CONTENTS

About this Guide xix

Audience xix
Conventions xix
Related Documents xx
Obtaining Documentation and Submitting a Service Request xxi

CHAPTER 1 Introduction to the AnyConnect Secure Mobility Client 1-1

AnyConnect License Options 1-2
  Overview 1-2
  AnyConnect Essentials and Premium Licenses 1-3
  AnyConnect Mobile License 1-4
  AnyConnect Flex License 1-4
  Advanced Endpoint Assessment License 1-4
  Cisco Secure Mobility for AnyConnect License 1-5
  Combining AnyConnect Licenses 1-6
Standalone and WebLaunch Options 1-6
Configuration and Deployment Overview 1-7
AnyConnect Secure Mobility Feature Configuration Guidelines 1-7
API 1-8
AnyConnect Accessibility 1-8

CHAPTER 2 Deploying the AnyConnect Secure Mobility Client 2-1

Introduction to the AnyConnect Client Profiles 2-1
Creating and Editing an AnyConnect Client Profile Using the Integrated AnyConnect Profile Editor 2-2
Deploying AnyConnect Client Profiles 2-4
  Deploying AnyConnect Client Profiles from the ASA 2-4
  Deploying Client Profiles Created by the Standalone Profile Editor 2-5
Web Deploying AnyConnect 2-5
  AnyConnect File Packages for ASA Deployment 2-7
  Ensuring Successful AnyConnect Installation 2-7
    Setting Up the Endpoint to Accept Self-signed Certificates 2-7
    Exempting AnyConnect Traffic from Network Address Translation (NAT) 2-8
    Configuring the ASA for DES-Only SSL Encryption Not Recommended 2-13

        Connecting with Mobile Broadband Cards **2-13**
        Disabling Group Policy Settings **2-14**
    Modifying Installer Behavior When Web Deploying **2-14**

Configuring the ASA to Download AnyConnect **2-14**

Configure a Method of Address Assignment **2-15**

Prompting Remote Users to Download AnyConnect **2-15**

User Control Over Upgrade **2-16**
    Deferred Update Custom Attributes **2-16**
        Adding Attributes in ASDM **2-17**
        Deferred Update GUI **2-18**

Enabling Modules for Additional Features **2-18**

Enabling IPsec IKEv2 Connections **2-19**
    Predeploying an IKEv2-Enabled Client Profile **2-20**

Predeploying AnyConnect **2-21**
    Predeployment Package File Information **2-22**

Predeploying to Windows Computers **2-22**
    Using the ISO File **2-22**
    Guidelines and Limitations **2-23**
        Resetting the System MTU **2-23**
        Turning on ActiveX Control **2-23**
    Using the Install Utility for Predeployment **2-23**
    Using an SMS to Predeploy AnyConnect Modules **2-24**
        Installing AnyConnect Modules for Windows (Recommended Order) **2-26**
        Uninstalling AnyConnect Modules for Windows (Recommended Order) **2-26**
        Packaging the MSI Files for Enterprise Software Deployment Systems **2-27**
        Instructing Users to Install Network Access Manager and Web Security as Stand-Alone Applications **2-28**
    Modifying Installer Behavior During Pre-deploy **2-29**

Predeploying to Linux and Mac OS X Computers **2-29**
    Modifying Installer Behavior **2-29**
    Disabling Customer Experience Feedback Module **2-30**
    Installing Modules for Linux and Mac OS X (Recommended Order) **2-30**
    Uninstalling Modules for Linux and Mac OS X (Recommended Order) **2-30**
    Restricting Applications on System **2-31**
    Verifying Server Certificates with Firefox **2-31**

AnyConnect File Information **2-31**
    Filenames of Modules on the Endpoint Computer **2-31**
    Locations to Deploy the AnyConnect Profiles **2-33**
    User Preferences Files Installed on the Local Computer **2-35**

Using Standalone AnyConnect Profile Editor 2-35
  System Requirements for Standalone Profile Editor 2-36
    Supported Operating Systems 2-36
    Java Requirement 2-36
    Browser Requirement 2-36
    Required Hard Drive Space 2-36
  Installing the Standalone AnyConnect Profile Editor 2-36
  Modifying the Standalone AnyConnect Profile Editor Installation 2-37
  Uninstalling the Standalone AnyConnect Profile Editor 2-37
  Creating a Client Profile Using the Standalone Profile Editor 2-37
  Editing a Client Profile Using the Standalone Profile Editor 2-38

CHAPTER 3 **Configuring VPN Access** 3-1

Configuring IP Addresses for AnyConnect Clients 3-2
  IP Address Assignment Policies 3-2
    Configuring IPv4 and IPv6 Address Assignments using ASDM 3-3
  Internal IP Address Pools 3-3
    Configuring Local IPv4 Address Pools Using ASDM 3-4
    Configuring Local IPv6 Address Pools Using ASDM 3-4
  Assigning an IP Address to an AnyConnect Connection 3-5
    Assigning IP Addresses using Internal Address Pools 3-5
    Assigning IP addresses using DHCP 3-6
    Assigning IP Addresses to a Local User 3-6
  Configuring IPv4 or IPv6 Traffic to Bypass the VPN 3-8

Creating and Editing an AnyConnect Profile 3-9

Deploying the AnyConnect Profile 3-12

Configuring VPN Load Balancing 3-12

Configuring Start Before Logon 3-13
  Installing Start Before Logon Components (Windows Only) 3-14
    Start Before Logon Differences Between Windows Versions 3-14
    Enabling SBL in the AnyConnect Profile 3-14
    Enabling SBL on the Security Appliance 3-15
    Troubleshooting SBL 3-15
  Configuring Start Before Logon (PLAP) on Windows 7 and Vista Systems 3-16
    Installing PLAP 3-16
    Logging on to a Windows 7 or Windows Vista PC using PLAP 3-17
    Disconnecting from AnyConnect Using PLAP 3-21

Trusted Network Detection 3-21
  Trusted Network Detection Requirements 3-21

    Configuring Trusted Network Detection 3-21
    TND and Users with Multiple Profiles Connecting to Multiple Security Appliances 3-23
Always-on VPN 3-23
    Always-on VPN Requirements 3-24
    Adding Load-Balancing Backup Cluster Members to the Server List 3-26
    Configuring Always-on VPN 3-27
    Configuring a Policy to Exempt Users from Always-on VPN 3-27
    Disconnect Button for Always-on VPN 3-28
    Disconnect Button Requirements 3-29
    Enabling and Disabling the Disconnect Button 3-29
Connect Failure Policy for Always-on VPN 3-30
    Connect Failure Policy Requirements 3-31
    Configuring a Connect Failure Policy 3-31
Captive Portal Hotspot Detection and Remediation 3-32
    Captive Portal Remediation Requirements 3-32
    Captive Portal Hotspot Detection 3-32
    Captive Portal Hotspot Remediation 3-33
        Configuring Support for Captive Portal Hotspot Remediation 3-33
        If Users Cannot Access a Captive Portal Page 3-33
    False Captive Portal Detection 3-34
Client Firewall with Local Printer and Tethered Device Support 3-34
    Usage Notes about Firewall Behavior 3-35
    Deploying a Client Firewall for Local Printer Support 3-35
    Tethered Devices Support 3-37
New Installation Directory Structure for Mac OS X 3-37
ScanCenter Hosted Configuration Support for Web Security Client Profile 3-37
Configuring Split Tunneling 3-38
Configuring DNS and WINS Servers for AnyConnect 3-40
    Configuring a DNS Server for an Internal Group Policy 3-40
    Configuring WINS Servers for an Internal Group Policy 3-40
Split DNS Functionality Enhancement 3-41
    Using AnyConnect Logs to Verify 3-42
    Checking Which Domains Use Split DNS 3-42
    Configuring Split DNS 3-42
Network Roaming 3-43
    Prerequisite 3-43
    Configuring Network Roaming Between IPv4 and IPv6 Networks 3-43
Configuring Certificate Enrollment using SCEP 3-44

    Information about Certificate Enrollment using SCEP **3-44**
        Supported Enrollment Methods **3-44**
        SCEP Enrollment Steps **3-45**
        Automatic Certificate Requests **3-45**
        Manual Certificate Requests **3-46**
        CA Password **3-46**
        Windows Certificate Warning **3-47**
    Guidelines and Limitations for Certificate Enrollment using SCEP **3-47**
    Prerequisites for Certificate Enrollment using SCEP **3-47**
        Using a Windows 2008 Server Certificate Authority for SCEP **3-47**
    Configuring Certificate Enrollment using SCEP **3-49**
        Configuring a VPN Client Profile for SCEP Enrollment **3-49**
        Configuring the ASA to support SCEP Proxy **3-50**
        Configuring the ASA to support SCEP Legacy **3-50**
        Configuring Certificate-Only Authentication on the ASA **3-51**
        DAP Records for SCEP **3-51**

Configuring Certificate Expiration Notice **3-51**

Configuring a Certificate Store **3-51**
    Controlling the Certificate Store on Windows **3-52**
    Creating a PEM Certificate Store for Mac and Linux **3-54**
        Restrictions for PEM File Filenames **3-54**
        Storing User Certificates **3-55**

Configuring Certificate Matching **3-55**
    Certificate Key Usage Matching **3-55**
    Extended Certificate Key Usage Matching **3-56**
    Custom Extended Match Key **3-56**
    Certificate Distinguished Name Mapping **3-56**
    Default Certificate Matching **3-58**
    Certificate Matching Example **3-58**

Prompting Users to Select Authentication Certificate **3-59**
    Users Configuring Automatic Certificate Selection in AnyConnect Preferences **3-59**

Configuring a Server List **3-60**
    Configuring Connections for Mobile Devices **3-63**

Configuring a Backup Server List **3-64**

Configuring Connect On Start-up **3-64**

Configuring Auto Reconnect **3-65**

Local Proxy Connections **3-66**
    Local Proxy Connections Requirements **3-66**
    Configuring Local Proxy Connections **3-66**

Optimal Gateway Selection 3-66
  Optimal Gateway Selection Requirements 3-67
  Configuring Optimal Gateway Selection 3-67
    OGS and Sleep Mode 3-68
    OGS and Proxy Detection 3-69
Writing and Deploying Scripts 3-69
  Scripting Requirements and Limitations 3-69
  Writing, Testing, and Deploying Scripts 3-71
  Configuring the AnyConnect Profile for Scripting 3-72
  Troubleshooting Scripts 3-72
Authentication Timeout Control 3-73
  Authentication Timeout Control Requirements 3-73
  Configuring Authentication Timeout 3-73
Proxy Support 3-73
  Configuring the Client to Ignore Browser Proxy Settings 3-74
  Private Proxy 3-74
    Private Proxy Requirements 3-74
    Configuring a Group Policy to Download a Private Proxy 3-74
  Internet Explorer Connections Tab Lockdown 3-75
  Proxy Auto-Configuration File Generation for Clientless Support 3-75
Using a Windows RDP Session to Launch a VPN Session 3-76
AnyConnect over L2TP or PPTP 3-77
  Configuring AnyConnect over L2TP or PPTP 3-77
  Instructing Users to Override PPP Exclusion 3-78
AnyConnect VPN Profile Editor Parameter Descriptions 3-79
  AnyConnect Profile Editor, Preferences (Part 1) 3-79
  AnyConnect Profile Editor, Preferences (Part 2) 3-81
  AnyConnect Profile Editor, Backup Servers 3-85
  AnyConnect Profile Editor, Certificate Matching 3-85
  AnyConnect Profile Editor, Certificate Enrollment 3-87
  AnyConnect Profile Editor, Mobile Policy 3-88
  AnyConnect Profile Editor, Server List 3-89
    AnyConnect Profile Editor, Add/Edit Server List 3-89

CHAPTER 4 **Configuring Network Access Manager** 4-1
Introduction 4-1
  Suite B and FIPS 4-2
  Single Sign On “Single User” Enforcement 4-2
    Configuring Single Sign-On Single User Enforcement 4-3

System Requirements for the Network Access Manager 4-3
    Licensing and Upgrading Requirements 4-4
Deploying Network Access Manager 4-4
Creating a Network Access Manager Profile 4-4
    Adding a New Profile from ASDM 4-4
Configuring a Network Access Manager Profile 4-5
    Client Policy Window 4-5
    Authentication Policy Window 4-8
    Networks Window 4-10
    Networks - Media Type Page 4-11
        Network Connection Notes 4-13
    Networks - Security Level Page 4-13
        Configuring Authenticating Network 4-14
        Configuring Open Network 4-16
        Configuring Shared Key Network 4-16
    Networks - Network Connection Type Pane 4-18
    Networks - User or Machine Authentication Page 4-19
        EAP Overview 4-21
        Configuring EAP-GTC 4-21
        Configuring EAP-TLS 4-22
        Configuring EAP-TTLS 4-22
        Configuring PEAP Options 4-24
        Configuring EAP-FAST Settings 4-25
        Configuring LEAP Settings 4-27
        Defining Networks Credentials 4-27
        Configuring Trusted Server Validation Rules 4-32
    Network Groups Window 4-33

CHAPTER 5 **Configuring Host Scan** 5-1
Host Scan Workflow 5-2
Features Enabled with the AnyConnect Posture Module 5-3
    Assessment 5-3
    Policies 5-4
    Keystroke Logger Detection 5-5
    Host Emulation Detection 5-6
        Keystroke Logger Detection and Host Emulation Detection Supported Operating Systems 5-6
    Cache Cleaner 5-6
    Host Scan 5-7
        Basic Host Scan Functionality 5-7

        Endpoint Assessment 5-8
        Advanced Endpoint Assessment - Antivirus, Antispyware, and Firewall Remediation 5-8
        Host Scan Support Charts 5-9
    Configuring Antivirus Applications for Host Scan 5-9
    Integration with Dynamic Access Policies 5-9
Difference Between the Posture Module and the Standalone Host Scan Package 5-10
AnyConnect Posture Module Dependencies and System Requirements 5-10
    Dependencies 5-10
    Host Scan, CSD, and AnyConnect Secure Mobility Client Interoperability 5-10
    System Requirements 5-11
    Licensing 5-11
    Entering an Activation Key to Support Advanced Endpoint Assessment 5-11
Host Scan Packaging 5-12
    Which Host Scan Image Gets Enabled When There is More than One Loaded on the ASA? 5-12
Deploying the AnyConnect Posture Module and Host Scan 5-13
    Pre-Deploying the AnyConnect Posture Module 5-13
Installing and Enabling Host Scan on the ASA 5-14
    Downloading the Latest Host Scan Engine Update 5-14
    Installing or Upgrading Host Scan 5-14
    Enabling or Disabling Host Scan on the ASA 5-16
    Enabling or Disabling CSD on the ASA 5-16
Host Scan and CSD Upgrades and Downgrades 5-17
Determining the Host Scan Image Enabled on the ASA 5-17
Uninstalling Host Scan 5-17
    Uninstalling the Host Scan Package 5-17
    Uninstalling CSD from the ASA 5-17
    Assigning AnyConnect Posture Module to a Group Policy 5-18
Host Scan Logging 5-18
Configuring the Logging Level for All Posture Module Components 5-19
    Posture Module Log Files and Locations 5-19
Using a BIOS Serial Number in a DAP 5-20
    Specifying the BIOS as a DAP Endpoint Attribute 5-20
    How to Obtain BIOS Serial Numbers 5-21

CHAPTER 6 **Configuring Web Security** 6-1
System Requirements 6-2
    AnyConnect Web Security Module 6-2
    ASA and ASDM Requirements 6-2

    System Limitations 6-2
  Licensing Requirements 6-3
    Web Security Deployed as a Standalone Component 6-3
    Web Security Deployed as a Component of AnyConnect 6-3
  User Guideline for Web Security Behavior with IPv6 Web Traffic 6-3
  Installing the AnyConnect Web Security Module for Use with an ASA 6-3
  Installing the AnyConnect Web Security Module for Use without an ASA 6-4
    Installing the Web Security Module on Windows Using the AnyConnect Installer 6-4
    Installing the Web Security Module on Mac OS X Using the AnyConnect Installer 6-5
    Installing the Web Security Module on Windows Using the Command Line Installation 6-7
  Creating an AnyConnect Web Security Client Profile 6-7
    Configuring Cisco Cloud Web Security Scanning Proxies in the Client Profile 6-8
      Updating the Scanning Proxy List 6-9
      Default Scanning Proxy Settings in a Web Security Client Profile 6-10
      Displaying or Hiding Scanning Proxies from Users 6-10
      Selecting a Default Scanning Proxy 6-11
      How Users Get Connected to Scanning Proxies 6-11
      Specifying an HTTP(S) Traffic Listening Port 6-12
    Excluding Endpoint Traffic from Web Scanning Service 6-12
      Host Exceptions 6-13
      Proxy Exceptions 6-14
      Static Exceptions 6-14
    Configuring Web Scanning Service Preferences 6-15
      Configuring User Controls and Calculating Fastest Scanning Proxy Response Time 6-15
      Configuring Secure Trusted Network Detection 6-16
    Configuring Authentication and Sending Group Memberships to the Cisco Cloud Web Security Proxy 6-17
    Configuring Advanced Web Security Settings 6-20
      Configuring KDF Listening Port 6-20
      Configuring Service Communication Port 6-21
      Configuring Connection Timeout 6-21
      Configuring DNS Cache Failure Lookup 6-22
      Configuring Debug Settings 6-22
      Configuring Fail Behavior 6-22
      Web Security Logging 6-22
    Web Security Client Profile Files 6-22
      Exporting the Plain Text Web Security Client Profile File 6-23
      Exporting the Plain Text Web Security Client Profile File for DART Bundle 6-23
      Editing and Importing Plain Text Web Security Client Profile Files from ASDM 6-23

Exporting the Obfuscated Web Security Client Profile File 6-24
Creating a Web Security Client Profile with the Standalone Editor 6-24
Configuring Split Exclusion Policy for Web Security 6-24
Configuring Cisco ScanCenter Hosted Configuration Support for Web Security Client Profile 6-25
Secure Trusted Network Detection 6-26
Switching off and Enabling the Cisco AnyConnect Web Security Agent 6-27
Switching Off and Enabling Filters using Windows 6-27
Switching Filters On and Off Using Mac OS X 6-27

CHAPTER 7 Configuring AnyConnect Telemetry to the WSA 7-1
System Requirements 7-1
ASA and ASDM Requirements 7-2
AnyConnect Secure Mobility Client Module Requirements 7-2
Requirements for Cisco IronPort Web Security Appliance Interoperability 7-2
Enable SenderBase on Cisco IronPort Web Security Appliance 7-2
Installing the AnyConnect Telemetry Module 7-3
Quick-Deploy of the AnyConnect Telemetry Module 7-3
AnyConnect Telemetry Module Interoperability 7-5
AnyConnect VPN Module 7-5
AnyConnect Posture Module 7-5
Third-Party Antivirus Software 7-5
Telemetry Activity History Repository 7-6
Telemetry Reports 7-7
Possible Transference of Personal Information by Telemetry Module 7-7
Telemetry Workflow 7-8
URL Encryption 7-8
Telemetry Report Encryption 7-9
Configuring the Telemetry Client Profile 7-9
Configuration Profile Hierarchy 7-11

CHAPTER 8 Using Cisco AnyConnect Customer Experience Feedback Module 8-1
Configuring Customer Experience Feedback Module 8-2
Disabling During Installation 8-2

CHAPTER 9 NGE, FIPS and Additional Security 9-1
Information About NGE and AnyConnect 9-1
Requirements 9-2
Guidelines and Limitations 9-3

    About AnyConnect Modules with NGE **9-4**

  Enabling FIPS for the AnyConnect Core VPN Client **9-4**
    Enabling FIPS for Windows Clients Using an MST File **9-5**
    Enabling FIPS and other Local Policy Parameters in an MST File **9-5**
    Enabling FIPS and Other Parameters with the Enable FIPS Tool **9-5**
    Changing Local Policy Parameters Manually in the Local Policy **9-6**
    Avoiding Endpoint Problems from AnyConnect FIPS Registry Changes **9-7**

  Enabling Software and Profile Locks **9-8**
    XML Tags for the Software and Profile Locks **9-10**
    Software Lock Use Cases **9-11**
    Software and Profile Lock Example **9-12**

  AnyConnect Local Policy Parameters and Values **9-13**
      Local Policy File Example **9-16**

  Enabling FIPS for the Network Access Manager **9-16**
    Enforcing FIPS Mode in the Network Access Manager **9-16**
    Installing the 3eTI Driver **9-17**
      Important Notes **9-17**
      3eTI CKL Driver Installer Overview **9-17**
      Running the Installer without Using Command-Line Options **9-19**
      Uninstalling Previous 3eTI Driver Software **9-22**
      Silent Driver Installation for Enterprise Deployment **9-23**
      Installing the Driver without a Previously Installed Network Adapter **9-23**
      Manually Upgrading the 3eTI Driver Software **9-24**
    Obtaining the 3eTI Driver Installer Software **9-29**

CHAPTER 10 **Interoperability Guidelines and Requirements** **10-1**

  Using Quarantine to Restrict Non-Compliant Clients **10-1**
    Quarantine Requirements **10-1**
    Configuring Quarantine **10-2**

  Using Microsoft Active Directory to Add the Security Appliance to the List of Internet Explorer Trusted Sites for Domain Users **10-2**

  Configuring CSA Interoperability with AnyConnect and Cisco Secure Desktop **10-3**

  Port Information for AnyConnect and the Legacy VPN Client **10-4**

  Differences in Client Split Tunneling Behavior for Traffic within the Subnet **10-4**

CHAPTER 11 **Managing VPN Authentication** **11-1**

  Configuring Certificate-only Authentication **11-1**

  AnyConnect Smart Card Support **11-2**

Avoiding SHA 2 Certificate Validation Failure **11-2**

SDI Token (SoftID) Integration **11-4**

Comparing Native SDI with RADIUS SDI **11-4**

Using SDI Authentication **11-5**
- Categories of SDI Authentication Exchanges **11-7**
  - Normal SDI Authentication Login **11-7**
- New User, Clear PIN, and New PIN Modes **11-7**
  - Getting a New PIN **11-8**
- "Next Passcode" and "Next Token Code" Challenges **11-9**

Ensuring RADIUS/SDI Proxy Compatibility with AnyConnect **11-9**
- AnyConnect and RADIUS/SDI Server Interaction **11-10**
- Configuring the Security Appliance to Support RADIUS/SDI Messages **11-10**

CHAPTER 12 **Customizing and Localizing the AnyConnect Client and Installer** **12-1**

Customizing AnyConnect **12-1**
- What Can Be Customized? **12-2**
  - Installer **12-2**
  - AnyConnect UI **12-2**
- Replacing Individual GUI Components with your Custom Components **12-2**
- Customizing the GUI with a Transform **12-4**
  - Sample Transform **12-6**
- Deploying Executables That Use the Client API **12-6**
- Information for Creating your Custom Icons and Logos **12-7**
  - Recommended Image Format for AnyConnect 3.0 and Later **12-7**
  - For Windows **12-7**
  - For Linux **12-12**
  - For Mac OS X **12-13**

Creating and Uploading an AnyConnect Client Help File **12-14**

Changing the Default AnyConnect English Messages **12-15**

Localizing the AnyConnect Client GUI and Installer **12-18**
- Localizing the AnyConnect GUI **12-18**
  - Specifying the AnyConnect Client Platform's System Locale **12-19**
  - Importing Available Translation Tables to the ASA **12-21**
  - Translating using the ASDM Translation Table Editor **12-21**
  - Translating by Exporting the Translation Table for Editing **12-26**
- Localizing the AnyConnect Installer Screens **12-29**
- Using Tools to Create Message Catalogs for Enterprise Deployment **12-31**
  - AnyConnect Message Template Directories **12-31**
  - Creating Message Catalogs **12-32**

Merging a Newer Translation Template with your Translation Table 12-32

CHAPTER 13 **Managing, Monitoring, and Troubleshooting AnyConnect Sessions** 13-1

Disconnecting All VPN Sessions 13-1

Disconnecting Individual VPN Sessions 13-2

Viewing Detailed Statistical Information 13-2

Resolving VPN Connection Issues 13-2

- Adjusting the MTU Size 13-3
    - Optimal MTU (OMTU) 13-3

Using DART to Gather Troubleshooting Information 13-4

- Getting the DART Software 13-4
- Installing DART 13-5
    - Installing DART with AnyConnect 13-5
    - Manually Installing DART on a Windows Device 13-6
- Manually Installing DART on a Linux Device 13-6
    - Manually Installing DART on a Mac OS X Device 13-7
- Running DART on Windows 13-7
- Running DART on Linux or Mac OS X 13-8

Installing the AnyConnect Client 13-10

Installing the Log Files 13-10

- Web Install of Log Files 13-10
- Standalone Install of Log Files 13-11

Problems Disconnecting AnyConnect or Establishing Initial Connection 13-11

Problems Passing Traffic 13-13

Problems with AnyConnect Crashing 13-14

Problems Connecting to the VPN Service 13-14

Obtaining the Computer System Information 13-15

- Obtaining a Systeminfo File Dump 13-15
- Checking the Registry File 13-15

Conflicts with Third-Party Applications 13-16

- Adobe and Apple—Bonjour Printing Service 13-16
- AT&T Communications Manager Versions 6.2 and 6.7 13-16
- AT&T Global Dialer 13-17
- Citrix Advanced Gateway Client Version 2.2.1 13-17
- Firewall Conflicts 13-17
- Juniper Odyssey Client 13-17
- Kaspersky AV Workstation 6.x 13-18
- McAfee Firewall 5 13-18

Microsoft Internet Explorer 8 **13-18**
Microsoft Routing and Remote Access Server **13-18**
Microsoft Windows Updates **13-19**
Microsoft Windows XP Service Pack 3 **13-19**
OpenVPN Client **13-20**
Load Balancers **13-20**
Wave EMBASSY Trust Suite **13-20**
Layered Service Provider (LSP) Modules and NOD32 AV **13-20**
LSP Symptom 2 Conflict **13-21**
LSP Slow Data Throughput Symptom 3 Conflict **13-21**
EVDO Wireless Cards and Venturi Driver **13-21**
DSL Routers Fail to Negotiate **13-21**
CheckPoint (and other Third-Party Software such as Kaspersky) **13-22**
Performance Issues with Virtual Machine Network Service Drivers **13-22**

APPENDIX A **VPN XML Reference** **A-1**
Local Proxy Connections **A-2**
Optimal Gateway Selection (OGS) **A-2**
Trusted Network Detection **A-3**
Always-on VPN and Subordinate Features **A-4**
Always-on VPN With Load Balancing **A-6**
Start Before Logon **A-7**
Certificate Store on Windows **A-7**
Restricting Certificate Store Use **A-8**
SCEP Protocol to Provision and Renew Certificates **A-8**
Certificate Matching **A-10**
Automatic Certificate Selection **A-15**
Backup Server List Parameters **A-15**
Windows Mobile Policy **A-15**
Auto Connect On Start **A-17**
Auto Reconnect **A-17**
Server List **A-18**
Scripting **A-19**
Authentication Timeout Control **A-20**
Ignore Proxy **A-21**
Allow AnyConnect Session from an RDP Session for Windows Users **A-21**
AnyConnect over L2TP or PPTP **A-22**

Other AnyConnect Profile Settings A-23

APPENDIX B

Telemetry XML Reference B-1