# epati

## High Accessibility With an Active and Passive Cluster Using Link Aggregation

Product: Antikor v2 - Next Generation Firewall

Configuration Examples

www.epati.com.tr

# ераті



### High Accessibility With an Active and Passive Cluster Using Link Aggregation

**High availability (HA) Cluster** systems are designed to ensure uninterrupted service by preventing accessibility from being blocked due to problems that may arise at a single point. The uninterrupted operation of very important services offered in a network is the primary purpose.

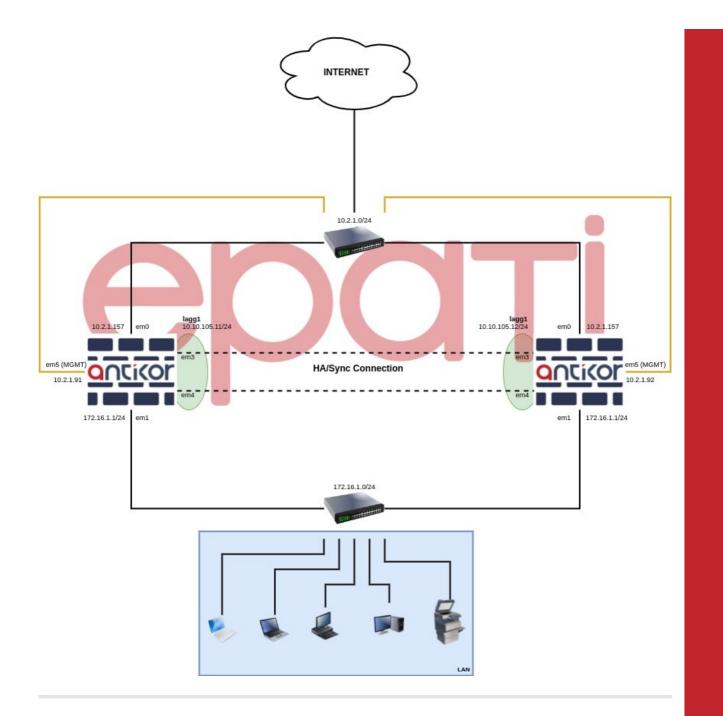
When a server running within the HA Cluster structure encounters any software or hardware errors, passive server is held and another server capable of providing the services provided by the principal server takes over. The service continues uninterrupted while the Master server is correcting the error. This working principle is called failover.

Antikor v2 Firewalls control each other by sending control messages over the network at intervals that we can specify. Task switching occurs between two firewalls when control messages cannot be transmitted due to an error.

#### The events that initiate the switching task are:

- If there is no access to one or more specified targets through the Active firewall;
- If the Active firewall does not respond to the control messages;
- If there is an error in the path monitoring route or critical software components on the Active firewall.

#### **Network Topology**



Common Configurations to Be Made on Both Servers

• Network Configuration is entered on the Ethernet Assignment page in the menu.

Network Configuration	~
IP Pools	
IP Alias	
Ethernet Assignment	
VLAN Configuration	
Virtual Ethernet - VLAN Interface	
Virtual Ethernet - Link Aggregation	
Virtual Ethernet - Loopback	
Virtual Ethernet - PPP	
Ethernet Status	
Gateway Monitoring	
WAN Groups	
Global NAT	
IPv6 6to4 Tunelling	

• It should be checked that the ethernet interfaces to be synchronized in the cluster are in the **Active** state of the **Cluster Membership**.

Ethernet Assignment CReload Add WAN Add LAN Add DMZ									Add DMZ Add PPPoE				
x	LS CSV	PDF						III Sho	w/Hide 👻	Records Per Pa	ge	ОК	▼ Filter
#		Cluster Membership	Web Interface Access 斗	Security Zone	Interface \$	Ethernet Name \$1	Selected Speed	MTU J1	IPv4 Address	IPv6 Address ↓↑	Options	Description	Actions
1	Active	Active	Active	lan1-zone (lan1-zone-15p)	LAN1	em1 - Physical	autoselect	1500	172.16.1.1/	/24	Anti-Spoof DHCPv4 Server Registration MAC-IP Pairing	LAN1	🕼 Edit 📋 Delete
2	Active	Active	Active	wan1-zone (wan1-zone-15p)	WAN1	em0 - Physical	autoselect	1500	10.2.1.157/	/24			🕼 Edit 💼 Delete
					æ	← 1 →	30						Go

Ethernet States		IPv4 Settings		
Status	Active		Obt	tain IPv4 Automatically
Security Zone	lan1-zone (lan1-zone-15p 💙	IPv4 Address	IPv4	172.16.1.1/24
Interface	LAN1 🗸	DHCPv4 Pool Mode	Distrib	pute IP to All Clients $\times$ $ imes$
Ethernet Name	em1 (LAN1) 🗸 🗸	DHCPv4 Start	IPv4	172.16.1.10
Speed	autoselect 🗸	DHCPv4 End	IPv4	172.16.1.250
MTU	1500	DHCPv4 Gateway	IPv4	172.16.1.1
Web Interface Access	Active	DHCPv4 Relay Address	IPv4	
Cluster Membership	Active			
Cluster Ethernet Name	em1	Options		
Description	LAN1	<ul><li>MAC-IP Pairing</li><li>Registration</li></ul>		✓ Anti-Spoof Make announcement
		DHCPv6 Server DHCPv6 Relay		DHCPv4 Server DHCPv4 Relay
IPv6 Settings		Managed Flag		Other Flag
	Obtain IPv6 Automatically			
EUI64	Passive			
IPv6 Address	IPv6 ffff::1/8			
DHCPv6 Start	IPv6			
DHCPv6 End	IPv6			
DHCPv6 Relay Address	IPv6			
				🖉 Cancel 📔 Sa

• Virtual Ethernet - Link Aggregation page is entered in the Network Configuration menu.

😧 Netwo	rk Configuration
IP Poo	ols
IP Alia	as
Ether	net Assignment
VLAN	Configuration
Virtua	al Ethernet - VLAN Interface
Virtua	al Ethernet - Link Aggregation
Virtua	al Ethernet - Loopback
Virtua	al Ethernet - PPP
Ether	net Status
Gatev	way Monitoring
WAN	Groups
Globa	il NAT
IPv6 6	5to4 Tunelling

Virtual Ethernet - Link Aggregation

Virtual	thernet - Link Aggr	egation		2 Reload + Add	
XLS	CSV PDF		⊞ Show/Hide	<ul> <li>Records Per Page</li> </ul>	OK Tilter Reset Filter
#	Name	🎼 Virtual Ethernet Type	👫 🛛 Member Ethernet	1 Description	11 Actions
			( ( ) )		Go

• In both servers, two ports are combined and save as LACP.

Virtual Ethernet - Link Agg	gregation - Edit Record	×	
Name	lagg1		
Member Ethernet	em3 × em4 ×		
Virtual Ethernet Type	LACP	~	
Description	lagg1		
		⊘ Cancel 🕒 Save	
Virtual Ethernet - Link Aggregation			C Reload + Add
XLS CSV PDF		B Show/Hide →     Records Per Page	OK 🛛 🏹 Filter 🖉 Reset Filter
#         Name         Iii         Virtual Ethernet Ty           1         lagg1         LACP	rpe I Member Ethernet	L1 Description	Actions
i noggi UNUP		10 <u>55</u> i	Go

• Definitions are applied by clicking the Apply Definitions button.

ocess list to be applied	Apply Ch	nanges 2
		📑 Apply All
ByPass Ethernets 1	Арр	ly 🖹
	Арр	
Virtual Ethernet - Aggregation 0	Арр	ly 🖹
rocess list to be applied		
Tüm Uyg	ulamalar Güncel	
onfigurations that Will be Made on the Device whe	re the Beginning Job Will be Active	
Entered Management Panel Settings page from M	lanagement Panel Settings menu.	
嶜 Management Panel Settings 🛛 🗸 👻		
Management Panel Settings		
Management Panel Settings User Roles		
User Roles		
User Roles Client Groups		
User Roles Client Groups Management Panel Users		
User Roles Client Groups		
User Roles Client Groups Management Panel Users Banned Users		
User Roles Client Groups Management Panel Users Banned Users		
User Roles Client Groups Management Panel Users Banned Users	Session Settings	
User Roles Client Groups Management Panel Users Banned Users	Log Traffic open	
User Roles Client Groups Management Panel Users Banned Users nagement Panel Settings Service Settings Web Interface Access Protocol  https _ https _ http	Log Traffic open	
User Roles Client Groups Management Panel Users Banned Users nagement Panel Settings	Log Traffic Cours	
User Roles Client Groups Management Panel Users Banned Users Banned Users Uservice Settings Uservice Port Number Bervice Port Number Bervice Port Number Bervice Port Number	Log Traffic oper	
User Roles Client Groups Management Panel Users Banned Users Banned Users Uservice Settings Web Interface Access Protocol Service Settings Uservice Port Number Service Port Number B800 Cpu Rezervation For Management Panel	Log Traffic open	
User Roles Client Groups Management Panel Users Banned Users Banned Users Service Settings Veb Interface Access Protocol Service Settings Cpu Rezervation For Management Panel Cpu Rezervation For Management Panel	Log Traffic open Certificate Based Authentication Closes Authentication From External Source Closes Concurrent Login open Operation Mode Limitless Access v	
User Roles Client Groups Management Panel Users Banned Users Banned Users Service Settings Veb Interface Access Protocol Service Settings Cpu Rezervation For Management Panel Cpu Rezervation For Management Panel	Log Traffic open	
User Roles Client Groups Management Panel Users Banned Users negement Panel Settings Web Interface Access Protocol • https • http Service Port Number 8800 Cpu Rezervation For Management Panel • owe Independent Management Infrastructur	Log Traffic oper  Certificate Based Authentication Concurrent Login Operation Mode Limitless Access Cogin Disclaimer Conce SSH Banner State Conce SSH Banner State Conce	
User Roles Client Groups Management Panel Users Banned Users Banned Users Uservice Settings Web Interface Access Protocol Service Settings User Roles () https ) http Service Port Number 8800 Cpu Rezervation For Management Panel Independent Management Infrastructure	Log Traffic Certificate Based Authentication Close Authentication From External Source Concurrent Login Operation Mode Limitless Access SSH Banner State Close	sload + Add
User Roles Client Groups Management Panel Users Banned Users megement Panel Settings	Log Traffic or Certificate Based Authentication conservations conservations Authentication From External Source conservations Concurrent Login Operation Mode Limitless Access v Operation Mode Limitless Access v Login Disclaimer conservations conserva	Hoad + Add
User Roles Client Groups Management Panel Users Banned Users magement Panel Settings Web Interface Access Protocol • https • http Service Port Number 8800 Cpu Rezervation For Management Panel • • • • • • • • • • • • • • • • • • •	Log Traffic ore Certificate Based Authentication conserved Authentication From External Source conserved Authentication From External Source conserved Authentication Mode Imittless Access v Operation Mode Imittless Access v Login Disclaimer conserved Authentication SSH Banner State conserved Authentication Conserved Authentication SSH Banner State conserved Authentication SSH Banner State conserved Authentication Conserved Authentication Conserved Authentication Authentication Mode Imittless Access v Accessible Networks XLS CSV PDF # IP Address I Description I Actions	slaad + Add
User Roles Client Groups Management Panel Users Banned Users service Port Number Boo Cpu Reservation For Management Panel Cpu Reservation For Management Panel Cpu Reservation For Management Panel Course Service Port Number Boo Course	Log Traffic ore Certificate Based Authentication Concer Authentication From External Source Concer Concurrent Login ore Login Disclaimer Conce SSH Banner State Conce SSH Banner State Conce SSH Banner State Conce SSH Banner State Conce SSW Concer Accessible Networks	Hoad + Add
User Roles Client Groups Management Panel Users Banned Users angement Panel Settings Veb Interface Access Protocol Number 000 00000000000000000000000000000000	Log Traffic ore Certificate Based Authentication conserved Authentication From External Source conserved Authentication From External Source conserved Authentication Mode Imittless Access v Operation Mode Imittless Access v Login Disclaimer conserved Authentication SSH Banner State conserved Authentication Conserved Authentication SSH Banner State conserved Authentication SSH Banner State conserved Authentication Conserved Authentication Conserved Authentication Authentication Mode Imittless Access v Accessible Networks XLS CSV PDF # IP Address I Description I Actions	Hoad + Add

• From the **Service Settings** tab **The Independent Management Infrastructure** is activated and the management IP address is given. In this configuration example, the IP address for the device that will be

active in the startup task is set to 10.2.1.91.(After applying cluster synchronization, independent management was used, since the WAN IP addresses of the two devices will be the same.)

Service Settings				
Web Interface Access Protocol Service Port Number	<ul> <li>https ) http</li> <li>8800</li> </ul>			
Cpu Rezervation For Management Panel	Closed			
Independent Management Infrastructure	Open			
Ethernet to be Assigned	em5	~		
IP Address	IPv4 10.2.1.91/24			
Default Gateway	IPv4 10.2.1.253			
Output Port for Update	Management	~		
🖺 Sav	ve			

- After entering the settings, the save button is clicked.
- Definitions are applied by clicking the Apply Definitions button.

Process list to be applied	Apply Changes 4
	🖴 Apply All
Web Panel Access Configuration 2	Apply 🔒
SSH Configuration	Apply
Management Panel Settings	Apply
Ethernet Web Interface Access 2	Apply

```
Process list to be applied
```

$\bigcirc$	Tüm Uygulamalar Güncel

• Entered Cluster Settings page from System Settings menu.

🕫 System Settings					
System Information					
DNS Settings					
Campus Settings					
RADIUS Settings					
Proxy Settings					
Syslog Settings					
Log Settings					
SSL Certificate Management					
Http(s) Server Forwarding					
DHCP Settings					
Cluster Settings					
SNMP Configurations					
Netflow Settings					
Session Settings					
Language Settings					
LLDP Settings					

Cluster Settings

c	Other Device's License Key is not verified! Please verify.						
Clu	ster Settings					✓ Verify Other Device's Li	cense
	Operation Mode Settings				Sync Se	ettings	
	Operation Mode	Standalone Active - Passiv	ve		Delegate job if other device is healthy	Active	
	Beginning Job	Active Passive			Connection States Sync	Passive	
	Keepalive Packet Send Frequency	100	ms		Update Package Sync	Passivo	
	Keepalive Packet Receive Timeout	400	ms		Sync Changes From Management	Active	
	Ethernet	Settings			Handshake	e Settings	
	Sync Ethernet	Select	~		VHID Value	1	
	IP Address	IPv4 10.10.10/32			Predefined Key	Ø	
	Other Device IP Address	IPv4 10.10.10.10			Other Device License Key	Ð	
				🖹 Save			

- In **Operation Mode** settings, after Working Mode is set to **Active-Passive**, **Beginning Job** is marked as **Active**.
- Keepalive Packet Send Frequency (default 100ms) and Keepalive Packet Receive Timeout (default 400ms) are left at default values.

Operation Mode	Standalone < Active - Pas	sive
Beginning Job	Active Passive	
Keepalive Packet Send Frequency	100	ms
Keepalive Packet Receive Timeout	400	ms

- In Sync Settings, Delegate job if other device is healthy and Sync Changes From Management are set to *Passive*.
- Connection States Sync and Update Package Sync are set to Active.

Sync Settings		
Delegate job if other device is healthy	Passive	
Connection States Sync	Active	
Update Package Sync	Active	
Sync Changes From Management	Passive	

- In Ethernet Settings, the ethernet interface to be synchronized is selected.
- The IP address of the Ethernet to be synchronized and the Cluster IP address of the opposite device are written. (The IP address to be entered here does not need to be added to the IP pools.)

Ethernet Settings				
Sync Ethernet	em4 (CLUSTER) 🗸			
IP Address	IPv4 10.10.105.11/24			
Other Device IP Address	IPv4 10.10.105.12			

Note: The IP addresses to be given to the two devices must be from the same IP block. For example, if the synchronization IP address of this server is 10.10.105.11/24, the IP address of the other server is different from the opposite server, but is located on the same IP block 10.10.105.12/24 is given.

• The VHID value entered in the **Handshake Settings** must be the same as the device opposite. If there is another device running VRRP on the network (such as a switch, router), there may be a VHID conflict. For

this reason, VHIDS on other devices or devices should be known and given a different value than them.

- The Predefined Key must be the same as the device opposite.
- The Other Device License Key is entered in the section of the License key of the opposite device.

Handshake Settings		
VHID Value	19	
Predefined Key	<i>¶</i> <sub>0</sub>	
Other Device License Key	<i>¶</i>	

• Click the Save button.

Cluster Settings			✓ Verify Other Device's License
Operation N	Node Settings	Sync S	Settings
Operation Mode	Standalone 🕑 Active - Passive	Delegate job if other device is healthy	Passivo
Beginning Job	Active Passive	Connection States Sync	Active
Keepalive Packet Send Frequency	100 ms	Update Package Sync	Active
Keepalive Packet Receive Timeout	400 ms	Sync Changes From Management	Passive
Etherne	et Settings	Handsha	ke Settings
Sync Ethernet	em4 (CLUSTER) 🗸	VHID Value	19
IP Address	IPv4 10.10.105.11/24	Predefined Key	Ø ·····
Other Device IP Address	IPv4 10.10.105.12	Other Device License Key	<i>¶</i> <sub>0</sub>
		🖺 Save	

• Definitions are applied by clicking the Apply Definitions button.

Process list to be applied	Apply Changes 1
	apply All
Cluster Settings	Apply

Process list to be applied

$\bigcirc$	Tüm Uygulamalar Güncel

Configurations that Will be Performed on the Device whose Beginning Job Will Be Passive

• Entered Management Panel Settings page from Management Panel Settings menu.

🖀 Management Panel Settings	~
Management Panel Settings	
User Roles	
Client Groups	
Management Panel Users	
Banned Users	

Management Panel Settings

Service	Settings	Sessio	n Settings
Web Interface Access Protocol Service Port Number	https () http 8800	Log Traffic Certificate Based Authentication	Copen Closed
Cpu Rezervation For Management Panel	Closed	Authentication From External Source	Closed
Independent Management Infrastructure	Closed	Concurrent Login	Open
B S	ave	Operation Mode	Limitless Access 🗸
		Login Disclaimer	Closed
		SSH Banner State	Closed
		8	Save
Service	e Cases	Accessib	e Networks
XLS         CSV         PDF           #         Ethernet Name         II         IP Address         II	C Reload	XLS CSV PDF # IP Address II Description	C Reload + Add ↓↑ Actions
1 em0 10.2.1.157/24	WAN1 Open	1 0.0.0/0	🕼 Edit 🕅 Delete
2 em1 172.16.1.1/24	LAN1 Open Go	( ( 1 ) )	Go

 Management IP address is given by activating Independent Management Infrastructure from Service Settings tab. In this configuration example, the IP address for the device whose initial task will be passive is set to 10.2.1.92. (Independent management is used since the WAN IP addresses of the two devices will be the same after cluster synchronization is applied.)

Service Settings		
Web Interface Access Protocol Service Port Number	<ul> <li>https ) http</li> <li>8800</li> </ul>	
Cpu Rezervation For Management Panel	Closed	
Independent Management Infrastructure	Open	
Ethernet to be Assigned	em5	~
IP Address	IPv4 10.2.1.92/24	
Default Gateway	IPv4 10.2.1.253	
Output Port for Update	Management	~
🖺 Sa	ve	

- After entering the settings, the save button is clicked.
- Definitions are applied by clicking the Apply Definitions button.

Process list to be applied	Apply Changes 4
	≅ Apply All
Web Panel Access Configuration 🔞	Apply
SSH Configuration 1	Apply
Management Panel Settings	Apply
Ethernet Web Interface Access 🔞	Apply

#### Process list to be applied

	$\bigcirc$	Tüm Uygulamalar Güncel
--	------------	------------------------

• Entered Cluster Settings page from System Settings menu.

🕫 System Settings
System Information
DNS Settings
Campus Settings
RADIUS Settings
Proxy Settings
Syslog Settings
Log Settings
SSL Certificate Management
Http(s) Server Forwarding
DHCP Settings
Cluster Settings
SNMP Configurations
Netflow Settings
Session Settings
Language Settings
LLDP Settings

Cluster Settings

	Other Device's License Key is not verified! Please verify.						
•	Cluster Settings					🗸 Veri	fy Other Device's License
	Operation M	lode Settings			Sync S	ettings	
	Operation Mode	Standalone Active - Passive			Delegate job if other device is healthy	Active	
	Beginning Job	Active Passive			Connection States Sync	Passive	
	Keepalive Packet Send Frequency	100	ms		Update Package Sync	Passive	
	Keepalive Packet Receive Timeout	400	ms		Sync Changes From Management	Active	
	Ethernet	Settings			Handshal	e Settings	
	Sync Ethernet	Select	~		VHID Value	1	
	IP Address	IPv4 10.10.10/32			Predefined Key	Ð	
	Other Device IP Address	IPv4 10.10.10.10			Other Device License Key	Ð	
			E	😫 Save	e		

- In **Operation Mode** settings, after Working Mode is set to **Active-Passive**, **Beginning Job** is marked as **Active**.
- Keepalive Packet Send Frequency (default 100ms) and Keepalive Packet Receive Timeout (default 400ms) are left at default values.

Operation Mode	🔵 Standalone < Active - Passive	
Beginning Job	Active 🖌 Passive	
Keepalive Packet Send Frequency	100	ms
Keepalive Packet Receive Timeout	400	ms

- In Sync Settings, Delegate job if other device is healthy and Sync Changes From Management are set to *Passive*.
- Connection States Sync and Update Package Sync are set to Active.

Sync S	ettings
Delegate job if other device is healthy	Passive
Connection States Sync	Active
Update Package Sync	Active
Sync Changes From Management	Passive

- In Ethernet Settings, the ethernet interface to be synchronized is selected.
- The IP address of the Ethernet to be synchronized and the Cluster IP address of the opposite device are written. (The IP address to be entered here does not need to be added to the IP pools.)

Ethernet S	Settings
Sync Ethernet	em4 (CLUSTER) 🗸
IP Address	IPv4 10.105.12/24
Other Device IP Address	IPv4 10.105.11

Note: The IP addresses to be given to the two devices must be from the same IP block. For example, if the synchronization IP address of this server is 10.10.105.12/24, the IP address of the other server is different from the opposite server, but is located on the same IP block 10.10.105.11/24 is given.

• The VHID value entered in the **Handshake Settings** must be the same as the device opposite. If there is another device running VRRP on the network (such as a switch, router), there may be a VHID conflict. For

this reason, VHIDS on other devices or devices should be known and given a different value than them.

- The Predefined Key must be the same as the device opposite.
- The Other Device License Key is entered in the section of the License key of the opposite device.

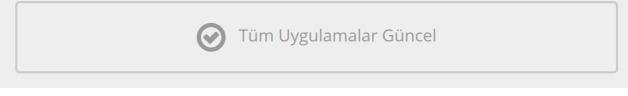
Handshake	Settings
VHID Value	19
Predefined Key	(4)
Other Device License Key	<

• Click the Save button.

Cluster Settings							
C C							✓ Verify Other Device's License
Operation Me	ode Setting	<u>1</u> 5				Sync S	ettings
Operation Mode	Sta	ndalone 🕑 Active - Passive			Delegate job if other device is h	althy	Passive
Beginning Job	Act	ive 🕑 Passive			Connection State	s Sync	Active
Keepalive Packet Send Frequency	100		ms		Update Packag	e Sync	Active
Keepalive Packet Receive Timeout	400		ms		Sync Changes From Manage	ement	Passive
Ethernet	Settings				F	landshak	ke Settings
Sync Ethernet	em4 (	CLUSTER)	~		VHID	Value	19
IP Address	IPv4	10.10.105.12/24			Predefine	d Key	Ф <b>·····</b>
Other Device IP Address	IPv4	10.10.105.11			Other Device Licens	e Key	•
				🖹 Save			

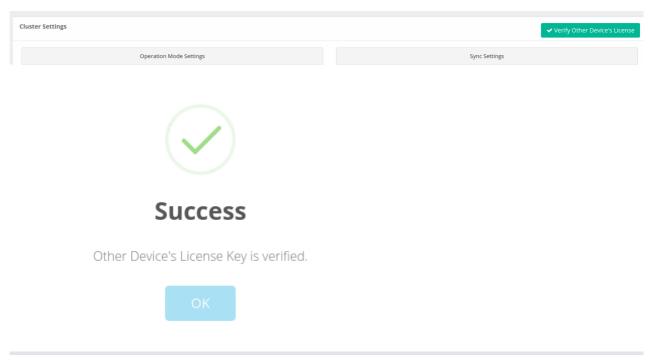
• Definitions are applied by clicking the Apply Definitions button.

Process list to be applied	Apply Changes 1
	🗃 Apply All
Cluster Settings	Apply
Process list to be applied	



• After applied the definitions, the connection is tested with the Verify License Key of Other Device button. It appears to be successful. In case of failure, the license key and connection between the two servers should be checked.

Cluster Settings



Note: If you want the settings to be the same on both devices;**Active** device **Cluster Status** on the **Dashboard** when the `Resynchronize' button is clicked on the tab, all the settings of the active device will be pressed on the Passive device.

4			
ACTIVE	Antikor NGFW 10.10.105.11	Antikor NGFW 10.10.105.12	Error Fostory O
	(ACTIVE)	(PASSIVE)	Error Factor: 0
Switch State	(	(Online)	
		(Last seen: 2021-10-	
		26T08:56:11.431Z)	

#### **Testing and Controls**

• The Cluster Status on the Dashboard should indicate that it isonline to the Passive device if the device status is **Active**. If it does not write, the cluster settings and physical connections should be checked.



• The Cluster Status on the dashboard should say Online for the Active device if the device status is **Passive**. If it does not write, the cluster settings and physical connections should be checked.



Antikor NGFW 10.10.105.12 (PASSIVE)



(Last seen: 2021-10-26T08:56:52.603Z)





ePati Cyber Security Technologies Inc. Mersin Universitesi Ciftlikkoy Kampusu Teknopark Idari Binasi Kat: 4 No: 411 Zip Code: 33343 Yenisehir / MERSIN / TURKIYE