

LANDesk® Management Suite Training



Prerequisites: Course DM88: Desktop Management with LANDesk® Management Suite 8.8 or Equivalent Experience

Level: Intermediate to Advanced

Course Description:

Focuses on provisioning and protecting the LANDesk® enterprise. Attendees should be comfortable with advanced tasks relating to the administration of LANDesk® solutions 8.6.1 or higher. Course consists of lectures and hands-on exercises using operating system deployment (OSD), profile migration, provisioning, LANDesk® Security Suite, LANDesk® Host Intrusion Prevention System (HIPS), LANDesk® Management Gateway and LANDesk® Trusted Access™ technology.

Duration: 5 days (32.5 hours)

Hours: Monday–Thursday 9:00 a.m.–5:00 p.m.; Friday 9:00 a.m.–2:30 p.m.

MSRP: \$2,495.00

Registration Information: Register online at <http://landesk.verite.com/>. For questions, please contact Veronica Wilson in LANDesk® Professional Services at 801-208-1664.

Sample Schedule: PE88

Monday	Tuesday	Wednesday	Thursday	Friday
<ul style="list-style-type: none"> ■ Operating System Deployment 	<ul style="list-style-type: none"> ■ Profile Migration ■ Provisioning 	<ul style="list-style-type: none"> ■ Preparing the Environment ■ Security and Patch Manager ■ LANDesk® Process Manager 	<ul style="list-style-type: none"> ■ LANDesk® Antivirus ■ Alerting and Reporting ■ Using Connection Control Manager 	<ul style="list-style-type: none"> ■ LANDesk® Host Intrusion Prevention System

Course Agenda

Operating System Deployment (OSD)

- Imaging basics
- Choosing OSD options
- Using agent-based OS deployment
- Understanding OSD scripts
- Using LANDesk® PXE services
- Implementing OSD with PXE
- Comparing tools used in the different imaging environments
- Troubleshooting OSD

Profile Migration

- Using profile migration
- Windows Vista readiness
- Understanding how profile migration works

Provisioning

- Agent-based architecture
- Managing provisioning templates
- Deploying provisioning templates

LANDesk® Security Suite

- Preparing the environment
 - Using role-based administration
 - Creating agent configurations
- Security and Patch Manager
 - Security and Patch Manager process
 - Download definitions
 - Scan devices
 - Download files
 - Definition details
 - Creating custom definitions and detection rules
 - Detection rule properties
 - Using custom groups
 - Activating and changing firewall configuration
 - Additional features of Security and Patch Manager
 - Autofix
 - Custom columns
 - Inventory settings
 - Frequent security scan
 - Scripts as a scheduled task
 - Software distribution as a policy
- LANDesk® Process Manager
 - Components
 - Installation and configuration
 - Working with the Process Designer
 - Examining and automating the patch deployment workflow

- Configuring and automating the patch deployment workflow
- Troubleshooting LANDesk Process Manager
- LANDesk® Antivirus
 - Managing LANDesk Antivirus
 - Antivirus settings
 - Change settings task
 - Launch an antivirus scan
 - Antivirus activity
- Alerting and Reporting
 - Alert tool
 - Editing alert rulesets
 - Publishing alert rulesets
 - Alert monitoring rules
 - Editing alert rules
 - Distributing alert rulesets
 - Removing alert rulesets
 - Alerting inventory record
 - Types of reports
- Using Connection Control Manager
 - Connection Control configuration
 - Device control configuration
 - Deploying configurations

LANDesk® Host Intrusion Prevention System (HIPS)

- The gap before the patch
- Device exposure
- Fastest is not fast enough
- How real is zero day
- Solving the zero day threat
- How LANDesk HIPS works
- LANDesk HIPS concepts
- LANDesk HIPS components
- LANDesk HIPS features
- Additional layers of security
- LANDesk HIPS architecture
- Protection components
- Behavior settings files
- Management console functionality
- Role-based administration
- Create a task
- Configure settings
- New settings
- Recent LANDesk HIPS activity
- Installation through agent configuration
- Inventory scanner reporting LANDesk HIPS
- LANDesk HIPS client functionality
- Deploying LANDesk HIPS

Appendix A:

LANDesk® Management Gateway Appliance

- LAN/WAN communication
- Remote/branch office communication
- Gateway server
- Managed device to core server communication
- Core server to gateway communication
- Gateway server security
- Gateway server requirements
- Configuring LANDesk® Management Gateway

Appendix B:

LANDesk® Trusted Access™ Technology

- LANDesk® Trusted Access™ solutions
- Implementation methods
- Component interaction
- LANDesk® DHCP components and communication process
- Posture validation process for device with no LANDesk® trust agent
- Configuring LANDesk Trusted Access services
- Setting up and testing LANDesk Trusted Access policies
- Installing and configuring the LANDesk DHCP server
- Creating and managing scopes
- Configure quarantine options
- Configure remediation server settings
- LANDesk DHCP watcher
- Installing the LANDesk trust agent on managed devices

Appendix C:

LANDesk® Management Gateway

- LAN/WAN communication
- Remote/branch office communication
- Gateway server
- Managed device to core server communication
- Core server to gateway communication
- Gateway server security
- Gateway server requirements
- Installing LANDesk Management Gateway
- Configuring LANDesk Management Gateway

Visit www.landesk.com for more information.

This information is provided in connection with LANDesk® products. No license, express or implied, by estoppel or otherwise, or warranty is granted by this document. LANDesk does not warrant that this material is error free, and LANDesk reserves the right to update, correct or modify this material, including any specifications and product descriptions, at any time, without notice. For the most current product information, visit <http://www.landesk.com>.

Copyright © 2008 LANDesk Software Ltd. or its affiliated companies. All rights reserved. LANDesk is a registered trademark or trademark of LANDesk Software Ltd. or its affiliated companies in the United States and/or other countries. Avocent and the Avocent logo are trademarks or registered trademarks of Avocent Corporation or its subsidiaries. Other names or brands may be claimed as the property of others. Each customer's results may vary based on its unique set of facts and circumstances. Other names or brands may be claimed as the property of others.

0208/BB/NH