

Servicefragen - Wolf Helpo... Secure Firewall Management Center Monitor | Secure Firewall Mani...
 https://10.41.7.30/ui/device-monitoring/health

Firewall Management Center
 System / Health / Monitor

Monitoring
 Home
 Firewall Management Center
 Devices (2)
 wde-ftd-HA
 wde-ftd-01 Active
 wde-ftd-02 Standby

Health Status
 3 total 2 critical 0 warnings 1 normal 0 disabled
 Filter using device name...

Firewall Management Center Devices

Device	Version	Model
FMC	7.2.5.1	Secure Firewall Management Center 1600
wde-ftd-01 Active	7.2.5	Cisco Firepower 4115 Threat Defense
wde-ftd-02 Standby	7.2.5	Cisco Firepower 4115 Threat Defense

Threat Data Updates on Devices
 Cisco Cloud Configuration - Unable to reach Cisco Cloud from the device. Please check the network connectors. [see more](#) Run All Mar 8, 2024 8:40 AM

Appliance Heartbeat
 All appliances are sending heartbeats correctly. Mar 8, 2024 8:40 AM

Automatic Application Bypass Status
 No applications were bypassed. Mar 8, 2024 8:40 AM

Cluster/HA Failure Status
 Process is running correctly. Mar 8, 2024 8:40 AM

Configuration Resource Utilization
 Deployed configurations are normal. Mar 8, 2024 8:40 AM

Disk Status
 Primary Disk Status is healthy
 No 2nd drive available. Mar 8, 2024 8:40 AM

Interface Status
 Interface 'Port-channel2.3519' is not receiving any packets. [see more](#) Run All Mar 8, 2024 8:42 AM

Threat Data Updates on Devices
 Cisco Cloud Configuration - Unable to reach Cisco Cloud from the device. Please check the network connectors. [see more](#) Mar 8, 2024 8:42 AM

Appliance Heartbeat
 All appliances are sending heartbeats correctly. Mar 8, 2024 8:42 AM

Automatic Application Bypass Status
 No applications were bypassed. Mar 8, 2024 8:42 AM

Cluster/HA Failure Status
 Process is running correctly. Mar 8, 2024 8:42 AM

Configuration Resource Utilization
 Deployed configurations are normal. Mar 8, 2024 8:42 AM

Firewall Management Center
 Devices / Secure Firewall Interfaces

Overview Analysis Policies **Devices** Objects Integration

wde-ftd-HA
 Cisco Firepower 4115 Threat Defense

Summary High Availability Device Routing **Interfaces** Inline Sets DHCP VTEP

Search by name Sync Device Add Interfaces

Interface	Logical Name	Type	Security Zones	MAC Address (Active/Standby)	IP Address	Path Monitoring	Virtual Router
Ethernet1/5		Physical				Disabled	
Ethernet1/6	diagnostic	Physical				Disabled	Global
Ethernet1/7		Physical				Disabled	
Ethernet1/8		Physical				Disabled	
Port-channel1		EtherChannel				Disabled	
Port-channel1.3017	RZ01_INFRA_VN-Global	Subinterface	SDA_INFRA	0000.3017.000A/0000.3017.000B	10.39.36.66/30(Static)	Disabled	Global
Port-channel1.3018	RZ01_CAMPUS_VN-Global	Subinterface	SDA_CAMPUS	0000.3018.000A/0000.3018.000B	10.39.36.70/30(Static)	Disabled	Global
Port-channel1.3019	RZ01_SECURE_VN-Global	Subinterface	SDA_SECURE	0000.3019.000A/0000.3019.000B	10.39.36.74/30(Static)	Disabled	Global
Port-channel1.3021	RZ02_INFRA_VN-Global	Subinterface	SDA_INFRA	0000.3021.000A/0000.3021.000B	10.39.36.78/30(Static)	Disabled	Global
Port-channel1.3022	RZ02_CAMPUS_VN-Global	Subinterface	SDA_CAMPUS	0000.3022.000A/0000.3022.000B	10.39.36.82/30(Static)	Disabled	Global
Port-channel1.3023	RZ02_SECURE_VN-Global	Subinterface	SDA_SECURE	0000.3023.000A/0000.3023.000B	10.39.36.86/30(Static)	Disabled	Global
Port-channel2		EtherChannel				Disabled	

Displaying 1-13 of 13 interfaces | Page 1 of 1

← → ↻ 🏠 <https://10.41.7.30/ddd/#PFSettings;uuid=10F920C6-31C6-0ed3-0000-060129543343?type=PG.PLATFORM.NgfwF>

Lesezeichen importier... Erste Schritte Erste Schritte Wolf Google Notizen Google Kontakte Google Kalender Startseite – Google Drive Posteingang -

Firewall Management Center Overview Analysis Policies **Devices** Objects Integration
Devices / Platform Settings Editor

plattform
Enter Description

ARP Inspection
Banner
DNS
External Authentication
Fragment Settings
HTTP Access
ICMP Access
SSH Access
SMTP Server
SNMP
SSL
Syslog
Timeouts
Time Synchronization
Time Zone
UCAPL/CC Compliance

DNS Settings **Trusted DNS Servers**

Applicable to only Firepower Threat Defense 7.1 version and onwards.

Trust Any DNS server

- DNS Servers discovered by dhcp-pool are considered trusted DNS servers
- DNS Servers discovered by dhcp-relay are considered trusted DNS servers
- DNS Servers discovered by dhcp-client are considered trusted DNS servers
- DNS Server Group are considered trusted DNS servers

Specify DNS Servers
List of Trusted DNS Servers

🔍 Search Edit

← → ↻ 🏠 <https://10.41.7.30/ddd/#PFSettings;uuid=10F920C6-31C6-0ed3-0000-060129543343?type=PG.PLATFORM.NgfwPFSettings>

Lesezeichen importier... Erste Schritte Erste Schritte Wolf Google Notizen Google Kontakte Google Kalender Startseite – Google Drive Posteingang - mario.li...

Firewall Management Center Overview Analysis Policies **Devices** Objects Integration
Devices / Platform Settings Editor

plattform
Enter Description

ARP Inspection
Banner
DNS
External Authentication
Fragment Settings
HTTP Access
ICMP Access
SSH Access
SMTP Server
SNMP
SSL
Syslog
Timeouts
Time Synchronization
Time Zone
UCAPL/CC Compliance

DNS Settings **Trusted DNS Servers**

DNS Resolution Settings
Specify DNS servers group and device interfaces to reach them.

⚠ At least one DNS server group is mandatory to be configured as default.

Enable DNS name resolution by device

DNS Server Groups Add

Expiry Entry Timer:
1 Range: 1-65535 minutes