

Useroam Cloud Sophos Entegrasyon Rehberi

1 - Useroam Panele Cihaz Ekleme

panel.useroam.com adresinden panelinize giriş yapıp **Yeni Cihaz** ekleyiniz. Sistem, lisansınızı otomatik olarak seçecektir.

- **Cihaz tipi:** Sophos seçiniz.
- **Cihaz adresi:** Firewall'un WAN IP adresini seçiniz. Eğer birden fazla WAN IP adresiniz varsa, Sophos cihazı bu isteği varsayılan olarak ilk WAN bacağından gönderir.

Not: Farklı bir WAN bacağından gönderim yapmak isterseniz, bir SNAT kuralı oluşturarak ilgili trafiği istediğiniz WAN bacağına yönlendirebilirsiniz.

Yeni Cihaz

**Cihaz Detayları**

AUVA3RYOZQ4E7F0LR7Z1640QD7XZ

Cihaz Tipi

Sophos

☒ 5651 Loglama

Cihaz Adresi

178.159.35.173

Cihaz Adı

GLX-Sophos-FW

2- Cihaz Erişim Ayarları (Device Access)

Sonra **Administration > Device Access** menüsüne gidiniz. Burada **Useroam'u** kullanacağınız **Zone'da** sadece **Captive Portal** ve **DNS** seçeneklerini işaretleyerek aktif hale getiriniz.

Dikkat: Radius SSO gibi farklı kimlik doğrulama mekanizmalarını aktif hale getirmeniz durumunda, yönlendirme sorunları veya Captive Portal sayfasının yavaş açılması gibi problemler yaşanabilir.

The screenshot shows the Sophos Administration web interface. The left sidebar contains navigation menus for 'MONITOR & ANALYZE', 'PROTECT', 'CONFIGURE', and 'SYSTEM'. The 'Administration' menu is highlighted. The main content area is titled 'Administration' and shows a 'Local service ACL' configuration page. The 'Device access' tab is selected. A table lists various services for different zones. The 'GUEST' zone is highlighted with a red box, showing that 'Captive portal' is enabled. Below the table, there is a note about turning off access to the captive portal and an 'Apply' button. At the bottom, there is a section for 'Local service ACL exception rule' which is currently empty.

Zone	Admin services		Authentication services					Network services		
	HTTPS	SSH	AD SSO	Captive portal *	Radius SSO	Clients	Chromebook SSO	Ping/Ping6	DNS	IP
LAN	☒	☒	☐	☒	☒	☒	☒	☒	☒	☐
WAN	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
DMZ	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
VPN	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
WiFi	☒	☒	☐	☒	☒	☒	☒	☒	☒	☐
GUEST	☐	☐	☐	☒	☐	☐	☐	☐	☒	☐

Turning off access to captive portal stops user notifications from appearing. Example: Web filter and zero-day protection notification pages.

Apply

Local service ACL exception rule

Show additional properties

#	Name	Source zone	Source	Destination
No records found				

3 - Radius Sunucu Ekleme

Authentication > Servers menüsünden yeni bir Radius sunucu ekleyiniz. [cite: 189, 190] Server IP kısmına, **panel.useroam.com** adresini pingleyerek çıkan IP adresini yazınız.

Ardından, **Useroam > Sistem Ayarları > Cihaz Ayarları** altında bulunan **Cihaz Şifresi** kısmının karşısında yazan kodu da **Shared Secret** kısmına giriniz.

Cihaz Detayları

Cihaz Adresi	178.159.35.173
☒ 5651 Loglama	
Cihaz Adı	Sophos-GLX-Test
Cihaz Şifresi	bjhcqhml

SOPHOS FW

Search

MONITOR & ANALYZE

Control center

Current activities

Reports

Zero-day protection

Diagnostics

PROTECT

Rules and policies

Intrusion prevention

Web

Applications

Wireless

Email

Web server

Active threat response

CONFIGURE

Remote access VPN

Site-to-site VPN

Network

Routing

Authentication

System services

SYSTEM

Sophos Central

Profiles

Hosts and services

Administration

Backup & firmware

Certificates

Edit external server

Servers

Services

Groups

Users

Multi-factor authentication

Server type

RADIUS server

Server name *

Useroam

Server IP *

104.247.174.120

Authentication port *

1812

Time-out *

3

☒ Enable accounting

Accounting port

1813

Shared secret *

***** [Change Shared secret](#)

Domain name ⁱ

Enter Domain name

Group name attribute *

Filter-Id

☐ Enable additional settings

Test connection

Save

Cancel

4 - Ba?lant? Testi (?ste?e Ba?l?)

Bu noktada bir test yapmak isterseniz:

Useroam Cloud panelinden **Kullanıcı Yönetimi > Yeni Kullanıcı** adımlarıyla yeni kullanıcı oluşturabilir; Firewall'da Radius Sunucu ayarının içinden **Test Connection** ile bağlantıyı kontrol

edebilirsiniz.

SOPHOS FW

Add external server

Search

MONITOR & ANALYZE

- Control center
- Current activities
- Reports
- Zero-day protection
- Diagnostics

PROTECT

- Rules and policies
- Intrusion prevention
- Web
- Applications
- Wireless
- Email
- Web server
- Active threat response

CONFIGURE

- Remote access VPN
- Site-to-site VPN
- Network
- Routing
- Authentication**
- System services

SYSTEM

- Sophos Central
- Profiles
- Hosts and services
- Administration
- Backup & firmware
- Certificates

Servers Services Groups Users Multi-factor authentication Web authentication Guest users

Server type: RADIUS server

Server name *: Useroam

Server IP *: 104.247.174.120

Authentication port *: 1812

Time-out *: 3

☐ Enable accounting

Accounting port:

Shared secret *:

Domain name: Enter Domain name

Group name attribute *: Filter-Id

☐ Enable additional settings

Test connection X

Username *: test1

Password *:

Test connection

Test connection Save Cancel

5 - Kimlik Do?rulama Önceli?i (Authentication Methods)

Sonra **Authentication > Services** menüsünden Useroam'u *Firewall Authentication Methods* kısmında en üste çekip, **Apply** butonuna basarak ayarları kaydediniz.

SOPHOS Fw

Search

MONITOR & ANALYZE
Control center
Current activities
Reports
Zero-day protection
Diagnostics

PROTECT
Rules and policies
Intrusion prevention
Web
Applications
Wireless
Email
Web server
Active threat response

CONFIGURE
Remote access VPN
Site-to-site VPN
Network
Routing
Authentication
System services

Authentication

Servers **Services** Groups

Firewall authentication methods

Authentication server list

type to search...

☒ Local
☒ Useroam

Selected authentication server

Useroam

Local

drag to change priority

Default group Open Group

Apply

User portal authentication methods

☒ Set authentication methods same as firewall

6 - Web Kimlik Do?rulama Ayarlar?

Ardından **Authentication > Web Authentication** menüsüne geçiniz. Burada **Sign Out User** kısmına gelerek, **When User is Inactive** seçeneğini işaretleyiniz.

Yan taraftaki **Traffic flow** kısmında ise 100 bytes için **1440 dk** (24 saate denk gelmektedir) olarak ayarlayınız; böylece bağlı her cihaz, 24 saat içinde en az 100 bytes veri yaptığı sürece oturumu Firewall'dan düşmeyecektir. İsterseniz bu süreyi kısaltabilirsiniz.

Son olarak **"Use insecure HTTP instead of HTTPS"** kutucuğunu seçerek ayarları kaydediniz.

SOPHOS

Search

MONITOR & ANALYZE

- Control center
- Current activities
- Reports
- Zero-day protection
- Diagnostics

PROTECT

- Rules and policies
- Intrusion prevention
- Web
- Applications
- Wireless
- Email
- Web server
- Active threat response

CONFIGURE

- Remote access VPN
- Site-to-site VPN
- Network
- Routing
- Authentication**
- System services

SYSTEM

- Sophos Central
- Profiles
- Hosts and services
- Administration
- Backup & firmware
- Certificates

Servers Services Groups Users Multi-factor authentication **Web authentication** Guest users Clientless

Authorize unauthenticated users for web access

If Active Directory (AD) SSO is configured

AD SSO mechanism

☐ NTLM only ☒ Kerberos & NTLM

If AD SSO fails, captive portal appears.

If AD SSO isn't configured

When unauthenticated user reaches a block page

☒ Show captive portal link

Captive portal behavior

☒ Show user portal link

☒ Show web page after sign-in

Open web page

☒ In new browser window

☐ In captive portal window

Web page

☒ Originally requested by user

☐ Custom

Sign out user

These options don't apply to Azure AD. Users are signed out based on the Azure AD token expiration time.

Traffic flow required to consider the user active

100 bytes in 140 minutes

☐ When captive portal page is closed or redirected

☒ When user is inactive

☐ Never

☒ Use insecure HTTP instead of HTTPS

Apply

7 - Captive Portal Tasarımın Entegrasyonu (Custom HTML)

Useroam > Sistem Ayarları > Template kısmından `<html>` kod satırı ile başlayan bölümün hepsini alarak, Sophos Firewall'daki **Authentication > Web Authentication > Captive portal appearance > Custom HTML** kısmına yapıştırınız ve kaydediniz.

Kurulum Dökümanı

Template

```
1 <html>
2 <head>
3 <meta http-equiv="Content-Type" content="text/html; charset=UTF-8" />
4 <meta name="viewport" content="width=device-width, initial-scale=1">
5 <meta http-equiv="X-UA-Compatible" content="IE=edge">
6 <link rel="shortcut icon" href="https://panel.useroam.com/sophos-cloud/img/favicon.ico">
7 <title>Useroam Captive Portal</title>
8 <link href="https://panel.useroam.com/sophos-cloud/css/Useroam.css" rel="stylesheet">
9 <!--[if lt IE 9]>
10 <script src="https://panel.useroam.com/sophos-cloud/js/html5shiv.js"></script>
11 <script src="https://panel.useroam.com/sophos-cloud/js/respond.min.js"></script>
12 <![endif]-->
13 </head>
14 <body>
15 <div class="container" id="login-block">
16 <div class="row">
17 <div class="col-sm-6 col-md-4 col-sm-offset-3 col-md-offset-4">
18 <div class="login-box clearfix animated flipInX">
19 <div class="login-logo"></div>
20 <div class="login-form">
```

Cihazı Sil

Servers Services Groups Users Multi-factor authentication **Web authentication**

☐ Use per-connection AD SSO authentication for multi-user hosts ⓘ

Multi-user hosts

Add new item

Apply

Captive portal appearance

Layout

☐ Default layout ☒ **Custom HTML**

Custom HTML must include a <div> element with id "loginbox", that is, <div id="loginbox">.

The required input elements are inserted into this div. You can customize these elements, using CSS and JavaScript.

Preview may not show the full result, since JavaScript code won't execute in the preview window.

```
<html>
<head>
<meta http-equiv="Content-Type" content="text/html; charset=UTF-8" />
<meta name="viewport" content="width=device-width, initial-scale=1">
<meta http-equiv="X-UA-Compatible" content="IE=edge">
<link rel="shortcut icon" href="https://panel.useroam.com/sophos-cloud/img/favicon.ico">
<title>Useroam Captive Portal</title>
<link href="https://panel.useroam.com/sophos-cloud/css/Useroam.css" rel="stylesheet">
<!--[if IE 9]>
<script src="https://panel.useroam.com/sophos-cloud/js/html5shiv.js"></script>
<script src="https://panel.useroam.com/sophos-cloud/js/respond.min.js"></script>
<![endif]-->
</head>
<body>
<div class="container" id="login-block">
<div class="row">
<div class="col-sm-6 col-md-4 col-sm-offset-3 col-md-offset-4">
<div class="login-box clearfix animated flipInX">
<div class="login-logo"></div>
<div class="login-form">
<div class="login-links" id="login-links">
</div>
<form action="#" id="cetus_form" method="POST" enctype="multipart/form-data">
```

Apply Preview >> Reset to default

Eşzamanlı Oturum Sınırlandırması: Bir hesabın birden fazla cihazda kullanılmasını sınırlandırmak istiyorsanız, Sophos Firewall altında **Configure > Authentication > Services > Global Settings** menüsünden düzenlemeyi yapabilirsiniz.

Sistem varsayılan olarak limitsiz cihaz ayarı ile gelmektedir.

SOPHOS FW

Search

MONITOR & ANALYZE

- Control center
- Current activities
- Reports
- Zero-day protection
- Diagnostics

PROTECT

- Rules and policies
- Intrusion prevention
- Web
- Applications
- Wireless
- Email
- Web server
- Active threat response

CONFIGURE

- Remote access VPN
- Site-to-site VPN
- Network
- Routing
- Authentication**
- System services

SYSTEM

- Sophos Central
- Profiles
- Hosts and services
- Administration
- Backup & firmware
- Certificates

Authentication

Servers Services Groups Users Multi-factor authentication

☒ Local
☐ Useroam

drag to change priority

Apply

Global settings

Maximum session time-out * ☒ Unlimited Minutes (between 3-1440)

Simultaneous logins * ☒ Unlimited (1-99)

Apply

AD SSO settings (NTLM and Kerberos)

Inactivity time 6 Minutes (between 6-1440)

Data transfer threshold 1024 bytes

HTTP challenge redirect on "Intranet zone" ☒ Enable

Apply

Firewall Kuralları Nasıl Oluşturulur?

Kuralları oluşturmak için önce Sophos Firewall altında **Protect > Rules and Policies** menüsünden **Add Firewall Rule** sayfasına geliniz.

KURAL 1: Guest to DNS

Tüm cihazlar, bağlandıkları ağda internet erişimi olup olmadığını anlamak için cihaza özel alan adına bir DNS sorgusu atar (Örn: `captive.apple.com`).

Bu sorgu sonucu gelince cihaz internet olduğunu anlayıp trafik akışını başlatır. Aksi takdirde hotspot yönlendirmesi yapılmayacaktır.

Bu kuralın misafirlerin internet çıkışı kuralının üstünde olması gerekiyor.

SOPHOS FW

Search

MONITOR & ANALYZE

Control center

Current activities

Reports

Zero-day protection

Diagnostics

PROTECT

Rules and policies

Intrusion prevention

Web

Applications

Wireless

Email

Web server

Active threat response

CONFIGURE

Remote access VPN

Site-to-site VPN

Network

Routing

Authentication

System services

SYSTEM

Sophos Central

Profiles

Hosts and services

Administration

Backup & firmware

Certificates

Add firewall rule

How-to guides Log viewer

☒ Rule status

Rule name *
GUEST TO DNS

Action
Accept

☒ Log firewall traffic
Log traffic, matching this firewall rule, on the appliance (by default) or on the configured syslog server.

Description
GUEST TO DNS

Rule position
Top

Rule group
GUEST

Source
Select the source zones, networks, and devices.
The rule applies to traffic from these sources during the scheduled time period.

Source zones *
GUEST
Add new item

Source networks and devices *
Any
Add new item

During scheduled time
All the time
Select to apply the rule to a specific time period and day of the week.

Destination and services
Select the destination zones, networks, devices, and services.
The rule applies to traffic to these destinations.

Destination zones *
WAN
Add new item

Destination networks *
Any
Add new item

Services *
DNS
Add new item
Services are traffic types based on a combination of protocols and ports.

KURAL 2: Guest to Useroam

Bu kural ile misafir ağındaki cihazların *.useroam.com'a erişmesini sağlayacaksınız.

Bunun için Services kısmında **HTTP/HTTPS** seçmeniz yeterli olacaktır.

SOPHOS FW

Search

MONITOR & ANALYZE

Control center

Current activities

Reports

Zero-day protection

Diagnostics

PROTECT

Rules and policies

Intrusion prevention

Web

Applications

Wireless

Email

Web server

Active threat response

CONFIGURE

Remote access VPN

Site-to-site VPN

Network

Routing

Authentication

System services

SYSTEM

Sophos Central

Profiles

Hosts and services

Administration

Backup & firmware

Certificates

Edit firewall rule

How-to guides Log viewer

☒ Rule status

Rule name *
GUEST TO USEROAM

Action
Accept

☒ Log firewall traffic
Log traffic, matching this firewall rule, on the appliance (by default) or on the configured syslog server.

Description
GUEST TO USEROAM

Rule group
GUEST

Source
Select the source zones, networks, and devices.
The rule applies to traffic from these sources during the scheduled time period.

Source zones *
GUEST
Add new item

Source networks and devices *
Any
Add new item

During scheduled time
All the time
Select to apply the rule to a specific time period and day of the week.

Destination and services
Select the destination zones, networks, devices, and services.
The rule applies to traffic to these destinations.

Destination zones *
WAN
Add new item

Destination networks *
panel.useroam.com
Add new item

Services *
HTTP
HTTPS
Add new item
Services are traffic types based on a combination of protocols and ports.

☐ Match known users

KURAL 3: Guest to Internet

Bu kuralda cihazlarınızın internet erişimi sağlanacak.

Log Firewall kutucuğunu seçiniz. Tanımsız kullanıcılara Hotspot ekranı gelmesi için **Match Known Users** ve **Use Web Authentication For Unknown Users** kutucuklarını da seçiniz. Web Policy ve Identify And Control Applications (App Control) kısımlarında *Allow All* ya da herhangi bir politika seçiniz.

MONITOR & ANALYZE

- Control center
- Current activities
- Reports
- Zero-day protection
- Diagnostics

PROTECT

- Rules and policies**
- Intrusion prevention
- Web
- Applications
- Wireless
- Email
- Web server
- Active threat response

CONFIGURE

- Remote access VPN
- Site-to-site VPN
- Network
- Routing
- Authentication
- System services

SYSTEM

- Sophos Central
- Profiles
- Hosts and services
- Administration
- Backup & firmware
- Certificates

Web server

- Active threat response

CONFIGURE

- Remote access VPN
- Site-to-site VPN
- Network
- Routing
- Authentication
- System services

SYSTEM

- Sophos Central
- Profiles
- Hosts and services
- Administration
- Backup & firmware
- Certificates

Rule status

Rule name *
GUEST TO INTERNET

Action
Accept

☒ Log firewall traffic
Log traffic, matching this firewall rule, on the appliance (by default) or on the configured syslog server.

Description
GUEST TO INTERNET

Rule position
Bottom

Rule group
GUEST

Source

Select the source zones, networks, and devices.
The rule applies to traffic from these sources during the scheduled time period.

Source zones *
GUEST

Source networks and devices *
Any

During scheduled time
All the time

Destination and services

Select the destination zones, networks, devices, and services.
The rule applies to traffic to these destinations.

Destination zones *
WAN

Destination networks *
Any

Services *
Any

☒ Match known users

☒ Use web authentication for unknown users

User or groups *
Any

☐ Exclude this user activity from data accounting

Security features

Web filtering

Web policy
Allow All

☐ Apply web category-based traffic shaping

☒ Block QUIC protocol

Malware and content scanning

☐ Scan HTTP and decrypted HTTPS

☐ Use zero-day protection

☐ Scan FTP for malware

Filtering common web ports

☐ Use web proxy instead of DPI engine

☒ DPI engine or web proxy?

Web proxy options

☐ Decrypt HTTPS during web proxy filtering

Configure Synchronized Security Heartbeat

Other security features

Identify and control applications (App control)

Allow All

☐ Apply application-based traffic shaping policy

Detect and prevent exploits (IPS)

None

Scan email content

Shape traffic
User's policy applied

DSCP marking
Select DSCP marking

İşlemler sonucunda **Protect > Rules and Policies** menüsü sıralaması görseldeki gibi görünmelidir. [cite: 566]

SOPHOS Firewall

Rules and policies

Firewall rules NAT rules

IPv4 IPv6 Disable filter Test your policies

Rule type Source zone Destination zone Status Rule ID Add Filter

#	Name	Source	Destination	What
1	GUEST TO DNS in 0 B, out 0 B	GUEST, Any host	WAN, Any host	DNS
2	GUEST TO USEROAM in 0 B, out 0 B	GUEST, Any host	WAN, panel.useroam.com	HTTP, HTTPS
3	GUEST TO INTERNET in 0 B, out 0 B	GUEST, Any host, Any live user...	WAN, Any host	Any service

Loglar?n Useroam Cihaz?na Yönlendirilmesi

1 - Syslog Server Tan?mlama

Öncelikle **System Services > Log Settings** menüsüne gelerek yeni bir Syslog server tanımlayınız.

SOPHOS Firewall

System services

High availability Traffic shaping settings RED Malware protection Log settings

Name * Useroam Cloud

IP address / Domain * panel.useroam.com

Secure log transmission ☐

Port * 514

Facility * DAEMON

Severity level * Information

Format * Standard syslog protocol

2 - Syslog Detaylar?n? Girme ve Ba?latma

Yeni eklenen syslog server için aşağıdaki bilgileri doldurunuz: [cite: 644]

- **Name:** Useroam Cloud [cite: 646]
- **IP address / Domain:** 104.247.174.120 [cite: 647]
- **Port:** 514 [cite: 654]
- **Facility:** DAEMON [cite: 655]
- **Severity level:** Debug [cite: 656]
- **Format:** Standard syslog protocol [cite: 657]

Name *	UseroamCloud
IP address / Domain *	104.247.174.120
Secure log transmission	☐
Port *	514
Facility *	DAEMON
Severity level *	Debug
Format *	Standard syslog protocol

Daha sonra yeni eklenen syslog server satırında sadece **Content Filtering** alanlarını seçerek loglamayı Useroam'a doğru başlatınız.

SOPHOS
Search
MONITOR & ANALYZE
Control center
Current activities
Reports
Zero-day protection
Diagnostics
PROTECT
Rules and policies
Intrusion prevention
Web
Applications
Wireless
Email
Web server
Active threat response
CONFIGURE
Remote access VPN
Site-to-site VPN
Network
Routing
Authentication
System services
SYSTEM
Sophos Central
Profiles
Hosts and services
Administration
Backup & firmware
Certificates

Feedback How-to guides Log viewer Help GLOX TEKNO

High availability	Traffic shaping settings	RED	Malware protection	Log settings	Notification list	Data anonymization	Traffic shaping
Anti-spam	☐	☐	☐	☐		☐	
SMTP		☒	☐	☐		☐	
POP3		☒	☐	☐		☐	
IMAP		☒	☐	☐		☐	
SMTPS		☒	☐	☐		☐	
POPS		☒	☐	☐		☐	
IMAPS		☒	☐	☐		☐	
Content filtering	☐	☐	☐	☐		☒	
Web filter		☒	☐	☐		☒	
Application filter		☒	☐	☐		☒	
Web content policy		☒	☐	☐		☒	
SSL/TLS filter		☒	☐	☐		☒	
Events	☐	☐	☐	☐		☐	
Admin events		☒	☐	☐		☐	
Authentication events		☒	☐	☐		☐	
System events		☒	☐	☐		☐	
Web server protection	☐	☐	☐	☐		☐	
Web server protection events		☒	☐	☐		☐	
Active threat response	☐	☐	☐	☐		☐	

3 - Log Paket Kontrolü

Bu işlem sonrasında Firewall'dan paketlerinizin gelip gelmediğini anlamak için Useroam paneline dönünüz.

Sağ üst köşedeki **Genel İstatistik** kısmını kontrol edip, **İmzalama Bekleyen** alanının altındaki kısmı kontrol ediniz.



Revizyon #5

tugay tarafından 6 Temmuz 2026 08:25:14 oluşturuldu

tugay tarafından 6 Temmuz 2026 12:55:20 güncellendi