalix.res/config/psdata on the machine with the Scalix Administration Console.

34 When you are done, click **Forward**.

The second *Secure Communication* screen appears.

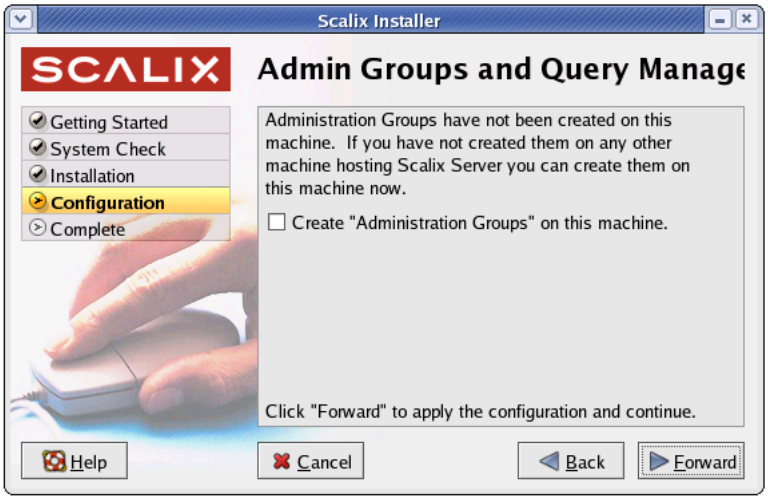
35 If you are not using Kerberos authentication between RES and Scalix Administration Console, click **Forward** to bypass this screen.

36 If you are utilizing Kerberos authentication between RES and SAC, you can do the following:

- Click the empty **Configure secure communications** checkbox.
- Click **Browse** to open a dialog box in which you can find and open the keytab file.
- Enter the fully qualified domain name of the KDC (Kerberos Distribution Center).
- Enter the Kerberos realm of your Scalix system, in ALL-CAP letters.

37 Click **Forward**.

The *Admin Groups and Query Manager* screen appears.



38 To create your Scalix administrative groups on this server (and not on the SAC host), click the checkbox by **Create Administrative Groups...**

Alert	If you install Scalix Admin Console (SAC) on a separate host from Scalix Server and RES, you need to create the Administrative Groups on the RES host. This can be done at this point during the Scalix/RES installation.

39 Click **Forward**.

When installation is finished, the *Done* screen appears. Your installation was successful.

40 Click **OK** to exit the installation wizard.

Installing the Scalix Administration Console

We strongly recommend that you verify the existence of all required software resources on the host computer before starting this installation. The complete list is printed in "Pre-Installation Requirements" on page 11.

Tip You will have an opportunity to install Tomcat, JRE and the JK Apache/Tomcat connector during the Scalix installation as the installers are bundled into the Scalix package. These packages are required for any host running SAC or SWA.

1. Log in to the target host computer as root.
2. Insert the Scalix Installation CD into the CD ROM drive.
   - Alternate: Change to the shared directory that contains Scalix installation files. If you downloaded a copy of the Scalix .tar file, you can copy it to a convenient directory on the host, then untar the archive and start the process.
3. If required, mount the CD ROM drive by entering this command:

   ```
   mount /mnt/cdrom
   ```

   ```
   cd /mnt/cdrom/
   ```
4. Enter this command:

   ```
   sh scalix-installer
   ```

   This starts the Scalix Installation Wizard, which displays the *Welcome* screen after a brief setup.
5. Read the introductory "Welcome" text, then click **Forward**.

   The *License Agreement* screen appears.
   - Read through the license agreement.
   - If you accept the conditions of installation and use, click the checkbox by "I have read and accept the above License Agreement"
6. Click the now-active **Forward** to proceed.

   The *Wizard Mode* screen appears.

Tip For an illustration of this screen and other screens not shown in this procedure, turn to the corresponding step in "Installing Scalix on a Single Host" on page 23.

7. Select this option: **Install one or more Scalix components (custom)**
8. Click **Forward**.

   The *Installation Files* screen appears.

   This screen confirms that the installation package has been located.
9. Click **Forward**.

   The *Choose Components* screen appears.

10 Click the checkbox by **Scalix Administration Console**.

11 Click **Forward** to continue.

The *System Check* screen appears, while the Scalix Installer assesses the current software resources on this host. This task may take several minutes to complete.

This task may require several minutes for completion.

12 Green checkmarks indicate a ready system, and you can click **Forward** to proceed.

If the system check fails to locate specific software applications or resources, one of two possible symbols will appear:

- A “stop sign” symbol indicates the absence of critical software. You cannot proceed with installation in this state.
- A “caution” symbol appears if critical software is missing that the installer will automatically add. This includes Java Runtime Environment and two related Tomcat packages.

13 If a system or dependency check results in an alert, click **View Log**. A dialog box reports on which system components are missing.

14 If the “cautions” report JRE or Tomcat as missing, you can proceed with installation, as the installer will install the missing packages in most cases.

15 Click **Forward** to continue.

The Scalix Installer begins installing the selected components (and any missing packages) and displays an *Installing (status)* screen.

This process will take several minutes to complete and this wizard will report on which package is currently being installed.

16 When installation is complete, click **Forward**.

The *JRE (Java Runtime Environment) Configuration* screen appears.

17 You have two options:

- Confirm the existence and directory pathway to the current installation, and skip this task.
- If not present on this host, install JRE at this time.

18 To install JRE using the Scalix Installer, look for the **Install** button in the JRE Configuration screen and click it.

- A dialog box appears listing the default installer package. Click **Install**, and when installation is complete, click **OK** to close this dialog box.

19 When JRE is confirmed as installed, click **Forward**.

The *Tomcat Configuration* screen appears.

You have two options:

- Confirm the existence and directory pathway to the current installation, and skip this task.
- If not present on this host, install Tomcat (and JK Connector) at this time.

20 To install Tomcat and the JK Connector using the Scalix Installer, click the check-box by **Enable JK Connector**.

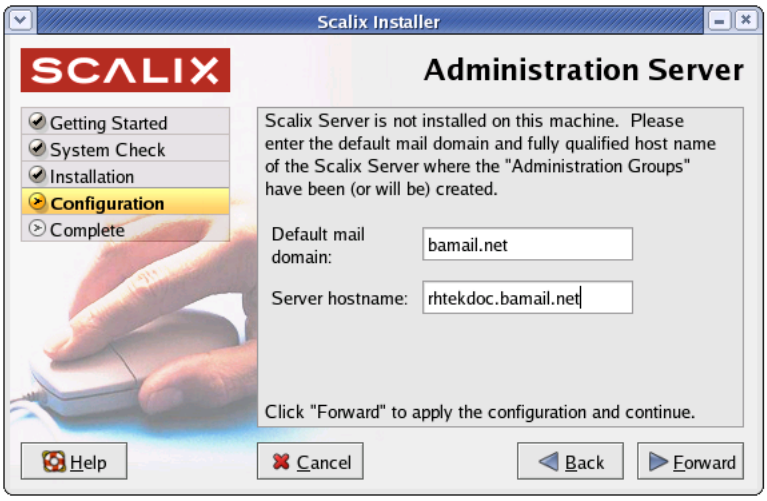
- You can modify the reserve memory settings, if needed.

21 Locate the **Install** button in the Tomcat Configuration screen and click it.

- A dialog box appears listing the default installer package. Click **Install**, and when installation is complete, click **OK** to close this dialog box.

22 When Tomcat is confirmed as installed, click **Forward**.

The *Administration Server* screen appears.



23 Make these entries pertaining to this host:

- The default mail domain (which you can edit if needed)
- The server hostname (as a fully qualified name)

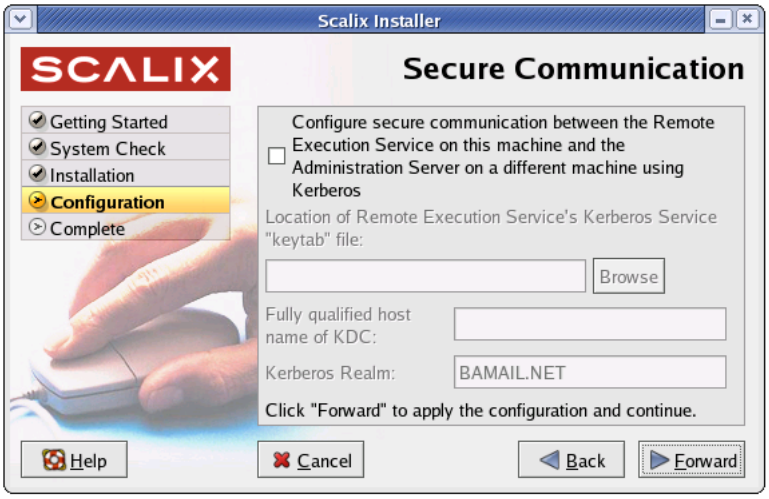
24 Click **Forward** to continue.

The first of two *Secure Communication* screens appear.

25 Enter a password that the Scalix Administration Console will use to authenticate against the LDAP server. This is a non-expiring password and is for a different account than the administrative login. Keep this password on file because you must enter the same exact same password on each server. If you lose the password, it is stored in /etc/opt/scalix/caa/scalix.res/config/psdata on the machine with the Scalix Administration Console.

26 When you are done, click **Forward**.

The second *Secure Communication* screen appears.

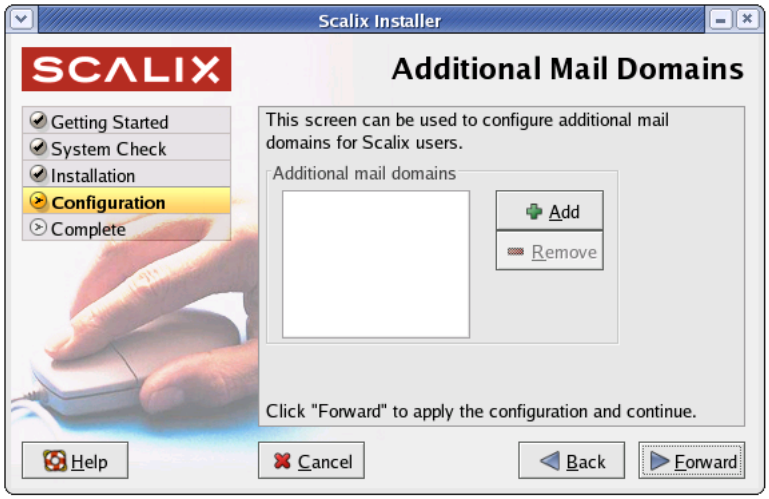


27 Make these entries, if you are configuring Kerberos authenticated connections:

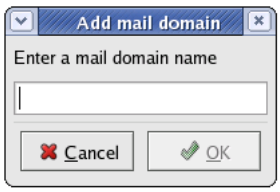
- Check the **Configure secure communication...** option to configure encrypted Kerberos communication between the Scalix Administration Console and all instances of the Remote Execution Service.
- Click **Browse** to locate the service keytab file for the Administration Console.
- Enter the **Fully qualified host** name of the KDC (Kerberos Distribution Center).
- Enter the **Kerberos Realm** (in UPPERCASE text).

28 Click **Forward** to continue.

The *Additional Mail Domains* screen appears.



- To add any other usable domains (that will help you create different e-mail addresses in the Administration Console), click **Add** and use the Add mail domains dialog box.



These domains will appears in a pull-down menu among the user account features in the Scalix Administrative Console.

Alert You cannot add new mail domains at this time unless they have been included in your Scalix license key.

29 Click **Forward**.

The *Done* screen appears, if the installation was successful.

30 Click **OK** to exit the installation wizard.

Installing the Scalix Web Access Server Software

To install Scalix components onto a prepared Linux host computer, start the Scalix Installer program and work through the Installation Wizard, as described in the following steps.

TIP You will have an opportunity to install JRE, Tomcat and the JK Apache/Tomcat connector during the Scalix installation as the installers were bundled into the Scalix package.

1. Log in to the target host computer as root.
2. Insert the Scalix Installation CD into the CD ROM drive.
   - Alternate: Change to the shared directory that contains Scalix installation files. If you downloaded a copy of the Scalix .tar file, you can copy it to a convenient directory on the host, then untar the archive and start the process.
3. If required, mount the CD ROM drive by entering this command:

   ```
   mount /mnt/cdrom
   ```

   ```
   cd /mnt/cdrom/
   ```
4. Enter this command:

   ```
   sh scalix-installer
   ```

   This starts the Installation Wizard, which displays the *Welcome* screen.
5. Read the introductory "Welcome" text, then click **Forward**.

   The *License Agreement* screen appears.
   - Read through the license agreement.
   - If you accept the conditions of installation and use, click the checkbox by "I have read and accept the above License Agreement"
6. Click the now-active **Forward** to proceed.

   The *Wizard Mode* screen appears.

Tip For an illustration of this screen and other screens not shown in this procedure, turn to the corresponding step in "Installing Scalix on a Single Host" on page 23.

7. Select this option: **Install one or more Scalix components**
8. Click **Forward**.

   The *Installation Files* screen appears.

   This screen confirms that the installation package has been located.
9. Click **Forward** to proceed.

   The *Choose Components* screen appears.
10. Click the checkbox by **Scalix Web Access**.
11. Click **Forward** to continue.

The *System Check* screen appears, while the Scalix Installer assesses the current software resources on this host.

This task may require several minutes for completion.

12 Green checkmarks indicate a ready system, and you can click **Forward** to proceed.

If the system check fails to locate specific software applications or resources, one of two possible symbols will appear:

- A “stop sign” symbol indicates the absence of critical software. You cannot proceed with installation in this state.
- A “caution” symbol appears if critical software is missing that the installer will automatically add. This includes Java Runtime Environment and two related Tomcat packages.

13 If a system or dependency check results in an alert, click **View Log**. A dialog box reports on which system components are missing.

14 If the “cautions” report JRE or Tomcat as missing, you can proceed with installation, as the installer will install the missing packages in most cases.

15 Click **Forward** to continue.

The Scalix Installer begins installing the selected components (and any missing packages) and displays an *Installing (status)* screen.

This process will take several minutes to complete and this wizard will report on which package is currently being installed. (If the system check did not find them, JRE, modjk and Tomcat will also be installed at this time.)

16 When installation is complete, click **Forward**.

The *JRE (Java Runtime Environment) Configuration* screen appears.

- Confirm the existence and directory pathway to the current installation, and skip this task.
- If not present on this host, install JRE at this time.

17 To install JRE using the Scalix Installer, look for the **Install** button in the JRE Configuration screen and click it.

- A dialog box appears listing the default installer package. Click **Install**, and when installation is complete, click **OK** to close this dialog box.

18 When JRE is confirmed as installed, click **Forward**.

The *Tomcat Configuration* screen appears. You have two options:

You have two options:

- Confirm the existence and directory pathway to the current installation, and skip this task.
- If not present on this host, install Tomcat (and JK Connector) at this time.

19 To install Tomcat and the JK Connector using the Scalix Installer, click the checkbox by **Enable JK Connector**.

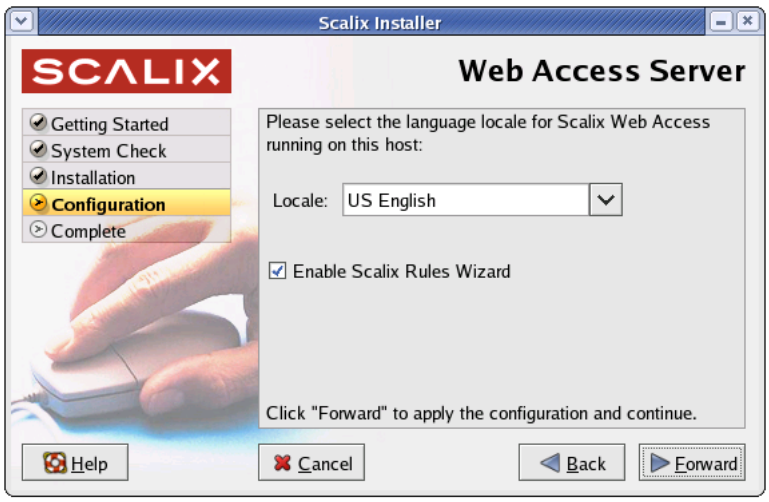
- You can modify the reserve memory settings, if needed.

20 Locate the **Install** button in the Tomcat Configuration screen and click it.

- A dialog box appears listing the default installer package. Click **Install**, and when installation is complete, click **OK** to close this dialog box.

21 When Tomcat is confirmed as installed, click **Forward**.

The *Web Access Server* screen appears.



22 Open the **Locale** menu and choose the primary language used by the majority of your Scalix Web Access users.

23 Determine whether you want the Scalix Rules Wizard active (for end-user benefit), or not. If you don't want it enabled, clear the **Enable Scalix Rules Wizard** check-box.

24 Click **Forward**.

The *Web Access Server (Continued)* screen appears.

A default mail domain is listed.

25 Change the **Default mail domain**, if needed.

26 Enter a **Server hostname** for this computer.

27 Click **Forward**.

The Scalix Installer configures Scalix Web Access and when it is finished, displays the *Done* screen, if the installation was successful.

28 Click **OK** to exit the installation wizard.

Confirming the Success of Your Scalix Installation

After successfully installing Scalix on the host computer, you can perform the following tasks to ensure that Scalix Server and other components installed correctly.

1: Verify that Apache has started

To verify that the Apache server has started, do the following:

1. Log in to the Scalix host as root.
2. If this host runs Red Hat Linux, enter this command:

   ```
   ps –ef | grep httpd
   ```

3. If this host runs SUSE Linux, enter this command:

   ```
   ps –ef | grep apache
   ```

   If Apache is running on the host, a list of Apache processes appears.
4. Open a web browser and connect to http://localhost/

   The Apache Test Page should appear, confirming your Apache server is working.

2: Verifying network connections

To verify that network protocol access and connectivity is sufficient for the Scalix Server, do the following:

1. Log in to the Scalix host as root.
2. Open a command line window.
3. Ping any address outside the corporate firewall that returns ping requests.
4. Ping other messaging servers inside the corporate firewall.
5. From inside the firewall, ping the Scalix Server using the hostname.
6. From outside the firewall, ping the Scalix Server using the hostname.
7. Depending on the usage requirements for the Scalix Server, make sure the following ports (with port number) are open:
   - Scalix UAL (5729)
   - LDAP (389)
   - HTTP (80)
   - HTTPS (443)
   - SMTP (25)
   - POP (110)
   - IMAP (143)
   - UDP (5757)

- Kerberos - Single Sign-on only (88 and 749)

3: Testing Scalix Web Access installation

To ensure that Scalix Web Access is installed correctly, follow these steps:

1. Log in to the Scalix host as root.
2. Open a command line window.
3. Make sure the Tomcat service is started, by entering this command:

   ```
   ps –ef | grep tomcat
   ```

4. In your web browser, enter this URL in the Location field:

   ```
   http://[server_name]/webmail/
   ```

   The Scalix Login page should appear in the browser window.

5. If the Login page does not appear, open this Tomcat log file:

   ```
   $TOMCAT_HOME/logs/scalix-swa_log.<date>.txt
   ```

6. Review this log file for any recorded errors.
7. Log in to Scalix Web Access using the administrator username and password you previously configured during installation.
8. Once these tests are successfully complete, you can proceed.

4: Testing the Administration Console installation

To ensure that the Administration Console is installed correctly, follow these steps:

1. Log in to the Scalix host as root.
2. Open a command line window.
3. Make sure the Tomcat service is started, by entering this command:

   ```
   ps –ef | grep tomcat
   ```

4. In your web browser, enter this URL in the Location field:

   ```
   http://[server_name]/sac/
   ```

   The Scalix SAC Login page should appear.

5. If the Login page does not appear, open this log file:

   ```
   $TOMCAT_HOME/logs/caa.log file
   ```

6. Review this log file for any recorded errors.
7. Log in to the Administration Console using admin_username@server.domain.ext as the username.

   The Administration Console requires the Authentication ID value for the username field. The default Authentication ID for the administrator account is automatically created by the Scalix Installer during the installation of Scalix Server and is in this format:

```
admin_username@server.domain.ext
```

The administrator_username is the name you specified during installation.

8 To view the Authentication ID for the administrator account, enter:

```
omshowu -n admin_username
```

9 An additional option: You can modify the authentication ID for the administrator account and all other users using the Scalix Administration Console or by executing the ommodu command on the Scalix Server as follows:

```
ommodu -o username --authid new_authid
```

Getting Started with Scalix

Now that you've successfully installed and started up your new Scalix mail system, you can proceed to put it to work. This can be done with both of the following toolsets:

Scalix Administrative Console

1 Open a web browser and log in to this URL—

http://[localhost.domain.com]/sac

Alert Do not try to log in as the user sxqueryadmin or change its settings in any way. It is a system user and should not be changed.

2 When the Scalix Administrative Console (SAC) appears, you can complete a wide range of tasks that fall into these categories:

- Scalix user account management
- Group (public distribution list) management
- Starting and stopping server services and daemons
- Monitoring queues
- Changing a limited set of server configuration settings.

You can also perform some level of system monitoring, to assess the current state of processes and resources as well as any load being made on Scalix queues.

The Scalix Administration Console can be used for most day-to-day system administration tasks.

See the separate publication, *Scalix Administrative Console Guide*, for more information.

Scalix CLI

Open a terminal window and use the complete set of CLI commands and extensions to configure and customize your system. For server setup tasks, or for high-end, advanced maintenance, you should use the extensive Linux-based command line interface. The CLI provides a full set of commands, or you can use the CLI to set up and run all needed administrative scripts.

See the separate publication, *Scalix Administration Guide*, for more information.

Reconfiguring Scalix with the Installer

You can reconfigure the Scalix server (the entirety or individual components) with Scalix CLI or with Scalix Administration Console, but a few efficient tasks can be accomplished with the “reconfiguration” process built into the Scalix installer.

The Scalix installer can be used to reconfigure key settings in Scalix RES, SAC or SWA. (Reconfiguring the Scalix server itself is complex enough to require the use of the full range of CLI commands, depending on the task you want to perform.)

If Scalix is on a single host, you can run the installer once, to efficiently re-configure all the components. Or, if you’ve installed the components on separate hosts, you can run the installer on each system, choose the selected components, and configure them separately.

Contents

This chapter details the procedure for using the installer to adjust:

- Scalix components (in separate processes):
- Scalix Remote Execution Service
- Scalix Administration Console
- Scalix Web Access

In every instance of reconfiguration, you’ll be given the opportunity to reinstall JRE, Tomcat and the JK Tomcat/Apache connector, if you choose. (This is optional.)

Reconfiguring Scalix RES

Tip You will have an opportunity to reinstall Tomcat, JRE and JK Connector during the Scalix reconfiguration as a "third party" installer is bundled into the Scalix package. These packages are required for any host running SAC or SWA.

1. Log in to the target host computer as root.
2. Insert the Scalix Installation CD into the CD ROM drive.
   - Alternate: Change to the shared directory that contains Scalix installation files. If you downloaded a copy of the Scalix .tar file, you can copy it to a convenient directory on the host, then untar the archive and start the process.
3. If required, mount the CD ROM drive by entering this command:

   ```
   mount /mnt/cdrom
   ```

   ```
   cd /mnt/cdrom/
   ```
4. Enter this command:

   ```
   sh scalix-installer
   ```

   This starts the Scalix Installation Wizard, which displays the *Welcome* screen after a brief setup.
5. Read the introductory "Welcome" text, then click **Forward**.

   The *License Agreement* screen appears.
   - Read through the license agreement.
   - If you accept the conditions of installation and use, click the checkbox by "I have read and accept the above License Agreement"
6. Click the now-active **Forward** to proceed.

   The *Wizard Mode* screen appears.

Tip For an illustration of this screen and other screens not shown in this procedure, turn to the corresponding step in "Installing Scalix on a Single Host" on page 23.

7. Select this option: **Reconfigure Scalix Components.**

   This option allows you to specify one or more Scalix components to reconfigure on the target host on the next wizard screen. (This does not include Scalix server.)
8. Click **Forward**.

   The *Reconfigure Components* screen appears.
9. Select **Scalix Remote Execution Service**.
10. Click **Forward**.

    The *JRE (Java Runtime Environment) Configuration* screen appears. You have two options:

- Confirm the existence and directory pathway to the current installation, and skip this task.
- If not present on this host, install JRE at this time.

11 To install JRE using the Scalix Installer, look for the **Install** button in the JRE Configuration screen and click it.

- A dialog box appears listing the default installer package. Click **Install**, and when installation is complete, click **OK** to close this dialog box.

12 When JRE is confirmed as installed, click **Forward**.

The *Tomcat Configuration* screen appears. You have the following options:

You have two options:

- Confirm the existence and directory pathway to the current installation, and skip this task.
- If not present on this host, install Tomcat (and JK Connector) at this time.

13 To install Tomcat and the JK Connector using the Scalix Installer, click the checkbox by **Enable JK Connector**.

- You can modify the reserve memory settings, if needed.

14 Locate the **Install** button in the Tomcat Configuration screen and click it.

- A dialog box appears listing the default installer package. Click **Install**, and when installation is complete, click **OK** to close this dialog box.

15 When Tomcat is confirmed as installed, click **Forward**.

The *Remote Execution Server* screen appears.

16 Make these entries pertaining to this host:

- The **Hostname** (an automatic entry, which you can edit if needed)
- The **Port** number (also an automatic entry, which you can edit)

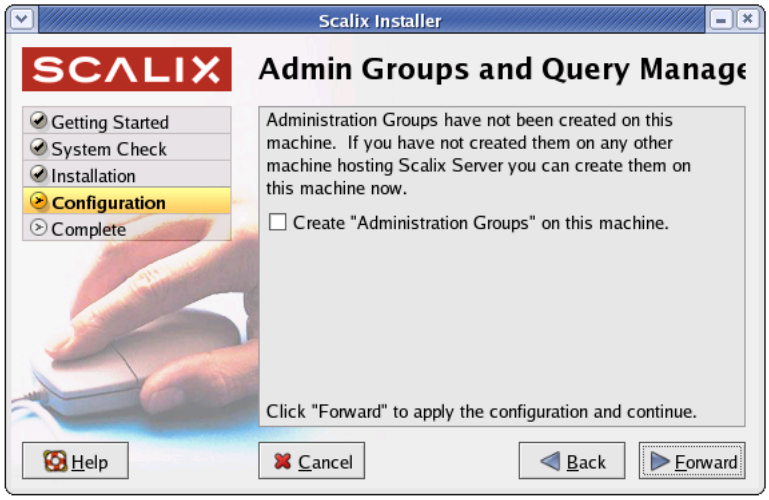
17 Click **Forward** to continue.

The *Secure Communication* screen appears.

18 Enter a password that the Scalix Administration Console will use to authenticate against the LDAP server. This is a non-expiring password and is for a different account than the administrative login. Keep this password on file because you must enter the same exact same password on each server. If you lose the password, it is stored in /etc/opt/scalix/caa/scalix.res/config/psdata on the machine with the Scalix Administration Console.

19 When you have entered and confirmed the password, click **Forward**.

The *Admin Groups and Query Management* screen appears.



- If you want to store your Scalix administration groups on this host, click the checkbox by “Create Administration Groups on this machine”.

20 Click **Forward**.

The *Done* screen appears, if the reconfiguration was successful.

21 Click **OK** to exit the installation wizard.

Reconfiguring Scalix Administration Console (SAC)

Tip You will have an opportunity to reinstall Tomcat, JRE and JK connector during the Scalix reconfiguration as an installer was bundled into the Scalix package. These packages are required for any host running SAC or SWA.

1. Log in to the target host computer as root.
2. Insert the Scalix Installation CD into the CD ROM drive.
   - Alternate: Change to the shared directory that contains Scalix installation files. If you downloaded a copy of the Scalix .tar file, you can copy it to a convenient directory on the host, then untar the archive and start the process.
3. If required, mount the CD ROM drive by entering this command:

   ```
   mount /mnt/cdrom
   ```

   ```
   cd /mnt/cdrom/
   ```
4. Enter this command:

   ```
   sh scalix-installer
   ```

   This starts the Scalix Installation Wizard, which displays the *Welcome* screen after a brief setup.
5. Read the introductory "Welcome" text, then click **Forward**.

   The *License Agreement* screen appears.
   - Read through the license agreement.
   - If you accept the conditions of installation and use, click the checkbox by "I have read and accept the above License Agreement"
6. Click the now-active **Forward** to proceed.

   The *Wizard Mode* screen appears.

Tip For an illustration of this screen and other screens not shown in this procedure, turn to the corresponding step in "Installing Scalix on a Single Host" on page 23.

7. Select this option: **Reconfigure Scalix Components.**

   This option allows you to specify one or more Scalix components to reconfigure on the target host on the next wizard screen. (This does not include Scalix server.)
8. Click **Forward**.

   The *Reconfigure Components* screen appears.
9. Select **Scalix Administration Console**.
10. Click **Forward**.

    The *JRE (Java Runtime Environment) Configuration* screen appears. You have two options:

- Confirm the existence and directory pathway to the current installation, and skip this task.
- If not present on this host, install JRE at this time.

11 To install JRE using the Scalix Installer, look for the **Install** button in the JRE Configuration screen and click it.

- A dialog box appears listing the default installer package. Click **Install**, and when installation is complete, click **OK** to close this dialog box.

12 When JRE is confirmed as installed, click **Forward**.

The *Tomcat Configuration* screen appears. You have the following options:

- Confirm the existence and directory pathway to the current installation, and skip this task.
- If not present on this host, install Tomcat (and JK Connector) at this time.

13 To install Tomcat and the JK Connector using the Scalix Installer, click the checkbox by **Enable JK Connector**.

- You can modify the reserve memory settings, if needed.

14 Locate the **Install** button in the Tomcat Configuration screen and click it.

- A dialog box appears listing the default installer package. Click **Install**, and when installation is complete, click **OK** to close this dialog box.

15 When Tomcat is confirmed as installed, click **Forward**.

The *Administration Server* screen appears.

16 Make these entries pertaining to this host:

- The default mail domain (which you can edit if needed)
- The server hostname (as a fully qualified name)

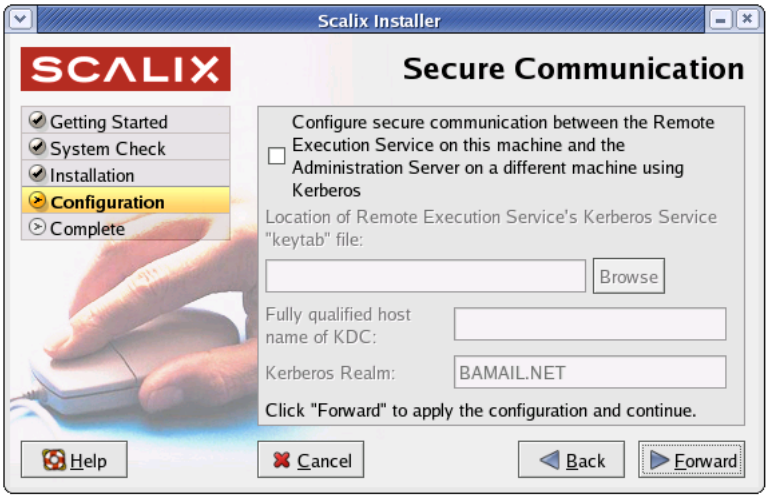
17 Click **Forward** to continue.

The *Secure Communication* screen appears.

18 Enter a password that the Scalix Administration Console will use to authenticate against the LDAP server. This is a non-expiring password and is for a different account than the administrative login. Keep this password on file because you must enter the same exact same password on each server. If you lose the password, it is stored in /etc/opt/scalix/caa/scalix.res/config/psdata on the machine with the Scalix Administration Console.

19 When you have entered and confirmed the password, click **Forward**.

A second *Secure Communication* screen appears.

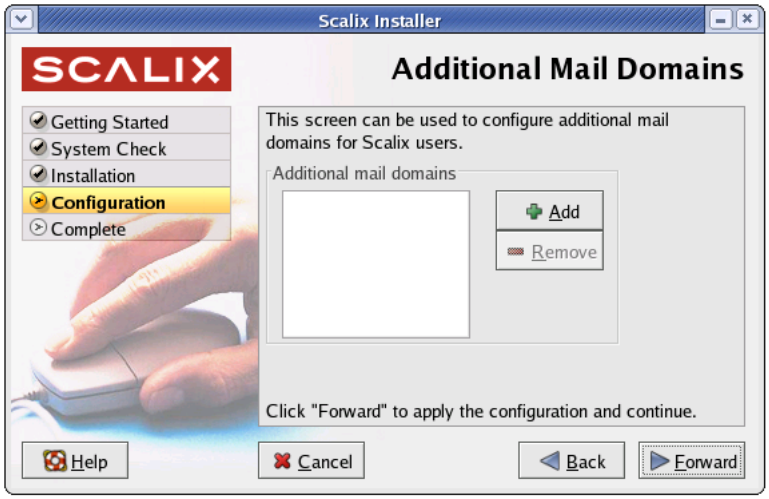


20 Make these entries, if you are configuring Kerberos authenticated connections:

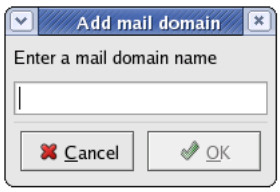
- Check the **Configure secure communication...** option to configure encrypted Kerberos communication between the Scalix Administration Console and all instances of the Remote Execution Service.
- Click **Browse** to locate the service keytab file for the Administration Console.
- Enter the **Fully qualified host** name of the KDC (Kerberos Distribution Center).
- Enter the **Kerberos Realm** (in UPPERCASE text).

21 Click **Forward** to continue.

The *Additional Mail Domains* screen appears.



- To add any other usable domains (that will help you create different e-mail addresses in the Administration Console), click Add and use the Add mail domains dialog box.



These domains will appears in a pull-down menu among the user account features in the Scalix Administrative Console.

Alert You cannot add new mail domains at this time unless they have been included in your Scalix license key.

22 Click **Forward**.

The *Done* screen appears, if the reconfiguration was successful.

23 Click **OK** to exit the installation wizard.

Reconfiguring Scalix Web Access (SWA)

Tip You will have an opportunity to reinstall Tomcat, JRE and JK connector during the Scalix reconfiguration as the installers were bundled into the Scalix package. These packages are required for any host running SAC or SWA.

1. Log in to the target host computer as root.
2. Insert the Scalix Installation CD into the CD ROM drive.
   - Alternate: Change to the shared directory that contains Scalix installation files. If you downloaded a copy of the Scalix .tar file, you can copy it to a convenient directory on the host, then untar the archive and start the process.
3. If required, mount the CD ROM drive by entering this command:

   ```
   mount /mnt/cdrom
   ```

   ```
   cd /mnt/cdrom/
   ```
4. Enter this command:

   ```
   sh scalix-installer
   ```

   This starts the Scalix Installation Wizard, which displays the *Welcome* screen after a brief setup.
5. Read the introductory "Welcome" text, then click **Forward**.

   The *License Agreement* screen appears.
   - Read through the license agreement.
   - If you accept the conditions of installation and use, click the checkbox by "I have read and accept the above License Agreement"
6. Click the now-active **Forward** to proceed.

   The *Wizard Mode* screen appears.

Tip For an illustration of this screen and other screens not shown in this procedure, turn to the corresponding step in "Reconfiguring Scalix with the Installer" on page 59.

7. Select this option: **Reconfigure Scalix Components.**

   This option allows you to specify one or more Scalix components to reconfigure on the target host on the next wizard screen. (This does not include Scalix server.)
8. Click **Forward**.

   The *Installation Files* screen appears.

   This screen confirms that the all-in-one installation package has been located.
9. Click **Forward**.

   The *Choose Components* screen appears.
10. Click the checkbox by **Scalix Web Access**.

11 Click **Forward** to continue.

The *JRE (Java Runtime Environment) Configuration* screen appears. You have two options:

- Confirm the existence and directory pathway to the current installation, and skip this task.
- If not present on this host, install JRE at this time.

12 To install JRE using the Scalix Installer, look for the **Install** button in the JRE Configuration screen and click it.

- A dialog box appears listing the default installer package. Click **Install**, and when installation is complete, click **OK** to close this dialog box.

13 When JRE is confirmed as installed, click **Forward**.

The *Tomcat Configuration* screen appears. You have the following options:

- Confirm the existence and directory pathway to the current installation, and skip this task.
- If not present on this host, install Tomcat (and JK Connector) at this time.

14 To install Tomcat and the JK Connector using the Scalix Installer, click the checkbox by **Enable JK Connector**.

- You can modify the reserve memory settings, if needed.

15 Locate the **Install** button in the Tomcat Configuration screen and click it.

- A dialog box appears listing the default installer package. Click **Install**, and when installation is complete, click **OK** to close this dialog box.

16 When Tomcat is confirmed as installed, click **Forward**.

The *Web Access Server* screen appears.

17 Open the **Locale** menu and choose the primary language used by the majority of your Scalix Web Access users.

18 Click **Forward**.

The *Web Access Server (Continued)* screen appears.

A default mail domain is listed.

- Change the **Default mail domain**, if needed.
- Enter a **Server hostname** for this computer.

19 Click **Forward**.

The *Done* screen appears, if the reconfiguration was successful.

20 Click **OK** to exit the installation wizard.

Installing, Upgrading and Uninstalling Scalix with CLI

This chapter describes, in step-by-step detail, the use of Scalix CLI (command line interface) in the following task-specific sections: S

Installing Scalix onto a Single Host with CLI

If you obtained a copy of the Scalix installation package from another source (other than Scalix or the Scalix CD), make sure it is stored in /usr/src before starting.

Tip Before you begin this task, h ave a .txt file containing the Scalix license key text stored in a convenient directory

1. Log in to the host computer as root.
2. Open a terminal window.
3. To start the installer, enter:

   [*directory_pathway*]/scalix-installer

   - Add a "--cli" extension if this host is running Xserver.

   The Scalix License Agreement scrolls on-screen in readable portions.
4. When you have read the entire agreement, you are prompted to accept it. Type "Yes" and press **Enter**, to proceed with installation.

   The actions menu appears, as shown here:

   ```
   Please choose an action from the list:
   [1] Install all Scalix components (typical)
   [2] Install one or more Scalix components (custom)
   ```
5. At this prompt:

   ```
   -> Please enter your choice [1]:
   ```

   Type "1" and press **Enter**.
6. After the installation components are located and listed, you are prompted:

   ```
   -> Do you want to continue installing the packages? (yes/no) [yes]:
   ```

   As "Yes" is the default, press **Enter**.
7. After a series of checks are completed, you may see this question:

   ```
   -> There were warnings during the system checks, are you sure you
   want to continue with installation? (yes/no/check again) [no]:
   ```

   As this most likely is a "dependency warning", you can type "Yes" and press **Enter**.

Tip Typing "Yes" will permit the installer to add missing accessory software (the "dependencies" needed by Scalix) that are not present on this host.

   The installation now begins, and status messages record the progress.
8. When installation is done, this prompt appears:

   ```
   -> Enter the name of the primary mailnode on this server
   [<server_name>,scalix]:
   ```

9 Press **Enter** to accept the default entry.

10 At this prompt:

```
-> Domain name [scalix.admin]:
```

- If the default entry is acceptable, press **Enter**.
- If the default entry is wrong, type the domain name in the suggested format, and press **Enter**.

A list of four display name formats appears.

11 Review the list, and at this prompt:

```
-> Please enter your choice [1]:
```

Type the number that represents the preferred display name format and press **Enter**.

A list of email (Internet) address formats appears.

12 Review this list, and at the prompt:

```
-> Please enter your choice [1]:
```

Type the number that represents the preferred email address format and press Enter.

You'll now be prompted for information about the primary administrative account for Scalix. "sxadmin@[fqdn]" is the default user name which you can edit or replace with a login ID of your choosing.

13 At this prompt:

```
-> Username [sxadmin@<fqdn>]:
```

Press **Enter** to accept the default user name.

14 At this prompt:

```
-> Enter password:
```

Type a password for the admin user account and press **Enter**.

15 At this prompt:

```
-> Confirm password:
```

Re-type the admin user password and press **Enter**.

16 At this prompt:

```
-> Unique Email Address [sxadmin-postoffice@scalix.admin]:
```

Press **Enter** to accept the default email address, which automatically applies the domain name, admin user name, and display name format.

The installer now configures the server.

17 After the server has been started, you are prompted for the location of the Scalix license text file:

```
-> Enter the location of your license key file or enter "None" to
run the server without a license []:
```

Type the full directory pathway and file name at the prompt and press **Enter**.

- If the pathway or file name are wrong, you'll be warned and prompted again for the pathway and name.

After the license is imported and validated, the installer will separately install Java Runtime Environment and Tomcat (including the JK Tomcat/Apache connector), then finish the configuration of Scalix.

18 Now the installer prompts for a non-expiring password that the Scalix Administration Console can use to authenticate against the LDAP server. This password must be different from the administrative login.

```
Please enter a password that will be used by the Scalix Administration Console to authenticate against Scalix Server. Please retain this password in a safe place if you plan to install multiple Scalix Servers. The same password MUST be used during installation of the additional servers.

-> Enter password:

-> Confirm password:
```

19 When the "Scalix Installer - stopped" message appears, you can exit the installer.

You can now proceed to testing of your new installation, or further customization of Scalix or to the entry of user accounts.

Getting Started with Scalix

Now that you've successfully installed and started up your new Scalix mail system, you can proceed to put it to work. This can be done with both of the following toolsets:

Scalix Administrative Console

1 Open a web browser and log in to this URL—

http://[localhost.domain.com]/sac

Alert	Do not try to log in as the user sxqueryadmin or change its settings in any way. It is a system user and should not be changed.

2 When the Scalix Administrative Console (SAC) appears, you can complete a wide range of tasks that fall into these categories:

- Scalix user account management
- Group (public distribution list) management
- Starting and stopping server services and daemons
- Monitoring queues
- Changing a limited set of server configuration settings.

You can also perform some level of system monitoring, to assess the current state of processes and resources as well as any load being made on Scalix queues.

The Scalix Administration Console can be used for most day-to-day system administration tasks.

See the separate publication, *Scalix Administrative Console Guide*, for more information.

Scalix CLI

Open a terminal window and use the complete set of CLI commands and extensions to configure and customize your system. For server setup tasks, or for high-end, advanced maintenance, you should use the extensive Linux-based command line interface. The CLI provides a full set of commands, or you can use the CLI to set up and run all needed administrative scripts.

See the separate publication, *Scalix Administration Guide,* for more information.

Installing Individual Scalix Components onto Separate Hosts with CLI

If you obtained a copy of the Scalix installation package from another source (other than Scalix or the Scalix CD), make sure it is stored in /usr/src before starting.

Tip Before you begin this task, h ave a .txt file containing the Scalix license key text stored in a convenient directory

1. Log in to the host computer as root.
2. Open a terminal window.
3. To start the installer, enter:

   [*directory_pathway*]/scalix-installer

   - Add a "--cli" extension if this host is running Xserver.

   The Scalix License Agreement scrolls on-screen in readable portions.
4. When you have read the entire agreement, you are prompted to accept it. Type "Yes" and press **Enter**, to proceed with installation.

   The actions menu appears, as shown here:
5. When the actions menu appears, as shown here:

   ```
   Please choose an action from the list:
   [1] Install all Scalix components (typical)
   [2] Install one or more Scalix components (custom)
   ```
6. Type "2" at this prompt:

   ```
   -> Please enter your choice [1]:
   ```

   and press **Enter**.
7. You are prompted for the location of the installer files:

   ```
   Choose the directory where the Scalix packages you intend to
   install reside [/root/scalix-intel-suse-10.0.0/software/
   scalix_server]:
   ```

   - To accept the default, press **Enter**.
   - If the installer files are in another directory, type the pathway and press **Enter**.
8. When the list of four Scalix components is displayed, a prompt appears:

   ```
   -> Please enter comma-separated list of numbers [1,2,3,4]:
   ```

Type the number(s) of the component(s) to be installed on this host and press **Enter**. If you are installing Scalix Server, [1], you must also install RES [4] on this host.

Note If you type two or more numbers, separate them with commas, and do not enter spaces.

9 After a series of checks are completed, you may see this question:

```
-> There were warnings during the system checks, are you sure you
want to continue with installation? (yes/no/check again) [no]:
```

As this most likely is due to a "dependency warning", you can type "Yes" and press **Enter**.

Tip Typing "Yes" will permit the installer to add missing accessory software (the "dependencies") needed by Scalix that are not present on this host.

The installation now begins, and status messages record the progress.

At this point the installation process changes, according to which Scalix component you are installing. If you are configuring all your components proceed to the next section.

If you are configuring a single component, turn to the appropriate section, as listed below:

- "Option: Configuring the Scalix server" on page 77
- "Option: Configuring Scalix Administration Console" on page 79
- "Option: Configuring RES" on page 80
- "Option: Configuring Scalix Web Access" on page 80

Option: Configuring the Scalix server

1 When installation is done, this prompt appears:

```
-> Enter the name of the primary mailnode on this server
[<server_name>,scalix]:
```

2 Press **Enter** to accept the default entry.

Note Your Scalix license is keyed to the default mailnode name. [true?] If you change it at this prompt, you'll need to replace and reinstall your license before you can run Scalix.

3 When this prompt appears:

```
-> Domain name [scalix.admin]:
```

- If the default entry (in brackets) is acceptable, press **Enter**.
- If the default entry is wrong, type the domain name in the suggested format, and press **Enter**.

A numbered list of four display name formats appears.

4 Review the list, and at this prompt:

```
-> Please enter your choice [1]:
```

Type the number that represents the preferred display name format and press **Enter**.

A numbered list of email (Internet) address formats appears.

5 Review this list, and at the prompt:

```
-> Please enter your choice [1]:
```

Type the number that represents the preferred email address format and press **Enter**.

You'll now be prompted for information about the primary administrative account for Scalix. "sxadmin@[fqdn]" is the default user name which you can edit or replace with a login ID of your choosing.

6 At this prompt:

```
-> Username [sxadmin@<qdn>]:
```

Press **Enter** to accept the default user name. (Or type a name of your choosing and press **Enter**.)

7 At this prompt:

```
-> Enter password:
```

Type a password for the admin user account and press **Enter**.

8 At this prompt:

```
-> Confirm password:
```

Re-type the admin user password and press **Enter**.

9 At this prompt:

```
-> Unique Email Address [sxadmin-postoffice@scalix.admin]:
```

Press **Enter** to accept the default email address, which automatically applies the domain name, admin user name, and display name format.

The installer now configures the newly-installed components. A series of status messages appears.

10 After the server has been started, you are prompted for the location of the Scalix license text file:

```
-> Enter the location of your license key file or enter "None" to
run the server without a license []:
```

Type the full directory pathway and file name at the prompt and press **Enter**.

- If the pathway or file name are wrong, you'll be warned and prompted again for a pathway and name.

After the license is imported and validated, the installer will separately install Java Runtime Environment and Tomcat (including the modjk Tomcat/Apache connector), then finish the configuration of Scalix.

Alert	If there already is an installation of JRE or Tomcat on this computer, you are asked to confirm the location of the existing installation. The installer may install JRE or Tomcat anyway, due to the location requirement: in the home Scalix directory.

11 Proceed to "Completing the installation" on page 81 to complete the installation.

Option: Configuring Scalix Administration Console

1 If you are installing Scalix Administration Console at this time, this prompt appears:

```
-> Please enter the default mail domain [scalix.admin]:
```

- Press **Enter** to accept the default mail domain (noted in brackets).
- Type the correct domain and press **Enter**.

2 When this prompt appears:

```
-> Please enter fully qualified host name of the Scalix Server
where the "Administration Groups" have been (or will be) created
[postoffice.scalix.admin]:
```

- Press **Enter** to accept the default Scalix Server host (noted in brackets).
- Type the correct host name and press **Enter**.

3 When this prompt appears:

```
-> Do you want to use secure communication between this machine and
Scalix Remote Execution Service using Kerberos? (yes/no) [no]
```

Type the answer (Yes or No) and press **Enter**.

4 When this prompt appears:

```
Please enter a password that will be used by the Scalix Administra-
tion Console to authenticate against Scalix Server. Please retain
this password in a safe place if you plan to install multiple
Scalix Servers. The same password MUST be used during installation
of the additional servers.

-> Enter password:

-> Confirm password:
```

Enter a non-expiring password that the Scalix Administration Console can use to authenticate against the LDAP server. This password must be different from the administrative login.

Configuring a Kerberos-based secure connection

1 If you entered "yes" at the previous prompt, agreeing to establish secure communications between this component and other Scalix components on separate hosts, a series of prompts appear, asking for the following:

- The directory location of the Kerberos keytab file
- The fully qualified domain name of the Kerberos host
- The NAME (in all caps) of the relevant Kerberos realm

2 Make the appropriate entries at the prompts to complete this phase of SAC configuration.

Option: Configuring RES

1 When this prompt appears:

```
-> Hostname [postoffice.scalix.admin]:
```

Enter the fully qualified hostname of the machine where Scalix Administration Console is to be installed.

2 When this prompt appears:

```
-> Port [8080]:
```

You have two options:

- Press **Enter** to accept the default port number (noted in brackets), or
- Type the correct port number and press **Enter**.

3 When this prompt appears:

```
-> Create “Administration Groups” on this machine? (yes/no) [yes]
```

Press **Enter** to accept the default “Yes” if administration groups are to be configured on this Scalix host.

4 Proceed to “Completing the installation” on page 81 to complete the installation.

Option: Configuring Scalix Web Access

1 When the “local language” prompt appears, three numbered options are listed:

```
Please select the language locale for Scalix Web Access running on
this host:

[1] US English

[2] UK English

[3] German
```

Type the number of your choice and press **Enter**.

2 When this prompt appears:

```
-> Do you want to enable Scalix Rules Wizard? (yes/no) [yes]:
```

- Press **Enter** to accept this action.

- Type “No” and press **Enter** if you do not want Scalix Rules Wizard activated on the SWA server.

Note	“No” simply disables the inclusion and use of Rules Wizard in SWA. it remains installed in Scalix, and can be enabled in the future.

The installer now displays a series of status reports as it completes the Scalix installation, configuration and initialization.

Completing the installation

1 When the “Scalix Installer - stopped” message appears, you can exit the installer.

Scalix is now basically ready for use.

You can now proceed to testing of your new installation, or further customization of Scalix or to the entry of user accounts.

Getting Started with Scalix

Now that you’ve successfully installed and started up your new Scalix mail system, you can proceed to put it to work. This can be done with both of the following toolsets:

Scalix Administrative Console

1 Open a web browser and log in to this URL—

http://[localhost.domain.com]/sac

Alert	Do not try to log in as the user sxqueryadmin or change its settings in any way. It is a system user and should not be changed.

2 When the Scalix Administrative Console (SAC) appears, you can complete a wide range of tasks that fall into these categories:

- Scalix user account management
- Group (public distribution list) management
- Starting and stopping server services and daemons
- Monitoring queues
- Changing a limited set of server configuration settings.

You can also perform some level of system monitoring, to assess the current state of processes and resources as well as any load being made on Scalix queues.

The Scalix Administration Console can be used for most day-to-day system administration tasks.

See the separate publication, *Scalix Administrative Console Guide*, for more information.

Scalix CLI

Open a terminal window and use the complete set of CLI commands and extensions to configure and customize your system. For server setup tasks, or for high-end, advanced maintenance, you should use the extensive Linux-based command line interface. The CLI provides a full set of commands, or you can use the CLI to set up and run all needed administrative scripts.

See the separate publication, *Scalix Administration Guide,* for more information.

Reconfiguring Scalix Web Components with CLI

You can re-use the Scalix installer to reconfigure key settings in Scalix RES, SAC or SWA by means of a built-in script, as detailed in this section. (Reconfiguring the Scalix server itself is complex enough to require the use of the full range of CLI commands, depending on the task you want to perform.)

Tip Before you begin this task, h ave a .txt file containing the Scalix license key text stored in a convenient directory

If Scalix is on a single host, you can work through this process once, to efficiently re-configure all the components. Or, if you've installed the components on separate hosts, you can work through variations of this process on each system, choose selected components, and configure them separately.

For complete information on CLI/Scalix Server configuration, see the separate publication, *Scalix Administration Guide*.

To run and use the CLI configuration script, follow these steps:

1. Log in to the host computer as root.
2. Open a terminal window.
3. To start the Scalix installer, enter:

   [*directory_pathway*]/scalix-installer

   - Add a "--cli" extension if this host is running Xserver.

   The Scalix License Agreement scrolls on-screen in readable portions.
4. When you have read the entire agreement, you are prompted to accept the agreement. Type "Yes" and press **Enter**, to proceed with installation.

   The actions menu appears, as shown here:

   ```
   [1] Upgrade all Scalix components (typical)
   [2] Upgrade one or more Scalix components (custom)
   [3] Reconfigure Scalix components
   [4] Uninstall Scalix components
   ```
5. At this prompt:

   -> Please enter your choice [1]:

   Type "3" and press **Enter** to proceed.

   A numbered list of configurable components appears:

   ```
   [1] Scalix Web Access
   (version 10.0.0.284)
   [2] Scalix Administration Console
   (version 10.0.0.284)
   ```

```
[3] Scalix Remote Execution Service

(version 10.0.0.284)
```

6 At this prompt:

```
-> Please enter comma-separated list of numbers:
```

Type one or more component numbers separated by commas, and press **Enter**.

The installer now stops Tomcat, then gives you the option to reconfigure Tomcat and JRE, before proceeding with the selected Scalix component options.

Configuring JRE and Tomcat

1 A prompt appears, asking if you want to keep your current installation of Java Runtime Environment (JRE) or reinstall the complete package.

The default is "(*keep*) existing".

Make your selection and press **Enter**.

2 If you chose "existing", a second JRE-specific prompt appears, asking you to confirm the directory location of the JRE installation, providing the original installation pathway as the default.

```
-> Enter the location of your Java installation: [/usr/java/
jre1.5.0_04]:
```

If needed, change the directory location, then press **Enter** to proceed.

The script now reports on the version and location of your current Scalix Tomcat installation.

3 At this prompt:

```
-> Enter the amount of memory reserved for Tomcat, or 0 for no
limit: [256]:
```

Press **Enter** to accept the default value, or make any changes, if needed, and press **Enter**.

4 At this prompt:

```
-> Do you want to integrate Tomcat with Apache using JK connector?
(yes/no) [no]
```

Type "yes" to confirm the Tomcat/Apache connection (via modjk), or type "no" if your installation does not incorporate Apache.

Note If you enter "yes", Scalix will automatically reserve ports 8080 and 8443 for Tomcat use.

5 If you enter "no" at the Tomcat/Apache integration prompt, a confirmation message will appear.

- Type "yes" to confirm your decision to NOT integrate Tomcat with Apache.
- Type "no" cancel your earlier "no" and to integrate Tomcat with Apache. The script will proceed to the next phase.

The script now displays a series of prompts related to the following components, in this order:

- Scalix Administration Console configuration (see page 85)
- Scalix Remote Execution Service configuration (see page 85)
- Scalix Web Access configuration (see page 86)

They display in the listed order, or if you choose just one component, the installer displays only the related prompts.

Option: Reconfiguring Scalix Administration Console (SAC)

1 At this prompt:

```
-> Please enter the default mail domain [scalix.admin]:
```

Press **Enter** to accept the default, or type the correct domain and press **Enter**.

2 At this prompt:

```
-> Please enter fully qualified host name of the Scalix Server
where the "Administration Groups" have been (or will be) created
[name.scalix.admin]:
```

Press **Enter** to accept the default, or type the correct host name and press **Enter**.

3 At this prompt:

```
-> Do you want to use secure communication between this machine and
Scalix Remote Execution Service using Kerberos? (yes/no) [no]
```

Press **Enter** to accept the default ["no"], or type "yes" and press **Enter**.

Configuring a Kerberos-based secure connection

If you entered "yes" at the previous prompt, agreeing to establish secure communications between this component and other Scalix components on separate hosts, a series of prompts appear, asking for the following:

- The directory location of the Kerberos keytab file
- The fully qualified domain name of the Kerberos host
- The NAME (in all caps) of the relevant Kerberos realm

Make the appropriate entries to complete this phase of SAC configuration.

The script now displays prompts related to Scalix RES configuration, or displays the closing sequence of messages, as detailed in "Completing the installation" on page 81.

Option: Reconfiguring Scalix Remote Execution Service (RES)

This phase of the script allows you to locate the current installation of SAC, to enable RES connection. First you are asked for the fully qualified hostname of the host on which Scalix Administration Console is installed.

1 At this prompt:

```
-> Hostname [mailbox.scalix.admin]:
```

Press **Enter** to accept the default host name, or type the correct name and press **Enter**.

2 At this prompt:

```
-> Port [80]:
```

Press **Enter** to accept the default port number, or type the port number reserved for RES on this host, and press **Enter**.

3 As a service, the script lists the number (and names) of existing administration groups.

The script now displays prompts related to Scalix Web Access configuration, or displays the closing sequence of messages, as detailed in "Completing the Configuration" on page 86.

Option: Reconfiguring Scalix Web Access (SWA)

There are two tasks in SWA configuration: picking the local language for SWA use and enabling Scalix Rules Wizard, if you choose.

1 The script lists the local language options, that control which language is used for the SWA GUI.

```
[1] US English

[2] UK English

[3] German
```

2 At this prompt:

```
-> Please enter your choice [1]:
```

Type the number representing your choice and press **Enter**.

3 At this prompt:

```
-> Do you want to enable Scalix Rules Wizard? (yes/no) [yes]
```

Press **Enter** to accept the default, or type "no" and press **Enter**.

Note	"No" simply disables the inclusion and use of Rules Wizard in SWA. it remains installed in Scalix, and can be enabled in the future.

At this point configuration is virtually complete except for the processes detailed in the next section.

Completing the Configuration

When you have finished your configuration tasks (one or all three components), the following happens:

1 A series of "cleaning up" or "starting" messages appear.

2 When the final message appears:

```
Scalix Installer - stopped.
```

You can now exit the installer.

Upgrading Scalix on a Single Host

If you obtained a copy of the Scalix version 10.x Installation/Upgrade package from another source (other than Scalix or the Scalix CD), make sure it is stored in /usr/src before starting.

Tip Before you begin this task, h ave a .txt file containing the Scalix license key text stored in a convenient directory

1. Log in to the host computer as root.
2. Open a terminal window.
3. To start the installer, enter:

   [*directory_pathway*]/scalix-installer

   - Add a "--cli" extension if this host is running Xserver.

   The Scalix License Agreement scrolls on-screen in readable portions.
4. When you have read the entire agreement, you are prompted to accept the agreement. Type "Yes" and press **Enter**, to proceed with installation.

   The actions menu appears, as shown here:

   ```
   Please choose an action from the list:
   [1] Upgrade all Scalix components (typical)
   [2] Upgrade one or more Scalix components (custom)
   [3] Reconfigure Scalix components
   [4] Uninstall Scalix components
   ```
5. At this prompt:

   ```
   -> Please enter your choice [1]:
   ```

   Type "1" and press **Enter**.
6. After the installation components are located and listed, you are prompted:

   ```
   -> Do you want to continue installing the packages? (yes/no) [yes]:
   ```

   As "Yes" is the default, press **Enter**.
7. After a series of checks are completed, you may see this question:

   ```
   -> There were warnings during the system checks, are you sure you
   want to continue with installation? (yes/no/check again) [no]:
   ```

   As this most likely is a "dependency warning", you can type "Yes" and press **Enter**.

Tip Typing "Yes" will permit the installer to add missing accessory software (the "dependencies" needed by Scalix) that are not present on this host.

8. At this prompt:

   ```
   -> Press Enter to begin installation:
   ```

Press Enter to proceed.

The installation now begins, and status messages record the progress.

9 When installation is done, this prompt appears:

```
-> Enter the name of the primary mailnode on this server
[<server_name>,domain]:
```

10 Press **Enter** to accept the default entry.

11 At this prompt:

```
-> Domain name [domain]:
```

- If the default entry is acceptable, press **Enter**.
- If the default entry is wrong, type the domain name in the suggested format, and press **Enter**.

A list of four display name formats appears.

12 Review the list, and at this prompt:

```
-> Please enter your choice [1]:
```

Type the number that represents the preferred display name format and press **Enter**.

A list of ten email (Internet) address formats appears.

13 Review this list, and at the prompt:

```
-> Please enter your choice [1]:
```

Type the number that represents the preferred email address format and press Enter.

You'll now be prompted for information about the primary administrative account for Scalix. "sxadmin@[fqdn]" is the default user name which you can edit or replace with a login ID of your choosing.

14 At this prompt:

```
-> Username [<name@fqdn>]:
```

Press **Enter** to accept the default user name.

15 At this prompt:

```
-> Enter password:
```

Type a password for the admin user account and press **Enter**.

16 At this prompt:

```
-> Confirm password:
```

Re-type the admin user password and press **Enter**.

17 At this prompt:

```
-> Unique Email Address [sxadmin-postoffice@scalix.admin]:
```

Press **Enter** to accept the default email address, which automatically applies the domain name, admin user name, and display name format.

The installer now configures the server.

18 After the server has been started, you are prompted for the location of the Scalix license text file:

```
-> Enter the location of your license key file or enter “None” to
run the server without a license []:
```

Type the full directory pathway and file name at the prompt and press **Enter**.

- If the pathway or file name are wrong, you’ll be warned and prompted again for the pathway and name.

After the license is imported and validated, the installer will separately install Java Runtime Environment and Tomcat (including the JK Tomcat/Apache connector), then finish the configuration of Scalix.

19 When the “Scalix Installer - stopped” message appears, you can exit the installer.

You can now proceed to testing of your new installation, or further customization of Scalix or to the entry of user accounts.

Alert If you are upgrading to v10 of Scalix, and plan to run ’omtidyu’ and ’omtidyallu’ after the upgrade is complete, you must be warned that doing so will remove all messages currently stored in each user’s Deleted Items folder. As a courtesy to your user base, you should avoid using these commands at this time.

Logging into SAC or SWA after an upgrade

Do NOT connect to Scalix Admin Console or Scalix Web Access by using the 8080 or 8443 port number in the URL. This is no longer needed in v10. The SAC URL is now simply [FQDN]/swa and the SWA URL is [FQDN]/swa. No port number is needed.

If you still have problems connecting, do not use the port number, and do NOT stop and restart Tomcat. It is critically important that you not stop Tomcat, as the v10 installation puts Tomcat in a new, different directory, and you may not restart the proper installation.

Upgrading Individual Scalix Components on Separate Hosts

If you obtained a copy of the Scalix installation package from another source (other than Scalix or the Scalix CD), make sure it is stored in /usr/src before starting.

Tip Before you begin this task, h ave a .txt file containing the Scalix license key text stored in a convenient directory

1. Log in to the host computer as root.
2. Open a terminal window.
3. To start the installer, enter:

   [*directory_pathway*]/scalix-installer

   - Add a "--cli" extension if this host is running Xserver.

   The Scalix License Agreement scrolls on-screen in readable portions.
4. When you have read the entire agreement, you are prompted to accept the agreement. Type "Yes" and press **Enter**, to proceed with installation.

   The actions menu appears, as shown here:

   The actions menu appears, as shown here:

   ```
   [1] Upgrade all Scalix components (typical)
   [2] Upgrade one or more Scalix components (custom)
   [3] Reconfigure Scalix components
   [4] Uninstall Scalix components
   ```
5. When this prompt appears:

   ```
   -> Please enter your choice [1]:
   ```

   Type "2" and press **Enter**.
6. You are prompted for the location of the installer files:

   ```
   Choose the directory where the Scalix packages you intend to
   install reside [/root/scalix-intel-suse-10.0.0/software/
   scalix_server]:
   ```

   - To accept the default, press **Enter**.
   - If the installer files are in another directory, type the pathway and press **Enter**.
7. After the list of four Scalix components is displayed, a prompt appears:

   ```
   -> Please enter comma-separated list of numbers [1,2,3,4]:
   ```

Type the number(s) of the component(s) to be upgraded ("installed") on this host and press **Enter**. If you are upgrading Scalix Server on this host, [1], you must also upgrade RES [4].

Note If you type two or more numbers, separate them with commas, and do not enter spaces.

8 After a series of checks are completed, you may see this question:

```
-> There were warnings during the system checks, are you sure you
want to continue with installation? (yes/no/check again) [no]:
```

As this most likely is due to a "dependency warning", you can type "Yes" and press **Enter**.

Tip Typing "Yes" will permit the installer to add missing accessory software (the "dependencies") needed by Scalix that are not present on this host.

9 When this prompt appears:

```
-> Press Enter to begin installation:
```

Press **Enter** to proceed.

The installation now begins, and status messages record the progress.

At this point the installation process changes, according to which Scalix component you are installing. If you are configuring all your components proceed to the next section.

If you are configuring a single component, turn to the appropriate section, as listed below:

- "Option: Configuring the Scalix server" on page 77
- "Option: Configuring Scalix Administration Console" on page 79
- "Option: Configuring RES" on page 80
- "Option: Configuring Scalix Web Access" on page 80

Option: Configuring the Scalix Server and Remote Execution Service (RES)

1 When installation is done, this prompt appears:

```
-> Enter the location of your license key file or enter "None" to
run the server without a license []:
```

You have two options at this time:

- If you are upgrading an existing Enterprise Edition server or upgrading from Community Edition to Enterprise Edition, enter the pathway to the required license key text file and press **Enter**
- If you are upgrading a Community Edition server, you do not need a license key. Type "None" and press **Enter** to proceed. (A confirmation note appears, before the installation continues.

After the license is imported and validated, the installer will separately prompt you to retain or re-install Java Runtime Environment and Tomcat (including the Scalix JK connector).

2 The SAC hostname prompt appears:

```
-> Hostname [FQDN]:
```

Verify the fully qualified hostname of the machine where Scalix Administration Console is to be upgraded.

3 The Scalix RES/SAC connection port prompt appears:

```
-> Port [80]:
```

You have two options:

- Press **Enter** to accept the default port number (noted in brackets), or
- Type the correct port number and press **Enter**.

A list of existing Administration Groups is displayed before the installer continues.

4 Proceed to “Completing the installation” on page 81 to complete the upgrade.

Option: Configuring Scalix Administration Console

The installer will separately prompt you to retain or re-install Java Runtime Environment and Tomcat (including the Scalix JK connector) on this host.

1 If you are upgrading Scalix Administration Console at this time, this prompt appears:

```
-> Please enter the default mail domain [server.domain]:
```

- Press **Enter** to accept the default mail domain (noted in brackets).
- If this is wrong, type the correct domain and press **Enter**.

2 When this prompt appears:

```
-> Please enter fully qualified host name of the Scalix Server
where the “Administration Groups” have been (or will be) created
[postoffice.scalix.admin]:
```

- Press **Enter** to accept the default Scalix Server host (noted in brackets).
- Type the correct host name and press **Enter**.

3 When this prompt appears:

```
-> Do you want to use secure communication between this machine and
Scalix Remote Execution Service using Kerberos? (yes/no) [no]
```

Type the answer (Yes or No) and press **Enter**.

Configuring a Kerberos-based secure connection

1 If you entered “yes” at the previous prompt, agreeing to establish secure communications between this component and other Scalix components on separate hosts, a series of prompts appear, asking for the following:

- The directory location of the Kerberos keytab file
- The fully qualified domain name of the Kerberos host
- The NAME (in all caps) of the relevant Kerberos realm

2 Make the appropriate entries at the prompts to complete this phase of SAC configuration.

3 Proceed to "Completing the installation" on page 81 to complete the upgrade.

Option: Configuring Scalix Web Access

The installer will separately prompt you to retain or re-install Java Runtime Environment and Tomcat (including the Scalix JK connector) on this host.

1 When the "local language" prompt appears, three numbered options are listed:

```
Please select the language locale for Scalix Web Access running on
this host:

[1] US English

[2] UK English

[3] German
```

Type the number of your choice at the prompt and press **Enter**.

2 When this prompt appears:

```
-> Do you want to enable Scalix Rules Wizard? (yes/no) [yes]:
```

- Press **Enter** to accept this action.
- Type "No" and press **Enter** if you do not want Scalix Rules Wizard activated on the SWA server.

Note "No" simply disables the inclusion and use of Rules Wizard in SWA. it remains installed in Scalix, and can be enabled in the future.

3 When this prompt appears:

```
Please enter the default mail domain and fully qualified host name
of the machine where Scalix Server is installed.
```

You are asked for the following:

```
-> Default mail domain [Domain]:

-> Server hostname [FQDN]:
```

Type the required information for each request and press Enter.

The installer now displays a series of status reports as it completes the Scalix installation, configuration and initialization. See the following section for information on concluding this upgrade.

Completing the installation

1 When the “Scalix Installer - stopped” message appears, you can exit the installer.

Scalix is now basically ready for use.

You can now proceed to testing of your new installation, or further customization of Scalix or to the entry of user accounts.

Alert If you are upgrading to v10 of Scalix, and plan to run ’omtidyu’ and ’omtidyallu’ after the upgrade is complete, you must be warned that doing so will remove all messages currently stored in each user’s Deleted Items folder. As a courtesy to your user base, you should avoid using these commands at this time.

Logging into SAC or SWA after an upgrade

Do NOT connect to Scalix Admin Console or Scalix Web Access by using the 8080 or 8443 port number in the URL. This is no longer needed in v10. The SAC URL is now simply [FQDN]/swa and the SWA URL is [FQDN]/swa. No port number is needed.

If you still have problems connecting, do not use the port number, and do NOT stop and restart Tomcat. It is critically important that you not stop Tomcat, as the v10 installation puts Tomcat in a new, different directory, and you may not restart the proper installation.

Uninstalling One or More Scalix Components with CLI

You can re-use the Scalix installer to remove one or more components or to uninstall the entire Scalix package, if you prefer. To do either task, follow these steps:

1. Log in to the host computer as root.
2. Open a terminal window.
3. To start the installer, enter:

   [*directory_pathway*]/scalix-installer

   - Add a "--cli" extension if this host is running Xserver.

   The Scalix License Agreement scrolls on-screen in readable portions.
4. When you have read the entire agreement, you are prompted to accept the agreement. Type "Yes" and press **Enter**, to proceed with installation.

   The actions menu appears, as shown here:

   ```
   Please choose an action from the list:
   [1] Upgrade all Scalix components (typical)
   [2] Upgrade one or more Scalix components (custom)
   [3] Reconfigure Scalix components
   [4] Uninstall Scalix components
   ```
5. At this prompt:

   ```
   -> Please enter your choice [1]:
   ```

   Type "4" and press **Enter**.
6. Review the numbered list of installed Scalix components that now appears. If you have installed Scalix components on separate hosts, the current host's component(s) are listed
7. At this prompt:

   ```
   -> Please enter comma-separated list of numbers:
   ```

   Type the component number(s) separated by commas and press **Enter**.
8. At this prompt:

   ```
   -> Do you want to remove Tomcat (version 5.0.28 in
   /opt/scalix-tomcat)? (yes/no) [no]:
   ```
9. Type "Yes" (or "No") and press **Enter**.
10. At this prompt:

    ```
    -> Are you sure you want to uninstall the selected components?
    (yes/no) [no]:
    ```

    Type "Yes" and press **Enter**.

11 At this prompt:

```
-> After uninstalling Scalix Server do you want to remove the
Scalix message store?

-> WARNING: Removing the message store will delete all existing
Scalix mailboxes on this machine. (yes/no) [no]:
```

Type “Yes” if you want to erase the message store and all its contents, and press **Enter**.

Note	You can choose to leave the message store intact (with all the records and data), then, later, reinstall Scalix “around” the existing store.

12 At this prompt:

```
-> Are you sure you want to remove the message store? (yes/no)
[no]:
```

Alert	This is your last chance to cancel the erasure of the message store, if you have any doubts or concerns.

Type “Yes” (or “No”) and press **Enter**.

A series of messages reports on the removal of Scalix components and software resources.

13 When the “Scalix Installer - stopped” message appears, you can exit the installer.

At this point you may choose to leave the installer on this host or manually delete it.

Post-Installation (Configuration) Tasks

This chapter describes a number of key post-installation tasks, including the following:

Configuring Linux Kernel Parameters

Before you begin using Scalix, you must modify the KERNEL_MIN_file_max parameter in the /etc/sysconfig/scalix file. This value specifies the maximum number of files that can be open at anytime. Scalix Server sets this parameter when the Scalix Server initialization script (/etc/init.d/scalix) is executed during the system boot-up process.

Before you start, estimate the number of users (current and prospective) your Scalix system will support, and note this number down.

To do this, follow these steps:

1. Log in to the Scalix host computer.
2. Using a text editor, open this file:

   ```
   /etc/sysconfig/scalix
   ```

3. Look for this parameter:

   ```
   KERNEL_MIN_file_max
   ```

4. Calculate up to 35–45 times the maximum number of users who might be simultaneously logged into a Scalix Server.

   Note If Scalix users use multiple client sessions to access their own (or other's) Message Store, make sure you include the number of additional client sessions in your calculation.

5. Enter this number as a "file_max" argument, with a minimum of 8192.
6. Save the change to this file.

Configuring SSL for Intel and AMD64 Hosts

Because Scalix Web Access (SWA) and the Administration Console (SAC) exchange data and credentials with Scalix Server without any encryption, Scalix Corporation recommends activating *Secure Socket Layer* (SSL) security for client connections to both Scalix applications.

Tip If you want to implement even more increased security over SWA and SAC access, you can implement the Kerberos authentication protocol as described in the *Scalix Administration Guide*.

You can use the apache mod_ssl module for this, as mod_ssl provides strong encryption using the secure sockets layer (SSL) and transport layer security (TLS) protocols for HTTP communication between a client and the Web server. For this purpose, the server sends an SSL certificate that holds information proving the server's valid identity before any request to a URL is answered. In turn, this guarantees that the server is the uniquely correct end point for the communication. Additionally, the certificate generates an encrypted connection between client and server that can transport information without the risk of exposing sensitive, plain-text content. The most visible effect of using mod_ssl with Apache is that URLs are prefixed with https:// instead of http://.

The default port for SSL and TLS requests on the Web server side is 443. There is no conflict between a regular Apache listening on port 80 and an SSL/TLS-enabled Apache listening on

port 443. In fact, HTTP and HTTPS can be run with the same Apache instance. Usually one virtual host (see Section 46.4, Virtual Hosts) is used to dispatch requests to port 80 and port 443 to separate virtual servers. Port 80 must be kept open for other Scalix services and should not be disabled.

IMPORTANT: Name-Based Virtual Hosts and SSL

It is not possible to run multiple SSL-enabled virtual hosts on a server with only one IP address. Users connecting to such a setup will receive a warning message stating that the certificate does not match the server name every time they visit the URL. A separate IP address or port is necessary for every SSL-enabled domain to achieve communication based on a valid SSL certificate. Despite the warning message, you still get the same level of encryption that you would have on any valid SSL site. This means that as long as the warning message is acceptable, communication between Web server and client is still secure. The concept of uniquely knowing the server's identity, which is guaranteed by a valid SSL certificate, is forfeited.

Setting up SSL (SUSE Linux)

To create a key and self-signed certificate, follow these steps. The process starts by activating mod_ssl by means of Yast:

1. Log in to Scalix as root.
2. Start Yast.
3. Navigate to **Network Services | Http Server**.
4. Verify that **Disabled** is selected. (Apache2 will need to be started manually)
5. Select **Modules** and click **Edit**.
6. Select **ssl** and click **Toggle Status**.
7. Click **OK**, then click **Finish**.
8. To create a test SSL certificate, enter these commands:

   ```
   $ cd /usr/share/doc/packages/apache2
   $./certificate.sh
   ```

9. Follow the on-screen instructions to build the SSL certificate. The resulting certificate files reside in the directories /etc/apache2/ssl*.

Completing the process

To make a copy of the vhost-ssl.template, follow these steps:

1. Log in to [name] as root.
2. Run these commands:

   ```
   # cd /etc/apache2/vhosts.d/
   # cp vhost-ssl.template vhost.conf
   ```

You now need to configure Apache to start with SSL by adding a flag directive to the Apache sysconfig file. To do so, follow these steps:

1. Log in to Scalix as root.
2. Use your preferred editor and open this file:

   ```
   /etc/sysconfig/apache2 +/APACHE_SERVER_FLAGS
   ```

3. Edit this line of code:

   ```
   APACHE_SERVER_FLAGS=""
   ```

   to match this example:

   ```
   APACHE_SERVER_FLAGS="SSL"
   ```

4. To force a restart of Apache, run this command:

   ```
   # rcapache2 restart
   ```

Tip If you have enabled SuSEfirewall2, do not forget to open the firewall for SSL-enabled Apache on port 443. This can be done via YaST by navigating to Security and Users > Firewall > Allowed Services. Add HTTPS Server to the list of Allowed Services.

Setting up SSL (Red Hat Linux)

To create a key and self-signed certificate, follow these steps.

1. Log in to Scalix as root.
2. Run the following command to create your key:

   ```
   # openssl genrsa 1024 > /etc/httpd/conf/ssl.key/server.key
   ```

3. Run the following command to make sure the permissions are set correctly for the key file:

   ```
   # chmod go-rwx /etc/httpd/conf/ssl.key/server.key
   #umask 77 ; \
   /usr/bin/openssl req -new -key /etc/httpd/conf/ssl.key/server.key
   \
   -x509 -days 365 -out /etc/httpd/conf/ssl.crt/server.crt
   ```

4. After you enter your passphrase, you are asked for more information. (You will not see a prompt if you created a key without a passphrase.)
5. After you provide the correct information, a self-signed certificate creates in /etc/httpd/conf/ssl.crt/server.crt. Restart your secure server after generating the certificate. To do so, run the following command:

   ```
   # service httpd restart
   ```

6. A real certificate with global validity can be obtained from vendors such as Thawte (http://www.thawte.com/) or Verisign (www.verisign.com). Instructions are provided for installing the certificate on Apache.

Configuring SSL on IBM Z-series Hosts

Because Scalix Web Access (SWA) and the Administration Console (SAC) exchange data and credentials with Scalix Server without any encryption, Scalix Corporation recommends activating Secure Socket Layer {SSL) security for connections to both Scalix applications.

Tip If you want to implement even more increased security over SWA and SAC access, you can implement the Kerberos authentication protocol as described in the *Scalix Administration Guide*.

To configure SSL encryption for Scalix applications distributed on any IBM Z-series systems, follow these steps:

1: Generating the SSL keystore

To generate a key, follow these steps:

1. Log in to the Scalix Server as root.
2. Open a terminal window and run this command:

```
openssl req -new -nodes -out name-req.pem -keyout name-key.pem
```

Note Replace the "name" placeholders(2) with file names of your choosing, and do NOT enter a password!

3. A series of prompts appears, as listed here:

Country name	Enter the two-letter ISO abbreviation.
State/province	Enter the complete name of the state or province. Do not abbreviate this entry.
City/locality	Enter the full city name.
Organization name	Enter the exact legal name of your organization.
Organizational unit	[*Optional*] Enter text that will remind you what the certificate is used for, such as "Web Server"
Common name	Enter the Scalix host name, in this format: *mail.company.domain* Or, enter the server's IP address.
Email address	Enter the Scalix administrator's email address in this format: *[name]@company.domain*

4. When you are finished, two files are generated:

   <name>-req.pem — This file is the request.

   <name>-key.pem — This file is the private key, stored in the "private" directory.

5. You have two options at this point:

   - Go to a third-party certifying authority (VeriSign, eTrust, etc.) and submit a request for a certificate (using your <name>-req.pem file)

- Generate your own certificate. This is detailed in the next section.

2: Editing the java.security File

1. Open a text editor and open this file:

   ```
   $JAVA/jre/lib/security/java.security
   ```

2. Change the security.provider.1= parameter to so that it includes this text:

   ```
   security.provider.1=com.ibm.jsse.IBMJSSEProvider
   ```

3. Uncomment the following entries so that Java runtime uses IBM classes when applications access the Java SSL API.

   ```
   ssl.SocketFactory.provider=com.ibm.jsse.JSSESocketFactory

   ssl.ServerSocketfactory.provider=com.ibm.jsse.JSSEServersocketFac-
   tory
   ```

3: Editing the server.xml file

1. Go to the /$TOMCAT_HOME/conf directory
2. Open the server.xml file and uncomment the following section to setup SSL on port 8443. It should look as follows when you are done.

   ```
   <!-- Define a SSL Coyote HTTP/1.1 Connector on port 8443 -->

   <Connector port="8443"

   maxThreads="150" minSpareThreads="25" maxSpareThreads="75"

   enableLookups="false" disableUploadTimeout="true"

   acceptCount="100" debug="1" scheme="https" secure="true"

   clientAuth="false" > <Factory className="org.apache.coy-
   ote.tomcat5.

   CoyoteServerSocketFactory" algorithm="IbmX509" clientAuth="false"
   protocol="SSL" /> </Connector>

   <!-- Define a Coyote/JK2 AJP 1.3 Connector on port 8009 -->
   ```

3. Then, prevent connections using Port 8080 by commenting out the section of the file.

   ```
   <!-- Define a non-SSL Coyote HTTP/1.1 Connector on port 8080 -->

   <!-- Connector port="8080"

   maxThreads="150" minSpareThreads="25" maxSpareThreads="75"

   enableLookups="false" redirectPort="8443" acceptCount="100"

   debug="0" connectionTimeout="20000" disableUploadTimeout="true" />

   -->
   ```

4. To stop Tomcat, enter these commands:

   ```
   cd /$TOMCAT_HOME/bin/

   ./shutdown.sh
   ```

5 To restart Tomcat, enter these commands:

```
cd /$TOMCAT_HOME/bin/
./startup.sh
```

4: Testing SSL for Scalix Applications

1 Start a web browser.

2 Enter this URL in the **Location** field:

```
https://server:8443/webmail
```

If the connection configuration was successful, the Scalix Web Access Login Page appears in the browser window.

3 Enter this URL in the **Location** field:

```
https://server:8443/sac
```

If the connection configuration was successful, the Scalix Administration Console Login Page should display.

You don't need to log in at this point; this confirms the connection.

Securing the Scalix SMTP Relay

In order for the Scalix SMTP Relay to prevent itself from being an open relay for external mailers, some rules are added to the file ~/sys/smtpd.cfg based upon the domain name of the Scalix server. For this to function correctly, reverse DNS lookups *must* be successful on the IP addresses used by both the Scalix server and any server that is being used as a SWA server (if different from the Scalix server).

Note ~ refers to the instance home directory. For more information on where an instance's home directory is located and how it is identified, see "Identifying the Instance Home Directory" on page 7.

1 To check this, run the command:

```
ipconfig | grep inet
```

The output is similar to the following:

```
inet addr:192.168.0.2 Bcast:192.168.0.255 Mask:255.255.255.0
inet addr:192.168.0.3 Bcast:192.168.0.255 Mask:255.255.255.0
inet addr:127.0.0.1 Mask:255.0.0.0
```

2 For each address, use the command

```
nslookup [address]
```

This will return output similar to:

```
Server: 192.168.0.2
Address: 192.168.0.2#53
2.0.168.192.in-addr.arpa name = host.domain.com
```

If there is no reverse resolution available, the following output displays:

```
Server: 192.168.0.2
Address: 192.168.0.2#53
** server can't find 2.3.168.192.in-addr.arpa: NXDOMAIN
```

Changes should be made to your DNS configuration to allow for reverse lookup on those addresses.

Customizing Scalix Web Access (SWA)

There are parameters in the /etc/opt/scalix/webmail/swa.properties file that you can configure if you install Scalix Web Access on a separate server, or, for example, want to use multiple LDAP servers.

You do not need to modify any of the parameters cataloged in the following tables if Scalix Web Access is installed on the same system as the Scalix Server. The default values for these parameters allow you to use Scalix Web Access immediately after installing the application.

swa.email.[option] parameters

The user configurable e-mail options in the /etc/opt/scalix/webmail/swa.properties file include the following parameters:

Parameter	Description
domain	Specifies the domain of the Scalix Server. For example: domainname.extension The default value is the domain name of the system onto which you installed Scalix Web Access.
imapServer	Specifies the name of the IMAP server. The default value is the fully qualified domain name of the system onto which you installed Scalix Web Access.
smtpServer	Specifies the name of the SMTP server. The default value is the fully qualified domain name of the system onto which you installed Scalix Web Access.

swa.ldapSource.[option] parameters

You can easily configure any number of LDAP server connections in the swa.properties file. Each server entry should be numbered separately, as shown here:

```
swa.ldap.3.type=system
swa.ldap.3.server=mailbox.corporate.com
swa.ldap.3.port=389
swa.ldap.3.baseDN=o=scalix
swa.ldap.3.displayName.resourceID=addressbooksearch_title_system
swa.ldap.3.addressSearchLimit=100
```

The user-adaptable LDAP options include (in part) the following parameters:

Parameter	Description
server	Specifies the name of the LDAP server. The default value is the domain name of the system onto which you installed Scalix Web Access.
	NOTE: If the LDAP server is a Scalix Server, you must edit the ~sys/smptd.cfg file on that Scalix Server before Scalix Web Access users can send messages to recipients outside of the Scalix network. Add the following line to the smptd.cfg file: `RELAY accept IP address or hostname of Scalix Web Access`
port	Specifies the LDAP port number. The default is port 389.
baseDN	Specifies the root from which Scalix Web Access searches the directory. The default is o=scalix.
authType	Specifies the type of authentication to use when connecting to the LDAP server. The options are: • simple • none The default is none.
filter	Specifies the filter to use when performing LDAP searches. The default is: (|(&(cn=%s*)(mail=*))(&(sn=%s*)(mail=*))(&(gn=%s*)(mail=*))(mail=%s*)(&(omalias=%s*)(mail=*))) %s is replaced by the search term.
addressSearchLimit	Specifies the maximum number of LDAP address search results to return. The default is 100.

The ldapSource section in the swa.properties file also includes parameters that allows you to use a second LDAP server in which users can search the Contacts directory for addresses (instead of the System directory). To do this, configure the second ldapSource section in the swa.properties file using the example below as a guideline:

```
server=server2.domain.ext
port=389
basedn=o=MyContacts
authtype=simple
filter=(|(&amp;(cn=%s*)(|(mail=*)(304=4)))(&amp;(sn=%s*)(mail=*))
(&amp;(gn=%s*)(mail=*))(mail=%s*)(&amp;(omalias=%s*)(mail=*)))
binddn=rfc822mailbox=%u
```

The binddn parameter specifies LDAP authentication information if you are using simple for LDAP authentication (authtype=simple). For example, you can enter rfc822mailbox=%u, where %u is replaced by a user's login name.

Scalix Corporation recommends that you add a third set of <ldapSource> parameters if you want to add another LDAP server to the Scalix messaging system. If you do this, make sure you add the characters in bold for the filter= parameter (displayed above).

Enabling the Server Rules Wizard

The Server Rules Wizard allows mail system users to create server-side rules for Scalix Web Access. For example, you can create a rule that allows you to forward messages received from a particular sender to a specific folder in your mailbox.

By default, the Server Rules Wizard is enabled after Scalix Web Access has been installed, however you may have disabled it at that time. If you did disable the Rules Wizard at installation, you can enable the Rules Wizard by following these steps:

1. Log in to the Scalix host.
2. Navigate to this directory:

   ```
   /etc/opt/scalix/webmail/
   ```

3. Open a text editor, then open and edit the swa.properties file as follows:

   ```
   <features
   ...
      rulesWizard="true"
   ```

   ALERT: The text in this file is case-sensitive.
4. Also, verify that the Server Rules Wizard URL is correct:

   ```
   <settings
      rulesWizardURL="http://[scalix_host]/Scalix/rw"
   ```

   (Replace "[scalix_host]" with the actual host name.)

Maximizing Scalix Web Access Performance

To maximize the performance of Scalix Web Access, you can modify the amount of memory allocated by the Java Virtual Machine. This requires adding a new variable:

```
JAVA_OPTS
```

To this file:

```
$TOMCAT_HOME/bin/setclasspath.sh
```

This variable can be inserted directly under the JAVA_HOME parameter.

The memory allocated is a subset of the total system memory. Therefore, the values you use for -Xms and -Xmx must be set appropriately. For example, here is a typical entry:

```
JAVA_OPTS="-server -Xms256m -Xmx512m"
```

This entry assumes that of the total system memory, there is generally 512 MB free. On a system that has 1 GB memory, but generally has 256MB free, the following line would be appropriate.

```
JAVA_OPTS="-server -Xms128m -Xmx256m"
```

For a system that contains 4 GB of memory, and generally has 1GB free, you could enter a larger value:

```
JAVA_OPTS="-server -Xms512m -Xmx1024m”
```

The two parameters for the JAVA_OPTS variable are described below:

Xmsn Specifies the initial size, in bytes, of the memory allocation pool. This value must be a multiple of 1024, and greater than 1 MB. Append the letter k (or K) to indicate kilobytes, or m (or M) to indicate megabytes. The default value is 2 MB.

Xmxn Specifies the maximum size, in bytes, of the memory allocation pool. This value must a multiple of 1024, and greater than 2 MB. Append the letter k or K to indicate kilobytes, or m or M to indicate megabytes. The default value is 64 MB.

Note The Scalix installer pre-sets this entry to a default value, that depends on your system’s memory. So, any value you find in this configuration is an optimal setting—that you are still free to customize.

Optimizing Firefox and Mozilla for Scalix Web Access

If you are using Mozilla Firefox to access Scalix Web Access, an alert dialog box might appear when you have logged in and are working on Scalix. This warning appears when a JavaScript action takes too long to complete.

- Just click **Cancel** to allow Scalix Web Access to continue processing.

Alert Do NOT click OK. If you do, Firefox aborts the script which may cause malfunctions in Scalix Web Access.

To resolve this problem if it recurs, modify the configuration settings for your browser as detailed here:

1. Open a new browser window (in addition to the existing browser window).
2. Enter this text in the **Location** field.

   ```
   about:config
   ```

   A long list appears.
3. Enter this text in the **Filter Bar** at the top of the about:config page:

   ```
   dom.max_script_run_time.
   ```

   The previous list is reduced to a single entry as you type.
4. Double-click the remaining line of text.

   The Enter Integer Value dialog box appears.

5 Click in the text field and enter **30**.

6 Click **OK**.

7 Close all browser windows, then reopen a window and reconnect to your Scalix mailbox.

Your Firefox browser should have no more javascript problems with Scalix.

Customizing the Scalix Administration Console (SAC)

When you create a new user in the Scalix Administration Console, the default country setting for the address book is "United States". To change the default country setting, follow these steps:

1 Log in to the SAC host computer.

2 Use a text editor to open this file:

```
/etc/opt/scalix/caa/scalix.res/config/ubermanager.properties
```

3 Change this value:

```
ubermanager.console.[defaultCountry]
```

4 Replace the "[defaultCountry]" option with the desired two-letter country code. For example, enter DE to have Deutschland/Germany be the default country setting.

Customizing the Scalix SWA Login Page

See the *Administrator's Resource Kit* (ARK) on your Scalix CD (or tarball) for a special package of instructions and template files you can use to customize and apply a new, company-specific Scalix Web Access login page for use by your users.

Setting up Single Sign-on Authentication

Single Sign-on Authentication allows users of Outlook (with Scalix Connect) to access your e-mail using the Kerberos security protocol. This authentication mechanism allows you to log in to your local domain in a Microsoft Active Directory environment and access your e-mail without any further authentication.

If you are configured for Single Sign-on authentication, neither the Scalix Login Information window nor the Login window will appear during the profile creation process. Instead, after you log in to your system and select the Scalix Server service during the profile creation process, the Single Sign-on window appears.

For more information about Single Sign-on authentication, see the *Scalix Administration Guide*.

About Webcal in Scalix

Webcal is a new protocol, added to Scalix in version 10, that allows users to use any calendaring client from a variety of operating systems (Sunbird, iCal, Evolution) to log in to the Scalix server via a "calendar-only" URL and review their current calendar. Viewing of calendars is on a "read-only" basis; no adding or editing of events/meetings is permitted via a Webcal connection.

Webcal is installed with all other Scalix components. No post-installation configuration or administration is necessary; you only need to let your mail system users know how to utilize this extra service via their regular email/calendaring client.

Using a Webcal-ready calendaring client

The user starts the application, then enters a URL similar to this example:

```
http://host.domain/webcal
```

After logging in with their Scalix user ID and password, they will see a copy of their current calendar.

What platforms support Webcal?

Most current calendar clients are Webcal-enabled. This means a user can use almost any Mac OS, Windows or Linux client from anywhere to log in to the Scalix server and check their calendar.

How many calendars can one access?

If one knows the pathway to a public calendar or any other calendar, one can append it to the Scalix Webcal URL and get access to the current contents of that calendar. For example, if a user wanted to see their workgroup's calendar in "Public Folders", they might enter this URL --

```
http://corporation.mail.com/webcal/Public Folders/Our Workgroup
```

After logging in, the workgroup calendar should appear in their client.

Additional Information

Most of the configuration and administration tasks can now be undertaken through the Scalix Administration Console (SAC), a browser-based toolbox that enables you to log in to and both monitor and maintain your Scalix system through an efficient web interface. See the separate Acrobat publication, *Managing a Scalix System with the Administrative Console*, for complete information.

For a complete overview of Scalix configuration information and full descriptions of administrative tasks and commands, see the *Scalix Administration Guide*.

Upgrading Scalix Software

This chapter covers the use of the Scalix Installation wizard in upgrading your Scalix system, whether the components are on a single host, or the components were independently installed on separate hosts.

IMPORTANT! Read this first!

If you are upgrading an existing Scalix Enterprise Edition system to version 10.x, or upgrading a Scalix Community Edition 9.x system to Enterprise Edition version 10.x, it is imperative that you obtain your Scalix license before starting the actual upgrade. If you do not have the license, your upgraded system will be limited to Community Edition-level functionality until you do obtain and import the needed license.

When you upgrade Scalix Server, the Scalix Installer might replace some of configuration files in the ~scalix/sys directory if the default settings for the new version of Scalix Server have changed (in regard to the currently installed version). If you previously made changes to any of these configuration files, the Scalix Installer will archive them, after renaming these files as noted here:

- By adding the letter “O” to the filename (for example, Osmtpd.cfg)
- By adding “save” to the filename (for example, general.confsave)
- By appending a number to the filename (for example, sendmail.cf.1)

Regardless of their current state, Scalix Corporation recommends that you back up the following files in a separate directory:

- /etc/opt/scalix/webmail/partner.xml (Scalix Web Access)

  Note that “partner.xml” is renamed to “swa.properties” in version 10.x of Scalix
- ~/sys/smtpd.cfg
- /etc/mail/sendmail.cf
- /~/sys/general.cfg

- Any mail address rules (if applicable)

Note If you are using SSL for Scalix applications, you must remove the SSL key file password before starting the Scalix Installer. The password must be blank (no password).

- If you customized the Scalix Web Access logon page with your own artwork, you will want to back up that file (and related resources) before upgrading your Scalix system.

Alert If you are upgrading to v10 of Scalix, and plan to run 'omtidyu' and 'omtidyallu' after the upgrade is complete, you must be warned that doing so will remove all messages currently stored in each user's Deleted Items folder. As a courtesy to your user base, you should avoid using these commands at this time.

Upgrading Scalix on a Single Host

1. Log in to the target host computer as root.
2. Insert the Scalix Installation CD into the CD ROM drive.
   - Alternate: Change to the shared directory that contains Scalix installation files. If you downloaded a copy of the Scalix .tar file, you can copy it to a convenient directory on the host, then untar the archive and start the process.
3. If required, mount the CD ROM drive by entering this command:

   ```
   mount /mnt/cdrom
   ```

   ```
   cd /mnt/cdrom/
   ```
4. Enter this command:

   ```
   sh scalix-installer
   ```

   This starts the Scalix Installer Wizard, which (after a brief setup) displays the *Welcome* screen.
5. Click **Forward**.

   The *License Agreement* screen appears.
   - Read through the license agreement.
   - If you accept the conditions of installation and use, click the checkbox by "I have read and accept the above License Agreement"
6. Click the now-active **Forward** to proceed.

   The *Wizard Mode screen* appears.
7. Click the option **Upgrade all Scalix Components**.
8. Click **Forward**.

   The *Component List* window appears with all components selected by default.
9. Click **Forward**.

   The *System Check* screen appears.

   This task may require several minutes for completion.

10 Green checkmarks indicate the system is ready, so you can click **Forward** to proceed.

If the system check fails to locate specific software applications or resources, one of two possible symbols will appear:

- A “stop sign” symbol indicates the absence of critical software. You cannot proceed with installation in this state.
- A “caution” symbol appears if critical software is missing that the installer will automatically add. This includes Java Runtime Environment and two related Tomcat packages.

11 If a system or dependency check results in an alert, click **View Log**. A dialog box reports on which system components are missing.

12 If the “cautions” report JRE or Tomcat as missing, you can proceed with installation, as the installer will install the missing packages in most cases.

13 Click **Forward** to continue.

The *Installing... (status)* screen appears.

The Scalix Installer begins upgrading the selected components.

14 When it’s done, click **Forward** to continue.

The *License Activation* screen appears.

15 Either paste the license text in to the window or browse to it.

16 Click **Forward** when you are done.

17 The *Third Party Components* screen appears.

This screen verifies the existence of the required software (JRE, Tomcat and JK Connector), and gives you an opportunity to complete any “missing” installations if needed.

18 When any additional third-party component installations are complete, click **Forward** to continue.

The *Secure Communication* screen appears.

19 Enter a password that the Scalix Administration Console uses to authenticate against the LDAP server. This is a non-expiring password and is for a different account than the administrative login. Keep the password on file because you will need to enter it on each server if you upgrade to a multi-server setup at some point. If you lose the password, it is stored in /etc/opt/scalix/caa/scalix.res/config/psdata.

20 When you have entered and confirmed the password, click **Forward**.

21 The installation completes and the *Done* screen appears.

22 Click **OK** to complete the upgrade and exit the installer.

Alert! — Logging into SAC or SWA after an upgrade

Do NOT connect to Scalix Admin Console or Scalix Web Access by using the 8080 or 8443 port number in the URL. This is no longer needed in v10. The SAC URL is now simply [FQDN]/sac and the SWA URL is [FQDN]/webmail. No port number is needed.

If you still have problems connecting, do not use the port number, and do NOT stop and restart Tomcat. It is critically important that you not stop Tomcat, as the v10 installation puts Tomcat in a new, different directory, and you may not restart the proper installation.

Upgrading Individual Scalix Components

Alert —**Important!**— Upgrade the Scalix Administration Console first, before undertaking Server/RES and Scalix Web Access upgrades. It is of primary importance (in a multiple host environment) that you upgrade the SAC component first if you are upgrading from Scalix version 9.4.

1: Scalix Administration Console

1. Log in to the target host computer as root.
2. Insert the Scalix Installation CD into the CD ROM drive.
   - Alternate: Change to the shared directory that contains Scalix installation files. If you downloaded a copy of the Scalix .tar file, you can copy it to a convenient directory on the host, then untar the archive and start the process.
3. If required, mount the CD ROM drive by entering this command:

   ```
   mount /mnt/cdrom
   ```

   ```
   cd /mnt/cdrom/
   ```

4. Enter this command:

   ```
   sh scalix-installer
   ```

   This starts the Scalix Installer Wizard, which (after a brief setup) displays the *Welcome* screen.
5. Click **Forward**.

   The *License Agreement* screen appears.
   - Read through the license agreement.
   - If you accept the conditions of installation and use, click the checkbox by "I have read and accept the above License Agreement"
6. Click the now-active **Forward** to proceed.

   The *Wizard Mode screen* appears.
7. Click **Upgrade one or more Scalix Components (custom)**.
8. Click **Forward**.

   The *Installation Files* screen appears.

9 Browse to the directory where you stored your installation package then click **Forward**.

The *Component List* screen appears.

- Make sure that **Scalix Administration Console** is the only active choice.

10 Click **Forward**.

The *System Check* screen appears.

This task may require several minutes for completion.

11 Green checkmarks indicate a ready system, and you can click **Forward** to proceed.

If the system check fails to locate specific software applications or resources, one of two possible symbols will appear:

- A “stop sign” symbol indicates the absence of critical software. You cannot proceed with installation in this state.
- A “caution” symbol appears if critical software is missing that the installer will automatically add. This includes Java Runtime Environment and two related Tomcat packages.

12 If a system or dependency check results in an alert, click **View Log**. A dialog box reports on which system components are missing.

13 If the “cautions” report JRE or Tomcat as missing, you can proceed with installation, as the installer will install the missing packages in most cases.

14 Click **Forward** to continue.

The *Installing... (status)* screen appears.

The Scalix Installer begins upgrading the selected components.

15 When it is done, click the now-active **Forward**.

The *JRE (Java Runtime Environment) Configuration* screen appears.

16 You have two options:

- Confirm the existence and directory pathway to the current installation, and skip this task.
- If not present on this host, install JRE at this time.

17 To install JRE using the Scalix Installer, look for the **Install** button in the JRE Configuration screen and click it.

- A dialog box appears listing the default installer package. Click **Install**, and when installation is complete, click **OK** to close this dialog box.

18 When JRE is confirmed as installed, click **Forward**.

The *Tomcat Configuration* screen appears.

You have two options:

- Confirm the existence and directory pathway to the current installation, and skip this task.

- If it's not currently installed on this host, install Tomcat (and JK Connector) at this time.

19 To install Tomcat and the JK Connector using the Scalix Installer, click the checkbox by **Enable JK Connector**.

- You can modify the reserve memory settings, if needed.

20 Locate the **Install** button in the Tomcat Configuration screen and click it.

- A dialog box appears listing the default installer package. Click **Install**, and when installation is complete, click **OK** to close this dialog box.

21 When Tomcat is confirmed as installed, click **Forward**.

The *Administration Server* screen appears.

22 Confirm these entries pertaining to this host:

- The default mail domain (which you can edit if needed)
- The server hostname (displayed as a fully qualified name)

23 Click **Forward** to continue.

The *Secure Communication* screen appears.

24 Enter a password that the Scalix Administration Console will use to authenticate against the LDAP server. This is a non-expiring password and is for a different account than the administrative login. Keep the password on file because you will need to enter it on each server. If you lose the password, it is stored in /etc/opt/scalix/caa/scalix.res/config/psdata on the machine with the Scalix Administration Console.

A second *Secure Communication* screen appears.

25 Verify these entries, if you previously configured Kerberos authenticated connections:

- The **Configure secure communication...** option is checked.
- The service keytab file for the Administration Console is listed. If not, browse to it at this time.
- The **Fully qualified host** name of the KDC (Kerberos Distribution Center).
- The **Kerberos Realm** (in UPPERCASE text).

26 Click **Forward** to continue.

The *Additional Mail Domains* screen appears.

- Verify the existing mail domains are still listed.
- To add any other usable domains (that will help you create different e-mail addresses in the Administration Console), click **Add** and use the Add mail domains dialog box.

Alert	You cannot add new mail domains at this time unless they have been included in your Scalix license key.

These domains will appears in a pull-down menu among the user account features in the Scalix Administrative Console.

27 Click **Forward**.

The *Done* screen appears.

28 Click **OK** to complete the upgrade.

2: Scalix Server and Remote Execution Service

These two components must not be installed on separate hosts.

1 Log in to the target host computer as root.

2 Insert the Scalix Installation CD into the CD ROM drive.

- Alternate: Change to the shared directory that contains Scalix installation files. If you downloaded a copy of the Scalix .tar file, you can copy it to a convenient directory on the host, then untar the archive and start the process.

3 If required, mount the CD ROM drive by entering this command:

```
mount /mnt/cdrom
```

```
cd /mnt/cdrom/
```

4 Enter this command:

```
sh scalix-installer
```

This starts the Scalix Installer Wizard, which (after a brief setup) displays the *Welcome* screen.

5 Click **Forward**.

The *License Agreement* screen appears.

- Read through the license agreement.
- If you accept the conditions of installation and use, click the checkbox by "I have read and accept the above License Agreement"

6 Click the now-active **Forward** to proceed.

The *Wizard Mode screen* appears.

7 Click **Upgrade one or more Scalix Components (custom)**.

8 Click **Forward**.

The *Installation Files* screen appears.

9 Browse to the directory where you stored your installation package then click **Forward**.

The *Choose Components* screen appears.

10 Make sure that only the two components are selected:

- Scalix Server

- Scalix Remote Execution Service (RES)

Alert Do **not** install these components (Server and RES) on separate host computers.

11 Click **Forward**.

The *System Check* screen appears.

12 The Scalix Installer verifies the system for the upgrade.

This task may require several minutes for completion.

13 Green checkmarks indicate a ready system, and you can click **Forward** to proceed.

If the system check fails to locate specific software applications or resources, one of two possible symbols will appear:

- A "stop sign" symbol indicates the absence of critical software. You cannot proceed with installation in this state.
- A "caution" symbol appears if critical software is missing that the installer will automatically add. This includes Java Runtime Environment and two related Tomcat packages.

14 If a system or dependency check results in an alert, click **View Log**. A dialog box reports on which system components are missing.

15 If the "cautions" report JRE or Tomcat as missing, you can proceed with installation, as the installer will install the missing packages in most cases.

16 Click **Forward** to continue.

The *Installing... (status)* screen appears.

The Scalix Installer begins upgrading the selected components.

17 Click the now-active **Forward** when upgrade installation is complete.

The *License Activation* screen appears.

18 If you have a license to run Scalix as an Enterprise Edition system, you have two options for inputting the license at this time:

- Use a text editor to cut-and-paste the text from any text file containing the exact license text.
- Click **Browse** to locate, open and import the contents of the file.
- After you enter a license, click **Forward** to continue.

19 If you want to run Scalix as a *Community Edition* system, you do not need a license. You can click **Forward.**

- When a warning dialog box asks you to confirm that "no license was entered", click **OK**.

The *JRE (Java Runtime Environment) Configuration* screen appears.

20 You have two options:

- Confirm the existence and directory pathway to the current installation, and skip this task.

- If not present on this host, install JRE at this time.

21 To install JRE using the Scalix Installer, look for the **Install** button in the JRE Configuration screen and click it.

- A dialog box appears listing the default installer package. Click **Install**, and when installation is complete, click **OK** to close this dialog box.

22 When JRE is confirmed as installed, click **Forward**.

The *Tomcat Configuration* screen appears.

You have two options:

- Confirm the existence and directory pathway to the current installation, and skip this task.
- If not present on this host, install Tomcat (and JK Connector) at this time.

23 To install Tomcat and the JK Connector using the Scalix Installer, click the checkbox by **Enable JK Connector**.

- You can modify the reserve memory settings, if needed.

24 Locate the **Install** button in the Tomcat Configuration screen and click it.

- A dialog box appears listing the default installer package. Click **Install**, and when installation is complete, click **OK** to close this dialog box.

25 When Tomcat is confirmed as installed, click **Forward**.

The *Remote Execution Service* screen appears.

- Verify the host name of the computer where the Scalix Administration Console (SAC) is to be installed.
- Confirm the **Port** used for communication to the Scalix Administration Console.

26 Click **Forward**.

The *Admin Groups and Query Manager* screen appears.

27 Verify that the checkbox by **Create Administrative Groups...** is checked, if you are storing administrative groups on this server. (All existing groups are listed in this screen.)

28 Click **Forward**.

The *Secure Communication* screen appears.

29 Enter a password that the Scalix Administration Console uses to authenticate against the LDAP server. This is a non-expiring password and is for a different account than the administrative login. Keep the password on file because you will need to enter it on each server. If you lose the password, it is stored in /etc/opt/scalix/caa/scalix.res/config/psdata on the machine with the Scalix Administration Console.

30 The *Done* screen appears.

31 Click **OK** to complete the upgrade.

3: Scalix Web Access

1. Log in to the target host computer as root.
2. Insert the Scalix Installation CD into the CD ROM drive.
   - Alternate: Change to the shared directory that contains Scalix installation files. If you downloaded a copy of the Scalix .tar file, you can copy it to a convenient directory on the host, then untar the archive and start the process.
3. If required, mount the CD ROM drive by entering this command:

   ```
   mount /mnt/cdrom
   ```

   ```
   cd /mnt/cdrom/
   ```

4. Enter this command:

   ```
   sh scalix-installer
   ```

   This starts the Scalix Installer Wizard, which (after a brief setup) displays the *Welcome* screen.
5. Click **Forward**.

   The *License Agreement* screen appears.
   - Read through the license agreement.
   - If you accept the conditions of installation and use, click the checkbox by "I have read and accept the above License Agreement"
6. Click the now-active **Forward** to proceed.

   The *Wizard Mode screen* appears.
7. Click the option **Upgrade one or more Scalix Component (Custom)**.
8. Click **Forward**.

   The *Installation Files* screen appears.
9. Browse to the directory where you stored your installation package then click **Forward**.

   The *Choose Components* window appears.
10. Make sure that only the **Scalix Web Access** option is actively selected.
11. Click **Forward**.

    The *System Check* screen appears.
12. The Scalix Installer verifies the system for the upgrade. If the system check is unsuccessful, click **View Log** for information about the failure.
13. Click **Forward** when the check is complete.

    The *Installing... (status)* screen appears.

    The Scalix Installer begins upgrading the selected components.
14. Click the now-active **Forward** when upgrade installation is complete.

    The *JRE (Java Runtime Environment) Configuration* screen appears.

15 You have two options:

- Confirm the existence and directory pathway to the current installation, and skip this task.
- If not present on this host, install JRE at this time.

16 To install JRE using the Scalix Installer, look for the **Install** button in the JRE Configuration screen and click it.

- A dialog box appears listing the default installer package. Click **Install**, and when installation is complete, click **OK** to close this dialog box.

17 When JRE is confirmed as installed, click **Forward**.

The *Tomcat Configuration* screen appears.

You have two options:

- Confirm the existence and directory pathway to the current installation, and skip this task.
- If not present on this host, install Tomcat (and JK Connector) at this time.

18 To install Tomcat and the JK Connector using the Scalix Installer, click the checkbox by **Enable JK Connector**.

- You can modify the reserve memory settings, if needed.

19 Locate the **Install** button in the Tomcat Configuration screen and click it.

- A dialog box appears listing the default installer package. Click **Install**, and when installation is complete, click **OK** to close this dialog box.

20 When Tomcat is confirmed as installed, click **Forward**.

The *Web Access Server* screen appears.

- You can enable the Scalix Rules Wizard at this time by clicking the related checkbox. (You can do this at a later time, if you prefer.)
- Verify the primary language used by the majority of your Scalix Web Access users.

21 Click **Forward**.

The *Web Access Server (Continued)* screen appears, listing a default mail domain.

- Change the **Default mail domain**, if needed.
- Enter a **Server hostname** for this computer.

22 Click **Forward**.

The *Done* screen appears.

23 Click **OK** to complete the upgrade.

Alert — Logging into SAC or SWA after an upgrade

Do NOT connect to Scalix Admin Console or Scalix Web Access by using the 8080 or 8443 port number in the URL. This is no longer needed in v10. The SAC URL is now simply [FQDN]/sac and the SWA URL is [FQDN]/webmail. No port number is needed.

If you still have problems connecting, do not use the port number, and do NOT stop and restart Tomcat. It is critically important that you not stop Tomcat, as the v10 installation puts Tomcat in a new, different directory, and you may not restart the proper installation.

Uninstalling Scalix

This chapter covers the uninstallations of Scalix server software from Linux host computers.

The uninstallation process for Scalix server software does not remove any files modified by an administrator. These files are saved as filename.rpmsave. If required, you can remove these files manually.

To uninstall Scalix, either the entire server package or individual Scalix components, follow these steps:

1. Open a terminal window and log in to the Scalix host computer as root.
2. At the prompt, enter this command:

   ```
   sh scalix-installer
   ```

   The Scalix Installer wizard appears, displaying the *Welcome* screen.
3. Click **Forward** to proceed.

   The Wizard Mode screen appears.
4. Accept the license agreement and click **Forward** again to proceed.
5. In the next screen, select **Uninstall Scalix Components** and click **Forward**.

   The *Uninstall Components* screen appears.

   This pane lists the components on the server, and allows you to select specific components to be removed.

Note	If this Scalix system includes JRE, that installation will be left intact on the host. You will, however, be given the opportunity to uninstall any Scalix-related Tomcat installations during this process. (This includes the JK Apache/Tomcat Connector.)

6. Make any changes if you want to remove one or more selected components, then click **Forward** to continue.

   A confirmation dialog box appears.
7. Click **Yes** to confirm the removal of Scalix components.

   A wizard screen appears, asking if you also want to delete the message store. You have two options:

   - Uninstall the entire message store database, including mailboxes, services and configurations.

- Leave the message store on the host, ready for a replacement installation of new Scalix software.

Note	You can leave the message store intact, and later perform a clean reinstallation of Scalix server software that will incorporate the existing store, ready for use. If you are not sure which option to choose, we suggest that you leave the message store on the host, for future considerations.

8 Click **Yes** —if you want to remove the Scalix message store, with all your user data and mailboxes.

As the Scalix Installer begins uninstalling Scalix components, it displays an *Uninstalling* status pane that dynamically reports which components are being deleted.

9 When the uninstallation is complete, you are prompted (at the end of the status messages) to click **Forward**.

The wizard *Done* screen appears.

10 Click **OK** to exit the Installer.

Installing Scalix Connect for Novell Evolution

Scalix Connect for Novell Evolution provides transparent, full function support for email on Linux desktops. It enables connectivity between Evolution and the Scalix Server, and supports IMAP and iCal for compatibility with the full range of functionality offered by Evolution.

You can use the connector with Novell Evolution 2.4 (or later), an email client bundled with Gnome 2.12. We recommend you completely update Gnome to 2.12, which automatically installs Evolution 2.4 before beginning installation of the Scalix Connect RPM.

Alert	The Scalix Connect plugin for Evolution works only with Scalix Server 10.0 or higher. Contact your mail system administrator for confirmation if your Scalix Connect does not work.

.

Note	Support for the Scalix Connect for Evolution binaries is provided by the Scalix Community Forum as well as Scalix Technical Support (via incident support or premium support). In addition, you can download the latest source from the GNOME CVS.

Features of Scalix Connect for Evolution

Mail
- Standard IMAP functionality
- Public folders
- Outlook-style handling of deleted items
- Search folders
- Encryption and signing of messages (PGP)
- Message receipts

Calendar
- Standard calendaring and scheduling functionality
- Reading and writing of freebusy information
- Create new calendar folders
- Access to calendars in public folders

Contacts
- View, create, modify and delete contacts and PDLs
- Lookup of system entries through LDAP (can be included in PDLs)
- Create new contact folders
- Access to contacts in public folders

Other
- Wizard-driven account setup
- Offline mode for mail
- Change password
- Easy access to Scalix Rules Wizard
- Localized for English and German

.

Note Group scheduling features and public folders in Scalix Connect for Evolution are available only to Scalix "premium" users, not "standard" users.

System Requirements

Any system already configured to work with Novell Evolution is assumed to meet the basic requirements for the Scalix connector. There are, however, some minimum system requirements for its use.

Scalix Connect for Novell Evolution requires:

Components	Requirements
Client Software	Novell Evolution 2.4 or later *Evolution is an email client included with Gnome 2.12. We recommend that you (1) completely update Gnome to 2.12, which automatically installs Evolution 2.4.

Components	Requirements
Operating System	Fedora Core 4 (or later) RedHat Enterprise Linux 4 (or later) *You can download and build the connector on another operating system, but it would be unsupported.

Approved Web Browsers and Email Clients

Components	Requirements
Approved web client software (Scalix Web Access client browsers)	• Internet Explorer 5.5 or 6.0 • Mozilla 1.7 or higher • Firefox 1.0 and later
Approved e-mail client software	• Microsoft Outlook versions 2000, XP, and 2003 and later (versions 9, 10, 11) • Novell Evolution, versions 2.4.2 and later
Approved Windows OS versions (for client workstations)	• Windows 2000 • Windows XP (All earlier versions of Windows are not supported, irrespective of which version of Outlook you have installed.)

Pre-Installation Steps

Before installation, update Gnome to 2.12, which automatically installs Evolution 2.4.

If your computer is running Fedora Core, follow these steps to update to the latest version of Gnome (and Evolution):

1. Completely update the Fedora installation with a yum update.
2. Download and install the NRPMS package for your Fedora version from this URL:

   www.nrpms.net/Docs/Yum
3. Complete a second yum update.
4. You can now install the connector.

Alert	The Scalix Connect plugin for Evolution works only with Scalix Server 10.0 or higher. Contact your mail system administrator for confirmation if your Scalix Connect does not work.

Users can access their Scalix mailbox including email, calendar and scheduling, contacts, public folders, free/busy information and system address book using Evolution 2.4 or later.

Features of Scalix Connect for Evolution

Mail
- Standard IMAP functionality
- Public folders
- Outlook-style handling of deleted items
- Search folders
- Encryption and signing of messages (PGP)
- Message receipts

Calendar
- Standard calendaring and scheduling functionality
- Reading and writing of freebusy information
- Create new calendar folders
- Access to calendars in public folders

Contacts
- View, create, modify and delete contacts and PDLs
- Lookup of system entries through LDAP (can be included in PDLs)
- Create new contact folders
- Access to contacts in public folders

Other
- Wizard-driven account setup
- Offline mode for mail
- Change password
- Easy access to Scalix Rules Wizard
- Localized for English and German

System Requirements

Scalix Connector for Evolution can be installed and used with Evolution 2.4 (or later), but Evolution must be on a client computer running on Fedora Core 4 or Red Hat Enterprise Linux 4.

Limitations on Community Edition users

Community Edition users are subject to the following functional limitations when they use Evolution:

- Participation in, or creation of public folders is not permitted.
- Calendaring is limited to personal events.
- Scheduling a meeting or replying to a meeting invitation is not permitted.
- Another person's freebusy status is inaccessible.

If you want to take advantage of Enterprise Edition functions, contact your mail system administrator and request a status change to “Premium user”.

Pre-Installation

Scalix Connect for Evolution can be installed and used with Novell Evolution 2.4 (or later), an email client bundled with Gnome 2.12. It is recommended that you completely update Gnome to 2.12, which automatically installs Evolution 2.4. At this point you can install the Scalix Connect RPM.

If your computer is running Fedora Core, follow these steps to update to the latest version of Gnome (and Evolution):

1. Completely update the Fedora installation with a yum update
2. Download and install the NRPMS package for your Fedora version from this URL:

   www.nrpms.net/Docs/Yum
3. Complete a second yum update
4. You can now install the connector.

Alert The Scalix Connect plugin for Evolution works only with Scalix Server 10.0 or higher. Contact your mail system administrator for confirmation if your Scalix Connect does not work.

Installing Scalix Connect for Evolution

This guide assumes that you already have the correct version of Evolution installed.

Download and install the RPM

1. Get the Scalix Connect for Evolution RPM.
2. As super-user or via sudo, install the RPM:

   rpm -ivh evolution-scalix-10.0.0.x-1.i386.rpm
3. If you have an older version of the connector installed, then upgrade as follows:

   rpm -Uvh evolution-scalix-10.0.0.x-1.i386.rpm

Setting up an account

You need to create an account profile--unless you were using the Connect before and have just upgraded it to a newer version. This wizard is useful if you have not previously configured mail accounts in Evolution. If you already have one or more accounts in Evolution,

choose **Edit -> Preferences** and add a new account with the **Mail Accounts** section. To create the profile, follow these steps:

Welcome Screen

Read the text in this window, then continue with the next step.

Uninstalling Scalix Connect for Evolution

Uninstalling Scalix Connect for Evolution is a two-step process:

1. Remove the account profile by choosing **Edit > Preferences > Mail Accounts**
2. Remove the connector by opening a terminal window and running this command:
3. **rpm -e evolution-scalix<version>**

Features of Scalix Connect for Evolution

Scalix Rules Wizard

Scalix Rules Wizard (SRW) lets you set up and monitor any number of server-side rules for message filtering. A browser-based application, SRW can be accessed through the Edit menu in Evolution. When SRW opens in a new browser window, your username will already be filled in.

You can change the location of SRW under the Defaults tab in your account settings (**Edit->Preferences->Mail Accounts**) in case the default location is wrong.

Evolution must be in the mail module before this link is usable. If you have no account selected in the tree view, a list of Scalix profiles displays from which you can choose.

Change Password

To change your Scalix account password in Evolution, select the mail module/ account. In the dialog box that appears, change your account password.

Deleting Messages

Deleting a message from a Scalix mailbox with Evolution is different from the same process in other email clients. This process resembles that of Microsoft Outlook, in which a message is first moved to the “Deleted Items” folder, then erased by use of a Empty Deleted Items command.

You have to be in the mail module to access this feature. If no account is selected in the tree view, a list of Scalix profiles displays from which you can choose.

About Scalix

To find information about the Scalix Connect for Evolution (as well as the version of the Scalix server you are using), choose **Help->About Scalix**.

Installing and Managing Scalix Connect

This chapter describes two collections of related tasks pertaining to Scalix Connect, a plugin for Microsoft Outlook that enables the email client to communicate fully with your Scalix system. The first task is to install Scalix Connect on a Scalix *Enterprise Edition* user's computer.

The remaining tasks concern the maintaining and upgrading of Scalix Connect, and if needed, the uninstalling of Connect from a client computer.

Contents

This chapter's contents have been organized into the following sections:

Alert	This version of Scalix Connect for Outlook does not work in a 64-bit Windows XP system. Future versions of Scalix will permit such installations.

Note	Scalix Connect does not support journaling, forms, message recall or MSN Messenger integration.

Introduction to Scalix Connect

Scalix Connect for Microsoft Outlook provides transparent, full function support for the Outlook email client on the Linux platform. It enables connectivity between the Outlook client and the Scalix Server, and supports the MAPI protocol for compatibility with the full range of functionality offered by Outlook. This includes full calendaring/scheduling, public folders, rules and all email tasks. And the Scalix Connect plugin for Outlook allows Outlook to match the feature set of a Microsoft Exchange server with no apparent difference to the user.

With Scalix, users continue to enjoy the functionality and productivity they are accustomed to with Microsoft Outlook. Scalix Connect for Microsoft Outlook uses native MAPI Properties and a MAPI Default Message Store to unlock the group productivity functionality of Outlook

operating in "Corporate or Workgroup" mode, such as rich electronic messaging, shared directories, shared calendars, free/busy lookups, public folders, and more.

Scalix Connect also enables advanced modes of operation such as offline folder synchronization and delegate access to mailboxes, calendars, and personal folders.

There are, however, some differences in the way Scalix handles Outlook features.

Unsupported Features

Scalix Connect does not support journaling, forms, message recall and MSN messenger integration.

Offline Folder Synchronization

Scalix Connect supports Outlook Offline Folder Synchronization with a different implementation than that of Microsoft Exchange. The functionality offered is similar to that of Exchange and is configured in a similar way. However, the local store is not implemented as an Exchange offline store (.ost). The network connection is initiated on demand and does not have to be established prior to performing the synchronization. The synchronization process itself operates as a background process.

Scalix Connect currently does not offer Offline Folder Synchronization for Public Folders.

Additional Services in the Same Profile

Scalix Connect for Microsoft Outlook supports simultaneous use of additional services such as PST and LDAP address lookup, but not Internet Mail Service or the Microsoft Exchange Service in the same profile. Scalix Connect for Microsoft Outlook specifically does not support the features for Hotmail integration and the ability to send using a specific email account selection.

Scalix Connect for Microsoft Outlook does not allow direct delivery of incoming messages into a PST-based inbox.

Third Party MAPI Add-Ins

Third party (MAPI) applications or Outlook add-ins have not been tested with Scalix Connect for Microsoft Outlook. These programs may operate correctly but are not supported by Scalix. If you require support for specific applications, please contact support or your Scalix representative.

Integration with software deployment solutions

Some application deployment solutions such as Microsoft's Systems Management Server require a Microsoft Windows Installer (.msi) file in order to deploy an application across multiple desktops without user intervention. A .msi file for Scalix Connect for Outlook can be generated by executing "setup.exe /e" from the command line. A file called "Scalix Connect for Microsoft Outlook.msi" will be created in the same directory as the Setup.exe application. This .msi file contains all of the necessary information to accomplish a complete installation of Scalix Connect for Outlook and it can be used with large-scale application deployment solutions such as the one mentioned above. The .msi files for both English and German languages are located in the /deployment directory of the CD or tarball.

System Requirements

There are some minimum system requirements for the use of Scalix Connect for Microsoft Outlook:

Components	Requirements
Client Software	Outlook 2000, XP, and 2003 * A legacy version of Scalix Connect forOutlook 98 and 2000 on Windows NT 4.0 is available to enterprise customers through Scalix support.
Operating System	Fedora Core 4 (or later) RedHat Enterprise Linux 4 (or later) *You can download and build the connector on another operating system, but it would be unsupported.
Disk Space	The installation of Scalix Connect for Microsoft Outlook requires approximately 13 MB of free disk space. 2 MB of this space is for the Microsoft Data Access Objects that might be present on user PCs already.
Access/Permissions	You must be a Power User, or have administration permissions to install Scalix Connect for Microsoft Outlook.

Additional Information

Detailed system requirements for Outlook is located at:

- Outlook 2000: http://support.microsoft.com/default.aspx pr=out2K&SD=OFFN
- Outlook 2002: http://support.microsoft.com/default.aspx?pr=ol2002&SD=OFFN
- Outlook 2003: http://support.microsoft.com/default.aspx?scid=fh;en-us;out2003

Alert	This version of Scalix Connect for Outlook does not work in a 64-bit Windows XP system. Future versions of Scalix will permit such installations.

•

Installing Scalix Connect on an Outlook Client

Scalix Connect can only be installed on a client computer by a user with “Administrator” permissions on the computer. For information on qualifying Outlook client versions, see “Pre-Installation Requirements” on page 11. Note, too, that all client PCs must be able to resolve the Scalix server by hostname and fully-qualified domain name.

Any upgrades to Scalix Connect can be made by the client system’s user, provided you have some means of distributing a copy of the updater to them.

You can also set up an automated update/upgrade process for Outlook users, as detailed in “Automatically Upgrading Scalix Connect for Outlook” on page 152.

To install Scalix Connect on a client computer, do the following steps:

1. Log in to the Outlook client user’s computer using an administrator account.
2. Insert the Scalix Installation CD into the CD ROM drive, or navigate through the network to the shared directory that contains Scalix installation files.
3. Double-click the setup.exe icon.

   The Preparing to Install window appears, followed by the Welcome window.
4. Click **Next** to proceed with installation.

   The Scalix Connect InstallShield begins installing the required files to the Outlook system MAPI directory.

   The Setup Status wizard pane appears, indicating the status of installation.
5. When installation is successfully complete, click **Finish** to exit the installer.

Automating the Scalix Connect Installation

If your mail system potentially involves hundreds or even thousands of desktops that will require Scalix Connect, some installation-automation resources exist, to help reduce the amount of end-user interaction. The following three files can be used for an automated deployment of Scalix Connect, on Windows desktops or through Windows desktop deployment tools.

Setup.exe This program actually installs Scalix Connect. When the Scalix release (most often distributed as a "zipped" tar file) is unpacked, it will contain a directory /software/scalix_connect_outlook/, where the setup.exe program will be located.

Install.ini This configuration file helps you to customize the Outlook profile settings. A template install.ini file is included with the latest Scalix release, and can be found in the /software/scalix_connect_outlook/deployment directory.

sxpro.exe This program that can be used to create Outlook profiles. This program is not included within the directories of the Scalix release, but it can be extracted from the setup.exe program by passing the /e switch.

c:\Connect\setup.exe /e

Method 1 – End-User Driven Deployment

With this process, the installation of the Scalix Connect program (setup.exe) and creation of the Scalix profile occurs through end-user interaction. The interaction is very simplistic, intuitive but ultimately requires the user knows how to answer what is presented to them on the screen.

Scalix Connect 9.4.2 or later requires Administrator or Power User privileges on the workstation where it is installed – subsequent upgrades to later versions of Connect that utilize the auto-upgrade service only require Power User.

1. Establish a shared networkable directory (samba share or any network file share) that all users can access.
2. In this directory (\\servername\sharename\Connect), you would place the following files, provided by Scalix.

   ```
   setup.exe

   install.ini
   ```

3. Customize the install.ini file, so that an Outlook profile can be created and automatically populated with some of the necessary Scalix mailbox data. (This provides a level of standardization across all desktops.)

   The following general guidelines should be used.

   - The value noted in the second line should point to a local drive and directory where the setup.exe can write data (hence the c:\windows\temp location specified above).
   - Directory paths must include a double backslash (\\).
   - Use "InstallMigrateExProfile=1" only if there is an existing default profile and you wish to migrate some data from that profile into the newly created Scalix profile.

- ¨Never use an IP address for the InstallMailServerName – a valid FQDN (either an A-record or C-name record) that is registered in DNS is required. Using a C-name (that points to an A-record) will be beneficial if there is ever a need to move users to a new physical server.

The following is a valid example of a working install.ini file:

```
[Install Flags]

InstallMailServerName=scalix01.company.com

InstallLogfileUploadLocation=c:\\windows\\temp\\install.log

InstallDefaultProfileName=Scalix1

InstallWithServerStore=1

InstallAllowSavedPassword=0

InstallSetDefaultProfile=1

InstallLogFileLocation=c:\\windows\\temp\\log.txt

InstallMigrateExProfile=0
```

The install.ini contains parameters, which can ultimately help streamline the installation, and help in the auditing the process of who has installed the Scalix Connect software. The settings in the install.ini can help standardize all profile settings across a group of people or an organization.

InstallMailServerName=

This should be set to the name of the Scalix server, which users will connect to, or optionally point to a DNS alias record (C-Name)

InstallLogFileUploadLocation=

This should be set to a directory on either the desktop PC or a mapped network drive. The user must have appropriate permissions (read/write).

InstallDefaultProfileName=

This value will be used for the Outlook profile name that setup creates on each desktop.

InstallWithServerStore=

This should be set to 1.

InstallAllowSavedPassword

In most deployments, you should set this value to 0, to force users to enter their password when they log in to their Scalix mailbox. With this value set to 1, users will not have to enter their password after their initial login to Scalix server.

InstallSetDefaultProfile=

By setting this value to 1, the new Outlook profile created by the setup (or sxpro) program, will be the profile that is opened the next time Outlook is opened.

InstallLogFileLocation=

This should be set to a directory on either the desktop PC or a mapped network drive. The user must have approriate permissions (read/write).

InstallMigrateExProfile=

With this value set to 1, it will migrate some information from the existing default profile to the newly created profile.

Additional notes about the install.ini file

- The InstallDefaultProfileName value should be set to some standard that is reflective of a group of users or a Scalix server they access.
- The InstallMailServerName value is where the user's mailbox would exist, hence in a multiple server environment it may be required to configure different install.ini files in different sub-directories for groups of users.
- The InstallWithServerStore=1, InstallAllowSavedPassword=0 and InstallSetDefaultProfile=1 are typically not changed.
- The two parameters that specify locations of log files, can be configured to point to a network drive and directory, but again this must be statically mapped by the client.
- The InstallMigrateExProfile parameter is only necessary in cases where existing Outlook profiles are being used prior to the transition to Scalix (such as an Exchange environment).

Password/Security

Installing Scalix Connect across your user population ought to be undertaken in a secure manner, and should involve the following considerations:

- If random passwords were used during the generation of the Scalix mailboxes, then some distribution mechanism will obviously need to take place prior to user installation of Connect. One solution that you can activate during the mailbox provisioning process is to set each mailbox to the same password, but with a pre-expiration. During installation, all users would enter the same initial password with their username, then each would immediately be prompted to enter a new, replacement password.
- If the Scalix environment is configured to use an external authentication source (such as an LDAP directory or Active Directory), then the user would simply need to provide the existing password text to this external source.

Enhancing Method 1 Using Scripts

By scripting a batch file, you can add error checking and automation that will help streamline the end-user deployment process. A batch file takes advantage of the following:

- Running setup with the /s switch will not prompt the user for Next and Finish buttons, it enables a silent install.
- The install.ini can contain a username value (bolded in the example below), which would then be placed inside the Outlook profile for the user.

Here is a sample batch file that you can script for your use:

```
[Install Flags]

InstallMailServerName=scalix01.company.com

InstallLogfileUploadLocation=c:\\windows\\temp\\install.log

InstallDefaultProfileName=Scalix1

InstallWithServerStore=1

InstallAllowSavedPassword=0

InstallSetDefaultProfile=1

InstallLogFileLocation=c:\\windows\\temp\\log.txt

InstallMigrateExProfile=0

InstallUsername=John Smith
```

The example shows how to utilize the following logic:

- A required variable is passed to the script (%1), which equates to a preset Username value.
- Verification that the appropriate static drive mapping exists, and if not automatic mapping of such drives and directories.
- In addition, if local directories are used, a check and subsequent creation, if needed, of the local directories.
- Check of permissions to the local drive (validating the Administrative user or equivalent requirement).
- Dynamic creation of the install.ini, whereby the value passed to the batch file is echoed into the last line (InstallUsername=).
- Moving to the correct working directory or providing full paths.
- Error handling should any of the operations fail.
- Messages echoed back to the user upon exit, based on success or failure.

Method 2 – Automation through Network/Domain Login

You also have the option to use network/domain login scripts or systems management tools (often triggered through network/domain login) that automatically deploy Scalix Connect and facilitate creation of the Scalix profile—with no user interaction. The network/domain login or systems management tools need to provide the ability to execute scripts and programs, and to trap the login name— potentially in an environment variable.

The Scalix tools include the following options:

- Running setup with the /s switch will bypass prompting the user with Next and Finish buttons, and instead, enables a silent install.
- Running “setup.exe /s” on a machine that has an existing Scalix Connect installation will simply not install anything, with no errors.
- The install.ini can contain a username value

- The ability to install Scalix Connect in advance on desktops without creation of an Outlook profile is possible, because Scalix Connect can exist on a Windows machine (observed under Add/Remove Programs) but be both dormant and unobtrusive.
- The installation permits you to create a Outlook profile separately, using the sxpro.exe executable.

The network/domain login scripts and/or the systems management tools offer varying capabilities, but in essence there are two basic options:

- Execute both Scalix Connect install and Outlook Profile generation together
- Execute the installation of Scalix Connect in advance, and then at a later date, execute the installation of the Outlook profile.

In the case where an organization wants to execute both Scalix Connect installation and Outlook profile creation within the same login session then the script logic would basically be the same as described in the previous section. The difference: a user simply logs into the domain, and the value required for the InstallUsername= parameter of the install.ini is extracted from a variable that stored the user's login name.

Deploying Scalix Connect without Outlook Profile Creation

In the case where an organization wants to deploy Scalix Connect first, and then create Outlook profiles for the users at a later time, the steps are quite simple. Because Scalix Connect installation program (setup.exe) can be run against an existing Windows machine that already has it installed with no error, just enable the executable to run upon domain login over a period of time (days or weeks). Naturally there would certainly be requirements to check whether the user is qualified to install Scalix Connect (e.g., is their system running Windows 2000 or a later OS).

The most important point: if no install.ini file exists in the current working directory where setup.exe is executed, then no Outlook profile will be created and no errors will occur. In this scenario the /s switch (silent install) should also be used.

Scalix Profile Creation

At some point, after each user's computer has had Scalix Connect installed, each computer will require creation of a Scalix profile. The utility sxpro.exe can be used to create the needed Scalix profile and it can be called in either of your network/domain login scripts or systems management tools.

The sxpro.exe utility must read an install.ini in order to create the profile, but considering the install.ini is plain text, it could again easily be created within the script facility that is launched upon domain login. Similar to what has been explained in prior sections, the InstallUsername= parameter would potentially be filled with the login name value that has been trapped in an environment variable at the beginning of the login session.

The necessary format for sxpro is:

```
sxpro –i c:\connect
```

In this example, c:\connect is the path to where the install.ini has been stored. Note that you do not need to specify the install.ini filename; it simply needs to exist in that directory.

Example: Batch File

The following batch file provides a good template that can easily be modified for any of the scenarios described previously for automating the deployment of Scalix Connect and cre-

ation of the Outlook Profile. In this example note that the creation of the Outlook profile occurs along with the Scalix Connect installation.

```
@ECHO Off

REM Modify the names of the Shares in the following two lines
REM Assume the username variable and the COMPUTERNAME variable either come
from the login
REM session, or are passed on the command line.
SET INSTALL_DIR=\\postoffice\Scalix
SET LOG_DIR=\\postoffice\ScalixLogs

IF NOT EXIST %INSTALL_DIR% GOTO CantFindInstallDir
IF NOT EXIST %LOG_DIR% GOTO CantFindLogDir

SET STARTTIME=%DATE% - %TIME%

IF NOT DEFINED TEMP GOTO NoTempDir
IF NOT EXIST %TEMP% GOTO CantFindTempDir
GOTO TempDirOK

:NoTempDir
SET NO_TEMP_VAR=TRUE
IF NOT EXIST \TEMP GOTO CantFindTempDir
SET TEMP=\TEMP
GOTO TempDirOK

:TempDirOK
SET CLIENT_LOG_FILE=%TEMP%\%COMPUTERNAME%_ScalixConnect_clientlog.txt
SET INSTALL_LOG_FILE=%TEMP%\%COMPUTERNAME%_ScalixConnect_InstallLog.txt
SET INI_FILE=%TEMP%\Install.ini

ECHO [Install Flags] > %INI_FILE%
ECHO InstallWithServerStore=1 >> %INI_FILE%
ECHO InstallAllowSavedPassword=0 >> %INI_FILE%
ECHO InstallSetDefaultProfile=1 >> %INI_FILE%
ECHO InstallMigrateExProfile=0 >> %INI_FILE%
ECHO InstallDefaultProfileName=Scalix1 >> %INI_FILE%
ECHO InstallMailServerName=sx1.company.com >> %INI_FILE%
ECHO InstallUsername=%username% >> %INI_FILE%
ECHO InstallLogfileUpLoadLocation=%CLIENT_LOG_FILE% >> %INI_FILE%
ECHO InstallLogFileLocation=%INSTALL_LOG_FILE% >> %INI_FILE%

CD %TEMP%
COPY %INSTALL_DIR%\setup.exe %TEMP%


%TEMP%\setup.exe /s

ERASE /q %TEMP%\setup.exe

ERASE /q %TEMP%\install.ini

ECHO  >> %CLIENT_LOG_FILE%
ECHO  >> %INSTALL_LOG_FILE%
ECHO Install Started at %STARTTIME% >> %CLIENT_LOG_FILE%
```

```
ECHO Install Started at %STARTTIME% >> %INSTALL_LOG_FILE%
SET ENDTIME=%DATE% - %TIME%
ECHO Install Ended at %ENDTIME% >> %CLIENT_LOG_FILE%
ECHO Install Ended at %ENDTIME% >> %INSTALL_LOG_FILE%

COPY /y %CLIENT_LOG_FILE% %LOG_DIR%
COPY /y %INSTALL_LOG_FILE% %LOG_DIR%
ERASE /q %CLIENT_LOG_FILE%
ERASE /q %INSTALL_LOG_FILE%

SET CLIENT_LOG_FILE=
SET INSTALL_LOG_FILE=
SET INI_FILE=
SET ENDTIME=

GOTO Exit


:CantFindInstallDir
:CantFindLogDir
:CantFindTempDir
GOTO Exit


:Exit
IF NOT DEFINED NO_TEMP_VAR GOTO ContinueExit
SET NO_TEMP_VAR=
SET TEMP=
GOTO ContinueExit

\:ContinueExit
SET INSTALL_DIR=
SET LOG_DIR=
SET STARTTIME=
```

Remotely Modifying a User's Outlook Profile

You can modify your mail user's Outlook client profiles to add a Scalix profile. This can be done remotely, when they first log in to the Scalix server. The process involves edits to a couple of files that are incorporated in your Scalix server.

Note that when a user first logs into Scalix, you can set up a dual-purpose process to install Connect in their Outlook, and create the needed Scalix profile.

For more information, review the Knowledgebase at Scalix support web site.

Setting up an Automatic Upgrade of Scalix Connect for Outlook

You have the option to set up a server-side upgrade process that will automatically upgrade Scalix Connect plugins on client systems, when the clients log in to your mail system. This process automatically detects log-ins, determines the version of Scalix Connect, then pauses the mail connection for the duration of the upgrade. The process results in a short interruption for the user, but the connection is reestablished afterwards and they can proceed to get their mail.

To set up such an automatic upgrade, follow this general process:

1. Modify the install.ini according to your preferences.
2. Create a client-accessible directory on the Scalix Server that includes the setup.exe file.

Note All users must have read/execute rights to this folder.

3. Create a template message for omsndmsg.
4. Generate the user password list using ommigu –show and copy the output file to the directory containing omsndmsg.
5. Run omsndmsg.

All of these tasks and options are detailed in this section.

Overview

You have the option to upgrade Scalix Connect on more than one client systems at the same time, and with only a minimum of client user interaction. Several options exist, including extended capabilities and tools included with Scalix Connect that you can use when installing Scalix Connect on user systems, such as:

- New mailbox password distribution
- Outlook profile standardization
- Outlook profile migration
- Logging

The Scalix Connect setup.exe file initiates the installation of Scalix client software on user systems. Depending on the options you specify in the install.ini file, setup.exe can also launch the Outlook profile creation wizard.

The first time you install Scalix Connect on client systems, make sure the install.ini file is in the same shared network directory as the setup.exe file. The install.ini file contains parameters which can:

- Streamline the installation process
- Generate installation audits to determine the users systems have been successfully upgraded
- Standardize all profile settings across a group of users or an organization

Customizing Directory and File Permissions

Make sure that all Scalix Connect users have the required access to the shared network directory that contains the following Scalix Connect installation files:

- setup.exe
- install.ini

"Administrator" permissions are required on user systems for the initial installation of Scalix Connect. After the initial installation, you can upgrade Scalix Connect using any system permissions. See "Automatically Upgrading Scalix Connect for Outlook" on page 152 for more information.

Configuring the install.ini file parameters

The Scalix Connect install.ini file includes parameters you can configure to customize the automatic installation of Scalix Connect.

Parameters	Description
InstallMailServerName=	The name of the Scalix Server to which users connect.
InstallLogfileUpLoadLocation=	Enter the path and file name for the file that progressively accumulates all installation information on a user system.
	The file stores data generated from the file specified in InstallLogFileLocation= parameter.
InstallDefaultProfileName=	The name of the Outlook Profile that you want to create for all users.
	Leave this parameter empty to disable Profile creation.
InstallWithServerStore=	This parameter must be set to 1.
InstallAllowSavedPassword=	Set this parameter to 0 to prompt users to enter their password when they log in to their Scalix Server mailbox.
	Set this parameter to 1 to disable the password prompt.

Parameters	Description
InstallSetDefaultProfile=	Set this parameter to 1 to configure the Profile created by InstallDefaultProfileName as the default Outlook Profile on user systems.
InstallLogFileLocation=	Enter the path and file name for the file that stores installation information on a user system.

Sample install.ini File

```
[Install Flags]
InstallMailServerName=server.domain
InstallLogfileUpLoadLocation=c:\\temp\\all_installs.log
InstallDefaultProfileName=Scalix Connect XYZ Corp
InstallWithServerStore=1
InstallAllowSavedPassword=1
InstallSetDefaultProfile=1
InstallLogFileLocation=c:\\temp\\install.log
```

Customizing password capabilities in the ommigu command

The ommigu Linux shell script is the mailbox provisioning and password management tool for Scalix Server. ommigu is in the /opt/scalix/bin directory. It provides a range of password-specific actions that you may want to employ.

Activating random password generation

Add the –g option to ommigu, to generate a random password for an individual mailbox or for a group of mailboxes.

Note You must notify each user about the new password for their mailbox, which can be done with the sxsendmsg command, detailed later in “Using omsndmsg to communicate to new Scalix Connect users” on page 149

Recording a specific password for a mailbox

Use the ommigu script with the –p option to specify a specific password for an individual mailbox or for a group of mailboxes.

Activating one-time, pre-expired passwords

You can enter one-time passwords that pre-expire at the first user login. The ommigu script –expire option directs Scalix Connect to prompt users to change their password the first time they log in to their mailbox with their regular password.

Generating a list of mailbox passwords in use

The ommigu command provides a –show option that collects status information about individual user mailboxes and the associated passwords.

```
ommigu –show
```

The output from the –show option includes (separated by semi-colons):

- common name
- password
- SMTP address
- distinguished name
- state (status)
- date

Here is a sample of output (a single user) from ommigu -show:

```
Hugh Packard;IsiPAi55;imap.mail.org;<???>;active;07/13/2005
```

To get only the mailbox password of a user, enter the -n option, followed by the user's common name wrapped in quotes (as shown below):

```
ommigu –n “Hugh Packard” –show
```

To save the output to a standalone file, add the “>*filename*” option:

```
ommigu –show >filename
```

The -userfile option t generates the common names of the users from which you want to generate data. For example,

```
ommigu --userfile /tmp/group1.txt --show>/tmp/list1.txt
```

You can then use the list1.txt output file to manage the dissemination of new Scalix Server mailbox passwords for the users in your organization.

Using omsndmsg to communicate to new Scalix Connect users

The omsndmsg application sends a message to user mailboxes without using mail transports. The message itself can contain text that streamlines the Scalix Connect automatic installation process by instructing users what (if any) action they need to take to ensure that the installation (or upgrade) process operates correctly.

You can add the following to an omsndmsg message:

- notification about a migration
- information about using the setup.exe file
- support contact information

omsndmsg can also read ommigu output files, which enables efficient and secure distribution of new mailbox passwords to users.

Here is an example on a omsndmsg message:

```
From: IT Team
To: John Stevens
Cc:
Subject: Important Notice - Your New Scalix Mailbox is Available

!!! Please Read !!!

You have now been migrated from Exchange to Scalix. Your previous
Exchange mailbox is still available but you will not be able to send
email from that account.

Please log into Scalix and use this password when requested: 4k$jU76

Use the following link to complete the installation of Scalix Con-
nect:
"\\server\share\ScalixMAPI\install.html\"

Please contact the IT Support Team at extension 9-8179 if you have any
problems or questions.

Thanks,

Information Technology Department
```

A complete guide to omsndmsg command options

The omsndmsg command includes the following extensions:

Option	Enter the following:	Description
-a	**<Exchange Administrator Profile Name>**	The system on which omsndmsg operates must be a 32-bit version of the Windows operating system (Windows NT, 2000, XP) and must contain an Outlook Profile for an Administrator account. This level of access is required to access all mailboxes.
-p	**<Administrator password>**	The password for the Administrator Outlook Profile.
-l	**<Logfile path/name>**	A log file is generated which contains omsndmsg information. A typical entry for this option is a filename in the local temporary directory.
-u	**<UserPasswordlist path/name>**	This is the path/file generated by ommigu.
		This text file must reside in a directory accessible by the Windows system running omsndmsg.
-t	**<Message template path/name>**	The message template included with Scalix must exist in a directory that is accessible by the Windows system running omsndmsg.

Option	Enter the following:	Description
-e	**<Administrators Return email address>**	The address you enter for this option is included in the From: line of the message which is delivered to each user.
		Entering an invalid address for this option results in undeliverable messages (if the user replies to the message). If you do not enter an address, no address displays in From: line.

Typically, you will install Scalix Connect on groups of user systems (instead of individually or all systems at the same time). Therefore, omsndmsg will likely be used several times. You can create a batch file to simplify to use of this application.

The following is an example of a batch file that you could use if it is executed from the same directory that contains the files referenced in the command line (omsndmsg.exe, group1.txt, template.txt).

```
omsndmsg -a "adminprof" -p "pass" -l "log1.txt" -u "group1.txt" -t
"template.txt" -e “IT Team”
```

A sample message template

The following illustration displays the contents of a customizable template text file included with Scalix for use in creating notification messages for users. Use the -t <Message template path/name> option to use the template.

Note the HTML delimiters in the various parts of the message.

```
<subject>Subject: Important Notice - Your New Scalix Mailbox is Avail-
able</subject>

<body>
!!! Please Read !!!

You have now been migrated from Exchange to Scalix. Your previous
Exchange mailbox is still available but you will not be able to send
email from that account.

Please log into Scalix and use this password when requested: <pass-
word></password>

Use the following link to complete the installation of Scalix Connect:
“\\server\share\ScalixMAPI\install.html\”

Please contact the IT Support Team at extension 9-8179 if you have any
problems or questions.

Thanks,

Information Technology Department
</body>
```

Automatically Upgrading Scalix Connect for Outlook

Once Scalix Connect is installed on the PC’s of your “Premium” *Outlook* client users, periodic upgrades of Scalix Connect are needed. These upgrades include new functionality and fixes that ensure the proper operation of Scalix Connect. You can configure your Scalix Server to perform automatic upgrades that work this way:

- The automatic upgrade process is configured and the resource files stored appropriately.
- A client “Premium” user connects to their Scalix mailbox.
- Scalix detects the connection, polls the version number of the Connect software. This involves a comparison of the version number of the mapi.cfg file on the server with the version number of the mapi.cfg file on the user system.
- If the version is not up-to-date, Scalix will pause the mailbox connection, and perform the upgrade (after confirming the user’s consent)
- Once the upgrade is complete, Scalix restores the mailbox connection and the user can check their mail.

The process involves a brief interruption, but is otherwise transparent to the user.

Creating the required mapi.cfg file

When a Premium user logs into Scalix with Outlook for the first time, a mapi.cfg file is automatically copied to the client system—if one already exists on the server. This master

server-side mapi.cfg file must be created manually using the values described in this section of the manual. (This file is not automatically created during installation.)

When a mapi.cfg file is copied to the client user's computer, it is stored in this Scalix directory:

```
C:\Documents and Settings\user\Local Settings\Application
Data\Scalix\Scalix\MAPI\Profiles\profile_name\Scalix
```

A sample mapi.cfg file showing [Autoupgrade] options

The following illustration shows the [AutoUpgrade] section of a typical server-side mapi.cfg file.

```
# MAPI Client configuration file

20

[AutoUpgrade]

SetupPath=\\server\\setuppath_location\\setup.exe (9.1 to 1.0x
upgrades)
HTTPSetupPath=http://address/directory/setup.exe (9.2 to 10.x
upgrades)
HTTPUpdateInstallMgr=1
HTTPUpgradeExemptList=username1;username2
MinimumScalixVersion=x.xx.xx.xx
ForwardInstallLogsTo=administrator@company.com
ForwardInstallLogsFrom=IT Team
ForwardInstallLogsSubject=Auto-upgrade Status
UseLocalTimeVSGMT=1
UpgradeIntervalTimeCheck=8
```

Setting up an automatic Scalix Connect upgrade process

To set up Scalix Server so that it automatically upgrades all current "Premium" users to a new version of Scalix Connect, follow these steps:

1. Place the new versions of setup.exe and SXInstallMgr.exe on a shared network directory that is accessible to all client user computers that will require upgrades.
2. Write down the directory pathway for use in the mapi.cfg file.

   See "Directory and File Permissions" on page 31 for more information about permissions.
3. Create the mapi.cfg file and store it in this directory:

   ~/nls/C/mapi.cfg

   - Use the example file text shown previously as a template.

4 Make the following changes to the mapi.cfg file:

[version number]	(*Represented by "20" in the previous example.*) Be sure the version number noted in the file is greater than the version number of the mapi.cfg file on the user systems you want to upgrade. For example, changing the value from **20** to **21** initiates the auto-upgrade process as all current client computers will have 20 in their mapi.cfg files.
SetupPath	Enter the pathway to the shared directory storing the setup.exe and SXInstallMgr.exe files. (Users must have read access to the files and their directories.)
MinimumScalixVersion	Enter the version of the sxmapi32.dll file that is part of the Scalix Connect release to which you want to upgrade. The Scalix Release Notes contain the version number.
UseLocalTimeVSGMT	Specify whether you want to use local time or Greenwich Mean Time (GMT) to auto-upgrade users. Enter **1** for local time, or **0** (zero) for GMT.
UpgradeIntervalTimeCheck	Enter a parameter to specify the (metric) time at which Scalix Server polls client systems to verify whether they are using the latest version of Scalix Connect. For example, enter 8 to poll for auto-upgrade status information at 8 am. Enter 22 to poll for information at 10 pm. Entering value of 24 or greater causes Scalix Server to poll for auto-upgrade information in intervals (by seconds). For example, if you want client systems to poll clients systems every hour, enter 3600.

5 Save the changes to the mapi.cfg file.

Note: See the Scalix Administration Guide for more information about information to be included in a mapi.cfg file.

More information about mapi.cfg [AutoUpgrade] parameters

This section provides a reference guide (in table format) to all the Auto-upgrade options:

Parameter	Description
n	The mapi.cfg version number that is used to determine whether auto-upgrades occur. This number is also used to determine whether mapi.cfg is downloaded to update other administrative settings. NOTE: If the version number of the mapi.cfg file on the user system is equal to or greater than the version number of the mapi.cfg file on the server, the system does not upgrade Scalix Connect on the user system with the latest version of the MAPI service provider and/or update the mapi.cfg file.
SetupPath	The path to the shared directory that contains the source Scalix Connect installation files. The SetupPath value must be a valid UNC path. Use this parameter if you are upgrading from 9.2 to 10.x
HTTPSetupPath	The path to the shared directory that contains the source Scalix Connect installation files. The HTTPSetupPath value must be a valid http:// address. Use this parameter if you are upgrading from 9.2 to 10.x.
HTTPUpdateInstallMgr	Set this parameter to 1 to install the SXInstallMgr.exe file on user systems. When set to 0, the SXInstallMgr.exe file is not installed on local systems.
HTTPUpgradeExemptList	Allows you to specify individual users that you do not want to upgrade to the latest version of Scalix Connect.
MinimumScalixVersion	The version number of the Scalix Connect dynamic link libraries.
ForwardInstallLogsTo	Enter the administrator mailbox to which auto-upgrade results are sent. Enter off to disable error logging.
ForwardInstallLogsFrom	The text that displays in the From field of the Auto-install log message.
ForwardInstallLogsSubject	The Subject line of the e-mail that includes the auto-upgrade results.
UseLocalTimeVSGMT	Specify whether you want to use local time or Greenwich Mean Time (GMT) to auto-upgrade users. Enter 1 to use local time, or 0 to use GMT.
UpgradeIntervalTimeCheck	The (metric) time at which Scalix polls client systems to verify whether they are using the latest version of Scalix Connect. For example, enter 8 to poll for Auto-upgrade status information at 8 am. Enter 22 to poll for information at 10 pm.
	Note: Entering value of 24 or greater causes Scalix to poll for Auto-upgrade information in intervals (by seconds). For example, if you want to poll client systems every hour, enter 3600.

Activating the Auto-upgrade logging

Auto-upgrade logging enables you to view a list of those users who have (or, by absence, have not) successfully upgraded their client systems to the latest version of Scalix Connect.

Status logs are saved to a temporary file location and then automatically sent from the user system to the mailbox previously specified in the mapi.cfg **ForwardInstallLogsTo** parameter.

You can also:

- Specify the text that displays in the From field of the auto-install log messages by entering a value in the ForwardInstallLogsFrom field
- Specify the Subject of the auto-install log messages by entering a text in the ForwardInstallLogsSubject field

See the *Scalix Administration Guide* for more information about configurable options of the mapi.cfg file.

Uninstalling Scalix Connect from a Client User's PC

If you need to remove the Scalix Connect software from a Premium user's client PC, you have two options:

- Use the Microsoft Windows *Add/Remove Programs* control panel
- Run the Scalix Installer wizard, which includes an "uninstallation" option

The Installer Wizard option is described in the following section:

Using the Installer "Uninstaller"

The following can be accomplished only by a user with "administration" privileges.

1. Insert the Scalix Installation CD into the CD ROM drive, or go to the network directory that contains Scalix installation files.
2. Double-click the setup.exe icon.
3. When the Repair/Remove window displays, select **Remove** and click **Next**.
4. When the process is complete, click Finish.

Alert	Do not remove Scalix Connect by deleting the component files. Many of these files (especially .dll files) might be used by other applications.