



Cisco Self-Service Phone Administration Installation and User Guide

Release 1.0
January, 2004

Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
<http://www.cisco.com>
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

Text Part Number: OL-5342-01



THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

CCIP, CCSP, the Cisco Arrow logo, the Cisco *Powered* Network mark, Cisco Unity, Follow Me Browsing, FormShare, and StackWise are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, and iQuick Study are service marks of Cisco Systems, Inc.; and Aironet, ASIST, BPX, Catalyst, CCDA, CCDP, CCIE, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, the Cisco IOS logo, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Empowering the Internet Generation, Enterprise/Solver, EtherChannel, EtherSwitch, Fast Step, GigaStack, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, LightStream, MGX, MICA, the Networkers logo, Networking Academy, Network Registrar, *Packet*, PIX, Post-Routing, Pre-Routing, RateMUX, Registrar, ScriptShare, SlideCast, SMARTnet, StrataView Plus, Stratm, SwitchProbe, TeleRouter, The Fastest Way to Increase Your Internet Quotient, TransPath, and VCO are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0401R)

Cisco SPA Installation and User Guide

Copyright © 2004 Cisco Systems, Inc. All rights reserved.



Preface vii

Purpose	vii
Audience	vii
Scope	viii
Related Documents Available on Cisco.com	viii
Online Help	viii
Conventions Used in This Guide	ix
Obtaining Documentation	ix
Cisco.com	ix
Ordering Documentation	x
Documentation Feedback	x
Obtaining Technical Assistance	x
Cisco TAC Website	x
Opening a TAC Case	xi
TAC Case Priority Definitions	xi
Obtaining Additional Publications and Information	xi

CHAPTER 1

Overview of Cisco SPA 1-1

About the Cisco SPA Workflow	1-1
About Cisco SPA	1-3
About Cisco SPA Applications	1-4
About the Cisco SPA Operation and Configuration Tool	1-4
About the Cisco SPA Web Server Application	1-5
About Cisco SPA in the Network Architecture	1-6
About Cisco SPA and Cisco BTS 10200 Softswitch Communications	1-6
About Cisco SPA User Levels	1-7
About Cisco SPA Service Provider Administrators	1-8
About Cisco SPA Account Administrators	1-9
About Cisco SPA Group Administrators (Optional)	1-10
About Cisco SPA End Users	1-10
About Cisco SPA Security	1-11
About Supported Phone Features in Cisco SPA	1-11
Call Forwarding Features	1-12

Call Management Features	1-12
Enterprise Features	1-12
Miscellaneous Features	1-12
Speed-Dialing Features	1-13

CHAPTER 2

Cisco BTS 10200 Softswitch Provisioning Prerequisites for Cisco SPA 2-1

About Cisco BTS 10200 Softswitch Provisioning for Cisco SPA	2-1
Creating an Account on Cisco SPA	2-2
Managing Phones on Cisco SPA	2-3
Managing End User Phones in Cisco SPA	2-3

CHAPTER 3

Installing Cisco SPA 3-1

About Prerequisites for Installing Cisco SPA	3-1
About Installing Cisco SPA Packages	3-1
Installing Cisco SPA	3-2
About Uninstalling Cisco SPA Packages	3-3
Uninstalling Cisco SPA	3-3
About Cisco SPA Upgrades and Downgrades	3-4
Upgrading Cisco SPA	3-5
Downgrading Cisco SPA	3-7

CHAPTER 4

Operating and Configuring Cisco SPA 4-1

After Installing Cisco SPA	4-1
Starting and Stopping Cisco SPA	4-1
Logging In to Cisco SPA	4-2
About Cisco SPA Operation and Configuration Tool Features	4-2
Starting the Cisco SPA Operation and Configuration Tool	4-2
About Using the Tabs in Cisco SPA OCT	4-3
Using the Status Tab	4-4
About the Operations Tab	4-4
Using the Configuration Tab	4-8
Implementing Cisco SPA Configuration Changes	4-11
About Enabling SSL Connections on Cisco SPA	4-12
Task 1: Generating and Downloading a Certificate Signing Request File	4-12
Task 2: Sending the Certificate Signing Request File to a Certificate Signing Authority	4-13
Task 3: Importing the New Certificate and Root Certificate	4-13
Branding Tab	4-13
Validation Tab	4-14

About the Audit Tool	4-15
Running the Audit Tool	4-15
About the Bulk Load Function	4-17
Location of Bulk Load Directories	4-17
Location of the Document Type Definition (DTD) File	4-17

CHAPTER 5

Troubleshooting Cisco SPA	5-1
Troubleshooting Cisco SPA	5-1
About Cisco SPA Alarms	5-2

INDEX



Preface

This Preface contains the following topics:

- Purpose, page vii
- Audience, page vii
- Scope, page viii
- Related Documents Available on Cisco.com, page viii
- Online Help, page viii
- Obtaining Documentation, page ix
- Documentation Feedback, page x
- Obtaining Technical Assistance, page x
- Obtaining Additional Publications and Information, page xi

Purpose

The *Cisco Self-Service Phone Administration Installation and User Guide* provides the following information:

- Overview of the Cisco Self-Service Phone Administration (Cisco SPA) product
- Cisco BTS10200 Softswitch product provisioning procedures that must be completed in order for Cisco SPA to manage phones in the network
- Installation and upgrade procedures
- Configuration, operation, and maintenance tasks
- Alarms and recovery procedures

Additional sources of information are listed under the “Related Documents Available on Cisco.com” section on page viii and the “Online Help” section on page viii.

Audience

The primary audience for this guide consists of service provider administrators who use Cisco SPA to create accounts and groups to effectively manage phones on the network.

Scope

This document describes Cisco SPA in the context of the Cisco BTS10200 Softswitch. Cisco SPA is installed in a network that contains an installed, provisioned, and operating Cisco BTS10200 with its necessary components.

Installation and provisioning procedures for the Cisco BTS10200 Softswitch are described in the documents listed in the “Related Documents Available on Cisco.com” section that follows.

Related Documents Available on Cisco.com

In addition to this user guide, these related documents contain information pertinent to the Cisco SPA product:

- *Cisco Self-Service Phone Administration Release Notes*
- *Cisco BTS 10200 Softswitch Release Notes for Release 4.1*
- *Cisco BTS 10200 Softswitch Operations, Maintenance, and Troubleshooting*
- *Cisco BTS 10200 Softswitch Release 4.1 Provisioning Guide*
- *Cisco BTS 10200 Softswitch Release 4.1 Command Line Interface Reference Guide*
- *Cisco BTS 10200 Softswitch CORBA Programmer's Specification*
- *Cisco BTS 10200 Softswitch System Description*

Online Help

Cisco SPA contains extensive online help that you access by clicking **Help** in the upper right corner of the window.



Cisco SPA online help provides window- and field-level help as you navigate through the application windows. For additional information see the “About Cisco SPA User Levels” section on page 1-7.

Conventions Used in This Guide



Note

This guide contains illustrations of Cisco SPA windows. While every effort is made to show the latest versions of these windows, there may be some differences between windows in this guide and actual application windows.

Convention	Description
bold	Command or keyword that you must enter.
<i>italic</i>	Argument for which you supply a value.
[x]	Optional keyword or argument that you enter.
{x y z}	Required keyword or argument that you must enter.
[x {y z}]	Optional keyword or argument that you enter with a required keyword or argument.
string	Set of characters that you enter. Do not use quotation marks around the character string, or the string will include the quotation marks.
window	Information that appears on the window.
^ or Ctrl	Control key—for example, ^D means press the Control and the D keys simultaneously.
< >	Nonprinting characters, such as passwords.
!	Comment line at the beginning of a line of code.

Obtaining Documentation

Cisco documentation and additional literature are available on Cisco.com. Cisco also provides several ways to obtain technical assistance and other technical resources. These sections explain how to obtain technical information from Cisco Systems.

Cisco.com

You can access the most current Cisco documentation on the World Wide Web at this URL:

<http://www.cisco.com/univercd/home/home.htm>

You can access the Cisco website at this URL:

<http://www.cisco.com>

International Cisco websites can be accessed from this URL:

http://www.cisco.com/public/countries_languages.shtml

Ordering Documentation

You can find instructions for ordering documentation at this URL:

http://www.cisco.com/univercd/cc/td/doc/es_inpk/pdi.htm

You can order Cisco documentation in these ways:

- Registered Cisco.com users (Cisco direct customers) can order Cisco product documentation from the Ordering tool:

<http://www.cisco.com/en/US/partner/ordering/index.shtml>

- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco Systems Corporate Headquarters (California, USA) at 408 526-7208 or, elsewhere in North America, by calling 800 553-NETS (6387).

Documentation Feedback

You can submit e-mail comments about technical documentation to bug-doc@cisco.com.

You can submit comments by using the response card (if present) behind the front cover of your document or by writing to the following address:

Cisco Systems
Attn: Customer Document Ordering
170 West Tasman Drive
San Jose, CA 95134-9883

We appreciate your comments.

Obtaining Technical Assistance

For all customers, partners, resellers, and distributors who hold valid Cisco service contracts, the Cisco Technical Assistance Center (TAC) provides 24-hour-a-day, award-winning technical support services, online and over the phone. Cisco.com features the Cisco TAC website as an online starting point for technical assistance. If you do not hold a valid Cisco service contract, please contact your reseller.

Cisco TAC Website

The Cisco TAC website provides online documents and tools for troubleshooting and resolving technical issues with Cisco products and technologies. The Cisco TAC website is available 24 hours a day, 365 days a year. The Cisco TAC website is located at this URL:

<http://www.cisco.com/tac>

Accessing all the tools on the Cisco TAC website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a login ID or password, register at this URL:

<http://tools.cisco.com/RPF/register/register.do>

Opening a TAC Case

Using the online TAC Case Open Tool is the fastest way to open P3 and P4 cases. (P3 and P4 cases are those in which your network is minimally impaired or for which you require product information.) After you describe your situation, the TAC Case Open Tool automatically recommends resources for an immediate solution. If your issue is not resolved using the recommended resources, your case will be assigned to a Cisco TAC engineer. The online TAC Case Open Tool is located at this URL:

<http://www.cisco.com/tac/caseopen>

For P1 or P2 cases (P1 and P2 cases are those in which your production network is down or severely degraded) or if you do not have Internet access, contact Cisco TAC by telephone. Cisco TAC engineers are assigned immediately to P1 and P2 cases to help keep your business operations running smoothly.

To open a case by telephone, use one of the following numbers:

Asia-Pacific: +61 2 8446 7411 (Australia: 1 800 805 227)

EMEA: +32 2 704 55 55

USA: 1 800 553-2447

For a complete listing of Cisco TAC contacts, go to this URL:

<http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml>

TAC Case Priority Definitions

To ensure that all cases are reported in a standard format, Cisco has established case priority definitions.

Priority 1 (P1)—Your network is “down” or there is a critical impact to your business operations. You and Cisco will commit all necessary resources around the clock to resolve the situation.

Priority 2 (P2)—Operation of an existing network is severely degraded, or significant aspects of your business operation are negatively affected by inadequate performance of Cisco products. You and Cisco will commit full-time resources during normal business hours to resolve the situation.

Priority 3 (P3)—Operational performance of your network is impaired, but most business operations remain functional. You and Cisco will commit resources during normal business hours to restore service to satisfactory levels.

Priority 4 (P4)—You require information or assistance with Cisco product capabilities, installation, or configuration. There is little or no effect on your business operations.

Obtaining Additional Publications and Information

Information about Cisco products, technologies, and network solutions is available from various online and printed sources.

- Cisco Marketplace provides a variety of Cisco books, reference guides, and logo merchandise. Go to this URL to visit the company store:

<http://www.cisco.com/go/marketplace/>

- The Cisco *Product Catalog* describes the networking products offered by Cisco Systems, as well as ordering and customer support services. Access the Cisco Product Catalog at this URL:

<http://cisco.com/univercd/cc/td/doc/pcat/>

- *Cisco Press* publishes a wide range of general networking, training and certification titles. Both new and experienced users will benefit from these publications. For current Cisco Press titles and other information, go to Cisco Press online at this URL:

<http://www.ciscopress.com>

- *Packet* magazine is the Cisco quarterly publication that provides the latest networking trends, technology breakthroughs, and Cisco products and solutions to help industry professionals get the most from their networking investment. Included are networking deployment and troubleshooting tips, configuration examples, customer case studies, tutorials and training, certification information, and links to numerous in-depth online resources. You can access Packet magazine at this URL:

<http://www.cisco.com/packet>

- *iQ Magazine* is the Cisco bimonthly publication that delivers the latest information about Internet business strategies for executives. You can access iQ Magazine at this URL:

<http://www.cisco.com/go/iqmagazine>

- *Internet Protocol Journal* is a quarterly journal published by Cisco Systems for engineering professionals involved in designing, developing, and operating public and private internets and intranets. You can access the Internet Protocol Journal at this URL:

<http://www.cisco.com/ipj>

- Training—Cisco offers world-class networking training. Current offerings in network training are listed at this URL:

<http://www.cisco.com/en/US/learning/index.html>



Overview of Cisco SPA

Cisco SPA enables the end user to manipulate existing phone features and query account information without service provider intervention.

This chapter contains the following topics:

- About the Cisco SPA Workflow, page 1-1
- About Cisco SPA, page 1-3
- About Cisco SPA Applications, page 1-4
- About Cisco SPA in the Network Architecture, page 1-6
- About Cisco SPA and Cisco BTS 10200 Softswitch Communications, page 1-6
- About Cisco SPA User Levels, page 1-7
- About Cisco SPA Security, page 1-11
- About Supported Phone Features in Cisco SPA, page 1-11

About the Cisco SPA Workflow

This section shows two workflows for Cisco SPA. Figure 1-1 shows the workflow for a new Cisco BTS 10200 Softswitch and Cisco SPA customer, whereas Figure 1-2 shows the workflow for an existing Cisco BTS 10200 Softswitch customer who has installed Cisco SPA for the first time.

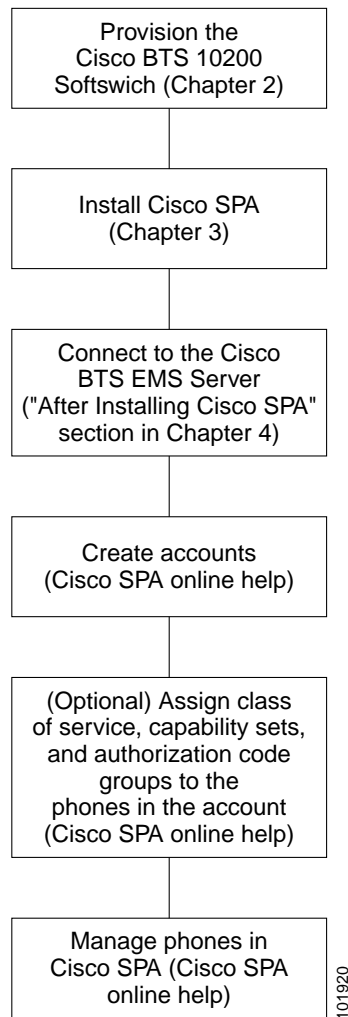
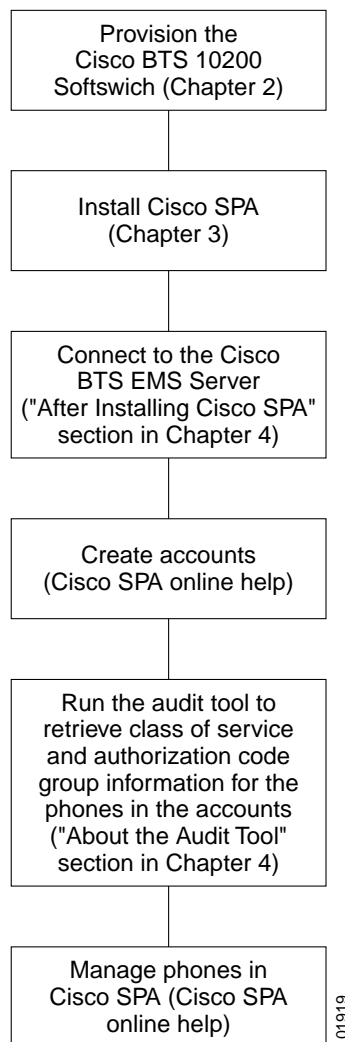
Figure 1-1 Workflow for New Cisco BTS 10200 Customers

Figure 1-2 Workflow for Existing Cisco BTS 10200 Customers

About Cisco SPA

Cisco SPA is an add-on product to the Cisco BTS 10200 Softswitch and allows phones to be organized into accounts and managed by non service personnel. This reduces service provider costs while enhancing the user's product experience. When the service provider has installed Cisco SPA and configured it by using the Cisco SPA operation and configuration tool, all that remains is creating accounts for users to manage their own phones. The Cisco SPA GUI interface is designed to be self-explanatory, and specific user tasks are accomplished by navigating the windows and consulting the help files that are included. The Cisco SPA application and the Cisco SPA operation and configuration tool are described in the "About Cisco SPA Applications" section on page 1-4.

Cisco SPA is based on accounts and their management. An account has the following characteristics:

- An account identifies (and is assigned to) a customer of the service provider. The customer can be an enterprise or residential user.
- An account consists of a logical grouping of phones, their assigned features, and related data.

Cisco SPA users have the following characteristics:

- A user exists within an account.
- Phones are assigned to users.
- The four types of Cisco SPA users are as follows:
 - Service provider administrator (see the “About Cisco SPA Service Provider Administrators” section on page 1-8)
 - Account administrator (see the “About Cisco SPA Account Administrators” section on page 1-9)
 - Group administrator (see the “About Cisco SPA Group Administrators (Optional)” section on page 1-10)
 - End user (see the “About Cisco SPA End Users” section on page 1-10)

About Cisco SPA Applications

Cisco SPA consists of two applications:

- Cisco SPA operation and configuration tool (see the “About the Cisco SPA Operation and Configuration Tool” section on page 1-4)
- Cisco SPA web server application (see the “About the Cisco SPA Web Server Application” section on page 1-5)

About the Cisco SPA Operation and Configuration Tool

The Cisco SPA operation and configuration tool is used by service providers to set up, configure, and operate the Cisco SPA web server application. This is a standalone (not web-based) GUI application that runs directly on the hardware platform on which Cisco SPA is installed. With this tool, you can configure initial settings as well as perform maintenance in the following areas:

- Customize Cisco SPA with your product brand
- Manage databases
- Configure Cisco BTS 10200 Softswitch connections
- Configure web servers
- Log levels of data
- Backup and restore database and configuration information
- Start and stop operations

The Cisco SPA operation and configuration tool is described in the “About Cisco SPA Operation and Configuration Tool Features” section on page 4-2.

About the Cisco SPA Web Server Application

The Cisco SPA web server application supports a number of capabilities that allow service providers to alter characteristics of the application and the content offered to end users.

- **Account management**—By using Cisco SPA windows, service providers can view and modify current accounts. For information on Cisco SPA windows, see the online help.
- **Store traps**—Service providers can check traps issued by Cisco SPA over a span of time extending up to the last 48 hours and check alarms generated by the Cisco SPA application or the underlying monitoring application. For more information, see the “Using the Configuration Tab” section on page 4-8.



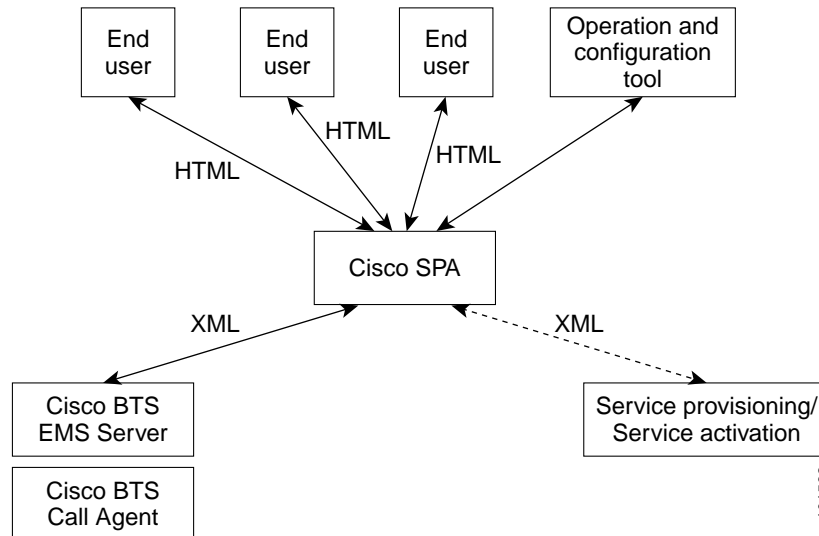
Note Cisco SPA does not manage the hardware computing platform that the application is running on. The operating system (Solaris) performs this function.

- **Security**—Cisco SPA provides intrusion detection, restricts multiple logins, and implements security checks for each Cisco SPA user level. For additional information, see the “About Cisco SPA Security” section on page 1-11.
- **Multiple user levels**—Cisco SPA enables you to establish from one to four user levels. The account administrator, group administrator, and end user are optionally created by the service provider administrator. The account administrator can also create group administrators and end users. For additional information, see the “About Cisco SPA User Levels” section on page 1-7.
- **Audit tool**—Cisco SPA contains a standalone application that compares the data in the Cisco SPA database with the data in the Cisco BTS EMS server database. For additional information, see the “Using the Audit Tab” section on page 4-5 and the “About the Audit Tool” section on page 4-15.
- **Bulk loading (XML interface)**—Use this interface to create, edit, and delete Cisco SPA accounts without using the GUI. For additional information, see the “About the Bulk Load Function” section on page 4-17.
- **Scalability**—Cisco SPA can handle up to 100,000 managed phones and up to 1000 simultaneous users. For additional information, see the “Using the Configuration Tab” section on page 4-8.
- **Localization**—Cisco SPA provides a platform that can be localized.
- **Simple Network Management Protocol (SNMP) support**—Generates trap information that can be stored on a specified server. For additional information, see the “Using the Configuration Tab” section on page 4-8.

About Cisco SPA in the Network Architecture

Figure 1-3 shows how Cisco SPA is positioned in a service provider network.

Figure 1-3 Cisco SPA Network Architecture



About Cisco SPA and Cisco BTS 10200 Softswitch Communications

The connection between Cisco SPA and the Cisco BTS 10200 Softswitch is described in the “Using the Configuration Tab” section on page 4-8.

Cisco SPA communicates with the Cisco BTS 10200 through the Common Object Request Broker Architecture (CORBA) interface. Multiple sessions including complex queries can be conducted simultaneously between the two servers.

The data on the Cisco BTS EMS server is not replicated in the Cisco SPA database. In order to avoid data synchronization issues, any references to Cisco BTS EMS server data are performed by querying the Cisco BTS EMS server.

The Cisco SPA audit tool compares information in the Cisco SPA database with that in the Cisco BTS EMS server database. If a discrepancy is detected, the audit tool displays error messages.

The audit tool is described in the “About the Audit Tool” section on page 4-15.

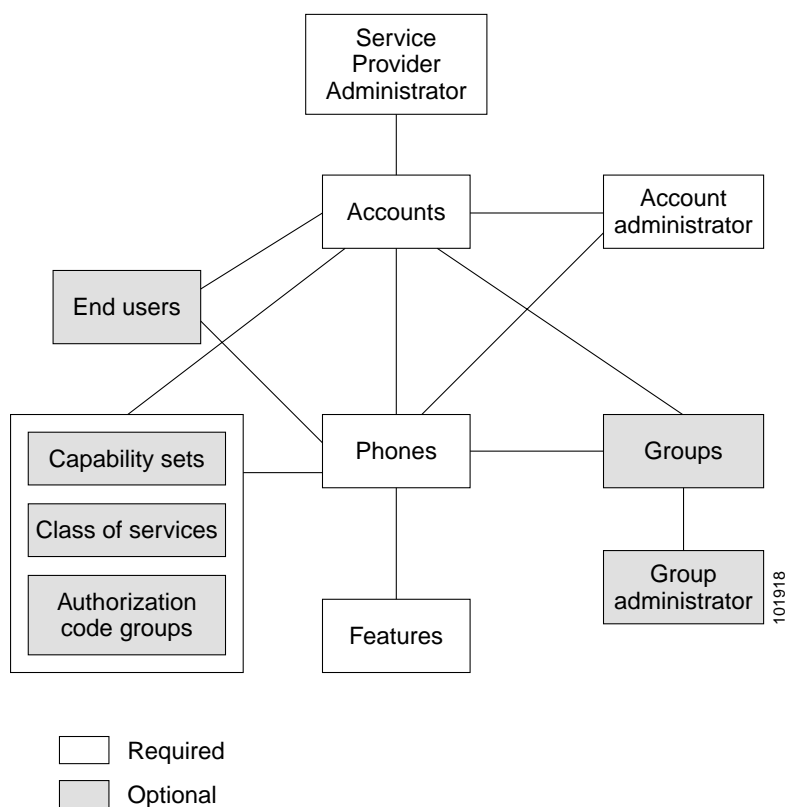
About Cisco SPA User Levels

Cisco SPA supports four levels of users who occupy a hierarchy with decreasing capabilities. From the highest to the lowest level, these users are described in the following sections:

- About Cisco SPA Service Provider Administrators, page 1-8
- About Cisco SPA Account Administrators, page 1-9
- About Cisco SPA Group Administrators (Optional), page 1-10
- About Cisco SPA End Users, page 1-10

Figure 1-4 shows the required and optional entities in Cisco SPA.

Figure 1-4 Cisco SPA Required and Optional Entities



About Cisco SPA Service Provider Administrators

Figure 1-5 Sample Service Provider Administrator Window



Service provider administrators have the highest level of access to Cisco SPA and can perform the following functions:

- Display and edit personal and account activity
- Create, modify, search, display, and delete user accounts
- Create, modify, search, and delete authorization codes
- Create, modify, search, and delete capability sets
- Create, modify, search, and delete class of services (CoS)
- Display and modify Centrex and multiline hunt groups
- Display system events and activities
- Display and modify phones
- Create, search, modify, and delete users
- Modify phone features



Note

The main users of Cisco SPA are customers of service providers (consisting of account administrators, group administrators, and end users).

About Cisco SPA Account Administrators

Figure 1-6 Sample Account Administrator Window



Account administrators have the second highest level of access to Cisco SPA. They can perform the following functions for phones and users in the account:

- Display personal and account activity
- Display user accounts
- Create, modify, search, and delete authorization codes
- Create, modify, search, and delete capability sets
- Create, search, edit, or delete class of services
- Display and modify Centrex and multiline hunt groups
- Search and modify phones
- Create, search, modify, and delete users
- Display and modify assigned phone features

About Cisco SPA Group Administrators (Optional)

Figure 1-7 Sample Group Administrator Window



Group administrators have the third highest level of access to Cisco SPA and can perform the following functions for the phones and users in the multiline hunt (MLH) or Centrex group within an account:

- Display group information
- Display and edit personal activity
- Search and display capability sets
- Modify groups
- Search and modify phones in the group
- Display and modify assigned phone features

About Cisco SPA End Users

Figure 1-8 Sample End User Window



End users have the lowest level of access to Cisco SPA and can perform the following functions for their assigned phones:

- Display and edit personal activity
- Display and modify assigned phone features

About Cisco SPA Security

Cisco SPA supports an HTTP-based interface for a web-based end user self-management GUI. This interface uses a combination of hypertext transfer protocol secure (HTTPS) and secure sockets layer (SSL) for security purposes. Access to this interface is through a known URL provided by the service provider. The HTTP connection is described in the “Using the Configuration Tab” section on page 4-8.

Cisco SPA security features consist of the following:

- Detecting intrusion—Cisco SPA logs and maintains a counter for the number of invalid login attempts for a user ID. The allowed number of consecutive failed passwords is configurable. When this number is exceeded, the user ID is locked and an alarm occurs. For additional information, see the “Using the Configuration Tab” section on page 4-8.

When you log in successfully, the failed login counter is reset.

Service provider and account administrators can unlock a locked user ID. For additional information, see the “Using the Configuration Tab” section on page 4-8.

- Restricting multiple logins—If you are already logged in to Cisco SPA and attempt to access the login page again from the same browser window, you are redirected to the Cisco SPA home page.

If you are already logged in to Cisco SPA and attempt to access the login page again from a second browser window, your second login is successful, but the earlier session is terminated.

- Checking access for user levels—Cisco SPA implements up to four levels of security checks before data access is granted:
 - Service provider administrator—Has access to all pages and resources.
 - Account administrator—Has access to all pages except the add and edit account pages. The content displayed is limited to the administrator’s account only.
 - Group administrator—Has access to pages pertaining to the group. This level of access allows the administrator to update hunt group types, update phones assigned to the group, and view capability sets in the account.
 - End user—Has access to features on the end user’s phones, personal information, and activity logs.

As each level of user is created by the administrators, Cisco SPA automatically sets up these levels of access.

About Supported Phone Features in Cisco SPA

You can view your phone features by using the Cisco SPA GUI windows. The features are also described in the online help which is accessed by clicking **Help** located at the upper right corner of each window (see the “About Cisco SPA User Levels” section on page 1-7).

Cisco SPA supports the following phone features:

- Call Forwarding Features, page 1-12
- Call Management Features, page 1-12
- Enterprise Features, page 1-12
- Miscellaneous Features, page 1-12
- Speed-Dialing Features, page 1-13

Call Forwarding Features

- **Call Forward Unconditional**—Forwards all incoming calls to another telephone number until you explicitly deactivate it.
- **Call Forward Busy**—Forwards incoming calls to another telephone number when you are already on a call.
- **Call Forward No Answer**—Instructs the network to forward calls when there is no answer from the subscriber phone. A typical forwarding address is to voice mail.

Call Management Features

- **Selective Call Acceptance**—Allows you to select which calls to accept.
- **Selective Call Forwarding**—Allows you to forward specific calls to another phone number.
- **Selective Call Reject**—Allows you to block calls from a selected list of numbers.
- **Distinctive Ring Call Waiting**—Allows you to set up different ringing sequences or call waiting indicators for calls received from numbers on a specified list.

Enterprise Features

- **Do Not Disturb**—Routes incoming calls either to an announcement or to a special tone.
- **Hotline**—Allows you to connect to a predefined phone number when you lift the handset.
- **Warmline**—Allows you a predetermined time to dial a number when you lift the handset. If you do not dial a number in that time, you are automatically connected to a predefined telephone number.

Miscellaneous Features

- **Automatic Callback**—Calls the last party whom you called without you redialing the telephone number. If the called party is busy, you can hang up and activate this feature; the call is automatically connected when the called party becomes idle.
- **Anonymous Call Rejection**—Rejects calls from parties that have set their privacy features to prevent their calling number to be displayed. The called party receives no alert for incoming calls that are rejected. The incoming call is rerouted to a denial announcement, indicating that private numbers are not accepted by the called party.
- **Busy Line Verification**—Connects to the operator in order to determine if a called line is in use.
- **Customer Originated Trace**—Generates a record of an incoming unwanted call. The data that is recorded is as follows:
 - Date and time of the trace
 - Calling directory number (DN)
 - Unique or nonunique nature of the calling DN
 - Customer's DN
 - Customer's termination ID
 - Answer indication

- Call-waiting indication
- Date and time of the call

Speed-Dialing Features

- One Digit Speed-Calling Features—Assigns a one digit code to frequently called numbers.
- Two Digit Speed-Calling Features—Assigns a two digit code to frequently called numbers.



Cisco BTS 10200 Softswitch Provisioning Prerequisites for Cisco SPA

Before installing and operating Cisco SPA, preprovision the Cisco BTS 10200 Softswitch with subscribers and have the phones working. You do not need to create all the components described in this chapter for each Cisco SPA addition; some components may have already been created by service providers.



Note

You must complete Cisco BTS Softswitch provisioning before creating accounts and assigning phones that will be managed by Cisco SPA.

This section contains the following topics:

- About Cisco BTS 10200 Softswitch Provisioning for Cisco SPA, page 2-1
- Creating an Account on Cisco SPA, page 2-2
- Managing Phones on Cisco SPA, page 2-3
- Managing End User Phones in Cisco SPA, page 2-3



Note

This chapter is not a comprehensive guide to provisioning the Cisco BTS 10200 Softswitch. Tasks that are listed here are fully described in the *Cisco BTS 10200 Softswitch Release 4.1 Provisioning Guide*.

About Cisco BTS 10200 Softswitch Provisioning for Cisco SPA



Note

The term *subscriber* in this section represents all user levels (account administrator, group administrator, and end user) that are below the service provider administrator.

Provision these components that directly or indirectly affect Cisco SPA operation:

- Add media gateway profiles—Required when new types of Customer Provided Equipment (CPE) are deployed.
- Add quality of service (QoS)—Required if new codec negotiation control is needed (not a typical operation).
- Add digit maps—Required if the subscriber is the first customer in a new geographical location.

- Add link-state advertisements (LSAs)—Required if the subscriber is the first customer in a new geographical location.
 - Add points of presence (POPs)—Required if the subscriber is the first customer in a new geographical location.
 - Add office codes—Required if the subscriber is allocated phone numbers that are beyond the current range assigned.
 - Add local access and transport areas (LATA)—Required if the subscriber is the first customer in a new geographical location.
 - Add LATA maps—Required if the subscriber is the first customer in a new geographical location.
 - Add features—Required for new installations or upgrades of the Cisco BTS 10200 Softswitch or when new features are offered to subscribers (not a typical operation).
 - Add services—Required if a new common package of features is to be offered to the subscriber.
 - Add policies—Required if the subscriber has specific and unique routing needs.
 - Add dial plans—Required if the subscriber is the first customer in a new geographical location.
-
- Add subscriber profiles—May be required if a new type of subscriber is created.
 - Add Centrex groups—Required when a new Centrex group is requested.
 - Add custom dial plan profiles—Required for a new subscriber.
 - Add custom dial plans—Required for a new subscriber.
 - Add Call Park subscriber groups—Required for a new Centrex group.
-
- Add media gateways—Required when new customer premises equipment (CPE) is deployed.
 - Add terminations—Required when new CPE is deployed.
 - Add subscribers—Required when new phone numbers are assigned.
 - Add subscriber service profiles—Required when new phone numbers are allocated.
 - Add multiline hunt (MLH) groups—Required when a new MLH group is requested.

**Note**

In order for Cisco SPA to make calls, all media gateways, terminations, and subscribers added to the Cisco BTS EMS server must be in service and operational.

Creating an Account on Cisco SPA

This section lists the steps that the service provider must perform to add an account to Cisco SPA. For details on how to complete each step, see the *Cisco BTS 10200 Softswitch Release 4.1 Provisioning Guide*.

**Tip**

When you create Centrex or multiline hunt (MLH) groups on the Cisco BTS 10200 Softswitch, make sure that you enter a value in the MainSubscriberId field. This field is optional for operating the Cisco BTS 10200 Softswitch, but is mandatory when operating Cisco SPA.

Step 1 Create the required subscribers on the Cisco BTS 10200 Softswitch.

- Step 2** Activate the media gateways, terminations, and subscribers on the Cisco BTS 10200 Softswitch.
- Step 3** Add subscriber service profiles to the Cisco BTS 10200 Softswitch for each requested subscriber. This establishes a default setting for new subscribers.
- Step 4** From the Add New Account window in Cisco SPA, add an account. This establishes that the account belongs to Cisco SPA.
- Step 5** Add Centrex or MLH groups to the Cisco BTS 10200 Softswitch (if required).
- Step 6** Supply the account administrator with the following:
- Account administrator ID
 - Password

**Note**

When the account is first created, all the phones are assigned to the account administrator who can then assign phones to one or more group administrators or end users.

Managing Phones on Cisco SPA

This section lists the steps that the account administrator performs to manage phones on Cisco SPA. For details on how to complete each step, see the *Cisco BTS 10200 Softswitch Release 4.1 Provisioning Guide*.

- Step 1** From the Add Capability Set in Cisco SPA, add a new capability set for phones on Cisco SPA.

**Note**

Capability sets are optional; they restrict the features (for a specific phone) that can be viewed or edited.

- Step 2** Assign the capability set to phones on Cisco SPA.
- Step 3** (Optional) Create class of service (CoS) restrictions to apply to phones on the Cisco BTS 10200 Softswitch.
- Step 4** Assign CoS restrictions to the phone on the Cisco BTS 10200 Softswitch.
- Step 5** Activate or deactivate applicable Cisco BTS 10200 Softswitch features for the phone.
- Step 6** Add a new user by navigating Cisco SPA windows.
- Step 7** Inform the user that web-based account management is now available.

Managing End User Phones in Cisco SPA

This section lists the action that the end user performs to manage phones in Cisco SPA.

- Change applicable Cisco BTS 10200 Softswitch feature settings for your phone.



Installing Cisco SPA

This chapter contains the following topics:

- About Prerequisites for Installing Cisco SPA, page 3-1
- About Installing Cisco SPA Packages, page 3-1
- Installing Cisco SPA, page 3-2
- About Uninstalling Cisco SPA Packages, page 3-3
- Uninstalling Cisco SPA, page 3-3
- About Cisco SPA Upgrades and Downgrades, page 3-4
- Upgrading Cisco SPA, page 3-5
- Downgrading Cisco SPA, page 3-7

About Prerequisites for Installing Cisco SPA

Before you install Cisco SPA, check that the Cisco BTScis package is installed on both the Cisco BTS 10200 EMS primary and secondary servers. Refer to the *Cisco BTS 10200 Softswitch Application Installation*.

You can also check if the CORBA application is running on the Cisco BTS 10200 EMS servers as described in the *Cisco BTS 10200 Softswitch Application Installation*.

About Installing Cisco SPA Packages

The Cisco SPA product consists of these packages that are installed during the installation process:

- CSCOspa—Cisco SPA application base package
- CSCOspaJV—Cisco SPA Java package
- CSCOspaTC—Cisco SPA Tomcat server package
- CSCOspaDB—Cisco SPA database package
- CSCOspaNM—Cisco SPA SNMP package

Installing Cisco SPA



Note

Install Cisco SPA on a separate server from that on which the Cisco BTS EMS server software is installed. Cisco Systems does not support the Cisco SPA application installed on the Cisco BTS EMS server or Call Agent server.

-
- Step 1** Log in as the root user.
- Step 2** Download the SPA_K9_<release>.tar.gz image from Cisco.com.
- Step 3** To uncompress and untar the Cisco SPA image, enter:
- ```
gunzip SPA_K9_<release>.tar.gz
tar -xvf SPA_K9_<release>.tar
```
- Step 4** Enter this command:
- ```
./install.sh
```
- The working Cisco SPA image is installed in the /opt/SPA directory.



Note

If you already have Cisco SPA installed and are installing the same version again, the following messages appear:

Previous installed 1.x(x) data will be used with this installation.
Continue installation of 1.x(y)? [n] [y,n,?,q]

Where,

- n**—Terminates the installation (default).
- y**—Proceeds with the installation.
- ?**—Explains the responses to this query.
- q**—Terminates the installation.

-
- Step 5** Specify a Cisco SPA user ID and group ID:
- ```
SPAUSR ID [70001]
SPA GID [70001]
```
- The default IDs are shown in brackets; press **Enter** to accept the defaults.
- As the installation proceeds, the following status messages may appear:
- Directory in which the package will be installed.
  - Package and system processing information.
  - Number of package pathnames that are installed.
  - Diskspace verification.
  - Checking for conflicts with installed packages.
- As each package is installed, a completion message appears:
- ```
Installation of <package name> was successful.
```
- When all the packages are installed, a final status message appears:
- ```
SPA installed successfully.
```



**Note**

After you install Cisco SPA, check that the Cisco BTS EMS host name (as defined on the Cisco BTS EMS host) is also defined in the `/etc/hosts` file on the Cisco SPA server.

After you have installed Cisco SPA, configure the product as described in Chapter 4, “Operating and Configuring Cisco SPA.”

## About Uninstalling Cisco SPA Packages

The following packages are uninstalled during the Cisco SPA uninstallation process:

- CSCOspaNM—Cisco SPA SNMP package
- CSCOspaDB—Cisco SPA database package
- CSCOspaTC—Cisco SPA Tomcat server package
- CSCOspaJV—Cisco SPA Java package
- CSCOspa—Cisco SPA application base package

For details, see the “Uninstalling Cisco SPA” section on page 3-3.

## Uninstalling Cisco SPA

- Step 1** Log in to the Cisco SPA server as `spausr` (see the “Starting and Stopping Cisco SPA” section on page 4-1).
- Step 2** Stop Cisco SPA operation.
- Step 3** Log in as the root user.
- Step 4** Check that you are in the directory where the uninstall script is located.
- Step 5** Run the uninstallation script by entering:

```
./uninstall.sh
```

- Step 6** Enter a response to the uninstallation query:

```
Do you want to uninstall Cisco SPA? [n] [y,n,?,q]
```

Where,

**n**—Terminates the installation (default).

**y**—Proceeds with the installation.

**?**—Explains the responses to this query.

**q**—Terminates the installation.

As the uninstallation proceeds, the following status messages may appear:

- Package dependency verification
- Package processing information
- Preremove script execution

- Stopping and restoring agents
- Removing pathnames
- Updating system information

As each package is uninstalled, a completion message appears:

```
Removal of <package name> was successful.
```

When all the packages are uninstalled, a final status message appears:

```
Removing group spagrp
```

```
Removing user spausr
```

```
SPA uninstalled successfully.
```

## About Cisco SPA Upgrades and Downgrades



### Note

Back up your data before upgrading or downgrading Cisco SPA. Database backup procedures are described in the “Using the Backup and Restore Tab” section on page 4-5.

When you upgrade to a later version of Cisco SPA, two versions of data are saved. The saved versions are the current data and the version that was created immediately before the current one.

The following table shows the various datasets that are preserved through upgrades and downgrades of Cisco SPA. Three versions of software that are shown in the table are 1.x, 1.y, and 1.z; the three sets of data are x, y, and z.

| Install | Uninstall | Current Dataset | Previous Dataset |
|---------|-----------|-----------------|------------------|
| 1.x     |           | x               |                  |
|         | 1.x       | x               |                  |
| 1.y     |           | y               | x                |
|         | 1.y       | y               | x                |
| 1.z     |           | z               | y                |
|         | 1.z       | z               | y                |
| 1.x     |           | x               | y                |
|         | 1.x       | x               | y                |
| 1.y     |           | y               | x                |

Cisco SPA informs you if there is data that can be reused with your upgrade or downgrade.

## Upgrading Cisco SPA

This procedure consists of the following tasks:

- Task 1: Downloading the New Cisco SPA Image, page 3-5
- Task 2: Stopping Cisco SPA Operation, page 3-5
- Task 3: Uninstalling the Old Cisco SPA Image, page 3-5
- Task 4: Installing the New Cisco SPA Image, page 3-6
- Task 5: Starting Cisco SPA Operation, page 3-6

**Note**

Install Cisco SPA on a separate server from that on which the Cisco BTS EMS Server software is installed. Cisco Systems does not support the Cisco SPA application installed on the Cisco BTS EMS Server or Call Agent server.

### Task 1: Downloading the New Cisco SPA Image

- 
- Step 1** Log in to the Cisco SPA server as the root user.
- Step 2** Download the SPA\_K9\_<release>.tar.gz image from Cisco.com.
- Step 3** To uncompress and untar the Cisco SPA image, enter:
- ```
gunzip SPA_K9_<release>.tar.gz
tar -xvf SPA_K9_<release>.tar
```
-

Task 2: Stopping Cisco SPA Operation

-
- Step 1** Log in to the Cisco SPA server as spausr (see the “Starting and Stopping Cisco SPA” section on page 4-1).
- Step 2** From the Cisco SPA operation and configuration tool, stop Cisco SPA operation.
-

Task 3: Uninstalling the Old Cisco SPA Image

-
- Step 1** Log in to the Cisco SPA server as the root user.
- Step 2** Check that you are in the directory where the uninstall script is located.
- Step 3** Run the uninstallation script by entering:
- ```
./uninstall.sh
```
- For details, see the “Uninstalling Cisco SPA” section on page 3-3.
-

## Task 4: Installing the New Cisco SPA Image

- Step 1** Install the new image by entering:

```
./install.sh
```

The working Cisco SPA image is installed in the /opt/SPA directory.

- Step 2** The following upgrade messages appear:

```
Upgrade Installation from 1.x(x) to 1.y(y).
```

```
Previously installed 1.x(x) data will be used or migrated with this installation.
```

```
Continue Installation of 1.y(y)? [n] [y,n,?,q]
```

Where,

**n**—Terminates the installation (default).

**y**—Proceeds with the installation.

**?**—Explains the responses to this query.

**q**—Terminates the installation.

- Step 3** Specify a Cisco SPA user ID and group ID:

```
SPAUSR ID [70001]
```

```
SPA GID [70001]
```

The default IDs are shown in brackets; press **Enter** to accept the defaults.

As each package is installed, a status message appears:

```
Installation of <package name> was successful.
```

When all the packages are installed, a final status message appears:

```
SPA installed successfully.
```

## Task 5: Starting Cisco SPA Operation

- Step 1** Log in as spaur (see the “Starting the Cisco SPA Operation and Configuration Tool” section on page 4-2).



**Note** The spaur is deleted and recreated during a Cisco SPA upgrade. Consequently, you must reset the password.

- Step 2** From the Cisco SPA operation and configuration tool, start Cisco SPA operation (see the “Starting and Stopping Cisco SPA” section on page 4-1).



**Note** After you install Cisco SPA, check that the Cisco BTS EMS host name (as defined on the Cisco BTS EMS host) is also defined in the /etc/hosts file on the Cisco SPA server.

After you have installed Cisco SPA, configure the product as described in Chapter 4, “Operating and Configuring Cisco SPA.”

## Downgrading Cisco SPA

This procedure consists of the following tasks:

- Task 1: Downloading a Previous Cisco SPA Image, page 3-7
- Task 2: Stopping Cisco SPA Operation, page 3-7
- Task 3: Uninstalling the Current Cisco SPA Image, page 3-7
- Task 4: Installing the Downloaded Cisco SPA Image, page 3-8
- Task 5: Starting Cisco SPA Operation, page 3-8

**Note**

Install Cisco SPA on a separate server from that on which the Cisco BTS EMS Server software is installed. Cisco Systems does not support the Cisco SPA application installed on the Cisco BTS EMS Server or Call Agent server.

### Task 1: Downloading a Previous Cisco SPA Image

- 
- Step 1** Log in to the Cisco SPA server as the root user.
- Step 2** Download the SPA\_K9\_<release>.tar.gz image from Cisco.com.
- Step 3** To uncompress and untar the Cisco SPA image, enter:
- ```
gunzip SPA_K9_<release>.tar.gz
tar -xvf SPA_K9_<release>.tar
```
-

Task 2: Stopping Cisco SPA Operation

-
- Step 1** Log in to the Cisco SPA server as spausr (see the “Starting and Stopping Cisco SPA” section on page 4-1).
- Step 2** From the Cisco SPA operation and configuration tool, stop Cisco SPA operation.
-

Task 3: Uninstalling the Current Cisco SPA Image

-
- Step 1** Log in to the Cisco SPA server as the root user.
- Step 2** Check that you are in the directory where the uninstall script is located.
- Step 3** Run the uninstallation script by entering:
- ```
./uninstall.sh
```
- For details, see the “Uninstalling Cisco SPA” section on page 3-3.
-

## Task 4: Installing the Downloaded Cisco SPA Image

- Step 1** Install the downloaded image by entering:

```
./install.sh
```

The working Cisco SPA image is installed in the /opt/SPA directory.

- Step 2** If Cisco SPA has saved data that can be used with the downgrade, these messages appear:

```
Downgrade Installation from 1.y(y) to 1.x(x).
Previously installed 1.x(x) data will be used or migrated with this installation.
Version 1.y(y) data will be lost with this installation.
Continue Installation of 1.y(y)? [n] [y,n,?,q]
```

If Cisco SPA has not saved data that can be used with the downgrade, these messages appear:

```
Downgrade Installation from 1.z(z) to 1.x(x).
Version 1.z(z) data will be lost with this installation.
Continue Installation of 1.x(x)? [n] [y,n,?,q]
```

Where,

**n**—Terminates the installation (default).  
**y**—Proceeds with the installation.  
**?**—Explains the responses to this query.  
**q**—Terminates the installation.

- Step 3** Specify a Cisco SPA user ID and group ID:

```
SPAUSR ID [70001]
```

```
SPA GID [70001]
```

The default IDs are shown in brackets; press **Enter** to accept the defaults.

As each package is installed, a status message appears:

```
Installation of <package name> was successful.
```

When all the packages are installed, a final status message appears:

```
SPA installed successfully.
```

## Task 5: Starting Cisco SPA Operation

- Step 1** Log in as spaur (see the “Starting the Cisco SPA Operation and Configuration Tool” section on page 4-2).



**Note** The spaur is deleted and recreated during a Cisco SPA downgrade. Consequently, you must reset the password.

- Step 2** From the Cisco SPA operation and configuration tool, start Cisco SPA operation (see the “Starting and Stopping Cisco SPA” section on page 4-1).

**Note**

---

After you install Cisco SPA, check that the Cisco BTS EMS host name (as defined on the Cisco BTS EMS host) is also defined in the `/etc/hosts` file on the Cisco SPA server.

---

After you have installed Cisco SPA, configure the product as described in Chapter 4, “Operating and Configuring Cisco SPA.”







# Operating and Configuring Cisco SPA

---

This chapter contains the following topics:

- After Installing Cisco SPA, page 4-1
- Starting and Stopping Cisco SPA, page 4-1
- Logging In to Cisco SPA, page 4-2
- About Cisco SPA Operation and Configuration Tool Features, page 4-2
- Starting the Cisco SPA Operation and Configuration Tool, page 4-2
- About Using the Tabs in Cisco SPA OCT, page 4-3
- About the Audit Tool, page 4-15
- About the Bulk Load Function, page 4-17

## After Installing Cisco SPA

When you have successfully installed Cisco SPA complete these steps before accessing the application.

- 
- |               |                                                                                                                                                                                                |
|---------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | Enter Cisco BTS EMS server information to establish a connection with the Cisco BTS EMS 10200 Softswitch (see the “Using the Configuration Tab” section on page 4-8).                          |
| <b>Step 2</b> | Set up a connection to the mail server (see the “Using the Configuration Tab” section on page 4-8).                                                                                            |
| <b>Step 3</b> | Generate and import security certificates to set up a Secure Socket Layer (SSL) connection from the service provider to Cisco SPA (see the “Using the Configuration Tab” section on page 4-8). |
| <b>Step 4</b> | If necessary, select the Use Secure HTTP Connections option (see the “Using the Configuration Tab” section on page 4-8).                                                                       |
- 

## Starting and Stopping Cisco SPA

You can start and stop Cisco SPA from the Cisco SPA configuration tool interface (see the “Using the Status Tab” section on page 4-4).

## Logging In to Cisco SPA

This section describes how to access the Cisco SPA application as an administrator by using a web browser.

- 
- Step 1** Start a web browser window. (For supported web browsers, see the *Release Notes for Cisco Self-Service Phone Administration*.)
- Step 2** Access Cisco SPA from a web browser. (For supported web browsers, see the *Release Notes for Cisco Self-Service Phone Administration*.)
- Step 3** Log in as the default administrator:
- User Name: **admin**
- Password: **admin**
- Step 4** Click **Login**.
- When you log in successfully, the failed login counter is reset.
- 

## About Cisco SPA Operation and Configuration Tool Features

After you have installed Cisco SPA, configure and customize the product by using the supplied operation and configuration tool. This tool is a standalone (not web-based) GUI application that runs directly on the hardware platform on which Cisco SPA is installed. With this tool, you can check the status of the application, configure initial settings and perform maintenance in the following areas:

- Branding customization
- Database management
- Cisco BTS 10200 Softswitch connection configuration
- Web server configuration
- Data logging level
- Backup and restore database and configuration information
- Start and stop operations

The Cisco SPA operation and configuration tool (OCT) is located in the `/opt/SPA/bin` directory.

## Starting the Cisco SPA Operation and Configuration Tool

- 
- Step 1** Log in to the server where Cisco SPA is installed:

Login: **spausr**



**Note**

The `spausr` is created at the time of Cisco SPA installation.

---

- Step 2** Set a password for future logins:

New password: **xxxxxxxx**

Reenter password: `xxxxxxxx`

Enter a new password that is up to 20 characters in length.



**Note**

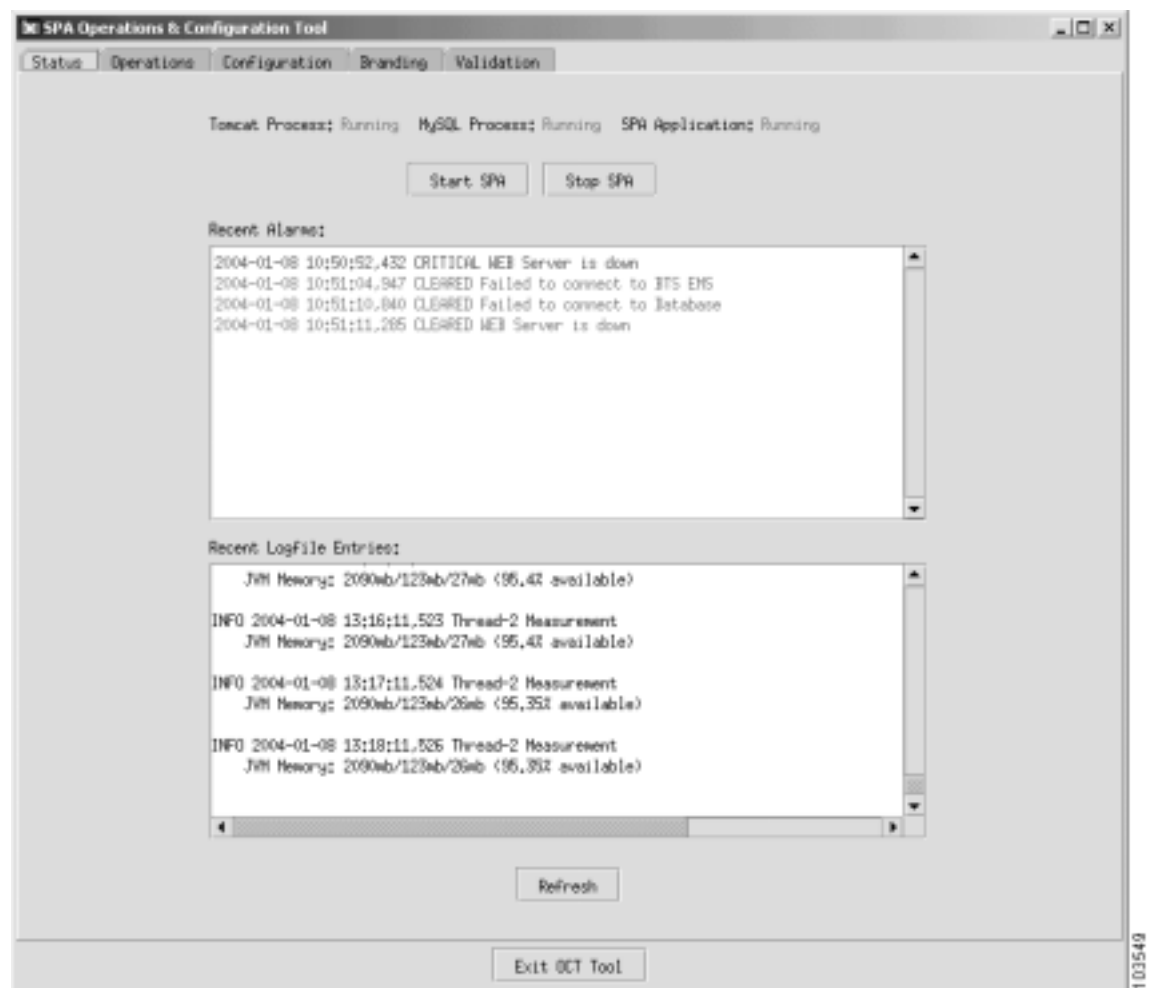
You are prompted for this password the first time that you log in (as spausr) to the Cisco SPA server.

**Step 3** Enter the following command:

```
oct.sh
```

The Cisco SPA OCT GUI opens (see Figure 4-1).

**Figure 4-1** Cisco SPA Operation and Configuration Tool



## About Using the Tabs in Cisco SPA OCT

The Cisco SPA operation and configuration tool (OCT) window contains five tabs described in the following sections:

- Using the Status Tab, page 4-4
- About the Operations Tab, page 4-4
- Using the Configuration Tab, page 4-8
- Branding Tab, page 4-13
- Validation Tab, page 4-14

**Note**

First set up the connection to the Cisco BTS 10200 Softswitch (see the “After Installing Cisco SPA” section on page 4-1; then to start the Cisco SPA application, see the “Using the Status Tab” section on page 4-4.

## Using the Status Tab

The Status tab in the Cisco SPA operation and configuration tool enables you to do the following:

- Start and stop Cisco SPA operation
- Check if Tomcat and MySQL processes are running
- Check if the Cisco SPA application is running
- View recent alarms generated by Cisco SPA
- View recent entries to Cisco SPA log files

| Field                  | Description                                                                                                                                                                                                                                                                                                                    |
|------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Tomcat Process         | Shows if this process is running. When you click <b>Start SPA</b> , the Tomcat and MySQL processes start running almost immediately, whereas the Cisco SPA application takes longer to start operation.<br><br>Click the <b>Refresh</b> button to check if processes have started running since you clicked <b>Start SPA</b> . |
| MySQL process          |                                                                                                                                                                                                                                                                                                                                |
| SPA Application        |                                                                                                                                                                                                                                                                                                                                |
| Start SPA              | Starts the Cisco SPA application.                                                                                                                                                                                                                                                                                              |
| Stop SPA               | Stops the Cisco SPA application.                                                                                                                                                                                                                                                                                               |
| Recent Alarms          | Shows recent alarms generated by Cisco SPA. <ul style="list-style-type: none"><li>• Red text indicates current alarm conditions.</li><li>• Green text indicates cleared alarm conditions.</li></ul>                                                                                                                            |
| Recent Logfile Entries | Shows recent entries to the log files located at /opt/SPA/data/log.                                                                                                                                                                                                                                                            |

## About the Operations Tab

The Operations tab in the Cisco SPA operation and configuration tool contains two tabs:

- Using the Backup and Restore Tab
- Using the Audit Tab

## Using the Backup and Restore Tab

The Backup and Restore tab enables you to do the following:

- Backup the Cisco SPA database and configuration settings either immediately or at a future time
- Restore the Cisco SPA database

| Field             | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|-------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Scheduled Backups | <p><b>Scheduling up to Five Data Backups</b></p> <ol style="list-style-type: none"> <li>1. Select a time for the backup. <ul style="list-style-type: none"> <li>– For the hour, enter a value from 0 to 23.</li> <li>– For the minute, enter a value from 00 to 59.</li> </ul> </li> <li>2. Select the days when you want the data backup to occur.</li> <li>3. Click <b>Save Schedule</b>.</li> </ol> <p>The backed up data is stored at /opt/SPA/data.</p> <p><b>Canceling a Scheduled Data Backup</b></p> <ol style="list-style-type: none"> <li>1. Select Delete for that data backup.</li> <li>2. Click <b>Save Schedule</b>.</li> </ol> |
| Save Schedule     | To save any changes to the scheduled data backups, click <b>Save Schedule</b> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| Backup Now        | <p>Starts an immediate data backup.</p> <p>You are prompted for a location where the data will be stored.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| Restore           | You are prompted to choose a dataset that you want to restore.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |



## Using the Audit Tab

The Audit tab enables you to schedule future audits that compare the data in the Cisco SPA database with the data in the Cisco BTS EMS server database. You can narrow the scope of the audit by selecting specific components to be audited.



### Note

To perform immediate database audits, follow the procedure described in “Running the Audit Tool” section on page 4-15.

| Field            | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Scheduled Audits | <p>You can schedule up to five database audits:</p> <ol style="list-style-type: none"> <li>1. Select a time for the audit. <ul style="list-style-type: none"> <li>– For the hour, enter a value from 0 to 23.</li> <li>– For the minute, enter a value from 00 to 59.</li> </ul> </li> <li>2. Select the days on which the audit will occur.</li> <li>3. Click <b>Save Schedule</b>.</li> </ol> <p>The audit results are stored at in a timestamped log file called <code>audit.log.yyyy-mm-dd_hh:mm:ss</code> which is located at <code>/opt/SPA/data/logs</code>.</p> <p>Where,</p> <p><code>yyyy-mm-dd</code> is the date (year, month, and day) when the audit was started.</p> <p><code>hh:mm:ss</code> is the time (hour, minute, and second) when the audit was started.</p> <p> <b>Tip</b> The audit function stores seven days of audit results.</p> <p><b>Canceling a Scheduled Database Audit</b></p> <ol style="list-style-type: none"> <li>1. Select Delete for that audit.</li> <li>2. Click <b>Save Schedule</b>.</li> </ol> |
| Options          | <p>To run a complete audit of all components, select all the options.</p> <p> <b>Note</b> To further restrict the scope of the audit, see the “Running the Audit Tool” section on page 4-15.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| Phones           | <ul style="list-style-type: none"> <li>• The audit tool checks if the phones on Cisco SPA exist in the Cisco BTS EMS server database. If a discrepancy is detected, the audit tool displays a message. For more information on messages, see the “About Cisco SPA Alarms” section on page 5-2.</li> <li>• The audit tool checks if phones in Centrex and multiline hunt groups on the Cisco BTS EMS server also exist on Cisco SPA. If a discrepancy is detected, the audit tool displays a message. For more information on messages, see the “About Cisco SPA Alarms” section on page 5-2.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |

| Field | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|-------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| COS   | <ul style="list-style-type: none"><li>• Checks if each class of services in Cisco SPA exists on the Cisco BTS EMS server. If a discrepancy is detected, the audit tool displays a message and the class of services is deleted from Cisco SPA. For more information on messages, see the “About Cisco SPA Alarms” section on page 5-2.</li><li>• Checks which phones are using each class of service on the Cisco BTS EMS server.<ul style="list-style-type: none"><li>– If a class of services is being used by phones assigned to more than one Cisco SPA account, the audit tool displays a message. A class of service ID is unique and can be used by only one account. For more information on messages, see the “About Cisco SPA Alarms” section on page 5-2.</li><li>– If a class of services is being used by phones on the Cisco BTS EMS server that are not on Cisco SPA, the audit tool displays a message. For more information on messages, see the “About Cisco SPA Alarms” section on page 5-2.</li><li>– If a class of services is not in the Cisco SPA database and there are no other errors, the audit tool displays a message and adds the class of service to the Cisco SPA database. For more information on messages, see the “About Cisco SPA Alarms” section on page 5-2.</li></ul></li></ul> |


| Field         | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|---------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| AC Group      | <ul style="list-style-type: none"> <li>• The audit tool checks if each authorization code group in the Cisco SPA database also exists on the Cisco BTS EMS server. If a discrepancy is detected, the audit tool displays a message and deletes the authorization code group from the Cisco SPA database.</li> <li>• The audit tool checks which class of services are using which authorization code group on the Cisco BTS EMS server. <ul style="list-style-type: none"> <li>– If an authorization code group on the Cisco BTS EMS server is being used by class of services in more than one Cisco SPA account, the audit tool displays a message. An authorization code group ID is unique and can be used by only one account. For more information on messages, see the “About Cisco SPA Alarms” section on page 5-2.</li> <li>– If an authorization code group is not in the Cisco SPA database and there are no other errors, the authorization code group is added to the Cisco SPA database, and the audit tool displays a message. For more information on messages, see the “About Cisco SPA Alarms” section on page 5-2.</li> </ul> </li> </ul> |
| Save Schedule | Saves any changes to the scheduled database audits.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |



## Using the Configuration Tab



The Configuration tab in the Cisco SPA operation and configuration tool enables you to do the following:

- Set up connectivity to the Cisco BTS EMS server
- Specify security parameters
- Import and generate security certificates
- Specify e-mail contact information
- Select secure HTTP connections
- Select a data logging level
- Perform administrative functions such as resetting the administrator’s password and unlocking the root account user
- Specify SNMP parameters



| Field                     | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|---------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| BTS Connection            |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| EMS Host Name             | <p>Enter the name or IP address of the Cisco BTS EMS server where the Cisco BTS 10200 Softswitch is installed.</p> <p> <b>Note</b> If you are using the IP aliasing feature on the Cisco BTS 10200 Softswitch, enter an IP address for this field.</p> <p>If you are not using the IP aliasing feature, enter either an IP address or a host name.</p>                                         |
| EMS Port Number           | <p>Enter the port number on the Cisco BTS EMS server that communicates with Cisco SPA.</p> <p>The default is 14001.</p>                                                                                                                                                                                                                                                                                                                                                         |
| EMS Site ID               | Enter the site ID of the Cisco BTS EMS server.                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| EMS Login User ID         | Login name that is already set on the Cisco BTS EMS server.                                                                                                                                                                                                                                                                                                                                                                                                                     |
| EMS Login Password        | <p>This password is used for the Cisco SPA application to log in to the Cisco BTS EMS server. If the Cisco BTS EMS server login password changes, you must specify a new password for Cisco SPA to communicate with the Cisco BTS EMS server.</p> <ol style="list-style-type: none"> <li>1. Enter a new password that is up to 20 characters in length.</li> <li>2. Verify the new password.</li> <li>3. Click <b>Save Configuration</b> to accept the new password.</li> </ol> |
| Confirm Password          |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| Number of BTS Connections | Enter the number of simultaneous connections allowed between Cisco SPA and the Cisco BTS EMS server.                                                                                                                                                                                                                                                                                                                                                                            |
| Security                  |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| SPAUSR Database Password  | <ol style="list-style-type: none"> <li>1. Enter a new password that is up to 20 characters in length.</li> <li>2. Verify the new password.</li> <li>3. Click <b>Save Configuration</b> to accept the new password.</li> </ol>                                                                                                                                                                                                                                                   |
| Confirm Password          |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| SPAROOT Database Password |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| Confirm Password          |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |

| Field                                           | Description                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|-------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Lock User Account after...failed login attempts | <p>Cisco SPA logs and maintains a counter for the number of consecutive failed passwords for a user ID. When this number is exceeded, the user ID is locked, and an alarm occurs.</p> <p>Enter a value in the range 1 to 6; the default is 5.</p> <p>The service provider or account administrator can unlock the user ID (see the Unlock Root Account field in this table).</p>                                                                    |
| Session Timeout (minutes)                       | Enter a value in the range 5 to 30; the default is 10.                                                                                                                                                                                                                                                                                                                                                                                              |
| Use Secure HTTP Connections                     | <p>For secure HTTP connections, select this checkbox.</p> <p>For secure connections, the port used is 443; for nonsecure connections, the port used is 80.</p>                                                                                                                                                                                                                                                                                      |
| SNMP                                            |                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| Community String                                | <p>Enter one of the following:</p> <ul style="list-style-type: none"> <li>• public—Same as RO (read-only).</li> <li>• private—Same as RW (read-write).</li> </ul>                                                                                                                                                                                                                                                                                   |
| Manager Host IP Address for Traps               | The IP address of the host where SNMP traps are stored.                                                                                                                                                                                                                                                                                                                                                                                             |
| Email Information                               |                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| Mail Server Name                                | Enter the name of the outgoing mail server that sends new passwords or user ID reminders.                                                                                                                                                                                                                                                                                                                                                           |
| Mail from Address                               | <p>Enter the sending address that is sent on password and user ID reminders.</p> <p></p> <p><b>Tip</b> Enter an invalid e-mail address, so that users do not reply to it.</p>                                                                                                                                                                                    |
| Logging                                         | <p>Select a level at which data will be logged:</p> <ul style="list-style-type: none"> <li>• Debug</li> <li>• Information</li> <li>• Warning</li> <li>• Error</li> <li>• Fatal</li> </ul> <p></p> <p><b>Note</b> Select the Debug log level for troubleshooting purposes only. During normal system operation, select either the Warning or Error log level.</p> |
| Keep log files for....                          | Enter a value in the range 1 to 30 days; the default is 7.                                                                                                                                                                                                                                                                                                                                                                                          |
| Miscellaneous                                   |                                                                                                                                                                                                                                                                                                                                                                                                                                                     |

| Field                | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|----------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Reset Admin Password | <p>To reset the current password to the default value of “admin,” click <b>Reset Admin Password</b>.</p>  <p><b>Note</b> This is the password that the admin user ID uses to log in to the Cisco SPA application.</p> <p>If the service provider root administrator account is locked, this button does not automatically unlock it. Click <b>Unlock Root Account</b> to unlock the account.</p> |
| Unlock Root Account  | <p>To unlock the root account, click this button.</p> <p>This action is necessary when the service provider root administrator has not created additional service provider administrators and is then locked out of the application because failed password attempts exceed the maximum number allowed.</p> <p>The maximum number of failed password attempts is specified in the “Lock User Account after...failed login attempts” field in this table.</p>                      |
| Import Certificate   | <p>To set up a Secure Socket Layer (SSL) connection from the service provider to Cisco SPA, see the “About Enabling SSL Connections on Cisco SPA” section on page 4-12.</p>                                                                                                                                                                                                                                                                                                       |
| Generate Certificate |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| Save Configuration   | <p>Click <b>Save Configuration</b> to save all changes that you make to this window.</p>  <p><b>Note</b> In order for configuration changes to take effect, first stop Cisco SPA (see the “Using the Status Tab” section on page 4-4), then click <b>Save Configuration</b>.</p>                                                                                                               |

## Implementing Cisco SPA Configuration Changes

In order for configuration changes to take effect, complete these steps:

- 
- Step 1** Stop Cisco SPA (see the “Using the Status Tab” section on page 4-4).
  - Step 2** Make changes on the Configuration tab.
  - Step 3** Click **Save Configuration**.

If Cisco SPA is running when you click **Save Configuration**, you are prompted to stop Cisco SPA and then click **Save Configuration**. If you leave the Configuration tab to stop Cisco SPA, your changes are kept intact until you return to save them.

---

# About Enabling SSL Connections on Cisco SPA


To set up a Secure Socket Layer (SSL) to Cisco SPA, follow these procedures:

- Task 1: Generating and Downloading a Certificate Signing Request File, page 4-12
- Task 2: Sending the Certificate Signing Request File to a Certificate Signing Authority, page 4-13
- Task 3: Importing the New Certificate and Root Certificate, page 4-13

## Task 1: Generating and Downloading a Certificate Signing Request File

- Step 1
- Log in to Cisco SPA as described in “Starting the Cisco SPA Operation and Configuration Tool” section on page 4-2.
- Step 2
- Select the Configuration tab.
- Step 3
- Click **Generate Certificate**.

Enter information in the Generate Key dialog fields:

| Field                                                                                | Description                                                                                                                                                                                                                                |
|--------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Host Name                                                                            | Enter the name of the server on which Cisco SPA is installed.                                                                                                                                                                              |
| Organizational Unit                                                                  | Enter the name of your company.                                                                                                                                                                                                            |
| Organization                                                                         | Enter the name of your organization within your company.                                                                                                                                                                                   |
| City or Locality                                                                     | Enter the name of your city.                                                                                                                                                                                                               |
| State or Province                                                                    | Enter the name of your state.                                                                                                                                                                                                              |
| Two Character Country Code                                                           | Enter the code for your country.                                                                                                                                                                                                           |
| Replace existing certificate file                                                    | Select this option to generate a new certificate. <div><div><b>Note</b> If you do not select this option, the existing certificate is used.</div></div> |
| Create a Certificate Signing Request File to send to Server Certificate Authorities. |                                                                                                                                                                                                                                            |
| Certificate File Name                                                                | Enter a location where the Certificate Signing Request (CSR) File will be stored. <div>The default storage location is /opt/SPA/spa_request.csr.</div>                                                                                     |

- Step 4
- Click **OK**.
- Step 5
- Download the spa\_request.csr file to your PC.

## Task 2: Sending the Certificate Signing Request File to a Certificate Signing Authority

- 
- Step 1** For signing, send the spa\_request.csr file to a Certificate Signing Authority (CSA), such as Verisign (www.verisign.com).
- Step 2** To get the CSR signed, follow the CSA's instructions.  
The CSA sends back a signed certificate.
- Step 3** Save the signed certificate in the signed-cert.txt file.
- Step 4** If the CSA also sends back a Root Certificate File, save it in the root-cert.txt file.
- Step 5** Upload the signed-cert.txt and root-cert.txt files to Cisco SPA, and store them at /opt/SPA/signed-cert.txt.
- 

## Task 3: Importing the New Certificate and Root Certificate

- 
- Step 1** Log in to Cisco SPA as described in “Starting the Cisco SPA Operation and Configuration Tool” section on page 4-2.
- Step 2** Select the Configuration tab.
- Step 3** Click **Import Certificate**.  
Enter information in the Import Certificates dialog fields:

| Field                                                | Description                                                                                                                            |
|------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------|
| Certification Authorities (CA) Root Certificate File | <ol style="list-style-type: none"><li>1. Click <b>Browse</b>.</li><li>2. Navigate to the root-cert.txt file and select it.</li></ol>   |
| New Certificate Issued for this Server               | <ol style="list-style-type: none"><li>1. Click <b>Browse</b>.</li><li>2. Navigate to the signed-cert.txt file and select it.</li></ol> |

- Step 4** Click **OK**.
- Step 5** From the Status tab, click **Stop SPA**.
- Step 6** Click **Start SPA**.
- 

## Branding Tab

The Branding tab in the operation and configuration tool enables you to customize product properties and the text displayed on the Cisco SPA home page.

The default logo (that displays on the home page) is the Cisco logo stored in logo.gif. You can replace this with the logo of your choice.

| Field                    | Description                                                                                                                                                                                                                                                                                                       |
|--------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Customer Support Info    |                                                                                                                                                                                                                                                                                                                   |
| Application Name         | Enter the name of your application or product.                                                                                                                                                                                                                                                                    |
| Support Email Address    | Enter up to 64 characters.                                                                                                                                                                                                                                                                                        |
| Support Phone Number     | Enter a phone number.                                                                                                                                                                                                                                                                                             |
| Logo                     | <p>Enter the name and location of a file in the .gif format. (Example: /opt/SPA/config/logo.gif.)</p> <p>To browse to a file:</p> <ol style="list-style-type: none"> <li>1. Click <b>Select</b>.</li> <li>2. When you locate the file, click <b>Open</b> to select it, or <b>Cancel</b> to start over.</li> </ol> |
| Customize your Home Page | <p>In the customization box, enter the text in HTML format.</p> <p>Example:</p> <pre>&lt;div valign='middle'&gt;&lt;h1 align='center'&gt;Welcome to SPA&lt;/h1&gt;&lt;/div&gt;</pre>                                                                                                                              |
| Save Branding            | To save any changes made to this dialog box, click <b>Save Branding</b> .                                                                                                                                                                                                                                         |

## Validation Tab

The Validation tab in the operation and configuration tool enables you to specify the minimum number of alphanumeric characters for these user entries and the validation patterns used for each entry.



### Note

You cannot change the maximum length of validations.

| Field                  | Description                                                                                         |
|------------------------|-----------------------------------------------------------------------------------------------------|
| Validation Rules       |                                                                                                     |
| Account Minimum Value  | The maximum length is 20 characters; the default minimum length is 6.                               |
| Email Minimum Value    | The maximum length is 64 characters; the default minimum length is 7.                               |
| Password Minimum Value | The maximum length is 20 characters; the default minimum length is 6.                               |
| Phone Minimum Value    | The maximum length varies depending on your geographical location; the default minimum length is 7. |
| User Id Minimum Value  | The maximum length is 20 characters; the default minimum length is 3.                               |
| Pattern                | Shows how each value is validated.                                                                  |

| Field                     | Description                                                                                                    |
|---------------------------|----------------------------------------------------------------------------------------------------------------|
| Update Validation Rules   | Click this to save any changes to either the minimum values or validation patterns entered in this dialog box. |
| Reset to Default Patterns | Click this to reinstate the default validation patterns for all the values.                                    |

## About the Audit Tool

Cisco SPA contains a standalone (not web-based) application that compares the data in the Cisco SPA database with the data in the Cisco BTS EMS server database.

The audit results are displayed and stored in a timestamped log file called `audit.log.yyyy-mm-dd_hh:mm:ss` which is located at `/opt/SPA/data/logs`.

Where,

`yyyy-mm-dd` is the date (year, month, and day) when the audit was started.

`hh:mm:ss` is the time (hour, minute, and second) when the audit was started.

The audit tool stores seven days of audit results.



### Note

For Existing Cisco BTS 10200 Softswitch customers:

If you are an existing Cisco BTS 10200 Softswitch customer who has installed Cisco SPA for the first time, run the audit tool immediately after creating Cisco SPA accounts (see Figure 1-2, Workflow for Existing Cisco BTS 10200 Customers).

The audit tool retrieves the class of service and authorization code group information (from the Cisco BTS EMS server) for the phones in your accounts and stores this information in the Cisco SPA database.

If you attempt to assign class of services and authorization code groups from Cisco SPA, the assignments fail because the phones already have these assigned on the Cisco BTS EMS server. In this event, an error message appears.

## Running the Audit Tool

This procedure enables you to run an immediate audit on the Cisco SPA and Cisco BTS EMS server databases. You can also schedule audits to run at a future time (see the “Using the Audit Tab” section on page 4-5).

**Step 1** Log in to the server where Cisco SPA is installed:

Login: **spausr**

**Step 2** Enter a password:

Password: **xxxxxxxx**

**Step 3** Enter the following command:

**audit.sh-value**

Where,

*value* is one of the following:

- **h**—Help. Displays all the options that you can enter with this command.
- **1**—Checks if the phones on Cisco SPA exist in the Cisco BTS EMS server database. If a discrepancy is detected, the audit tool displays a message. For more information on messages, see the “About Cisco SPA Alarms” section on page 5-2.
- **2**—Checks if phones in Centrex and multiline hunt groups on the Cisco BTS EMS server also exist on Cisco SPA. If a discrepancy is detected, the audit tool displays a message. For more information on messages, see the “About Cisco SPA Alarms” section on page 5-2.



**Note** This check is for phones in groups only. If a certain number of phones exist in a group on the Cisco BTS EMS server, the audit tool checks that the same number of phones exist in the same group on Cisco SPA.

- **3**—Checks if each class of service in Cisco SPA exists on the Cisco BTS EMS server. If a discrepancy is detected, the audit tool displays a message, and the class of service is deleted from Cisco SPA. For more information on messages, see the “About Cisco SPA Alarms” section on page 5-2.
- **4**—Checks which phones are using which class of service on the Cisco BTS EMS server.
  - If a class of service is being used by phones assigned to more than one Cisco SPA account, the audit tool displays a message. A class of service ID is unique and can be used by only one account. For more information on messages, see the “About Cisco SPA Alarms” section on page 5-2.
  - If a class of service is being used by phones on the Cisco BTS EMS server and is not on Cisco SPA, the audit tool displays a message. For more information on messages, see the “About Cisco SPA Alarms” section on page 5-2.
  - If a class of service is not in the Cisco SPA database and there are no other errors, the audit tool displays a message and adds the class of service to the Cisco SPA database. For more information on messages, see the “About Cisco SPA Alarms” section on page 5-2.
- **5**—Checks if each authorization code group in the Cisco SPA database also exists on the Cisco BTS EMS server. If a discrepancy is detected, the audit tool displays a message and deletes the authorization code group from the Cisco SPA database.
- **6**—Checks which class of services is using which authorization code group on the Cisco BTS EMS server.
  - If an authorization code group on the Cisco BTS EMS server is being used by a class of services in more than one Cisco SPA account, the audit tool displays a message. An authorization code group ID is unique and can be used by only one account. For more information on messages, see the “About Cisco SPA Alarms” section on page 5-2.
  - If an authorization code group is not in the Cisco SPA database and there are no other errors, the authorization code group is added to the Cisco SPA database, and the audit tool displays a message. For more information on messages, see the “About Cisco SPA Alarms” section on page 5-2.
- **a**—Runs all the checks described in options 1 through 6.
- **b**—Runs the audit in batch mode and does not display results.



The audit results are displayed as well as written to the log file (see the “About the Audit Tool” section on page 4-15).

---

## About the Bulk Load Function

The bulk load function allows you to create, edit, and delete accounts in Cisco SPA without using the GUI. Because service providers have existing systems for tracking their customers, the data from these systems can be extracted and placed in an XML file that Cisco SPA processes.

The bulk load function checks the bulk load depot directory once a minute to determine if there are files to process. These checks start when Cisco SPA is started and stop when Cisco SPA is shut down.

If Cisco SPA is shut down while processing a file, the processing stops, and a results file indicates that the processing was interrupted. The status of the records processed up to that point will be in the results directory. You can resubmit the records that were not processed in the last attempt.

## Location of Bulk Load Directories

You can find the bulk load directories at the following locations:

/opt/SPA/bulk-load/depot

/opt/SPA/bulk-load/results



### Note

You can place multiple bulk load files in the depot directory, and as each file is processed successfully a response is sent to the results directory.

---

## Location of the Document Type Definition (DTD) File

The DTD describes the format of the XML file and is found at the following location:

/opt/SPA/bulk-load/spa-bulk-load.dtd

## Example of an XML Input File

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE spa-bulk-load SYSTEM "/vob/bts-spa/spa-bulk-load.dtd">
<spa-bulk-load>
 <records>
 <record id="1">
 <account verb="delete">
 <id>account-1</id>
 </account>
 </record>
 <record id="2">
 <account verb="add">
 <id>account-1</id>
 </account>
 </record>
 </records>
</spa-bulk-load>
```

```

<description>account 1</description>
<allow-auth-codes>true</allow-auth-codes>
<allow-cos>true</allow-cos>
<allow-groups>true</allow-groups>
<admin-id>account-1-adm</admin-id>
<admin-password>test123</admin-password>
<admin-email>account-1-adm@hd.com</admin-email>
<phones>
 <phone verb="add">
 <fdn>7035550001</fdn>
 </phone>
 <phone verb="add">
 <fdn>7035550002</fdn>
 </phone>
 <phone verb="add">
 <fdn>7035550003</fdn>
 </phone>
 <phone verb="add">
 <fdn>7035550004</fdn>
 </phone>
</phones>
</account>
</record>
<record id="3">
<account verb="edit">
 <id>account-1</id>
 <phones>
 <phone verb="add">
 <fdn>7035563784</fdn>
 </phone>
 </phones>
</account>
</record>
</records>
</spa-bulk-load>

```

## Example of an Output File

```

<?xml version="1.0" encoding="UTF-8"?>
<spa-bulk-load>
<results>
<result id="1" status="success"/>
<result id="2" status="success"/>

```

```
<result id="3" status="success"/>
</results>
<summary status="success">
<msgs>
<msg>File processed succesfully.</msg>
<msg>Processed 3 records. Success (3) Failed (0)</msg>
</msgs>
</summary>
</spa-bulk-load>
```





## Troubleshooting Cisco SPA

This chapter contains Cisco SPA-specific troubleshooting procedures. For information on troubleshooting the Cisco BTS 10200 Softswitch, refer to the *Cisco BTS 10200 Softswitch Operations Manual*.

This chapter contains the following topics:

- Troubleshooting Cisco SPA, page 5-1
- About Cisco SPA Alarms, page 5-2

### Troubleshooting Cisco SPA

Problem	Troubleshooting Action
Problems in launching Cisco SPA	<ul style="list-style-type: none"><li>• Check the information in the Cisco BTS EMS server definition to make sure that it is correct.</li><li>• Check connectivity between Cisco SPA and the Cisco BTS EMS: Log in to the Cisco SPA server and ping the Cisco BTS EMS server.</li><li>• Verify that the correct CORBA adapter has been installed on the Cisco BTS EMS server.</li></ul>
Problems in Cisco SPA communicating with the Cisco BTS EMS server.	<ul style="list-style-type: none"><li>• View log files: log files are stored in /opt/SPA/data/log. Use log files for debugging Cisco SPA problems or for supplying information to Cisco TAC.</li><li>• Check that the Cisco BTS EMS host name (as defined on the Cisco Cisco BTS EMS host) is also defined in the /etc/hosts file on the Cisco SPA server.</li></ul>
Excessive time for a Cisco SPA query.	<p>Cisco SPA queries the Cisco BTS EMS server in real time. Response time is directly related to responsiveness of the Cisco BTS EMS server.</p> <p>Check the log files stored in /opt/SPA/data/log.</p>

# About Cisco SPA Alarms

Cisco SPA alarms are converted into SNMP traps and are categorized by their severity level:

- INFO—information; service (call processing) is not affected
- MINOR—service (call processing) is not affected
- MAJOR—service is degraded
- CRITICAL—service is severely affected

The alarms in this section are organized alphabetically:

- Failed To Connect to BTS EMS, page 5-2
- Failed To Connect to Database, page 5-2
- Free Memory in Web Server Is Exhausted, page 5-3
- Free Memory in Web Server Is Running Low, page 5-3
- Number of SP Admin Sessions on System Exceeds Limit, page 5-4
- Number of User Sessions on System Exceeds Limit, page 5-4
- Phone Number in a Centrex Group in the BTS EMS Is not Found in SPA, page 5-4
- Phone Number in a Multiline Hunt Group in the BTS EMS Is Not Found in SPA, page 5-4
- Phone Number Not Found in the BTS EMS, page 5-5
- Security Violation, User Locked, page 5-5
- User Locked for Repeated Failed Login Attempts, page 5-5
- User Locked, page 5-5
- User Unlocked, page 5-6

## Failed To Connect to BTS EMS

### Description

Cisco SPA failed to connect to the Cisco BTS EMS server.

### Severity

CRITICAL

### Recovery

View the log files stored in `/opt/SPA/data/log`.

These log files are used to debug Cisco SPA problems or for supplying information to Cisco TAC.

## Failed To Connect to Database

### Description

Cisco SPA failed to connect to the MySQL database.

### Severity

CRITICAL

**Recovery**

- Stop and restart Cisco SPA:
  - Stop Cisco SPA operation (see the “Using the Status Tab” section on page 4-4).
  - Confirm that all the processes have stopped (see the “Using the Status Tab” section on page 4-4).
  - Start Cisco SPA (see the “Using the Status Tab” section on page 4-4).
- Reboot the server (performed by a root user):
  - Stop Cisco SPA operation (see the “Using the Status Tab” section on page 4-4).
  - Enter the command:  
**/usr/sbin/reboot**
  - Start Cisco SPA (see the “Using the Status Tab” section on page 4-4).

**Free Memory in Web Server Is Exhausted****Description**

Free memory left on the Cisco SPA server is less than 5% of capacity.

**Severity**

MAJOR

**Recovery**

- If there are many user sessions open on Cisco SPA, this condition is corrected when users log off.
- During a lull in operation, reboot the server (performed by a root user):
  - Stop Cisco SPA operation (see the “Using the Status Tab” section on page 4-4).
  - Enter the command:  
**/usr/sbin/reboot**
  - Start Cisco SPA (see the “Using the Status Tab” section on page 4-4).
- If the condition persists, contact Cisco TAC.

**Free Memory in Web Server Is Running Low****Description**

Free memory left on the Cisco SPA server is less than 20% of capacity.

**Severity**

MINOR

**Recovery**

- If there are many user sessions open on Cisco SPA, this condition is corrected when users log off.
- During a lull in operation, reboot the server (performed by a root user):
  - Stop Cisco SPA operation (see the “Using the Status Tab” section on page 4-4).
  - Enter the command:

**/usr/sbin/reboot**

- Start Cisco SPA (see the “Using the Status Tab” section on page 4-4).
- If the condition persists, contact Cisco TAC.

**Number of SP Admin Sessions on System Exceeds Limit****Description**

The number of active Cisco SPA service provider administrator sessions exceeds the limit of 100.

**Severity**

MINOR

**Recovery**

Log out of any Cisco SPA service provider administrator sessions that exceed 100.

**Number of User Sessions on System Exceeds Limit****Description**

The number of active Cisco SPA user sessions exceeds 1000. These consist of sessions opened by all Cisco SPA users below the level of service provider administrator.

**Severity**

MINOR

**Recovery**

Log out of any Cisco SPA user sessions that are in excess of 1000.

**Phone Number in a Centrex Group in the BTS EMS Is not Found in SPA****Description**

A phone number in a Centrex group on the Cisco BTS EMS server is not present in the Centrex group on Cisco SPA.

**Severity**

INFO

**Recovery**

Add the phone number to the account on Cisco SPA (see the Edit User window in Cisco SPA).

**Phone Number in a Multiline Hunt Group in the BTS EMS Is Not Found in SPA****Description**

A phone number in a multiline hunt group on the Cisco BTS EMS server is not present in the multiline hunt group on Cisco SPA.

**Severity**

INFO



**Recovery**

Add the phone number to the account on Cisco SPA (see the Edit User window in Cisco SPA).

**Phone Number Not Found in the BTS EMS****Description**

A phone number on Cisco SPA does not exist on the Cisco BTS EMS server.

**Severity**

INFO

**Recovery**

- Delete the phone number from the account on Cisco SPA.
- Create the phone number on the Cisco BTS EMS server (see the Edit User window in Cisco SPA).

**Security Violation, User Locked****Description**

A Cisco SPA user, who is already logged in, tried to access a restricted window or data.

**Severity**

INFO

**Recovery**

The service provider or account administrator unlocks the user (see the “Using the Configuration Tab” section on page 4-8).

**User Locked for Repeated Failed Login Attempts****Description**

The number of times that the user mistyped the user name or password exceeds the specified limit (see the “Using the Configuration Tab” section on page 4-8).

**Severity**

INFO

**Recovery**

The service provider or account administrator unlocks the user (see the “Using the Configuration Tab” section on page 4-8).

**User Locked****Description**

The service provider or account administrator locked the user account specified in the alarm.

**Severity**

INFO

**Recovery**

The service provider or account administrator unlocks the user (see the “Using the Configuration Tab” section on page 4-8).

**User Unlocked****Description**

The service provider or account administrator unlocked the user (see the “Using the Status Tab” section on page 4-4).

**Severity**

INFO

**Recovery**

None



---

## A

- accessing Cisco SPA operation and configuration tool 4-1
- account administrator 1-9
  - functions 1-9
- accounts 1-3
  - characteristics 1-3
- alarms 5-2
- audit tool 1-6, 4-15
  - running 4-15

---

## B

- bulk load directories
  - location 4-17
- bulk load interface function 4-17
  - DTD location 4-17
  - output file 4-18
  - XML input file 4-17

---

## C

- Certificate Signing Request file
  - downloading 4-12
  - generating 4-12
  - sending 4-13
- Cisco BTS 10200 Softswitch 1-3
  - communication with Cisco SPA 1-6, 4-1
- Cisco SPA
  - accounts 1-3
  - alarms 5-2
  - communication with Cisco BTS 10200 Softswitch 1-6
  - concept 1-3

- connections to the Cisco BTS EMS server 4-9
- downgrading 3-7
- installing 3-2
- logging in 4-2
- network architecture 1-6
- overview 1-1
- password to log in to Cisco BTS EMS server 4-9
- required and optional entities 1-7
- saved datasets 3-4
- security 1-11
- software applications 1-4
- uninstalling 3-3
- upgrading 3-5
- user levels 1-7
- users 1-4
- web server application 1-5
- workflow 1-1
- Cisco SPA database 1-6
- Cisco SPA installation
  - prerequisites 3-1
- Cisco SPA operation and configuration tool
  - features 4-2
  - GUI description 4-3
  - launching 4-2
- concept 1-3
- CORBA interface 1-6

---

## D

- documentation
  - conventions used ix
  - online help viii
  - purpose vii

related documents **viii**  
 scope **viii**  
 downgrading Cisco SPA **3-7**

---

## E

end user **1-10**  
 functions **1-10**

---

## F

failed passwords counter **4-10**

---

## G

Generate Certificate button **4-12**  
 group administrator **1-10**  
 functions **1-10**

---

## H

Help button **viii**

---

## L

length  
   account name **4-14**  
   email address **4-14**  
   password **4-14**  
   phone number **4-14**  
   user ID **4-14**  
 logger level  
   debug **4-10**  
   error **4-10**  
   fatal **4-10**  
   information **4-10**  
   warning **4-10**

---

## M

mail server  
   connection **4-1**

---

## O

online help **viii**  
 operation and configuration tool **1-4**  
 overview **1-1**

---

## P

Preface **vii**

---

## S

security **1-11**  
 security certificates **4-1**  
 service provider administrator **1-8**  
   functions **1-8**  
 Setting up SSL connections **4-12**  
 supported phone features **1-11**  
   call forwarding **1-12**  
   call management **1-12**  
   enterprise **1-12**  
   miscellaneous **1-12**  
   speed-dialing **1-13**

---

## U

upgrading Cisco SPA **3-5**  
 user levels **1-7**  
 users **1-4**  
   characteristics **1-4**

---

## W

### workflow

- for existing customer 1-1

- for new customer 1-1