C

Factory Default Settings

This chapter describes the factory default settings for the primary features, and provides the lists of predefined service and address objects. It includes the following sections:

Device Management

Feature	Setting
Remote Administration	Disable
Remote management using HTTPS	Disable
Access type	All IP addresses
HTTPS listen port number	8080

Feature	Setting
Remote management using HTTP	Disable
HTTP listen port number	80
Remote SNMP	Disable
User Session Settings	
Inactivity timeout	15 minutes (0 to 1000 minutes)
Limit login session for web logins	Disable
Login session limit	10 minutes (0 to 1000 minutes)
SNMP	Disable
SNMP Versions	SNMP Version 1 and 2, SNMP Version 3
Maximum number of certificates	128
Remote Support	Disable
Cisco OnPlus	Enable
Send Diagnostics	Disable
Date and Time	Dynamically set system time
Daylight saving time adjustment	Disable
Default NTP servers	Enable
Host Name	“router” and first three bytes of the MAC address
UPnP	Disable
Bonjour	Enable
CDP	Disable
LLDP	Disable
Syslog Settings	Disable
Email Alert Settings	
CPU Overload Alert	Disable

Feature	Setting
CPU threshold setting	90% (10% to 100%)
New Firmware Alert	Disable
License Expiration Alert	Disable
Alert before the license expires	15 days
Syslog Email	Disable
Site-to-Site VPN Up/Down Alert	Disable
WAN Up/Down Alert	Disable
WAN Up/Down alert interval	5 minutes (3 to 1440 minutes)
Traffic Meter Alert	Disable
Anti-Virus Alert	Disable
Anti-Virus alert interval	30 minutes (1 to 1440 minutes)
IPS Alert	Disable
Web URL Filtering Alert	Disable

User Management

Feature	Setting
User Groups	
Default administrator user group	admin
Available services for user groups	Web Login, SSL VPN, IPsec Remote Access, and Captive Portal
Maximum number of user groups	50
Local Users	
Default administrator username	cisco

Feature	Setting
Default administrator password	cisco
Maximum number of local users	100
User Authentication Methods	Local Database (default) RADIUS RADIUS+Local Database LDAP LDAP+Local Database

Networking

Feature	Setting
IPv4 or IPv6 Routing	IPv4 only
WAN Interfaces	
Maximum number of WAN interfaces	2
WAN1-Physical Port	GE1
WAN1-IP Address Assignment	DHCP Client
WAN1-MTU	Auto
WAN1-MTU Value	1500
WAN1-DNS Server Source	Get Dynamically from ISP
WAN1-MAC Address Source	Use Default MAC address
WAN1-Zone Mapping	WAN
Network Addressing Modes	DHCP Client, L2TP, PPTP, PPPoE, and Static IP
Port Mirroring	Disable

Feature	Setting
Port-based Access Control	Disable
WAN Redundancy Operation Modes	Equal Load Balancing (default) Load Balancing Failover Routing Table
VLANs	
Maximum number of VLANs	16
DEFAULT VLAN	VID=1 IP Address=192.168.75.1 Subnet=255.255.255.0 Spanning Tree=Disable DHCP Mode=DHCP Server DHCP Pool=192.168.75.100 to 200 Lease Time=1 day Default Gateway=192.168.75.1 Mapped Zone=LAN

Feature	Setting
GUEST VLAN	VID=2 IP Address=192.168.25.1 Subnet=255.255.255.0 Spanning Tree=Disable DHCP Mode=DHCP Server DHCP Pool=192.168.25.100 to 200 Lease Time=1 day Default Gateway=192.168.25.1 Mapped Zone=GUEST
VOICE VLAN	VID=100 IP Address=10.1.1.2 Subnet=255.255.255.0 Spanning Tree=Enable Mapped Zone=VOICE DHCP Mode=Disable
Zones	
Maximum number of zones	32
Predefined zones	WAN, LAN, DMZ, VPN, GUEST, SSLVPN, VOICE
Routing	
Routing mode	Disable
Maximum number of Static Routing rules	150
Dynamic Routing (RIP)	Disable
Policy-Based Routing	Disable

Feature	Setting
Maximum number of Policy-Based Routing rules	100
WAN QoS	Disable
Maximum number of traffic selectors	256
Maximum number of WAN QoS policy profiles	32
Maximum number of traffic selectors associated with one WAN QoS policy profile	64
LAN QOS	Disable
WLAN QoS	Disable
Service Management	
Maximum number of service groups	64
Maximum number of services	150
Maximum number of services in one service group	64
Address Management	
Maximum number of address groups	64
Maximum number of addresses	150
Maximum number of addresses in one address group	100
Maximum number of DDNS profiles	16
VRRP	Disable
IGMP Proxy	Enable
IGMP Snooping	Enable
IGMP Version (Default)	IGMP Version 3

Wireless

Feature	Setting
Wireless Radio	Disable
Basic Radio Settings	
Wireless mode	802.11b/g/n mixed
Wireless channel	Auto
Bandwidth channel	Auto
Extension channel	Lower
U-APSD	Disable
SSID isolation (between SSIDs)	Disable
Default SSIDs (cisco-data, cisco-guest, cisco3, cisco4)	Disable
SSID broadcast	Enable
Station isolation (between clients)	Disable
Security mode	Open
Wi-Fi Multimedia (WMM)	Enable
Wireless MAC Filtering	Disable
Advanced Radio Settings	
Guard interval	Long (800 ns)
CTS protection mode	Auto
Beacon interval	100 ms (20 to 999 ms)
DTIM interval	1 ms (1 to 255 ms)
RTS threshold	2347 ms (1 to 2347 ms)
Fragmentation threshold	2346 ms (256 to 2346 ms)
Power output	100%

Feature	Setting
Wi-Fi Protected Setup (WPS)	Disable
Rogue AP Detection	Disable
Captive Portal	Disable
Session timeout	60 minutes (0 to 480 minutes)
Idle timeout	5 minutes (0 to 480 minutes)

VPN

Feature	Setting
Site-to-Site VPN	Disable
Maximum number of Site-to-Site VPN tunnels	100 for ISA570 and ISA570W 50 for ISA550 and ISA550W
IKE Policies	
Maximum number of IKE policies	16
DefaultIke, Hash	SHA1
DefaultIke, Authentication	Pre-shared Key
DefaultIke, D-H Group	Group 2
DefaultIke, Encryption	ESP_AES_256
DefaultIke, Lifetime	24 hours
Transform Policies	
Maximum number of transform policies	16
DefaultTrans, Integrity	ESP_SHA1_HMAC
DefaultTrans, Encryption	ESP_AES_256

Feature	Setting
IPsec Remote Access	Disable
Maximum number of group policies	16
Teleworker VPN Client	Disable
Maximum number of group policies	16
Auto initiation retry	Disable
Retry interval	120 seconds (120 to 1800 seconds)
Retry limit	0 (0 to 16)
SSL VPN	disable
Maximum number of group policies	32
Gateway interface	WAN1
Gateway port number	443
Certificate file	Default
Client address pool	192.168.200.0
Client netmask	255.255.255.0
Idle timeout	2100 seconds (60 to 86400 seconds)
Session timeout	0 seconds (0, 60 to 1209600 seconds)
Client DPD timeout	300 seconds (0 to 3600 seconds)
Gateway DPD timeout	300 seconds (0 to 3600 seconds)
Keep alive	30 seconds (0 to 600 seconds)
Lease duration	43200 seconds (600 to 1209600 seconds)
Max MTU	1406 bytes (256 to 1406 bytes)

Feature	Setting
Rekey method	SSL
Rekey interval	3600 seconds (0 to 43200 seconds)
L2TP Server	Disable
IPsec Passthrough	Enable
PPTP Passthrough	Enable
L2TP Passthrough	Enable

Security Services

Feature	Setting
Anti-Virus	Disable
Application Control	Disable
Spam Filter	Disable
Intrusion Prevention (IPS)	Disable
Web Reputation Filtering	Disable
Web URL Filtering	Disable
Network Reputation	Enable

Firewall

Features	Setting
Default Firewall Rules	Prevent all inbound traffic and allow all outbound traffic

Features	Setting
Maximum number of custom firewall rules	100
NAT	
Dynamic PAT	Enable
Maximum number of Static NAT rules	64
Maximum number of Port Forwarding rules	64
Maximum number of Port Triggering rules	15
Maximum number of Advanced NAT rules	32
Content Filtering	Disable
MAC Address Filtering	Disable
Maximum number of MAC Address Filtering rules	100
IP - MAC Binding	
Maximum number of IP - MAC Binding rules	100
Attack Protection	
Block Ping WAN Interface	Enable
Stealth Mode	Enable
Block TCP Flood	Enable
Block UDP Flood	Enable
Block ICMP Notification	Enable
Block Fragmented Packets	Disable
Block Multicast Packets	Enable

Features	Setting
SYN Flood Detect Rate	128 max/sec (0 to 65535)
Echo Storm	15 packets/sec (0 to 65535)
ICMP Flood	100 packets/sec (0 to 65535)
Session Limits	
Maximum number of connections	60000 (1000 to 60000)
TCP timeout	1200 seconds (5 to 3600 seconds)
UDP timeout	180 seconds (5 to 3600 seconds)
Application Level Gateway (ALG)	
SIP ALG	Enable
H.323 ALG	Enable

Reports

Feature	Setting
Bandwidth Usage Reports	
Bandwidth Usage Report by IP Address	Disable
Bandwidth Usage Report by Internet Service	Disable
Website Visits Report	Disable
WAN Bandwidth Reports	Disable
Security Services Reports	
Anti-Virus Report	Disable
Application Control Report	Disable

Feature	Setting
Email Security Report	Disable
IPS Report	Disable
Network Reputation Report	Enable
Web Security Report	Disable

Default Service Objects

The following table displays all predefined service objects on the security appliance.

Service Name	Protocol	Port Start	Port End	Description
AIM-CONNECT	TCP	4443	4443	AOL Instant Messenger, direct connect
AIM-CHAT	TCP	5190	5190	AOL Instant Messenger, file transfer and chat
BGP	TCP	179	179	Border Gateway Protocol
BOOTP_client	UDP	68	68	Bootstrap Protocol
BOOTP_server	UDP	67	67	Bootstrap Protocol
CU-SEEME	TCP/UDP	7648	7652	Internet Videoconferencing Protocol
DHCP	UDP	67	67	Dynamic Host Configuration Protocol
DNS	TCP/UDP	53	53	Domain Name System
ESP	IP			Protocol 50
FINGER	TCP	79	79	Exchange of human-oriented status and user information

Service Name	Protocol	Port Start	Port End	Description
FTP-DATA	TCP	20	20	File Transfer Protocol, data transfer
FTP-CONTROL	TCP	21	21	File Transfer Protocol, control command
HTTP	TCP	80	80	HyperText Transfer Protocol
HTTPS	TCP	443	443	HTTP over SSL/TLS
ICMP Destination Unreachable	ICMP	3	0	
ICMP Ping Reply	ICMP	0	0	
ICMP Ping Request	ICMP	8	0	
ICMP Redirect Message	ICMP	5	0	
ICMP Router Advertisement	ICMP	9	0	
ICMP Router Solicitation	ICMP	10	0	
ICMP Source Quench	ICMP	4	0	
ICMP Time Exceeded	ICMP	11	0	
ICMP Timestamp	ICMP	13	0	
ICMP Type-6	ICMP	6	0	Alternate Host Address
ICMP Type-7	ICMP	7	0	Reserved
ICQ	TCP	5190	5190	Instant Messenger
IDENT	TCP	113	113	Authentication Service/Identification Protocol

Service Name	Protocol	Port Start	Port End	Description
IKE	UDP	500	500	IPsec Key Exchange
IMAP	TCP	143	143	Internet Message Access Protocol
IMAP2	TCP	143	143	Internet Message Access Protocol Version 2
IMAP3	TCP	220	220	Internet Message Access Protocol Version 3
IPSEC-UDP-ENCAP	UDP	4500	4500	IPsec over UDP
IRC	TCP	6660	6660	Internet Relay Chat, de facto port: 6660 to 6669
ISAKMP	UDP	500	500	
L2TP	UDP	1701	1701	Layer 2 Tunneling Protocol
NEWS	TCP	144	144	
NFS	UDP	2049	2049	Network File System
NNTP	TCP	119	119	Network News Transfer Protocol, NNTP over SSL uses the port 563
POP3	TCP	110	110	Post Office Protocol Version 3
PPTP	TCP	1723	1723	Microsoft Point-to-Point Tunneling Protocol
RCMD	TCP	512	512	
REAL-AUDIO	TCP	7070	7070	
REXEC	TCP	512	512	Remote Process Execution
RIP	UDP	520	520	Routing Information Protocol
RLOGIN	TCP	513	513	

Service Name	Protocol	Port Start	Port End	Description
RTELNET	TCP	107	107	Remote TELNET service
RTSP	TCP/UDP	554	554	Real Time Streaming Protocol
SFTP	TCP	115	115	Simple File Transfer Protocol
SHTTPD	TCP	8080	8080	Simple HTTPD
SHTTPDS	TCP	443	443	Simple HTTPD over SSL
SIP	TCP/UDP	5060	5060	Session Initiation Protocol
SMTP	TCP	25	25	Simple Mail Transfer Protocol
SNMP	TCP/UDP	161	161	Simple Network Management Protocol
SNMP-TRAPS	TCP/UDP	162	162	Simple Network Management Protocol - Trap
SQL-NET	TCP	1521	1521	
SSH	TCP/UDP	22	22	Secure Shell Protocol
STRMWORKS	UDP	1558	1558	
TACACS	TCP	49	49	Login Host Protocol
TELNET	TCP	23	23	
TELNET Secondary	TCP	8023	8023	
TELNET SSL	TCP	992	992	
TFTP	UDP	69	69	Trivial FTP
VDOLIVE	TCP	7000	7000	VDOLive Protocol

Default Address Objects

The following table displays all predefined address objects on the security appliance. The IP address, IP address and netmask, or IP range for these objects will be automatically modified depending on your configuration or network connection.

Address Name	Type	IP, IP/Netmask, or IP Range
WAN1_IP	Host	0.0.0.0
WAN1_GW	Host	0.0.0.0
WAN1_DNS1	Host	0.0.0.0
WAN1_DNS2	Host	0.0.0.0
WAN1_USER_DNS1	Host	0.0.0.0
WAN1_USER_DNS2	Host	0.0.0.0
WAN1_NETWORK	Network	0.0.0.0/255.255.255.255
WAN1_MAC	MAC	N/A
DEFAULT_IP	Host	192.168.75.1
DEFAULT_Network	Network	192.168.75.0/255.255.255.0
DEFAULT_DHCP_POOL	Range	192.168.75.100 to 192.168.75.200
GUEST_IP	Host	192.168.25.1
GUEST_Network	Network	192.168.25.0/255.255.255.0
GUEST_DHCP_POOL	Range	192.168.25.100 to 192.168.25.200
IPv4_Multicast	Range	224.0.0.0 to 239.255.255.255
SSLVPN_ADDRESS_POOL	Network	192.168.200.0/255.255.255.0