

CONTENTS

Preface xi

Cisco Trust Agent 2.1 Release xi Qualified Deployments of CTA 2.1 xii Product Versioning xii Audience xii Conventions xiii Related Documentation xiv Obtaining Documentation xiv Cisco.com xiv Product Documentation DVD xv Ordering Documentation xv Documentation Feedback xv Cisco Product Security Overview xvi Reporting Security Problems in Cisco Products xvi Product Alerts and Field Notices xvii Obtaining Technical Assistance xviii Cisco Support Website xviii Submitting a Service Request xix Definitions of Service Request Severity xx Obtaining Additional Publications and Information xx

CHAPTER 1

Cisco Trust Agent Overview 1-1

Cisco NAC Overview 1-1

	Posture Validation Process Overview 1-2
	Initial Posture Validation Process 1-2
	Posture Revalidation Process 1-4
	Cisco Trust Agent Deployment Considerations 1-5
CHAPTER 2	Installing the Cisco Trust Agent on Linux Operating Systems 2-1
	Verifying System Requirements on Linux 2-2
	Installation Files 2-3
	Initial Deployments 2-3
	CTA Scripting Interface Feature 2-3
	Installing Cisco Trust Agent 2-4
	General Installation Instructions 2-4
	Extracting the Installation File and Accepting the EULA 2-4
	Installing CTA from the Command Line 2-5
	Creating a Custom CTA Installation Package 2-5
	Upgrading to Cisco Trust Agent, Release 2.1 2-7
	Verifying Cisco Trust Agent Installation on Linux 2-8
	Verifying CTA is Running 2-8
	Verifying CTA Package Information 2-9
	Uninstalling Cisco Trust Agent on Linux 2-9
CHAPTER 3	Installing the Cisco Trust Agent on Macintosh Operating Systems 3-1
	System Requirements for Mac OS X 3-2
	CTA Scripting Interface Feature 3-3
	Installation Files 3-3
	Installing Cisco Trust Agent 3-3
	General Installation Instructions 3-3
	Extracting the Installation Image and Accepting the EULA 3-4

	Installing CTA from the Command Line 3-4
	Installing CTA Using an Installation Wizard 3-6
	Installing CTA Using a Custom Installation Package 3-12
	Repairing or Upgrading an Existing CTA Installation 3-14
	Verifying Cisco Trust Agent Installation 3-16
	Uninstalling Cisco Trust Agent 3-16
	Uninstalling CTA and the CTA Scripting Interface 3-16
	Uninstalling Only the CTA Scripting Interface 3-17
CHAPTER 4	Installing the Cisco Trust Agent on Windows Operating Systems 4-1
	System Requirements for Installation 4-2
	Optional Features You Can Install with CTA 4-4
	CTA 802.1x Wired Client 4-4
	CTA Scripting Interface 4-4
	Installation Files 4-5
	Installing Cisco Trust Agent 4-5
	General Installation Instructions 4-6
	Installing CTA Using MSI Commands 4-7
	Installing CTA Using an Installation Wizard 4-13
	Installing CTA Using a Custom Installation Package 4-22
	Upgrading to Cisco Trust Agent, Release 2.1 4-27
	Upgrading from Cisco Trust Agent, Release 1.0 4-27
	Upgrading from Cisco Trust Agent, Release 2.0.0.30 4-28
	Upgrading from Cisco Trust Agent, Release 2.0.1 4-29
	Upgrading from CTA 2.1 Selective Availability and Beta Releases to CTA 2.1.103.0 4-29
	Verifying the Cisco Trust Agent Installation 4-30
	Uninstalling Cisco Trust Agent on Windows 4-31

L

CHAPTER 5	Configuring Cisco Trust Agent 5-1
	The ctad.ini Configuration File 5-2
	Editing the ctad.ini Configuration File 5-3 ctad.ini Configuration Parameters 5-4 Configuring EAP over UDP Communication 5-12 Configuring Posture Plugins 5-13 Configuring CTA and Posture Plugin Interaction 5-13 Configuring the Default Posture Plug-in Message Size 5-16 Configuring an Application-Specific Posture Plug-in Message Size 5-17 Configuring PPMsgSize for Host Posture Plugin 5-18
	Configuring PPMsgSize for Symantec Posture Plugin 5-19
	Configuring Asynchronous Posture Status Query 5-19 Configuring User Notifications 5-20 Configuring Windows User Notifications 5-20
	Configuring Mac OS X User Notifications 5-22
	Logging Notifications 5-24
	Certificate Distinguished Name Matching 5-25
	DN Matching Rule Syntax 5-25
	Configuring Certificate DN Matching 5-27
	Configuring the Scripting Interface 5-27
	Sample Windows ctad.ini File 5-28
	Sample Linux ctad.ini File 5-32
	Sample Mac OS X ctad.ini File 5-37
CHAPTER 6	Cisco Trust Agent Event Logging 6-1
	How Logging Works 6-2

Administrator Guide for Cisco Trust Agent, Release 2.1

CTA Log Files 6-2

	Log File Format 6-3
	Logging Considerations 6-4
	The clogcli Logging Utility 6-4
	Logging Levels 6-11
	Configuring CTA Logging For Large Deployments 6-11
	Sample ctalogd-temp.ini File 6-13
CHAPTER 7	Posture Plugins 7-1
	Types of Posture Plugins Installed by Default 7-2
	Host Posture Plugin 7-2
	Package Information Retrieved by Host Posture Plugin for Mac OS X Platforms 7-5
	Cisco Trust Agent Posture Plugin 7-5
	CTA Scripting Posture Plugin 7-9
	Plugin Installation and Upgrade 7-9
CHAPTER 8	Cisco Trust Agent's Use of Certificates 8-1
	About The ACS Server Root Certificate 8-3
	About The ctacert Utility 8-3
	Installing or Updating Certificates Using the ctacert Utility 8-4 Installing or Updating a Certificate on Linux Operating Systems 8-4 Installing or Updating a Certificate on Mac OS X Operating System 8-4 Installing or Updating a Certificate on Windows Operating Systems 8-5
	Listing Certificates in the Certificate Store 8-6
	Listing Certificates in the Certificate Store on Linux Operating Systems 8-6 Listing Certificates in the Certificate Store on Mac OS X Operating System 8-7
	Deleting Certificates from the Certificate Store 8-8

L

	Deleting a Certificate from the Certificate Store on Linux Operating Systems 8-8
	Deleting a Certificate from the Certificate Store on Mac OS X Operating System 8-9
	Clearing Certificates from the Certificate Store 8-9
	Clearing All Certificates from the Certificate Store on Linux Operating Systems 8-9
	Clearing All Certificates from the Certificate Store on Mac OS X Operating Systems 8-10
	Configuring Machine Authentication Using Certificates 8-10
	Requesting the Machine Certificate for Machine Authentication 8-11
	Configuring User Authentication Using Certificates 8-12
	Importing the User Certificate for User Authentication 8-12
	Configuring Machine and User Authentication Using Certificates 8-13
	Distinguished Name Matching 8-14
	Converting DER Formatted Certificates to PEM Formatted Certificates 8-14
CHAPTER 9	Cisco Trust Agent 802.1x Wired Client 9-1
	802.1x Wired Client Features 9-3
	802.1x Wired Client Administrative and Client Versions 9-4
	802.1x Wired Client User Interface 9-4
	Administrative 802.1x Wired Client Automatic Startup 9-4
	Network Connection Status 9-5
	Disabling the 802.1x Wired Client System Tray Icon 9-6
	802.1x Wired Client System Tray Shortcut Menu 9-7
	802.1x Wired Client Window 9-7
	Network Connection Status 9-8
	Access Device Connection Status 9-9
	Basic 802.1x Wired Client Procedures 9-11
	Opening the 802.1x Wired Client 9-11

Manually Connecting To the Network 9-12 Manually Disconnecting From the Network 9-12 Viewing Network Summary 9-12 Viewing Access Device Status 9-13 Getting Started with 802.1x Wired Client Functions 9-16 Administrative 802.1x Wired Client Overview 9-16 Authentication Methods Overview 9-16 Overview of FAST Connections in a User Logon Context 9-17 Overview of FAST Connections in a Machine Credentials Context 9-18 User Credentials 9-20 Initial Credential Provisioning 9-20 Machine Credentials 9-21 Pre-PAC or no-PAC Provisioning 9-22 Post-PAC Provisioning 9-22 Credential Revalidation 9-23 Server-Initiated Credential Revalidation 9-23 User-Initiated Credential Revalidation 9-23 Understanding Policies and Profiles 9-24 802.1x Wired Client Policy File 9-24 802.1x Wired Client Network Policy File 9-25 Create Deployment Package Wizard 9-26 User Credentials Area 9-27 Automatically Establishing Machine Connection 9-27 Allow Unprotected Client Cert Area 9-28 Trusted Server Validation Area 9-29 User Identity Protection Area 9-32 Authentication Retries Wired / Ethernet Settings 9-34 Deploying End-User 802.1x Wired Clients 9-35 Creating Deployment Packages 9-36

	Installing Server Certificates on the Host 9-42 Installing Deployment Packages on Hosts 9-43 Changing Deployment Packages on Hosts 9-44 Replacing a Deployment Package on a Host 9-44
CHAPTER 10	Cisco Trust Agent 802.1x Wired Client Logging 10-1
	Technical Log 10-2
	Understanding the Technical Log Status and Error Messages 10-3 Technical Log Message Format 10-3 Technical Log Message Content 10-5 Additional Message <value> Descriptions 10-11 Port Status Values 10-12</value>
	System Report 10-15
	Creating a System Report 10-16
CHAPTER 11	Using the Scripting Interface 11-1
	Scripting Interface Overview 11-3
	How the Scripting Interface Relays Posture Credentials to ACS 11-3
	ctasi Scripting Interface File 11-4
	ctascriptpp Posture Plugin File 11-5
	Information Files 11-5
	Posture Scripts 11-7
	Posture Data Files 11-7
	Configuring the NAC Environment to Use Your Posture Script 11-13
	Write a Posture Script 11-14
	Write an Information File for the Posture Script 11-14
	Register Posture Scripts 11-14
	Add Script Interface Attributes to the ACS Dictionary 11-15

	Configure ACS Rules to Determine Posture Based on the Script's Posture Attributes 11-18
	Posture Scripts Invoking ctasi 11-18
	Status Change 11-20
	Stale Posture Data 11-20
	Managing Stale Posture Database with CTA 11-21
	Managing Stale Posture Database on the ACS Server 11-22
APPENDIX A	ctastat Diagnostic Tool A-1
	Running the ctastat Utility A-2
	Running ctastat on a Linux Operating System A-2
	Running ctastat on a Mac OS X Operating System A-2
	Running ctastat on a Windows Operating System A-2
	ctastat Utility Output A-3
	General CTA Information A-3
	Session Information A-3
	Plugins Information A-4
	ctastat Utility Sample Output A-4
APPENDIX B	Alternate Methods of Installing CTA B-1
	Installing CTA 2.1 Using CSA MC 5.2 B-1
APPENDIX C	Open Source License Acknowledgement C-1
	OpenSSL/Open SSL Project C-1
	License Issues C-1
	Info-ZIP C-4

L

Administrator Guide for Cisco Trust Agent, Release 2.1