



INTUITY™ AUDIX® LX

Release 1

Installation Checklist

585-313-158

Issue 2

June 2003

Notice

Every effort was made to ensure that the information in this book was complete and accurate at the time of printing. However, information is subject to change.

Avaya Web Page

The world wide web home page for Avaya is:
<http://www.avaya.com>

Preventing Toll Fraud

Toll Fraud is the unauthorized use of your telecommunications system by an unauthorized party (for example, a person who is not a corporate employee, agent, subcontractor, or working on your company's behalf). Be aware that there is a risk of toll fraud associated with your system and that, if toll fraud occurs, it can result in substantial additional charges for your telecommunications services.

Avaya Fraud Intervention

If you *suspect that you are being victimized* by toll fraud and you need technical assistance or support, call the Technical Service Center's Toll Fraud Intervention Hotline at 1.800.643.2353.

Providing Telecommunications Security

Telecommunications security of voice, data, and/or video communications is the prevention of any type of intrusion to, that is, either unauthorized or malicious access to or use of, your company's telecommunications equipment by some party.

Your company's "telecommunications equipment" includes both this Avaya product and any other voice/data/video equipment that could be accessed via this Avaya product (that is, "networked equipment").

An "outside party" is anyone who is not a corporate employee, agent, subcontractor, or working on your company's behalf. Whereas, a "malicious party" is Anyone, including someone who may be otherwise authorized, who accesses your telecommunications equipment with either malicious or mischievous intent.

Such intrusions may be either to/through synchronous (time-multiplexed and/or circuit-based) or asynchronous (character-, message-, or packet-based) equipment or interfaces for reasons of:

- Utilization (of capabilities special to the accessed equipment)
- Theft (such as, of intellectual property, financial assets, or toll-facility access)
- Eavesdropping (privacy invasions to humans)
- Mischief (troubling, but apparently innocuous, tampering)
- Harm (such as harmful tampering, data loss or alteration, regardless of motive or intent)

Be aware that there may be a risk of unauthorized intrusions associated with your system and/or its networked equipment. Also realize that, if such an intrusion should occur, it could result in a variety of losses to your company, including but not limited to, human/data privacy, intellectual property, material assets, financial resources, labor costs, and/or legal costs).

Your Responsibility for Your Company's Telecommunications Security

The final responsibility for securing both this system and its networked equipment rests with you – an Avaya customer's system administrator, your telecommunications peers, and your managers. Base the fulfillment of your responsibility on acquired knowledge and resources from a variety of sources including but not limited to:

- Installation documents
- System administration documents
- Security documents
- Hardware-/software-based security tools
- Shared information between you and your peers
- Telecommunications security experts

To prevent intrusions to your telecommunications equipment, you and your peers should carefully program and configure your:

- Avaya provided telecommunications systems and their interfaces
- Avaya provided software applications, as well as their underlying hardware/software platforms and interfaces
- Any other equipment networked to your Avaya products

Federal Communications Commission Statement

Part 15: Class A Statement. This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio-frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case the user will be required to correct the interference at his own expense.

Industry Canada (IC) Interference Information

This digital apparatus does not exceed the Class A limits for radio noise emissions set out in the radio interference regulations of Industry Canada.

Le Présent Appareil Numérique n'émet pas de bruits radioélectriques dépassant les limites applicables aux appareils numériques de la class A prescrites dans le règlement sur le brouillage radioélectrique édicté par le Industrie Canada.

Trademarks

All trademarks identified by ® and ™ are registered trademarks or trademarks of Avaya Inc. All other trademarks are the property of their respective owners.

Ordering Information

Call: Avaya Publications Center
Voice 1 800 457-1235 International Voice +1 207 866 6701
Fax 1 800 457-1764 International Fax +1 207 626 7269

Write: GlobalWare Solutions
200 Ward Hill Avenue
Haverhill, MA 01835 USA
Attn: Avaya Account Management

Email: totalware@gwsmail.com

Obtaining Products

To learn more about Avaya products and to order products, visit www.avaya.com.

European Union Declaration of Conformity

The "CE" mark affixed to the equipment means that it conforms to the referenced European Union (EU) Directives listed below:

EMC Directive 89/336/EEC

Low-Voltage Directive 73/23/EEC

For more information on standards compliance, contact your local distributor.

Warranty

Avaya Inc. provides a limited warranty on this product. Refer to your sales agreement to establish the terms of the limited warranty. In addition, Avaya's standard warranty language as well as information regarding support for this product, while under warranty, is available through the following web site:
<http://www.avaya.com/support>.



INTUITY AUDIX LX

Home Getting Started Administration Maintenance Reference

[Home](#) > [Getting Started](#) > [Installation](#) > System Installation Checklist



System Installation Checklist

This installation checklist provides descriptions of the required procedures, in sequence, to use when you install an assembled, loaded, and tested (ALT) Avaya INTUITY AUDIX LX system. For more information on installation or other procedures, you can use the:

- [Installation Printable Guide for the INTUITY AUDIX LX \(pdf\)](#) that includes all of the first-time installation processes in order.
- *INTUITY™ AUDIX® LX Release 1 Documentation* CD-ROM, 585-313-818, Issue 2.

Note: If you need to install a feature for the customer on an ALT system, contact your project manager to verify the requirements and contact your remote support center.

The following table provides a checklist for the system installation including integration with most switches.

Task	Description	Comments and Screens	✓
1.	Review Installation Planning and Prerequisites .	This section includes: • General precautions • FCC statement • DOC interference information • Site preparation ○ Environmental considerations ○ Installation area considerations ○ Weight and space considerations ○ Power requirements	
2.	Gather the required tools .		
3.	Verify that the switch has been administered in preparation for the new system.	See the switch administrator. Required switch administration is listed in Initial Switch Administration .	

Task	Description	Comments and Screens	✓
4.	Determine if you need to notify the LAN administrator to arrange for administration of the LAN for the system. Note: Avaya is not responsible for the installation, administration, or test of communications between customer PCs and the LAN.	See the LAN administrator. Note: Some LANs may be administered prior to your arrival on site. Other LANs require that the administration for a new machine be done at the time of installation because an open connection may cause the LAN to fail.	
5.	Review Demarcation Points .	All systems, application dependent.	
6.	Review Security issues.	All systems.	
7.	Unpack and check the shipment contents .	Open boxes as instructed to reuse packing materials .	
8.	Place the chassis in the designated operating area. Ensure sufficient airspace around it and turn the stabilizing feet out to the side.	Note: If stabilizing feet have not been installed, use a Phillips screwdriver to fasten the 4 stabilizing feet to the bottom of the chassis.	
9.	Connect Peripheral Devices .	This includes monitor, keyboard, and modem.	
10.	Connect the Analog-line Interface Cards (voice cards).		
11.	Connect the LAN cable.		
12.	Restore Power to the System .		
13.	Check Voice System, Modem, and Network Addressing .	• System Status • Install Modem/Terminal Software • Network Addressing	
14.	Load Language Packages .	This is optional, depending on customer preference.	
15.	Load Switch Integration Software .	NOTE: Before continuing, confirm that the switch integration you plan is generally available (GA). For more information about the GA integrations or to submit your integration for Controlled Introduction testing, see Switch Integration in the Concepts and Features section. • Install Software • Switch Selection	

Task	Description	Comments and Screens	✓
16.	Administer the Switch Integration.	If additional administration is needed, reference the applicable Switch Integration procedures.	
17.	Perform Initial System Administration.	Follow the Initial System Administration procedure for a complete listing of pages and screens to be completed.	
18.	Create remote administration logins.	Create the logins and passwords for use within or outside of an intranet firewall.	
19.	Activate Alarm Origination.	Note: Complete this step if your location is <i>outside</i> of the United States. Installations inside the United States are set up automatically for alarm origination by the Remote Service Center.	
20.	Perform System Acceptance Testing.		
21.	Perform a System Backup.		

[Top of page](#)[Search This CD](#) [Index](#) [Contact Us](#)

© 2003 Avaya Inc. All rights reserved.

