

epati

Kimlik Saęlayıcı Tanımları

Ürün: Antikor v2 - Yeni Nesil Güvenlik Duvarı
Kılavuzlar

Kimlik Sağlayıcı Tanımları

Kimlik doğrulama için açılan kullanıcılara ek olarak, harici sistemler üzerinden de kimlik doğrulaması yapılabilmektedir.

Kimlik Sağlayıcı Tanımları Yenile Ekle

#	Durum	Sağlayıcı Türü	Adı	Etki Alanı	Sunucu Adresi	Açıklama	İşlemler
1	Aktif	Yerel Gruplar	Sw_Radius Kullanıcıları				Düzenle Sil
2	Aktif	Yerel Gruplar	Proxy Kullanıcıları				Düzenle Sil
3	Aktif	SMS	TELSAM			SMS Kayıt	Düzenle Sil
4	Aktif	Yerel Gruplar	L2TP Kullanıcıları				Düzenle Sil
5	Aktif	RADIUS	radtest		10.10.255.254		Düzenle Sil
6	Aktif	Yerel Gruplar	SSL VPN Kullanıcıları				Düzenle Sil
7	Aktif	RADIUS	SwitchYonetimradius		10.0.255.254/16		Düzenle Sil
8	Aktif	LDAP	Edurom Ldap	eskimail.mersin.edu.tr	192.168.254.3	Edurom LDAP	Düzenle Sil
9	Aktif	Yerel Gruplar	İdare				Düzenle Sil
10	Aktif	POP3/IMAP	Mersin Üniv. Pop sunucusu	mersin.edu.tr	192.168.254.3		Düzenle Sil

< > 1 < > Get

Yeni Kayıt

Kimlik Sağlayıcı Tanımları - Yeni Kayıt

Durum

Aktif

Sağlayıcı Türü

Seçiniz...

İptal

Kaydet

ALAN	AÇIKLAMA
Durum	Aktif ya da pasif olma durumu seçilir.
Sağlayıcı Türü	Kimlik sağlayıcı türlerinden biri seçilir.

HTTP(s) API - (Raw, JSON, XML, REST)

Durum	<input checked="" type="checkbox"/> Aktif
Sağlayıcı Türü	http(s) API - (Raw, JSON, XML, REST) ▾
Kullanılacak Arayüz	Management ▾
Adı	<input type="text"/>
Etki Alanı	<input type="text"/>
Sunucu Adresi	<input type="text"/>
Metod	▾
Karakter Seti	▾
	<input type="checkbox"/> MDS
Gönderilen Bilgiler	<input type="text"/>
Başlıklar	Anahtar <input type="text"/> Değer <input type="text"/>
Değişkenler	Anahtar <input type="text"/> Değer <input type="text"/>
Doğrulama Türü	▾
Doğrulama Kullanıcı Adı	<input type="text"/>
Doğrulama Şifre	<input type="text"/>
Kullanıcı Adı Değişkeni	<input type="text"/>
Kullanıcı Şifre Değişkeni	<input type="text"/>
Gelen Bilgiler	<input type="text"/>
Başarılı Cevap Kodu	<input type="text"/>
Açıklama	<input type="text"/>

[İptal](#)[Kaydet](#)

ALAN	AÇIKLAMA
Kullanılacak Arayüz	Kullanılacak arayüz seçilir.
Adı	HTTP (Api) adı girilir.
Etki Alanı	HTTP (Api) a ait etki alanı girilir.
Sunucu adresi	HTTP (Api) sunucu adresi girilir.
Metod	Hangi metod ile haberleşileceği seçilir.
Karakter Seti	Kullanılacak olan karakter seti seçilir.
MD5	MD5 kullanılıp kullanılmadığı seçilir.
Gönderilen Bilgiler	Gönderilen bilgiler girilir.
Başlıklar	
Anahtar	Başlıklara ait anahtar ve değer girilir.
Değer	Başlıklara ait anahtar ve değer girilir.
Değişkenler	
Anahtar	Değişkenlere ait anahtar ve değer girilir.
Değer	Değişkenlere ait anahtar ve değer girilir.
Doğrulama Türü	—
Doğrulama Kullanıcı Adı	—
Doğrulama Şifre	—
Kullanıcı Adı Değişkeni	—
Kullanıcı Şifre Değişkeni	—
Gelen Bilgiler	—
Başarılı Cevap Kodu	—
Açıklama	Açıklama girilir.

HTTP(s) Authentication (Basic, Digest)

Kurumda mevcut olan otomasyonlar ile kimlik doğrulaması yapabilmek için HTTP Web Servis entegrasyonu yapılabilir.

Entegrasyon süreci için, kullanılan otomasyona antiKor'a uygun bir web servisi eklenmesi gerekmektedir.

Web servis entegrasyonu için teknik destek ekibimizden yardım alınabilir.

Durum	<input checked="" type="checkbox"/> Aktif
Sağlayıcı Türü	http(s) Authentication (Basic, Digest) ▼
Kullanılacak Arayüz	Management ▼
Adı	<input type="text"/>
	<input type="checkbox"/> Kullanıcı ve Etki Alanı birlikte
Etki Alanı	<input type="text"/>
Sunucu Adresi	<input type="text"/>
	<input type="checkbox"/> MD5
Doğrulama Türü	▼
Doğrulama Kullanıcı Adı	Bu alan sadece Basic ve Digest doğrulama türleri için geçerlidir.
Doğrulama Şifre	Bu alan sadece Basic ve Digest doğrulama türleri için geçerlidir.
Kullanıcı Adı Değişkeni	<input type="text"/>
Kullanıcı Şifre Değişkeni	<input type="text"/>
Başarılı Cevap Kodu	<input type="text"/>
Açıklama	<input type="text"/>

İptal

Kaydet

ALAN	AÇIKLAMA
Kullanılacak Arayüz	Kullanılacak arayüz seçilir.
Adı	Kullanılacak olan HTTP adı girilir.
Etki Alanı	Etki alanı girilir.
Sunucu adresi	Sunucuya ait adres girilir.
MD5	MD5 kullanılıp kullanılmadığı seçilir.
Doğrulama Türü	Basic veya Digest türü seçilir.
Doğrulama Kullanıcı Adı	—
Doğrulama Şifre	—
Kullanıcı Adı Değişkeni	—
Kullanıcı Şifre Değişkeni	—
Başarılı Cevap Kodu	—
Açıklama	Açıklama girilir.

LDAP

LDAP veya Active Directory kullanıcıları kolaylıkla entegre edilebilir.

LDAP Sunucu Adresi bölümüne sunucunun IP adresini girdikten sonra, LDAP Base DN alanı güncellenmelidir.

Kimlik Sağlayıcı Tanımları - Yeni Kayıt

×

Durum	<input checked="" type="checkbox"/> Aktif
Sağlayıcı Türü	LDAP
Kullanılacak Arayüz	Management
Adı	<input type="text"/>
	<input type="checkbox"/> Kullanıcı ve Etki Alanı birlikte
Etki Alanı	<input type="text"/>
Sunucu Adresi	<input type="text"/>
BaseDn	<input type="text"/>
Açıklama	<input type="text"/>

İptal

Kaydet

ALAN	AÇIKLAMA
Kullanılacak Arayüz	Kullanılacak arayüz seçilir.
Adı	LDAP adı girilir.
Etki Alanı	LDAP'a ait etki alanı girilir.
Sunucu adresi	LDAP sunucu adresi girilir.
BaseDn	LDAP da bulunan BaseDn girilir.
Açıklama	Açıklama girilir.

RADIUS

RADIUS sunucusu ile entegrasyonu kolayca yapılabilir, hatta EDUROAM ile de entegre edilebilmektedir.

antiKor'un kendi üzerindeki EDUROAM Servisi ile entegre etmek için Sunucu Adresi olarak 127.0.0.1 girilmelidir.

EDUROAM ayarlarında, NAS tanımları bölümünde 127.0.0.1 IP si de tanımlı olmalıdır.

Durum	<input checked="" type="checkbox"/> Aktif
Sağlayıcı Türü	RADIUS
Kullanılacak Arayüz	Management
Adı	
Kapsülleme	
	<input type="checkbox"/> Kullanıcı ve Etki Alanı birlikte
Etki Alanı	
Sunucu Adresi	
Gizli Anahtar	
Zaman Aşımı	
Azami Deneme Sayısı	
Açıklama	

İptal

Kaydet

ALAN	AÇIKLAMA
Kullanılacak Arayüz	Kullanılacak arayüz seçilir.
Adı	RADIUS adı girilir
Kapsülleme	Kapsülleme seçilir.
Etki Alanı	RADIUS'a ait etki alanı girilir.
Sunucu adresi	RADIUS sunucu adresi girilir.
Gizli Anahtar	RADIUS'a ait gizli anahtar girilir.
Zaman Aşımı	Zaman aşımının ne kadar olacağı belirlenir.
Azami Deneme Sayısı	Maksimum deneme sayısı yazılır.
Açıklama	Açıklama girilir.

POP3 - IMAP

Kuruma/kuruluşa ait e-posta sunucusu ile entegrasyonunu sağlamak için alan adı, mail sunucu IP adresi ve protokol bilgilerinin forma girilmesi gerekmektedir.

Durum	<input checked="" type="checkbox"/> Aktif
Sağlayıcı Türü	POP3/IMAP
Kullanılacak Arayüz	Management
Adı	<input type="text"/>
	<input type="checkbox"/> Kullanıcı ve Etki Alanı birlikte
Etki Alanı	<input type="text"/>
Sunucu Adresi	<input type="text"/>
Protokol	<input type="text"/>
Port	<input type="text"/>
Deneme Sayısı	<input type="text"/>
	<input type="checkbox"/> SSL
	<input type="checkbox"/> TLS
Açıklama	<input type="text"/>

İptal

Kaydet

ALAN	AÇIKLAMA
Kullanılacak Arayüz	Kullanılacak arayüz seçilir.
Adı	POP3 / IMAP adı girilir.
Etki Alanı	POP3 / IMAP a ait etki alanı girilir.
Sunucu adresi	POP3 / IMAP sunucu adresi girilir.
Protokol	POP3 / IMAP protokollerinden hangisi kullanılacaksa seçilir.
Port	POP3 / IMAP kullandığı port numarası yazılır.
Deneme Sayısı	Maksimum deneme sayısı yazılır.
SSL	SSL kullanılıp kullanılmadığı seçilir.
TLS	TLS kullanılıp kullanılmadığı seçilir.
Açıklama	Açıklama girilir.

SMS

Durum

Aktif

Sağlayıcı Türü

SMS

SMS Ayarları

Mesaj Ön Metni

Açıklama

İptal

Kaydet

ALAN	AÇIKLAMA
SMS Ayarları	Bildirim yönetimi - Bildirim Sağlayıcı Tanımları (SMS, E-posta) bölümünde tanımlanmış olan sms ayarlarından biri seçilir.
Mesaj Ön Metni	Mesaj ön metni yazılır.
Açıklama	Açıklama yazılır.

Yerel Gruplar

Durum

Aktif

Sağlayıcı Türü

Yerel Gruplar

Adı

Açıklama

Yetkili Kullanıcı

Seçiniz...

İptal

Kaydet

ALAN	AÇIKLAMA
Adı	Kullanılacak olan yerel grubun adı yazılır.
Açıklama	Açıklama yazılır.
Yetkili Kullanıcı	AntiKor NGFW'da tanımlı olan sistem kullanıcılardan, yerel kullanıcılar bölümünde kullanıcı eklemesine izin verilecek olan sistem kullanıcı(ları)sı seçilir.

SSO: Negotiate/Kerberos - Active Directory

Durum

Aktif

Sağlayıcı Türü

SSO: Negotiate/Kerberos - Active Directory



Domain Controller / Kerberos Key Distribution Center ile saat uyumsuzluğu halinde Tek Oturum Açma (SSO) başarısız olabilir. Lütfen Tarih Saat Ayarları menüsünden NTP senkronizasyonu yapıldığından emin olun.

Etki Alanı

KDC / DC DNS Adı

Antikora atanan DNS Adı

Açıklama

İptal

Kaydet

ALAN	AÇIKLAMA
Etki Alanı	Etki alanı bilgisi girilir.
KDC/DC DNS Adı	KDC/DC DNS Adı bilgisi girilir.
Antikora atanan DNS Adı	Antikora atanan DNS Adı bilgisi girilir.
Açıklama	Açıklama yazılır.

TACACS+

TACACS+ (Terminal erişim denetleyicisi Erişim Kontrol Sistemi) radius benzeri bir kimlik doğrulama ve yetkilendirme sunucusudur. TACACS+ iletim kontrol protokolünü (TCP) kullanmaktadır. RADIUS ise Datagram protokolünü (UDP) kullanmaktadır.

Durum	<input checked="" type="checkbox"/> Aktif
Sağlayıcı Türü	TACACS+ ▼
Kullanılacak Arayüz	Management ▼
Adı	<input type="text"/>
	<input type="checkbox"/> Kullanıcı ve Etki Alanı birlikte
Etki Alanı	<input type="text"/>
Sunucu Adresi	<input type="text"/>
Gizli Anahtar	<input type="text"/>
Açıklama	<input type="text"/>

[İptal](#)[Kaydet](#)

ALAN	AÇIKLAMA
Kullanılacak Arayüz	Kullanılacak arayüz seçilir.
Adı	TACACS+ adı girilir.
Etki Alanı	TACACS+ sunucusuna ait etki alanı girilir.
Sunucu adresi	TACACS+ sunucu adresi girilir.
Gizli Anahtar	TACACS+ ait gizli anahtar girilir. Şifreyi gösterme seçeneği mevcuttur.
Açıklama	Açıklama girilir.

