

	deleting software images 3-3
A	editing properties 2-3
AAA authentication for immediate auto updates 2-4	errors adding image files A-4
ACS	managing 2-1
privileges B-1	managing image file assignments 4-1
roles and permissions 1-3	modifying polling period 2-5
user roles B-3	policy restrictions 1-10
Adaptive Security Device Manager (ASDM)	supported 1-1
adding images 3-2	updating configuration files 1-8
assigning to multiple devices 4-4	using NAT 1-2
assigning to single device 4-3	viewing configuration files 3-3
configuring image boot order C-2	viewing image file assignments 4-2, 4-3
deleting images 3-3	viewing summary 2-1
errors adding image files A-4	AUS_IMMEDIATE_FAILURE events 5-3
managing image file assignments 4-1	AUS_IMMEDIATE_SUCCESS events 5-3
managing images 3-1	AUS policy in Security Manager, configuring 1-10
starting 2-7	AUS Remote Interface role B-3
viewing device assignments 4-2, 4-3	authentication errors A-2
viewing image list 3-1	Auto Update Immediate
API Reader role B-3	credential requirements 2-4
API Writer role B-3	HTTPS port number requirement 2-6
Approver role B-2	performing 2-6
ASA devices	auto updates
adding manually 2-3	canceling a schedule 2-5
adding software images 3-2	disabling or blocking 2-7
adding through Security Manager 1-3	immediately updating configurations 2-6
adding to Security Manager 1-9	modifying polling period 2-5
assigning files 4-3, 4-4	scheduling 2-4
blocking auto updates 2-7	auto update schedule types
bootstrapping to work with AUS C-1	any time 2-4, 2-5
configuring image boot order C-2	daily 2-4
credentials for contacting AUS 2-3	never 2-5
deleting 2-6	one time 2-4

weekly 2-4	managing 3-1
Auto Update Server	policy restrictions 1-10
ACS roles B-3	preventing a device from downloading A-5
adding devices 1-3	troubleshooting errors A-6
adding to Security Manager 1-9	troubleshooting errors adding A-4
checking connection to devices A-6	troubleshooting files not current A-3
CiscoWorks roles B-2	updating 1-8
credentials for device contact 2-3	viewing 3-3
database backup and recovery 1-3	viewing device assignments 4-2, 4-3
deploying configuration files 1-8	viewing list 3-1
device support 1-1	CONNECT_FAILURE events 5-3
error messages A-6	CONNECT_SUCCESS events 5-3
getting started 1-1	credentials
logging into or exiting 1-5	editing device 2-3
overview 1-1	enable password 2-4
policy restrictions 1-10	requirements for device contacting AUS 2-3
privileges B-1	TACACS+ 2-4
understanding event types 5-2	troubleshooting A-2
usage statistics 5-1	
user account, configuring 2-3	D
user interface overview 1-7	b
using NAT 1-2	daemon manager, restarting 1-6
	database, backup and recovery 1-3
n	DEVICE_CONFIG_ERROR events 5-3
•	device managers, starting 2-7
browser-server security 1-6	devices
	adding manually 2-3
6	adding through Security Manager 1-3
U	assigning files 4-3, 4-4
Cisco Security Management Suite server, logging into or	blocking updates 2-7
exiting 1-5	bootstrapping to work with AUS C-1
CiscoWorks Common Services	checking connection with AUS A-6
logging into or exiting 1-5	configuring image boot order C-2
roles and permissions 1-3	credentials for contacting AUS 2-3
user roles B-2	deleting 2-6
configuration files	device properties 2-2
assigning to device 4-3	editing properties 2-3
deleting 3-3	managing 2-1
immediately updating 2-6	managing image file assignments 4-1

modifying polling period 2-5	viewing configuration 3-3
rebooting after image update A-5	viewing device assignments 4-2, 4-3
supported 1-1	viewing list 3-1
troubleshooting	
image files that are not current A-4	G
immediate auto updates A-3	G
not appearing in list A-1	GENERAL_DEVICE_ERROR events 5-3
not contacting AUS A-2	greyed out buttons A-5
repeatedly downloads same file A-5	GUI Reader role B-3
viewing image file assignments 4-2, 4-3	GUI Writer role B-3
viewing summary 2-1	
DOWNLOAD_FAILURE events 5-3	
DOWNLOAD_SUCCESS events 5-3	н
	Help Desk role
	ACS B-3
=	CiscoWorks B-2
editing 2-3	HTTPS port number
enable credentials	requirements for immediate auto update 2-6
authentication for immediate updates 2-4	requirements for starting device managers 2-7
editing 2-3	
error messages A-6	-
event failure summary report 5-4	ı
event report 5-4	image files
event success summary report 5-5	adding 3-2
event types 5-2	assigning to multiple devices 4-4
	assigning to single device 4-3
	deleting 3-3
-	managing 3-1
ïles	managing assignments 4-1
adding 3-2	viewing device assignments 4-2, 4-3
assigning to multiple devices 4-4	viewing list 3-1
assigning to single device 4-3	immediate auto updates
deleting 3-3	credential requirements 2-4
managing 3-1	HTTPS port number requirement 2-6
managing assignments 4-1	performing 2-6
policy restrictions 1-10	troubleshooting A-3
troubleshooting errors adding A-4	
updating 1-8	

М	deleting 2-6 deleting software images 3-3
messages, error A-6	editing properties 2-3
mode requirements 1-1	errors adding image files A-4
	managing 2-1
N	managing image file assignments 4-1
•	modifying polling period 2-5
NAT, configuring settings 1-2	policy restrictions 1-10
Network Administrator role	supported 1-1
ACS B-3	updating configuration files 1-8
CiscoWorks B-2	using NAT 1-2
Network Operator role	viewing configuration files 3-3
ACS B-3	viewing image file assignments 4-2, 4-3
CiscoWorks B-2	viewing summary 2-1
no contact since report 5-6	polling interval, modifying 2-5, C-2
P	
PIX Device Manager (PDM)	reports
adding images 3-2	event failure summary report 5-4
assigning to multiple devices 4-4	event report 5-4
assigning to single device 4-3	event success summary report 5-5
deleting images 3-3	no contact since report 5-6
errors adding image files A-4	overview 5-1
managing image file assignments 4-1	system information report 5-1
managing images 3-1	understanding event types 5-2
starting 2-7	January Committee Committe
viewing device assignments 4-2, 4-3	
viewing image list 3-1	S
PIX firewalls	security, enabling SSL 1-6
adding manually 2-3	security, chapling 332 1-1 security context limitations 1-1
adding software images 3-2	Security Manager
adding through Security Manager 1-3	adding devices to AUS 1-3
adding to Security Manager 1-9	
assigning files 4-3, 4-4	deploying configuration files 1-8
blocking updates 2-7	modifying polling period 2-5
bootstrapping to work with AUS C-1	policy restrictions when using with AUS 1-10
configuring image boot order C-2	single-context mode requirements 1-1
credentials for contacting AUS 2-3	software images
creachinais for contacting AUS (-1)	

adding 3-2	performance issues when requesting multiple devices contact AUS 2-7
assigning to multiple devices 4-4 assigning to single device 4-3	preventing a device from downloading a configuration file A-5 types, understanding event 5-2
deleting 3-3	
managing 3-1	
managing assignments 4-1	U
troubleshooting assigning two images to same device A-5	updates
troubleshooting errors adding files A-4	blocking 2-7
viewing device assignments 4-2, 4-3	credential requirements for update now 2-4
viewing list 3-1	performing immediate auto updates 2-6
SSL, enabling on the server 1-6	update schedules
statistics for past 24 hours 5-1	any time schedules 2-4, 2-5
SYSTEM_ERROR events 5-3	canceling 2-5
System Administrator role	configuring 2-4
ACS B-3	daily schedules 2-4
CiscoWorks B-2	managing 2-1
system information report 5-1	never schedules 2-5
	one time schedules 2-4
	viewing summary 2-1
Т	weekly schedules 2-4
TACACS+ credentials 2-3, 2-4	URN for AUS 5-1
troubleshooting	usage statistics 5-1
assigning two images to same device A-5	user interface overview 1-7
AUS startup problems A-5	username, for AUS contact 2-3
authentication errors A-2	user roles and permissions
checking connection between device and AUS A-6	ACS B-3
configuration errors A-6	AUS B-1
device not appearing in list A-1	CiscoWorks B-2
device not contacting AUS A-2	supported 1-3
device reboot after image update A-5	
device repeatedly downloads same file A-5	
error messages A-6	
errors adding configuration files A-4	
errors adding files A-4	
greyed out buttons A-5	
image files that are not current A-4	
immediate auto updates A-3	
where were aparted 11 v	

Index