TREND MICRO

9.0 Worry-Free™ Business Security Standard ve Advanced Sürümler Service Pack 2

Yönetici Kılavuzu

Securing Your Journey to the Cloud

Korumalı Bulut

Ağ Güvenliği

Trend Micro Incorporated bu belgede ve burada açıklanan ürün'e haber vermeden değişiklik yapma hakkını saklı tutar. ürün yüklemeden ve kullanmadan önce, lütfen benioku dosyalarını, sürüm notlarını ve Trend Microç web sitesinden temin edilebilen geçerli kullanıcı belgelerinin aşağıdaki adresteki en son sürümünü gözden geçirin:

http://docs.trendmicro.com/tr-tr/smb/worry-free-business-security.aspx

Trend Micro, Trend Micro t-ball logosu, TrendProtect, TrendSecure, Worry-Free, OfficeScan, ServerProtect, PC-cillin, InterScan ve ScanMail Trend Micro Incorporated ticari markaları veya tescilli ticari markalarıdır. Tüm diğer ürünler veya şirket adları, kendi sahiplerinin ticari markaları veya tescilli ticari markaları olabilir.

Telif Hakkı © 2015. Trend Micro Incorporated. Her hakkı saklıdır.

Belge Kısım No.: WFUM97097/150730

Çıkış Tarihi: Ağustos 2015

Şu numaralı ABD Patentleri kapsamında korunmaktadır: 5,951,698 ve 7,188,369

Bu belge ürün için ana özelliklerini ve/veya üretim ortamınız için yükleme yönergelerini açıklamayı amaçlar. ürün yüklemeden veya kullanmadan önce belgeleri dikkatle okuyun.

ürün için belirli özelliklerin kullanımına ilişkin ayrıntılı bilgi, Trend Micro web sitesinde Çevrimiçi Yardım Merkezi'nde ve/veya Trend Micro Bilgi Bankası'nda mevcuttur.

Trend Micro her zaman belgelerini iyileştirmek için çalışmaktadır. Bu veya herhangi bir Trend Micro belgesi hakkında soru, yorum veya önerileriniz olursa, lütfen docs@trendmicro.com adresinden bize ulaşın.

Bu belgeyi lütfen aşağıdaki adreste değerlendirin:

http://www.trendmicro.com/download/documentation/rating.asp

İçindekiler Tablosu

Önsöz

Önsöz xi

Worry-Free Business Security Belgeleri xii

Hedef Kitle xii

Belge Kuralları xiii

Bölüm 1: Worry-Free Business Security Standard ve Advanced Tanıtımı

Trend Micro Worry-Free Business Security'e Genel Bakış 1-2

Bu Sürümde Yeni (WFBS 9.0 SP2) 1-2

- WFBS 9.0 SP1'deki Yenilikler 1-7
- WFBS 9.0'daki Yenilikler 1-16

Önemli Özellikleri ve Faydaları 1-18

- Trend Micro Smart Protection Network 1-19
- File Reputation Hizmetleri 1-19
- Web Reputation Hizmetleri 1-19
- Email Reputation (Yalnızca Advanced) 1-20
- Smart Feedback 1-21
- URL Filtreleme 1-22

Korumanın Yararları 1-22

Tehditleri Anlama 1-23

- Virüsler ve Kötü Amaçlı Yazılımlar 1-23
- Casus Yazılım ve Grayware 1-25
- Spam 1-26
- İzinsiz girişler 1-26
- Kötü Amaçlı Davranış 1-26
- Sahte Erişim Noktaları 1-27
- Kimlik Avı Olayları 1-27
- Toplu Posta Saldırıları 1-27
- Web Tehditleri 1-28

Bölüm 2: Başlarken

Worry-Free Business Security Network 2-2

Security Server 2-2
Tarama Sunucusu 2-2

Aracılar 2-3

Web Konsolu 2-4
Web Konsolunu Açma 2-5
Web Konsolunda Gezinme 2-7
Web Konsolu Simgeleri 2-10
Canlı Durum 2-11

Bölüm 3: Aracıları Yükleme

Security Agent Yüklemesi 3-2
Security Agent Yükleme Gereksinimleri 3-2
Security Agent Yükleme Hususları 3-2
Kullanılabilir Security Agent Özellikleri 3-3
Security Agent Yüklemesi ve IPv6 Desteği 3-7

Security Agent Yükleme Yöntemleri 3-9
Dahili Web Sayfasından Yükleme 3-12
Oturum Açma Komut Dizesi Kurulumu ile Yükleme 3-14
Client Packager ile Yükleme 3-16
Uzaktan Yükleme ile Yükleme 3-19
Güvenlik Açığı Tarayıcısıyla Yükleme 3-23
E-posta Bildirimiyle Yükleme 3-33
Security Agent'a Geçme 3-34
Security Agent'larda Yükleme Sonrası Görevleri Gerçekleştirme 3-35

Messaging Security Agent Yükleme 3-37
Messaging Security Agent Yükleme Gereksinimleri 3-37
Messaging Security Agent'ı Yükleme (Yalnızca Advanced) 3-37

Aracıları Kaldırma 3-39
Aracıları Web Konsolundan Kaldırma 3-40
Aracıları Web Konsolundan Kaldırma 3-41
İstemciden Security Agent'ı Kaldırma 3-42
SA Kaldırma Aracını Kullanma 3-43

Microsoft Exchange Server'dan Messaging Security Agent'ı Kaldırma (Yalnızca Advanced) 3-45

Bölüm 4: Grupları Yönetme

Gruplar 4-2

Grup Ekleme 4-10

Gruplara Aracı Ekleme 4-11

Aracıları Taşıma 4-12
- Gruplar Arasında Security Agent'ları Taşıma 4-13
- Web Konsolunu Kullanarak Security Server'lar Arasında Aracıları Taşıma 4-14
- Client Mover Kullanarak Security Server'lar Arasında bir Security Agent'ı Taşıma 4-15

Ayarları Çoğaltma 4-17
- Security Agent Grup Ayarlarını Çoğaltma 4-17
- Messaging Security Agent Ayarlarını Çoğaltma (Yalnızca Advanced) 4-18

Security Agent Gruplarının Ayarlarını İçe ve Dışa Aktarma 4-19
- Ayarları Dışa Aktarma 4-21
- Ayarları İçe Aktarma 4-22

Bölüm 5: Security Agent için Temel Güvenlik Ayarlarını Yönetme

Security Agent için Temel Güvenlik Ayarlarının Özeti 5-2

Tarama Yöntemleri 5-3
- Tarama Yöntemlerini Yapılandırma 5-5

Security Agent'lar için Gerçek Zamanlı Tarama 5-7
- Security Agent'lar için Gerçek Zamanlı Tarama Yapılandırma 5-7

Güvenlik Duvarı 5-8
- Güvenlik Duvarını Yapılandırma 5-10
- Güvenlik Duvarı Kural Dışı Durumlarıyla Çalışma 5-12
- Bir Agent Grubu Üzerindeki Güvenlik Duvarını Devre Dışı Bırakma 5-14

Tüm Aracılar Üzerindeki Güvenlik Duvarını Devre Dışı Bırakma 5-15

Web Reputation 5-15
Security Agent'lar için Web Reputation Yapılandırma 5-17

URL Filtreleme 5-18
URL Filtrelemeyi Yapılandırma 5-18

Onaylanmış/Engellenmiş URL'ler 5-19
Onaylanmış/Engellenmiş URL'leri Yapılandırma 5-19

Behavior Monitoring 5-20
Behavior Monitoring'i Yapılandırma 5-21

Güvenilen Program 5-24
Güvenilen Program Yapılandırma 5-24

Cihaz Denetimi 5-25
Aygıt Denetimini Yapılandırma 5-25

Kullanıcı Araçları 5-27
Kullanıcı Araçlarını Yapılandırma 5-27

İstemci Ayrıcalıkları 5-28
Aracı Ayrıcalıklarını Yapılandırma 5-28

Karantina Dizini 5-30
Karantina Dizinini Yapılandırma 5-33

Bölüm 6: Messaging Security Agent için Temel Güvenlik Ayarlarını Yönetme (Yalnızca Advanced)

Messaging Security Agent'lar 6-2
Messaging Security Agent E-Posta İletilerini Nasıl Tarar 6-3
Varsayılan Messaging Security Agent Ayarları 6-4

Messaging Security Agent'lar için Gerçek Zamanlı Tarama 6-5
Messaging Security Agent'lar için Gerçek Zamanlı Tarama Yapılandırma 6-5

İstenmeyen e-postadan koruma 6-6
Email Reputation 6-7
İçerik Taraması 6-9

İçerik Filtreleme 6-14
İçerik Filtreleme Kurallarını Yönetme 6-15
İçerik Filtreleme Kurallarının Türleri 6-19
Tüm Eşleşme Koşulları için bir İçerik Filtreleme Kuralı Ekleme . 6-20
Herhangi bir Eşleşme Koşulu için bir İçerik Filtreleme Kuralı Ekleme 6-23
İçerik Filtreleme İzleme Kuralı Ekleme 6-25
İçerik Filtreleme Kurallarına Kural Dışı Durumlar Oluşturma 6-28

Veri Kaybını Önleme 6-29
Ön Çalışma 6-30
Veri Kaybını Önleme Kurallarını Yönetme 6-30
Varsayılan Veri Kaybını Önleme Kuralları 6-38
Veri Kaybını Önleme Kuralları Ekleme 6-39

Ek Engelleme 6-44
Ek Engellemeyi Yapılandırma 6-45

Web Reputation 6-47
Messaging Security Agent'lar için Web Reputation Yapılandırma 6-49

Mobil Güvenlik 6-51
Mobil Güvenlik Desteği 6-51
Aygıt Erişim Denetimini Yapılandırma 6-52
Bekleyen Aygıt Silmeyi İptal Etme 6-53
Aygıtları Manuel Olarak Silme 6-54
Güvenlik İlkelerini Yapılandırma 6-55

Messaging Security Agent'lar için Karantina 6-60
Karantina Dizinlerini Sorgulama 6-61
Sorgu Sonuçlarını Alma ve Eyleme Geçme 6-63
Karantina Dizinlerinin Bakımı 6-64
Karantina Dizinlerini Yapılandırma 6-65

Messaging Security Agent'lar için Bildirim Ayarları 6-67
Messaging Security Agent'lar için Bildirim Ayarlarını Yapılandırma 6-68

Spam Bakımını Yapılandırma 6-68
Son Kullanıcı Karantinasını Yönetme 6-70

Trend Micro Destek/Hata Ayıklayıcı 6-72
Sistem Hata Ayıklayıcı Raporları Oluşturma 6-72

Gerçek Zamanlı İzleme 6-73
Gerçek Zamanlı İzleme ile Çalışma 6-74
Giden E-posta İletilerine Feragatname Ekleme 6-74

Bölüm 7: Taramaları Yönetme

Taramalar Hakkında 7-2
Gerçek Zamanlı Tarama 7-2
Manuel Tarama 7-3
Manuel Taramaları Çalıştırma 7-3
Zamanlanmış Tarama 7-6
Zamanlanmış Taramaları Yapılandırma 7-6
Security Agent'lar için Tarama Hedefleri ve Eylemler 7-9
Tarama Hedefleri ve Messaging Security Agent'lar için Eylemler 7-17

Bölüm 8: Güncellemeleri Yönetme

Güncellemeye Genel Bakış 8-2
Güncellenebilir Bileşenler 8-3
Düzeltmeler, Yamalar ve Hizmet Paketleri 8-10
Security Server Güncellemeleri 8-10
Security Server Güncelleme Kaynağını Yapılandırılma 8-12
Security Server'ı Manuel Olarak Güncelleme 8-13
Security Server için Planlı Güncellemeleri Yapılandırma 8-14
Bileşenleri Geri Alma 8-15
Security Agent ve Messaging Security Agent Güncellemeleri 8-16
Otomatik Güncellemeler 8-16
Manuel Güncellemeler 8-16
Aracı Güncelleme Hatırlatmaları ve İpuçları 8-16
Güncelleme Aracıları 8-17
Güncelleme Aracılarını Yapılandırma 8-20

Bölüm 9: Bildirimleri Yönetme

Bildirimler 9-2

Bildirimler için Olayları Yapılandırma 9-3
Sembol Değişkenleri 9-4

Bölüm 10: Salgın Savunmasını Kullanma

Salgın Savunması Stratejisi 10-2
Salgın Savunmasını Yapılandırma 10-2
Salgın Savunması Mevcut Durumu 10-3

Güvenlik Açığı Değerlendirmesi 10-4
Güvenlik Açığı Değerlendirmesini Yapılandırma 10-5
Talep Üzerine Güvenlik Açığı Değerlendirmelerinin Çalıştırılması 10-6

Hasar Temizleme 10-6
Talep Üzerine Temizlemenin Çalıştırılması 10-7

Bölüm 11: Genel Ayarları Yönetme

Genel Ayarlar 11-2

Internet Proxy Ayarlarını Yapılandırma 11-3

SMTP Sunucusu Ayarlarını Yapılandırma 11-4

Masaüstü/Sunucu Ayarlarını Yapılandırma 11-5

Sistem Ayarlarını Yapılandırma 11-10

Bölüm 12: Günlükleri ve Raporları Kullanma

Günlükler 12-2
Günlük Sorgusu Kullanma 12-4

Raporlar 12-5
Tek Seferlik Raporlarla Çalışma 12-5
Zamanlanmış Raporlarla Çalışma 12-7
Raporları Yorumlama 12-11

Raporlar ve Günlükler için Bakım Görevlerini Gerçekleştirme 12-14

Bölüm 13: Yönetici Görevlerinin Gerçekleştirilmesi

Web Konsolu Parolasını Değiştirme 13-2

Plug-in Manager ile Çalışma 13-2
Ürün Lisansını Yönetme 13-3
Smart Feedback Program'ına Katılma 13-5
Aracı Arayüzü Dilini Değiştirme 13-5
Program Ayarlarını Kaydetme ve Geri Yükleme 13-6
Security Server'ı Kaldırma 13-8

Bölüm 14: Yönetim Araçlarını Kullanma

Araç Türleri 14-2
Trend Micro Remote Manager Agent'ı Yükleme 14-3
Disk Alanı Kazanma 14-5
Security Server üzerinde Disk Temizleyiciyi Çalıştırma 14-6
Komut Satırı Arayüzünü Kullanarak Security Server Üzerinde Disk Temizleyiciyi Çalıştırma 14-7
İstemciler üzerinde Disk Alanı Kazanma 14-8
Scan Server Veritabanının Taşınması 14-8
Şifrelenmiş Dosyaları Geri Yükleme 14-9
Security Agent üzerindeki Dosyaların Şifresinin Açılması ve Geri Yüklenmesi 14-10
Security Server üzerindeki Dosyaların Şifresini Açma ve Geri Yükleme, Özel Karantina Dizini veya Messaging Security Agent Transport Neutral Encapsulation Format E-Posta İletilerinin Geri Yüklenmesi 14-11 14-13
ReGenID Aracını Kullanma 14-13
SBS ve EBS Eklentilerini Yönetme 14-14
SBS ve EBS Eklentilerini Manuel Yükleme 14-14
SBS veya EBS Eklentilerini Kullanma 14-15

Ek A: Security Agent Simgeleri

Security Agent Durumunu Kontrol Etme A-2
Windows Görev Çubuğu üzerindeki Security Agent Simgelerini Görüntüleme A-4

Konsol Geçidine Erişme A-5

Ek B: WFBS içinde IPv6 Desteği

WFBS için IPv6 Desteği ve Security Agent'lar B-2
Security Server IPv6 Gereksinimleri B-2
Security Agent Gereksinimleri B-3
Messaging Security Agent Gereksinimleri B-3
Salt IPv6 Sunucu Sınırlamaları B-3
Salt IPv6 Security Agent Sınırlamaları B-4
IPv6 Adreslerini Yapılandırma B-5
IP Adreslerini Gösteren Ekranlar B-6

Ek C: Yardım Alma

Trend Micro Bilgi Bankası C-2
Trend Micro'ya Başvurma C-2
Durum Tanı Aracı C-3
Destek Çağrısını Hızlandırma C-3
Şüpheli İçeriği Trend Micro'ya Gönderme C-3
File Reputation Hizmetleri C-4
Email Reputation Hizmetleri C-4
Web Reputation Hizmetleri C-4
Tehdit Ansiklopedisi C-4
TrendLabs C-5
Belgelerin Geribildirimi C-6

Ek D: Ürün Terminolojisi ve Kavramlar

Kritik Yama D-2
Düzeltme D-2
IntelliScan D-2
IntelliTrap D-2
Davetsiz Misafir Algılama Sistemi D-4

Anahtar Sözcükler D-5
Yama D-9
Kurallı İfadeler D-10
Tarama Dışlama Listeleri D-18
Hizmet Paketi D-24
Truva Atı Bağlantı Noktası D-24
Temizlenemeyen Dosyalar D-25

Dizin

Dizin IN-1

Önsöz

Önsöz

Trend Micro™ Worry-Free™ Business Security *Yönetici Kılavuzu*'na hoş geldiniz. Bu belge; başlangıç bilgilerini, aracı yükleme prosedürlerini ve Security Server ve aracı yönetimini açıklamaktadır.

Worry-Free Business Security Belgeleri

Worry-Free Business Security belgeleri aşağıdakileri içermektedir:

TABLO 1. Worry-Free Business Security Belgeleri

BELGELER	AÇIKLAMA
Yükleme ve Yükseltme Kılavuzu	Security Server yüklemek ve server ve agent yükseltmelerini gerçekleştirmek için gereksinimleri ve prosedürleri açıklayan bir PDF belgesidir
Yönetici Kılavuzu	Başlangıç bilgisini, istemci yükleme prosedürlerini ve Security Server ve agent yönetimini açıklayan bir PDF belgesidir
Yardım	WebHelp veya CHM biçiminde derlenmiş ve "nasıl yapılır", kullanım tavsiyesi ve alana özel bilgileri sağlayan HTML dosyaları
Benioku dosyası	Bilinen sorunların listesini ve temel yükleme adımlarını içerir. Yardım veya basılı belgelerde bulunmayan en güncel ürün bilgilerini de içerebilir.
Bilgi Bankası	Problem çözme ve sorun giderme bilgilerinin çevrimiçi veritabanıdır. Bilinen ürün sorunları hakkında en son bilgileri sağlar. Bilgi Bankası'na erişmek için aşağıdaki web sitesine gidin: http://esupport.trendmicro.com

PDF belgelerin ve benioku dosyasının en son sürümlerini şuradan indirin:

http://docs.trendmicro.com/tr-tr/smb/worry-free-business-security.aspx

Hedef Kitle

Worry-Free Business Security belgeleri aşağıdaki kullanıcılar amaçlanarak hazırlanmıştır:

- **Güvenlik Yöneticileri**: Security Server ve aracı yüklemesi ve yönetimi dahil olmak üzere Worry-Free Business Security yönetiminden sorumludur. Bu kullanıcıların gelişmiş ağ ve sunucu yönetimi bilgisine sahip olmaları beklenmektedir.

- **Son kullanıcılar**: Bilgisayarlarında Security Agent yüklenmiş olan kullanıcılar. Bu kişilerin bilgisayar yeteneği düzeyi başlangıç ile yoğun kullanıcı arasındadır.

Belge Kuralları

Bilgileri kolayca bulmanıza ve yorumlamanıza yardımcı olmak için, Worry-Free Business Security belgeleri aşağıdaki kuralları kullanır.

TABLO 2. Belge Kuralları

KURAL	AÇIKLAMA
HEPSİ BÜYÜK HARF	Akronimler, kısaltmalar ve klavyedeki belirli komutların ve tuşların adları
Kalın	Menüler ve menü komutları, komut düğmeleri, sekmeler, seçenekler ve görevler
İtalik	Diğer belgelere veya yeni teknoloji bileşenlerine referanslar
<Metin>	Açılı ayıraç içerisindeki metnin güncel veri ile değiştirilmesi gerektiğini belirtir. Örneğin, C:\Program Files\<file_name> C:\Program Files\sample.jpg olabilir.
Nota	Yapılandırma notlarını veya önerileri sağlar
İpucu	En iyi uygulama bilgisini ve Trend Micro önerilerini sağlar
UYARI!	Ağınızdaki bilgisayarlara zarar verebilecek etkinlikler hakkında uyarılar sağlar

Bölüm 1

Worry-Free™ Business Security Standard ve Advanced Tanıtımı

Bu bölüm, Worry-Free Business Security (WFBS) hakkında bir genel görünüm sağlamaktadır.

Trend Micro Worry-Free Business Security'e Genel Bakış

Trend Micro Worry-Free Business Security (WFBS) küçük işletme kullanıcılarını ve varlıklarını veri hırsızlığından, kimlik hırsızlığından, riskli web sitelerinden ve spam'den korur (Yalnızca Advanced).

Bu belge, WFBS Standard ve Advanced sürümlerinin ikisi için de bilgi sağlamaktadır. Yalnızca Advanced sürüme ilişkin kısımlar ve bölümler "(Yalnızca Advanced)" şeklinde işaretlenmiştir.

Trend Micro Smart Protection Network tarafından desteklenen WFBS;

- **Daha güvenli**: Virüslerin, casus yazılımın, spam'in (Yalnızca Advanced) ve web tehditlerinin istemcilere ulaşmasını engeller. URL filtreleme özelliği, riskli web sitelerine erişimi engeller ve kullanıcının verimini artırmaya yardımcı olur.
- **Daha akıllı**: Hızlı taramalar ve sürekli güncellemeler, istemcilerde en az etkiyi yaratarak yeni tehditleri önler.
- **Daha kolay**: Dağıtması kolay olan ve sıfır yönetim gerektiren WFBS, tehditleri daha etkin bir şekilde algılar, bu sayede güvenlik yerine işe odaklanabilirsiniz.

Bu Sürümde Yeni (WFBS 9.0 SP2)

Worry-Free Business Security aşağıdaki yeni özellikleri ve geliştirmeleri sağlar:

TABLO 1-1. WFBS 9.0 SP2'deki Yenilikler

ÖZELLİK/İYİLEŞTİRME	AÇIKLAMA
Windows 10 desteği	Worry-Free Business Security şimdi Windows 10'da Security Agent yüklemesini destekler.

Özellik/İyileştirme	Açıklama
Belgeler için Fidye Yazılımı Koruması	Gelişmiş tarama özellikleri, yaygın davranışları belirleyerek ve fidye yazılımı programlarıyla yaygın olarak bağlantılı olan işlemleri engelleyerek uç noktalarda çalışan belgeleri hedefleyen fidye yazılımı programlarını belirleyip engelleyebilir.

Tablo 1-2. Çözülmüş Bilinen Sorunlar

Mad de No.	Hot Fix/ Kritik Yama Numarası	Sorun	Çözüm
1	B2363	Security Agent, kullanıcı Intuit QuickBooks Koruması işlevini devre dışı bıraktıktan sonra da Intuit dosyalarını koruyabilir.	Bu hot fix, kullanıcıların Intuit Quickbooks Koruması işlevini başarıyla devre dışı bırakabilmesini sağlar.
2	B2363	Security Agent, kullanıcı klasör koruması işlevini devre dışı bıraktıktan sonra da klasörleri koruyabilir.	Bu hot fix, kullanıcıların klasör koruması işlevini başarıyla devre dışı bırakabilmesini sağlar.
3	B2453	Worry-Free Business Security 9.0 Service Pack 1 Agent, POP3 e-posta taraması etkinleştirilmiş şekilde başlatılırken, Trend Micro Security Agent Dinleyici (TmListen.exe) hizmetiyle zamanlama çakışması nedeniyle Gerçek Zamanlı Tarama (Ntrtscan.exe) hizmeti başlatılamayabilir.	Bu kritik yama, Trend Micro Security Agent Dinleyici hizmetinin diğer hizmetler başlamadan önce Gerçek Zamanlı Tarama hizmetinin başlatılmasına izin vermesini sağlayarak zamanlama çakışmasını çözümler.

Mad de No.	Hot Fix/ Kritik Yama Numarası	Sorun	Çözüm
4	B2453	Bazı ortamlarda tarama işleminin bir kısmı gecikebilir veWorry-Free Business Security 9.0 Service Pack 1 Agent, algılanan kötü amaçlı yazılımda herhangi bir işlem uygulayamaz. Bu durumda Worry-Free Business Security, açılan bir uyarı görüntülemez veya bir algılama günlüğü oluşturmaz.	Bu kritik yama, Worry-Free Business Security 9.0 Service Pack 1 Agent'ın yukarıda açıklanan senaryoda algılanan kötü amaçlı yazılımlar üzerinde gerekli işlemi gerçekleştirmesini sağlar.
5	B2479	Manuel Tarama ilerleme penceresi, manuel tarama sırasında yanıt vermeyi durdurur.	Bu hot fix, manuel taramaların normal şekilde çalışıp tamamlanmasını sağlar.
6	B2500	Bir sorun, Worry-Free Business Security 9.0 Service Pack 1 sunucularının Smart Scan Modelini başarıyla güncellemesini önler. Bu durumda, sunucunun web konsolunda Smart Scan Service'in canlı durumuna “erişilemez”.	Bu hot fix, Worry-Free Business Security 9.0 Service Pack 1 sunucularının Smart Scan Modelini başarıyla güncelleyebilmesini sağlar.
7	B2502	Bir sorun, Worry-Free Business Security 9.0 Service Pack 1 sunucularının şu genel ayarı devre dışı bırakmasını engelliyor: “Web Reputation ve URL Filtreleme Günlüklerini Security Server'a Gönder”.	Bu hot fix, Worry-Free Business Security 9.0 Service Pack 1 sunucularının “Web Reputation ve URL Filtreleme Günlüklerini Security Server'a Gönder” ayarını devre dışı bırakabilmelerini sağlar.

Mad de No.	Hot Fix/ Kritik Yama Numarası	Sorun	Çözüm
8	B2503	Microsoft(TM) 64 bit işletim sistemlerinde Internet Explorer 9'un 32 bit sürümü, Security Agent ile aynı anda kurulu olduğunda çökebilir.	Bu hot fix, Microsoft 64 bit işletim sistemlerinde Security Agent ile birlikte var olduğunda tarayıcının mükemmel bir şekilde çalışmasını sağlar.
9	B2510	Worry-Free Business Security 9.0 Service Pack 1 agent, Microsoft(TM) Windows(TM) 8.0, 8.1 veya Server 2012 R2 platformuna yüklendiğinde SMTP posta tarama özelliği varsayılan olarak etkinleştirilir. Bu durumda hem platformun e-posta sunucusu hem de istemcisi bazı e-posta iletilerini gönderemeyebilir veya alamayabilir.	Bu hot fix, Security Agent'ın platform e-posta sunucu ve istemcisi ile düzgün çalışmasını sağlar.
10	B2514	Kullanıcılar, Worry-Free Business Security 9.0 Service Pack 1 Agent'ın yüklü olduğu bilgisayarlarda performans sorunlarıyla karşılaşabilir.	Bu hot fix, etkilenen bilgisayarlardaki performans sorunlarını giderir.
11	B2515	“coreTaskManager.dll” ikili dosyasıyla ilgili bir sorun, bilgisayara Worry-Free Business Security 9.0 Service Pack 1 Agent yüklendikten sonra bir yığın bellek sızıntısı sorununu tetikleyebilir.	Bu hot fix, etkilenen bilgisayarlardaki yığın bellek sızıntısı sorununu giderir.

Mad de No.	Hot Fix/ Kritik Yama Numarası	Sorun	Çözüm
12	B2516	Kullanıcılar, Worry-Free Business Security 9.0 Service Pack 1 sunucusunun yüklü olduğu bilgisayarlara Trend Micro Remote Manager aracısını yükleyemeyebilir. Bu durumda kullanıcılar mevcut GUID'lerini kullanarak Worry-Free Business Security uygulamasını Trend Micro Remote Manager'a kaydedemez.	Bu hot fix, kullanıcıların, Worry-Free Business Security 9.0 Service Pack 1 sunucusunun yüklü olduğu bilgisayarlara Trend Micro Remote Manager aracısını yükleyebilmesini sağlamak için yükleme sorunlarını çözer.
13	B2517	Worry-Free Business Security 9.0 Service Pack 1 Agent'ın yüklü olduğu bilgisayarlar, Gerçek Zamanlı Tarama özelliği etkinleştirildikten sonra yanıt vermeyi durdurabilir.	Bu hot fix, Gerçek Zamanlı Tarama özelliğini Worry-Free Business Security 9.0 Service Pack 1 Agent'larının normal şekilde çalışmasını sağlar.
14	B2519	Kullanıcılar, Worry-Free Business Security 9.0 Service Pack 1 Agent'ı yüklerken sistem çökmesi sorunlarıyla karşılaşabilir.	Bu hot fix, Worry-Free Business Security 9.0 Service Pack 1 Agent yüklenirken oluşan sistem çökmesi sorunlarını çözer.
15	B2520	Bazen Worry-Free Business Security 9.0 Service Pack 1, korumalı bir bilgisayardan çıkarılıp geri takılan bir USB disk aygıtını algılayamaz.	Bu hot fix, Worry-Free Business Security 9.0 Service Pack 1'in korumalı bilgisayarlara takılan USB disk aygıtlarını algılayabilmesini sağlar.
16	B2534	Kullanıcılar, Worry-Free Business Security 9.0 Service Pack 1 Agent'ı yükledikten sonra sistem çökmesi sorunlarıyla karşılaşabilir.	Bu hot fix, Worry-Free Business Security 9.0 Service Pack 1 Agent yüklenirken oluşan sistem çökmesi sorunlarını çözer.

Mad de No.	Hot Fix/ Kritik Yama Numarası	Sorun	Çözüm
17	B2541	Küme Paylaşılan Birimleri (CSV) diski olan bir Microsoft™ Windows™ Server ortamında Worry-Free Business Security 9.0 Service Pack 1 beklenmedik şekilde durdurulabilir veya mavi ekran verebilir.	Bu hot fix, Worry-Free Business Security 9.0 Service Pack 1'in Windows Server Yük Devretme Kümesi'nde CSV diskleriyle düzgün şekilde çalışmasını sağlar.

WFBS 9.0 SP1'deki Yenilikler

Worry-Free Business Security aşağıdaki yeni özellikleri ve geliştirmeleri sağlar:

Tablo 1-3. WFBS 9.0 SP1'deki Yenilikler

Özellik/İyileştirme	Açıklama
Algılama gelişmeleri	• Sıkıştırılmış çalıştırılabilir dosyalara karşı salgın önleme koruması (paketleyiciler) • Geliştirilmiş Hasar Temizleme Motoru performansı
İyileştirmeler	Web reputation günlükleri çalışan süreçlerin bilgileri içerir
Kullanılabilirlik iyileştirmeleri	• Security Server sürümü ekranda günlükte gösterilir • WFBS nasıl çalıştığını daha iyi yansıtmak için güncellenmiş UI metni

TABLO 1-4. Çözülmüş Bilinen Sorunlar

MAD DE NO.	HOT FIX/ KRİTİK YAMA NUMARASI	SORUN	ÇÖZÜM
1	Yok	Bir kullanıcı Messaging Security Agent'ı karantinaya alınan spam e-posta mesajlarındaki ekleri açmak-engellemek amacıyla yapılandırmak için bir yol talep ediyor (MSA 11.1.1254).	Bu hot fix Messaging Security Agent'ı karantinaya alınan spam e-posta mesajlarındaki ekleri açmak-engellemek amacıyla yapılandırmak için bir seçenek ekler.
2	1433	Worry-Free Business Security sunucusunu 8.0 veya 8.0 Service Pack 1'den 9.0'a yükselttikten sonra, sunucu web konsolunda Smart Scan Service'in canlı durumu “kullanılamıyor” oluyor. Bu, Worry-Free Business Security 9.0 sunucusu Smart Scan kalıbını başarıyla güncelleyemediği için oluşur.	Bu hot fix Worry-Free Business Security 9.0 sunucusunun Smart Scan Kalıbını başarıyla güncellemesini sağlar.
3	1439	Worry-Free Business Security 9.0 sunucu paketi Heartbleed güvenlik açığından etkilenen bir OpenSSL şifreli yazılım kütüphanesini içerir.	Bu kritik yama bu sorunu çözmek için Worry-Free Business Security 9.0 SP1 sunucu paketinde OpenSSL kriptografik yazılım kitaplığını günceller.
4	1440	Eğer Microsoft™ Windows™ yüksek kontrast modunda ise ve kullanıcılar Microsoft Internet Explorer'da Worry-Free Business Security 9.0 konsoluna erişebiliyorlarsa, kullanıcıların istemcileri bir gruptan diğerine taşıması mümkün olmayacaktır.	Bu hot fix, Windows, yüksek-kontrast modunda olduğunda Internet Explorer'ın düzgün bilgi almasını sağlamak amacıyla etkinleştirmek için bir fonksiyon özelliğini düzeltir. Bu, kullanıcıların bu senaryoda istemcileri başarıyla gruplar arasında taşıyabilmelerine yardımcı olur.

Mad de No.	Hot Fix/ Kritik Yama Numarası	Sorun	Çözüm
5	1442	Worry-Free Business Security Aracıların ağ sürücülerinde manuel taramaları çalıştırmaları mümkün olmayabilir.	Bu hot fix Worry-Free Business Security Aracıların ağ sürücülerinde manuel taramaları çalıştırmalarını sağlar.
6	1445	Worry-Free Business Security sunucu veritabanı işlemi Casus yazılım günlük sorgusu sırasında bellek kaçağı ile karşılaşabilir.	Bu hot fix Worry-Free Business Security Casus yazılım günlük sorgusu sırasında sunucu veritabanı işleminin bellek kaçağı ile karşılaşmamasını sağlar.
7	1451	Kullanıcılar sunucu kullanıcı arayüzünün istemci ağacındaki "Algılanan Virüsler", “Algılanan Casus Yazılım”, “Algılanan Spam” ve “İhlal Edilen URL'ler” sütunlarına tıklayarak verileri sıraladığı zaman, Worry-Free Business Security verileri doğru şekilde sıralayamıyor.	Bu hot fix “Algılanan Virüsler”, “Algılanan Casus Yazılım”, “Algılanan Spam” ve “İhlal Edilen URL'ler” sütunlarını etkileyen verileri sıralama sorununu düzeltir.
8	1452	Security Agent yöneticiler istemcileri konuşlandırmak için AutoPCC oturum açma komut dosyası kullanıyorlarsa hizmetlerin yüklenmesi başlangıçta başarısız oluyor.	Bu hot fix Security Agent yöneticiler istemcileri konuşlandırmak için AutoPCC oturum açma komut dosyası kullanıyorsa hizmetlerin başlangıçta düzgün çalışmasını sağlar.
9	1454	Kullanıcılar belli bir neden olmaksızın Security Agent öğesinden rastgele açılır pencereler alıyorlar.	Bu hot fix kullanıcıların Security Agent öğesinden sadece kendi bildirim yapılandırmasına göre gerekli etkinlikler için açılır pencereler almasını sağlar.

Mad de No.	Hot Fix/ Kritik Yama Numarası	Sorun	Çözüm
10	1456	Microsoft™ 64-bit işletim sistemlerinde (OS), Internet Explorer 9'un 32-bit sürümü Security Agent ile beraber mevcutsa çökebilir.	Bu hot fix Microsoft 64-bit işletim sistemlerinde Security Agent ile birlikte var olduğunda tarayıcının mükemmel bir şekilde çalışmasını sağlar.
11	1457	“Gerçekleştirilen Eylem” alanı Worry-Free Business Security Sunucusundan aktarılan virüs günlüklerinde herhangi bir bilgi içermiyor.	Bu hot fix Worry-Free Business Security Sunucusundan virüs günlüklerinin düzgün bir şekilde içe aktarılmasını sağlar.
12	1458	Worry-Free Business Security Sunucusunun POP3 mail günlüğü ve Security Agent günlüğü arasında "Tarih/Saat" alanında bir tutarsızlık var .	Bu hot fix Worry-Free Business Security Sunucusunun POP3 mail günlüğündeki bilgilerin Security Agent günlüğündekiler ile tutarlı olmasını sağlar.
13	1459	Kullanıcılar, bir HTTP yeniden yönlendirme kaynağından Smart Scan Kalıbını güncelleştiremeyebilir.	Bu hot fix kullanıcıların başarıyla HTTP yeniden yönlendirme kaynağından Smart Scan Kalıbını güncelleştirebilmeleri için HTTP yeniden yönlendirme yanıtlarındaki dolar işareti karakterinin işlenebilmesini sağlar.
14	1459	Security Agent'lar aracı program dosyalarını güncellerken balon bildirimleri alıyor. İstemci bu tipteki balon bildirimini devre dışı bırakmak için bir yol istiyor.	Bu hot fix aracı program dosyalarını güncellerken beliren balon bildirimini devre dışı bırakmak için bir seçenek sunar.

Mad de No.	Hot Fix/ Kritik Yama Numarası	Sorun	Çözüm
15	1466	Worry-Free Business Security Agent'ı kurduktan sonra PccNTMon.exe bir tanıtıcı kaçak sorunuyla karşılaşabilir.	Bu hot fix etkilenen bilgisayarlardaki tanıtıcı kaçak sorunu giderir.
16	2062	Worry-Free Business Security paketi ile birlikte gelen ve bir üçüncü taraf sürücüsü ile çalışan EYES sürücüsü bazen yanlış pozitif bildirimde bulunabilir.	Bu hot fix yanlış pozitif bildirimin engellenmesine yardımcı olmak için EYES sürücüsünü günceller.
17	2063	TmListenWorry-Free Business Security Agent yüklemesinden sonra beklenmedik bir şekilde durabilir.	Bu hot fix TmListen'ın Worry-Free Business Security Agent yüklemesinden sonra başarıyla çalışmasını sağlar.
18	5215	Windows XP işletim sistemi ile çalışan bilgisayarlarda yüklü Security Agent kullanıcılar yönetici hesabı olmayan bir hesap ile Windows'ta oturum açtıklarında USB aygıtından önyükleme bölümünde bulunan kötü amaçlı yazılımı tespit edemez.	Bu hot fix bu sorunu çözmek için Security Agent dosyalarını günceller.
19	5215	Ntrtscan.exe hizmeti Security Agent 260 karakterden uzun bir yol uzunluğuna sahip bir yerde manuel tarama gerçekleştirirken beklenmedik bir şekilde durabilir.	Bu hot fix Ntrtscan.exe'nin beklenmedik bir şekilde durmasını önlemek için Security Agent tarafından tarama esnasında dosya yollarını saklamak için sabit değişken yerine esnek değişken kullanılmasını sağlar.

Mad de No.	Hot Fix/ Kritik Yama Numarası	Sorun	Çözüm
20	5215	Bazı durumlarda,Security Agent başlarken Security Agent Dinleyici hizmeti, TmListen.exe beklenmedik bir şekilde durur.	Bu hot fix Security Agent başlarken TmListen.exe 'nin beklenmedik bir şekilde durmasını önlemek için Security Agent hata işleme mekanizmasını güçlendirir.
21	5215	Bazı durumlarda, bir Security Agent bilgisayarının durumu Security Agent bilgisayarda etkin olmasına rağmen Microsoft™ Windows™ Eylem Merkezi'nde "Trend Micro Security Agent kapatılmış" olarak görülebilir.	Bu hot fix Security Agent durumunun Windows Eylem Merkezi'nde doğru şekilde görülmesini sağlamak için Security Agent dosyalarını günceller.
22	5227	Novell™ ZENworks™ Uygulama platformunda Security Agent konsolunda oturum açmak Virüs Tarama Motoru ayarlarındaki bir sorundan ötürü uzun zaman alabilir.	Bu hot fix, kullanıcıların Worry-Free Business Security sunucusunda Virüs Tarama Motoru ayarlarını değiştirmelerine ve yeni Virüs Tarama Motoru ayarlarını küresel ölçekte Worry-Free Business Security istemcilerine dağıtmalarına izin vererek bu sorunu çözer.
23	5238	Security Server cgiCheckIP.exe işlevi kullanıcıların herhangi bir ağ içinde herhangi bir bağlantı noktasını taramalarını sağlar.	Bu hot fix cgiCheckIP.exe işlevinin bağlantı noktası kontrol mekanizmasını bağlantı noktasını taramadan önce istemciden gelen bağlantı noktasının numarasını doğrulayacak şekilde geliştirir.

MAD DE NO.	HOT FIX/ KRİTİK YAMA NUMARASI	SORUN	ÇÖZÜM
24	5245	Microsoft™ Office™ paylaşılan klasörlerdeki Office dosyalarını açarken takılıyor. Bu sorun CheckRtPCWOplock parametresini uygulayarak çözülebilir.	Bu hot fix kullanıcıların **Genel Ayar**'da aşağıdaki CheckRtPCWOplock parametresinin ayarlanmasını ve bu gecikme sorunun giderilmesi için istemciye uygulamasını sağlar.
25	5248	Bazı durumlarda, bir Security Agent bilgisayarın VPN ağ ortamındaki durumu Microsoft™ Windows™ Eylem Merkezi'nde "Trend Micro Security Agent olarak kapalı" görünür.	Bu hot fix istemci durumunun Windows Eylem Merkezi'nde doğru şekilde görülmesini sağlamak için Security Agent dosyalarını günceller.
26	5248	Security Agent her zaman bu istemci kayıt defteri anahtarının üzerine yazar ve güvenlik duvarı modülü için varsayılan değer olarak ayarlar: HKLM\SYSTEM \CurrentControlSet\services\tmtdi \Parameters\ RedirectIpv6	Bu hot fix Redirect IPv6 işlevini RedirectIpv6 anahtarının üzerine yazarak ve varsayılan değer olarak ayarlayarak manüel olarak (ancak zorlamadan) değiştirir.

MAD DE NO.	HOT FIX/ KRİTİK YAMA NUMARASI	SORUN	ÇÖZÜM
27	5274	Security Agent güncelleştirmeleri esnasında, Security Agent Diğer Güncelleme Kaynakları'nın (OUS) ayarlarını ClientAllSetting.ini dosyasından alır ve alınan bilgileri kullanarak Ous.inidosyasını günceller. Ancak Security Server Ana Hizmet durduğunda, "ClientAllSetting.ini" dosyası silinir. Sonuç olarak, Security Agent Ous.ini dosyasını güncelleştirmek için OUS ayarlarını alamaz ve Security Agent güncellemesinin başarısız olmasına sebep olabilir.	Bu hot fix ClientAllSetting.ini dosyasından OUS ayarları alınamıyorsa Security Agent öğesinin Ous.ini dosyasında değişiklik yapmasını engelleyen bir kontrol mekanizması ekler. Bu Security Agent'lar öğesinin ClientAllSetting.ini dosyası boşken dahi güncelleştirmeleri tamamlayabilmesini sağlar.
28	5339	Bazen, Virüs Temizleme Şablonu sürümü Security Agent konsolunda istemci şablonu güncelledikten ve yeni sürümü yükledikten sonra “0” olur.	Bu hot fix Security Agent konsolunda doğru Virüs Temizleme Şablonu sürümünün görünür olmasını sağlamak için sürüm kontrol mekanizmasını güçlendirir.
29	5350	Kullanıcılar Security Agent Web Reputation Hizmeti'ne (WRS) URL'leri yeniden yönlendirmek için IPv6 kullandığı zaman dahili web sitelerine erişemeyebilir.	Bu hot fix WRS'ye URL'lerin IPv6 yerine IPv4 kullanılarak yeniden yönlendirilmesini ve genel olarak bu ayarın uygulanmasını sağlamak amacıyla Security Agent'lar yapılandırılması için bir seçenek sunarak bu sorunu çözer.

Mad de No.	Hot Fix/ Kritik Yama Numarası	Sorun	Çözüm
30	5366	Microsoft™ Outlook™Security Agent Behavior Monitoring hizmetinin çalıştığı bilgisayarda yanıt vermeyi durdurdu.	Hotfix bu durumda Behavior Monitoring ayarlarının beklenmedik şekilde Outlook'un durmasını önleyebilecek şekilde yapılmasını sağlar.
31	5369	Security Agent kendi kendine açılan sıkıştırılmış bir dosyada casus yazılım algıladığında ve dosya üzerinde yaptığı tüm eylemleri başarısız olduğunda bir casus yazılım günlüğü oluşturmuyor.	Bu hot fix Security Agent öğesinin kendi kendine açılan sıkıştırılmış bir dosyada casus yazılım algıladığında ve dosya üzerinde yaptığı tüm eylemleri başarısız olduğunda bir casus yazılım günlüğü oluşturmasını sağlar.
32	5390	Security Agent öğesinin Ous.ini dosyası güncellemeden sonra kırpılmış. Bu Ous.ini dosyası kopyalama işlemi için ayrılan hafıza tamponundan büyükse dosyanın tampona sığmasını sağlamak için kırpılması durumunda olur.	Bu hot fix Ous.ini kopyalama işlevi için hafıza tamponunu arttırarak Security Agent'lar Ous.ini dosyasının güncellemeleri sırasında kırpılmasını önler.
33	5399	Bazen, OfficeScan istemci konsolunda Virüs Temizleme Şablonu sürümü istemci şablonu güncelledikten ve yeni sürümü yükledikten sonra “0” olur.	Bu hot fix konsolunda doğru Virüs Temizleme Şablonu sürümünün OfficeScan istemci konsolunda görünür olmasını sağlamak için sürüm kontrol mekanizmasını güçlendirir.
34	5443	Smart Scan Agent ve virüs kalıp dosyaları geri alma işlemi düzgün çalışmayabilir.	Bu hot fix Smart Scan Agent ve virüs kalıp dosyaları geri alma işleminin doğru çalışmasını sağlar.

MAD DE NO.	HOT FIX/ KRİTİK YAMA NUMARASI	SORUN	ÇÖZÜM
35	5463	Bir üçüncü taraf yazılımı Security Agent bilgisayarında istemcinin hem Yetkisiz Değişiklikleri Önleme Hizmeti hem de Güvenlik Duvarı Hizmetleri etkinse yanıt vermeyebilir.	Bu hot fix istemcinin hem Yetkisiz Değişiklikleri Önleme Hizmeti hem de Güvenlik Duvarı Hizmetleri etkin olduğunda Security Agent bilgisayarlarında üçüncü taraf yazılımlarının beklenmedik bir şekilde durmalarını önlemek için kullanıcıların güvenlik duvarı ayarlarını değiştirmelerini sağlar.
36	5485	Security Agent manuel tarama yapıyorsa ve tarama yolu 63 karakterden uzun değilse, ilgili tarama günlüğü "Virüs Günlükleri" görüntüleyicisinde görünmez.	Bu hot fix tarama yolunun 63 karakterden daha uzun olmadığı durumlarda tarama günlüklerinin başarıyla kaydedilmesini sağlar.
37	5492	Security Agent'lar 64-bit platformlarda yüklü olanların güncelleme aracısından güncelleştirilmesi mümkün olmayabilir.	Bu hot fix Security Agent'lar öğesinin güncelleme aracısı tarafından başarıyla güncellenmesini sağlar.
38	5495	Bazı bileşenler, modülleri Security Agent güncellemesi esnasında bazı özellikler tarafından kullanıldığı zaman güncellenmemiş olabilir.	Bu düzeltme, Security Agent güncellemesi esnasında tüm bileşenlerin güncellenmesini sağlar.

WFBS 9.0'daki Yenilikler

Worry-Free Business Security aşağıdaki yeni özellikleri ve geliştirmeleri sağlar:

TABLO 1-5. WFBS 9.0'daki Yenilikler

ÖZELLİK/İYİLEŞTİRME	AÇIKLAMA
Microsoft Exchange desteği	WFBS artık Microsoft Exchange Server 2010 SP3 ve Microsoft Exchange Server 2013'ü desteklemektedir.
Windows desteği	WFBS artık Microsoft Windows 8.1 ve Windows Server 2012 R2'yi desteklemektedir.

Mobil aygıt güvenliği	WFBS Gelişmiş, artık mobil cihaz veri koruması ve erişim kontrolünü desteklemektedir. Mobil cihaz güvenliği aşağıdaki özelliklere sahiptir:
	• Aygıt Erişim Denetimi
	  • Kullanıcı, işletim sistemi ve/veya e-posta sunucusuna göre Exchange sunucusuna erişim sağlar
	  • Özel posta kutusu bileşenlerine verilen erişimi özelleştirin
	• Aygıt Yönetimi
	  • Kayıp veya çalınan aygıtlarda silme işlemi gerçekleştirin
	  • Özel kullanıcılar için şu güvenlik ayarlarını uygulayın:
	  • Parola güvenlik düzeyi gereklilikleri
	  • Aygıtın devreden çıktıktan sonra otomatik olarak kilitlenmesi
	  • Şifreleme
	  • Başarısız giriş verilerini silme işlemi

Etkinleştirme Kodu geliştirmesi	Sonradan ödemeli etkinleştirme Kodu desteği

Özellik/İyileştirme	Açıklama
Algılama gelişmeleri	• Gerçek zamanlı tarama için Gelişmiş Bellek Taraması • Behavior Monitoring için bilinen olası tehdit modu • Tarayıcı Exploit Önleme • Yeni karşılaşılan program indirme algılaması
Performans gelişmeleri	• Security Agent'in yükleme ve kaldırma süresi • Gerçek Zamanlı Tarama için Ertelenmiş Tarama
Kullanılabilirlik iyileştirmeleri	• Web Reputation ve URL Filtreleme için genel ve grup Onay/Engelleme listeleri • Genel Ayarlarda Web Reputation ve URL Filtreleme için IP istisna listesi • ActiveX'in İstemci Ağacından ve Uzaktan yükleme sayfasından kaldırılması • Özelleştirilmiş Salgın Savunması • Trend Micro Anti-Spam Araç Çubuğu için Outlook 2013 ve Windows Live Mail 2012 desteği • Sadece Trend Micro ActiveUpdate'den günceleme için Update Aracısı • Sunucu güncellemelerini durdur • Sunucu ve Aracı'yı yükseltirken kalıpları koru • Yardım Bağlantısı ve Etkilenme Kaynağı virüs günlükleri

Önemli Özellikleri ve Faydaları

Worry-Free Business Security aşağıdaki özellikleri ve faydaları sağlar:

Trend Micro™ Smart Protection Network™

Trend Micro™ Smart Protection Network™, müşterileri güvenlik tehlikelerinden ve web tehditlerinden korumak için tasarlanmış yeni nesil, bulut-istemci içerik güvenlik alt yapısıdır. Kullanıcıları gerek ağ üzerinde, gerek evde, gerekse yolda korumak için hem yerindeki, hem de Trend Micro ev sahipliğindeki çözümleri desteklemektedir. Smart Protection Network, e-posta, web ve dosya reputation teknolojilerine ve tehdit veritabanlarına eşsiz bulut-içi ilişkisiyle erişim için daha hafif aracılar kullanmaktadır. Ağ üzerindeki ürünler, hizmetler ve kullanıcılar arttıkça kullanıcıları için gerçek zamanlı bir komşuluk izleme koruması hizmeti oluşturarak, müşterilerin korumasını otomatik olarak güncellemekte ve güçlendirmektedir.

Smart Protection Network hakkında daha fazla bilgi için şu adresi ziyaret edin:

http://www.trendmicro.com.tr/teknoloji-yenilik/teknolojimiz/smart-protection-network/index.html

File Reputation Hizmetleri

File Reputation (dosya geçmişi) hizmetleri, her dosyanın geçmişini kapsamlı bir bulut içi veritabanını kullanarak kontrol eder. Kötü amaçlı yazılım bilgileri bulut içinde depolandığından, tüm kullanıcılara anında sunulur. Yüksek performanslı içerik dağıtım ağları ve yerel önbelleğe alma sunucuları, denetim işlemi sırasında gecikme süresini en aza indirir. Bulut-istemci mimarisi, daha hızlı koruma sağlar ve istemcinin genel iş yükünü önemli ölçüde azaltırken kalıp dağıtımı yükünü ortadan kaldırır.

File Reputation hizmetlerinin kullanılması için Security Agent'ların smart scan modunda olması gereklidir. Bu aracılardan bu belgede **smart scan aracıları** olarak bahsedilecektir. Smart scan modunda olmayan aracılar File Reputation Hizmetlerini kullanmaz ve **geleneksel tarama aracıları** olarak adlandırılır. Worry-Free Business Security yöneticileri tüm veya belirli aracıların smart scan modunda olmasını yapılandırabilir.

Web Reputation Hizmetleri

Dünyanın en büyük etki alanı geçmişi veritabanlarından birine sahip olan Trend Micro web reputation teknolojisi, web sitesinin yaşı, geçmişteki yer değişiklikleri ve kötü amaçlı yazılım davranış analizleriyle tespit edilen şüpheli etkinlikler gibi faktörlere dayanarak bir

geçmiş puanı atama yoluyla web etki alanlarının güvenilirliğini izler. Web reputation, siteleri taramaya ve kullanıcıların etkilenmiş sitelere erişmesini engellemeye devam eder. Web reputation, kullanıcıların eriştiği sayfaların güvenli ve kötü amaçlı yazılımlar, casus yazılımlar ve kullanıcıları kişisel bilgilerini vermeleri için kandırmak üzere tasarlanmış kimlik avı dolandırıcılığı gibi web tehditlerinden arınmış olmasını sağlamaya yardımcı olur. Doğruluk oranını artırmak ve hatalı pozitif sonuçları azaltmak için, Trend Micro Web reputation teknolojisi, birçok zaman yasal sitelerin yalnızca bazı kısımları saldırılardan etkilendiğinden ve geçmiş durumu zaman içinde dinamik olarak değişebildiğinden sitelerin tamamını sınıflandırmak veya engellemek yerine belirli sayfalara veya bağlantılara geçmiş puanları atar.

Web reputation ilkelerine tabi olan aracılar Web Reputation Hizmetlerini kullanır. Worry-Free Business Security yöneticiler tüm veya belirli aracıları web reputation ilkelerine tabi tutabilir.

Email Reputation (Yalnızca Advanced)

Trend Micro e-posta geçmişi teknolojisi, IP adreslerini bilinen spam kaynaklarından oluşan bir geçmiş veritabanında bulunup bulunmadıklarını kontrol ederek ve e-postayı gönderen kaynağın geçmişini gerçek zamanlı değerlendirebilen dinamik bir hizmet kullanarak IP adreslerini doğrular. Geçmiş derecelendirmeleri, IP adreslerinin "davranışı", etkinlik kapsamı ve geçmişi sürekli olarak analiz edilerek hassaslaştırılır. Kötü amaçlı e-postalar, göndericinin IP adresine bağlı olarak bulut içinde engellenir ve böylece zombi veya botnet gibi tehlikelerin ağa veya kullanıcının bilgisayarına ulaşması önlenir.

Email Reputation teknolojisi, kaynak Posta Aktarım Aracısı'nın (MTA) geçmişine bağlı olarak spam'i belirler. Bu, Security Server'ı bu görevin yükünden kurtarır. Email Reputation etkinleştirildiğinde, kaynak IP adresinin temiz olduğundan ve bilinen bir spam vektörü olarak kara listeye alınmadığından emin olmak üzere tüm gelen SMTP trafiği IP veritabanları tarafından denetlenir.

Email Reputation için iki hizmet düzeyi vardır:

- **Standart**: Standard hizmeti, yaklaşık iki milyar IP adresinin geçmişini izleyen bir veritabanını kullanır. Sıklıkla spam iletileriyle ilişkilendirilen IP adresleri, veritabanına eklenir ve nadiren veritabanından çıkarılır.

- **Gelişmiş**: Advanced hizmet düzeyi Standart hizmet gibi sorguya dayalı bir hizmet olan DNS'dir. Bu hizmetin temelinde standart geçmiş veritabanı ile bilinen ve şüpheli spam kaynaklarından gelen iletileri engelleyen dinamik geçmiş, gerçek zamanlı veritabanı yer alır.

Engellenen veya şüpheli bir IP adresinden gelen bir e-posta iletisi tespit edildiğinde, bu ileti sizin mesajlaşma altyapınıza ulaşmadan önce Email Reputation Services (ERS) tarafından durdurulur. ERS, sizin güvenli olduğuna inandığınız bir IP adresinden gelen e-posta iletilerini engelliyorsa, o IP adresini Onaylanan IP Adresi listesine ekleyin.

Smart Feedback

Trend Micro Smart Feedback, Trend Microürünleri ve 24/7 tehdit araştırma merkezleri ve teknolojileri arasında kesintisiz iletişim sağlar. Her bir müşterinin rutin geçmiş denetimi sırasında tespit edilen her yeni tehdit, Trend Micro tehdit veritabanlarının tümünü otomatik olarak günceller ve müşterilerin söz konusu tehditle bir daha karşılaşmamasını sağlar.

Müşteri ve ortaklardan oluşan kapsamlı genel ağı üzerinden topladığı tehdit bilgilerini sürekli olarak işleyen Trend Micro, en yeni tehditlere karşı otomatik, gerçek zamanlı koruma sağlar ve komşuların birbirinin evine göz kulak olduğu, otomatikleştirilmiş semt gözetimi programları gibi "elbirliğiyle" güvenlik sağlar. Elde edilen tehdit bilgileri, söz konusu iletişimin içeriğine değil, iletişim kaynağının geçmişine bağlı olduğundan, müşterinin kişisel veya işletme bilgilerinin gizliliği her zaman korunur.

Trend Micro şirketine gönderilen bilgi örnekleri:

- Dosya sağlamaları
- Erişilen web siteleri
- Boyutlar ve yollar dahil olmak üzere dosya bilgileri
- Yürütülebilir dosyaların adları

Programa katılımınızı herhangi bir anda web konsolundan sonlandırabilirsiniz.

Ayrıntılar için, bkz. *Smart Feedback Program'ına Katılma sayfa 13-5*.

İpucu

istemciler cihazınızı korumak için Smart Feedback'e katılmanız gerekli değildir. Katılımınız isteğe bağlıdır ve istediğiniz zaman çıkabilirsiniz. Trend Micro, tüm Trend Micro müşterileri için daha iyi bir genel koruma sağlamaya yardımcı olmak amacıyla Smart Feedback'e katılmanızı önerir.

Smart Protection Network hakkında daha fazla bilgi için şu adresi ziyaret edin:

http://www.trendmicro.com.tr/teknoloji-yenilik/teknolojimiz/smart-protection-network/index.html

URL Filtreleme

URL filtreleme, çalışanların iş dışında uğraşlara ayırdığı zamanı kısıtlamak, Internet bant genişliği kullanımını azaltmak ve daha güvenli bir Internet ortamı yaratmak amacıyla web sitelerine erişimi denetlemenize yardımcı olur. Bir URL filtreleme koruması düzeyi seçebilir veya taramak istediğiniz Web sitesi türlerini özelleştirebilirsiniz.

Korumanın Yararları

Aşağıdaki tabloda farklı Worry-Free Business Security bileşenlerinin bilgisayarlarınızı tehditlerden nasıl koruduğu anlatılmaktadır.

TABLO 1-6. Korumanın Yararları

TEHDİT	KORUMA
Virüs/Kötü Amaçlı Yazılım. Virüsler, Truva Atları, Solucanlar, Arka Kapı Programları ve Davetsiz Misafirler **Casus Yazılım/Grayware**. Casus Yazılımlar, Numara Çeviriciler, Korsanlık araçları, Parola kırma uygulamaları, Reklam yazılımları, Şaka programları ve Tuş kaydediciler	Dosya bazlı taramalar (Gerçek Zamanlı Tarama, Manuel Tarama, Zamanlanmış Tarama)

TEHDİT	KORUMA
E-posta iletileri üzerinden iletilen güvenlik tehditleri	Security Agent içerisindeki **POP3 Posta Taraması**
Ağ solucanları/virüsler ve izinsiz girişler	Security Agent'ta Güvenlik Duvarı
Zararlı olabilecek web siteleri/Kimlik Avı siteleri	Security Agent'taki Web Reputation ve URL Filtreleme
USB ve diğer harici aygıtlar üzerinden yayılan güvenlik tehditleri.	Security Agent'ta Aygıt Denetimi
Kötü Amaçlı Davranış	Security Agent'ta Behavior Monitoring

Tehditleri Anlama

Özel güvenlik personeli bulunmayan ve zayıf güvenlik ilkeleri olan kuruluşlar, temel güvenlik altyapısına sahip olsalar bile tehditlere gittikçe daha fazla maruz kalmaktadır. Keşfedildiği zaman bu tehditler çoğu hesaplama kaynağına yayılmış olabilir ve tamamen giderilmesi ciddi süre ve çaba gerektirebilir. Tehdidin giderilmesi için öngörülmeyen masraflar sarsıcı olabilir.

Trend Micro Smart Protection Network'ün parçası olan Trend Micro ağ güvenliği bilgisi ve bulut-içi sunucuları, sonraki nesail tehditleri tanımlar ve bunlara yanıt verir.

Virüsler ve Kötü Amaçlı Yazılımlar

On binlerce virüs/kötü amaçlı yazılım bulunmakta olup her gün yenisi oluşturulmaktadır. Bir zamanlar DOS veya Windows içinde daha yaygın olsa da, günümüzde bilgisayar virüsleri, kurumsal ağlardaki, e-posta sistemlerindeki ve web sitelerindeki güvenlik açıklarından faydalanarak büyük zarara neden olabilmektedir.

- **Şaka programı**: Çoğunlukla bilgisayar monitöründeki görüntülere müdahale eden virüs benzeri bir programdır.
- **Olası virüs/kötü amaçlı yazılım**: Virüs/kötü amaçlı yazılım özelliklerinin bazılarına sahip olan şüpheli dosyalar. Ayrıntılar için, bkz. Trend Micro virüs ansiklopedisi:

http://about-threats.trendmicro.com/threatencyclopedia.aspx

- **Davetsiz misafirler**: Son kullanıcının onayı veya bilgisi olmadan bir sistemde bir kod yükleyen ve yürüten bir program (veya programlar derlemesi). Makinede kalıcı ve algılanamayan bir şekilde varlığını sürdürmek için gizlilik kullanır. Kök kullanıcı takımları makineleri etkilemez, daha çok zararlı kodu yürütmek için algılanamayan bir ortam sağlama amaçlıdır. Kök kullanıcı takımları, sosyal tasarımlar aracılığıyla, kötü amaçlı yazılımların yürütülmesiyle veya sadece zararlı bir web sitesinin açılmasıyla sistemlere yüklenirler. Bir kez yüklendikten sonra, saldırgan sistem üzerinde; uzaktan erişim, gizli dinleme, işlemleri, dosyaları, kayıt defteri girişlerini ve iletişim kanallarını gizleme dahil neredeyse her işlemi gerçekleştirebilir,

- **Truva atı**: Bu tehdit türü, bilgisayarlara ve yürütülebilir programlara erişim sağlamak için genellikle bağlantı noktalarını kullanır. Truva atı programları çoğalmaz ancak bilgisayar korsanlarının girmesi için bağlantı noktalarını açmak gibi zararlı eylemler gerçekleştirmek üzere bilgisayarlarda yerleşir. Geleneksel antivirüs çözümleri virüsleri algılayıp kaldırabilir, ancak Truva atları, özellikle de sisteminizde çalışmakta olanlar için bu durum geçerli değildir.

- **Virus**: Çoğalan bir program. Çoğalmak için virüsün kendisini başka program dosyalarına iliştirmesi ve ana sistem programı yürütüldüğünde yürütülmesi gerekir, örneğin;

  - **ActiveX zararlı kodu**: ActiveX™ kontrollerini yürüten web sayfalarında yerleşen kod.

  - **Önyükleme kesimi virüsü**: Bir bölüm veya diskin önyükleme kesimini etkileyen bir virüstür.

  - **COM ve EXE dosyası bulaştırıcısı**: Dosya uzantısı .com veya .exe olan yürütülebilir bir program.

  - **Java zararlı kodu**: Java™'da yazılmış veya gömülü, işletim sisteminden bağımsız virüs kodudur

  - **Makro virüs**: Uygulama makrosu olarak kodlanmış ve genellikle bir belgeye dahil edilmiş bir virüstür.

  - **Paketleyici**: Genellikle Truva atı programı gibi Windows ya da Linux™ ile yürütülebilir sıkıştırılmış ve/veya şifrelenmiş bir programdır. Yürütülebilir bileşenleri sıkıştırmak, antivirus ürününün paketleyiciyi algılamasını zorlaştırır.

- **Test Virüsü**: Gerçek bir virüs gibi davranan ve virüs tarama yazılımı tarafından algılanabilen etkisiz bir dosya. Antivirüs yüklemenizin düzgün bir şekilde tarama yaptığını doğrulamak için EICAR test komut dosyası gibi test virüsleri kullanın.
- **VBScript**, **JavaScript** veya **HTML virüsü**: Web sayfalarında bulunan ve tarayıcı aracılığıyla indiren bir virüstür.
- **Solucan**: Kendi işlevsel kopyalarını veya bunların bir kısmını diğer bilgisayar sistemlerine genellikle e-posta yoluyla yayabilen kendi içinde bir program veya bir program grubudur.
- **Diğerleri**: Diğer herhangi bir virüs/kötü amaçlı yazılım türü kategorisine dahil olmayan virüsleri/kötü amaçlı yazılımlar.

Casus Yazılım ve Grayware

Son noktalar, virüsler ve kötü amaçlı yazılımlar dışındaki olası tehditlerden dolayı da tehlikededir. Casus yazılım/Grayware, virüsler veya truva atları olarak sınıflandırılmayan, ancak yine de ağınızdaki istemciler performansını olumsuz olarak etkileyen ve kuruluşunuza önemli güvenlik, gizlilik ve hukuki tehlikeler doğuran uygulamalar veya dosyalar için kullanılır. Casus yazılım/grayware genellikle açılır pencerelerle, kullanıcıların bastığı tuşları kaydederek ve istemci güvenlik açıklarını saldırıya maruz bırakarak kullanıcıları sinirlendirmek gibi istenmeyen ve tehdit edici eylemler gerçekleştirir.

Worry-Free Business Security'nin grayware olarak algılayamadığı ama bir grayware türü olduğunu düşündüğünüz bir uygulama veya dosya bulursanız, analiz için Trend Micro'ya gönderin:

http://esupport.trendmicro.com/solution/en-us/1059565.aspx

TÜR	AÇIKLAMA
Casus Yazılım	Hesap kullanıcı adları ve parolaları gibi veriyi alır ve üçüncü taraflara iletir.
Reklam Yazılımı	Reklamları görüntüler ve web tarayıcısı üzerinden kullanıcı hedefli reklamlar göndermek için kullanılan kullanıcının web gezinme tercihleri gibi verileri alır

Tür	Açıklama
Çevirici	istemci İnternet ayarlarını değiştirir ve modem aracılığıyla istemci'ın önceden yapılandırılmış telefon numaralarını çevirmesini sağlayabilir. Bu numaralar, genellikle çağrı başına ücret uygulanan veya uluslararası numaralar olup, kuruluşunuzun büyük bir masrafa girmesine neden olabilir.
Şaka programı	CD-ROM tepsisini açıp kapatmak ve çeşitli ileti kutuları görüntülemek gibi anormal istemci davranışlarına neden olur.
Korsanlık aracı	Bilgisayar korsanlarının bilgisayarlara girmesine yardım eder.
Uzaktan erişim aracı	Bilgisayar korsanlarının bilgisayarlara uzaktan erişmesine ve kontrol etmesine yardım eder.
Parola kırma uygulaması	Bilgisayar korsanlarının kullanıcı adlarını ve parolaları çözmesine yardım eder.
Diğerleri	Diğer potansiyel olarak zararlı program türleri.

Spam

Spam, genellikle ticari amaçlı, ayrım yapılmaksızın birden çok posta listesine, kullanıcıya veya haber grubuna gönderilen istenmeyen e-posta iletilerinden (önemsiz e-posta iletileri) oluşur. İki tür istenmeyen posta vardır: İstenmeyen ticari e-posta iletileri (UCE) veya istenmeyen toplu e-posta iletileri (UBE).

İzinsiz girişler

İzinsiz girişler, ağlara veya istemciler'a güç kullanarak ya da izinsiz girmek anlamına gelir. Bir ağın veya istemci'ın güvenliğini atlatmak anlamına da gelebilir.

Kötü Amaçlı Davranış

Kötü Amaçlı Davranış, bir yazılım tarafından işletim sisteminde, kayıt defteri girdilerinde, diğer yazılımlarda veya dosya ve klasörlerde yapılabilecek yetkisiz değişiklikler anlamına gelir.

Sahte Erişim Noktaları

Kötü İkiz olarak da bilinen Sahte Erişim Noktaları, kullanıcının bulunduğu yerde sağlanan yasal bir erişim noktası gibi görünen, ama aslında kablosuz iletişimleri izlemek üzere bir korsan tarafından oluşturulmuş sahte bir Wi-Fi erişim noktasına verilen addır.

Kimlik Avı Olayları

Kimlik avı veya kimlik avcılığı, normal bir web sitesini taklit ederek web kullanıcılarını aldatıp özel bilgilerini açıklamalarını sağlamaya çalışan ve hızla artan bir dolandırıcılık biçimidir.

Tipik bir senaryoda, durumdan şüphelenmeyen kullanıcılar, kendilerine hesaplarıyla ilgili bir sorun olduğunu ve hesabın kapatılmaması için sorunun hemen giderilmesi gerektiğini söyleyen, acil gibi görünen (orijinal görünümlü) bir e-posta alır. Bu e-posta, aynen gerçek gibi görünen web sitesine giden bir URL içerir. Normal bir e-postayı ve normal bir web sitesini kopyalayarak toplanan verileri alan arka plan adlı kısmı değiştirmek kolaydır.

Bu e-posta, kullanıcıdan sitede oturum açmasını ve bazı hesap bilgilerini doğrulamasını ister. Bir bilgisayar korsanı, kullanıcının verdiği oturum açma adı, parola, kredi kartı numarası veya sosyal güvenlik numarası gibi verileri alır.

Kimlik avı dolandırıcılığı hızlıdır, ucuzdur ve sürdürmesi kolaydır. Ayrıca, bunu yapan suçlular için potansiyel olarak oldukça kazançlıdır. Kimlik avını algılamak bilgisayar meraklısı kullanıcılar için bile zordur. Ayrıca, kanunlar tarafından takip edilmesi de zordur. Daha kötüsü, bu suçu kovuşturmak neredeyse imkansızdır.

Lütfen kimlik avcısı olabileceğinden şüphelendiğiniz web sitelerini Trend Micro'ya bildirin. Daha fazla bilgi için bkz. *Şüpheli İçeriği Trend Micro'ya Gönderme sayfa C-3*.

Toplu Posta Saldırıları

E-postaya duyarlı virüsler/kötü amaçlı yazılımlar, etkilenen bilgisayarın e-posta istemcilerini otomatik hale getirerek veya virüsü/kötü amaçlı yazılımı kendileri dağıtarak e-posta iletisi yoluyla yayılabilir. Toplu posta davranışı, bir enfeksiyonun Microsoft Exchange ortamında hızla yayıldığı durumları anlatır. Trend Micro, toplu posta saldırılarının genellikle sergilediği davranışları tespit edecek şekilde tasarlanmıştır. Söz

konusu davranışlar, Trend Micro ActiveUpdate Sunucuları kullanılarak güncellenen Virüs Kalıbı dosyasına kaydedilir.

Messaging Security Agent'ın (yalnızca Advanced), toplu postalama davranışı algıladığında toplu posta saldırılarına karşı önlem almasını sağlayabilirsiniz. Toplu postalama davranışı için ayarlanan eylem diğer tüm eylemlere göre öncelikli olur. Toplu postalama saldırıları için varsayılan eylem iletinin tamamını sil eylemidir.

Örneğin: Messaging Security Agent'ı, iletilerin bir solucan veya Truva atından etkilendiğini algıladığında iletileri karantinaya alacak şekilde yapılandırabilirsiniz. Ayrıca toplu postalama davranışını etkinleştirebilir ve Agent'ı toplu postalama davranışı gösteren tüm iletileri silmek üzere ayarlayabilirsiniz. Bu Agent, bir MyDoom varyasyonu gibi bir solucan içeren bir ileti alır. Bu solucan, etkilenen bilgisayarlardan topladığı e-posta adreslerine kendisini göndermek için kendi SMTP motorunu kullanır. Agent, MyDoom solucanını algılayıp bunu bir toplu postalama davranışı olarak tanımladığında, toplu postalama davranışı sergilemeyen solucanlar için uygulanan karantinaya alma eyleminin aksine, solucanın bulunduğu e-postayı siler.

Web Tehditleri

Web tehditleri Internet'te türeyen geniş bir tehdit dizisini kapsar. Tek bir dosya veya yaklaşım yerine, çeşitli dosya kombinasyonları ve teknikler kullanan Web tehditleri yöntemleri bakımından niteliklidir. Örneğin, web tehdidini oluşturanlar kullanılan sürüm veya değişkeni sürekli olarak değiştirir. Web tehdidi, etkilenmiş bir istemci yerine sabit bir web sitesi konumunda yer aldığı için, web tehdidini oluşturanlar tehdidin algılanmasını önlemek için kodunu sürekli olarak değiştirir.

Son yıllarda, eskiden bilgisayar korsanı, virüs yazılımcısı, spam mail gönderenler ve casus yazılım üreticisi olarak nitelenen kişiler artık siber suçlular olarak tanınmaktadır. Web tehditleri bu kişilerin iki amaçtan birini takip etmelerine yardımcı olur. Bu amaçlardan biri, daha sonra satmak üzere bilgi çalmaktır. Bunun yol açtığı etki, kimlik kaybı biçimindeki gizli bilgi sızıntısıdır. Etkilenmiş istemci da kimlik avı saldırılarını veya başka bilgi yakalama faaliyetlerini gönderecek bir vektör haline gelebilir. Diğer etkilerden biri, bu tehdidin web ticaretine olan güveni yok etme potansiyeline sahip olması ve böylece Internet işlemleri için gereken güveni zedelemesidir. İkinci amaç, bir kullanıcının CPU gücünü kazançlı faaliyetlerde bulunmak için bir araç olarak kullanmak üzere ele geçirmektir. Bu faaliyetlerden bazıları, spam gönderme, dağıtılmış servis reddi saldırısı biçiminde şantaj yapma veya tıklama başına ücret almayı içerir.

Bölüm 2

Başlarken

Bu bölümde, Worry-Free Business Security'nin hazır ve çalışır duruma getirilmesi açıklanmaktadır.

Worry-Free Business Security Network

Worry-Free Business Security aşağıdakileri içermektedir:

- *Security Server sayfa 2-2*
- *Aracılar sayfa 2-3*
- *Web Konsolu sayfa 2-4*

Security Server

Worry-Free Business Security'nin merkezinde Security Server bulunur. Security Server, Worry-Free Business Security için merkezi web tabanlı yönetim konsolu olan web konsolunu barındırır. Security Server, aracıları ağdaki istemcilere yükler ve aracılarla birlikte bir aracı-sunucu ilişkisi oluşturur. Security Server, tek bir merkezden güvenlik durumu bilgilerini görüntülemeyi, aracıları görüntülemeyi, sistem güvenliğini yapılandırmayı ve bileşenleri indirmeyi etkinleştirir. Security Server ayrıca aracılar tarafından kendisine bildirilen tespit edilmiş Internet tehditlerinin günlüklerini kaydettiği veritabanını içerir.

Security Server şu önemli işlevleri yerine getirir:

- Aracıları yükler, izler ve yönetir.
- Aracıların gereksinim duyduğu bileşenleri indirir. Varsayılan olarak, Security Server, bileşenleri Trend Micro ActiveUpdate sunucusundan indirir ve ardından bunları aracılara dağıtır.

Tarama Sunucusu

Security Server'da Security Server yüklemesi sırasında otomatik olarak yüklenen Tarama Sunucusu adında bir hizmet içermektedir. Bu şekilde, ayrı olarak yüklenmesi gerekmez. Tarama Sunucusu iCRCService.exe işlem adı altında çalışır ve Microsoft Yönetim Konsolu'nda **Trend Micro Smart Scan Service** olarak belirir.

Security Agent'lar **smart scan** adı verilen bir tarama yöntemi kullandığında, Tarama Sunucusu bu aracıların daha verimli tarama yapmasına yardımcı olur. Smart scan işlemi aşağıdaki gibi açıklanabilir:

- Security Agent, geleneksel Virüs Kalıbı'nın daha hafif bir sürümü olan **Smart Scan Agent Pattern**'nı kullanarak istemciyi güvenlik tehditleri için tarar.. Smart Scan Agent Kalıbı, Virüs Kalıbında yer alan tehdit imzalarının çoğunu içerir.

- Tarama sırasında dosyanın tehlikesini belirleyemeyen bir Security Agent, Tarama Sunucusu'na bir tarama sorgusu göndererek tehlikeyi doğrular. Tarama Sunucusu, **Smart Scan Kalıbı** kullanarak tehlikeyi doğrular, bu kalıpta Smart Scan Aracı Kalıbı'nda bulunmayan tehdit imzaları da yer almaktadır.

- Security Agent, tarama performansını iyileştirmek için Tarama Sunucusu tarafından sağlanan tarama sorgusu sonucunu "saklar".

Tehdit tanımlarının bazılarını bulundurarak, Tarama Sunucusu bileşenleri indirirken Security Agent'ların bant genişliği tüketimini azaltmaya yardımcı olur. Security Agent'lar, Virüs Kalıbı'nı indirmek yerine, boyut olarak çok daha küçük olan Smart Scan Aracı Kalıbı'nı indirir.

Security Agent'lar Tarama Sunucusuna bağlanamadığı zaman, Tarama Sunucusu ile aynı işleve sahip Trend Micro Smart Protection Network'e tarama sorguları gönderir.

Tarama Sunucusunu Security Server'dan ayrı olarak kaldırmak mümkün değildir. Tarama Sunucusunu kullanmak istemiyorsanız:

1. Security Server bilgisayarında, Microsoft Yönetim Konsolunu açın ve **Trend Micro Smart Scan Service** öğesini devre dışı bırakın.

2. Web konsolunda, **Tercihler** > **Genel Ayarlar** > **Masaüstü/Sunucu** sekmesine giderek ve **Disable Smart Scan Service** seçeneğini seçerek Security Agent'ları geleneksel taramaya geçirin.

Aracılar

Aracılar, istemcileri güvenlik tehditlerinden korur. İstemciler; masaüstü bilgisayarları, sunucuları ve Microsoft Exchange sunucularını içerir. WFBS aracıları:

TABLO 2-1. WFBS Aracıları

ARACI	AÇIKLAMA
Security Agent	Masaüstü bilgisayarlarını ve sunucuları güvenlik tehditlerinden ve izinsiz girişlerden korur
Messaging Security Agent (Yalnızca Advanced)	Microsoft Exchange sunucularını e-posta kaynaklı güvenlik tehditlerinden korur

Aracı, yüklenmiş olduğu Security Server'a bildirimde bulunur. Security Server'a en son istemci bilgilerini sağlamak için, aracı, olay durum bilgilerini gerçek zamanlı olarak gönderir. Aracılar, tehdit algılama, başlangıç, kapanış, tarama başlangıcı ve bir güncellenmenin tamamlaması gibi olayları rapor eder.

Web Konsolu

Web konsolu, bir kuruluş ağı üzerindeki istemcileri izlemek için merkezi bir noktadır. Güvenlik gereksinimlerinize ve özelliklerinize göre yapılandırabileceğiniz bir dizi varsayılan ayar ve değerle gelir. Web konsolu; Java, CGI, HTML ve HTTP gibi standart Internet teknolojilerini kullanır.

Web konsolunu kullanarak aşağıdakileri yapabilirsiniz:

- Aracıları istemcilere dağıtma.
- Eşzamanlı yapılandırma ve yönetim için aracıları mantıksal gruplar halinde düzenleme.
- Ürün ayarlarını yapılandırın ve tek bir grupta veya birden çok grupta Manuel Tarama'yı başlatma.
- Bildirimleri alma ve tehditle ilişkili etkinlikler için günlük raporlarını görüntüleme.
- İstemciler üzerinde tehdit algılandığında e-posta iletileri ile bildirim alın ve salgın uyarıları gönderin.
- Salgın Savunması'nı yapılandırarak ve etkinleştirerek salgınları önleme.

Web Konsolunu Açma

Başlamadan önce

Ağ üzerinde aşağıdaki kaynaklara sahip olan herhangi bir istemciden web konsolunu açın:

- Internet Explorer 7.0 veya üzeri
- 1024x768 veya daha yüksek çözünürlüklü, yüksek renkli ekran
- HTTPS bağlantısı üzerinde Microsoft Edge

İpucu

Messaging Security Agent sunucu konsolu, Windows 10 Microsoft Edge tarayıcısını desteklemez.

Edge tarayıcısını kullanarak konsola erişirken herhangi bir sorunla karşı karşıya kalırsanız, Internet Explorer 7 ya da üzerini kullanın.

Prosedür

1. Web konsolunu açmak için aşağıdaki seçeneklerden birini seçin:
   - Security Server'ı barındıran bilgisayar üzerinde, masaüstüne gidin ve Worry-Free Business Security kısayoluna tıklayın.
   - Security Server'ı barındıran bilgisayar üzerinde, **Windows Başlat menüsü** > **Trend Micro Worry-Free Business Security** > **Worry-Free Business Security** öğelerine tıklayın.
   - Ağ üzerindeki herhangi bir istemci üzerinde, bir web tarayıcısı açın ve adres çubuğuna aşağıdakini yazın:

     `https://{Security_Server_Name veya IP Adresi }:{bağlantı noktası numarası}/SMB`

     Örneğin:

     `https://my-test-server:4343/SMB`

     `https://192.168.0.10:4343/SMB`

`http://my-test-server:8059/SMB`

`http://192.168.0.10:8059/SMB`

İpucu

SSL KULLANMIYORSANIZ, `http` yerine `https` yazın. HTTP bağlantıları için varsayılan bağlantı noktası 8059 ve HTTPS bağlantıları için de 4343'tür.

Ortam sunucu adlarını DNS ile çözümleyemiyorsa, IP adresi yerine sunucu adı kullanın.

Tarayıcı, Worry-Free Business Security oturum açma ekranını görüntüler.

2. Parolanızı yazın ve **Oturum aç** öğesine tıklayın.

   Tarayıcı, **Canlı Durum** ekranını görüntüler.

Bundan sonra ne yapılacak

Web konsoluna erişemiyorsanız, aşağıdakileri kontrol edin.

KONTROL EDİLECEK ÖĞE	AYRINTILAR
Parola	Parolanızı unuttuysanız, parolayı sıfırlamak için Konsol Parolası Sıfırlama Aracını kullanın. Security Server bilgisayarındaki bu araca Windows Başlat menüsündeki Trend Micro Worry-Free Business Security klasörü altından erişin.
Tarayıcı Önbelleği	WFBS'nin önceki bir sürümünden yükselttiyseniz, web tarayıcı ve proxy server önbellek dosyaları web konsolunun yüklenmesini engelleyebilir. Tarayıcınızda ve Trend Micro Security Server ile web konsoluna erişmek için kullandığınız istemci arasında bulunan tüm proxy sunucularında önbelleği temizleyin.

KONTROL EDİLECEK ÖĞE	AYRINTILAR
SSL Sertifikası	Web sunucunuzun düzgün çalıştığını doğrulayın. SSL kullanıyorsanız, SSL sertifikanızın geçerliliğini koruduğunu doğrulayın. Ayrıntılar için web sunucusu belgelerine bakın.

Sanal Dizin Ayarları	Web konsolunu IIS sunucusunda çalıştırıyorsanız ve aşağıdaki ileti görünüyorsa, sanal dizin ayarlarıyla ilgili bir sorun olabilir:
	`Sayfa görüntülenemiyor`
	`HTTP Hatası 403.1 - İzin Yok: Yürütme erişimi reddedildi.`
	`Internet Information Services (IIS)`
	Konsola erişmek için aşağıdaki adreslerden herhangi biri kullanıldığında bu ileti görünebilir:
	http://{sunucu adı}/SMB/
	http://{sunucu adı}/SMB/default.htm
	Ancak, şu adresi kullanırken konsol sorunsuz bir şekilde açılabilir:
	http://{sunucu adı}/SMB/console/html/cgi/cgichkmasterpwd.exe
	Bu sorunu çözmek için, SMB sanal dizininin yürütme izinlerini kontrol edin.
	Komut dosyalarını etkinleştirmek için:
	1. Internet Information Services (IIS) yöneticisini açın.
	2. SMB sanal dizininde, **Özellikler**'i seçin.
	3. Sanal Dizin sekmesini seçin ve yürütme izinlerini `hiçbiri` seçeneğinden `Komut Dosyaları`'na getirin. Ayrıca, istemci yükleme sanal dizininin yürütme izinlerini de değiştirin.

Web Konsolunda Gezinme

Web Konsolunun Ana Bölümleri

Web konsolu, aşağıdaki ana bölümleri içerir:

BÖLÜM	AÇIKLAMA
A. Ana menü	Web konsolunun üst kısmında ana menü bulunmaktadır. Sağ üst köşede yöneticilerin sıklıkla gerçekleştirdikleri görevlere kısayolları içeren aşağı açılır bir kutu bulunmaktadır. Ayrıca oturumunuzu sonlandırmanıza imkan sağlamak için **Oturum kapat** bağlantısı da sağlanmaktadır.
B. Yapılandırma alanı	Ana menü öğelerinin alt kısmı, yapılandırma alanıdır. Bu alanı, seçtiğiniz menü öğesine uygun seçenekleri belirlemek için kullanın.
C. Menü kenar çubuğu (tüm ekranlarda mevcut değildir)	**Güvenlik Ayarları** ekranından bir Security Agent grubu seçtiğinizde ve **Ayarları Yapılandır** öğesine tıkladığınızda, bir menü kenar çubuğu görüntülenir. Kenar çubuğunu, gruba ait masaüstü bilgisayarlar ve sunucular için güvenlik ayarlarını ve taramaları yapılandırmak üzere kullanın. Güvenlik Ayarları ekranından (Yalnızca Advanced) bir Messaging Security Agent seçtiğinizde, kenar çubuğunu Microsoft Exchange sunucularınız için güvenlik ayarlarını ve taramaları yapılandırmak üzere kullanabilirsiniz.

Web Konsolu Menü Seçenekleri

Web konsolundan aşağıdaki menü seçeneklerini kullanın:

Menü Seçenekleri	Açıklama
Canlı Durum	Worry-Free Business Security stratejisinde merkezi bir işlev sunar. Salgınlar ve kritik güvenlik riskleri hakkındaki uyarıları ve bildirimleri görüntülemek için Canlı Durum kullanın. • Trend Micro tarafından gönderilen kırmızı veya sarı uyarıları görüntüleyin • Ağınızdaki istemcilere yönelik en son tehditleri görüntüleyin • Microsoft Exchange sunucularına yönelik en son tehditleri görüntüleyin (Yalnızca Advanced) • Risk altındaki istemcilere güncelleme dağıtın
Güvenlik Ayarları	• Aracılar için güvenlik ayarlarını yapılandırın • Gruplar arasında ayarları çoğaltın
Salgın Savunması	Salgın Savunması, Güvenlik Açığı Değerlendirmesi ve Hasar Temizleme'yi yapılandır ve yay.
Taramalar	• İstemcileri tehditler için tarayın • İstemciler için taramayı zamanlayın
Güncellemeler	• Virüs kalıbı, tarama motoru, temizleme bileşenleri ve aracı programı içeren en son güncellenen bileşenler için Trend Micro ActiveUpdate sunucusunu (veya özel bir güncelleme kaynağını) denetleyin • Güncelleme kaynağını yapılandırın • Security Agent'ları Güncelleme Aracıları olarak atayın
Raporlar	Tehditleri ve diğer güvenlikle ilgili etkinlikleri takip etmek için raporlar oluşturun

Menü Seçenekleri	Açıklama
Tercihler	• Anormal tehditle alakalı veya sistemle alakalı olaylar için bildirim ayarlayın • Bakım kolaylığı için genel ayarlar belirleyin • Ağ ve istemcilere yönelik güvenliği yönetmeye yardımcı olması için yönetim araçlarını kullanın • Smart Geribildirim programına katılarak ürün lisans bilgisini görüntüleyin, yönetici parolası edinin ve dijital bilgi alışverişi için iş ortamının güvenli tutulmasına yardımcı olun
Yardım	• Özel içerik ve konu arayın • Yönetici Kılavuzu'nu görüntüleyin • Bilgi Bankası'ndan en yeni bilgilere erişin • Güvenlik, Satış, Destek ve sürüm bilgilerini görüntüleyin.

Web Konsolu Simgeleri

Aşağıdaki tablo, web konsolunda görüntülenen simgeleri tanımlamakta ve onların hangi amaçla kullanıldığını açıklamaktadır.

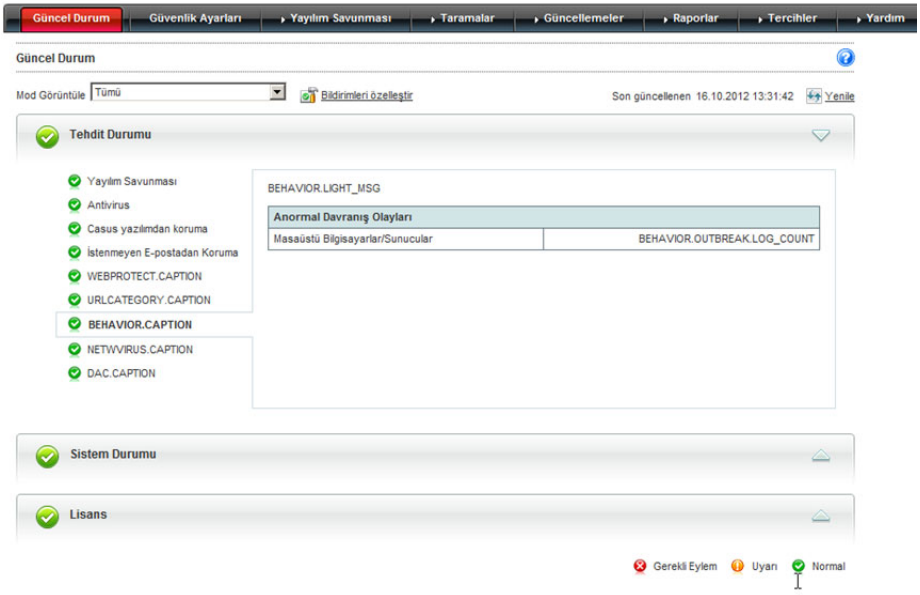
Tablo 2-2. Web Konsolu Simgeleri

Simge	Açıklama
	Yardım simgesi. Çevrimiçi yardımı açar.
	Yenile simgesi. Mevcut ekranın görünümünü yeniler.
	Bölümü Genişlet/Daralt simgesi. Bölümleri görüntüler/gizler. Bir defada yalnızca tek bir kısmı genişletebilirsiniz.
	Bilgi simgesi. Belirli bir öğeye ilişkin bilgileri görüntüler.
	Bildirimleri özelleştir simgesi. Çeşitli bildirim seçeneklerini görüntüler.

Canlı Durum

Canlı Durum ekranını ağınızın tehlike güvenliğinin genel bir görünümü almak için kullanın.

Canlı Durum ekranında görüntülenen bilgileri yenileme hızı her bölüme göre farklılık gösterir. Yenileme hızı genellikle 1 ila 10 dakika arasındadır. Ekran bilgilerini manuel olarak yenilemek için, tarayıcınızın **Yenile** düğmesine tıklatın.



Simgeleri Anlama

Eylem gerçekleştirilmesi gerektiğinde simgeler sizi uyarır. Daha fazla bilgi görüntülemek için bölümleri genişletin. Ayrıca, belirli ayrıntıları görüntülemek için tablodaki öğelere tıklayabilirsiniz. Belirli istemciler hakkında daha fazla bilgi edinmek için, tablolarda görünen numara bağlantılarına tıklayın.

TABLO 2-3. Canlı Durum Simgeleri

SİMGE	AÇIKLAMA
	Normal Yalnızca birkaç istemci yama uygulamayı gerektirir. Virüs, casus yazılım, cihazlarınız ve ağınızdaki diğer kötü amaçlı yazılım etkinlikleri önemli ölçüde risk taşır.
	Uyarı Ağınızın daha fazla risk altında kalmasını önlemek için harekete geçin. Bir uyarı simgesi, tipik olarak, çok fazla virüs ve diğer kötü amaçlı yazılım olayları bildiren, güvenlik açığı olan çeşitli bilgisayarlarınız olduğu anlamına gelir. Trend Micro tarafından Sarı Uyarı gönderildiğinde, uyarı Salgın Savunması için görüntülenir.
	Gerekli eylem Bir uyarı simgesi, güvenlik sorununu çözmek için yöneticinin eylemde bulunması gerektiği anlamına gelir.

Canlı Durum ekranında görüntülenen bilgiler, WFBS tarafından oluşturulur ve istemcilerden toplanan verilere dayanır.

Tehdit Durumu

Bu bölümde aşağıdaki bilgiler gösterilmektedir:

TABLO 2-4. Tehdit Durumu Bölümleri ve Görüntülenen Bilgiler

BÖLÜM	AÇIKLAMA
Salgın Savunması	Ağınızdaki olası bir virüs salgını.

Bölüm	Açıklama
Antivirüs	Olaydan itibaren, durum simgesi Uyarı simgesini görüntülemek üzere değişir. Eylemde bulunmanız gerekiyorsa: • Security Agent, gerçekleştirmek üzere ayarlandığı eylemi başarıyla gerçekleştirmedi. Security Agent'ın eylemi gerçekleştiremediği bilgisayarlar hakkında ayrıntılı bilgileri görüntülemek için numara bağlantısına tıklayın. • Security Agent'larda Gerçek Zamanlı tarama devre dışı. Gerçek Zamanlı taramayı tekrar başlatmak için **Şimdi Etkinleştir**'i tıklatın. • Messaging Security Agent'ta gerçek zamanlı tarama devre dışı.
Casus yazılımdan koruma	En son casus yazılım tarama sonuçlarını ve casus yazılım günlük girdilerini görüntüler. Casus Yazılım Tehdit Olayları tablosunun **Olay Sayısı** sütununda en son casus yazılım taramasının sonuçları görüntülenir. Belirli istemciler hakkında daha fazla bilgi için, Casus Yazılım Tehdit Olayları tablosunun **Algılanan Olaylar** sütununun altında bulunan numara bağlantısını tıklatın. Buradan, istemcilerinizi etkileyen belirli casus yazılım tehditleriyle ilgili bilgi bulabilirsiniz.
İstenmeyen E-postadan Koruma	Seçili Microsoft Exchange sunucusunun İstenmeyen e-postadan koruma ekranından eşik düzeyini ayarlayabileceğiniz yapılandırma ekranına yeniden yönlendirilmek için **Yüksek**, **Orta** veya **Düşük** bağlantısına tıklayın. İlgili ekrana yeniden yönlendirilmek için **Devre Dışı**'yı tıklatın. Bu bilgi, saatlik bir şekilde güncellenir.
Web Reputation	Trend Micro tarafından belirlenen potansiyel olarak tehlikeli web siteleri.
URL Filtreleme	Yönetici tarafından belirlenen kısıtlanmış web siteleri.
Behavior Monitoring	Davranış izleme ilkelerinin ihlalleri.
Ağ Virüsleri	Güvenlik duvarı ayarları tarafından belirlenen algılamalar.

BÖLÜM	AÇIKLAMA
Aygıt Denetimi	USB aygıtları ve ağ sürücülerine erişimi sınırlar **Nota** WFBS, akıllı telefon ve dijital fotoğraf makinesi dışında USB arayüzü yoluyla bağlanan her tür depolama aygıtını destekler.

Sistem Durumu

Bu bölümde, güncellenen bileşenlerle ilgili bilgi ve aracıların yüklendiği istemcilerdeki boş alan gösterilmektedir.

TABLO 2-5. Sistem Durumu Bölümleri ve Görüntülenen Bilgiler

BÖLÜM	AÇIKLAMA
Bileşen Güncellemeleri	Güncellenmiş bileşenlerin aracılara dağıtımı için bileşen güncellemelerinin durumu.
Smart Scan	Tarama Sunucusu'na bağlanamayan Security Agent'lar. **Nota** Tarama Sunucusu, Security Server üzerinde bulunan bir hizmettir.
Olağan dışı sistem olayları	Sunucu olarak görev yapan (sunucu işletim sistemlerini çalıştıran) istemcilere ilişkin disk alanı bilgisi.

Web konsolunu Uyarı veya Eylem Gerekli simgesini görüntüleyecek şekilde tetikleyen parametreleri, **Yönetim** > **Bildirimler** seçeneklerinden özelleştirebilirsiniz.

Lisans Durumu

Bu bölüm, ürün lisansınızın durumuna ilişkin bilgileri, özellikle geçerlilik sonu bilgilerini göstermektedir.

Canlı Durum Güncelleme Aralıkları

Canlı Durum bilgilerinin hangi sıklıkta güncelleneceğini anlamak amacıyla aşağıdaki tabloya bakın.

Tablo 2-6. Canlı Durum Güncelleme Aralıkları

Öğe	Güncelleme Aralığı (dakika)	Aracı Günlükleri Sunucuya Şunun Ardından Gönderir... (dakika)
Salgın Savunması	3	Yok
Antivirüs	1	Security Agent: Hemen Messaging Security Agent: 5
Casus yazılımdan koruma	3	1
İstenmeyen E-postadan Koruma	3	60
Web Reputation	3	Hemen
URL Filtreleme	3	Hemen
Behavior Monitoring	3	2
Ağ Virüsleri	3	2
Aygıt Denetimi	3	2
Smart Scan	60	Yok
Lisans	10	Yok
Bileşen Güncellemeleri	3	Yok
Olağan Dışı Sistem Olayları	10	Dinleme hizmeti TmListen başlatıldığında

Bölüm 3

Aracıları Yükleme

Bu bölümde, Security Agent ve Messaging Security Agent'ların yüklenmesi için gerekli adımları açıklamaktadır (yalnızca Advanced). Ayrıca, bu Agent'ları kaldırmayla ilgili bilgiler de verilmektedir.

Security Agent Yüklemesi

Windows istemcileri (masaüstleri ve sunucular) üzerinde Security Agent için yeni bir yükleme gerçekleştirin. Gereksinimlerinize en uygun yükleme yöntemini kullanın.

Security Agent'ı yüklemeden önce istemci üzerinde çalışan tüm uygulamaları kapatın. Diğer uygulamalar çalışırken yükleme yaparsanız, yükleme işleminin tamamlanması daha uzun sürebilir.

Nota

Messaging Security Agent'ı bu sürüme yükseltmek hakkında bilgi için, *Yükleme ve Yükseltme Kılavuzu*'na bakın.

Security Agent Yükleme Gereksinimleri

Yükleme gereksinimlerinin ve uyumlu üçüncü taraf ürünlerin tam bir listesi için aşağıdaki web sitesini ziyaret edin:

http://docs.trendmicro.com/tr-tr/smb/worry-free-business-security.aspx

Security Agent Yükleme Hususları

Security Agent'ları yüklemeden önce, aşağıdakileri dikkate alın:

- **Aracı özellikleri:** Bazı Security Agent özellikleri bazı Windows platformlarında kullanılabilir değildir. Ayrıntılar için, bkz. *Kullanılabilir Security Agent Özellikleri sayfa 3-3*.
- **x64 platformları**: x64 platformu için Security Agent'ın azaltılmış bir sürümü mevcuttur. Ancak, IA-64 platformu henüz desteklenmemektedir.
- **IPv6 desteği**: Security Agent, çift yığınlı veya salt IPv6 istemciler üzerine yüklenebilir. Ancak:
  - Aracının yüklü olabileceği bazı Windows işletim sistemleri IPv6 adreslemesini desteklememektedir.

- Bazı yükleme yöntemleri için, aracının başarıyla yüklenmesi için belirli gereksinimler mevcuttur.

Ayrıntılar için, bkz. *Security Agent Yüklemesi ve IPv6 Desteği sayfa 3-7*.

- **Kural Dışı Durum Listeleri**: Aşağıdaki özellikler için kural dışı listesinin düzgün bir şekilde yapılandırıldığından emin olun:
  - **Davranış İzleme**: Kritik istemci uygulamalarını Security Agent'ın bu uygulamaları engellemesini önlemek için Onaylanan Programlar listesine ekleyin. Daha fazla bilgi için bkz. *Behavior Monitoring'i Yapılandırma sayfa 5-21*.
  - **Web Reputation**: Güvenli olduğunu düşündüğünüz web sitelerini, Security Agent'ın bu web sitelerine erişimi engellemesini önlemek için Onaylanan URL Listesine ekleyin. Daha fazla bilgi için bkz. *Security Agent'lar için Web Reputation Yapılandırma sayfa 5-17*.
- **Aracı yükleme dizini**: Security Server yüklemesi sırasında, Kurulum, varsayılan olarak $ProgramFiles\Trend Micro\Security Agent olan aracı yükleme dizinini belirtmeniz için istemde bulunur. Security Agent'ları farklı bir dizine yüklemek istiyorsanız, yeni dizini **Tercihler** > **Genel Ayarlar** > **Sistem** > **Security Agent Yüklemesi** bölümünde belirtin.

Kullanılabilir Security Agent Özellikleri

Bir istemci üzerindeki kullanılabilir Security Agent özellikleri, istemcinin işletim sistemine bağlıdır. Belirli bir işletim sistemine bir aracı yüklerken, desteklenmeyen özelliklerin farkında olun.

TABLO 3-1. Security Agent Özellikleri

ÖZELLİK	WINDOWS İŞLETİM SİSTEMİ								
	XP	VISTA	7	8/8.1	10	SERVER/SBS 2003	SERVER/SBS 2008	SERVER 2008 R2/SBS 2011	SERVER 2012/R2
Manuel Tarama, Gerçek Zamanlı Tarama ve Zamanlanmış Tarama	Evet	Evet	Evet	Evet	Evet	Evet	Evet	Evet	Evet
Güvenlik Duvarı	Evet	Evet	Evet	Evet	Evet	Evet	Evet	Evet	Evet
Web reputation	Evet	Evet	Evet	Evet	Evet	Evet	Evet	Evet	Evet
URL Filtreleme	Evet	Evet	Evet	Evet	Evet	Evet	Evet	Evet	Evet
Behavior Monitoring	Evet (32-bit) Hayır (64-bit)	Evet (32/64-bit) Hayır (SP1 olmadan 64-bit)	Evet	Evet	Evet	Evet (32-bit) Hayır (64-bit)	Evet	Evet	Evet

Özellik	Windows İşletim Sistemi								
	XP	Vista	7	8/8.1	10	Server/SBS 2003	Server/SBS 2008	Server 2008 R2/SBS 2011	Server 2012/R2
Aygıt Denetimi	Evet (32-bit) Hayır (64-bit)	Evet (32/64-bit) Hayır (SP1 olmadan 64-bit)	Evet	Evet	Evet	Evet (32-bit) Hayır (64-bit)	Evet	Evet	Evet
Hasar Temizleme Hizmetleri	Evet	Evet	Evet	Evet	Evet	Evet	Evet	Evet	Evet
POP3 posta taraması	Evet	Evet	Evet	Evet	Evet	Evet	Evet	Evet	Evet
Manuel ve zamanlanmış güncellemeler	Evet	Evet	Evet	Evet	Evet	Evet	Evet	Evet	Evet
Güncelleme Aracısı	Evet	Evet	Evet	Evet	Evet	Evet	Evet	Evet	Evet
Agent Plug-in Manager	Evet	Evet	Evet	Evet	Evet	Evet	Evet	Evet	Evet

Özellik	Windows İşletim Sistemi								
	XP	Vista	7	8/8.1	10	Server/SBS 2003	Server/SBS 2008	Server 2008 R2/SBS 2011	Server 2012/R2
Smart Feedback	Evet	Evet	Evet	Evet	Evet	Evet	Evet	Evet	Evet
Trend Micro Anti-spam Toolbar	Evet (32-bit) Hayır (64-bit)	Evet	Evet	Evet	Evet	Hayır	Hayır	Hayır	Hayır
	Desteklenen eposta istemcileri: • Microsoft Outlook 2003 (32 bit), 2007 (32 bit), 2010 (32 ve 64 bit), 2013 (32 ve 64 bit) • Service Pack 2 veya üzeri ile Outlook Express 6.0 • Windows Mail 6.0 • Windows Live Mail 2011, 2012								
HouseCall	Evet	Evet	Evet	Evet	Evet	Evet	Evet	Evet	Evet
Durum Tanı Aracı	Evet	Evet	Evet	Evet	Evet	Evet	Evet	Evet	Evet
Wi-Fi Advisor	Evet	Evet	Evet	Evet	Evet	Hayır	Hayır	Hayır	Hayır

Security Agent Yüklemesi ve IPv6 Desteği

Bu bölümde, Security Agent'ı çift yığınlı veya salt IPv6 istemcilere yüklerken dikkate alınacak hususlar açıklanmaktadır.

İşletim Sistemi

Security Agent sadece IPv6 adreslemesini destekleyen aşağıdaki işletim sistemlerine yüklenebilir:

- Windows Vista (tüm sürümler)
- Windows Server 2008/2008 R2 (tüm sürümler)
- Windows 7 (tüm sürümler)
- Windows SBS 2008/2011
- Windows 8/8.1 (tüm sürümler)
- Windows 10 (tüm sürümler)
- Windows Server 2012/2012 R2 (tüm sürümler)

Sistem gereksinimlerinin tam bir listesi için aşağıdaki web sitesini ziyaret edin:

http://docs.trendmicro.com/tr-tr/smb/worry-free-business-security.aspx

Desteklenen Yükleme Yöntemleri

Mevcut yükleme yöntemlerinin tümü salt IPv6 veya çift yığınlı istemciler üzerine Security Agent yüklemek için kullanılabilir. Bazı yükleme yöntemleri için, Security Agent'ın başarıyla yüklenmesi için belirli gereksinimler mevcuttur.

TABLO 3-2. Yükleme Yöntemleri ve IPv6 Desteği

YÜKLEME YÖNTEMİ	GEREKSİNİMLER/HUSUSLAR
Dahili Web Sayfası ve E-posta Bildirimi Yüklemesi	Eğer salt bir IPv6 istemcisine yüklüyorsanız, Security Server çift yığınlı veya salt IPv6 olmalıdır ve ana makine adı veya IPv6 adresi URL'nin bir parçası olmalıdır. Çift yığınlı istemciler için, yükleme durum ekranında görüntülenen IPv6 adresi, **Tercihler** > **Genel Ayarlar** > **Masaüstü/Sunucu** sekmesinin **Tercih Edilen IP Adresi** bölümünde seçilen seçeneğe bağlıdır.
Güvenlik ÇAığı Tarayıcısı ve Uzaktan Yükleme	Salt bir IPv6 Security Server, salt IPv4 istemciler üzerine Security Agent yükleyemez. Benzer şekilde, salt bir IPv4 Security Server, aracıyı salt IPv6 istemciler üzerine yükleyemez.

Security Agent IP Adresleri

IPv6 adreslemesini destekleyen bir ortamda yüklenen bir Security Server, aşağıdaki Security Agent'ları yönetebilir:

- Salt IPv6 istemci üzerine yüklenen bir Security Server salt IPv6 Security Agent'ları yönetebilir.
- Çift yığınlı bir istemci üzerine yüklenen ve IPv4 ve IPv6 adreslerinin ikisi de atanmış bir Security Server, salt IPv6, çift yığınlı ve salt IPv4 Security Agent'ları yönetebilir.

Security Agent'ları yükledikten veya yükselttikten sonra, aracılar bir IP adresi kullanarak Security Server'a kaydolur.

- Salt IPv6 Security Agent'lar IPv6 adreslerini kullanarak kaydolur.
- Salt IPv4 Security Agent'lar IPv4 adreslerini kullanarak kaydolur.
- Çift yığınlı Security Agent'lar IPv4 veya IPv6 adreslerini kullanarak kaydolur. Bu aracıların, **Tercihler** > **Genel Ayarlar** > **Masaüstü/Sunucu** sekmesinde **Tercih Edilen IP Adresi** bölümünde kullanacakları IP adresini seçebilirsiniz.

Security Agent Yükleme Yöntemleri

Bu bölümde, temiz bir Security Agent yüklemesi gerçekleştirmek için farklı yükleme yöntemlerinin bir özeti sağlanmaktadır. Tüm yükleme yöntemleri, hedef istemciler üzerinde yerel yönetici haklarını gerektirir.

Security Agent'lar yüklüyorsanız ve IPv6 desteğini etkinleştirmek istiyorsanız, *Security Agent Yüklemesi ve IPv6 Desteği sayfa 3-7* kısmındaki yönergeleri okuyun.

TABLO 3-3. Yükleme Yöntemleri

YÜKLEME YÖNTEMİ/ İŞLETİM SİSTEMİ DESTEĞİ	DAĞITIM HUSUSLARI					
	WAN DAĞITIMI	MERKEZİ YÖNETİLEN	KULLANICI MÜDAHALESİ GEREKTİRİR	BT KAYNAĞI GEREKTİRİR	TOPLU DAĞITIM	TÜKETİLEN BANT GENİŞLİĞİ
Dahili Web Sayfası Tüm işletim sistemlerinde desteklenmektedir	Evet	Evet	Evet	Hayır	Hayır	Düşük, zamanlanırsa
E-posta Bildirimi Tüm işletim sistemlerinde desteklenmektedir	Evet	Evet	Evet	Hayır	Hayır	Yüksek, yüklemeler aynı anda başlatılırsa

Yükleme Yöntemi/ İşletim Sistemi Desteği	Dağıtım Hususları					
	WAN Dağıtımı	Merkezi Yönetilen	Kullanıcı Müdahalesi Gerektirir	BT Kaynağı Gerektirir	Toplu dağıtım	Tüketilen Bant Genişliği
Uzaktan Yükleme Aşağıdakiler hariç tüm işletim sistemlerinde desteklenmektedir: • Windows Vista Home Basic Edition ve Home Premium Edition • Windows XP Home Edition • Windows 7 Home Basic/ Home Premium • Windows 8/8.1 Basic • Windows 10 Home	Hayır	Evet	Hayır	Evet	Evet	Düşük, zamanlanırsa
Oturum Açma Komut Dizesi Kurulumu Tüm işletim sistemlerinde desteklenmektedir	Hayır	Evet	Hayır	Evet	Evet	Yüksek, yüklemeler aynı anda başlatılırsa

Yükleme Yöntemi/ İşletim Sistemi Desteği	Dağıtım Hususları					
	WAN Dağıtımı	Merkezi Yönetilen	Kullanıcı Müdahalesi Gerektirir	BT Kaynağı Gerektirir	Toplu dağıtım	Tüketilen Bant Genişliği
Client Packager Tüm işletim sistemlerinde desteklenmektedir	Evet	Hayır	Evet	Evet	Hayır	Düşük, zamanlanırsa
Trend Micro Güvenlik Açığı Tarayıcısı (TMVS) Aşağıdakiler hariç tüm işletim sistemlerinde desteklenmektedir: • Windows Vista Home Basic Edition ve Home Premium Edition • Windows XP Home Edition • Windows 7 Home Basic/ Home Premium • Windows 8/8.1 Basic • Windows 10 Home	Hayır	Evet	Hayır	Evet	Evet	Düşük, zamanlanırsa

Tek sahada dağıtım için ve BT ilkelerinin sıkı uygulandığı kuruluşlarda, BT yöneticileri **Uzaktan Yükleme** veya **Oturum Açma Dizesi Kurulumu** kullanarak dağıtımı seçebilir.

BT politikalarının daha esnek bir şekilde uygulandığı kuruluşlarda, Trend Micro Security Agent'ların **Dahili Web sayfası** kullanılarak yüklenmesini önerir. Ancak bu yöntemi kullanmak, Security Agent'ı yükleyecek son kullanıcıların yönetici ayrıcalığına sahip olmasını gerektirir.

Uzaktan Yükleme, Active Directory kullanan ağlar için etkilidir. Ağınız Active Directory kullanmıyorsa, Dahili Web Sayfasını kullanın.

Dahili Web Sayfasından Yükleme

Başlamadan önce

Dahili Web Sayfasından yükleme yapmak için aşağıdakiler gereklidir:

KONTROL EDİLECEK ÖĞE	GEREKSİNİM
Security Server	Security Server aşağıdakiler üzerine yüklenmelidir: • Windows XP, Vista, 7, 8, 8.1, Server 2003/2008/2008 R2/2012/2012 R2 veya SBS 2003/2008/2011 • Internet Information Server (IIS) 6.0, 7.0, 7.5, 8.0, 8.5 veya Apache 2.0.6x ile birlikte
Hedef istemci	• Hedef istemcide Internet Explorer 7.0 veya üzeri bulunmalıdır. • Kullanıcılar istemcide oturum açmak için bir yönetici hesabı kullanmalıdır. **Nota** Hedef istemci Windows 7 çalıştırıyorsa, önce yerleşik yönetici hesabını etkinleştirin. Windows 7 varsayılan olarak yerleşik yönetici hesabını devre dışı bırakmaktadır. Daha fazla bilgi için, Microsoft destek sitesine başvurun (http://technet.microsoft.com/en-us/library/dd744293%28WS.10%29.aspx).

KONTROL EDİLECEK ÖĞE	GEREKSİNİM
Windows XP, 7, 8, 8.1, 10, Vista, Server 2003, 2008, 2008 R2, 2012, 2012 R2 veya SBS 2003, 2008, 2011 çalıştıran hedef istemci	Kullanıcılar aşağıdaki adımları gerçekleştirmelidir: 1. Internet Explorer'ı başlatın ve Security Server URL'sini (örn. https://<Security Server adı>:4343/SMB/console/html/client) güvenilen siteler listesine ekleyin. Windows XP üzerinde, **Araçlar** > **Internet Seçenekleri** > **Güvenlik** sekmesine giderek, **Güvenilen Siteler** simgesini seçerek ve **Siteler** öğesine tıklayarak listeye erişin. 2. **ActiveX denetimlerinin otomatik sorulması** özelliğini etkinleştirmek için Internet Explorer güvenlik ayarlarını değiştirin. Windows XP üzerinde, **Araçlar** > **Internet Seçenekleri** > **Güvenlik** sekmesine gidin ve **Özel seviye** öğesine tıklayın.
Windows Vista çalıştıran hedef istemci	Kullanıcılar Korunan Modu etkinleştirmelidir. Korunan Modu etkinleştirmek için, Internet Explorer'da **Araçlar** > **Internet Seçenekleri** > **Güvenlik** sekmesine tıklayın.
IPv6	Salt IPv4, salt IPv6 ve çift yığınlı istemcilerden oluşan karışık bir ortamınız mevcutsa, Security Server'ın hem IPv4 hem de IPv6 adresleri olmalıdır, böylece tüm istemciler Security Server üzerindeki Dahili Web Sayfası'na bağlanabilir.

Dahili Web Sayfasından Security Agent'ı yüklemek için, kullanıcılara aşağıdaki talimatları gönderin. E-posta üzerinden bir yükleme bildirimi göndermek için, bkz. *E-posta Bildirimiyle Yükleme sayfa 3-33*.

Prosedür

1. Bir yönetici hesabını kullanarak istemcide oturum açın.
2. Bir Internet Explorer penceresi açın ve aşağıdakilerden birini girin:
   - SSL ile Security Server:

     https://<Security Server adı veya IP Adresi>:4343/SMB/console/html/client
   - SSL olmadan Security Server:

     http://<Security Server adı veya IP Adresi>:8059/SMB/console/html/client

3. Security Agent yüklemesini başlatmak için **Şimdi Yükle** öğesine tıklayın.

   Yükleme başlayacaktır. İstemde bulunulduğunda ActiveX denetimi yüklemesine izin verin. Yükleme sonrasında Windows görev çubuğunda Security Agent simgesi belirir.

Nota

Windows görev çubuğu üzerinde görüntülenen simgelerin bir listesi için, bkz. *Security Agent Durumunu Kontrol Etme sayfa A-2*.

Bundan sonra ne yapılacak

Kullanıcılar Dahili Web Sayfası üzerinden yükleme yapamadıklarını bildiriyorsa, aşağıdaki yöntemleri deneyin.

- Ping ve telnet kullanarak istemci-sunucu iletişiminin var olduğunu doğrulayın.
- İstemcide TCP/IP'nin etkinleştirildiğini ve düzgün şekilde yapılandırıldığını doğrulayın.
- İstemci-sunucu iletişimi için proxy sunucu kullanıyorsanız, proxy ayarlarının doğru yapılandırılıp yapılandırılmadığını denetleyin
- Web tarayıcısında, Trend Micro eklentilerini ve gözatma geçmişini silin.

Oturum Açma Komut Dizesi Kurulumu ile Yükleme

Oturum Açma Komut Dizesi Kurulumu, ağ oturumu açtıklarında korumasız istemcilerin Security Agent yükleme işlemini otomatikleştirir. Oturum Açma Komut Dizesi Kurulumu, sunucu oturum açma komut dosyasına AutoPcc.exe adlı bir program ekler.

AutoPcc.exe korumasız istemcilere Security Agent kurar ve program dosyalarını ve bileşenleri günceller. İstemcilerin, oturum açma komut dizesi üzerinden AutoPcc'yi kullanabilmesi için etki alanının parçası olmalıdır.

Mevcut bir oturum açma komut dizeniz varsa, Oturum Açma Komut Dizesi Kurulumu, AutoPcc.exe dosyasını yürüten bir komut ekler. Aksi takdirde, ofcscan.bat isimli bir toplu iş dosyası oluşturur, bu dosya AutoPcc.exe dosyasını çalıştıran komutu içerir.

Oturum Açma Komut Dosyası Kurulumu, komut dosyasının sonuna şunu ekler:

\\<Server_name>\ofcscan\autopcc

burada:

- <Server_name>, Security Server bilgisayarının bilgisayar adı veya IP adresidir.
- "ofcscan" Security Server üzerindeki paylaşılan klasör adıdır.
- "autopcc" Security Agent'ı yükleyen autopcc yürütülebilir dosyasına bağlantıdır.

Tüm Windows Server sürümlerinde oturum açma komut dizesi (net oturum açma paylaşımlı dizini üzerinden):

\\Windows server\system drive\windir\sysvol\domain\scripts\ofcscan.bat

---

Prosedür

1. Sürücü yüklemesini çalıştırmak için kullandığınız bilgisayarda, <Security Server yükleme klasörü>\PCCSRV\Admin yolunu açın.
2. SetupUsr.exe öğesine çift tıklayın.

   Oturum Açma Komut Dizesi Kurulumu yardımcı programı yüklenir. Konsol, ağ üzerindeki tüm etki alanlarını gösteren bir ağaç görüntüler.
3. Oturum açma komut dizesini değiştirmek istediğiniz sunucuyu konumlandırın, seçin ve **Seç** öğesine tıklayın. Sunucunun birincil etki alanı kontrolörü olduğundan ve sunucuda yönetici erişimine sahip olduğunuzdan emin olun.

   Oturum Açma Komut Dosyası Kurulumu bir kullanıcı adı ve parola belirlemenizi ister.
4. Kullanıcı adını ve parolayı girin. Devam etmek için **TAMAM** öğesine tıklayın.

   Kullanıcı Seçimi ekranı belirir. **Kullanıcılar** listesi, sunucuda oturum açan kullanıcıların profillerini gösterir. **Seçilen kullanıcılar** listesi, oturum açma komut dizesini değiştirmek istediğiniz kullanıcı profillerini gösterir.
5. Bir kullanıcı profili için oturum açma komut dizesini değiştirmek için, Kullanıcılar listesinden kullanıcı profilini seçin ve ardından **Ekle** öğesine tıklayın.
6. Tüm kullanıcıların oturum açma komut dizesini değiştirmek için, **Tümünü Ekle** öğesine tıklayın.

7. Daha önce seçtiğiniz bir kullanıcını profilini hariç tutmak için, adını **Seçilen kullanıcılar** listesinden seçin ve **Sil** öğesine tıklayın.
8. Seçimlerinizi sıfırlamak için, **Tümünü Sil** öğesine tıklayın.
9. Tüm hedef kullanıcı profilleri **Seçilen kullanıcılar** liestesindeyken, **Uygula** öğesine tıklayın.

   Bir ileti, sunucu oturum açma komut dizelerini başarıyla değiştirdiğinizi belirtir.
10. **TAMAM** öğesine tıklayın.

    Oturum Açma Komut Dizesi Kurulumu, başlangıç ekranına döner.
11. Oturum Açma Komut Dizesi Kurulumunu kapatmak için, **Çık** öğesine tıklayın.

Client Packager ile Yükleme

Client Packager, kullanıcılara CD-ROM gibi geleneksel ortamları kullanarak gönderebileceğiniz bir yükleme paketi oluşturur. Kullanıcılar, Security Agent'ı yüklemek veya yükseltmek ve bileşenleri güncellemek için istemci üzerinde paketi çalıştırır.

Client Packager özellikle şu durumlarda faydalıdır:

- Security Agent'ın düşük bant genişliğine sahip ofislerdeki istemcilere dağıtımını yaparken.
- Ortamınızda Internet'e bağlanmaya yönelik kısıtlamalar varsa, Internet bağlantısının olmaması veya kapalı LAN durumunda.

Client Packager kullanılarak yüklenen Security Agent'lar paketin oluşturulduğu sunucuya rapor verirler.

Prosedür

1. Security Server bilgisayarında <Sunucu yükleme klasörü>\PCCSRV\Admin\Utility \ClientPackager kısmına gözatın.
2. ClnPack.exe dosyasına çift tıklayın.

   Client Packager konsolu açılır.

3. Paketi oluşturmak istediğiniz işletim sistemini seçin. Paketi sadece işletim sistemi türünü çalıştıran istemcilere dağıtın. Başka işletim sistemi türüne dağıtım için başka bir paket oluşturun.

4. Paket için tarama yöntemini seçin.

   Tarama yöntemleri hakkında ayrıntılar için, bkz. *Tarama Yöntemleri sayfa 5-3*.

   Pakette içerilen bileşenler seçtiğiniz tarama yöntemine bağlıdır. Smart scan için, Virüs Kalıbı hariç tüm bileşenler dahil olacaktır. Geleneksel tarama için, Smart Scan Aracı Kalıbı hariç tüm bileşenler dahil edilecektir.

5. Oluşturmak istediğiniz paket türünü seçin.

   TABLO 3-4. İstemci Paket Türleri

PAKETLEYİCİ TÜRÜ	AÇIKLAMA
Kurulum	Paketi, Microsoft Yükleme Paketi formatına uygun olarak bir MSI dosyası olarak oluşturmak için **Kurulum** öğesini seçin. Paket, Security Server'da mevcut olan bileşenlerle Security Agent programını yükler. Hedef istemcide yüklenmiş daha önceki Security Agent sürümü varsa ve yükseltmek istiyorsanız, MSI dosyasını aracıyı yöneten Security Server'da oluşturun. Aksi takdirde, aracı yükseltilmeyecektir.
Güncelleme	Security Server'da mevcut olan bileşenleri içeren bir paket oluşturmak için **Güncelle** öğesini seçin. Bu paket, yürütülebilir bir dosya olarak oluşturulacaktır. Security Agent'ın yüklü olduğu bilgisayarda bileşenlerin güncellenmesinde sorunlar varsa bu paketi kullanın.

6. İstemcide arkaplanda yüklenen, istemci kullanıcısı tarafından farkedilmeyen ve bilgi durum penceresi görüntülemeyen bir paket oluşturmak için **Sessiz mod** öğesine tıklayın. Paketi istemciye uzaktan dağıtmayı planlıyorsanız bu seçeneği etkinleştirin.

7. Security Agent'ı yüklemeden önce istemciyi tehditler için taramak istemiyorsanız **Ön taramayı devre dışı bırak (sadece yeni yükleme)** öğesine tıklayın. Bunu istemcide tehdit bulunmadığından eminseniz gerçekleştirin.

   Ön tarama etkinleştirilirse, Kurulum, aşağıdakiler dahil bilgisayarın en çok güvenlik açığı olabilecek alanlarını virüs/kötü amaçlı yazılım için tarayacaktır:

- Önyükleme alanı ve önyükleme dizini (önyükleme virüsleri için)
- Windows klasörü
- Program dosyaları klasörü

8. **Kaynak dosyası** yanında, ofcscan.ini dosyasının konumunun doğru olduğundan emin olun. Yolu değiştirmek için, ofcscan.ini dosyasına gözatmak üzere (...) öğesine tıklayın. Varsayılan olarak bu dosya şu konumdadır: <Server yükleme klasörü>\PCCSRV.

9. Çıktı dosyasında, (...) öğesine tıklayın, paketi nerede oluşturmak istediğinizi belirtin ve paket dosya adını girin (örneğin, `ClientSetup.exe`).

10. **Oluştur** öğesine tıklayın.

    Client Packager paketi oluşturduktan sonra, "Paket başarıyla oluşturuldu" iletisi belirir. Paketi önceki adımda belirttiğiniz dizinde konumlandırın.

Bundan sonra ne yapılacak

Paketi istemcilere dağıtın.

İstemci Gereksinimleri:

- Paket için tarama yöntemi geleneksel tarama ise 1GB, smart scan ise 500MB boş disk alanı
- Windows Installer 3.0 (MSI paketini çalıştırmak için)

Paket Dağıtım Yönergeleri:

- Paketi kullanıcılara gönderin ve dosyaya (.msi veya .exe) çift tıklayarak paketi çalıştırmalarını isteyin..

Nota

Paketi sadece paketin oluşturulduğu sunucuya rapor verecek Security Agent'a sahip kullanıcılara gönderin.

- .exe paketini Windows Vista, 7, 8/8.1, 10, Server 2008, SBS 2011, Server 2012 veya Server 2012 R2 çalıştıran bilgisayarlarda çalıştıracak kullanıcılarınız varsa, onlara.exe dosyasına sağ tıklamalarını ve **Yönetici olarak çalıştır**'ı seçmelerini söyleyin.
- Active Directory kullanıyorsanız, her kullanıcının kendi başlarına Security Agent kurmalarını gerektirmek yerine, Security Agent'ı tüm istemcilere .msi dosyasıyla otomatik olarak eşzamanlı dağıtabilirsiniz. **Kullanıcı Yapılandırması** yerine **Bilgisayar Yapılandırması** kullanın, böylece istemcide hangi kullanıcının oturum açtığından bağımsız olarak Security Agent yüklenebilir.
- Yeni yüklenmiş bir Security Agent, Security Server'a bağlanamazsa, Security Agent varsayılan ayarları koruyacaktır. Security Agent, Security Server'a bağlandığında, web konsolundaki grubu için ayarları edinecektir.
- Security Agent'ı Client Packager ile yükseltmede sorun yaşıyorsanız, Trend Micro öncelikle Security Agent'ın önceki sürümünü kaldırmanızı, ardından da yeni sürümü yüklemenizi önerir. Kaldırma talimatları için, bkz. *Aracıları Kaldırma sayfa 3-39*.

Uzaktan Yükleme ile Yükleme

Başlamadan önce

Security Agent'ı ağa bağlı bir veya daha çok istemciye uzaktan yükleyin.

Uzaktan Yükleme ile yüklemek için aşağıdakiler gereklidir:

Kontrol Edilecek Öğe	Gereksinim
Hedef istemci	• Her hedef istemcide oturum açmak için bir yönetici hesabı kullanın.

KONTROL EDİLECEK ÖĞE	GEREKSİNİM
	Nota Hedef istemci Windows 7 çalıştırıyorsa, önce yerleşik yönetici hesabını etkinleştirin. Windows 7 varsayılan olarak yerleşik yönetici hesabını devre dışı bırakmaktadır. Daha fazla bilgi için, Microsoft destek sitesine başvurun (http://technet.microsoft.com/en-us/library/dd744293%28WS.10%29.aspx). • Hedef istemcide Security Server kurulu olmamalıdır. Uzaktan Yükleme, Security Server çalıştırmakta olan bir bilgisayara Security Agent yüklemez.
Windows Vista, 7, 8/8.1, 10, Server 2008, 2012/2012 R2 veya SBS 2011 çalıştıran hedef istemci	Aşağıdaki görevleri gerçekleştirin: **Nota** Windows 8/8.1 veya 10 üzerinde uzaktan yükleme gerçekleştirirken, hedef istemcide oturum açmak için Microsoft hesabı kullanılamaz. 1. İstemcide Dosya ve Yazıcı Paylaşımı'nı geçici olarak etkinleştirin. **Nota** Şirketin güvenlik ilkesi Windows Güvenlik Duvarı'nı devre dışı bırakmaksa, Uzak Kayıt Defteri hizmetini başlatmak için adım 2'ye ilerleyin. a. Denetim Masası'nda Windows Güvenlik Duvarı'nı açın. b. **Programa Windows Güvenlik Duvarı aracılığıyla izin ver** öğesine tıklayın. Yönetici parolasını ve onayını girmeniz istenirse, parolayı girin ve onayı sağlayın. Windows Güvenlik Duvarı Ayarları penceresi görünür. c. **Program veya bağlantı noktası listesi** altında **Kural dışı durumlar** sekmesi içinde, **Dosya ve Yazıcı Paylaşımı** onay kutusunun seçili olduğundan emin olun. d. **TAMAM** öğesine tıklayın.

KONTROL EDİLECEK ÖĞE	GEREKSİNİM
	2. Kullanıcı Hesabı Denetimini Devre Dışı Bırak. **Nota** Windows 8/8.1, 10 veya 2012/2012 R2 için: Şu kayıt defteri anahtarını değiştirerek Kullanıcı Hesabı Denetimini açın: [HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System] "EnableLUA"=dword:00000000. 3. Uzak Kayıt Defteri hizmetini geçici olarak başlatın. a. Microsoft Yönetim Konsolu'nu açın. **Nota** Microsoft Yönetim Konsolu'nu açmak için Çalıştır penceresine `services.msc` yazın. b. **Uzak Kayıt Defteri** öğeisne sağ tıklayın ve **Başlat** seçin. 4. Gerekirse, Security Agent'ları Windows Vista, 7, 8/8.1 veya 10 Vista istemcisine yükledikten sonra orijinal ayarlara geri dönün.
Windows XP çalıştıran hedef istemci	İstemcide Basit Dosya Paylaşımı'nı geçici olarak devre dışı bırakın. 1. Windows Gezgini'ni açın. 2. **Araçlar** > **Klasör Seçenekleri**'ne tıklayın 3. Görünüm sekmesinde, **Basit Dosya Paylaşımı (Önerilir)** öğesini temizleyin. 4. **Uygula** öğesine tıklayın.
IPv6	Çift yığınlı bir Security Server, Security Agent'ı herhangi bir istemciye yükleyebilir. Salt bir IPv6 Security Server, Security Agent'ı sadece salt IPv6 veya çift yığınlı istemcilere yükleyebilir.

Prosedür

1. Web konsolundan **Güvenlik Ayarları** > **Bilgisayar Ekle** kısmına gidin.

   Yeni bir ekran açılır.

2. **Bilgisayar Türü** bölümünden **Masaüstü veya Sunucu** seçin.
3. **Yöntem** bölümünden **Uzaktan Yükleme** öğesini seçin.
4. **İleri** öğesine tıklayın.

   Yeni bir ekran belirir.
5. **Gruplar ve Bilgisayarlar** kutusundaki bilgisayar listesinden bir istemci seçin ve ardından **Ekle** öğesine tıklayın İstemci için kullanıcı adı ve parola istemi görünür.
6. Kullanıcı adınızı ve parolanızı girin ve ardından **Oturum Aç** öğesine tıklayın. İstemci, **Seçilen Bilgisayarlar** liste kutusunda belirir.
7. Liste, tüm istemcileri **Seçilen Bilgisayar** liste kutusunda görüntüleyinceye kadar bu adımları tekrar edin.
8. **Yükle** öğesine tıklayın.

   Bir onay kutusu görünür.
9. Aracıyı istemciye yüklemek istediğinizi onaylamak için **Evet** öğesine tıklayın

   Program, Security Agent dosyalarını istemcilerin her birine kopyalarken bir ilerleme ekranı görünür.

   Security Server bir istemciye yüklemeyi tamamladığında, yükleme durumu **Seçilen Bilgisayarlar** liste kutusunun **Durum** alanında görünür ve istemci adı yeşil bir onay işaretiyle birlikte görünür.

Bundan sonra ne yapılacak

Uzaktan yükleme ile yükleme başarısız olursa, şu görevleri gerçekleştirin:

- Ping ve telnet kullanarak istemci-sunucu iletişiminin var olduğunu doğrulayın.
- İstemcide TCP/IP'nin etkinleştirildiğini ve düzgün şekilde yapılandırıldığını doğrulayın.
- İstemci-sunucu iletişimi için proxy sunucu kullanıyorsanız, proxy ayarlarının doğru yapılandırılıp yapılandırılmadığını kontrol edin.
- Web tarayıcısında, Trend Micro eklentilerini ve gözatma geçmişini silin.

Güvenlik Açığı Tarayıcısıyla Yükleme

Başlamadan önce

Yüklenen antivirüs çözümlerini algılamak için güvenlik açığı taramalarını çalıştırın, korumasız istemcileri arayın ve istemcilere Security Agent'ları yükleyin.

Güvenlik Açığı Tarayıcısı ile yüklemek için, aşağıdakiler gereklidir:

KONTROL EDİLECEK ÖĞE	GEREKSİNİM
Güvenlik açığı nerede çalıştırılmalı	Güvenlik Açığı Tarayıcısını, Security Server üzerinde veya ağ üzerindeki herhangi bir istemci üzerinde çalıştırabilirsiniz. İstemci Terminal Server çalıştırmıyor olmalıdır.
Hedef istemci	• Hedef istemcide Security Server kurulu olmamalıdır. Güvenlik Açığı Tarayıcısı, Security Server çalıştırmakta olan bir bilgisayara Security Agent yüklemez. • Kullanıcılar istemcide oturum açmak için bir yönetici hesabı kullanmalıdır. **Nota** Hedef istemci Windows 7 çalıştırıyorsa, önce yerleşik yönetici hesabını etkinleştirin. Windows 7 varsayılan olarak yerleşik yönetici hesabını devre dışı bırakmaktadır. Daha fazla bilgi için, Microsoft destek sitesine başvurun (http://technet.microsoft.com/en-us/library/dd744293%28WS.10%29.aspx).

Güvenlik açığı taramalarını çalıştırmanın çeşitli yolları vardır.

- *Manuel bir Güvenlik Açığı Taramasını Çalıştırma sayfa 3-23*
- *Bir DHCP Taramasını Çalıştırma sayfa 3-25*
- *Zamanlanmış bir Güvenlik Açığı Taramasını Yapılandırma sayfa 3-27*

Manuel bir Güvenlik Açığı Taramasını Çalıştırma

Güvenlik açığı taramalarını talep üzerine çalıştırın.

Prosedür

1. Güvenlik Açığı Tarayıcısını başlatın.

GÜVENLİK AÇIĞI TARAYICISINI BAŞLATMAK İÇİN:	ADIMLAR
Security Server	a. <Server yükleme klasörü>\PCCSRV\Admin\Utility\TMVS adresine gidin. b. TMVS.exe'ye çift tıklayın.
Ağ üzerinde bir istemci	a. Security Server üzerinde <Server yükleme klasörü>\PCCSRV\Admin\Utility kısmına gidin. b. TMVS klasörünü diğer istemciye kopyalayın. c. Diğer istemci üzerinde, TMVS klasörünü açın ve TMVS.exe dosyasına çift tıklayın.

2. **Manuel Tarama** kısmına gidin.
3. Kontrol etmek istediğiniz aracıların IP adres aralığını girin.
   a. Bir IPv4 adres aralığı girin.

   Nota

   Güvenlik Açığı Tarayıcısı, salt IPv4 veya çift-yığınlı istemci üzerinde çalışıyorsa, sadece IPv4 adres aralığını sorgulayabilir. Güvenlik Açığı Tarayıcısı sadece sınıf B IP adresi aralığını desteklemektedir, örneğin 168.212.1.1 ila 168.212.254.254.

   b. Bir IPv6 adres aralığı için, IPv6 önekini ve uzunluğunu girin.

   Nota

   Güvenlik Açığı Tarayıcısı, salt IPv6 veya çift-yığınlı istemci üzerinde çalışıyorsa, sadece IPv6 adres aralığını sorgulayabilir.
4. **Ayarlar** öğesine tıklayın.

   Ayarlar ekranı görünür.

5. Güvenlik açığı tarama ayarlarını yapılandırın. Ayrıntılar için, bkz. *Güvenlik Açığı Tarama Ayarları sayfa 3-29*.

6. **TAMAM** öğesine tıklayın.

   Ayarlar ekranı kapanır.

7. **Başlat** öğesine tıklayın.

   Güvenlik açığı tarama sonuçları **Manuel Tarama** sekmesi altındaki **Sonuçlar** tablosunda belirir.

   Nota

   Bilgisayar, Windows Server 2008 çalıştırıyorsa, MAC adresi bilgisi **Sonuçlar** tablosunda görüntülenmez.

8. Sonuçları bir virgülle ayrılan değer (CSV) dosyasına kaydetmek için, **Dışa Aktar** öğesine tıklayın, dosyayı kaydetmek istediğiniz klasörü konumlandırın, dosya adını girin ve **Kaydet** öğesine tıklayın.

Bir DHCP Taramasını Çalıştırma

Bir DHCP sunucusundan IP adresleri isteyen istemcilerde güvenlik açığı taraması çalıştırın.

Güvenlik Açığı Tarayıcı, DHCP sunucusunun DHCP talepleri için dinleme bağlantı noktası olan bağlantı noktası 67'yi dinler. Bir istemciden bir DHCP talebi algılarsa, güvenlik açığı taraması istemci üzerinde çalışır.

Nota

Güvenlik Açığı Tarayıcı, Windows Server 2008 veya Windows 7 üzerinde başlatılmışsa, DHCP taleplerini algılayamaz.

Prosedür

1. Aşağıdaki klasör altında bulunan TMVS.ini dosyasındaki DHCP ayarlarını yapılandırın: <Server yükleme klasörü>\PCCSRV\Admin\Utility\TMVS.

TABLO 3-5. TMVS.ini Dosyasındaki DHCP Ayarları

AYAR	AÇIKLAMA
DhcpThreadNum=x	DHCP modu için tehdit numarasını belirtin. Minimumu 3, maksimumu 100'dür. Varsayılan değer 3'tır.
DhcpDelayScan=x	Bu, talepte bulunan bilgisayarda yüklenmiş antivirüs yazılımı kontrolü yapmadan önce saniye olarak gecikme süresidir. Minimumu 0 (beklemez), maksimumu 600'dür. Varsayılan değer 60'tır.
LogReport=x	0 günlüğe almayı devre dışı bırakır, 1 etkinleştirir. Güvenlik Açığı Tarayıcısı, tarama sonuçlarını WFBS sunucusuna gönderir. Günlükler, web konsolu üzerinde **Sistem Etkinlik Günlükleri** ekranında görüntülenir.
OsceServer=x	Bu, WFBS sunucusunun IP adresi veya DNS adıdır.
OsceServerPort=x	Bu, WFBS sunucusunun web sunucu bağlantı noktasıdır.

2. Güvenlik Açığı Tarayıcısını başlatın.

GÜVENLİK AÇIĞI TARAYICISINI BAŞLATMAK İÇİN:	ADIMLAR
Security Server	a. <Server yükleme klasörü>\PCCSRV\Admin\Utility\TMVS adresine gidin. b. TMVS.exe'ye çift tıklayın.
Ağ üzerinde bir istemci	a. Security Server üzerinde <Server yükleme klasörü>\PCCSRV\Admin\Utility kısmına gidin. b. TMVS klasörünü diğer istemciye kopyalayın. c. Diğer istemci üzerinde, TMVS klasörünü açın ve TMVS.exe dosyasına çift tıklayın.

3. **Manuel Tarama** bölümünün yanında **Ayarlar** öğesine tıklayın.

Ayarlar ekranı görünür.

4. Güvenlik açığı tarama ayarlarını yapılandırın. Ayrıntılar için, bkz. *Güvenlik Açığı Tarama Ayarları sayfa 3-29*.

5. **TAMAM** öğesine tıklayın.

   Ayarlar ekranı kapanır.

6. **Sonuçlar** tablosunda, **DHCP Taraması** sekmesine tıklayın.

   Nota

   DHCP Taraması sekmesi, Windows Server 2008 ve Windows 7 çalıştırılan bilgisayarlarda mevcut değildir.

7. **DHCP Başlat**'ı tıklatın.

   Güvenlik Açığı Tarayıcısı DHCP isteklerini dinlemeye ve istemcilerde ağda oturum açtıkça güvenlik açığı kontrolleri gerçekleştirmeye başlar.

8. Sonuçları bir virgülle ayrılan değer (CSV) dosyasına kaydetmek için, **Dışa Aktar** öğesine tıklayın, dosyayı kaydetmek istediğiniz klasörü konumlandırın, dosya adını girin ve **Kaydet** öğesine tıklayın.

Zamanlanmış bir Güvenlik Açığı Taramasını Yapılandırma

Güvenlik açığı taramaları, bir programa göre otomatik olarak çalışır.

Prosedür

1. Güvenlik Açığı Tarayıcısını başlatın.

Güvenlik Açığı Tarayıcısını Başlatmak İçin:	Adımlar
Security Server	a. <Server yükleme klasörü>\PCCSRV\Admin\Utility\TMVS adresine gidin. b. TMVS.exe'ye çift tıklayın.

GÜVENLİK AÇIĞI TARAYICISINI BAŞLATMAK İÇİN:	ADIMLAR
Ağ üzerinde bir istemci	a. Security Server üzerinde <Server yükleme klasörü>\PCCSRV\Admin\Utility kısmına gidin. b. TMVS klasörünü diğer istemciye kopyalayın. c. Diğer istemci üzerinde, TMVS klasörünü açın ve TMVS.exe dosyasına çift tıklayın.

2. **Zamanlanmış Tarama** kısmına gidin.
3. **Ekle/Düzenle** öğesine tıklayın.

   Zamanlanmış Tarama ekranı belirir.
4. Zamanlanmış güvenlik açığı taraması için bir ad girin.
5. Kontrol etmek istediğiniz bilgisayarların IP adres aralığını girin.
   a. Bir IPv4 adres aralığı girin.

   Nota

   Güvenlik Açığı Tarayıcısı, kullanılabilir bir IPv4 adresi olan, salt IPv4 veya çift-yığınlı istemci üzerinde çalışıyorsa, sadece IPv4 adres aralığını sorgulayabilir. Güvenlik Açığı Tarayıcısı sadece sınıf B IP adresi aralığını desteklemektedir, örneğin 168.212.1.1 ila 168.212.254.254.

   b. Bir IPv6 adres aralığı için, IPv6 önekini ve uzunluğunu girin.

   Nota

   Güvenlik Açığı Tarayıcısı, kullanılabilir bir IPv6 adresi olan, salt IPv6 veya çift-yığınlı istemci üzerinde çalışıyorsa, sadece IPv6 adres aralığını sorgulayabilir.
6. Başlatma zamanını 24 saatlik saat biçimini kullanarak belirtin ve ardından taramanın ne kadar sık çalışacağını seçin. Günlük, haftalık veya aylık seçeneklerinden birini seçin.
7. Manuel güvenlik açığı tarama ayarlarını yapılandırdıysanız ve kullanmak istiyorsanız **Mevcut ayarları kullan** seçeneğini seçin. Manuel güvenlik açığı tarama ayarları

hakkında ayrıntılar için, bkz. *Manuel bir Güvenlik Açığı Taramasını Çalıştırma sayfa 3-23*.

Manuel güvenlik açığı tarama ayarlarını belirtmediyseniz veya başka bir ayar seti kullanmak istemiyorsanız, **Ayarları değiştir** seçin ve adından **Ayarlar** öğesine tıklayın. **Ayarlar** ekranı görünür. Tarama ayarlarını yapılandırın ve ardından **TAMAM** öğesine tıklayın. Ayrıntılar için, bkz. *Güvenlik Açığı Tarama Ayarları sayfa 3-29*.

8. **TAMAM** öğesine tıklayın.

   Zamanlanmış Tarama ekranı kapanır. Oluşturduğunuz zamanlanmış güvenlik açığı taraması, **Zamanlanmış Tarama** bölümünün altında belirir. Bildirimleri etkinleştirdiyseniz, Güvenlik Açığı Tarayıcısı size zamanlanmış güvenlik açığı tarama sonuçlarını gönderecektir.

9. Zamanlanmış güvenlik açığı taramasını derhal yürütmek için, **Şimdi Çalıştır** öğesine tıklayın.

   Güvenlik açığı tarama sonuçları **Zamanlanmış Tarama** sekmesi altındaki **Sonuçlar** tablosunda belirir.

Nota

Bilgisayar, Windows Server 2008 çalıştırıyorsa, MAC adresi bilgisi **Sonuçlar tablosunda** görüntülenmez.

---

10. Sonuçları bir virgülle ayrılan değer (CSV) dosyasına kaydetmek için, **Dışa Aktar** öğesine tıklayın, dosyayı kaydetmek istediğiniz klasörü konumlandırın, dosya adını girin ve **Kaydet** öğesine tıklayın.

11. Zamanlanmış güvenlik açığı taramalarının çalışmasını durdurmak için, **Zamanlanmış Taramalar** bölümüne gidin, zamanlanmış taramayı seçin ve **Sil** öğesine tıklayın.

Güvenlik Açığı Tarama Ayarları

Güvenlik açığı taramalarını çalıştırırken aşağıdaki ayarları yapılandırın. Farklı güvenlik açığı taramaları hakkında ayrıntılar için, bkz. *Güvenlik Açığı Tarayıcısıyla Yükleme sayfa 3-23*.

Ayarlar	Açıklamalar ve Talimatlar
Ürün Sorgusu	Güvenlik Açığı Tarayıcısı hedef istemcilerdeki güvenlik yazılımı mevcudiyetini kontrol edebilir. 1. Kontrol edilecek güvenlik yazılımını seçin. 2. Güvenlik Açığı Tarayıcısı, yazılımı kontrol etmek için ekranda gösterilen varsayılan bağlantı noktalarını kullanır. Yazılım yöneticisi varsayılan bağlantı noktalarını değiştirdiyse, gerekli değişiklikleri yapın, yoksa Güvenlik Açığı Tarayıcısı yazılımı algılamayacaktır. 3. Norton Antivirus Corporate Edition için, zaman aşımı ayarlarını **Ayarlar** öğesine tıklayarak değiştirebilirsiniz.
	Diğer Ürün Sorgu Ayarları Güvenlik Açığı Tarayıcısının aynı anda güvenlik yazılımı kontrolü yapacağı istemci sayısını ayarlayın. 1. <Sunucu yükleme klasörü>\PCCSRV\Admin\Utility\TMVS kısmına gidin ve Notepad gibi bir metin düzenleyici kullanarak TMVS.ini dosyasını açın. 2. Kontrol edilen istemcilerin sayısını ayarlamak için: • Manuel güvenlik açığı taramaları için, `ThreadNumManual` değerini değiştirin. 8 ve 64 arasında bir değer belirleyin. Örneğin, Güvenlik Açığı Tarayıcısının aynı anda 60 istemciyi kontrol etmesini istiyorsanız `ThreadNumManual=60` yazın. • Zamanlanmış güvenlik açığı taramaları için, `ThreadNumSchedule` değerini değiştirin. 8 ve 64 arasında bir değer belirtin. Örneğin, Güvenlik Açığı Tarayıcısının aynı anda 50 istemciyi kontrol etmesini istiyorsanız `ThreadNumManual=50` yazın. 3. TMVS.ini dosyasını kaydedin.

Ayarlar	Açıklamalar ve Talimatlar
Açıklama Alma Ayarları	Güvenlik Açığı Tarayıcısı istemcilere "ping" atabildiği zaman, istemciler hakkında ilave bilgileri de edinebilir. Bilgileri almak için iki yöntem mevcuttur: • **Normal alım**: Hem etki alanı, hem de bilgisayar bilgilerini alır • **Hızlı alım**: Yalnızca bilgisayar adını alır
Uyarı Ayarları	Güvenlik Açığı Tarayıcısı sonuçlarını kendinize veya kuruluşunuzdaki diğer yöneticilere otomatik olarak göndermek için: 1. **Sonuçları sistem yöneticisine e-postala** seçin. 2. E-posta ayarlarını belirtmek için **Yapılandır** öğesine tıklayın. 3. **Kime** alanına, alıcının e-posta adresini yazın. 4. **Kimden** alanına, gönderenin e-posta adresini yazın. 5. **SMTP sunucusu** alanına, SMTP sunucu adresini girin. Örneğin, `smtp.company.com` yazın. SMTP sunucusu bilgileri gereklidir. 6. **Konu** alanına, ileti için yeni bir konu girin veya varsayılan konuyu kabul edin. 7. **TAMAM** öğesine tıklayın. Kullanıcılara bilgisayarlarında güvenlik yazılımı yüklü olmadığını bildirmek için: 1. **Korunmasız bilgisayarlarda bir bildirim görüntüle** seçin. 2. Ardından, bildirim iletisini yapılandırmak için **Özelleştir** düğmesine tıklayın. 3. **Bildirim İletisi** ekranında, yeni bir ileti girin veya varsayılan iletiyi kabul edin. 4. **TAMAM** ögesine tıklayın.

Ayarlar	Açıklamalar ve Talimatlar
Bir CSV Dosyası Olarak Kaydet	Güvenlik açığı tarama sonuçlarını bir virgülle ayrılan değer (CSV) dosyasına kaydedin. Bu dosya, Güvenlik Açığı Tarayıcısının başlatıldığı istemcide kaydedilecektir. Varsayılan dosya yolunu kabul edin veya tercihlerinize göre değiştirin.
Ping Ayarları	Bir istemcinin mevcut olduğunu doğrulamak ve işletim sistemini belirlemek için "ping" ayarlarını kullanın. Bu ayarlar devre dışı bırakılırsa, Güvenlik Açığı Tarayıcısı belirtilen IP adresi aralığındaki tüm IP adreslerini tarar - herhangi bir istemci tarafından kullanılmıyor olsa da - böylece tarama denemesi olması gerekenden uzun sürebilir. 1. **Paket boyutu** ve **Zaman aşımı** alanlarında, varsayılan değerleri kabul edin veya değiştirin. 2. **ICMP OS parmak izini kullanarak işletim sisteminin türünü algıla** seçin. Bu seçeneği seçerseniz, Güvenlik Açığı Tarayıcısı bir istemcinin Windows veya başka bir işletim sistemi çalıştırdığını belirler. Windows çalıştıran istemciler için, Güvenlik Açığı Tarayıcısı, Windows sürümünü tanımlayabilir.
	Diğer Ping Ayarları Güvenlik Açığı Tarayıcısının aynı anda ping atacağı istemci sayısını ayarlamak için: 1. <Sunucu yükleme klasörü>\PCCSRV\Admin\Utility\TMVS kısmına gidin ve Notepad gibi bir metin düzenleyici kullanarak TMVS.ini dosyasını açın. 2. `EchoNum` için değeri değiştirin. 1 ve 64 arasında bir değer belirleyin. Örneğin, Güvenlik Açığı Tarayıcısının aynı anda 60 bilgisayara ping atmasını istiyorsanız `EchoNum=60` yazın. 3. TMVS.ini dosyasını kaydedin.

Ayarlar	Açıklamalar ve Talimatlar
Security Server ayarları	1. Güvenlik Açığı Tarayıcısının tarayacağı istemcilere Security Agent yüklemek için, **Korunmasız bilgisayarlara otomatik olarak Security Agent yükle** seçin. 2. Security Server ana makine adını veya IPv4/IPv6 adresini ve bağlantı noktası numarasını girin. Güvenlik Açığı Tarayıcısı tarafından yüklenen Security Agent'lar, bu sunucuya rapor verecektir. 3. **Hesap Yükle** öğesine tıklayarak istemcilerde oturum açarken yönetici haklarını kullanmayı yapılandırın. **Hesap Bilgisi** ekranında, bir kullanıcı adı ve parola girin ve **TAMAM** öğesine tıklayın.

E-posta Bildirimiyle Yükleme

Bu yükleme yöntemini, yükleyiciye bağlantı içeren bir e-posta iletisi göndermek için kullanın.

Prosedür

1. Web konsolundan **Güvenlik Ayarları** > **Bilgisayar Ekle** kısmına gidin.

   Yeni bir ekran açılır.

2. **Bilgisayar Türü** bölümünden **Masaüstü veya Sunucu** seçin.

3. **Yöntem** bölümünden **E-posta bildirimiyle yükle** seçin.

4. **İleri** öğesine tıklayın.

   Yeni bir ekran belirir.

5. E-postanın konusunu ve alıcıları girin.

6. **Uygula** öğesine tıklayın. Varsayılan e-posta istemcisi; alıcılar, konu ve yükleyiciye bağlantı ile açılır.

Security Agent'a Geçme

Security Agent'ı kurduğunuzda, Kurulum istemcide herhangi bir Trend Micro veya üçüncü taraf son nokta güvenlik yazılımı yüklü olup olmadığını kontrol eder.

Kurulum aşağıdaki işlemleri gerçekleştirebilir:

- İstemcide yüklenmiş olan başka bir güvenlik yazılımını kaldırır ve Security Agent ile değiştirir
- Başka bir son nokta güvenlik yazılımı tespit eder ama kaldırmaz

Son nokta güvenlik yazılımı listesi için aşağıdaki web sitesini ziyaret edin:

http://esupport.trendmicro.com/solution/en-US/1060980.aspx

İstemcideki yazılım otomatik olarak kaldırılamıyorsa veya algılanıyorsa ama kaldırılamıyorsa, önce manuel olarak kaldırın Yazılımın kaldırma işlemine bağlı olarak, istemcinin kaldırma sonrasında yeniden başlatması gerekli olabilir veya olmayabilir.

Geçiş Sorunları ve Olası Çözümler

Üçüncü taraf güvenlik yazılımının otomatik olarak kaldırılması aşağıdaki sebeplerden dolayı başarısız olabilir:

- Üçüncü taraf yazılımın sürüm numarası veya ürün anahtarı tutarsız.
- Üçüncü taraf yazılımın kaldırma programı çalışmıyor.
- Üçüncü taraf yazılımın bazı dosyaları eksik veya bozuk.
- Üçüncü taraf yazılımın kayıt defteri anahtarı temizlenemiyor.
- Üçüncü taraf yazılımın kaldırma programı yok.

Bu sorunların olası çözümleri:

- Üçüncü taraf yazılımı manuel olarak kaldırın.
- Üçüncü taraf yazılım hizmetini durdurun.
- Üçüncü taraf yazılım hizmetini veya işlemini kaldırın.

Security Agent'larda Yükleme Sonrası Görevleri Gerçekleştirme

Prosedür

1. Aşağıdakileri doğrulayın:

   - Security Agent kısayolları, istemci üzerindeki Windows başlat menüsü üzerinde belirir.
   - **Trend Micro Worry-Free Business Security Agent** istemcinin Denetim Masasının Program Ekle/Kaldır listesinde listelenmektedir.
   - Security Agent, web konsolunda Güvenlik Ayarları ekranında belirir ve istemcinin işletim sistemi türüne göre **Sunucular (varsayılan)** veya **Masaüstü (varsayılan)** grubu altında gruplanır.

     Nota

     Security Agent'ı görmüyorsanız, **Tercihler** > **Genel Ayarlar** > **Sistem (sekme)** > **Aracı Bağlantı Doğrulaması** kısmından bir bağlantı doğrulama görevi çalıştırın.

   - Aşağıdaki Security Agent hizmetleri, **Microsoft Management Console** üzerinde görüntülenir:
     - Trend Micro Security Agent Dinleyici (tmlisten.exe)
     - Trend Micro Security Agent Gerçek Zamanlı Tarama (ntrtscan.exe)
     - Trend Micro Security Agent NT Proxy Hizmeti (TmProxy.exe)

       Nota

       Bu hizmet, Windows 8/8.1, 10, Server 2012 ve Server 2012 R2 üzerinde kullanılabilir değildir.

     - Trend Micro Security Agent Güvenlik Duvarı (TmPfw.exe) yükleme esnasında güvenlik duvarı etkinleştirilmişse

- Trend Micro Yetkisiz Değişiklik Önleme Hizmeti (TMBMSRV.exe) yükleme sırasında Behavior Monitoring veya Aygıt Denetimi etkinleştirilmişse

2. Security Agent, web konsolunda görünmüyorsa, durumunu sunucuya gönderememiş olması mümkündür. Aşağıdaki adımlardan herhangi birini gerçekleştirin:

   - İstemcide bir Web tarayıcısı açın, adres metin kutusuna https://{Trend Micro Security Server_Name}:{port number}/SMB/cgi/cgionstart.exe yazın ve ardından ENTER'a basın.

     Sonraki ekranda -2 gösteriliyorsa, istemcinin sunucuyla iletişim kurabildiği anlamına gelir. Bu, aynı zamanda, aracının kaydı olmayabilir ve sorunun sunucu veritabanında olduğunu belirtebilir.

   - Ping ve telnet kullanarak istemci-sunucu iletişiminin var olduğunu doğrulayın.

   - Kısıtlı bant genişliğine sahipseniz, bunun sunucu ve istemci arasında bağlantı zaman aşımına neden olup olmadığını kontrol edin.

   - Sunucudaki \PCCSRV klasörünün paylaşma ayrıcalıklarına sahip olup olmadığını ve tüm kullanıcılara tam kontrol ayrıcalıklarının verilip verilmediğini kontrol edin

   - Trend Micro Security Server proxy ayarlarının doğru olduğunu onaylayın.

3. Security Agent'ı EICAR test komut dizesini kullanarak test etme

   European Institute for Computer Antivirus Research (EICAR), yüklemenizi ve yapılandırmanızı test etmek üzere kullanabileceğiniz bir test virüsü geliştirmiştir. Bu dosya, ikili kalıbı çoğu antivirüs satıcısından alınan virüs kalıbı dosyasına dahil edilen sabit bir metin dosyasıdır. Bir virüs değildir ve herhangi bir program kodu içermez.

   EICAR test virüsünü şu URL'den indirebilirsiniz:

   http://www.eicar.org/anti_virus_test_file.htm

   Alternatif olarak, aşağıdakileri metin dosyasına girerek, ardından da dosyayı eicar.com olarak adlandırarak kendi EICAR test virüsünüzü oluşturabilirsiniz.

```
X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-
FILE!$H+H*
```

Nota

Testten önce önbellek sunucusundaki ve yerel tarayıcıdaki önbelleği temizleyin.

Messaging Security Agent Yükleme

Messaging Security Agent'ları yalnızca Worry-Free Business Security Advanced sürümünüz varsa yüklenebilir.

Microsoft Exchange sunucular üzerinde Messaging Security Agent'ın taze bir kurulumunu gerçekleştirin.

Nota

Messaging Security Agent'ı bu sürüme yükseltmek hakkında bilgi için, Yükleme ve Yükseltme Kılavuzu'na bakın.

Messaging Security Agent Yükleme Gereksinimleri

Yükleme gereksinimlerinin tam bir listesi için aşağıdaki web sitesini ziyaret edin:

http://docs.trendmicro.com/tr-tr/smb/worry-free-business-security.aspx

Messaging Security Agent'ı Yükleme (Yalnızca Advanced)

Başlamadan önce

Yükleme Notları ve Hatırlatıcılar:

- Yükleme işleminden önce veya sonra Microsoft Exchange hizmetlerini durdurmanız veya başlatmanız gerekmez.
- İstemcide önceki Messaging Security Agent yüklemesinden bilgi varsa, Messaging Security Agent'ı başarıyla yükleyemezsiniz. Önceki yüklemenin kalıntılarını

temizlemek için Windows Installer Temizleme Yardımcı Programı'nı kullanın. Windows Installer Temizleme Yardımcı Programı'nı indirmek için şu adresi ziyaret edin:

http://support.microsoft.com/kb/290301/en-us

- Messaging Security Agent'ı kilit araçları çalıştıran bir sunucuya yüklüyorsanız, IIS hizmetini devre dışı bırakmaması ve yükleme işleminin başarısız olmasına yol açmaması için kilit aracını kaldırın.
- Ayrıca, Messaging Security Agent, Security Server yüklemesi sırasında da yüklenebilir. Ayrıntılar için, bkz. Yükleme ve Yükseltme Kılavuzu.

Prosedür

1. **Güvenlik Ayarları** > **Bilgisayar Ekle** kısmına gidin.

   Yeni bir ekran açılır.

2. **Exchange sunucusunu** seçin.

3. **Exchange Server Bilgileri** altında, aşağıdaki bilgileri girin:

   - **Sunucu adı**: Aracıyı yüklemek istediğiniz Microsoft Exchange sunucusunun adı.
   - **Hesap**: Yerleşik etki alanı yöneticisinin kullanıcı adı.
   - **Parola**: Yerleşik etki alanı yöneticisinin parolası.

4. **İleri** öğesine tıklayın.

   Yükleme sihirbazı, ihtiyacınız olan yükleme türüne bağlı olarak bir ekran görüntüler.

   - **Yeni yükleme**: Aracı Microsoft Exchange sunucusu üzerinde yer almıyor ve yüklenecektir.
   - **Yükseltme**: Aracının önceki bir sürümü Microsoft Exchange sunucusu üzerinde yer alıyor ve güncel sürüme yükseltilecektir.

- **Yükleme gerekmez**: Microsoft Exchange sunucusu üzerinde mevcut olan aracının güncel sürümü. Aracı Güvenlik Grupları Ağacı içinde mevcut olarak belirmiyorsa, otomatik olarak eklenecektir.
- **Geçersiz**: Aracıyı yüklerken bir sorun oluştu.

Nota

Spam Yönetim Türü için, **Son Kullanıcı Karantinası** kullanılacaktır.

5. **Dizinler** altından, Messaging Security Agent yüklemesi için varsayılan hedefi ve paylaşılan dizinleri değiştirin veya kabul edin. Varsayılan hedef ve paylaşılan dizinler, sırayla C:\Program Files\Trend Micro\Messaging Security Agent ve C$ şeklindedir.
6. **İleri** öğesine tıklayın.

   Yeni bir ekran açılır.
7. Önceki ekranlarda belirttiğiniz Microsoft Exchange sunucusu ayarlarının doğruluğunu onaylayın ve ardından yüklemeyi başlatmak için **İleri** öğesine tıklayın.
8. Yüklemenin durumunu görüntülemek için, **Canlı Durum** sekmesine tıklayın.

Aracıları Kaldırma

Security Agent'ları ve **Messaging Security Agent'ları** kaldırmak için iki yöntem vardır (yalnızca Advanced):

Aracıları Web Konsolundan Kaldırma

Etkin olmayan aracılar için bu seçeneği kullanın. Etkin olmayan bir aracı, web konsolunda sürekli olarak çevrimdışı görünecektir, çünkü aracının üzerinde yüklü olduğu istemci çok uzun süre boyunca kapalı kalmış olabilir veya aracı kaldırılmadan önce yeniden biçimlendirilmiş olabilir.

Web konsolundan aracıları kaldırdığınızda:

- Aracı hala istemci üzerinde mevcutsa, kaldırılmayacaktır.

- Sunucu, aracının yönetimini durdurur.
- Aracı sunucuyla tekrar iletişim kurmaya başladığında (örneğin, istemciye güç verdikten sonra), aracı web konsoluna tekrar eklenir. Security Agent, orijinal grubunun ayarlarını uygular. Grup artık mevcut değilse, aracı istemcinin işletim sistemine bağlı olarak **Sunucular (varsayılan)** veya **Masaüstü (varsayılan)** altında gruplanacaktır ve bu grubun ayarları uygulanacaktır.

İpucu

WFBS, etkin olmayan aracıların kontrol edilmesi ve web konsolundan kaldırılması için başka bir özellik sunmaktadır. Aracı kaldırma görevini otomatikleştirmek için bu özelliği kullanın. Bu özelliği kullanmak için, **Tercihler** > **Genel Ayarlar** > **Sistem** sekmesine gidin ve Aktif Olmayan Security Agent Kaldırma kısmına gidin.

Aracıyı Kaldırma

Aracı programıyla ilgili sorunlarla karşılaşırsanız, aracıyı kaldırabilirsiniz (ve ardından web konsolundan çıkartabilirsiniz). Trend Micro, istemcinin tehditlerden korunmuş kalması için aracının hemen yeniden yüklenmesini önermektedir.

Aracıları Web Konsolundan Kaldırma

Prosedür

1. **Güvenlik Ayarları** kısmına gidin.
2. Security Agent'ları kaldırmak için, bir grup seçin ve ardından aracıları seçin. Bir Messaging Security Agent'ı kaldırmak için, onu seçin.

İpucu

Birden çok, bitişik Security Agent seçmek için aralıktaki ilk aracıyı seçin, ÜST KRKT tuşuna uzun basın ve ardından aralıktaki son aracıyı tıklayın. Bitişik olmayan aracılar aralığını seçmek için, aralıktaki ilk aracıya tıklayın, CTRL tuşuna basılı tutun ve seçmek istediğiniz aracılara tıklayın.

3. **İstemci Ağacını Yönet** > **Grubu/İstemciyi Kaldır** öğesine tıklayın.

Yeni bir ekran belirir.

4. **Seçilen aracıyı/aracıları kaldır** öğesine tıklayın.

5. **Uygula** öğesine tıklayın.

Aracıları Web Konsolundan Kaldırma

Messaging Security Agent'ı kaldırırken, IIS Admin hizmeti/Apache server ve ilgili tüm hizmetler otomatik olarak durdurulup yeniden başlatılacaktır.

Prosedür

1. **Güvenlik Ayarları** kısmına gidin.

2. Security Agent'ları kaldırmak için, bir grup seçin ve ardından aracıları seçin. Bir Messaging Security Agent'ı kaldırmak için, onu seçin.

İpucu

Birden çok, bitişik Security Agent seçmek için aralıktaki ilk aracıyı seçin, ÜST KRKT tuşuna uzun basın ve ardından aralıktaki son aracıyı tıklayın. Bitişik olmayan aracılar aralığını seçmek için, aralıktaki ilk aracıya tıklayın, CTRL tuşuna basılı tutun ve seçmek istediğiniz aracılara tıklayın.

3. **İstemci Ağacını Yönet** > **Grubu/İstemciyi Kaldır** öğesine tıklayın.

   Yeni bir ekran belirir.

4. **Seçilen aracıyı/aracıları kaldır** öğesine tıklayın.

5. **Uygula** öğesine tıklayın.

   Bir açılır pencere belirir ve sunucu tarafından gönderilen kaldırma bildirimlerinin sayısını ve bildirimi alan areacıların sayısını görüntüler.

Nota

Bir Messaging Security Agent için, istemde bulunulduğunda ilgili Microsoft Exchange sunucusu hesap adını ve parolasını girin.

6. **TAMAM** öğesine tıklayın.

7. Aracının kaldırıldığını doğrulamak için, Güvenlik Ayarları ekranını yenileyin. Aracı, artık Güvenlik Grupları Ağacında belirmemelidir.

   Security Agent kaldırması başarısız olursa, bkz. *SA Kaldırma Aracını Kullanma sayfa 3-43*.

İstemciden Security Agent'ı Kaldırma

Kullanıcılar istemciden aracıyı kaldırabilir.

Yapılandırmanıza bağlı olarak, kaldırma işlemi parola isteyebilir veya istemeyebilir. Eğer parola gerekiyorsa, parolayı sadece kaldırma programını çalıştıracak kullanıcılarla paylaştığınızdan emin olun ve başka kullanıcılara da açıklanmışsa parolayı derhal değiştirin.

Parola, **Tercihler** > **Global Ayarlar** > **Masaüstü/Sunucu sekmesi** > **Security Agent Kaldırma Parolası** kısmından ayarlanabilir veya devre dışı bırakılabilir.

Prosedür

1. **Denetim Masası** > **Program Ekle veya Kaldır** öğesine tıklayın.

2. **Trend Micro Worry-Free Business Security Agent**'ı konumlandırın ve **Değiştir** veya **Kaldır** öğelerinden kullanılabilir olana tıklayın.

3. Ekrandaki talimatları takip edin.

4. İstenirse kaldırma parolasını girin.

   Security Server, kullanıcıya kaldırma ilerlemesi ve tamamlanması hakkında bildirim yapacaktır. Kullanıcının kaldırmayı tamamlaması için istemciyi yeniden başlatması gerekli değildir.

   Bu işlemin başarısız olması durumunda, bkz. *SA Kaldırma Aracını Kullanma sayfa 3-43*.

SA Kaldırma Aracını Kullanma

SA Kaldırma Aracını Kullanın:

- Yükleme başarısız olduğunda veya tamamen kaldırmanın gerekli olduğu durumlarda. Bu araç, bir istemciden tüm Security Agent bileşenlerini otomatik olarak kaldırır.
- Security Agent'ı kaldırmak için

Prosedür

1. Security Server üzerinde <Server yükleme klasörü>\PCCSRV\Private kısmına gidin.
2. SA_Uninstall.exe dosyasını hedef istemciye kopyalayın.
3. Hedef istemcide SA_Uninstall.exe dosyasını çalıştırın.
4. Windows'ta Yönetici olarak (veya Yönetici ayrıcalıklarına sahip herhangi bir hesap ile) oturum açın.
5. Gerçekleştirmek istediğiniz görev için adımları takip edin.

GÖREV	ADIMLAR
Security Agent'ı Kaldır	a. **Uninstall.bat** dosyasını çalıştırın. Bu adımı gerçekleştirmenin çeşitli yolları vardır. • Windows Vista, 7, 8/8.1, 10, Server 2008/2012/2012 R2 veya SBS 2011 üzerinde, aracın klasörüne gidin, **Uninstall.bat** dosyasına sağ tıklayın ve **Yönetici olarak Çalıştır** öğesini seçin. UAC ekranından, **Kabul Ediyorum** seçin. • Windows XP/2003 üzerinde **Uninstall.bat** üzerine çift tıklayın. b. **Şimdi yeniden başlatmak istiyor musunuz? (E/H)** belirdiğinde, aşağıdakilerden birini seçin: • **H [Giriş]**: Bazı sürücüler siz yeniden başlatana kadar kaldırılmaz. • **E [Giriş]**: 30 saniyelik gerisayımdan sonra yeniden başlatılır. SA Kaldırma Aracı aracıyı otomatik olarak durdurur.
Security Agent'ı Kaldır	a. **Stop.bat** dosyasını çalıştırın. Bu adımı gerçekleştirmenin çeşitli yolları vardır. • Windows Vista, 7, 8/8.1, 10, Server 2008/2012/2012 R2 veya SBS 2011 üzerinde, aracın klasörüne gidin, **Stop.bat** dosyasına sağ tıklayın ve **Yönetici olarak Çalıştır** öğesini seçin. UAC ekranından, **Kabul Ediyorum** seçin. • Windows XP/2003 üzerinde **Stop.bat** üzerine çift tıklayın. b. İstemci durduğunda programın sona erdiğini doğrulayın.

Microsoft Exchange Server'dan Messaging Security Agent'ı Kaldırma (Yalnızca Advanced)

Messaging Security Agent'ı kaldırırken, IIS Admin hizmeti/Apache server ve ilgili tüm hizmetler otomatik olarak durdurulup yeniden başlatılacaktır.

Prosedür

1. Yönetici haklarıyla Microsoft Exchange Server'da oturum açın.
2. **Denetim Masası** > **Program Ekle veya Kaldır** öğesine tıklayın.
3. **Trend Micro Messaging Security Agent**'ı konumlandırın ve **Değiştir** öğesine tıklayın.
4. Ekrandaki talimatları takip edin.

Bölüm 4

Grupları Yönetme

Bu bölümde, Worry-Free Business Security içindeki grupların kavramı ve kullanımı açıklanmaktadır.

Gruplar

Worry-Free Business Security'de gruplar, aynı yapılandırmayı paylaşan ve aynı görevleri çalıştıran aracıların bir derlemesidir. Aracıları, Güvenlik Ayarları ekranında, eş zamanlı yapılandırabileceğiniz ve yönetebileceğiniz şekilde gruplar halinde düzenleyin.

Güvenlik Grupları Ağacı ve Aracılar Listesi

ŞEKİL 4-1. Aracıları grup içinde görüntüleyen Güvenlik Ayarları ekranı

Gruplar, Güvenlik Ayarları ekranında sol taraftaki **Güvenlik Grupları Ağacı** bölümünün altında belirir. Yönetim kolaylığı için, şirketinizdeki bölümleri veya işlevleri temsil eden gruplar oluşturun. Ayrıca, özel gruplar oluşturabilirsiniz. Örneğin, daha yüksek etkilenme tehlikesine sahip istemciler üzerindeki Security Agent'ları içeren bir grup oluşturun, böylece bu gruba daha sıkı güvenlik ilkeleri ve ayarları uygulayabilirsiniz.

Bir gruba tıkladığınızda, o gruba ait olan aracılar sağ taraftaki **Aracılar Listesi**'nde görüntülenir.

Aracılar Listesi Sütunları

Aracılar Listesi'ndeki sütunlar her aracı için aşağıdaki bilgileri gösterir:

İpucu

Aracılar Listesi'nde kırmızı gölgeli hücreler dikkat etmenizi gerektiren bilgileri içermektedir.

SÜTUN	GÖSTERİLEN BİLGİ
Security Agent'lar için	
Ad	Aracının yüklendiği istemcinin ana bilgisayar adı
IP Adresi	Aracının yüklendiği istemcinin IP adresi
Çevrimiçi/Çevrimdışı	• **Çevrimiçi**: Aracı, Security Server'a bağlı. • **Çevrimdışı**: Aracı, Security Server'a bağlı değil.
Zamanlanmış Tarama	Son Zamanlanmış Taramanın tarihi ve saati
Manuel Tarama	Son Manuel Taramanın tarihi ve saati
Platform	Aracının yüklendiği istemcinin işletim sistemi
Mimari	• **x64**: 64-bit işletim sistemi • **x86**: 32-bit işletim sistemi
Tarama Yöntemi	• **Akıllı**: Yerel ve bulut içi taramalar • **Geleneksel**: Sadece yerel taramalar Ayrıntılar için, bkz. *Tarama Yöntemleri sayfa 5-3*.
Virüs Motoru	Virüs Tarama Motoru sürümü
Smart Scan Agent Pattern **Nota** Bu sütun sadece tarama türü smart scan ise görüntülenir.	Smart Scan Agent Kalıbı sürümü

SÜTUN	GÖSTERİLEN BİLGİ
Smart Scan Service **Nota** Bu sütun sadece tarama türü smart scan ise görüntülenir.	• **Bağlandı**: Aracı, Smart Scan Hizmetine bağlı. • **Bağlantı Kesildi**: Aracının, Smart Scan Service bağlantısı kesildi. **Nota** Smart Scan Hizmeti, Security Server üzerinde bulunmaktadır. Bir aracının bağlantısı kesildiğinde, Security Server'a bağlanamıyor veya Smart Scan Hizmeti işlevsel değil (örneğin, hizmet durdurulmuşsa) anlamına gelmektedir.
Virüs Kalıbı **Nota** Bu sütun sadece tarama türü geleneksel tarama ise görüntülenir.	Virüs Kalıbı sürümü
Algılanan Virüsler	Algılanan virüs/kötü amaçlı yazılım sayısı
Algılanan Casus Yazılım	Algılanan casus yazılım/grayware sayısı
Sürüm	Aracının sürümü
İhlal Edilen URL'ler	Erişilen yasaklı URL sayısı
Algılanan spam	Spam e-posta iletileri sayısı
POP3 Taraması	• **Etkin** • **Devre dışı bırakıldı**
Messaging Security Agent'lar için (Yalnızca Advanced)	
Ad	Aracının yüklendiği istemcinin ana bilgisayar adı
IP Adresi	Aracının yüklendiği istemcinin IP adresi

SÜTUN	GÖSTERİLEN BİLGİ
Çevrimiçi/Çevrimdışı	• **Online**: Aracı, Security Server'a bağlı. • **Offline**: Aracı, Security Server'a bağlı değil.
Platform	Aracının yüklendiği istemcinin işletim sistemi
Mimari	• **x64**: 64-bit işletim sistemi • **x86**: 32-bit işletim sistemi
Exchange Sürümü	Microsoft Exchange sunucu sürümü
Virüs Kalıbı	Virüs Kalıbı sürümü
Virüs Motoru	Virüs Tarama Motoru sürümü
Sürüm	Aracının sürümü

Gruplar ve Aracılar için Görevler

Bir grup veya bir veya daha çok aracı üzerinde görevleri çalıştırın.

Bir görevin çalıştırılması iki adımı içerir:

1. Bir hedef seçin.
2. Görev için düğmeye tıklayın.

Aşağıdaki tabloda gerçekleştirebileceğiniz görevler listelenmektedir.

GÖREV	HEDEF	AÇIKLAMA
Yapılandır	Tek Security Agent grubu (masaüstü veya sunucu)	Seçilen gruba ait tüm Security Agent'lar için aşağıdaki temel güvenlik ayarlarını yapılandırın: • Tarama yöntemi Bkz. *Tarama Yöntemlerini Yapılandırma sayfa 5-5*. • Antivirüs/Casus yazılımdan koruma. Bkz. *Security Agent'lar için Gerçek Zamanlı Tarama Yapılandırma sayfa 5-7*. • Güvenlik duvarı. Bkz. *Güvenlik Duvarını Yapılandırma sayfa 5-10*. • Web Reputation. Bkz. *Security Agent'lar için Web Reputation Yapılandırma sayfa 5-17*. • URL Filtreleme. Bkz. *URL Filtrelemeyi Yapılandırma sayfa 5-18*. • Onaylanmış/Engellenmiş URL'ler. Bkz. *Onaylanmış/Engellenmiş URL'ler sayfa 5-19*. • Behavior Monitoring. Bkz. *Behavior Monitoring'i Yapılandırma sayfa 5-21*. • Aygıt Denetimi. Bkz. *Aygıt Denetimini Yapılandırma sayfa 5-25*. • Kullanıcı Araçları (sadece masaüstü grupları). Bkz. *Kullanıcı Araçlarını Yapılandırma sayfa 5-27*. • İstemci Ayrıcalıkları. Bkz. *Aracı Ayrıcalıklarını Yapılandırma sayfa 5-28*. • Karantinaya al. Bkz. *Karantina Dizinini Yapılandırma sayfa 5-33*.

GÖREV	HEDEF	AÇIKLAMA
Yapılandır	Tek Messaging Security Agent (Yalnızca Advanced)	Seçilen Messaging Security Agent için aşağıdaki temel güvenlik ayarlarını yapılandırın: • Virüsten Koruma. Bkz. *Messaging Security Agent'lar için Gerçek Zamanlı Tarama Yapılandırma sayfa 6-5*. • İstenmeyen E-postadan Koruma. Bkz. *Email Reputation'ı Yapılandırma sayfa 6-8* ve *İçerik Taramasını Yapılandırma sayfa 6-9*. • İçerik Filtreleme. Bkz. *İçerik Filtreleme Kurallarını Yönetme sayfa 6-15*. • Ek Engelleme. Bkz. *Ek Engellemeyi Yapılandırma sayfa 6-45*. • Web Reputation. Bkz. *Messaging Security Agent'lar için Web Reputation Yapılandırma sayfa 6-49*. • Karantinaya al. Bkz. *Karantina Dizinlerini Sorgulama sayfa 6-61*, *Karantina Dizinlerinin Bakımı sayfa 6-64* ve *Karantina Dizinlerini Yapılandırma sayfa 6-65*. • İşlemler. Bkz. *Messaging Security Agent'lar için Bildirim Ayarlarını Yapılandırma sayfa 6-68*, *Spam Bakımını Yapılandırma sayfa 6-68* ve *Sistem Hata Ayıklayıcı Raporları Oluşturma sayfa 6-72*.
Ayarları Çoğalt	Tek Security Agent grubu (masaüstü veya sunucu)	Seçilen grubun ayarları, aynı türdeki başka bir grup tarafından uygulanacaktır (masaüstü grubu veya sunucu grubu). Ayrıntılar için, bkz. *Ayarları Çoğaltma sayfa 4-17*.

GÖREV	HEDEF	AÇIKLAMA
İçe Aktar	Tek Security Agent grubu (masaüstü veya sunucu)	Bir kaynak grubun ayarlarını seçilen hedef gruba içe aktarın. İçe aktarmadan önce, kaynak grubun ayarlarını bir dosyaya dışa aktardığınızdan emin olun. Ayrıntılar için, bkz. *Security Agent Gruplarının Ayarlarını İçe ve Dışa Aktarma sayfa 4-19*.
Dışa Aktar	Tek Security Agent grubu (masaüstü veya sunucu)	Seçilen hedef grubun ayarlarını bir dosyaya dışa aktarın. Ayarları yedeklemek veya başka bir gruba içe aktarmak için bu görevi gerçekleştirin. Ayrıntılar için, bkz. *Security Agent Gruplarının Ayarlarını İçe ve Dışa Aktarma sayfa 4-19*.
Grup Ekle	Güvenlik Grupları Ağacı ( )	Yeni bir Security Agent grubu ekle (masaüstü veya sunucu grubu). Ayrıntılar için, bkz. *Grup Ekleme sayfa 4-10*.
Ekle	Güvenlik Grupları Ağacı ( )	Aşağıdakilerden birini yükleyin: • **Security Agent**'tan bir istemciye (masaüstü veya sunucu) • **Messaging Security Agent**'tan bir Microsoft Exchange Server'a (yalnızca Advanced) Ayrıntılar için, bkz. *Gruplara Aracı Ekleme sayfa 4-11*.

GÖREV	HEDEF	AÇIKLAMA
Kaldır	Tek Security Agent grubu (masaüstü veya sunucu)	Seçilen grubu **Güvenlik Grupları Ağacı**'ndan çıkartın. Grupta herhangi bir aracı bulunmadığından emin olun, yoksa grup silinmeyecektir. Ayrıntılar için, bkz. *Aracıları Kaldırma sayfa 3-39*.
	Bir gruba ait bir veya daha çok Security Agent	İki seçeneğiniz mevcuttur: • Seçilen Security Agent'ları gruplarından çıkartın. • Seçilen Security Agent'ları istemcilerinden kaldırın ve gruplarından çıkartın. Ayrıntılar için, bkz. *Aracıları Kaldırma sayfa 3-39*.
	Tek Messaging Security Agent (Yalnızca Advanced)	İki seçeneğiniz mevcuttur: • Seçilen Messaging Security Agent'ı ve grubunu kaldırın. • Seçilen Messaging Security Agent'ları Microsoft Exchange sunucusundan kaldırın ve grubundan çıkartın. Ayrıntılar için, bkz. *Aracıları Kaldırma sayfa 3-39*.
Taşı	Bir gruba ait bir veya daha çok Security Agent	Seçilen Security Agent'ları başka bir gruba veya başka bir Security Server'a taşıyın Ayrıntılar için, bkz. *Aracıları Taşıma sayfa 4-12*.

GÖREV	HEDEF	AÇIKLAMA
Sayaçları Sıfırla	Güvenlik Grupları Ağacı ( )	Tüm Security Agent'lar üzerindeki tehdit sayaçlarını sıfıra getirir. Özellikle, **Aracılar Listesi**'nde aşağıdaki sütunlardaki değerler sıfırlanacaktır: • Algılanan Virüsler • Algılanan Casus Yazılım • Algılanan spam • İhlal Edilen URL'ler Bu sütunlar hakkında ayrıntılar için, bkz. *Güvenlik Grupları Ağacı ve Aracılar Listesi sayfa 4-2*.

Grup Ekleme

Bir veya daha çok Security Agent içerebilecek sunucu grubu veya masaüstü grubu ekleyin.

Messaging Security Agent içeren bir grup eklemek mümkün değildir. Bir Messaging Security Agent yüklendikten ve Security Server'a rapor verdikten sonra, **Güvenlik Grupları Ağacı** içerisinde otomatik olarak kendi grubunda olacaktır.

Prosedür

1. **Güvenlik Ayarları** kısmına gidin.
2. **Grup Ekle** öğesine tıklayın.

   Yeni bir ekran belirir.
3. Bir grup türü seçin.
   - **Masaüstü Bilgisayarlar**
   - **Sunucular**
4. Grup için bir ad girin.

5. Mevcut bir grubun ayarlarını eklemekte olduğunuz gruba uygulamak için, **Gruptan ayarları içe aktar** öğesine tıklayın ve grubu seçin. Sadece seçilen grup türü için gruplar gösterilecektir.

6. **Kaydet** öğesine tıklayın.

Gruplara Aracı Ekleme

Bir aracı yüklendikten ve Security Server'a bildirimde bulunduktan sonra, sunucu bunu bir gruba ekler.

- Windows Server 2003 ve Windows Server 2008 gibi sunucu platformlarında yüklenmiş Security Agent'lar, **Sunucular (varsayılan)** grubuna eklenir.
- Windows XP, Windows Vista ve Windows 7 gibi masaüstü platformlarında yüklenmiş Security Agent'lar, **Masaüstü (varsayılan)** grubuna eklenir.

Nota

Security Agent'ları taşıyarak diğer gruplara atayabilirsiniz. Ayrıntılar için, bkz. *Aracıları Taşıma sayfa 4-12*.

- Her Messaging Security Agent (yalnızca Advanced) kendi grubundadır. Çeşitli Messaging Security Agent'ları bir grupta düzenlemek mümkün değildir.

Güvenlik Grupları Ağacı'nda yansıtılan aracıların sayısı hatalıysa, aracıların sunucuya bildirim yapılmadan kaldırılmış olması mümkündür (örneğin, aracı kaldırılırken istemci-sunucu iletişimi kesilmişse). Bu, sunucunun aracı bilgisini veritabanında tutmasına ve web konsolunda aracıyı çevrimdışı olarak göstermesine nedne olur. Aracıyı yeniden yüklediğinizde, sunucu veritabanında yeni bir kayıt oluşturur ve aracıyla yeni olarak işlem yapar, bu da Güvenlik Grupları Ağacında çift aracıların belirmesine neden olur. Çift aracı kayıtlarını kontrol etmek için, **Tercihler** > **Genel Ayarlar** > **Sistem** kısmında Aracı Bağlantı Doğrulaması özelliğini kullanın.

Security Agent'ları Yükleme

Aşağıdaki başlıklara bakın:

- *Security Agent Yükleme Gereksinimleri sayfa 3-2*
- *Security Agent Yükleme Hususları sayfa 3-2*
- *Security Agent Yükleme Yöntemleri sayfa 3-9*
  - *Dahili Web Sayfasından Yükleme sayfa 3-12*
  - *Oturum Açma Komut Dizesi Kurulumu ile Yükleme sayfa 3-14*
  - *Client Packager ile Yükleme sayfa 3-16*
  - *Uzaktan Yükleme ile Yükleme sayfa 3-19*
  - *Güvenlik Açığı Tarayıcısıyla Yükleme sayfa 3-23*
  - *E-posta Bildirimiyle Yükleme sayfa 3-33*
- *Security Agent'larda Yükleme Sonrası Görevleri Gerçekleştirme sayfa 3-35*

Messaging Security Agent'ları Yükleme (Yalnızca Advanced)

Aşağıdaki başlıklara bakın:

- *Messaging Security Agent Yükleme Gereksinimleri sayfa 3-37*
- *Messaging Security Agent'ı Yükleme (Yalnızca Advanced) sayfa 3-37*

Aracıları Taşıma

Aracıları taşımanın çeşitli yolları vardır.

Taşınacak Aracı	Ayrıntılar	Aracıların Taşınması
Security Agent	Gruplar arasında Security Agent'ları taşıyın. Taşıma sonrasında, aracılar yeni grubunun ayarlarını devralır.	Bir veya daha çok aracıyı taşımak için web konsolunu kullanın. Bkz. *Gruplar Arasında Security Agent'ları Taşıma sayfa 4-13*.
	En az iki Security Server varsa, Security Agent'ları sunucular arasında taşıyın. Taşıdıktan sonra, istemcinin işletim sistemine bağlı olarak, aracı diğer Security Server'ın **Masaüstü (varsayılan)** veya **Sunucular (varsayılan)** grubu altında gruplanır. Aracı, yeni grubunun ayarlarını devralır.	• Bir veya daha çok aracıyı taşımak için web konsolunu kullanın. Bkz. *Web Konsolunu Kullanarak Security Server'lar Arasında Aracıları Taşıma sayfa 4-14*. • Bir istemci üzerinde yüklü olan aracıyı taşımak için o istemci üzerindeki Client Mover aracını çalıştırın. Bkz. *Client Mover Kullanarak Security Server'lar Arasında bir Security Agent'ı Taşıma sayfa 4-15*.
Messaging Security Agent (Yalnızca Advanced)	En az iki Security Server varsa, Messaging Security Agent'ları sunucular arasında taşıyın. Taşıdıktan sonra, bir aracı diğer Security Server'da kendi grubunda olacaktır ve ayarlarını koruyacaktır.	Bir seferde bir aracıyı taşımak için web konsolunu kullanın: Bkz. *Web Konsolunu Kullanarak Security Server'lar Arasında Aracıları Taşıma sayfa 4-14*.

Gruplar Arasında Security Agent'ları Taşıma

Prosedür

1. **Güvenlik Ayarları** kısmına gidin.

2. Bir masaüstü veya sunucu grubu seçin.
3. Taşınacak aracıları seçin.

İpucu

Birden çok, bitişik Security Agent seçmek için aralıktaki ilk aracıyı seçin, ÜST KRKT tuşuna uzun basın ve ardından aralıktaki son aracıyı tıklayın. Bitişik olmayan aracılar aralığını seçmek için, aralıktaki ilk aracıya tıklayın, CTRL tuşuna basılı tutun ve seçmek istediğiniz aracılara tıklayın.

4. Aracıları yeni gruba sürükleyin ve bırakın.

Web Konsolunu Kullanarak Security Server'lar Arasında Aracıları Taşıma

Başlamadan önce

Bir aracıyı Security Server'lar arasında taşırken:

- Daha önceki bir sürümü çalıştıran bir aracı, mevcut sürümü çalıştıran bir Security Server'a taşınırsa, aracı otomatik olarak yükseltilecektir.
- Mevcut sürümü çalıştıran bir aracıyı önceki sürümü çalıştıran bir Security Server'a taşımayın, çünkü aracı yönetimsiz kalacaktır (aracının kaydı önceki sunucudan kaldırılacaktır ancak yeni sunucuya kayıt yapamayacaktır, dolayısıyla her iki web konsolunda da belirmeyecektir). Aracı mevcut sürümünü koruyacaktır ve aşağı indirilmeyecektir.
- Security Server'lar aynı dil sürümünde olmalıdır.
- Bir aracının taşınacağı Security Server'ın ana makine adını ve dinleme bağlantı noktasını kaydedin. Ana makine adı ve dinleme bağlantı noktası, Security Server'ın Güvenlik Ayarları ekranında Görevler panelinin üzerinde bulunur.

Prosedür

1. Aracıları mevcut olarak yöneten Security Server'ın web konsolunda, **Güvenlik Ayarları** kısmına gidin.

2. Security Agent'ları taşımak için, bir grup seçin ve ardından aracıları seçin. Bir Messaging Security Agent'ı taşımak için, onu seçin.

İpucu

Birden çok, bitişik Security Agent seçmek için aralıktaki ilk aracıyı seçin, ÜST KRKT tuşuna uzun basın ve ardından aralıktaki son aracıyı tıklayın. Bitişik olmayan aracılar aralığını seçmek için, aralıktaki ilk aracıya tıklayın, CTRL tuşuna basılı tutun ve seçmek istediğiniz aracılara tıklayın.

3. **İstemci Ağacını Yönet** > **Grubu/İstemciyi Taşı** öğesine tıklayın.

   Yeni bir ekran belirir.

4. Aracıların taşınacağı Security Server'ın ana makine adını ve dinleme bağlantı noktasını girin.

5. **Taşı** öğesine tıklayın.

6. Aracıların artık Security Server'a rapor verip vermediğini kontrol etmek için, o sunucunun web konsolunu açın ve Güvenlik Grupları Ağacı'nda aracıları konumlandırın.

Nota

Aracılar, Güvenlik Grupları Ağacı'nda belirmiyorsa, sunucunun Ana Hizmetini (ofservice.exe) yeniden başlatın.

Client Mover Kullanarak Security Server'lar Arasında bir Security Agent'ı Taşıma

Başlamadan önce

Bir aracıyı Security Server'lar arasında taşırken:

- Daha önceki bir sürümü çalıştıran bir aracı, mevcut sürümü çalıştıran bir Security Server'a taşınırsa, aracı otomatik olarak yükseltilecektir.
- Mevcut sürümü çalıştıran bir aracıyı önceki sürümü çalıştıran bir Security Server'a taşımayın, çünkü aracı yönetimsiz kalacaktır (aracının kaydı önceki sunucudan

kaldırılacaktır ancak yeni sunucuya kayıt yapamayacaktır, dolayısıyla her iki web konsolunda da belirmeyecektir). Aracı mevcut sürümünü koruyacaktır ve aşağı indirilmeyecektir.

- Security Server'lar aynı dil sürümünde olmalıdır.
- Bir aracının taşınacağı Security Server'ın ana makine adını ve dinleme bağlantı noktasını kaydedin. Ana makine adı ve dinleme bağlantı noktası, Security Server'ın Güvenlik Ayarları ekranında Görevler panelinin üzerinde bulunur.
- Bir yönetici hesabını kullanarak istemcide oturum açın.

Prosedür

1. İstemci üzerinde, bir komut istemi penceresi açın.

   Nota

   Komut istemi penceresini yönetici olarak açmalısınız.

2. `cd` ve Security Agent yükleme klasörü yolunu yazın. Örneğin: `cd C:\Program Files\Trend Micro\Security Agent`

3. Aşağıdaki sözdizimini kullanarak Client Mover'ı çalıştırın:

   ```
   <yürütülebilir dosya adı> -s <sunucu adı> -p <sunucu dinleme bağlantı noktası> -c <istemci dinleme bağlantı noktası>
   ```

   TABLO 4-1. Client Mover Parametreleri

PARAMETRE	AÇIKLAMA
`<yürütülebilir dosya adı>`	IpXfer.exe
`<sunucu adı>`	Hedef WFBS Server'ın adı (aracının aktarılacağı sunucu)
`<sunucu dinleme bağlantı noktası>`	Hedef Security Server'ın dinleme bağlantı noktası (veya güvenilir bağlantı noktası)

PARAMETRE	AÇIKLAMA
`<istemci dinleme bağlantı noktası>`	Security Agent tarafından sunucu ile iletişim kurmak için kullanılan bağlantı noktası numarası

Örnek:

```
ipXfer.exe -s Server01 -p 8080 -c 21112
```

4. Security Agent'ın artık Security Server'a rapor verip vermediğini kontrol etmek için, o sunucunun web konsolunu açın ve Güvenlik Grupları Ağacı'nda aracıyı konumlandırın.

Nota

Aracı Güvenlik Grupları Ağacı'nda belirmiyorsa, sunucunun Ana Hizmetini (ofservice.exe) yeniden başlatın.

Ayarları Çoğaltma

Security Agent grupları arasında veya Messaging Security Agent'lar arasında (sadece Advanced) ayarları çoğaltın.

Security Agent Grup Ayarlarını Çoğaltma

Belirli bir masaüstü veya sunucu grubunun ayarlarını aynı türde başka bir gruba uygulamak için bu özelliği kullanın. Bir sunucu grubunun ayarlarını bir masaüstü grubuna veya tam tersi şekilde çoğaltmak mümkün değildir.

Belirli bir grup türü için sadece bir grup mevcutsa, bu özellik devre dışı olacaktır.

Prosedür

1. **Güvenlik Ayarları** kısmına gidin.
2. Bir masaüstü veya sunucu grubu seçin.

3. **Daha Fazla** > **Ayarları Çoğalt** öğesine tıklayın.

   Yeni bir ekran belirir.

4. Ayarları devralacak hedef gruplarını seçin.

5. **Uygula** öğesine tıklayın.

Messaging Security Agent Ayarlarını Çoğaltma (Yalnızca Advanced)

Messaging Security Agent'lar arasında ayarları sadece aynı etki alanını paylaşıyorlarsa çoğaltabilirsiniz.

Prosedür

1. **Güvenlik Ayarları** kısmına gidin.
2. Bir Messaging Security Agent seçin.
3. **Daha Fazla** > **Ayarları Çoğalt** öğesine tıklayın.

   Yeni bir ekran belirir.

4. Ayarları devralacak Messaging Security Agent'ı seçin.
5. **Uygula** öğesine tıklayın.
6. Çoğaltma başarısız olursa:
   a. Kayıt Düzenleyici'yi başlatın (regedit).
   b. HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurePipeServers\winreg kısmına gidin.
   c. **winreg** > **İzinler** kısmına sağ tıklayın.
   d. Hedef etki alanının **Smex Yönetici Grubu**'nu ekleyin ve **Okuma İzni Ver**'i etkinleştirin.

Security Agent Gruplarının Ayarlarını İçe ve Dışa Aktarma

Ayarları yedeklemek için, bir masaüstü veya sunucu grubunun ayarlarını bir .dat dosyasına dışa aktarın. Ayrıca, ayarları başka bir gruba aktarmak için .dat dosyasını da kullanabilirsiniz.

Nota

Masaüstü ve sunucu grupları arasında ayarları içe/dışa aktarabilirsiniz. Ayarlar grup türüne bağlı değildir. Ayrıca, bu özellik grup türüne bağlı olsa da, Ayarları Çoğalt özelliğini de kullanabilirsiniz. Ayarları Çoğalt özelliği hakkında ayrıntılar için, bkz. *Ayarları Çoğaltma sayfa 4-17*.

İçe ve Dışa Aktarılabilen Ayarlar

İçe ve dışa aktarılabilen ayarlar Güvenlik Grupları Ağacı simgesini ( ) veya belirli bir masaüstü/sunucu grubunu seçmenize bağlıdır.

SEÇİM	AYARLARI İÇEREN EKRAN	İÇE/DIŞA AKTARILABİLEN AYARLAR
Güvenlik Grupları Ağacı simgesi ( )	Güvenlik Ayarları (**Güvenlik Ayarları** > **Ayarları Yapılandır**)	**Sunucular (Varsayılan)** ve **Masaüstü (Varsayılan)** grupları için aşağıdaki ayarlar: • Tarama Yöntemi • Güvenlik Duvarı • Web Reputation • URL Filtreleme • Onaylanmış/Engellenmiş URL'ler • Behavior Monitoring • Güvenilen Program

Seçim	Ayarları İçeren Ekran	İçe/Dışa Aktarılabilen Ayarlar
		• Kullanıcı Araçları (Sadece masaüstü gruplarında kullanılabilir) • İstemci Ayrıcalıkları • Karantinaya Al • Aygıt Denetimi
	Manuel Güncelleme (**Güncellemeler** > **Manuel**)	Manuel Güncelleme ekranında seçilen bileşenler
	Zamanlanmış Güncelleme (**Güncellemeler** > **Zamanlanmış**)	Zamanlanmış Güncelleme ekranında seçilen bileşenler ve zamanlama
	Zamanlanmış Raporlar (**Raporlar** > **Zamanlanmış Raporlar**)	Tüm ayarlar
	Rapor Bakımı (**Raporlar** > **Bakım**)	Tüm ayarlar
	Bildirimler (**Tercihler** > **Bildirimler**)	Tüm ayarlar
	Genel Ayarlar (**Tercihler** > **Genel Ayarlar**)	Aşağıdaki sekmelerdeki tüm ayarlar: • **Proxy** • **SMTP** • **Masaüstü Bilgisayar/ Sunucu** • **Sistem**
Masaüstü grubu ( ) veya Sunucu grubu ( )	Güvenlik Ayarları (**Güvenlik Ayarları** > **Ayarları Yapılandır**)	• Antivirüs/Casus Yazılımdan Koruma Gerçek Zamanlı Tarama • Güvenlik Duvarı • Web Reputation

Seçim	Ayarları İçeren Ekran	İçe/Dışa Aktarılabilen Ayarlar
		• URL Filtreleme • Behavior Monitoring • Güvenilen Program • Kullanıcı Araçları (**Sadece masaüstü gruplarında kullanılabilir**) • İstemci Ayrıcalıkları • Karantinaya Al • Aygıt Denetimi
	Manuel Tarama ekranı (**Taramalar** > **Manuel Tarama**)	Tüm ayarlar
	Zamanlanmış Tarama ekranı (**Taramalar** > **Zamanlanmış Tarama**)	Tüm ayarlar

Ayarları Dışa Aktarma

Prosedür

1. **Güvenlik Ayarları** kısmına gidin.
2. Güvenlik Grupları Ağacı'nı veya masaüstü/server grubunu seçin.
3. **Daha fazla** > **Dışa Aktar** öğesine tıklayın.

   Yeni bir ekran belirir.
4. Güvenlik Grupları Ağacı seçtiyseniz, dışa aktarılacak ayarları seçin.
5. **Daha fazla** > **Dışa Aktar** öğesine tıklayın.

   Bir iletişim kutusu belirir.

6. **Kaydet** öğesine tıklayın, tercih ettiğiniz konuma gözatın ve ardından **Kaydet** öğesine tıklayın.

Ayarları İçe Aktarma

Prosedür

1. **Güvenlik Ayarları** kısmına gidin.
2. Güvenlik Grupları Ağacı'nı veya masaüstü/server grubunu seçin.
3. **Fazlası** > **İçe Aktar** öğesine tıklayın.

   Yeni bir ekran belirir.
4. **Gözat** öğesine tıklayın, dosyayı bulun ve ardından **İçe Aktar** öğesine tıklayın.

Bölüm 5

Security Agent için Temel Güvenlik Ayarlarını Yönetme

Bu bölüm, Security Agent için temel güvenlik ayarlarının nasıl yapılandırılacağını açıklar.

Security Agent için Temel Güvenlik Ayarlarının Özeti

TABLO 5-1. Security Agent için Temel Güvenlik Ayarlarının Özeti

SEÇENEK	AÇIKLAMA	VARSAYILAN
Tarama Yöntemi	Smart Scan'ın etkinleştirilip etkinleştirilmeyeceğini yapılandırın.	Etkin veya Devre Dışı yükleme sırasında seçilir.
Antivirüs/Casus yazılımdan koruma	Gerçek Zamanlı Taramayı, antivirüsü ve casus yazılımdan korunma seçeneklerini yapılandırma	Etkin (Gerçek Zamanlı Tarama)
Güvenlik Duvarı	Güvenlik Duvarı seçeneklerini yapılandırma	Devre dışı bırakıldı
Web Reputation	Ofis İçinde ve Ofis Dışında Web Reputation seçeneklerini yapılandırma	Ofis İçinde: Etkin, Düşük Ofis Dışında: Etkin, Orta
URL Filtreleme	URL filtrelemesi, yapılandırılan ilkeleri ihlal eden web sitelerini engeller.	Etkin, Düşük
Onaylanmış/Engellenmiş URL'ler	Küresel çapta onaylanmış/engellenmiş listeleri yapılandır	Devre dışı bırakıldı
Behavior Monitoring	Behavior Monitoring seçeneklerini yapılandırma	Masaüstü Grupları için Etkin Sunucu Grupları için Devre Dışı
Güvenilen Program	Şüpheli davranışa karşı izlenmesi gerekmeyen programları belirleme	Yok
Aygıt Denetimi	Otomatik Çalıştırma ve USB ve ağ erişimini yapılandırma	Devre dışı bırakıldı

SEÇENEK	AÇIKLAMA	VARSAYILAN
Kullanıcı Araçları	Wi-Fi Advisor Yapılandırma ve Trend Micro Anti-spam Araç Çubuğu	Devre dışı bırakıldı: Wi-Fi Advisor Devre dışı bırakıldı: Desteklenen e-posta istemcilerinde Anti-spam Araç Çubuğu
İstemci Ayrıcalıkları	Aracı konsolundan ayarlara erişimi yapılandırma Security Agent yükseltmesini ve düzeltme dağıtımını devre dışı bırak	Yok
Karantinaya Al	Karantina dizinini belirleme	http://<Security Server adı veya IP adresi>

Tarama Yöntemleri

Security Agent'lar güvenlik tehditleri için tarama yaparken, iki tarama yönteminden birini kullanabilir.

- **Smart scan**: Security Agent'lar smart scan kullananlar bu belgede **smart scan aracıları** olarak bahsedilecektir. Smart scan aracıları, yerel taramalardan ve File Reputation Hizmetleri tarafından sağlanan bulut-içi sorgulardan faydalanır.
- **Geleneksel tarama**: Security Agent'lar Smart scan kullanmayanlar **geleneksel tarama aracıları** olarak adlandırılır. Geleneksel tarama aracısı tüm bileşenleri istemci üzerinde depolar ve tüm dosyaları yerel olarak tarar.

Aşağıdaki tablo, iki tarama yöntemi arasında bir karşılaştırma sağlamaktadır:

TABLO 5-2. Geleneksel Tarama ve Smart Scan Karşılaştırması

KARŞILAŞTIRMA ESASI	GELENEKSEL TARAMA	SMART SCAN
Tarama davranışı	Geleneksel taramaSecurity Agent istemci üzerinde tarama gerçekleştirir.	• Smart scan aracısı istemci üzerinde tarama gerçekleştirir. • Eğer Security Agent tarama sırasında dosyanın tehlikesini belirleyemezse, Security AgentTarama Sunucusuna (Smart Scan Server bağlantılı Security Agent'lar için) veya Trend Micro Smart Protection Network'e (Smart Scan Server bağlantısı kesilmiş Security Agent'lar için) bir tarama sorgusu göndererek tehlikeyi doğrular. **Nota** Tarama Sunucusu, Smart Scan Server üzerinde çalışan bir hizmettir. • Security Agent, tarama performansını iyileştirmek için tarama sorgusu sonucunu "saklar".
Kullanımdaki ve güncellenen bileşenler	Akıllı Tarama Grubu dışında güncelleme kaynağı üzerinde mevcut olan tüm Security Agentbileşenleri	Virüs Kalıbı hariç güncelleme kaynağında mevcut olan tüm bileşenler
Normal güncelleme kaynağı	ActiveUpdate Server	ActiveUpdate Server

Tarama Yöntemlerini Yapılandırma

Başlamadan önce

Security Server'ı yüklediğinizde, smart scan etkinleştirme seçeneği verilir. Bu seçeneği etkinleştirdiyseniz, varsayılan tarama yöntemi smart scan'dir, bu, tüm Security Agent'ların smart scan kullanacağı anlamına gelir. Aksi takdirde, varsayılanı geleneksel taramadır. Mevcut gereksinimlerinize göre aracılarda bu tarama yöntemleri arasında geçiş yapabilirsiniz. Örneğin:

- Aracılar mevcut olarak geleneksel taramayı kullanıyorsa ve taramanın tamamlanması önemli ölçüde zaman alıyorsa, daha hızlı ve daha verimli olması için tasarlanan smart scan özelliğine geçebilirsiniz. Smart scan'e geçebileceğiniz başka bir durum ise, aracı üzerindeki disk alanının azalmasıdır, çünkü smart scan aracıları daha küçük boyutlu kalıplar indirmektedir ve dolayısıyla daha az disk alanı gerektirmektedir.

  Smart scan'e geçmeden önce **Tercihler** > **Genel Ayarlar** > **Masaüstü/Sunucular** sekmesine gidin ve **Genel Tarama Ayarları** bölümüne gidin. **Smart Scan Hizmetini Devre Dışı Bırak** seçeneğinin devre dışı olduğundan emin olun.

- Security Server performansında bir düşüş fark ettiyseniz aracıları geleneksel taramaya geçirin, aracılardan tüm tarama sorgularını zamanında gerçekleştiremediğinin bir göstergesi olabilir.

Aşağıdaki tabloda, tarama yöntemleri arasında geçiş yaparken dikkat edilecek bazı hususlar listelenmektedir:

TABLO 5-3. Tarama Yöntemleri Arasında Geçiş için Hususlar

HUSUSLAR	AYRINTILAR
Security Server bağlantısı	Security Agent'ların Security Server'a bağlanabilmesini sağlar. Farklı bir tarama yöntemibe geçmek için sadece çevrimiçi aracılara bildirim yapılacaktır. Çevrimiçi olduklarında çevrimdışı aracılara da bildirim yapılacaktır. Ayrıca, Security Server'da en son bileşenlerin mevcut olduğunu doğrulayın, çünkü smart scan'e geçiş yapacak aracılar için Smart Scan Aracı Kalıbı ve geleneksel taramaya geçiş yapacak aracılar için Virüs Kalıbı olmak üzere aracıların Security Server'dan yeni bileşenleri indirmesi gereklidir.

Hususlar	Ayrıntılar
Geçiş yapılacak Security Agent'ların Sayısı	Bir seferde nispeten daha küçük sayıda Security Agent geçişinin yapılması, Security Server kaynaklarının daha verimli kullanımını sağlayacaktır. Aracılar tarama yöntemlerini değiştirirken Security Server diğer kritik görevleri gerçekleştirebilir.
Zamanlama	Security Agent'larda ilk defa geçiş yapıldığında, aracıların Smart Scan Aracı Kalıbının (smart scan'e geçiş yapacak aracılar için) veya Virüs Kalıbının (geleneksel taramaya geçiş yapacak aracılar için) **tam sürümünü** indirmesi gereklidir. İndirme işleminin kısa bir sürede tamamlanmasını sağlamak için yoğun olmayan saatlerde geçiş yapmayı dikkate alın. Ayrıca, kullanıcı tarafından başlatılan güncellemeleri önlemek için aracılar üzerindeki "Şimdi Güncelle" seçeneğini geçici olarak devre dışı bırakın ve aracılar tarama yöntemlerinde geçişi tamamladıktan sonra yeniden etkinleştirin. **Nota** Bunun ardından, sıklıkla güncellendikleri müddetçe, aracılar Smart Scan Aracı Kalıbı veya Virüs Kalıbı için **daha küçük, artımlı** sürümleri indirecektir.
IPv6 desteği	Çevrimdışı olan salt bir IPv6 smart scan aracısı, Trend Micro Smart Protection Network'e sorguları doğrudan gönderemez. Smart scan aracısının sorgular göndermesine imkan sağlamak için, DeleGate gibi IP adreslerini dönüştürebilen çift yığınlı proxy sunucu gereklidir.

Prosedür

1. **Güvenlik Ayarları** kısmına gidin.
2. Bir masaüstü veya sunucu grubu seçin.
3. **Ayarları Yapılandır** öğesine tıklayın.

   Yeni bir ekran belirir.

4. Tercih ettiğiniz tarama yöntemini seçin.
5. **Kaydet** öğesine tıklayın.

Security Agent'lar için Gerçek Zamanlı Tarama

Gerçek Zamanlı Tarama tutarlı ve sürekli bir taramadır. Bir dosya her açıldığında, indirildiğinde, kopyalandığında veya değiştirildiğinde, **Security Agent** içindeki Gerçek Zamanlı Tarama dosyayı tehditlere karşı tarar.

Security Agent'lar için Gerçek Zamanlı Tarama Yapılandırma

Prosedür

1. **Güvenlik Ayarları** kısmına gidin.
2. Bir masaüstü veya sunucu grubu seçin.
3. **Ayarları Yapılandır** öğesine tıklayın.

   Yeni bir ekran belirir.
4. **Antivirüs/Casus Yazılımdan Koruma**'yı tıklatın.

   Yeni bir ekran belirir.
5. **Gerçek zamanlı Antivirus/Casus yazılımdan korumayı etkinleştir** öğesini seçin.
6. Tarama ayarlarını yapılandırın. Ayrıntılar için, bkz. *Security Agent'lar için Tarama Hedefleri ve Eylemler sayfa 7-9*:

Nota

Kullanıcılara kendi tarama ayarlarını yapılandırma ayrıcalığını verirseniz, tarama sırasında kullanıcı tarafından yapılandırılmış ayarlar kullanılacaktır.

7. **Kaydet** öğesine tıklayın.

Güvenlik Duvarı

Güvenlik duvarı, istemci ile ağ arasında bir bariyer oluşturarak bazı ağ trafiği türlerini engelleyebilir veya bunlara izin verebilir. Ek olarak, Güvenlik Duvarı istemcilere bir saldırıyı gösterebilen ağ paketlerindeki kalıpları da belirleyecektir.

WFBS, Güvenlik Duvarı yapılandırılırken seçilecek iki seçeneğe sahiptir. basit mod ve gelişmiş mod. Basit mod, Trend Micro tarafından önerilen varsayılan ayarlar ile güvenlik duvarını etkinleştirir. Güvenlik duvarı ayarlarını özelleştirmek için gelişmiş modu kullanın.

İpucu

Trend Micro, Trend Micro güvenlik duvarını dağıtıp etkinleştirmeden önce diğer yazılım tabanlı güvenlik duvarlarını kaldırmanızı önerir.

Varsayılan Güvenlik Duvarı Basit Mod Ayarları

Güvenlik duvarı, istemci güvenlik duvarı koruma stratejinizi uygulamanız için size bir temel sağlayan varsayılan ayarları sağlar. Varsayılanlar, internet erişimi ihtiyacı ve FTP kullanarak dosyaları indirme veya yükleme gibi istemciler üzerinde mevcut olabilecek ortak koşulları içermeyi amacını taşır.

Nota

Varsayılan olarak, WFBS tüm yeni gruplar ve Security Agent'lar üzerinde güvenlik duvarını devre dışı bırakır.

TABLO 5-4. Varsayılan Güvenlik Duvarı Ayarları

AYARLAR	DURUM
Güvenlik Düzeyi	Düşük Gelen ve giden trafiğe izin verildi, yalnız ağ virüsleri engellendi.
Davetsiz Misafir Algılama Sistemi	Devre dışı bırakıldı
Uyarı İletisi (gönderme)	Devre dışı bırakıldı

TABLO 5-5. Varsayılan Güvenlik Duvarı Kural Dışı Durumları

KURAL DIŞI DURUM ADI	EYLEM	YÖN	PROTOKOL	BAĞLANTI NOKTASI
DNS	İzin ver	Gelen ve giden	TCP/UDP	53
NetBIOS	İzin ver	Gelen ve giden	TCP/UDP	137, 138, 139, 445
HTTPS	İzin ver	Gelen ve giden	TCP	443
HTTP	İzin ver	Gelen ve giden	TCP	80
Telnet	İzin ver	Gelen ve giden	TCP	23
SMTP	İzin ver	Gelen ve giden	TCP	25
FTP	İzin ver	Gelen ve giden	TCP	21
POP3	İzin ver	Gelen ve giden	TCP	110
MSA	İzin ver	Gelen ve giden	TCP	16372, 16373
LDAP	İzin ver	Gelen ve giden	TCP/UDP	389

TABLO 5-6. Konuma göre Varsayılan Güvenlik Duvarı Ayarları

KONUM	GÜVENLİK DUVARI AYARLARI
Ofis İçi	Kapalı
Ofis Dışı	Kapalı

Trafik Filtreleme

Güvenlik duvarı, aşağıdaki ölçütlere dayanarak belirli trafik türlerini engellenebilmesini sağlayarak tüm gelen ve giden trafiği filtreler:

- Yön (içeri/dışarı)
- Protokol (TCP/UDP/ICMP/ICMPv6)
- Hedef bağlantı noktaları
- Hedef bilgisayar

Ağ Virüsleri Taraması Yapılıyor

Güvenlik duvarı ayrıca her paketi ağ virüslerine karşı inceler.

Durum Denetlemesi

Güvenlik duvarı, bir durum denetlemesi güvenlik duvarıdır; istemciye yapılan tüm bağlantıları izler ve tüm bağlantı durumlarını hatırlar. Herhangi bir bağlantıdaki belirli koşulları tanımlayabilir, hangi işlemlerin izlenmesi gerektiğini öngörebilir ve normal bir bağlantıdaki bozulmaları tespit edebilir. Dolayısıyla, güvenlik duvarının etkin kullanılması sadece profillerin ve ilkelerin oluşturulmasını değil, aynı zamanda güvenlik duvarından geçen bağlantıların analiz edilmesini ve paketlerin filtrelenmesini de içerir.

Genel Güvenlik Duvarı Sürücüsü

Genel Güvenlik Duvarı Sürücüsü, Güvenlik Duvarı'nın kullanıcı tanımlı ayarlarıyla birlikte salgın sırasında bağlantı noktalarını engeller. Genel Güvenlik Duvarı Sürücüsü, ağ virüslerini algılamak için Ağ Virüsü Kalıbı dosyasını da kullanır.

Güvenlik Duvarını Yapılandırma

Ofis İçi ve Ofis Dışı için güvenlik duvarını yapılandırın. Konum Tanıma devre dışı bırakılmışsa, Ofis İçi ayarları Ofis Dışı bağlantılar için kullanılacaktır. Konum Tanıma hakkında ayrıntılar için, bkz. *Masaüstü/Sunucu Ayarlarını Yapılandırma sayfa 11-5*.

Trend Micro, varsayılan olarak güvenlik duvarını devre dışı bırakır.

Prosedür

1. **Güvenlik Ayarları** kısmına gidin.
2. Bir masaüstü veya sunucu grubu seçin.
3. **Ayarları Yapılandır** öğesine tıklayın.
4. **Güvenlik Duvarı** > **Ofis İçi** veya **Güvenlik Duvarı** > **Ofis Dışı** seçin.
5. **Güvenlik Duvarını Etkinleştir** öğesini seçin.
6. Aşağıdakilerden birini seçin:
   - **Basit Mod**: Güvenlik duvarını varsayılan ayarlarla etkinleştirir.

     Ayrıntılar için, bkz. *Güvenlik Duvarı sayfa 5-8*.
   - **Gelişmiş Mod**: Güvenlik duvarını özel ayarlarla etkinleştirir.
7. **Gelişmiş Mod** seçtiyseniz, aşağıdaki seçenekleri gerektiği gibi güncelleyin:
   - **Güvenlik Düzeyi**: Güvenlik düzeyi, kural dışı durum listesinde olmayan bağlantı noktaları için uygulanacak trafik kurallarını denetler.
     - **Yüksek**: kural dışı durum listesinde izin verilen trafikler dışındaki tüm gelen ve giden trafiği engeller.
     - **Orta**: kural dışı durum listesinde izin verilen ve engellenen trafikler dışındaki tüm gelen trafiği engeller ve tüm giden trafiğe izin verir.
     - **Düşük**: kural dışı durum listesinde engellenen trafikler dışındaki tüm gelen ve giden trafiğe izin verir. Basit mod için varsayılan ayardır.
   - **Ayarlar**
     - **Davetsiz Misafir Algılama Sistemi**: Davetsiz Misafir Algılama Sistemi, bir saldırıyı belirtebilecek ağ paketlerindeki kalıpları tanımlar. Bkz. *Davetsiz Misafir Algılama Sistemi sayfa D-4*.
     - **Uyarı İletilerini Etkinleştir**: WFBS bir ihlal algıladığında istemciye bildirilir.
   - **Kural dışı durumlar**: Kural dışı durum listesindeki bağlantı noktaları engellenmeyecektir.

Ayrıntılar için, bkz. *Güvenlik Duvarı Kural Dışı Durumlarıyla Çalışma sayfa 5-12*

8. **Kaydet** öğesine tıklayın.

Güvenlik Duvarı Kural Dışı Durumlarıyla Çalışma

Güvenlik Duvarı kural dışı durum listesi, istemci bağlantı noktası numaraları ve IP adreslerine göre farklı ağ trafiği türlerini engellemek veya bunlara izin vermek üzere yapılandırabileceğiniz girdileri içerir. Bir salgın sırasında Security Server, kural dışı durumları ağınızı korumak için otomatik olarak dağıtılan Trend Micro ilkelerine uygular.

Örneğin, bir salgın sırasında HTTP bağlantı noktası (bağlantı noktası 80) dahil tüm istemci trafiğini engellemek isteyebilirsiniz. Ancak engellenen istemcilere internet erişimi vermek istiyorsanız kural dışı durum listesine Web proxy sunucusunu ekleyebilirsiniz.

Prosedür

1. **Güvenlik Ayarları** kısmına gidin.
2. Bir masaüstü veya sunucu grubu seçin.
3. **Ayarları Yapılandır** öğesine tıklayın.

   Yeni bir ekran belirir.
4. **Güvenlik Duvarı** > **Ofis İçi** veya **Güvenlik Duvarı** > **Ofis Dışı** seçin.

   Yeni bir ekran belirir.
5. **Güvenlik Duvarını Etkinleştir** öğesini seçin.
6. **Gelişmiş Mod** seçin.
7. Kural dışı bir durum eklemek için:
   a. **Ekle** öğesine tıklayın.

      Yeni bir ekran belirir.

   b. Kural dışı durum için adı girin.

c. **Eylem** seçeneğinin yanında, aşağıdakilerden birine tıklayın:

- **Tüm ağ trafiğine izin ver**
- **Tüm ağ trafiğini reddet**

d. **Yön** seçeneğinin yanında, kural dışı durum ayarlarının uygulanacağı trafik türünü seçmek için **Gelen** veya **Giden** seçeneğine tıklayın.

e. Protokol listesinden ağ protokolü türünü seçin:

- **Tümü**
- **TCP/UDP** (varsayılan)
- **TCP**
- **UDP**
- **ICMP**
- **ICMPv6**

f. İstemci bağlantı noktalarını belirlemek için aşağıdakilerden birini tıklatın:

- **Tüm bağlantı noktaları** (varsayılan)
- **Aralık**: bağlantı noktası aralığını girin
- **Belirlenen bağlantı noktaları**: tek tek bağlantı noktalarını belirleyin. Bağlantı noktası numaralarını ayırmak için virgül "," kullanın.

g. **Makineler** seçeneğinin altında kural dışı duruma dahil edeceğiniz istemci IP adreslerini seçin. Örneğin, **Tüm ağ trafiğini reddet (Gelen ve Giden)** seçeneğini belirler ve ağ üzerindeki tek bir bilgisayar için IP adresini girerseniz, o zaman ilkesinde bu kural dışı durum bulunan İstemcilerin hiçbiri bu IP adresine veri gönderemez veya buradan veri alamaz. Aşağıdakilerden birine tıklayın:

- **Tüm IP adresleri** (varsayılan)
- **Tek IP**: Bir IPv4 veya IPv6 adresi veya bir ana makine adı girin. İstemci ana makine adını bir IP adresine çözmek için **Çöz** öğesine tıklayın.

- **IP aralığı (IPv4 veya IPv6 için)**: **Kimden** ve **Kime** alanlarına iki adet IPv4 veya iki adet IPv6 adresi girin. Bir alanda IPv6 adresi girmek ve diğer alanda IPv4 adresi girmek mümkün değildir.
- **IP aralığı (IPv6 için)**: Bir IPv6 adresi önekini ve uzunluğunu girin.

h. **Kaydet** öğesine tıklayın.

8. Kural dışı bir durumu düzenlemek için, **Düzenle** öğesine tıklayın ve ardından görüntülenen ekranda ayarları değiştirin.
9. Kural dışı bir durumu listede yukarı veya aşağı taşımak için, kural dışı durumu seçin ve ardından tercih ettiğiniz konumda olana kadar **Yukarı Taşı** veya **Aşağı Taşı** öğesine tıklayın.
10. Bir kural dışı durumu kaldırmak için, kural dışı durumu seçin ve **Kaldır** öğesine tıklayın.

Bir Agent Grubu Üzerindeki Güvenlik Duvarını Devre Dışı Bırakma

Prosedür

1. **Güvenlik Ayarları** kısmına gidin.
2. Bir masaüstü veya sunucu grubu seçin.
3. **Ayarları Yapılandır** öğesine tıklayın.

   Yeni bir ekran belirir.
4. **Güvenlik Duvarı** > **Ofis İçi** veya **Güvenlik Duvarı** > **Ofis Dışı** seçin.

   Yeni bir ekran belirir.
5. **Güvenlik Duvarını Devre Dışı Bırak** seçin.
6. **Kaydet** öğesine tıklayın.

Tüm Aracılar Üzerindeki Güvenlik Duvarını Devre Dışı Bırakma

Prosedür

1. **Tercihler** > **Global Ayarlar** > **Masaüstü/Sunucu** sekmesine gidin.
2. **Güvenlik Duvarı Ayarları** altından, **Güvenlik Duvarını Devre Dışı Bırak ve sürücüleri kaldır** seçin.
3. **Kaydet** öğesine tıklayın.

Web Reputation

Web Reputation, güvenlik tehditleri oluşturan webdeki veya e-posta mesajlarında gömülü URL'lere erişimi önlemeye yardımcı olur. Web Reputation, Trend Micro web reputation sunucularından URL'nin geçmişini kontrol edecektir ve istemci üzerinde zorlanan belirli web reputation ilkelerine göre geçmişi ilişkilendirecektir. Kullanımda olan ilkeye bağlı olarak:

- Security Agent, web sitesini engelleyecek veya erişime izin verecektir.
- Messaging Security Agent (yalnızca Advanced), zararlı URL'leri içeren e-posta mesajını karantinaya alacak, silecek veya etiketleyecektir ya da URL'ler güvenliyse iletinin gönderilmesine izin verecektir.

Web Reputation, algılamalar hakkında hem yöneticilere e-posta bildirimleri hem de kullanıcıya satır içi bildirimler sağlar.

Security Agent'lar için, istemcinin konumuna bağlı olarak (Ofis İçi/Ofis Dışı) farklı bir güvenlik düzeyi yapılandırır.

Web Reputation sizin güvenli olduğuna inandığınız bir URL'yi engelliyorsa, o URL'yi Onaylanan URL listesine ekleyin.

İpucu

Ağ bant genişliği kazanmak için, Trend Micro şirketin dahili web sitelerini Web reputation onaylı URL listesine eklemeyi önerir.

Geçmiş Puanı

Bir URL'nin "geçmiş puanı" onun bir web tehdidi olup olmadığını belirler. Trend Micro, puanı özel ölçümlerden yararlanarak hesaplar.

Trend Micro, bir URL'yi puanı tanımlanan bir eşik altındaysa bir web tehditi olarak ve puanı eşiğin üzerindeyse güvenli olarak dikkate alacaktır.

Bir Security Agent'ın bir URL'ye erişime izin vereceğini veya engelleyeceğini belirleyen üç güvenlik düzeyi vardır.

- **Yüksek**: Aşağıdaki özelliklere sahip sayfaları engeller:
  - **Tehlikeli**: Dolandırıcılık sayfası veya bilinen tehdit kaynağı olduğu doğrulandı
  - **Çok şüpheli**: Dolandırıcılık sayfası veya olası tehdit kaynağı olduğundan şüpheleniliyor
  - **Şüpheli**: Spam ile ilişkili veya muhtemelen tehlikeli olan sayfalar
  - **Test edilmemiş**: Trend Micro web sayfalarını aktif olarak güvenlik için test ediyor olsa da, kullanıcılar yeni veya az popüler web sitelerini ziyaret ederken test edilmemiş sayfalarla karşılaşabilir. Test edilmemiş sayfalara erişimin engellenmesi güvenliği arttırabilir, ancak aynı zamanda güvenli sayfalara erişimi de önleyebilir.
- **Orta**: Aşağıdaki özelliklere sahip sayfaları engeller:
  - **Tehlikeli**: Dolandırıcılık sayfası veya bilinen tehdit kaynağı olduğu doğrulandı
  - **Çok şüpheli**: Dolandırıcılık sayfası veya olası tehdit kaynağı olduğundan şüpheleniliyor
- **Düşük**: Aşağıdaki özelliklere sahip sayfaları engeller:
  - **Tehlikeli**: Dolandırıcılık sayfası veya bilinen tehdit kaynağı olduğu doğrulandı

Security Agent'lar için Web Reputation Yapılandırma

Web Reputation, her HTTP/HTTPS isteğinde Trend Micro Security veritabanını sorgulayarak istenen tüm URL'lerin olası güvenlik riskini değerlendirir.

Nota

(Yalnızca Standard) Ofis İçi ve Ofis Dışı için Web Reputation'ı yapılandırın. Konum Tanıma devre dışı bırakılmışsa, Ofis İçi ayarları Ofis Dışı bağlantılar için kullanılacaktır. Konum Tanıma hakkında ayrıntılar için, bkz. *Masaüstü/Sunucu Ayarlarını Yapılandırma sayfa 11-5*.

Hem Web Reputation hem de Tarayıcı Exploit Önleme etkinleştirilmişse Web Reputation tarafından engellenmemiş URL'ler daha sonra Tarayıcı Exploit Önleme tarafından taranır. Tarayıcı Exploit Önleme, URL'nin internet sitelerindeki gömülü nesneleri tarar (örneğin: jar, class, pdf, swf, html, js).

Prosedür

1. **Güvenlik Ayarları** kısmına gidin.
2. Bir masaüstü veya sunucu grubu seçin.
3. **Ayarları Yapılandır** öğesine tıklayın.

   Yeni bir ekran belirir.
4. **Web Reputation** > **Ofis İçi** veya**Web Reputation** > **Ofis Dışı** seçin.

   Yeni bir ekran belirir.
5. Aşağıdakileri gerektiği gibi güncelleyin:
   - **Web Reputation'ı etkinleştir**
   - Güvenlik Düzeyi: **Yüksek**, **Orta** veya **Düşük**
   - Tarayıcı Exploit Önleme: **Kötü amaçlı komut dosyası içeren sayfaları engelle**
6. **Kaydet** öğesine tıklayın.

URL Filtreleme

URL filtreleme, çalışanların iş dışında uğraşlara ayırdığı zamanı kısıtlamak, Internet bant genişliği kullanımını azaltmak ve daha güvenli bir Internet ortamı yaratmak amacıyla web sitelerine erişimi denetlemenize yardımcı olur. Bir URL filtreleme koruması düzeyi seçebilir veya taramak istediğiniz Web sitesi türlerini özelleştirebilirsiniz.

Nota

Müşterileri korumak için, Trend Micro dünyanın birçok yerinde yasadışı olarak kabul edilen içerik içeren tüm URL'leri otomatik olarak engeller.

URL Filtrelemeyi Yapılandırma

Özel seçeneğini işaretleyerek günün farklı zamanlarında engellenecek özel web sitesi türlerini seçebilirsiniz.

Prosedür

1. **Güvenlik Ayarları** kısmına gidin.
2. Bir masaüstü veya sunucu grubu seçin.
3. **Ayarları Yapılandır** öğesine tıklayın.

   Yeni bir ekran belirir.
4. **URL Filtreleme**'ye tıklayın.

   Yeni bir ekran belirir.
5. Aşağıdakileri gerektiği gibi güncelleyin:
   - **URL Filtrelemeyi Etkinleştir**
   - **Filtre Gücü**
     - **Yüksek**: Bilinen veya potansiyel güvenlik tehditlerini, uygun olmayan veya saldırgan olabilecek içerikleri, üretkenliği veya bant genişliğini etkileyebilecek içeriği ve derecelendirilmemiş sayfaları engeller.

- **Orta**: Bilinen güvenlik tehditlerini ve uygun olmayan içeriği engeller
- **Düşük**: Bilinen güvenlik tehditlerini engeller
- **Özel**: Kendi kategorilerinizi ve çalışma saatlerinde veya çalışma saatleri dışındaki saatlerde kategorilerin engellenmesini isteyip istemediğinizi seçin.

- **Filtre Kuralları**: Engellenecek kategorilerin veya alt kategorilerin tamamını seçin.
- **Çalışma Saatleri**: Çalışma Saatleri altında tanımlanmayan günler veya saatler, Çalışma Saatleri Dışındaki saatler olarak kabul edilir.

6. **Kaydet** öğesine tıklayın.

Onaylanmış/Engellenmiş URL'ler

Otomatik URL onayı ve engellemesi web sitelerine erişimi kontrol etmenize yardımcı olur ve daha güvenli bir İnternet ortamı oluşturur. Global Ayarlar'da onaylanmış veya engellenmiş URL'leri tanımlayın.

Ayrıca, belirli gruplar için özelleştirilmiş URL onay ve engelleme listeleri oluşturmak da mümkündür. **Bu grup için onaylı/engellenmiş URL'leri Özelleştir** seçildiğinde, Security Agent web sitelerine erişimi kontrol etmek için grubun özelleştirilmiş onaylı veya engellenmiş URL'lerinin listesini kullanır.

Onaylanmış/Engellenmiş URL'leri Yapılandırma

Prosedür

1. **Güvenlik Ayarları** kısmına gidin.
2. Bir masaüstü veya sunucu grubu seçin.
3. **Ayarları Yapılandır** öğesine tıklayın.

   Yeni bir ekran belirir.

4. **Onaylanmış/Engellenmiş URL'ler** öğesine tıklayın.

   Yeni bir ekran belirir.

5. Aşağıdakileri gerektiği gibi güncelleyin.

   - **Customize approved/blocked URLs for this group**: Bu listede belirtilen URL'ler diğer tüm ayarları geçersiz kılar.
   - **Onaylanacak URL'ler** metin kutusunda, Web Reputation ve URL Filtreleme doğrulamalarının dışında bırakılacak web sitelerinin URL'lerini girin. Birden fazla URL'yi noktalı virgülle (;) ayırın. **Ekle** öğesine tıklayın.

     İpucu

     Tüm girişleri girmek için **Genel Ayarlar'dan içe aktar** öğesine tıklayın. Daha sonra bu grup için URL'leri özelleştirebilirsiniz.

   - **Engellenecek URL'ler** metin kutusunda, URL Filtreleme sırasında engellenecek web sitelerinin URL'lerini girin. Birden fazla URL'yi noktalı virgülle (;) ayırın. **Ekle** öğesine tıklayın.

     İpucu

     Tüm girişleri girmek için **Genel Ayarlar'dan içe aktar** öğesine tıklayın. Daha sonra bu grup için URL'leri özelleştirebilirsiniz.

6. **Kaydet** öğesine tıklayın.

Behavior Monitoring

Security Agent'lar, istemcilerin işletim sistemi veya yüklenen yazılım üzerindeki normal olmayan değişikliklerini sürekli olarak izler. Yöneticiler (veya kullanıcılar), belirli programların izlenen değişikliği ihlal ederken başlatılmasına veya belirli programların tamamen engellenmesine izin veren kural dışı durum listeleri oluşturabilir. Ek olarak, geçerli bir dijital imza içeren programların başlatılmasına her zaman izin verilir.

Behavior Monitoring'in diğer bir özelliği EXE ve DLL dosyalarını silinmeye veya değiştirilmeye karşı korur. Behavior Monitoring etkinleştirildiğinde, kullanıcılar onaylama

veya belirli programları engelleme için özel durumlar oluştururlar. Ek olarak, kullanıcılar tüm Intuit QuickBooks programlarının toplu olarak korunmasını seçebilir.

Behavior Monitoring'i Yapılandırma

Prosedür

1. **Güvenlik Ayarları** kısmına gidin.
2. Bir masaüstü veya sunucu grubu seçin.
3. **Ayarları Yapılandır** öğesine tıklayın.
4. **Behavior Monitoring** öğesine tıklayın.
5. Aşağıdakileri gerektiği gibi güncelleyin:
   - **Behavior Monitoring'i Etkinleştir**

     Nota

     Kullanıcıların kendi Behavior Monitoring ayarlarını özelleştirmelerine olanak tanımak için, **Güvenlik Ayarları** > **{grup}** > **Yapılandır** > **İstemci Ayrıcalıkları** > **Behavior Monitoring**'e gidin ve **Kullanıcıların Behavior Monitoring ayarlarını değiştirmesine izin ver**'i seçin.

   - **Bilinen ve potansiyel tehditler için Malware Behavior Blocking'i etkinleştir**: Malware behavior blocking'e, **kalıp dosyalarında** tanımlanan bir dizi iç kural kullanılarak ulaşılır. Bu kurallar, kötü amaçlı yazılımlar arasında yaygın olan bilinen şüpheli tehdit davranışını tanımlar. Şüpheli davranış örnekleri, ani ve açıklanamayan yeni çalışan hizmetler, güvenlik duvarında değişiklikler, veya sistem dosyası değişikliklerini içerir.
     - **Bilinen tehditler**: Bilinen tehditlerle bağlantılı davranışı engeller
     - **Bilinen potansiyel tehditler**: Bilinen tehditlerle bağlantılı davranışı engeller ve kötü amaçlı olma olasılığı olan davranışla ilgili işlem yapar
   - **HTTP ile indirilmiş, daha önceden karşılaşılmamış programları çalıştırmadan önce kullanıcılara haber ver (sunucu platformları hariç)**:

Behavior Monitoring, HTTP kanalları veya e-posta uygulamaları yoluyla indirilmiş dosyaların geçerliliğini doğrulamak için Web Reputation ile birlikte çalışır. "Yeni karşılaşılan" bir dosya tespit ettikten sonra, yönetici dosyayı çalıştırmadan önce kullanıcılara sormayı tercih edebilir. Trend Micro, bir programı dosya tespit sayısına veya Smart Protection Network tarafından belirlenen dosyanın tarihi yaşına dayalı olarak yeni karşılaşılan olarak sınıflandırır.

Nota

HTTP kanalları için çalıştırılabilir (.exe) dosyaları taranır. Eposta uygulamalarında (sadece Outlook ve Windows Live Mail), parola koruması olmayan arşivli (zip/rar) dosyalardaki çalıştırılabilir (.exe) dosyalar taranır.

- **Intuit QuickBooks Korumasını Etkinleştir**: Tüm Intuit QuickBooks dosyalarını ve klasörlerini diğer programlar tarafından yapılacak yetkisiz değişiklere karşı korur. Bu özelliği etkinleştirilmesi Intuit QuickBooks programları içinde yapılan değişiklikleri etkilemez, yalnız diğer yetkisiz uygulamalar tarafından dosyalara yapılan değişiklikleri önler.

  Aşağıdaki ürünler desteklenir:

  - QuickBooks Basit Başlatma
  - QuickBooks Pro
  - QuickBooks Premier
  - QuickBooks Çevrimiçi

Nota

Tüm yürütülebilir Intuit dosyaları, dijital bir imzaya sahiptir ve bu dosyaların güncellemeleri engellenmez. Başka programlar Intuit ikili dosyasını değiştirmeye çalışıyorsa, Aracı ikili dosyaları güncellemeye çalışan programın adını içeren bir ileti görüntüler. Diğer programların Intuit dosyalarını güncellemesine izin verilebilir. Bunu yapmak için, Aracıda Behavior Monitoring Kural Dışı Durum Listesine gerekli programı ekleyin. Güncellemenin ardından programı kural dışı durum listesinden kaldırmayı unutmayın.

- **Fidye Yazılımı Koruması** altında aşağıdakileri güncelleyin:

Nota

Fidye Yazılımı Koruması, "fidye yazılımı" tehditleri tarafından bilgisayarlardaki dosyaların yetkisiz değiştirilmesini veya şifrelenmesini önler. Fidye yazılımı, dosyalara erişimi kısıtlayan ve etkilenen dosyaları geri yüklemek için ödeme talep eden bir kötü amaçlı yazılım türüdür.

- **Yetkisiz şifreleme veya değişikliğe karşı belge korumasını etkinleştir**: Belgeleri yetkisiz değişikliklere karşı korur.
    - **Şüpheli programların değiştirdiği dosyaları otomatik yedekle**: Belge koruması etkinleştirildiyse şüpheli programların değiştirdiği dosyaları otomatik olarak yedekler.
- **Yaygın olarak fidye yazılımı ile bağlantılı olan işlemlerin engellenmesini etkinleştir**: Genel olarak bilgisayar korsanlığı girişimleriyle bağlantılandırılan işlemleri engelleyerek uç noktaları fidye yazılımı saldırılarına karşı korur.

Nota

WFBS uygulamasının güvenli bir işlemi kötü amaçlı olarak algılama olasılığını azaltmak için bilgisayarın Trend Micro sunucularını kullanarak ek doğrulama işlemleri gerçekleştirmek için İnternet erişiminin olduğundan emin olun.

- **Kural dışı durumlar**: Kural dışı durumlar, Onaylanan Program Listesini ve Engellenen Program Listesini içerir. Engellenen Program Listesi içindeki programlar asla başlatılamazken, Onaylanan Programlar Listesi içindeki programlar izlenen değişikliği ihlal etseler bile başlatılabilir.
    - **Program Tam Yolunu Gir**: Programın tam Windows veya UNC yolunu yazın. Birden fazla girdileri noktalı virgülle ayırın. **Onaylanan Listesine Ekle** veya **Engellenen Listesine Ekle** öğesine tıklayın. Gerekirse yolları belirtmek için ortam değişkenlerini kullanın.

ORTAM DEĞİŞKENİ	İŞARET ETTİĞİ YER...
$windir$	Windows klasörü
$rootdir$	kök klasör

Ortam Değişkeni	İşaret ettiği yer...
$tempdir$	Windows geçici klasörü
$programdir$	Program Dosyaları klasörü

- **Onaylanan Program Listesi**: Bu listedeki programlar (maksimum 100) başlatılabilir. Bir girişi silmek için ilişkili simgeye tıklayın
- **Engellenen Program Listesi**: Bu listedeki programlar (maksimum 100) hiçbir zaman başlatılamaz. Bir girişi silmek için ilişkili simgeye tıklayın

6. **Kaydet** öğesine tıklayın.

Güvenilen Program

Güvenilen Program Listesinde yer alan programlar, şüpheli dosya erişim etkinlikleri için izlenmeyecektir.

Güvenilen Program Yapılandırma

Prosedür

1. **Güvenlik Ayarları** kısmına gidin.
2. Bir masaüstü veya sunucu grubu seçin.
3. **Ayarları Yapılandır** öğesine tıklayın.

   Yeni bir ekran belirir.
4. **Güvenilen Program** öğesine tıklayın.

   Yeni bir ekran belirir.
5. Bir programı şüpheli dosya etkinliği izlemesinden hariç tutmak için özel bir dosya yolu kullanarak tüm dosya yolunu girin ve **Güvenilen Programlar Listesine Ekle** öğesine tıklayın.

<drive_name>:/<path>/<file_name>

Örnek 1: C:\Windows\system32\regedit.exe

Örnek 2: D:\backup\tool.exe

Bu, saldırganların program adlarını dışlama listesinde kullanmasını engeller ancak bu programlar farklı bir dosya yoluna düşer.

6. **Kaydet** öğesine tıklayın.

Cihaz Denetimi

Cihaz Denetimi, istemcilere bağlı olan harici depolama aygıtlarına ve ağ kaynaklarına erişimi düzenler. Cihaz Denetimi, akıllı telefonlar ve dijital kameralar hariç, özellikle bir USB arayüzü aracılığıyla bağlanan tüm türdeki depolama aygıtlarına erişimi kısıtlar.

Aygıt Denetimini Yapılandırma

Prosedür

1. **Güvenlik Ayarları** kısmına gidin.
2. Bir masaüstü veya sunucu grubu seçin.
3. **Politikayı Yapılandır** öğesine tıklayın.

   Yeni bir ekran belirir.
4. **Aygıt Denetimi** öğesine tıklayın.

   Yeni bir ekran belirir.
5. Aşağıdakileri gerektiği gibi güncelleyin:
   - **Aygıt Denetimini Etkinleştir**
   - **USB Otomatik Çalıştırma Önlemeyi Etkinleştir**

- **İzinler**: Hem USB aygıtları hem de ağ kaynakları için ayarlayın.

TABLO 5-7. Aygıt Denetimi İzinleri

İZİNLER	AYGIT ÜZERİNDEKİ DOSYALAR	GELEN DOSYALAR
Tam erişim	İzin verilen işlemler: Kopyala, Taşı, Aç, Kaydet, Sil, Yürüt	İzin verilen işlemler: Kaydet, Taşı, Kopyala Bu, bir dosyanın kaydedilebileceği, taşınabileceği ve bir aygıta kopyalanabileceği anlamına gelir.
Değiştirme	İzin verilen işlemler: Kopyala, Taşı, Aç, Kaydet, Sil İzin verilmeyen işlemler: Yürüt	İzin verilen işlemler: Kaydet, Taşı, Kopyala
Oku ve yürüt	İzin verilen işlemler: Kopyala, Aç, Yürüt İzin verilmeyen işlemler: Kaydet, Taşı, Sil	İzin verilmeyen işlemler: Kaydet, Taşı, Kopyala
Oku	İzin verilen işlemler: Kopyala, Aç İzin verilmeyen işlemler: Kaydet, Taşı, Sil, Yürüt	İzin verilmeyen işlemler: Kaydet, Taşı, Kopyala
Erişilemiyor	İzin verilmeyen işlemler: Tüm işlemler Aygıt ve içerdiği dosyalar kullanıcı tarafından görülür (örneğin, Windows Explorer'dan).	İzin verilmeyen işlemler: Kaydet, Taşı, Kopyala

- **Kural dışı durumlar**: Kullanıcıya belirli bir aygıt için okuma izni verilmediyse de, Onaylanan Listesi'ndeki herhangi bir dosyayı veya programı çalıştırma veya açma izni verilir.

Ancak, Otomatik Çalıştırma önleme etkinse, bir dosya Onaylanan Listesi'nde yer alsa bile çalışmasına izin verilmez.

Onaylanan Listesi'ne kural dışı durum eklemek için yolu veya dijital imzayı içeren dosya adını girin ve **Onaylanan Listesi'ne Ekle** öğesine tıklayın

6. **Kaydet** öğesine tıklayın.

Kullanıcı Araçları

- **Anti-Spam Araç Çubuğu**: Microsoft Outlook'ta spam iletileri filtreler, istatistikleri verir ve belirli ayarları değiştirmenize imkan sağlar.
- **HouseCall**: SSID'lerinin geçerliliğine, kimlik doğrulama yöntemlerine ve şifreleme gereksinimlerine dayanarak erişim noktalarının doğrululuğunu denetlemek suretiyle bir kablosuz bağlantının güvenli olup olmadığını belirler. Bir bağlantı güvenli değilse, açılan bir uyarı ile gösterilir.
- **Durum Tanı Aracı**: Trend Micro Durum Tanı Aracı (CDT), problemler oluştuğunda bir müşterinin ürününden gerekli hata ayıklama bilgisini toplar. Ürünün hata ayıklama durumunu otomatik olarak açık veya kapalı hale getirir ve problem kategorilerine göre gerekli dosyaları toplar. Trend Micro, bu bilgileri ürünler ilgili problemlerde sorun giderme için kullanır.

  Bu araç sadece Security Agent konsolu üzerinde kullanılabilir.
- **Client Mover**: İstemcileri bir sunucudan diğerine aktarmak için bu aracı kullanın. Sunucular aynı dil sürümü ve türüne sahip olmalıdır.
- **İstemci-Sunucu Haberleşme Aracı**: İstemci-sunucu haberleşme sorunlarını gidermek için bu aracı kullanın.

Kullanıcı Araçlarını Yapılandırma

Prosedür

1. **Güvenlik Ayarları** kısmına gidin.

2. Bir masaüstü veya sunucu grubu seçin.
3. **Ayarları Yapılandır** öğesine tıklayın.

   Yeni bir ekran belirir.
4. **Kullanıcı Araçları**'nı tıklayın.

   Yeni bir ekran belirir.
5. Aşağıdakileri gerektiği gibi güncelleyin:
   - **Wi-Fi Advisor**: SSID'lerinin geçerliliğine, kimlik doğrulama yöntemlerine ve şifreleme gereksinimlerine dayanılarak kablosuz ağların güvenliğini denetler.
   - **Anti-Spam Araç Çubuğu**: Microsoft Outlook'taki spam'i filtreler.
6. **Kaydet** öğesine tıklayın.

İstemci Ayrıcalıkları

Kullanıcıların, istemci üzerindeki Security Agent ayarlarını değiştirmesine izin vermek için istemci ayrıcalıkları verin.

İpucu

Organizasyonunuz içinde düzenlenmiş bir güvenlik ilkesini gerçekleştirmek için Trend Micro kullanıcılara sınırlı ayrıcalık vermenizi önerir. Bu, kullanıcıların tarama ayarlarını değiştirmemesini veya Security Agent'ı bellekten kaldırmamasını sağlar.

Aracı Ayrıcalıklarını Yapılandırma

Prosedür

1. **Güvenlik Ayarları** kısmına gidin.
2. Bir masaüstü veya sunucu grubu seçin.

3. **Ayarları Yapılandır** öğesine tıklayın.
4. **Aracı Ayrıcalıkları** öğesine tıklayın.
5. Aşağıdakileri gerektiği gibi güncelleyin:

BÖLÜM	AYRICALIKLAR
Antivirüs/Casus yazılımdan koruma	• Manuel Tarama ayarları • Zamanlanmış Tarama ayarları • Gerçek Zamanlı Tarama ayarları • Zamanlanmış Taramayı Atla
Güvenlik Duvarı	Güvenlik Duvarı Ayarları
Web Reputation - Taramaya Devam Et	Bilgisayar yeniden başlatılana kadar kullanıcıların belirli bir kötü amaçlı URL'yi taramasına olanak sağlayan bir bağlantı gösterir. Diğer kötü amaçlı URL'lerle ilgili uyarılar gösterilmeye devam eder.
URL Filtreleme - Taramaya Devam Et	Bilgisayar yeniden başlatılana kadar kullanıcıların belirli bir kısıtlanmış URL'yi taramasına olanak sağlayan bir bağlantı gösterir. Diğer kısıtlanmış URL'lerle ilgili uyarılar gösterilmeye devam eder.
Behavior Monitoring	Kullanıcıların Behavior Monitoring ayarlarını değiştirmesine olanak sağlayın.
Güvenilir Program	Kullanıcıların Güvenilir Program listesini değiştirmesine olanak sağlayın.
Proxy Ayarları	Kullanıcıların proxy ayarlarını yapılandırmasına olanak sağlayın. **Nota** Bu özelliği devre dışı bırakmak proxy ayarlarını varsayılan değerlerine döndürür.

BÖLÜM	AYRICALIKLAR
Güncelleme Ayrıcalıkları	• Kullanıcıların manuel güncellemeler yapmasına olanak sağlar • Trend Micro ActiveUpdate'i ikincil güncelleme kaynağı olarak kullan • Düzeltme dağıtımını devre dışı bırak **Nota** Düzeltmeleri, yamaları, güvenlik yamalarını/kritik yamaları ve hizmet paketlerini çok sayıda aracıya aynı anda dağıtmak ağ trafiğini önemli ölçüde arttırabilir. Bu seçeneği birkaç grupta etkinleştirerek dağıtımı kademelendirebilirsiniz. Bu seçeneği etkinleştirmek aracılardaki otomatik **yapı yükseltmelerini** (örneğin, geçerli ürün sürümünün Beta yapısından sürüm yapısına) de devre dışı bırakır; ancak otomatik **sürüm yükseltmelerini** (örneğin, 7.x sürümünden güncel sürüme) devre dışı BIRAKMAZ. Otomatik sürüm yükseltmelerini devre dışı bırakmak için, Security Server yükleme paketini çalıştırın ve güncellemeleri erteleme seçeneğini belirleyin.
Client Security	Kullanıcıların veya diğer işlemlerin Trend Micro program dosyalarında, kayıt defterlerinde ve işlemlerinde değişiklik yapmasını önleyin.

6. **Kaydet** öğesine tıklayın.

Karantina Dizini

Etkilenmiş bir dosya için eylem "Karantina" ise, security Agent dosyayı şifreler ve **geçici** olarak şuradaki karantina dosyasına taşır:

- <Security Agent yükleme klasörü>\quarantine , sürüm 6.x veya öncesinden yükseltilen aracılar için

- <Security Agent yükleme klasörü>\SUSPECT\Backup, yeni kurulmuş aracılar ve sürüm 7.x veya sonrasından yükseltilmişler için

Security Agent etkilenmiş dosyayı, web konsolundan yapılandırabileceğiniz merkezi karantina dizinine gönderir, **Güvenlik Ayarları** > **{Grup}** > **Yapılandır** > **Karantina**.

Varsayılan Merkezi Karantina Dizini

Varsayılan merkezi karantina dizini Security Server üzerinde yer alır. Dizin, URL biçimindedir ve http://server gibi Security Server'ın ana makine adını veya IP adresini içermektedir. Eşdeğer mutlak yol, <Security Server yükleme klasörü>\PCCSRV\Virus.

- Sunucu IPv4 ve IPv6 aracılarının ikisini de yönetiyorsa, ana makine adını tüm aracılar karantinaya alınmış dosyaları sunucuya gönderebilecek şekilde kullanın.
- Sunucuda sadece IPv4 adresi mevcutsa veya sadece bu adresle tanımlanıyorsa, sadece salt IPv4 ve çift-yığın aracılar karantinaya alınmış dosyaları sunucuya gönderebilir.
- Sunucuda sadece IPv6 adresi mevcutsa veya sadece bu adresle tanımlanıyorsa, sadece salt IPv6 ve çift-yığın aracılar karantinaya alınmış dosyaları sunucuya gönderebilir.

Alternatif Merkezi Karantina Dizini

Konumu URL, UNC yolu veya mutlak dosya yolu biçiminde girerek alternatif bir merkezi karantina dizini belirtebilirsiniz. Security Agent'lar bu dizine bağlanabiliyor olmalıdır. Örneğin, çift yığınlı ve salt IPv6 aracılardan karantinaya alınmış dosyaları alacaksa, dizinin IPv6 adresi olmalıdır. Trend Micro, çift yığınlı bir dizin belirtmenizi, dizini ana makine adıyla tanımlamanızı ve dizini girerken UNC yolunu kullanmanızı tavsiye eder.

Merkezi Karantina Dizinini Belirtme Yönergeleri

Ne zaman URL, UNC yolu veya mutlak dosya yolu kullanılacağı hakkında kılavuzluk etmesi için aşağıdaki tabloya bakın:

TABLO 5-8. Karantina Dizini

KARANTİNA DİZİNİ	KABUL EDİLEN BİÇİM	ÖRNEK	NOTLAR
Security Server üzerindeki varsayılan dizin	URL	http:// <sunucu ana makine adı veya IP>	Varsayılan dizini tutarsanız, **Tercihler** > **Genel Ayarlar** > **Sistem sekmesi** > **Karantina Bakımı** bölümünden dizin için karantina klasörünün boyutu gibi bakım ayarlarını yapılandırın.
	UNC yolu	\\<sunucu ana makine adı veya IP>\ ofcscan \Virus	
Security Server üzerinde başka bir dizin	UNC yolu	\\<sunucu ana makine adı veya IP>\ D$ \Quarantined Files	Varsayılan dizini kullanmak istemiyorsanız (örneğin disk alanı yetersizse), UNC yolu için başka bir dizin girin. Bunu yaparsanız, bakım ayarlarının etkin olmasına imkan sağlamak için **Tercihler** > **Genel Ayarlar** > **Sistem sekmesi** > **Karantina Bakımı** bölümünden denk gelen mutlak yolu girin.
Başka bir Security Server üzerindeki bir dizin (ağ üzerinde başka Security Server'lar varsa)	URL	http:// <sunucu2 ana makine adı veya IP>	Aracıların bu dizine bağlanabileceğinden emin olun. Hatalı bir dizin belirtirseniz, aracı doğru karantina dizini belirtilene kadar karantinaya alınmış dosyaları tutar. Sunucunun virüs/ kötü amaçlı yazılım günlüklerinde, tarama sonucu "Karantinaya alınan dosyalar belirlenen karantina klasörüne gönderilemedi" olur. UNC yolunu kullanırsanız, karantina dizini klasörünün "Herkes" grubuyla paylaşımda olduğundan ve bu gruba okuma ve yazma izni atadığınızdan emin olun.
	UNC yolu	\\<sunucu2 ana makine adı veya IP>\ ofcscan \Virus	
Ağ üzerinde başka bir bilgisayar	UNC yolu	\\<computer_ name> \temp	

KARANTİNA DİZİNİ	KABUL EDİLEN BİÇİM	ÖRNEK	NOTLAR
İstemci üzerinde farklı bir dizin	Mutlak yol	C:\temp	Şu durumda mutlak bir yol belirtin: • Karantinaya alınan dosyaları sadece istemcide tutmak istiyorsanız. • Aracıların dosyaları istemcideki varsayılan dizinde tutmasını istemiyorsanız. Yol mevcut değilse, Security Agent otomatik olarak oluşturacaktır.

Karantina Dizinini Yapılandırma

Prosedür

1. **Güvenlik Ayarları** kısmına gidin.
2. Bir masaüstü veya sunucu grubu seçin.
3. **Ayarları Yapılandır** öğesine tıklayın.

   Yeni bir ekran belirir.
4. **Karantinaya Al** öğesine tıklayın.

   Yeni bir ekran belirir.
5. Karantina dizinini yapılandırın. Ayrıntılar için, bkz. *Karantina Dizini sayfa 5-30*.
6. **Kaydet** öğesine tıklayın.

Bölüm 6

Messaging Security Agent için Temel Güvenlik Ayarlarını Yönetme (Yalnızca Advanced)

Bu bölümde Messaging Security Agent tanımlanmakta ve aracı için Gerçek Zamanlı Tarama seçeneklerinin nasıl ayarlanacağı ve anti-spam, içerik filtreleme, ek engelleme, karantina bakımı seçeneklerinin nasıl yapılandırılacağı açıklanmaktadır.

Messaging Security Agent'lar

Messaging Security Agent'lar, Microsoft Exchange sunucularını korur. Aracı, Microsoft Exchange Posta Kutusu Deposu içine giren ve oradan çıkan e-postalarının yanı sıra Microsoft Exchange Server ile harici hedefler arasında gidip gelen e-postaları da tarayarak e-posta kaynaklı tehditlerin önlenmesine yardımcı olur. Buna ek olarak, Messaging Security Agent şunları da yapabilir:

- Spam'i azaltma
- içeriğe dayalı olarak e-posta iletilerini engelleme
- Ekli e-postaları engelleyebilir veya sınırlama
- E-postadaki zararlı URL'leri algılama
- Gizli veri sızıntılarını önleme

Messaging Security Agent'lar hakkında Önemli Bilgiler

- Messaging Security Agent'lar, yalnızca Microsoft Exchange sunucularına yüklenebilir.
- Web konsolundaki Güvenlik Grupları Ağacı, tüm Messaging Security Agent'ları görüntüler. Birden çok Messaging Security Agent bir grup içinde birleştirilemez; her Messaging Security Agent ayrı olarak idare edilir ve yönetilir.
- WFBS, Microsoft Exchange sunucularından güvenlik bilgisi toplamak için Messaging Security Agent'ı kullanır. Örneğin, spam algılamaları veya bileşen güncellemelerinin tamamlanması, Messaging Security Agent tarafından Security Server'a bildirilir. Bu bilgiler Web konsolunda görüntülenir. Security Server, bu bilgileri aynı zamanda Microsoft Exchange sunucularınızın güvenlik durumu hakkında günlük ve raporlar oluşturmak için de kullanır.

  Algılanan her tehdit bir günlük girişi/bildirimi oluşturur. Bu, Messaging Security Agent'ın tek bir e-postada birden fazla tehdit algılaması durumunda birden fazla günlük girişi ve bildirimi oluşturacağı anlamına gelir. Özellikle, Outlook 2003'te önbellek modunu kullanıyorsanız, aynı tehdidin birden fazla kez algılandığı durumlar da olabilir. Önbellek modu etkinleştirildiğinde, aynı tehdit hem taşıma sırası klasöründe hem de Gönderilmiş Öğeler klasöründe veya Giden Kutusu klasöründe algılanabilir.

- Messaging Security Agent, Microsoft Exchange Server 2007 çalıştıran bilgisayarlarda SQL Server veritabanı kullanır. Sorunları önlemek için, Messaging Security Agent hizmetleri SQL Sunucu hizmeti durumuna `MSSQL$SCANMAIL` bağlı olarak tasarlanmıştır. Bu örnek her durdurulduğunda veya yeniden başlatıldığında, aşağıdaki Messaging Security Agent hizmetleri de durdurulur:

  - `ScanMail_Master`
  - `ScanMail_RemoteConfig`

  `MSSQL$SCANMAIL` durdurulursa veya yeniden başlatılırsa, bu hizmetleri manuel olarak yeniden başlatın. SQL Server'ın güncellenmesi gibi farklı olaylar, `MSSQL $SCANMAIL`'in yeniden başlatılmasına veya durdurulmasına neden olabilir.

Messaging Security Agent E-Posta İletilerini Nasıl Tarar

Messaging Security Agent, e-posta iletilerini taramak için aşağıdaki sıralamayı kullanır:

1. Spam taraması yapar (Anti-spam)
   a. E-postayı Yönetici'nin Onaylanan/Engellenen Gönderenler listesiyle karşılaştırır
   b. Kimlik avı olaylarını kontrol eder
   c. E-postayı Trend Micro tarafından sağlanan kural dışı durum listesiyle karşılaştırır
   d. E-postayı Spam imzası veritabanıyla karşılaştırır.
   e. Tahmini tarama kurallarını uygular
2. İçerik filtreleme kuralı ihlalleri için tarama yapar
3. Kullanıcı tanımlı parametreleri aşan ekler için tarama yapar
4. Virüs/kötü amaçlı yazılım için tarama yapar (Antivirüs)
5. Zararlı URL taraması yapar

Varsayılan Messaging Security Agent Ayarları

Messaging Security Agent yapılandırmalarınızı en iyi duruma getirmeye yardımcı olmak için, tabloda listelenen seçenekleri göz önünde bulundurun.

TABLO 6-1. Messaging Security Agent için Trend Micro Varsayılan Eylemleri

TARAMA SEÇENEĞİ	GERÇEK ZAMANLI TARAMA	MANUEL VE ZAMANLANMIŞ TARAMA
İstenmeyen E-postadan Koruma		
Spam	İletiyi kullanıcının spam klasöründe karantinaya al (varsayılan, Outlook Önemsiz E-posta veya Son Kullanıcı Karantinası yüklüyse)	Uygulanamaz
Kimlik Avı	İletinin tamamını sil	Uygulanamaz
İçerik filtreleme		
Tanımlanan herhangi bir koşulla eşleşen iletileri filtrele	İletinin tamamını karantinaya al	Değiştir
Tanımlanan tüm koşullarla eşleşen iletileri filtrele	İletinin tamamını karantinaya al	Uygulanamaz
Belirli e-posta hesaplarının ileti içeriğini izle	İletinin tamamını karantinaya al	Değiştir
Belirli e-posta hesapları için kural dışı durum oluştur	Geçiş	Geçiş
Ek engelleme		
Eylem	Eki metin/dosya ile değiştir	Eki metin/dosya ile değiştir
Diğer		

Tarama Seçeneği	Gerçek Zamanlı Tarama	Manuel ve Zamanlanmış Tarama
Şifrelenmiş ve Parola korumalı dosyalar	Geçiş (Eylemi Geçiş olarak yapılandırdığınızda, şifrelenmiş ve parola korumalı dosyalar geçer ve bu etkinliğin günlüğü tutulmaz)	Geçiş (Eylemi Geçiş olarak yapılandırdığınızda, şifrelenmiş ve parola korumalı dosyalar geçer ve bu etkinliğin günlüğü tutulmaz)
Dışlanan dosyalar (Belirlenmiş tarama kısıtlamalarının üstündeki dosyalar)	Geçiş (Eylemi Geçiş olarak yapılandırdığınızda, belirlenmiş tarama kısıtlamalarının üstündeki dosyalar ya da ileti gövdesi geçer ve bu etkinliğin günlüğü tutulmaz)	Geçiş (Eylemi Geçiş olarak yapılandırdığınızda, belirlenmiş tarama kısıtlamalarının üstündeki dosyalar ya da ileti gövdesi geçer ve bu etkinliğin günlüğü tutulmaz)

Messaging Security Agent'lar için Gerçek Zamanlı Tarama

Gerçek Zamanlı Tarama tutarlı ve sürekli bir taramadır. **Messaging Security Agent** (yalnızca Advanced); gelen iletilerin, SMTP iletilerinin, ortak klasörlere kopyalanan belgelerin ve diğer Microsoft Exchange sunucularından çoğaltılan dosyaların taramasını yaparak bilinen tüm virüs giriş noktalarını korur.

Messaging Security Agent'lar için Gerçek Zamanlı Tarama Yapılandırma

Prosedür

1. **Güvenlik Ayarları** kısmına gidin.
2. Bir Messaging Security Agent seçin.
3. **Ayarları Yapılandır** öğesine tıklayın.

   Yeni bir ekran belirir.

4. **Antivirüs** öğesine tıklayın.

   Yeni bir ekran belirir.

5. **Gerçek zamanlı antivirüsü etkinleştir** seçin.

6. Tarama ayarlarını yapılandırın. Ayrıntılar için, bkz. *Tarama Hedefleri ve Messaging Security Agent'lar için Eylemler sayfa 7-17*.

7. **Kaydet** öğesine tıklayın.

   Bir etkinlik gerçekleştiğinde bildirim alacak kişileri yapılandırın. Bkz. *Bildirimler için Olayları Yapılandırma sayfa 9-3*.

İstenmeyen e-postadan koruma

WFBS, spam'le mücadele etmek için iki yöntem sunar—**Email Reputation** ve **İçerik Taraması**.

Messaging Security Agent, spam ve kimlik avı olaylarına ilişkin e-posta iletilerini filtrelemek için aşağıdaki bileşenleri kullanır:

- Trend Micro Anti-Spam Motoru
- Trend Micro spam kalıp dosyaları

Trend Micro motoru ve kalıp dosyasını sık sık günceller ve indirmeye hazır duruma getirir. Security Server bu bileşenleri manuel veya zamanlanmış güncelleme yoluyla indirebilir.

Anti-spam motoru, e-posta iletilerini filtrelemek için spam imzaları ve tahmini kuralları kullanır. E-posta iletilerini tarar ve her birine kalıp dosyasındaki kurallara ve kalıplara ne kadar yakından uyduğuna dayalı olarak bir spam puanı atar. Messaging Security Agent, spam puanını kullanıcı tarafından tanımlanan spam algılama düzeyiyle karşılaştırır. Spam puanı algılama düzeyini geçtiğinde, aracı spam'e karşı eylemde bulunur.

Örneğin: Spam gönderenler çoğu zaman e-posta iletilerinde birçok ünlem işareti veya birçok ardışık ünlem işareti (!!!!) kullanırlar. Messaging Security Agent, bu şekilde ünlem işaretleri kullanan bir ileti algıladığında, söz konusu e-posta iletisi için spam puanını arttırır.

İpucu

Spam kontrolü yapmak için Anti-Spam kullanmaya ek olarak, ileti başlığı, konusu, gövdesi ve ek bilgisini spam ve diğer istenmeyen içeriğe karşı filtrelemek için İçerik Filtreleme özelliğini yapılandırabilirsiniz.

Kullanıcılar istenmeyen e-postadan koruma motorunun spam puanlarını atamak için kullandığı yöntemi değiştiremezler, ancak Messaging Security Agent tarafından nelerin spam olduğuna ve nelerin olmadığına karar vermek için kullanılan algılama düzeylerini ayarlayabilirler.

Nota

Microsoft Outlook, Messaging Security Agent'ın spam olarak algıladığı iletileri otomatik olarak filtreleyebilir ve Önemsiz E-posta klasörüne gönderebilir.

Email Reputation

Email Reputation teknolojisi, kaynak Posta Aktarım Aracısı'nın (MTA) geçmişine bağlı olarak spam'i belirler. Bu, Security Server'ı bu görevin yükünden kurtarır. Email Reputation etkinleştirildiğinde, kaynak IP adresinin temiz olduğundan ve bilinen bir spam vektörü olarak listeye alınmadığından emin olmak üzere tüm gelen SMTP trafiği IP veritabanları tarafından denetlenir.

Email Reputation için iki hizmet düzeyi vardır. Bunlar şu şekildedir:

- **Standart**: Standard hizmeti, yaklaşık iki milyar IP adresinin geçmişini izleyen bir veritabanını kullanır. Sıklıkla spam iletileriyle ilişkilendirilen IP adresleri, veritabanına eklenir ve nadiren veritabanından çıkarılır.
- **Gelişmiş**: Advanced hizmet düzeyi Standart hizmet gibi sorguya dayalı bir hizmet olan DNS'dir. Bu hizmetin temelinde standart geçmiş veritabanı ile bilinen ve şüpheli spam kaynaklarından gelen iletileri engelleyen dinamik geçmiş, gerçek zamanlı veritabanı yer alır.

Engellenmiş veya şüpheli bir IP adresinden gelen bir e-posta iletisi bulunduğunda, Email Reputation iletiyi geçidinize ulaşmadan engeller.

Email Reputation'ı Yapılandırma

Email Reputation'ı, bilinen veya şüphe duyulan spam kaynaklarından gelen iletileri engelleyecek şekilde yapılandırın. Ayrıca, diğer gönderenlerden gelen iletilere izin vermek veya onları engellemek için kural dışı durumlar oluşturun.

Prosedür

1. **Güvenlik Ayarları** kısmına gidin.
2. Bir Messaging Security Agent seçin.
3. **Ayarları Yapılandır** öğesine tıklayın.

   Yeni bir ekran belirir.
4. **Anti-spam** > **Email Reputation** öğesine tıklayın.

   Yeni bir ekran belirir.
5. **Hedef** sekmesinden, aşağıdakileri gerektiği gibi güncelleyin:
   - **Gerçek zamanlı Anti-Spam'ı etkinleştir (Email Reputation)**
   - **Hizmet Düzeyi**:
     - **Standart**
     - **Gelişmiş**
   - **Onaylanan IP Adresleri**: Bu IP adreslerinden gelen e-posta iletileri hiçbir zaman engellenmeyecektir. Onaylanacak IP adresini girin ve **Ekle** öğesine tıklayın. Gerekirse, bir metin dosyasından IP adreslerinin listesini içe aktarabilirsiniz. Bir IP adresini kaldırmak için, adresi seçin ve **Kaldır** öğesine tıklayın.
   - **Engellenen IP Adresleri**: Bu IP adreslerinden gelen e-posta iletileri her zaman engellenecektir. Engellenecek IP adresini girin ve **Ekle** öğesine tıklayın. Gerekirse, bir metin dosyasından IP adreslerinin listesini içe aktarabilirsiniz. Bir IP adresini kaldırmak için, adresi seçin ve **Kaldır** öğesine tıklayın.
6. **Kaydet** öğesine tıklayın.

7. Raporları görüntülemek için, http://ers.trendmicro.com/ adresine gidin.

Nota

Email Reputation, Web tabanlı bir hizmettir. Yöneticiler, hizmet düzeyini yalnızca web konsolundan yapılandırabilir.

İçerik Taraması

İçerik Taraması, spam'i kaynak IP yerine iletinin içeriğine dayalı olarak tanımlar. Messaging Security Agent, her e-posta iletisini Bilgi Deposu'na iletmeden önce spam'e karşı taramak için Trend Micro anti-spam motorunu ve spam kalıbı dosyalarını kullanır. Microsoft Exchange server, reddedilen spam postayı işlemeyecek, böylece iletiler kullanıcının posta kutularına ulaşmayacaktır.

Nota

İçerik Taraması ile (imza ve tahminlere dayalı istenmeyen e-postadan korunma) İçerik Filtrelemeyi (sınıflandırılmış anahtar kelimelere dayalı e-posta tarama ve engelleme) birbirine karıştırmayın. Bkz. *İçerik Filtreleme sayfa 6-14*.

İçerik Taramasını Yapılandırma

Messaging Security Agent, Microsoft Exchange Sunucularını korumak için spam iletileri **gerçek zamanlı** olarak algılar ve gerekli eylemleri gerçekleştirir.

Prosedür

1. **Güvenlik Ayarları** kısmına gidin.
2. Bir Messaging Security Agent seçin.
3. **Ayarları Yapılandır** öğesine tıklayın.

   Yeni bir ekran belirir.
4. **Anti-spam** > **İçerik Taraması** öğesine tıklayın.

Yeni bir ekran belirir.

5. **Gerçek zamanlı Anti-Spam'i Etkinleştir** öğesine tıklayın.

6. Messaging Security Agent'ın spam'i filtrelemekte kullandığı yöntemi ve spam algılama oranını belirlemek için **Hedef** sekmesini seçin:

   a. Spam algılama oranı listesinden **düşük**, **orta** veya **yüksek** şeklindeki algılama düzeyini seçin. Messaging Security Agent bu oranı tüm iletileri filtrelemek için kullanır.

      - **Yüksek**: Bu, spam algılamanın en sert düzeyidir. Messaging Security Agent tüm e-posta iletilerini şüpheli dosya veya metinlere karşı izler ancak daha fazla hatalı pozitif olasılığı vardır. Hatalı pozitifler, geçerli e-posta iletileri oldukları halde Messaging Security Agent tarafından spam olarak filtrelenen e-posta iletileridir.

      - **Orta**: Bu, varsayılan ve tavsiye edilen ayardır. Messaging Security Agent yüksek düzeyde spam algılaması için izleme yapar ve bu düzeyde hatalı pozitiflerin filtrelenmesi olasılığı orta düzeydedir.

      - **Düşük**: Bu, en hafif spam algılama düzeyidir. Messaging Security Agent yalnızca en belirgin ve yaygın spam iletileri filtreler, ancak hatalı pozitifleri filtrelemesi de çok düşük olasılıkla mümkündür. Spam puanına göre filtreleme.

   b. Messaging Security Agent'ın Kimlik Avı Olaylarını filtrelemesi için **Kimlik Avını Algıla** öğesine tıklayın. Ayrıntılar için, bkz. *Kimlik Avı Olayları sayfa 1-27*.

   c. Adresleri Onaylanan Gönderenler ve Engellenen Gönderenler listenize ekleyin. Ayrıntılar için, bkz. *Onaylanan ve Engellenen Gönderenler Listesi sayfa 6-12*.

      - **Onaylanan Gönderenler**: Bu adreslerden veya etki alanı adlarından gelen e-posta iletileri hiçbir zaman engellenmeyecektir. Onaylanacak adresleri veya etki alanlarını girin ve **Ekle**'ye tıklayın. Gerekirse, bir metin dosyasından adreslerin veya etki alanı adlarının listesini içe aktarabilirsiniz. Adresleri veya etki alanı adlarını kaldırmak için, adresi seçin ve **Kaldır**'a tıklayın.

      - **Engellenen Gönderenler**: Bu adreslerden veya etki alanı adlarından gelen e-posta iletileri her zaman engellenecektir. Engellenecek adresleri

veya etki alanlarını girin ve **Ekle**'ye tıklayın. Gerekirse, bir metin dosyasından adreslerin veya etki alanı adlarının listesini içe aktarabilirsiniz. Adresleri veya etki alanı adlarını kaldırmak için, adresi seçin ve **Kaldır**'a tıklayın.

Nota

Microsoft Exchange yöneticisi, Microsoft Exchange sunucusu için ayrı bir Onaylanan ve Engellenen Gönderenler listesi tutar. Bir son kullanıcı, yöneticinin Engellenen Gönderenler listesinde bulunan bir onaylanan gönderen oluştururursa, Messaging Security Agent söz konusu engellenen gönderenden gelen iletileri spam olarak algılar ve bu iletilere yönelik eylem gerçekleştirir.

7. Messaging Security Agent'ın bir spam iletisi veya kimlik avı olayı algıladığında gerçekleştireceği eylemleri ayarlamak için **Eylem** sekmesine tıklayın.

Nota

Eylemler hakkında ayrıntılar için, bkz. *Tarama Hedefleri ve Messaging Security Agent'lar için Eylemler sayfa 7-17*.

Messaging Security Agent, yapılandırmanıza bağlı olarak aşağıdaki eylemlerden birini gerçekleştirir:

- **İletiyi sunucu tarafındaki spam klasöründe karantinaya al**
- **İletiyi kullanıcının spam klasöründe karantinaya al**

Nota

Bu eylemi seçerseniz, Son Kullanıcı Karantinası'nı yapılandırın. Ayrıntılar için, bkz. *Spam Bakımını Yapılandırma sayfa 6-68*.

- **İletinin tamamını sil**
- **Etiketle ve teslim et**

8. **Kaydet** öğesine tıklayın.

Onaylanan ve Engellenen Gönderenler Listesi

Onaylanan Gönderenler listesi, güvenilir e-posta adreslerinin bir listesidir. Messaging Security Agent, **Kimlik Avı olaylarını algıla** etkinleştirilmediği sürece bu adreslerden gelen iletileri spam olarak filtrelemez. **Kimlik Avı olaylarını algıla**'yı etkinleştirdiğinizde ve agent bir e-postada kimlik avı olayı algıladığında, söz konusu e-posta iletisi onaylanan bir gönderen listesine ait olsa bile iletilmez. Engellenen Gönderenler listesi, şüpheli e-posta adreslerinin bir listesidir. Agent, engellenen gönderenlerden gelen e-posta iletilerini her zaman spam olarak kategorilendirir ve uygun eylemi gerçekleştirir.

İki tane Onaylanan Gönderenler listesi vardır: biri Microsoft Exchange Yöneticisi ve biri de son kullanıcılar içindir.

- Microsoft Exchange Yöneticisi'nin Onaylanan Gönderenler ve Engellenen Gönderenler listesi (**Anti-spam** ekranında), Messaging Security Agent'ın Microsoft Exchange sunucusuna bağlı e-posta iletilerini nasıl işleyeceğini kontrol eder.
- Son kullanıcı, yükleme sırasında kendisi için oluşturulan Spam Klasörünü yönetir. Son kullanıcıların listeleri, her bir son kullanıcı için yalnızca sunucu tarafındaki posta kutusu deposuna bağlı iletileri etkiler.

Genel Yönergeler

- Microsoft Exchange sunucusundaki Onaylanan ve Engellenen Gönderenler listeleri, istemcideki Onaylanan ve Engellenen Gönderenler listelerini geçersiz kılar. Örneğin, gönderen adresi “kullanici@ornek.com”, Yöneticinin Engellenen Gönderenler listesindedir, ancak son kullanıcı bu adresi kendine ait Onaylanan Gönderenler listesine eklemiştir. Bu gönderenden gelen iletiler Microsoft Exchange deposuna ulaşır ve Messaging Security Agent bu iletileri spam olarak algılayarak onlara karşı eylemde bulunur. Agent iletiyi kullanıcının spam klasöründe karantinaya al eylemini gerçekleştirirse, iletiyi son kullanıcının Spam klasörüne teslim etmeyi deneyecektir; ancak son kullanıcı söz konusu göndereni onayladığı için ileti bunun yerine son kullanıcının gelen kutusuna yönlendirilecektir.
- Outlook'u kullanırken, listedeki adreslerin miktarı ve boyutuna yönelik bir boyut sınırı vardır. Messaging Security Agent, sistem hatasını önlemek için son kullanıcının kendi onaylanan gönderen listesine ekleyebileceği adreslerin miktarını sınırlar (bu sınır, e-posta adreslerinin uzunluğuna ve sayısına göre hesaplanır).

Joker Eşlemesi

Messaging Security Agent, Onaylanan ve Engellenen Gönderenler listeleri için joker eşlemesini destekler. Joker karakter olarak yıldız işareti (*) kullanır.

Messaging Security Agent, kullanıcı adı bölümünde joker eşlemeyi desteklemez. Ancak "*@trend.com" şeklinde bir kalıp girerseniz, Agent bunu "@trend.com" olarak algılamaya devam eder.

Bir jokeri ancak şu koşullarda kullanabilirsiniz:

- Tek başına bir noktanın yanında ve bir dizenin ilk veya son karakterindeyse
- @ işaretinin solundaysa ve dizenin ilk karakteriyse
- Bir dizenin başlangıcı veya bitişinde eksik olan herhangi bir bölüm joker işaretiyle aynı işlevi görür

TABLO 6-2. Jokerler İçin E-posta Adresi Eşlemeleri

KALIP	EŞLENEN ÖRNEKLER	EŞLENMEYEN ÖRNEKLER
john@example.com	john@example.com	Kalıptan farklı herhangi bir adres
@example.com *@example.com	john@example.com mary@example.com	john@ms1.example.com john@example.com.us mary@example.com.us
example.com	john@example.com john@ms1.example.com mary@ms1.rd.example.com mary@example.com	john@example.com.us mary@myexample.com.us joe@example.comon
*.example.com	john@ms1.example.com mary@ms1.rd.example.com joe@ms1.example.com	john@example.com john@myexample.com.us mary@ms1.example.comon

KALIP	EŞLENEN ÖRNEKLER	EŞLENMEYEN ÖRNEKLER
example.com.*	john@example.com.us john@ms1.example.com.us john@ms1.rd.example.com.us mary@example.com.us	john@example.com mary@ms1.example.com john@myexample.com.us
.example.com.	john@ms1.example.com.us john@ms1.rd.example.com.us mary@ms1.example.com.us	john@example.com john@ms1.example.com john@trend.example.us
..*.example.com *****.example.com	"*.example.com" ile aynı	
example.com example.com example.*.com @*.example.com	Geçersiz kalıplar	

İçerik Filtreleme

İçerik Filtreleme, gelen ve giden e-posta iletilerini kullanıcı tanımlı kuralları temel alarak değerlendirir. Her kural bir anahtar sözcük veya tümcecik listesi içerir. İçerik filtreleme, iletileri anahtar sözcük listesiyle karşılaştırarak iletilerin başlığını ve/veya içeriğini değerlendirir. İçerik filtresi anahtar sözcükle eşleşen bir kelime bulduğunda, istenmeyen içeriğin Microsoft Exchange istemcilerine teslim edilmesini önlemek için eylemde bulunabilir. Messaging Security Agent, istenmeyen içeriğe karşı her eylemde bulunduğunda bildirim gönderebilir.

Nota

İçerik Taraması ile (imza ve tahminlere dayalı istenmeyen e-postadan korunma) İçerik Filtrelemeyi (sınıflandırılmış anahtar kelimelere dayalı e-posta tarama ve engelleme) birbirine karıştırmayın. Bkz. *İçerik Taraması sayfa 6-9*.

İçerik filtresi, Yöneticiye e-posta teslimini ileti metninin kendisini temel alarak değerlendirme ve kontrol etme yöntemleri sunar. Rahatsız edici, saldırgan veya başka bir şekilde itiraz edilebilir ileti içeriğinin varlığını kontrol etmek üzere gelen ve giden iletileri izlemek için kullanılabilir. İçerik filtresi, aynı zamanda ilkelerinizin ulaştığı alanı genişletmenize izin veren eşanlamlı kontrol özelliğini de sunmaktadır. Örneğin, şunları kontrol etmek için kuralları oluşturabilirsiniz:

- Cinsel taciz içeren dil
- Irkçı dil
- Bir e-posta iletisinin gövdesine gömülü spam

Nota

Varsayılan olarak, içerik filtreleme etkinleştirilmemiştir.

İçerik Filtreleme Kurallarını Yönetme

Messaging Security Agent, **İçerik Filtreleme** ekranında tüm içerik filtreleme kuralları görüntülenir. Şuraya giderek bu ekrana erişin:

- Gerçek Zamanlı Tarama için:

  Güvenlik Ayarları > {Messaging Security Agent} > Yapılandır > İçerik Filtreleme

- Manuel Tarama için:

  Taramalar > Manuel > {Expand Messaging Security Agent} > İçerik Filtreleme

- Zamanlanmış Tarama için:

Taramalar > Zamanlanmış > {Expand Messaging Security Agent} > İçerik Filtreleme

Prosedür

1. Aşağıdakiler dahil, kurallar hakkındaki özet bilgileri görüntüleyin:

   - **Kural**: WFBS, içeriği aşağıdaki kategorilere göre filtreleyen varsayılan kurallarla gelir: **Küfür**, **Irksal Ayrımcılık**, **Cinsel Ayrımcılık**, **Aldatmacalar** ve **Posta zincirleri**. Bu kurallar varsayılan olarak devre dışıdır. Gereksinimlerinize göre bu kuralları değiştirebilir veya silebilirsiniz. Bu kuralların hiçbiri gereksinimlerinizi karşılamıyorsa, kendi kurallarınızı ekleyin.
   - **Action**: İstenmeyen bir içerik algıladığında, Messaging Security Agent bu eylemi gerçekleştirir.
   - **Öncelik**: Messaging Security Agent, her filtreyi bu sayfada gösterilen sıraya göre art arda uygular.
   - **Etkin**: Yeşil bir simge etkin bir kuralı belirtirken, kırmızı bir simge devre dışı bırakılmış bir kuralı belirtir.

2. Aşağıdaki görevleri gerçekleştirin:

GÖREV	ADIMLAR
İçerik Filtreleme Etkinleştir/Devre dışı bırak	Ekranın üstünde **Gerçek zamanlı içerik filtrelemeyi etkinleştir** seçin veya temizleyin.
Bir kural ekle	**Ekle** öğesine tıklayın. Eklenecek kuralın türünü seçebileceğiniz yeni bir ekran açılır. Ayrıntılar için, bkz. *İçerik Filtreleme Kurallarının Türleri sayfa 6-19*.

GÖREV	ADIMLAR
Bir kuralı değiştir	a. Kural adına tıklayın. Yeni bir ekran açılır. b. Ekranda kullanılabilir seçenekler kural türüne bağlıdır. Kural türünü belirlemek için, ekranın üstündeki yolları kontrol edin ve ikinci öğeye dikkat edin. Örneğin: İçerik Filtreleme > **Herhangi Bir Koşulu Eşleştir Kuralı** > Kuralı Düzenle Değiştirebileceğiniz kural ayarları hakkında ayrıntılar için, aşağıdaki konulardan herhangi birine bakın: • *Herhangi bir Eşleşme Koşulu için bir İçerik Filtreleme Kuralı Ekleme sayfa 6-23* • *Tüm Eşleşme Koşulları için bir İçerik Filtreleme Kuralı Ekleme sayfa 6-20* **Nota** Bu kural türü Manuel veya Zamanlanmış İçerik Filtreleme Taramaları için kullanılamaz. • *İçerik Filtreleme İzleme Kuralı Ekleme sayfa 6-25* • *İçerik Filtreleme Kurallarına Kural Dışı Durumlar Oluşturma sayfa 6-28*

GÖREV	ADIMLAR
Kuralları yeniden düzenle	Messaging Security Agent içerik filtreleme kurallarını **İçerik Filtreleme** ekranında gösterilen sıraya göre e-posta iletilerine uygular. Kuralların uygulandığı sırayı yapılandırın. Aracı, bir içerik ihlali daha fazla taramayı önleyecek bir eylemi tetikleyinceye kadar tüm e-posta iletilerini her kurala göre filtreler (örneğin silme veya karantinaya alma). İçerik filtrelemeyi en iyi duruma getirmek için bu kuralların sırasını değiştirin. a. Sırasını değiştirmek istediğiniz kurala karşılık gelen onay kutusunu işaretleyin. b. **Yeniden düzenle** öğesine tıklayın. Kural için sıra numarasının etrafında bir kutu görünür. c. **Öncelik** sütun kutusunda, mevcut sıra numarasını silin ve yeni bir numara girin. **Nota** Listedeki kuralların toplam sayısından daha büyük bir sayı girmediğinizden emin olun. Kuralların toplam sayısından büyük bir sayı girdiyseniz, WFBS girdiyi yok sayar ve kuralın sırasını değiştirmez. d. **Yeniden Düzenlemeyi Kaydet** öğesine tıklayın. Kural, girdiğiniz öncelik düzeyine taşınır ve diğer tüm kural sıra numaraları buna göre değişir. Örneğin, kural numarası 5'i seçer ve bunu kural numarası 3 olarak değiştirirseniz, 1 ve 2 numaralı kurallar aynı kalır, 3 numaralı kural ve üzerindeki kurallar bir sayı artar.
Kuralları Etkinleştir/Devre dışı bırak	Etkin sütunu altındaki simgeye tıklayın.

GÖREV	ADIMLAR
Kuralları kaldır	Bir kuralı sildiğinizde, değişimin yansıtılması için Messaging Security Agent diğer kuralların sıralamasını günceller. **Nota** Bir kuralın silinmesi geri döndürülemez, bir kuralı silmek yerine devre dışı bırakmayı düşünün. a. Bir kural seçin. b. **Kaldır** öğesine tıklayın.

3. **Kaydet** öğesine tıklayın.

İçerik Filtreleme Kurallarının Türleri

E-posta iletilerini sizin belirttiğiniz koşullara veya gönderen ya da alıcının e-posta adreslerine göre filtreleyen kurallar oluşturabilirsiniz. Kuralda belirtebileceğiniz koşullar şunları içerir: hangi başlık alanlarının taranacağı, e-posta iletisinin gövdesinde aranıp aranmayacağı ve hangi anahtar sözcüklerin aranacağı.

Şunları gerçekleştirebilen kurallar oluşturabilirsiniz:

- **Tanımlanan herhangi bir koşulla eşleşen iletileri filtrele**: Bu kural türü, bir tarama sırasında herhangi bir iletiden gelen içeriği filtreleyebilir. Ayrıntılar için, bkz. *Herhangi bir Eşleşme Koşulu için bir İçerik Filtreleme Kuralı Ekleme sayfa 6-23*.
- **Tanımlanan tüm koşullarla eşleşen iletileri filtrele**: Bu kural türü, bir tarama sırasında herhangi bir iletiden gelen içeriği filtreleyebilir. Ayrıntılar için, bkz. *Tüm Eşleşme Koşulları için bir İçerik Filtreleme Kuralı Ekleme sayfa 6-20*.

Nota

Bu kural türü Manuel veya Zamanlanmış İçerik Filtreleme Taramaları için kullanılamaz.

- **Belirli e-posta hesaplarının ileti içeriğini izle**: Bu kural türü, belirli e-posta hesaplarının ileti içeriğini izler. İzleme kuralları, yalnızca belirtilen e-posta

hesaplarından gelen içeriği filtrelemeleri dışında genel içerik filtresi kurallarına benzerdir. Ayrıntılar için, bkz. *İçerik Filtreleme İzleme Kuralı Ekleme sayfa 6-25*.

- **Belirli e-posta hesapları için kural dışı durum oluştur**: Bu kural türü, belirli e-posta hesapları için kural dışı bir durum oluşturur. Belirli bir e-posta hesabını muaf tuttuğunuzda, bu hesap içerik kuralı ihlallerine karşı filtrelenmeyecektir. Ayrıntılar için, bkz. *İçerik Filtreleme Kurallarına Kural Dışı Durumlar Oluşturma sayfa 6-28*.

Kuralınızı oluşturduktan sonra, Messaging Security Agent tüm gelen ve giden iletilerinizi kuralınıza göre filtrelemeye başlar. Messaging Security Agent, herhangi bir içerik ihlali gerçekleştiğinde ihlal eden e-posta iletisine karşı eylemde bulunur. Security Server'ın gerçekleştirdiği eylem de kuralınızda ayarladığınız eylemlere bağlıdır.

Tüm Eşleşme Koşulları için bir İçerik Filtreleme Kuralı Ekleme

Bu kural türü Manuel veya Zamanlanmış İçerik Filtreleme Taramaları için kullanılamaz.

Prosedür

1. **Güvenlik Ayarları** kısmına gidin.
2. Bir Messaging Security Agent seçin.
3. **Ayarları Yapılandır** öğesine tıklayın.

   Yeni bir ekran belirir.
4. **İçerik Filtreleme** öğesine tıklayın.

   Yeni bir ekran belirir.
5. **Ekle** öğesine tıklayın.

   Yeni bir ekran belirir.
6. **Tanımlanan tüm koşullarla eşleşen iletiyi filtrele** seçin.
7. **İleri** öğesine tıklayın.
8. Kuralınızın adını **Kural adı** alanına girin.

9. İstenmeyen içerik nedeniyle filtrelemek istediğiniz ileti bölümünü seçin. Messaging Security Agent, e-posta iletilerini şunlara göre filtreleyebilir:

   - Üstbilgi (Kimden, Kime ve Cc)
   - Konu
   - İleti gövdesinin veya ekin boyutu
   - Ek dosya adı

   Nota

   Messaging Security Agent, gerçek zamanlı tarama sırasında yalnızca başlık ve konu içeriği filtrelemesini destekler.

10. **İleri** öğesine tıklayın.

11. Messaging Security Agent'ın istenmeyen içerik algılaması durumunda gerçekleştireceği eylemi seçin. Messaging Security Agent aşağıdaki işlemleri gerçekleştirebilir (Açıklamalar için, bkz. *Tarama Hedefleri ve Messaging Security Agent'lar için Eylemler sayfa 7-17*):

   - Metin/dosya ile değiştir

     Nota

     Kimden, Kime, Cc veya konu alanlarından metin değiştiremezsiniz.

   - İletinin tamamını karantinaya al
   - İleti bölümünü karantinaya al
   - İletinin tamamını sil
   - Arşiv
   - İletinin tamamını geç

12. Messaging Security Agent'ı filtrelenen içeriğe sahip e-posta iletilerinin hedeflenen alıcılarına bildirimde bulunacak şekilde ayarlamak için, **Alıcılara bildir** seçeneğini seçin.

Bildirimleri yalnızca dahili posta alıcılarına göndermek için, **Harici alıcılara bildirme** seçeneğini seçin. **İşlemler** > **Bildirim Ayarları** > **Dahili Posta Tanımı** seçeneklerinden dahili adresleri tanımlayın.

13. Messaging Security Agent'ı filtrelenen içeriğe sahip e-posta iletilerini gönderenlere bildirimde bulunacak şekilde ayarlamak için, **Gönderenlere bildir** öğesini seçin.

    Bildirimleri yalnızca dahili posta gönderenlere iletmek için, **Harici gönderenlere bildirme** öğesini seçin. **İşlemler** > **Bildirim Ayarları** > **Dahili Posta Tanımı** seçeneklerinden dahili adresleri tanımlayın.

14. **Gelişmiş Seçenekler** bölümünde, **Arşiv Ayarı** alt bölümünü genişletmek için artı (+) simgesine tıklayın.

    a. **Karantina dizini** alanında, İçerik Filtreleme'nin karantinaya alınan e-postayı yerleştireceği veya varsayılan değeri kabul edeceği klasör yolunu girin: <Messaging Security Agent Installation folder>\storage\quarantine

    b. **Arşiv dizini** alanında, İçerik Filtreleme'nin arşivlenen e-postayı yerleştireceği veya varsayılan değeri kabul edeceği klasör yolunu girin: <Messaging Security Agent Installation folder>\storage\backup for content filter

15. **Değiştirme Ayarları** alt bölümünü genişletmek için artı (+) simgesine tıklayın.

    a. **Değiştirme dosyası adı** alanında, "Metin/dosya ile değiştir" eylemini kullanan bir kural tetiklendiğinde İçerik Filtreleme'nin e-posta iletisiyle değiştireceği dosyanın adını girin veya varsayılan değeri kabul edin:

    b. **Değiştirme metni** alanına, bir e-posta iletisi, gerçekleştireceği eylem "Metin/dosya ile değiştir" olan bir kuralı tetiklediğinde İçerik Filtreleme'nin kullanacağı değiştirme metninin içeriğini yazın veya yapıştırın ya da varsayılan metni kabul edin:

16. **Son** öğesine tıklayın.

    Sihirbaz kapanır ve İçerik Filtreleme ekranına geri döner.

Herhangi bir Eşleşme Koşulu için bir İçerik Filtreleme Kuralı Ekleme

- Gerçek Zamanlı Tarama için:

  Güvenlik Ayarları > **{Messaging Security Agent}** > **Ayarları Yapılandır** > **İçerik Filtreleme**

- Manuel Tarama için:

  Taramalar > **Manuel** > **{Expand Messaging Security Agent}** > **İçerik Filtreleme**

- Zamanlanmış Tarama için:

  Taramalar > **Zamanlanmış** > **{Expand Messaging Security Agent}** > **İçerik Filtreleme**

Prosedür

1. **Ekle** öğesine tıklayın.

   Yeni bir ekran belirir.

2. **Tanımlanan herhangi bir koşulla eşleşen iletiyi filtrele** seçin.

3. **İleri** öğesine tıklayın.

4. Kuralınızın adını **Kural adı** alanına girin.

5. İstenmeyen içerik nedeniyle filtrelemek istediğiniz ileti bölümünü seçin. Messaging Security Agent, e-posta iletilerini şunlara göre filtreleyebilir:

   - Üstbilgi (Kimden, Kime ve Cc)
   - Konu
   - Gövde
   - Ek

Nota

Messaging Security Agent, gerçek zamanlı tarama sırasında yalnızca başlık ve konu içeriği filtrelemesini destekler.

6. **İleri** öğesine tıklayın.

7. İstenmeyen içerik için filtrelenmesini istediğiniz hedef bölümüne anahtar sözcükler ekleyin. Anahtar sözcüklerle çalışma hakkında ayrıntılar için, bkz. *Anahtar Sözcükler sayfa D-5*.

   a. Gerekli ise, içerik filtrelemeyi büyük/küçük harfe duyarlı veya duyarsız hale getirin.

   b. Yeni anahtar sözcük dosyalarını gerektiği şekilde bir .txt dosyasından içe aktarın.

   c. Eşanlamlılar listesini tanımlayın.

8. **İleri** öğesine tıklayın.

9. Messaging Security Agent'ın istenmeyen içerik algılaması durumunda gerçekleştireceği eylemi seçin. Messaging Security Agent aşağıdaki işlemleri gerçekleştirebilir (Açıklamalar için, bkz. *Tarama Hedefleri ve Messaging Security Agent'lar için Eylemler sayfa 7-17*):

   - Metin/dosya ile değiştir

     Nota

     Kimden, Kime, Cc veya konu alanlarından metin değiştiremezsiniz.

   - İletinin tamamını karantinaya al
   - İleti bölümünü karantinaya al
   - İletinin tamamını sil
   - Arşiv

10. Messaging Security Agent'ı filtrelenen içeriğe sahip e-posta iletilerinin hedeflenen alıcılarına bildirimde bulunacak şekilde ayarlamak için, **Alıcılara bildir** seçeneğini seçin.

Bildirimleri yalnızca dahili posta alıcılarına göndermek için, **Harici alıcılara bildirme** seçeneğini seçin. **İşlemler** > **Bildirim Ayarları** > **Dahili Posta Tanımı** seçeneklerinden dahili adresleri tanımlayın.

11. Messaging Security Agent'ı filtrelenen içeriğe sahip e-posta iletilerini gönderenlere bildirimde bulunacak şekilde ayarlamak için, **Gönderenlere bildir** öğesini seçin.

    Bildirimleri yalnızca dahili posta gönderenlere iletmek için, **Harici gönderenlere bildirme** öğesini seçin. **İşlemler** > **Bildirim Ayarları** > **Dahili Posta Tanımı** seçeneklerinden dahili adresleri tanımlayın.

12. **Gelişmiş Seçenekler** bölümünde, **Arşiv Ayarı** alt bölümünü genişletmek için artı (+) simgesine tıklayın.

    a. **Karantina dizini** alanında, İçerik Filtreleme'nin karantinaya alınan e-postayı yerleştireceği veya varsayılan değeri kabul edeceği klasör yolunu girin: <Messaging Security Agent Installation folder>\storage\quarantine

    b. **Arşiv dizini** alanında, İçerik Filtreleme'nin arşivlenen e-postayı yerleştireceği veya varsayılan değeri kabul edeceği klasör yolunu girin: <Messaging Security Agent Installation folder>\storage\backup for content filter

13. **Değiştirme Ayarları** alt bölümünü genişletmek için artı (+) simgesine tıklayın.

    a. **Değiştirme dosyası adı** alanında, "Metin/dosya ile değiştir" eylemini kullanan bir kural tetiklendiğinde İçerik Filtreleme'nin e-posta iletisiyle değiştireceği dosyanın adını girin veya varsayılan değeri kabul edin:

    b. **Değiştirme metni** alanına, bir e-posta iletisi, gerçekleştireceği eylem "Metin/dosya ile değiştir" olan bir kuralı tetiklediğinde İçerik Filtreleme'nin kullanacağı değiştirme metninin içeriğini yazın veya yapıştırın ya da varsayılan metni kabul edin:

14. **Son** öğesine tıklayın.

    Sihirbaz kapanır ve İçerik Filtreleme ekranına geri döner.

İçerik Filtreleme İzleme Kuralı Ekleme

- Gerçek Zamanlı Tarama için:

Güvenlik Ayarları > {Messaging Security Agent} > Ayarları Yapılandır > İçerik Filtreleme

- Manuel Tarama için:

  Taramalar > Manuel > {Expand Messaging Security Agent} > İçerik Filtreleme

- Zamanlanmış Tarama için:

  Taramalar > Zamanlanmış > {Expand Messaging Security Agent} > İçerik Filtreleme

---

Prosedür

1. **Ekle** öğesine tıklayın.

   Yeni bir ekran belirir.

2. **Belirli e-posta hesaplarının ileti içeriğini izleme** seçin.

3. **İleri** öğesine tıklayın.

4. Kuralınızın adını **Kural adı** alanına girin.

5. İzlenecek eposta hesaplarını ayarlayın.

6. **İleri** öğesine tıklayın.

7. İstenmeyen içerik nedeniyle filtrelemek istediğiniz ileti bölümünü seçin. Messaging Security Agent, e-posta iletilerini şunlara göre filtreleyebilir:

   - Konu
   - Gövde
   - Ek

Nota

Messaging Security Agent, e-posta iletisinin bu bölümlerinin filtrelenmesini yalnızca gerçek zamanlı tarama sırasında destekler. Manuel ve zamanlanmış taramalar sırasında, başlık ve konu içeriğinin filtrelenmesini desteklemez.

---

8. İstenmeyen içerik için filtrelenmesini istediğiniz hedef bölümüne anahtar sözcükler ekleyin. Anahtar sözcüklerle çalışma hakkında ayrıntılar için, bkz. *Anahtar Sözcükler sayfa D-5*.

   a. Gerekli ise, içerik filtrelemeyi büyük/küçük harfe duyarlı veya duyarsız hale getirin.

   b. Yeni anahtar sözcük dosyalarını gerektiği şekilde bir .txt dosyasından içe aktarın.

   c. Eşanlamlılar listesini tanımlayın.

9. **İleri** öğesine tıklayın.

10. Messaging Security Agent'ın istenmeyen içerik algılaması durumunda gerçekleştireceği eylemi seçin. Messaging Security Agent aşağıdaki işlemleri gerçekleştirebilir (Açıklamalar için, bkz. *Tarama Hedefleri ve Messaging Security Agent'lar için Eylemler sayfa 7-17*):

    - Metin/dosya ile değiştir

      Nota

      Kimden, Kime, Cc veya konu alanlarından metin değiştiremezsiniz.

    - İletinin tamamını karantinaya al
    - İleti bölümünü karantinaya al
    - İletinin tamamını sil
    - Arşiv

11. Messaging Security Agent'ı filtrelenen içeriğe sahip e-posta iletilerinin hedeflenen alıcılarına bildirimde bulunacak şekilde ayarlamak için, **Alıcılara bildir** seçeneğini seçin.

    Bildirimleri yalnızca dahili posta alıcılarına göndermek için, **Harici alıcılara bildirme** seçeneğini seçin. **İşlemler** > **Bildirim Ayarları** > **Dahili Posta Tanımı** seçeneklerinden dahili adresleri tanımlayın.

12. Messaging Security Agent'ı filtrelenen içeriğe sahip e-posta iletilerini gönderenlere bildirimde bulunacak şekilde ayarlamak için, **Gönderenlere bildir** öğesini seçin.

Bildirimleri yalnızca dahili posta gönderenlere iletmek için, **Harici gönderenlere bildirme** öğesini seçin. **İşlemler > Bildirim Ayarları > Dahili Posta Tanımı** seçeneklerinden dahili adresleri tanımlayın.

13. **Gelişmiş Seçenekler** bölümünde, **Arşiv Ayarı** alt bölümünü genişletmek için artı (+) simgesine tıklayın.

    a. **Karantina dizini** alanında, İçerik Filtreleme'nin karantinaya alınan e-postayı yerleştireceği veya varsayılan değeri kabul edeceği klasör yolunu girin: <Messaging Security Agent Yükleme klasörü>\storage\quarantine

    b. **Arşiv dizini** alanında, İçerik Filtreleme'nin arşivlenen e-postayı yerleştireceği veya varsayılan değeri kabul edeceği klasör yolunu girin: <Messaging Security Agent Yükleme klasörü>\storage\backup for content filter

14. **Değiştirme Ayarları** alt bölümünü genişletmek için artı (+) simgesine tıklayın.

    a. **Değiştirme dosyası adı** alanında, "Metin/dosya ile değiştir" eylemini kullanan bir kural tetiklendiğinde İçerik Filtreleme'nin e-posta iletisiyle değiştireceği dosyanın adını girin veya varsayılan değeri kabul edin:

    b. **Değiştirme metni** alanına, bir e-posta iletisi, gerçekleştireceği eylem "Metin/dosya ile değiştir" olan bir kuralı tetiklediğinde İçerik Filtreleme'nin kullanacağı değiştirme metninin içeriğini yazın veya yapıştırın ya da varsayılan metni kabul edin:

15. **Son** öğesine tıklayın.

    Sihirbaz kapanır ve İçerik Filtreleme ekranına geri döner.

İçerik Filtreleme Kurallarına Kural Dışı Durumlar Oluşturma

- Gerçek Zamanlı Tarama için:

  Güvenlik Ayarları > {Messaging Security Agent} > Ayarları Yapılandır > İçerik Filtreleme

- Manuel Tarama için:

Taramalar > Manuel > {Expand Messaging Security Agent} > İçerik Filtreleme

- Zamanlanmış Tarama için:

  Taramalar > Zamanlanmış > {Expand Messaging Security Agent} > İçerik Filtreleme

---

Prosedür

1. **Ekle** öğesine tıklayın.

   Yeni bir ekran belirir.

2. **Belirli e-posta hesapları için kural dışı durum oluştur** seçin.

3. **İleri** öğesine tıklayın.

4. Bir kural adı girin.

5. Sağlanan alana içerik filtrelemesinden muaf tutmak istediğiniz e-posta hesaplarını girin ve **Ekle** öğesine tıklayın.

   E-posta hesabı, muaf tutulan e-posta hesapları listenize eklenir. Messaging Security Agent, bu listedeki e-posta hesaplarına bu kuraldan daha düşük önceliğe sahip içerik kurallarını uygulamaz.

6. E-posta hesapları listeniz istediğiniz gibiyse, **Son** öğesine tıklayın.

   Sihirbaz kapanır ve sizi **İçerik Filtreleme** ekranına geri getirir.

Veri Kaybını Önleme

Giden e-posta yoluyla veri kaybına karşı koruma sağlamak için Veri Kaybını Önleme'yi kullanın. Bu özellik, sosyal güvenlik numaraları, telefon numaraları, banka hesap numaraları ve belirlenmiş bir kalıpla eşleşen diğer gizli iş bilgileri gibi verilere koruma sağlayabilir.

Aşağıdaki Microsoft Exchange sürümleri bu sürümde desteklenmektedir:

TABLO 6-3. Desteklenen Microsoft Exchange Sürümleri

DESTEKLENIYOR	DESTEKLENMIYOR
2007 x64	2003 x86/x64
2010 x64	2007 x86
	2010 x86

Ön Çalışma

Olası kayba karşı hassas verileri izlemeden önce, şunları belirleyin:

- Hangi veriler yetkisiz kullanıcılara karşı koruma altına alınmalıdır
- Verilerin bulunduğu konum
- Verilerin nereye ve nasıl aktarıldığı
- Hangi kullanıcıların bu bilgiye erişmek veya bu bilgiyi aktarmak için yetkisi var

Bu önemli denetim tipik olarak, kuruluşunuzdaki hassas bilgilere aşina olan birden çok bölüm ve personelden girdi gerektirir. Aşağıdaki prosedürler, hassas bilgiyi tanımladığınızı ve gizli iş bilgilerinin ele alınması ile ilgili güvenlik ilkelerini kurduğunuzu varsayar.

Veri Kaybını Önleme özelliği üç temel kısımdan oluşur:

- **Kurallar** (aranacak kalıplar)
- **Filtrelemeden dışlanacak** etki alanları
- **Onaylanan Gönderenler** (filtrelemeden dışlanacak e-posta hesapları)

Ayrıntılar için, bkz. *Veri Kaybını Önleme Kurallarını Yönetme sayfa 6-30*.

Veri Kaybını Önleme Kurallarını Yönetme

Messaging Security Agent, tüm Veri Kaybını Önleme kurallarını **Veri Kaybını Önleme** ekranında (**Güvenlik Ayarları** > **{Messaging Security Agent}** > **Ayarları Yapılandır** > **Veri Kaybını Önleme**) gösterir.

Prosedür

1. Aşağıdakiler dahil, kurallar hakkındaki özet bilgileri görüntüleyin:

   - **Rule**: WFBS, varsayılan kurallarla gelir (bkz. *Varsayılan Veri Kaybını Önleme Kuralları sayfa 6-38*). Bu kurallar varsayılan olarak devre dışıdır. Gereksinimlerinize göre bu kuralları değiştirebilir veya silebilirsiniz. Bu kuralların hiçbiri gereksinimlerinizi karşılamıyorsa, kendi kurallarınızı ekleyin.

     İpucu

     Kuralı görüntülemek için farenizin imlecini kural adının üzerine götürün. Kurallı bir ifade kullanan kurallar büyüteç ([A-Z]+) simgesiyle işaretlenir.

   - **Action**: Bir kural tetiklendiğinde, Messaging Security Agent bu eylemi gerçekleştirir.
   - **Priority**: Messaging Security Agent, her kuralı bu sayfada gösterilen sıraya göre art arda uygular.
   - **Enabled**: Yeşil bir simge etkin bir kuralı belirtirken, kırmızı bir simge devre dışı bırakılmış bir kuralı belirtir.

2. Aşağıdaki görevleri gerçekleştirin:

GÖREV	ADIMLAR
Veri Kaybını Önleme'yi Etkinleştir/Devre Dışı Bırak	Ekranın üstünde **Gerçek zamanlı Veri Kaybını Önlemeyi Etkinleştir** seçin veya temizleyin.
Bir kural ekle	**Ekle** öğesine tıklayın. Eklenecek kuralın türünü seçebileceğiniz yeni bir ekran açılır. Ayrıntılar için, bkz. *Veri Kaybını Önleme Kuralları Ekleme sayfa 6-39*.

GÖREV	ADIMLAR
Bir kuralı değiştir	Kural adına tıklayın. Yeni bir ekran açılır. Değiştirebileceğiniz kural ayarları hakkında ayrıntılar için, bkz. *Veri Kaybını Önleme Kuralları Ekleme sayfa 6-39*.

Kuralları içe aktarma ve dışa aktarma	Düz metin dosyasından bir veya daha çok kuralı aşağıda gösterildiği gibi içe (veya dışa) aktarın. İsterseniz, bu dosyayı kullanarak kuralları doğrudan düzenleyebilirsiniz.
	
	`[SMEX_SUB_CFG_CF_RULE43ca5aea-6e75-44c5-94c9-d0b35d2be599]`
	
	`RuleName=Bubbly`
	
	`UserExample=`
	
	`Value=Bubbly`
	
	`[SMEX_SUB_CFG_CF_RULE8b752cf2-aca9-4730-a4dd-8e174f9147b6]`
	
	`RuleName=Master Card No.`
	
	`UserExample=Value=.REG. \b5[1-5]\d{2}\-?\x20?\d{4}\-?\x20?\d{4}\-?\x20?\d{4}\b`

	Kuralları düz metin dosyasına dışa aktarmak için, listeden bir veya daha çok kural seçin ve ardından **Dışa Aktar** öğesini seçin. **İpucu** Yalnızca bir ekranda görünen kuralları seçebilirsiniz. Farklı ekranlarda görüntülenmekte olan kuralları seçmek için, dışa aktarılacak tüm kuralları içerecek kadar satır görüntülemek amacıyla Kural listesi tablosunun üst kısmındaki "Sayfa başına satır" değerini arttırın.

GÖREV	ADIMLAR
	Kuralları içe aktarmak için: a. Yukarıda gösterilen biçimde düz bir metin dosyası oluşturun. Tablonun altından **Daha fazla varsayılan kural indir** öğesine tıklayabilir ve kuralları kaydedebilirsiniz. b. **İçe Aktar** öğesine tıklayın. Yeni bir pencere açılır. c. İçe aktarılacak dosyayı bulmak için **Gözat** öğesine ve ardından **İçe Aktar** öğesine tıklayın. Veri Kaybını Önleme, dosyadaki kuralları içe aktarır ve bunları mevcut kurallar listesinin sonuna ekler. **İpucu** Zaten 10'dan fazla kuralınız varsa, içe aktarılan kurallar ilk sayfada görünmez. Listenin son sayfasını görüntülemek için kurallar listesinin üstündeki veya altındaki sayfa gezinme simgelerini kullanın. Yeni içe aktarılan kurallar burada olmalıdır.

GÖREV	ADIMLAR
Kuralları yeniden düzenle	Messaging Security Agent, Veri Kaybını Önleme kurallarını **Veri Kaybını Önleme** ekranında gösterilen sıraya göre e-posta iletilerine uygular. Kuralların uygulandığı sırayı yapılandırın. Aracı, bir içerik ihlali daha fazla taramayı önleyecek bir eylemi tetikleyinceye kadar tüm e-posta iletilerini her kurala göre filtreler (örneğin silme veya karantinaya alma). Veri Kaybını Önlemeyi en iyi duruma getirmek için bu kuralların sırasını değiştirin. a. Sırasını değiştirmek istediğiniz kurala karşılık gelen onay kutusunu işaretleyin. b. **Yeniden düzenle** öğesine tıklayın. Kural için sıra numarasının etrafında bir kutu görünür. c. **Öncelik** sütun kutusunda, mevcut sıra numarasını silin ve yeni bir numara girin. **Nota** Listedeki kuralların toplam sayısından daha büyük bir sayı girmediğinizden emin olun. Kuralların toplam sayısından büyük bir sayı girdiyseniz, WFBS girdiyi yok sayar ve kuralın sırasını değiştirmez. d. **Yeniden Düzenlemeyi Kaydet** öğesine tıklayın. Kural, girdiğiniz öncelik düzeyine taşınır ve diğer tüm kural sıra numaraları buna göre değişir. Örneğin, kural numarası 5'i seçer ve bunu kural numarası 3 olarak değiştirirseniz, 1 ve 2 numaralı kurallar aynı kalır, 3 numaralı kural ve üzerindeki kurallar bir sayı artar.
Kuralları Etkinleştir/Devre dışı bırak	Etkin sütunu altındaki simgeye tıklayın.

GÖREV	ADIMLAR
Kuralları kaldır	Bir kuralı sildiğinizde, değişimin yansıtılması için Messaging Security Agent diğer kuralların sıralamasını günceller. **Nota** Bir kuralın silinmesi geri döndürülemez, bir kuralı silmek yerine devre dışı bırakmayı düşünün. a. Bir kural seçin. b. **Kaldır** öğesine tıklayın.

GÖREV	ADIMLAR
Belirli etki alanı hesaplarını dışla	Bir şirketin sınırları içerisinde, gizli işletme bilgileri alışverişinin günlük olarak gerçekleşmesi gerekir. Ayrıca, Veri Kaybını Önleme'nin tüm dahili iletileri filtrelemesi gerektiğinde Security Server'lar üzerindeki işlem yükü aşırı olacaktır. Bu nedenlerle, şirket içi e-posta trafiğinizi temsil eden bir veya daha fazla varsayılan etki alanı ayarlamanız gerekir, böylece Veri Kaybını Önleme, şirket etki alanınızın içerisindeki bir e-posta hesabından diğerine gönderilen iletileri filtrelemez. Bu liste, tüm dahili e-posta iletilerinin (şirketinizin etki alanı içinde bulunanlar) Veri Kaybını Önleme kurallarını atlamasına olanak tanır. Bunun gibi en az bir etki alanı gerekir. Birden fazla etki alanı kullanıyorsanız listeye ekleyin. Örneğin: `*@example.com` a. **Veri Kaybını Önleme'den dışlanan Belirli Etki Alanı Hesabı/Hesapları** bölümünü genişletmek için artı (+) simgesine tıklayın. b. İmlecinizi **Ekle** alanına götürün ve şu kalıbı kullanarak etki alanını girin: `*@example.com` c. **Ekle** öğesine tıklayın. Etki alanı, **Ekle** alanının altında gösterilen listede görüntülenir. d. İşlemi tamamlamak için **Kaydet** öğesine tıklayın. **UYARI!** Veri Kaybını Önleme, **Kaydet** öğesine tıklayana kadar etki alanınızı eklemez. **Ekle** öğesine tıklayıp **Kaydet** öğesine tıklamazsanız etki alanınız eklenmeyecektir.

GÖREV	ADIMLAR
E-posta hesaplarını Onaylanan Gönderenler listesine ekle	Onaylanan gönderenlerin postaları, ağınızın dışına Veri Kaybını Önleme tarafından filtrelenmeden çıkar. Veri Kaybını Önleme, onaylanan listesindeki e-posta hesaplarından gönderilen postaların içeriğini yoksayar. a. **Onaylanan Gönderenler** bölümünü genişletmek için artı (+) simgesine tıklayın. b. İmlecinizi **Ekle** alanına götürün ve şu kalıbı kullanarak tam e-posta adresini girin: `example@example.com` c. **Ekle** öğesine tıklayın. Adres, **Ekle** alanının altında gösterilen listede görüntülenir. d. İşlemi tamamlamak için **Kaydet** öğesine tıklayın. **Nota** Veri Kaybını Önleme,**Kaydet** öğesine tıklayana kadar adresi eklemez. **Ekle** öğesine tıklayıp **Kaydet** öğesine tıklamazsanız adres eklenmeyecektir..

GÖREV	ADIMLAR

E-posta hesaplarını Onaylanan Gönderenler listesine aktar	Her satırda bir e-posta hesabı bulunacak şekilde biçimlendirilmiş düz metin dosyasından bir e-posta adresi listesi aktarabilirsiniz, örneğin:
	`admin@ornek.com`
	`ceo@ornek.com`
	`president@ornek.com`
	a. **Onaylanan Gönderenler** bölümünü genişletmek için artı (+) simgesine tıklayın.
	b. **İçe Aktar** öğesine tıklayın.
	Yeni bir pencere açılır.
	c. İçe aktarılacak düz metin dosyasını bulmak için **Gözat** öğesine ve ardından **İçe Aktar** öğesine tıklayın.
	Veri Kaybını Önleme, dosyadaki kuralları içe aktarır ve bunları mevcut listenin sonuna ekler.

3. **Kaydet** öğesine tıklayın.

Varsayılan Veri Kaybını Önleme Kuralları

Aşağıdaki tabloda gösterildiği gibi, Veri Kaybını Önleme varsayılan birkaç kuralla birlikte gelir.

TABLO 6-4. Varsayılan Veri Kaybını Önleme Kuralları

KURAL ADI	ÖRNEK	KURALLI İFADE
Visa Card hesap numarası	4111-1111-1111-1111	.REG. \b4\d{3}\-?\x20?\d{4}\-?\x20?\d{4}\-?\x20?\d{4}\b
MasterCard hesap numarası	5111-1111-1111-1111	.REG. \b5[1-5]\d{2}\-?\x20?\d{4}\-?\x20?\d{4}\-?\x20?\d{4}\b

Kural Adı	Örnek	Kuralli İfade
American Express hesap numarası	3111-111111-11111	.REG. \b3[4,7]\d{2}\-?\x20?\d{6}\-?\x20?\d{5}\b
Diners Club/ Carte Blanche hesap numarası	3111-111111-1111	.REG. [^\d-]((36\d{2}|38\d{2}|30[0-5]\d)-?\d{6}-?\d{4})[^\d-]
IBAN	BE68 5390 0754 7034, FR14 2004 1010 0505 0001 3M02 606, DK50 0040 0440 1162 43	.REG. [^\w](([A-Z]{2}\d{2}[-|\s]?)([A-Za-z0-9]{11,27}|([A-Za-z0-9]{4}[-|\s]){3,6}[A-Za-z0-9]{0,3}|([A-Za-z0-9]{4}[-|\s]){2}[A-Za-z0-9]{3,4}))[^\w]
Swift BIC	BANK US 99	.REG. [^\w-]([A-Z]{6}[A-Z0-9]{2}([A-Z0-9]{3})?)[^\w-]
ISO tarihi	2004/01/23, 04/01/23, 2004-01-23, 04-01-23	.REG. [^\d\/-]([1-2]\d{3}[-\/][0-1]?\d[-\/][0-3]?\d|\d{2}[-\/][0-1]?\d[-\/][0-3]?\d)[^\d\/-]

Nota

Daha fazla DLP kuralı içeren sıkıştırılmış bir dosya web konsolundan indirilebilir. **Güvenlik Ayarları** > **{Messaging Security Agent}** > **Ayarları Yapılandır** > **Veri Kaybını Önleme** kısmına gidin ve **Daha fazla varsayılan kural indir** öğesine tıklayın.

Veri Kaybını Önleme Kuralları Ekleme

Prosedür

1. **Güvenlik Ayarları** kısmına gidin.
2. Bir Messaging Security Agent seçin.
3. **Ayarları Yapılandır** öğesine tıklayın.

   Yeni bir ekran belirir.

4. **Veri Kaybını Önleme** öğesine tıklayın

   Yeni bir ekran belirir.

5. **Ekle** öğesine tıklayın.

   Yeni bir ekran belirir.

6. Değerlendirmek istediğiniz ileti kısmını seçin. Messaging Security Agent, e-posta iletilerini şunlara göre filtreleyebilir:

   - Üstbilgi (Kimden, Kime ve Cc)
   - Konu
   - Gövde
   - Ek

7. Bir kural ekleyin.

   Bir anahtar sözcüğe dayalı bir kural eklemek için:

   a. **Anahtar sözcük** öğesini seçin.

   b. Gösterilen alana anahtar sözcüğü girin. Anahtar sözcük 1 ila 64 alfasayısal karakter uzunluğunda olmalıdır.

   c. **İleri** öğesine tıklayın.

   Otomatik oluşturulmuş ifadelere dayalı bir kural eklemek için:

   a. Kurallı ifadeleri tanımlamak hakkında yönergeler için *Kurallı İfadeler sayfa D-10* kısmına bakın.

   b. **Kurallı ifade (otomatik oluşturulmuş)** seçin.

   c. Sağlanan alana bir **Kural Adı** girin. Bu alan doldurulmalıdır.

   d. **Örnek** alanına, kurallı ifadenin eşleşmesi istenen örnek bir dize türü girin veya yapıştırın (en fazla 40 karakter uzunluğunda). Alfasayısal karakterler, **Örnek** alanının altında sıralı kutuların bulunduğu gölgeli alanda tamamı büyük harfli olarak görünür.

e. İfadede sabitler bulunuyorsa, karakterlerin görüntülendiği kutulara tıklayarak bunları seçin.

Kutulardan her birine tıklattığınızda, kenarları kırmızıya dönerek bunun sabit olduğunu gösterir ve otomatik oluşturma aracı gölgeli alanın altında gösterilen kurallı ifadeyi değiştirir.

Nota

Alfasayısal olmayan karakterler (örneğin boşluklar, noktalı virgüller ve diğer noktalama işaretleri) otomatik olarak sabit gibi algılanır ve değişkenlere dönüştürülemez.

f. Oluşturulan kurallı ifadenin istenen kalıpla eşleştiğini doğrulamak için, **Kuralı doğrulamak için başka bir örnek verin (İsteğe Bağlı)** seçeneğini seçin.

Bu seçeneğin altında bir test alanı görüntülenir.

g. Az önce girdiğiniz kalıba başka bir örnek verin.

Örneğin, bu ifadenin "01-EX?????20??" kalıbının hesap numarası serisiyle eşleşmesi gerekiyorsa, “01-Extreme 2010” gibi eşleşen başka bir örnek girin ve ardından **Test** öğesine tıklayın.

Araç, yeni örneği mevcut kurallı ifadeyle karşılaştırarak doğrular ve yeni örnek eşleşirse alanın yanına yeşil renkli bir onay işareti simgesi yerleştirir. Kurallı ifade yeni örnekle eşleşmezse, alanın yanında kırmızı renkli bir X simgesi görüntülenir.

UYARI!

Bu aracın oluşturduğu kurallı ifadeler küçük/büyük harf duyarlıdır. Bu ifadeler yalnızca örneğinizle aynı sayıda karakter içeren kalıplarla eşleşebilir; bunlar "bir veya daha fazla" belirli karakter kalıbını değerlendiremez.

h. **İleri** öğesine tıklayın.

Kullanıcı tanımlı ifadelere dayalı bir kural eklemek için:

UYARI!

Kurallı ifadeler, güçlü bir dize eşleme aracıdır. Bu ifadeleri kullanmadan önce kurallı ifade sözdiziminin sizin için uygun olduğundan emin olun. Başarıyla yazılmayan kurallı ifadeler, performansı dramatik bir şekilde etkileyebilir. Trend Micro, basit kurallı ifadelerle başlamanızı önerir. Yeni kurallar oluştururken, "arşivleme" eylemini kullanın ve Veri Kaybını Önleme'nin bu kuralı kullanarak iletileri nasıl yönettiğini gözlemleyin. Kuralın beklenmedik herhangi bir sonuca neden olmayacağından emin olduğunuzda, eylemi değiştirebilirsiniz.

a. Kurallı ifadeleri tanımlamak hakkında yönergeler için *Kurallı İfadeler sayfa D-10* kısmına bakın.

b. **Kurallı ifade (kullanıcı tanımlı)** seçin.

   Bir **Kural Adı** ve **Kurallı İfade** alanı görüntülenir.

c. Sağlanan alana bir **Kural Adı** girin. Bu alan doldurulmalıdır.

d. **Kurallı İfade** alanına "`.REG.`" önekiyle başlayıp önek dahil en fazla 255 karakter uzunluğunda olan kurallı bir ifade girin.

   UYARI!

   Bu alana yapıştırırken çok dikkatli olun. Panonuzun içeriğinde İşletim Sistemine özel bir satır veya bir HTML etiketi gibi yabancı karakterler bulunuyorsa, yapıştırılan ifade yanlış olacaktır. Bu nedenle, Trend Micro ifadeyi elle yazmanızı önerir.

e. Kurallı ifadenin istenen kalıpla eşleştiğini doğrulamak için, **Kuralı doğrulamak için başka bir örnek verin (İsteğe Bağlı)** seçeneğini belirleyin.

   Bu seçeneğin altında bir test alanı görüntülenir.

f. Az önce girdiğiniz kalıba başka bir örnek verin (40 karakter veya daha az).

   Örneğin, bu ifadenin "ACC-????? 20??" kalıbının hesap numarası serisiyle eşleşmesi gerekiyorsa, "Acc-65432 2012" gibi eşleşen başka bir örnek girin ve ardından **Test** öğesine tıklayın.

   Araç, yeni örneği mevcut kurallı ifadeyle karşılaştırarak doğrular ve yeni örnek eşleşirse alanın yanına yeşil renkli bir onay işareti simgesi yerleştirir. Kurallı

ifade yeni örnekle eşleşmezse, alanın yanında kırmızı renkli bir X simgesi görüntülenir.

g. **İleri** öğesine tıklayın.

8. Bir kural tetiklendiğinde gerçekleştirilmek üzere Messaging Security Agent için bir eylem seçin (Açıklamalar için, bkz. *Tarama Hedefleri ve Messaging Security Agent'lar için Eylemler sayfa 7-17*):

   - Metin/dosya ile değiştir

   Nota

   Kimden, Kime, Cc veya konu alanlarından metin değiştiremezsiniz.

   - İletinin tamamını karantinaya al
   - İleti bölümünü karantinaya al
   - İletinin tamamını sil
   - Arşiv
   - İletinin tamamını geç

9. Veri Kaybını Önleme, belirli bir e-posta iletisine karşı önlem alırken, Messaging Security Agent'ı hedeflenen alıcılarına bildirimde bulunacak şekilde ayarlamak için, **Alıcılara bildir** seçeneğini seçin.

   Çeşitli nedenlerden ötürü, harici posta alıcılarına hassas bilgiler içeren bir iletinin engellendiğini bildirmek istemeyebilirsiniz. Bildirimleri yalnızca dahili posta alıcılarına göndermek için, **Harici alıcılara bildirme** seçeneğini seçin. **İşlemler** > **Bildirim Ayarları** > **Dahili Posta Tanımı** seçeneklerinden dahili adresleri tanımlayın.

10. Veri Kaybını Önleme belirli bir eposta mesajına karşı işlem yaptığında, Messaging Security Agent'ı amaçlanan gönderenlere bildirim yapmak üzere ayarlamak için **Gönderenlere bildir** seçeneğini seçin.

    Çeşitli nedenlerden ötürü, harici posta göndericilerine hassas bilgiler içeren bir iletinin engellendiğini bildirmek istemeyebilirsiniz. Bildirimleri yalnızca dahili posta gönderenlere iletmek için, **Harici gönderenlere bildirme** öğesini seçin. **İşlemler**

> **Bildirim Ayarları** > **Dahili Posta Tanımı** seçeneklerinden dahili adresleri tanımlayın.

11. **Gelişmiş Seçenekler** bölümünde, **Arşiv Ayarı** alt bölümünü genişletmek için artı (+) simgesine tıklayın.

    a. **Karantina dizini** alanında, Veri Kaybını Önleme'nin karantinaya alınan e-postayı yerleştireceği veya varsayılan değeri kabul edeceği klasör yolunu girin: <Messaging Security Agent Installation folder>\storage\quarantine

    b. **Arşiv dizini** alanında, Veri Kaybını Önleme'nin arşivlenen e-postayı yerleştireceği veya varsayılan değeri kabul edeceği klasör yolunu girin: <Messaging Security Agent Installation folder>\storage\backup for content filter

12. **Değiştirme Ayarları** alt bölümünü genişletmek için artı (+) simgesine tıklayın.

    a. **Değiştirme dosyası adı** alanında, "Metin/dosya ile değiştir" eylemini kullanan bir kural tetiklendiğinde Veri Kaybını Önleme'nin e-posta iletisiyle değiştireceği dosyanın adını girin veya varsayılan değeri kabul edin:

    b. **Değiştirme metni** alanına, bir e-posta iletisi, gerçekleştireceği eylem "Metin/dosya ile değiştir" olan bir kuralı tetiklediğinde Veri Kaybını Önleme'nin kullanacağı değiştirme metninin içeriğini yazın veya yapıştırın ya da varsayılan metni kabul edin:

13. **Son** öğesine tıklayın.

    Sihirbaz kapanır ve Veri Kaybını Önleme ekranına geri döner.

Ek Engelleme

Ek engelleme, e-posta iletilerindeki eklerin Microsoft Exchange Bilgi Deposu'na teslim edilmesini önler. Messaging Security Agent'ı ek türüne veya ek adına göre ekleri engelleyecek şekilde yapılandırarak ölçütlere uyan eklere sahip tüm iletileri değiştirin, karantinaya alın veya silin.

Engelleme Gerçek Zamanlı, Manuel veya Zamanlanmış Tarama sırasında gerçekleşebilir, ancak silme ve karantinaya alma eylemleri Manuel ve Zamanlanmış Taramalar için kullanılabilir değildir.

Bir ekin uzantısı dosyanın türünü tanımlar, örneğin, .txt, .exe veya .dll. Ancak, Messaging Security Agent, gerçek dosya türünü belirlemek için dosya adı yerine dosya başlığını inceler. Çoğu virüs/kötü amaçlı yazılım, çeşitli dosya türleriyle yakından ilişkilidir. Messaging Security Agent'ı dosya türüne göre engelleme yapacak şekilde yapılandırarak, Microsoft Exchange sunucularınıza bu dosya türlerinden gelen güvenlik risklerini azaltabilirsiniz. Benzer şekilde, belirli saldırılar genellikle belirli bir dosya adıyla ilişkilidir.

İpucu

Engellemeyi kullanmak, virüs salgınlarını kontrol etmenin verimli bir yöntemidir. Yüksek riskli dosya türlerinin veya bilinen bir virüs/kötü amaçlı yazılımla ilişkili belirli ada sahip dosya türlerinin tamamını geçici olarak karantinaya alabilirsiniz. Daha sonra, daha çok vaktiniz olduğunda, karantina klasörünü inceleyebilir ve etkilenen dosyalara karşı eylemde bulunabilirsiniz.

Ek Engellemeyi Yapılandırma

Microsoft Exchange sunucuları için ek engelleme seçeneklerini yapılandırma, belirli eklere sahip iletileri engellemeye ilişkin kurallar belirlemeyi içerir.

- Gerçek Zamanlı Tarama için:

  Güvenlik Ayarları > **{Messaging Security Agent}** > **Yapılandırma Ayarları** > **Ek Engelleme**

- Manuel Tarama için:

  Taramalar > **Manuel** > **{Expand Messaging Security Agent}** > **Ek Engelleme**

- Zamanlanmış Tarama için:

  Taramalar > **Zamanlanmış** > **{Expand Messaging Security Agent}** > **Ek Engelleme**

Prosedür

1. **Hedef** sekmesinden, aşağıdakileri gerektiği gibi güncelleyin:

- **Tüm ekler**: Aracı, ek içeren tüm e-posta iletilerini engelleyebilir. Ancak, bu türde tarama pek çok işleme gerektirir. Dışlanacak ek türlerini veya adlarını seçerek bu tür taramayı daraltın.
  - **Dışlanacak ek türleri**
  - **Dışlanacak ek adları**
- **Belirli ekler**: Bu tür taramayı seçtiğinizde, aracı, yalnızca tanımladığınız ekleri içeren e-posta iletileri için tarama yapar. Bu tür tarama çok dışlayıcı olabilir ve tehdit içerdiğinden şüphe duyduğunuz ekleri içeren e-posta iletilerinin algılanması için idealdir. Bu tarama, görece daha düşük miktarda ek adları veya türleri belirttiğinizde çok hızlı çalışır.
  - **Ek türleri**: Aracı, gerçek dosya türünü belirlemek için dosya adı yerine dosya üstbilgisini inceler.
  - **Ek adları**: Varsayılan olarak, aracı gerçek dosya türünü belirlemek için dosya adı yerine dosya başlığını inceler. Ek Engellemeyi belirli adları tarayacak şekilde ayarladığınızda, aracı ek türlerini adlarına göre algılayacaktır.
- **ZIP dosyalarının içindeki ek türlerini veya adlarını engelle**

2. Messaging Security Agent'ın ek algıladığında gerçekleştireceği eylemleri ayarlamak için **Eylem** sekmesine tıklayın. Messaging Security Agent aşağıdaki işlemleri gerçekleştirebilir (Açıklamalar için, bkz. *Tarama Hedefleri ve Messaging Security Agent'lar için Eylemler sayfa 7-17*):
   - Metin/dosya ile değiştir
   - İletinin tamamını karantinaya al
   - İleti bölümünü karantinaya al
   - İletinin tamamını sil
3. Messaging Security Agent'ı eke sahip e-posta iletilerinin hedeflenen alıcılarına bildirimde bulunacak şekilde ayarlamak için, **Alıcılara bildir** seçeneğini seçin.

   Bildirimleri yalnızca dahili posta alıcılarına göndermek için, **Harici alıcılara bildirme** seçeneğini seçin. **İşlemler** > **Bildirim Ayarları** > **Dahili Posta Tanımı** seçeneklerinden dahili adresleri tanımlayın.

4. Messaging Security Agent'ı eke sahip e-posta iletilerinin gönderenlerine bildirimde bulunacak şekilde ayarlamak için, **Gönderenlere bildir** seçeneğini seçin.

   Bildirimleri yalnızca dahili posta gönderenlere iletmek için, **Harici gönderenlere bildirme** öğesini seçin. **İşlemler** > **Bildirim Ayarları** > **Dahili Posta Tanımı** seçeneklerinden dahili adresleri tanımlayın.

5. **Değiştirme Ayarları** alt bölümünü genişletmek için artı (+) simgesine tıklayın.

   a. **Değiştirme dosyası adı** alanında, "Metin/dosya ile değiştir" eylemini kullanan bir kural tetiklendiğinde Ek Engelleme'nin e-posta iletisiyle değiştireceği dosyanın adını girin veya varsayılan değeri kabul edin:

   b. **Değiştirme metni** alanına, bir e-posta iletisi, gerçekleştireceği eylem "Metin/dosya ile değiştir" olan bir kuralı tetiklediğinde Ek Engelleme'nin kullanacağı değiştirme metninin içeriğini yazın veya yapıştırın ya da varsayılan metni kabul edin:

6. **Kaydet** öğesine tıklayın.

Web Reputation

Web Reputation, güvenlik tehditleri oluşturan webdeki veya e-posta mesajlarında gömülü URL'lere erişimi önlemeye yardımcı olur. Web Reputation, Trend Micro web reputation sunucularından URL'nin geçmişini kontrol edecektir ve istemci üzerinde zorlanan belirli web reputation ilkelerine göre geçmişi ilişkilendirecektir. Kullanımda olan ilkeye bağlı olarak:

- Security Agent, web sitesini engelleyecek veya erişime izin verecektir.
- Messaging Security Agent (yalnızca Advanced), zararlı URL'leri içeren e-posta mesajını karantinaya alacak, silecek veya etiketleyecektir ya da URL'ler güvenliyse iletinin gönderilmesine izin verecektir.

Web Reputation, algılamalar hakkında hem yöneticilere e-posta bildirimleri hem de kullanıcıya satır içi bildirimler sağlar.

Security Agent'lar için, istemcinin konumuna bağlı olarak (Ofis İçi/Ofis Dışı) farklı bir güvenlik düzeyi yapılandırır.

Web Reputation sizin güvenli olduğuna inandığınız bir URL'yi engelliyorsa, o URL'yi Onaylanan URL listesine ekleyin.

İpucu

Ağ bant genişliği kazanmak için, Trend Micro şirketin dahili web sitelerini Web reputation onaylı URL listesine eklemeyi önerir.

Geçmiş Puanı

Bir URL'nin "geçmiş puanı" onun bir web tehdidi olup olmadığını belirler. Trend Micro, puanı özel ölçümlerden yararlanarak hesaplar.

Trend Micro, bir URL'yi puanı tanımlanan bir eşik altındaysa bir web tehditi olarak ve puanı eşiğin üzerindeyse güvenli olarak dikkate alacaktır.

Bir Security Agent'ın bir URL'ye erişime izin vereceğini veya engelleyeceğini belirleyen üç güvenlik düzeyi vardır.

- **Yüksek**: Aşağıdaki özelliklere sahip sayfaları engeller:
  - **Tehlikeli**: Dolandırıcılık sayfası veya bilinen tehdit kaynağı olduğu doğrulandı
  - **Çok şüpheli**: Dolandırıcılık sayfası veya olası tehdit kaynağı olduğundan şüpheleniliyor
  - **Şüpheli**: Spam ile ilişkili veya muhtemelen tehlikeli olan sayfalar
  - **Test edilmemiş**: Trend Micro web sayfalarını aktif olarak güvenlik için test ediyor olsa da, kullanıcılar yeni veya az popüler web sitelerini ziyaret ederken test edilmemiş sayfalarla karşılaşabilir. Test edilmemiş sayfalara erişimin engellenmesi güvenliği arttırabilir, ancak aynı zamanda güvenli sayfalara erişimi de önleyebilir.
- **Orta**: Aşağıdaki özelliklere sahip sayfaları engeller:
  - **Tehlikeli**: Dolandırıcılık sayfası veya bilinen tehdit kaynağı olduğu doğrulandı
  - **Çok şüpheli**: Dolandırıcılık sayfası veya olası tehdit kaynağı olduğundan şüpheleniliyor
- **Düşük**: Aşağıdaki özelliklere sahip sayfaları engeller:

- **Tehlikeli**: Dolandırıcılık sayfası veya bilinen tehdit kaynağı olduğu doğrulandı

Messaging Security Agent'lar için Web Reputation Yapılandırma

Prosedür

1. **Güvenlik Ayarları** kısmına gidin.
2. Bir Messaging Security Agent seçin.
3. **Ayarları Yapılandır** öğesine tıklayın.

   Yeni bir ekran belirir.
4. **Web Reputation** öğesine tıklayın.

   Yeni bir ekran belirir.
5. Aşağıdakileri gerektiği gibi güncelleyin:
   - **Web Reputation'ı etkinleştir**
   - Güvenlik Düzeyi: **Yüksek**, **Orta** veya **Düşük**
   - Onaylanan URL/URL'ler
     - **Onaylanacak URL'ler**: Birden fazla URL'yi noktalı virgülle (;) ayırın. **Ekle** öğesine tıklayın.

       Nota

       URL'nin onaylanması, tüm alt etki alanlarının onaylanması anlamına gelir.

       Jokerleri, çok sayıda URL'ye izin verebileceği için dikkatli kullanın.
     - **Onaylanan URL listesi**: Bu listedeki URL'ler engellenmez.
6. **Eylem** sekmesine tıklayın ve bir web reputation ilkesi tetiklendiğinde gerçekleştirilmek üzere Messaging Security Agent için bir eylem seçin (Açıklamalar için, bkz. *Tarama Hedefleri ve Messaging Security Agent'lar için Eylemler sayfa 7-17*):

- Metin/dosya ile değiştir

Nota

Kimden, Kime, Cc veya konu alanlarından metin değiştiremezsiniz.

- İletiyi kullanıcının spam klasöründe karantinaya al
- İletinin tamamını sil
- Etiketle ve teslim et

7. Sınıflandırılmamış URL'leri şüpheli olarak işlemek için **Trend Micro tarafından değerlendirilmemiş URL'ler için önlem al** seçin. Sınıflandırılmamış URL'ler içeren e-posta iletilerinde, önceki adımda belirtilenle aynı işlem gerçekleştirilecektir.

8. Web Reputation, belirli bir e-posta iletisine karşı önlem alırken, Messaging Security Agent'ı hedeflenen alıcılarına bildirimde bulunacak şekilde ayarlamak için, **Alıcılara bildir** seçeneğini seçin.

   Çeşitli nedenlerden ötürü, harici posta alıcılarına zararlı URL'ler içeren bir iletinin engellendiğini bildirmek istemeyebilirsiniz. Bildirimleri yalnızca dahili posta alıcılarına göndermek için, **Harici alıcılara bildirme** seçeneğini seçin. **İşlemler** > **Bildirim Ayarları** > **Dahili Posta Tanımı** seçeneklerinden dahili adresleri tanımlayın.

9. Web Reputation belirli bir eposta mesajına karşı işlem yaptığında, Messaging Security Agent'ı amaçlanan gönderenlere bildirim yapmak üzere ayarlamak için **Gönderenlere bildir** seçeneğini seçin.

   Çeşitli nedenlerden ötürü, harici posta göndericilerine kötü niyetli URL'ler içeren bir iletinin engellendiğini bildirmek istemeyebilirsiniz. Bildirimleri yalnızca dahili posta gönderenlere iletmek için, **Harici gönderenlere bildirme** öğesini seçin. **İşlemler** > **Bildirim Ayarları** > **Dahili Posta Tanımı** seçeneklerinden dahili adresleri tanımlayın.

10. **Kaydet** öğesine tıklayın.

Mobil Güvenlik

Mobil güvenlik ayarları, Microsoft Exchange Server'daki bilgilere erişimin ve karşıdan yüklenmesinin yetkisiz cihazlar tarafından yapılmasına karşı koruma sağlar. Yöneticiler hangi cihazların Microsoft Exchange Server'a erişimine izin verileceğini belirler ve ardından bu cihazların kullanıcılarının eposta, takvim, adres defteri veya görevleri indirip indiremeyeceğini veya güncelleyip güncelleyemeyeceğini tanımlar.

Ayrıca yöneticiler cihazlara güvenlik ilkeleri uygulayabilir. Bu ilkeler parola uzunluğunu ve karmaşıklığını, cihazların belirli bir süre kullanılmaması durumunda kilitlenmesi gerekip gerekmediğini, cihazların şifreleme kullanmasının gerekip gerekmediğini ve başarısız giriş denemeleri sonunda cihaz verisinin silinip silinmemesini kontrol eder.

Mobil Güvenlik Desteği

TABLO 6-5. Mobil Cihaz Desteği

OS	IIS VERSİYONU	CİHAZ VERİSİ KORUMA İLKELERİ		ERİŞİM DENETİMİ		
		EXCHANGE 2007 (VEYA ÜZERİ) 64-BİT	EXCHANGE 2003 32-BİT	EXCHANGE 2010 (VE ÜZERİ) 64-BİT	EXCHANGE 2007 64-BİT	EXCHANGE 2003 32-BİT
• Windows 2008 (64-bit) • SBS 2008 (64-bit)	7 +	Evet	Uyumsuz	Evet	Hayır	Uyumsuz
Windows 2003 (64-bit)	6.0	Evet	Uyumsuz	Hayır	Hayır	Uyumsuz

OS	IIS Versiyonu	Cihaz Verisi Koruma İlkeleri		Erişim Denetimi		
		Exchange 2007 (veya üzeri) 64-bit	Exchange 2003 32-bit	Exchange 2010 (ve üzeri) 64-bit	Exchange 2007 64-bit	Exchange 2003 32-bit
• Windows 2003 (32-bit) • SBS 2003 (32-bit)	6.0	Uyumsuz	Hayır	Uyumsuz	Uyumsuz	Hayır

Tablo 6-6. Mobil Cihaz OS Desteği

Mobil OS	OS Versiyonu
iOS	3.0 - 6.1 (4.3 - 7.0)
Android	2.2 - 4.2
WM/WP (Windows)	7.0 - 8.0
BB (BlackBerry)	7.0 - 10.1

Aygıt Erişim Denetimini Yapılandırma

Prosedür

1. **Güvenlik Ayarları** kısmına gidin.
2. Bir Messaging Security Agent seçin.
3. **Ayarları Yapılandır** öğesine tıklayın.

   Yeni bir ekran belirir.

4. **Mobil Güvenlik** > **Aygıt Erişim Denetimi** öğesine tıklayın.

   Yeni bir ekran belirir.

5. **Aygıt Erişim Denetimini Etkinleştir** öğesini seçin.

6. **Ekle** öğesine tıklayın.

7. Bir ilke adı ve ilke için anlamlı bir açıklama girin.

8. Aygıt sahip(ler)ini tanımlayarak Microsoft Exchange Server'a erişimine izin verilecek/engellenecek aygıtları seçin:

   - **Herkes**
   - **Aygıt sahiplerini belirleyin**

9. **Aygıt sahiplerini belirleyin** seçilirse:

   a. Aygıt sahibinin adını girin ve aygıt sahibini Microsoft Exchange Server'ın Global Adres Listesinde bulmak için **Ara** öğesine tıklayın.

   b. Aygıt sahibini seçin ve **Ekle** öğesine tıklayın.

10. Biliniyorsa, **Tür** açılan listesinden aygıtın işletim sistemini seçin.

11. Biliniyorsa, **Sürüm numara aralığını belirleyin** öğesini seçin ve hangi işletim sistemi sürümlerine izin verildiğini tanımlayın.

12. Messaging Security Agent'in, aygıt sahibinin posta, takvim, kişiler veya görevlerine erişmesine izin vermesi veya engellemesi gerekip gerekmediğini belirtin.

13. **Kaydet** öğesine tıklayın.

Bekleyen Aygıt Silmeyi İptal Etme

Prosedür

1. **Güvenlik Ayarları** kısmına gidin.

2. Bir Messaging Security Agent seçin.

3. **Ayarları Yapılandır** öğesine tıklayın.

   Yeni bir ekran belirir.

4. **Mobil Güvenlik** > **Aygıt Sil** öğesine tıklayın.

   Yeni bir ekran belirir.

5. Aygıt silme tablosundaki aygıtı tanımlayın ve **Silmeyi İptal Et** öğesine tıklayın.

6. **TAMAM** öğesine tıklayın.

Aygıtları Manuel Olarak Silme

Prosedür

1. **Güvenlik Ayarları** kısmına gidin.

2. Bir Messaging Security Agent seçin.

3. **Ayarları Yapılandır** öğesine tıklayın.

   Yeni bir ekran belirir.

4. **Mobil Güvenlik** > **Aygıt Sil** öğesine tıklayın.

   Yeni bir ekran belirir.

5. **Aygıtları Seç** öğesine tıklayın.

   Yeni bir ekran belirir.

6. Aygıt sahibinin adını yazın ve aygıtlarını bulmak için **Ara** öğesine tıklayın.

7. Aygıt silinmeye müsaitse, aygıtı seçin ve **Sil** öğesine tıklayın.

Nota

Arama sonrasında aygıt durumu**Silme başarılı** veya **Silme bekliyor** ise aygıtı seçmek mümkün olmaz.

Güvenlik İlkelerini Yapılandırma

WFBS, varsayılan ilke olarak Windows Exchange varsayılan ilkesini kullanır. Varsayılan ilke, Güvenlik İlkeleri listesinde yer alır.

WFBS, Microsoft Exchange yönetim konsolu veya Exchange Cmdlet ile eklenen varsayılanlar içinde olmayan ilkeleri saklamaz.

Trend Micro, yöneticilerin güvenlik ilkelerini WFBS yönetim konsolu veya Microsoft Exchange üzerinden idare etmesini önermektedir.

Prosedür

1. **Güvenlik Ayarları** kısmına gidin.
2. Bir Messaging Security Agent seçin.
3. **Ayarları Yapılandır** öğesine tıklayın.

   Yeni bir ekran belirir.
4. **Mobile Güvenlik** > **Güvenlik İlkeleri** öğesine tıklayın.

   Yeni bir ekran belirir.
5. **Ekle** öğesine tıklayın.
6. Bir ilke adı ve ilke için anlamlı bir açıklama girin.
7. Cihaz sahibinin adını girin ve cihaz sahibini Microsoft Exchange Server'ın Global Adres Listesinde bulmak için **Ara** öğesine tıklayın.
8. Cihaz sahibini seçin ve **Ekle** öğesine tıklayın.
9. Cihaza uygulanacak güvenlik kriterini seçin:
   - **Minimum şifre uzunluğu**: Mobil aygıt parolaları hakkında yönergeler için *Parola Karmaşıklık Koşulları sayfa 6-56* kısmına bakın.
   - **Gerekli minimum sayıda karakter kümesi**: Mobil aygıt parolaları hakkında yönergeler için *Parola Karmaşıklık Koşulları sayfa 6-56* kısmına bakın.
   - **Aktif olmama sonrası aygıtı kilitle**

- **Cihazda şifreleme gerekliliği**: Mobil aygıt şifrelemeyi desteklemelidir.
- **Başarısız giriş sonrasında cihazı sil**

10. **Kaydet** öğesine tıklayın.

Parola Karmaşıklık Koşulları

Parola karmaşıklık koşulları, aygıt türü ve işletim sistemlerine göre değişiklik gösterir.

Aşağıdaki tablolarda WFBS 9.0 SP1 piyasaya çıktığında test edilen aygıtlar için karmaşıklık "Seçenek"lerinin davranışları listelenmektedir.

Nota

Parola karmaşıklığı fonksiyonu aygıt türü ve işletim sistemi versiyonuna bağlıdır. Belirlenen parola karmaşıklık gereklerine uygun olmazsa birçok aygıt kullanıcılara aygıta özel gereklilikleri belirten bir mesaj verir.

TABLO 6-7. Android Aygıtlar

KARMAŞIKLIK DÜZEYİ	KARMAŞIKLIK KOŞULLARI	
	ANDROİD 4	ANDROİD 2
Seçenek 1	Aşağıdaki karakter çeşitleri kullanılarak oluşturulan kombinasyon: • En az bir büyük harf (A-Z) veya küçük harf (a-z) • En az bir rakam (0-9) veya özel karakter (!@#$ %^&*()_-= +~`[]{}|;:'"?/<>,.)	Alfanümerik

Karmaşıklık Düzeyi	Karmaşıklık Koşulları	
	Android 4	Android 2
Seçenek 2	Aşağıdaki karakter çeşitleri kullanılarak oluşturulan kombinasyon: • En az bir büyük harf (A-Z) veya küçük harf (a-z) • En az iki rakam (0-9) veya özel karakterler (!@#$ %^&*()_-=+~`[]{}|;:'"?/<>,.)	Aşağıdaki karakter çeşitleri kullanılarak oluşturulan kombinasyon: • Alfanümerik • En az iki rakam (0-9) veya özel karakterler (!@#$ %^&*()_-=+~`[]{}|;:'"?/<>,.)
Seçenek 3	Aşağıdaki karakter çeşitleri kullanılarak oluşturulan kombinasyon: • En az bir büyük harf (A-Z) veya küçük harf (a-z) • En az üç rakam (0-9) veya özel karakterler (!@#$ %^&*()_-=+~`[]{}|;:'"?/<>,.)	Aşağıdaki karakter çeşitleri kullanılarak oluşturulan kombinasyon: • Alfanümerik • En az üç rakam (0-9) veya özel karakterler (!@#$ %^&*()_-=+~`[]{}|;:'"?/<>,.)
Seçenek 4	Aşağıdaki karakter çeşitleri kullanılarak oluşturulan kombinasyon: • En az bir büyük harf (A-Z) veya küçük harf (a-z) • En az dört rakam (0-9) veya özel karakterler (!@#$ %^&*()_-=+~`[]{}|;:'"?/<>,.)	Aşağıdaki karakter çeşitleri kullanılarak oluşturulan kombinasyon: • Alfanümerik • En az dört rakam (0-9) veya özel karakterler (!@#$ %^&*()_-=+~`[]{}|;:'"?/<>,.)

Tablo 6-8. iOS Aygıtlar

Karmaşıklık Düzeyi	Karmaşıklık Koşulları
Seçenek 1	Aşağıdaki karakter çeşitleri kullanılarak oluşturulan kombinasyon: • Alfanümerik • En az bir özel karakter (!@#$ %^&*()_-=+~`[]{}|;:'"?/<>,.)

Karmaşıklık Düzeyi	Karmaşıklık Koşulları
Seçenek 2	Aşağıdaki karakter çeşitleri kullanılarak oluşturulan kombinasyon: • Alfanümerik • En az iki özel karakter (!@#$ %^&*()_-=+~`[]{}|;:'"?/<>,.)
Seçenek 3	Aşağıdaki karakter çeşitleri kullanılarak oluşturulan kombinasyon: • Alfanümerik • En az üç özel karakter (!@#$ %^&*()_-=+~`[]{}|;:'"?/<>,.)
Seçenek 4	Aşağıdaki karakter çeşitleri kullanılarak oluşturulan kombinasyon: • Alfanümerik • En az dört özel karakter (!@#$ %^&*()_-=+~`[]{}|;:'"?/<>,.)

Tablo 6-9. Windows Telefonlar

Karmaşıklık Düzeyi	Karmaşıklık Koşulları	
	Windows Phone 8	Windows Phone 7
Seçenek 1	Aşağıdaki karakter çeşitlerinden en az biri: • Büyük harfler (A-Z) • Küçük harfler (a-z) • Rakamlar (0-9) • Özel karakterler (!@#$ %^&*()_-=+~`[]{}|;:'"?/<>,.)	Aşağıdaki karakter çeşitlerinden en az ikisinden oluşturulan kombinasyon: • Büyük harfler (A-Z) • Küçük harfler (a-z) • Rakamlar (0-9) • Özel karakterler (!@#$ %^&*()_-=+~`[]{}|;:'"?/<>,.)

Karmaşıklık Düzeyi	Karmaşıklık Koşulları	
	Windows Phone 8	Windows Phone 7
Seçenek 2	Aşağıdaki karakter çeşitlerinden en az ikisinden oluşturulan kombinasyon: • Büyük harfler (A-Z) • Küçük harfler (a-z) • Rakamlar (0-9) • Özel karakterler (!@#$ %^&*()_-=+~`[]{}|;:'"?/<>,.)	Aşağıdaki karakter çeşitlerinden en az ikisinden oluşturulan kombinasyon: • Büyük harfler (A-Z) • Küçük harfler (a-z) • Rakamlar (0-9) • Özel karakterler (!@#$ %^&*()_-=+~`[]{}|;:'"?/<>,.)
Seçenek 3	Aşağıdaki karakter çeşitlerinden en az üçünden oluşturulan kombinasyon: • Büyük harfler (A-Z) • Küçük harfler (a-z) • Rakamlar (0-9) • Özel karakterler (!@#$ %^&*()_-=+~`[]{}|;:'"?/<>,.)	Aşağıdaki karakter çeşitlerinden en az üçünden oluşturulan kombinasyon: • Büyük harfler (A-Z) • Küçük harfler (a-z) • Rakamlar (0-9) • Özel karakterler (!@#$ %^&*()_-=+~`[]{}|;:'"?/<>,.)
Seçenek 4	Aşağıdaki karakter çeşitlerinin hepsi kullanılarak oluşturulan kombinasyon: • Büyük harfler (A-Z) • Küçük harfler (a-z) • Rakamlar (0-9) • Özel karakterler (!@#$ %^&*()_-=+~`[]{}|;:'"?/<>,.)	Aşağıdaki karakter çeşitlerinin hepsi kullanılarak oluşturulan kombinasyon: • Büyük harfler (A-Z) • Küçük harfler (a-z) • Rakamlar (0-9) • Özel karakterler (!@#$ %^&*()_-=+~`[]{}|;:'"?/<>,.)

TABLO 6-10. BlackBerry Aygıtları

KARMAŞIKLIK DÜZEYİ	KARMAŞIKLIK KOŞULLARI
Seçenek 1	En az bir büyük harf (A-Z) veya küçük harf (a-z)
Seçenek 2	Aşağıdaki karakter çeşitlerinden en az ikisinden oluşturulan kombinasyon: • Büyük harfler (A-Z) • Küçük harfler (a-z) • Rakamlar (0-9) • Özel karakterler (!@#$%^&*()_-=+~`[]{}|;:'"?/<>,.)
Seçenek 3	Aşağıdaki karakter çeşitlerinden en az üçünden oluşturulan kombinasyon: • Büyük harfler (A-Z) • Küçük harfler (a-z) • Rakamlar (0-9) • Özel karakterler (!@#$%^&*()_-=+~`[]{}|;:'"?/<>,.)
Seçenek 4	Aşağıdaki karakter çeşitlerinin hepsi kullanılarak oluşturulan kombinasyon: • Büyük harfler (A-Z) • Küçük harfler (a-z) • Rakamlar (0-9) • Özel karakterler (!@#$%^&*()_-=+~`[]{}|;:'"?/<>,.)

Messaging Security Agent'lar için Karantina

Messaging Security Agent, e-posta iletileri içinde bir tehdit, spam, sınırlandırılmış ek ve/veya sınırlandırılmış içerik algıladığında, aracı iletiyi bir karantina klasörüne taşıyabilir. Bu işlem, ileti/ek silmeye alternatif görevini üstlenir ve kullanıcıların etkilenen iletiyi açmalarını ve tehdidi yaymalarını önler.

Message Security Agent'taki varsayılan karantina klasörü:

<Messaging Security Agent yükleme klasörü>\storage\quarantine

Karantinaya alınan dosyalar, ek güvenlik için şifrelenir. Şifreli dosyayı açmak için, Restore Encrypted Virus ve Spyware (VSEncode.exe) aracını kullanın. Bkz. *Şifrelenmiş Dosyaları Geri Yükleme sayfa 14-9*.

Yöneticiler, karantinaya alınan iletiler hakkında bilgi toplamak için karantina veritabanını sorgulayabilir.

Karantinayı şu amaçlarla kullanın:

- Güçlü filtreler tarafından hatalı bir şekilde algılanmaları durumunda, önemli iletilerin kalıcı olarak silinme ihtimalini yok etme
- İlke ihlalinin önem düzeyini belirlemek için içerik filtrelerini tetikleyen iletileri inceleme
- Bir çalışanın şirketin mesajlaşma sistemini amaç dışı kullanma olasılığının kanıtlarını koruma

Nota

Karantina klasörünü son kullanıcının spam klasörü ile karıştırmayın. Karantina klasörü, dosya tabanlı bir klasördür. Messaging Security Agent bir e-posta iletisini her karantinaya aldığında, iletiyi karantina klasörüne gönderir. Son kullanıcının spam klasörü, her kullanıcının posta kutusu için Bilgi Deposu'ndadır. Son kullanıcının spam klasörü; içerik filtreleme, antivirus/casus yazılımdan koruma veya ek engelleme ilkelerinin sonucu olarak karantina eylemlerini değil, yalnızca istenmeyen e-postadan koruma karantinasından kaynaklanan e-posta iletilerini kullanıcının spam klasörüne alır.

Karantina Dizinlerini Sorgulama

Prosedür

1. **Güvenlik Ayarları** kısmına gidin.
2. Bir Messaging Security Agent seçin.

3. **Ayarları Yapılandır** öğesine tıklayın.

   Yeni bir ekran belirir.

4. **Karantina** > **Sorgu** öğesine tıklayın.

   Yeni bir ekran belirir.

5. Aşağıdakileri gerektiği gibi güncelleyin:

   - Tarih/Saat Aralığı
   - Karantinaya Alınma Nedenleri
     - **Tüm Nedenler**
     - **Belirtilen Türler**: Virüs taraması, Anti-Spam, İçerik filtreleme, Ek engelleme ve/veya Taranamayan ileti bölümlerinden seçim yapın.
   - Yeniden Gönderme Durumu
     - **Hiç yeniden gönderilmedi**
     - **En az bir kez yeniden gönderildi**
     - **Yukarıdakilerin her ikisi**
   - Gelişmiş Ölçütler
     - **Gönderen**: Belirli gönderenlerden gelen iletiler. Gerekirse jokerler kullanın.
     - **Alıcı**: Belirli alıcılardan gelen iletiler. Gerekirse jokerler kullanın.
     - **Konu**: Belirli konulara sahip iletiler. Gerekirse jokerler kullanın.
     - **Sıralama ölçütü**: Sonuç sayfası için sıralama koşulunu yapılandırın.
     - **Görüntüle**: Sayfa başına sonuç sayısı.

6. **Ara** öğesine tıklayın. Bkz. *Sorgu Sonuçlarını Alma ve Eyleme Geçme sayfa 6-63*.

Sorgu Sonuçlarını Alma ve Eyleme Geçme

Karantina Sorgu Sonuçları ekranında, iletiler hakkında aşağıdaki bilgiler görüntülenir:

- **Tarama zamanı**
- **Gönderen**
- **Alıcı**
- **Konu**
- **Nedeni**: E-posta iletisinin karantinaya alınma sebebi.
- **Dosya adı**: Engellenen dosyanın e-posta iletisindeki adı.
- **Karantina yolu**: E-posta iletisinin karantinaya alındığı konum. Yöneticiler, VSEncoder.exe (bkz. *Şifrelenmiş Dosyaları Geri Yükleme sayfa 14-9*) kullanarak dosyanın şifresini çözebilir ve ardından dosyayı görüntülemek için .eml olarak yeniden adlandırabilir.

  UYARI!

  Etkilenen dosyaların görüntülenmesi etkilenmeyi yayabilir.

- **Yeniden gönderme durumu**

Prosedür

1. İletinin güvensiz olduğunu düşünüyorsanız, iletiyi silin.

   UYARI!

   Karantina klasörü, yüksek düzeyde etkilenme riskine sahip e-posta iletilerini içerir. İstemciyi yanlışlıkla etkilememek için, karantina klasöründen gelen e-posta iletileriyle ilgilenirken dikkatli olun.

2. İletinin güvenli olduğunu düşünüyorsanız, iletiyi seçin ve yeniden gönder simgesine ( ) tıklayın.

Nota

Orijinalinde Microsoft Outlook kullanılarak gönderilen, karantinaya alınmış bir iletiyi yeniden gönderirseniz, alıcı aynı iletinin birden fazla kopyasını alabilir. Bu, Virüs Tarama motoru taradığı her iletiyi çeşitli bölümlere ayırdığı için gerçekleşebilir.

3. İletiyi yeniden gönderemiyorsanız, Microsoft Exchange sunucusu üzerinde sistem yöneticisi hesabının mevcut bulunmuyor olması mümkündür.

   a. Windows Kayıt Defteri Editörü'nü kullanarak, sunucuda aşağıdaki kayıt defteri girişini açın:

      HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\ScanMail for Exchange \CurrentVersion

   b. Girişi şu şekilde düzenleyin:

      UYARI!

      Kayıt defterinin yanlış düzenlenmesi sisteminizde ciddi hasara neden olabilir. Kayıt defterinde değişiklik yapmadan önce, bilgisayarınızdaki tüm önemli verileri yedeklemeniz gerekir.

      - `ResendMailbox {Yönetici Posta Kutusu}`

        Örnek: `admin@ornek.com`

      - `ResendMailboxDomain {Yönetici Etki Alanı}`

        Örnek: `example.com`

      - `ResendMailSender {Yönetici E-posta Hesabı}`

        Örnek: `yönetici`

   c. Kayıt Defteri Editörü'nü kapatın.

Karantina Dizinlerinin Bakımı

Karantinaya alınan iletileri manuel veya otomatik olarak silmek için bu özelliği kullanın. Bu özellik; tüm iletileri, yeniden gönderilen ve yeniden gönderilmeyen iletileri silebilir.

Prosedür

1. **Güvenlik Ayarları** kısmına gidin.
2. Bir Messaging Security Agent seçin.
3. **Ayarları Yapılandır** öğesine tıklayın.

   Yeni bir ekran belirir.
4. **Karantina** > **Bakım** öğesine tıklayın.

   Yeni bir ekran belirir.
5. Aşağıdakileri gerektiği gibi güncelleyin:
   - **Otomatik bakımı etkinleştir**: Yalnızca otomatik bakım için kullanılabilir.
   - Silinecek dosyalar
     - **Karantinaya alınan tüm dosyalar**
     - **Karantinaya alınan, yeniden gönderilmemiş dosyalar**
     - **Karantinaya alınan, en az bir kez yeniden gönderilmiş dosyalar**
   - **Eylem**: İletilerin saklanması gereken gün sayısı. Örneğini tarih 21 Kasım ise ve **Şu tarihten eski seçili dosyaları sil** alanına `10` yazdıysanız, Messaging Security Agent otomatik silme işlemi gerçekleştirdiğinde 11 Kasım'dan önceki tüm dosyaları siler.
6. **Kaydet** öğesine tıklayın.

Karantina Dizinlerini Yapılandırma

Microsoft Exchange Server'daki karantina dizinlerini yapılandırın. Karantina dizini taramadan dışlanacaktır.

Nota

Karantina dizinleri dosya tabanlıdır ve Bilgi Deposu'na yerleşmez.

Messaging Security Agent, e-posta iletilerini yapılandırılmış eylemlere göre karantinaya alır. Aşağıdakiler karantina dizinleridir:

- **Antivirüs**: Virüs/kötü amaçlı yazılım, casus yazılım/grayware, solucanlar, Truva Atları ve diğer zararlı tehditleri içeren e-posta iletilerini karantinaya alır.
- **İstenmeyen E-postadan Koruma**: Spam ve kimlik avı e-postasını karantinaya alır.
- **Ek engelleme**: Sınırlanmış ekler içeren e-posta iletilerini karantinaya alır.
- **İçerik filtreleme**: Sınırlanmış içeriğe sahip e-posta iletilerini karantinaya alır.

Varsayılan olarak, tüm dizinler aynı yollara sahiptir (<Messaging Security Agent yükleme klasörü>\storage\quarantine). Dizinler için ayrı olarak veya tamamının yollarını değiştirebilirsiniz.

Prosedür

1. **Güvenlik Ayarları** kısmına gidin.
2. Bir Messaging Security Agent seçin.
3. **Ayarları Yapılandır** öğesine tıklayın.

   Yeni bir ekran belirir.
4. **Karantina** > **Dizin** öğesine tıklayın.

   Yeni bir ekran belirir.
5. Aşağıdaki karantina dizinleri için yolu ayarlayın:
   - **Antivirüs**
   - **İstenmeyen e-postadan koruma**
   - **İçerik Filtreleme**
   - **Ek Engelleme**
6. **Kaydet** öğesine tıklayın.

Messaging Security Agent'lar için Bildirim Ayarları

WFBS çeşitli uyarılara ilişkin e-posta iletileri şeklinde bildirimler gönderebilir.

Özel Dahili E-posta Tanımları kullanarak sadece dahili e-posta mesajlarını uygulamak için bildirimleri yapılandırın. Şirketiniz iki veya daha fazla etki alanına sahipse ve her iki etki alanından gelen iletilerin de dahili e-posta iletileri olarak algılanmasını isterseniz kullanışlı olacaktır. Örneğin, example.com ve example.net.

Dahili E-posta Tanımları listenizdeki alıcılar; **Antivirüs**, **İçerik Filtreleme** ve **Ek Engelleme** altındaki Bildirim ayarlarında **Harici alıcılara bildirme** onay kutusunu işaretlediğinizde bildirim iletileri alacaktır. Dahili E-Posta Tanımları listesini Onaylanan Gönderenler listesi ile karıştırmayın.

Harici etki alanlarını içeren adreslerden gelen e-postaların spam olarak etiketlenmesini önlemek için, harici e-posta adresini Anti-Spam için **Onaylanan Gönderenler** listesine ekleyin.

Özel Dahili E-posta Tanımları Hakkında

Messaging Security Agent e-posta trafiğini iki ağ kategorisine ayırır: dahili ve harici. Aracı, dahili ve harici adreslerin nasıl tanımlandığını öğrenmek için Microsoft Exchange sunucusuna sorgu gönderir. Tüm dahili adresler ortak bir etki alanını paylaşır ve harici adreslerin hiçbiri bu etki alanına ait değildir.

Örneğin eğer dahili etki alanı adresi “@trend_1.com”, ise, Messaging Security Agent “abc@trend_1.com” ve “xyz@trend_1.com” gibi adresleri dahili adresler olarak sınıflandırır. Aracı, “abc@trend_2.com” ve “jondoe@123.com” gibi tüm diğer adresleri harici olarak sınıflandırır.

Messaging Security Agent için dahili adres olarak yalnızca bir etki alanı tanımlayabilirsiniz. Bir sunucuda birincil adresinizi değiştirmek için Microsoft Exchange Sistem Yöneticisi kullanıyorsanız, Messaging Security Agent alıcı ilkesinin değiştiğini algılayamadığı için yeni adresi dahili adres olarak tanımaz.

Örneğin, şirketiniz için iki tane etki alanı adresiniz var: @example_1.com ve @example2.com. Birincil adres olarak @example_1.com'u ayarladınız. Messaging Security Agent, birincil adresli e-posta iletilerini dahili olarak algılar (yani, abc@example_1.com veya xyz@example_1.com dahilidir). Daha sonra, birincil adresi

@example_2.com olarak değiştirmek için Microsoft Exchange Sistem Yöneticisi'ni kullanıyorsunuz. Bu, Microsoft Exchange'in artık abc@example_2.com ve xyz@example_2.com gibi adresleri dahili adresler olarak algılaması anlamına geliyor.

Messaging Security Agent'lar için Bildirim Ayarlarını Yapılandırma

Prosedür

1. **Güvenlik Ayarları** kısmına gidin.
2. Bir Messaging Security Agent seçin.
3. **Ayarları Yapılandır** öğesine tıklayın.

   Yeni bir ekran belirir.
4. **İşlemler** > **Bildirim Ayarları** kısmına gidin.

   Yeni bir ekran belirir.
5. Aşağıdakileri gerektiği gibi güncelleyin:
   - **E-posta adresi**: WFBS'nin adına bildirim iletileri göndereceği adres.
   - **İç E-posta Tanımı**
     - **Varsayılan**: WFBS aynı etki alanından gelen e-posta iletilerini Dahili E-postalar olarak algılayacaktır.
     - **Özel**: Dahili e-posta iletileri olarak algılanmak üzere ayrı e-posta adresleri veya etki alanları belirtin.
6. **Kaydet** öğesine tıklayın.

Spam Bakımını Yapılandırma

Spam Bakımı ekranı, Son Kullanıcı Karantinası (EUQ) veya Sunucu tarafı karantinası ayarlarını yapılandırmanıza olanak sağlar.

Prosedür

1. **Güvenlik Ayarları** kısmına gidin.
2. Bir Messaging Security Agent seçin.
3. **Ayarları Yapılandır** öğesine tıklayın.

   Yeni bir ekran belirir.
4. **İşlemler** > **Spam Bakımı** öğesine tıklayın.

   Yeni bir ekran belirir.
5. **Son Kullanıcı Karantina aracını etkinleştir** öğesine tıklayın.

   Aracı etkinleştirdiğinizde, her bir İstemci'nin posta kutusunun sunucu tarafında bir karantina klasörü oluşturulur ve son kullanıcının Outlook klasör ağacında bir Spam Posta klasörü görünür. EUQ etkinleştirildikten ve Spam Posta klasörleri oluşturulduktan sonra EUQ, spam iletilerini kullanıcının Spam posta klasörüne filtreler. Ayrıntılar için, bkz. *Son Kullanıcı Karantinasını Yönetme sayfa 6-70*.

   İpucu

   Bu seçeneği belirlerseniz, Trend Micro, istemcilerdeki performansı arttırmak amacıyla aracılarda Trend Micro Anti-Spam toolbar seçeneğini devre dışı bırakmanızı önerir.

   Microsoft Exchange sunucunuzdaki tüm posta kutularının son kullanıcı karantina aracını devre dışı bırakmak için **Son Kullanıcı Karantinası aracını etkinleştir**'i temizleyin. EUQ aracını devre dışı bıraktığınızda, kullanıcıların Spam Posta klasörleri kalır ancak spam olarak algılanan iletiler Spam Posta klasörlerine taşınmaz.
6. Yeni oluşturulan posta istemcileri ve Spam Posta klasörünü silmiş mevcut posta istemcileri için (derhal) Spam Posta klasörleri oluşturmak için **Spam klasörü oluştur ve spam iletileri sil** öğesine tıklayın. Diğer mevcut posta istemcileri için, İstemci Spam Klasörü Ayarları alanında belirtilen günden daha eski olan spam iletileri silinir.
7. **{sayı} günden daha eski spam iletilerini sil** içerisinde, spam iletilerinin Messaging Security Agent tarafından saklanacağı süreyi değiştirin. Varsayılan değer 14 gün ve en uzun süre sınırı 30 gündür.

8. Son Kullanıcı Karantina aracını seçilen kullanıcılar için devre dışı bırakmak için:

   a. **Son Kullanıcı Karantina aracı kural dışı durum listesi** altında, EUQ seçeneğini devre dışı bırakmak istediğiniz son kullanıcının e-posta adresini girin.

   b. **Ekle** öğesine tıklayın.

      Son kullanıcının e-posta adresi, EUQ seçeneği devre dışı bırakılmış adresler listesine eklenir.

      Bir son kullanıcıyı listeden kaldırıp EUQ hizmetini geri yüklemek için, listeden son kullanıcının e-posta adresini seçip **Sil** öğesine tıklayın.

9. **Kaydet** öğesine tıklayın.

Son Kullanıcı Karantinasını Yönetme

Yükleme sırasında, Messaging Security Agent her son kullanıcının sunucu tarafındaki posta kutusuna Spam Posta adlı bir klasör ekler. Spam iletiler ulaştığında, sistem bunları Messaging Security Agent tarafından önceden tanımlanan spam filtresi kurallarına göre bu klasörde karantinaya alır. Son kullanıcılar, şüpheli e-posta iletilerini açmak, okumak veya silmek için bu spam klasörünü görüntüleyebilir. Bkz. *Spam Bakımını Yapılandırma sayfa 6-68*.

Alternatif olarak, Yöneticiler Microsoft Exchange'de Spam Posta klasörü oluşturabilir. Bir Yönetici, posta kutusu hesabı oluşturduğunda posta kutusu varlığı Microsoft Exchange sunucusunda hemen oluşturulmaz, ancak şu koşullar altında oluşturulur:

- Bir son kullanıcı posta kutusunda ilk defa oturum açarsa
- İlk e-posta, posta kutusuna ulaşırsa

EUQ'nin Spam Klasörü oluşturabilmesi için, öncelikle Yöneticinin posta kutusu varlığını oluşturması gerekir.

İstemci Taraflı Spam Posta Klasörü

Son kullanıcılar, spam klasöründe karantinaya alınan e-posta iletilerini açabilir. Bu iletilerden herhangi birini açtıklarında, gerçek e-posta iletisinin üzerinde iki düğme görünür: **Onaylanan Gönderen** ve **Onaylanan Gönderen Listesini Görüntüle**.

- Bir son kullanıcı, Spam Posta klasöründeki bir e-posta iletisini açıp **Onaylanan Gönderen** öğesine tıkladığında söz konusu e-posta için gönderenin adresi son kullanıcının **Onaylanan Gönderenler** listesine eklenir.
- **Onaylanan Gönderen Listesini Görüntüle** öğesine tıklandığında, son kullanıcının onaylanan gönderenler listesini e-posta adresine veya etki alanına göre görüntüleyebileceği ve değiştirebileceği başka bir ekran açılır.

Onaylanan Gönderenler

Son kullanıcı Spam Posta klasörüne bir e-posta alıp **Göndereni Onayla** öğesine tıkladığında, Messaging Security Agent iletiyi son kullanıcıların yerel gelen kutusu içine taşır ve gönderenin adresini son kullanıcının kişisel Onaylanan Gönderen Listesi'ne ekler. Messaging Security Agent olayı günlüğe alır.

Microsoft Exchange server, son kullanıcının Onaylanan Gönderen listesindeki adreslerden gelen iletileri aldığında, iletinin başlığına veya içeriğine bakmaksızın son kullanıcının gelen kutusuna teslim eder.

Nota

Messaging Security Agent ayrıca, yöneticiler için Onaylanan Gönderenler ve Engellenen Gönderenler listesi sağlar. Messaging Security Agent, son kullanıcı listesini göz önünde bulundurmadan önce yöneticinin onaylanan gönderenler ve engellenen gönderenler listesini uygular.

Son Kullanıcı Karantina Hazırlığı Özelliği

Messaging Security Agent hazırlık özelliği, her 24 saatte bir varsayılan olarak 2:30 AM'de aşağıdaki görevleri gerçekleştirir:

- Süresi dolan spam iletileri otomatik olarak siler
- Silinmişse spam klasörünü yeniden oluşturur
- Yeni oluşturulan posta hesapları için spam klasörleri oluşturur
- E-posta iletisi kurallarını korur

Hazırlık özelliği, Messaging Security Agent'ın entegre bir parçasıdır ve yapılandırma gerektirmez.

Trend Micro Destek/Hata Ayıklayıcı

Destek/Hata Ayıklayıcı, hata ayıklamada ya da yalnızca Messaging Security Agent işlemlerinin durumunu raporlamada size yardımcı olabilir. Beklenmedik zorluklarla karşılaştığınızda, hata ayıklayıcı raporları oluşturmak için hata ayıklayıcıyı kullanabilir ve bu raporları incelenmeleri için Trend Micro teknik desteğine gönderebilirsiniz.

Her Messaging Security Agent, programa iletiler ekler ve ardından yürütme sonrasında eylemi günlük dosyalarına kaydeder. Günlükleri, ortamınızdaki gerçek program akışının hatalarını ayıklamalarına yardımcı olmak için Trend Micro Teknik Destek çalışanlarına iletebilirsiniz.

Şu modüllerde günlük oluşturmak için hata ayıklayıcıyı kullanın:

- Messaging Security Agent Ana Hizmeti
- Messaging Security Agent Remote Configuration Server
- Messaging Security Agent System Watcher
- Virus Scan API (VSAPI)
- Basit Posta Aktarım Protokolü (SMTP)
- Ortak Ağ Geçidi Arayüzü (CGI)

Varsayılan olarak, MSA günlükleri aşağıdaki dizinde tutar:

<Messaging Security Agent yükleme klasörü>\Debug

Çıktıyı herhangi bir metin düzenleyiciyle görüntüleyin.

Sistem Hata Ayıklayıcı Raporları Oluşturma

Sorununuzu giderme konusunda Trend Desteğe yardımcı olmak için hata ayıklayıcı raporları oluşturun.

Prosedür

1. **Güvenlik Ayarları** kısmına gidin.

2. Bir Messaging Security Agent seçin.
3. **Ayarları Yapılandır** öğesine tıklayın.

   Yeni bir ekran belirir.
4. **İşlemler** > **Destek/Hata Ayıklayıcı** öğesine tıklayın.

   Yeni bir ekran belirir.
5. İzlenecek modülleri seçin:
   - Messaging Security Agent **Ana Hizmeti**
   - Messaging Security Agent **Remote Configuration Server**
   - Messaging Security Agent **System Watcher**
   - Exchange Server 2003, 2007 veya 2010 üzerinde **Virus Scan API (VSAPI)**
   - Exchange Server 2013 üzerinde **Depo Düzeyinde Tarama**
   - Exchange Server 2003 üzerinde **Basit Posta Aktarım Protokolü (SMTP)**
   - Exchange Server 2007, 2010 veya 2013 üzerinde **Aktarım Hizmeti**
   - **Ortak Ağ Geçidi Arayüzü (CGI)**
6. **Uygula** öğesine tıklayın.

   Hata ayıklayıcı, seçilen modüller için veri toplamaya başlar.

Gerçek Zamanlı İzleme

Gerçek Zamanlı İzleme, seçilen Microsoft Exchange Server ve onun Messaging Security Agent'ı hakkında geçerli bilgileri görüntüler. Bulunan virüslerin ve spam'lerin sayısı, engellenen eklerin sayısı ve içerik ihlalinin sayısı da dahil olmak üzere taranmış iletilerle ilgili bilgileri veya koruma istatistiklerini gösterir. Ayrıca, aracının düzgün çalışıp çalışmadığını kontrol eder.

Gerçek Zamanlı İzleme ile Çalışma

Prosedür

1. Web konsolundan Gerçek Zamanlı İzlemeye erişmek için:
   a. **Güvenlik Ayarları** kısmına gidin.
   b. Bir aracı seçin.
   c. **Ayarları Yapılandır** öğesine tıklayın.

      Yeni bir ekran belirir.

   d. Ekranın sağ üst kısmındaki **Gerçek Zamanlı İzleme** bağlantısına tıklayın.
2. Windows Başlat menüsünden Gerçek Zamanlı İzleme'ye erişmek için, **Tüm Programlar > Trend Micro Messaging Security Agent > Gerçek Zamanlı İzleme** öğesine tıklayın.
3. Koruma istatistiklerini sıfırlamak için **Sıfırla** öğesine tıklayın.
4. Taranmış iletiler hakkındaki eski bilgileri temizlemek için, **İçeriği Temizle** öğesine tıklayın.

Giden E-posta İletilerine Feragatname Ekleme

Feragatname iletisini yalnızca giden e-posta iletilerine ekleyebilirsiniz.

Prosedür

1. Bir metin dosyası oluşturun ve feragatname metnini bu dosyaya ekleyin.
2. Kayıt defterinde şu anahtarları değiştirin:
   - İlk anahtar:

     Yol: HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\ScanMail for Exchange\CurrentVersion

Anahtar: EnableDisclaimer

Tür: REG_DWORD

Veri değeri: 0 - Devre Dışı Bırak, 1 - Etkinleştir

- İkinci anahtar:

  Yol: HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\ScanMail for Exchange\CurrentVersion

  Anahtar: DisclaimerSource

  Tür: REG_SZ

  Değer: Feragatname içeriği dosyasının tam yolu.

  Örneğin, C:\Data\Disclaimer.txt

  Nota

  WFBS, varsayılan olarak, dahili veya harici etki alanlarına giden posta gönderildiğini algılar ve harici etki alanlarına gönderilen her postaya bir feragatname ekler. Kullanıcı, varsayılan ayarın üzerine yazabilir ve şu kayıt defterine dahil edilen etki alanları dışında giden her postaya bir feragatname ekleyebilir:

- Üçüncü anahtar:

  Yol: HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\ScanMail for Exchange\CurrentVersion

  Anahtar: InternalDomains

  Tür: REG_SZ

  Değer: Dışlanacak etki alanı adlarını girin. Birden fazla öğeyi ayırmak için noktalı virgül (;) kullanın.

  Örneğin: domain1.org;domain2.org

Nota

Buradaki etki alanı adları, Exchange sunucularının DNS adlarıdır.

Bölüm 7

Taramaları Yönetme

Bu bölümde, ağınızı ve istemcilerinizi tehditlerden korumak için Security Agents ve Messaging Security Agents (yalnızca Advanced) üzerinde taramaları nasıl çalıştıracağınız anlatılmaktadır.

Taramalar Hakkında

Tarama sırasında, Trend Micro tarama motoru, kalıp eşleme olarak adlandırılan bir işlemi kullanarak ilk düzey algılamayı gerçekleştirmek için kalıp dosyası ile birlikte çalışır. Her tehdit kendisini diğer kodlardan ayıran benzersiz bir imza veya anormal karakter dizisi içerdiğinden, kalıp dosyasında bu kodun etkisiz parçaları yakalanır. Ardından motor, taranan her dosyanın belirli bölümlerini kalıp dosyasındaki kalıpla karşılaştırarak bir eşleşme arar.

Tarama motoru tehdit içeren diğer bir dosya algıladığında, temizleme, karantinaya alma, silme veya metin/dosya ile değiştirme gibi bir eylem gerçekleştirir (yalnızca Advanced). Tarama görevlerinizi ayarlarken bu eylemleri özelleştirebilirsiniz.

Worry-Free Business Security, **üç tarama türü** sağlar. Her bir taramanın farklı amacı ve kullanımı vardır, ancak tümü yaklaşık olarak aynı şekilde yapılandırılır.

- Gerçek Zamanlı Tarama. Ayrıntılar için bakınız, *Gerçek Zamanlı Tarama sayfa 7-2*.
- Manuel Tarama. Ayrıntılar için bakınız, *Manuel Tarama sayfa 7-3*.
- Zamanlanmış Tarama. Ayrıntılar için bakınız, *Zamanlanmış Tarama sayfa 7-6*.

Security Agents'lar taramaları çalıştırırken iki tarama tönteminden birini kullanır:

- Smart scan
- Geleneksel tarama

Ayrıntılar için bakınız, *Tarama Yöntemleri sayfa 5-3*.

Gerçek Zamanlı Tarama

Gerçek Zamanlı Tarama tutarlı ve sürekli bir taramadır.

Bir dosya her açıldığında, indirildiğinde, kopyalandığında veya değiştirildiğinde, **Security Agent** içindeki Gerçek Zamanlı Tarama dosyayı tehditlere karşı tarar. Gerçek Zamanlı Tarama yapılandırması hakkında ayrıntılar için, bkz. *Security Agent'lar için Gerçek Zamanlı Tarama Yapılandırma sayfa 5-7*.

E-posta iletileri durumunda, **Messaging Security Agent** (yalnızca Advanced); gelen iletilerin, SMTP iletilerinin, ortak klasörlere kopyalanan belgelerin ve diğer Microsoft Exchange sunucularından çoğaltılan dosyaların taramasını yaparak bilinen tüm virüs giriş noktalarını korur. Gerçek Zamanlı Tarama yapılandırması hakkında ayrıntılar için, bkz. *Messaging Security Agent'lar için Gerçek Zamanlı Tarama Yapılandırma sayfa 6-5*.

Manuel Tarama

Manuel Tarama, isteğe bağlı bir taramadır.

Security Agent'lar üzerindeki Manuel Tarama, dosyalardaki tehditleri giderir ve varsa eski etkilenmeleri yok ederek tekrar etkilenmeyi en aza indirir.

Messaging Security Agent'lar (yalnızca Advanced) üzerindeki Manuel Tarama, Microsoft Exchange sunucunuzun Bilgi Deposu'ndaki tüm dosyaları tarar.

Tarama için geçen zaman istemcinin donanım kaynaklarına ve taranacak dosya sayısına bağlıdır. İlerlemekte olan bir Manuel Tarama, eğer tarama web konsolu üzerinden uzaktan çalıştırılmışsa Security Server yöneticisi tarafından veya doğrudan istemci üzerinden çalıştırılmışsa kullanıcı tarafından durdurulabilir.

İpucu

Trend Micro, bir tehdit salgınından sonra Manuel Taramalar gerçekleştirilmesini önerir.

Manuel Taramaları Çalıştırma

Bu prosedür, Security Server yöneticilerinin web konsolundan **Security Agent'lar** ve **Messaging Security Agent'lar** (yalnızca Advanced) üzerinde nasıl Manuel Tarama çalıştırabileceğini açıklamaktadır.

Nota

Manuel Tarama ayrıca, Windows Görev Çubuğu üzerinde Security Agent simgesine sağ tıklayarak ve ardından **Şimdi Tara** üzerine tıklayarak da doğrudan çalıştırılabilir. Manuel Taramayı Microsoft Exchange sunucuları üzerinde doğrudan çalıştırmak mümkün değildir.

Prosedür

1. **Taramalar** > **Manuel Tarama** kısmına gidin.
2. (İsteğe bağlı) Manuel Tarama çalıştırmadan önce tarama ayarlarını özelleştirin.

TALİMATLAR VE NOTLAR	ÖNERİLEN TARAMA AYARLARI
Security Agent için tarama ayarlarını özelleştirmek için, bir masaüstü veya sunucu grubuna tıklayın. Bkz. *Security Agent'lar için Tarama Hedefleri ve Eylemler sayfa 7-9*. **Nota** Security Agent'lar için tarama ayarları ayrıca, kullanıcılar istemcilerden Manuel Tarama çalıştırırken de kullanılır. Ancak, kullanıcılara kendi tarama ayarlarını yapılandırma ayrıcalığını verirseniz, tarama sırasında kullanıcı tarafından yapılandırılmış ayarlar kullanılacaktır.	Hedef • Tüm taranabilir dosyalar: Tüm taranabilir dosyaları içerir. Taranamayan dosyalar; parola korumalı, şifrelenmiş veya kullanıcı tanımlı tarama kısıtlamalarını aşan dosyalardır. • Sıkıştırılmış dosyaları 1. katmana kadar tara: 1 sıkıştırma katmanı olan sıkıştırılmış dosyaları tarar. Varsayılan ayar, varsayılan sunucu grubu için "kapalı" ve varsayılan masaüstü bilgisayar grubu için "açık"tır. Dışlamalar • Trend Micro ürünlerinin yüklendiği dizinleri tarama Gelişmiş Ayarlar • Casus Yazılım/Grayware Onaylanan Listesini değiştir (yalnızca Casus Yazılımdan Koruma için)

Talimatlar ve Notlar	Önerilen Tarama Ayarları
Messaging Security Agent için tarama ayarlarını özelleştirmek için, bir aracıyı genişletin ve aşağıdakine tıklayın: • **Antivirüs**: Aracının virüsler ve kötü amaçlı yazılımlara karşı tarama yapması için tıklayın. Bkz. *Tarama Hedefleri ve Messaging Security Agent'lar için Eylemler sayfa 7-17*. • **İçerik Filtreleme**: Aracının postalarda yasaklanmış içerik taraması yapması için tıklayın. Bkz. *İçerik Filtreleme Kurallarını Yönetme sayfa 6-15*. • **Ek Engelleme**: Aracının ek kuralı ihlallerine karşı e-postayı taraması için seçin. Bkz. *Ek Engellemeyi Yapılandırma sayfa 6-45*.	• Aracı, tüm taranabilir dosyaları tarar. E-posta iletilerinin ileti gövdelerini de taramaya dahil eder. • Aracı, virüs veya başka kötü amaçlı yazılım içeren bir dosya algıladığında, dosyayı temizler. Dosyayı temizleyemezse, bunun yerine metinle/dosyayla değiştirir. • Aracı, Truva Atı veya solucan içeren bir dosya algıladığında, Truva Atını veya solucanı bir metinle veya dosyayla değiştirir. • Aracı, Paketleyici içeren bir dosya algıladığında, Paketleyiciyi bir metin veya dosyayla değiştirir. • Aracı, etkilenmiş sıkıştırılmış dosyaları temizlemez. Bu, gerçek zamanlı tarama sırasında gereken zamanı azaltır.

3. Taranacak grupları veya Messaging Security Agent'ları seçin.

4. **Şimdi Tara** öğesine tıklayın.

   Security Server, Manuel Tarama'yı çalıştırmak için aracılara bir bildirim gönderir. Beliren Tarama Bildirim Sonuçları ekranı size, bildirimi alan ve almayan aracıların sayısını gösterecektir.

5. Devam etmekte olan taramaları durdurmak için, **Taramayı Durdur** öğesine tıklayın.

   Security Server, Manuel Tarama'yı durdurmak için aracılara başka bir bildirim gönderir. Beliren Tarama Durdurma Bildirim Sonuçları ekranı size, bildirimi alan ve almayan aracıların sayısını gösterecektir. Security Agent'lar tarama çalıştırıldıktan sonra çevrimdışı olmuşlarsa veya ağ kesintileri varsa, bildirimi alamayabilir.

Zamanlanmış Tarama

Zamanlanmış Tarama, Manuel Taramaya benzerdir, ancak tüm dosyaları ve e-posta iletilerini (yalnızca Advanced) yapılandırılan zamanda ve sıklıkta tarar. İstemcilerde rutin taramaları otomatik hale getirmek ve tehdit yönetimi verimliliğini geliştirmek için Zamanlanmış Taramaları kullanın.

İpucu

Kullanıcılarda ve ağda olası kesintileri en aza indirmek için, Zamanlanmış Taramaları yoğun olmayan saatlerde çalıştırın.

Zamanlanmış Taramaları Yapılandırma

Trend Micro, zamanlanmış bir güncellemeyle aynı zamanda tarama zamanlaması yapmamanızı önerir. Bu, Zamanlanmış Tarama'nın erken olarak durmasına neden olabilir. Benzer şekilde, Zamanlanmış Tarama çalışıyorken Manuel Tarama'ya başlarsanız, tarama duracaktır ama zamanlamasına göre tekrar çalışacaktır.

Prosedür

1. **Taramalar** > **Zamanlanmış Tarama** kısmına gidin.
2. **Zamanlama** sekmesine tıklayın.
   a. Tarama sıklığını (günlük, haftalık veya aylık) ve başlangıç zamanını yapılandırın. Her grup veya Messaging Security Agent kendi zamanlamasına sahip olabilir.

      Nota

      Aylık Zamanlanmış Taramalar için; 31, 30 veya 29 gün seçerseniz ve bundan daha az güne sahip bir ay olursa, tarama o ay çalışmayacaktır.

   b. (İsteğe bağlı) **Zamanlanmış bir tarama tamamlandıktan sonra istemciyi kapat** seçin.
   c. **Kaydet** öğesine tıklayın.

3. (İsteğe bağlı) Zamanlanmış Tarama ayarlarını özelleştirmek için **Ayarlar** sekmesine tıklayın.

Talimatlar ve Notlar	Önerilen Tarama Ayarları
Security Agent için tarama ayarlarını özelleştirmek için, bir masaüstü veya sunucu grubuna tıklayın. Bkz. *Security Agent'lar için Tarama Hedefleri ve Eylemler sayfa 7-9*. **Nota** Kullanıcılara kendi tarama ayarlarını yapılandırma ayrıcalığını verirseniz, tarama sırasında kullanıcı tarafından yapılandırılmış ayarlar kullanılacaktır.	Hedef • Tüm taranabilir dosyalar: Tüm taranabilir dosyaları içerir. Taranamayan dosyalar; parola korumalı, şifrelenmiş veya kullanıcı tanımlı tarama kısıtlamalarını aşan dosyalardır. • Sıkıştırılmış dosyaları 2. katmana kadar tara: 2 sıkıştırma katmanı olan sıkıştırılmış dosyaları tarar. Dışlamalar • Trend Micro ürünlerinin yüklendiği dizinleri tarama Gelişmiş Ayarlar • Casus Yazılım/Grayware Onaylanan Listesini değiştir (yalnızca Casus Yazılımdan Koruma için)

TALİMATLAR VE NOTLAR	ÖNERİLEN TARAMA AYARLARI
Messaging Security Agent için tarama ayarlarını özelleştirmek için, bir aracıyı genişletin ve aşağıdakine tıklayın: • **Antivirüs**: Aracının virüsler ve kötü amaçlı yazılımlara karşı tarama yapması için tıklayın. Bkz. *Tarama Hedefleri ve Messaging Security Agent'lar için Eylemler sayfa 7-17*. • **İçerik Filtreleme**: Aracının postalarda yasaklanmış içerik taraması yapması için tıklayın. Bkz. *İçerik Filtreleme Kurallarını Yönetme sayfa 6-15*. • **Ek Engelleme**: Aracının ek kuralı ihlallerine karşı e-postayı taraması için seçin. Bkz. *Ek Engellemeyi Yapılandırma sayfa 6-45*.	• Aracı, her Pazar günü 5:00'te başlayacak şekilde bir tarama gerçekleştirir. • Bu zamanlamayı, istemcileriniz için yoğunluğun düşük olduğu zamanlarda yürütülecek şekilde özelleştirin. Aracı, tüm taranabilir dosyaları tarar. E-posta iletilerinin ileti gövdelerini de taramaya dahil eder. • Aracı, virüs veya başka kötü amaçlı yazılım içeren bir dosya algıladığında, dosyayı temizler. Dosyayı temizleyemezse, bunun yerine metinle/dosyayla değiştirir. • Aracı, Truva Atı veya solucan içeren bir dosya algıladığında, Truva Atını veya solucanı bir metinle/dosyayla değiştirir. • Aracı, Paketleyici içeren bir dosya algıladığında, metinle/dosyayla değiştirir. • Aracı, etkilenmiş sıkıştırılmış dosyaları temizlemez.

4. Zamanlanmış Tarama ayarlarını uygulayacak grupları veya Messaging Security Agent'ları seçin.

Nota

Zamanlanmış Tarama'yı devre dışı bırakmak için, grup veya Messaging Security Agent için onay kutusundaki işareti kaldırın.

5. **Kaydet** öğesine tıklayın.

Security Agent'lar için Tarama Hedefleri ve Eylemler

Her tarama türü (Manuel tarama, Zamanlanmış Tarama ve Gerçek Zamanlı Tarama) için aşağıdaki ayarları yapılandırın:

Hedef Sekmesi

Yöntem seçin:

- **Tüm taranabilir dosyalar**: tüm taranabilir dosyaları içerir. Taranamayan dosyalar; parola korumalı, şifrelenmiş veya kullanıcı tanımlı tarama kısıtlamalarını aşan dosyalardır.

  Nota

  Bu seçenek olası en yüksek güvenliği sağlar. Ancak, her dosyanın taranması çok büyük zaman ve kaynak gerektirir ve bazı durumlarda gereksiz olabilir. Bu nedenle, aracının taramaya dahil edeceği dosyaların miktarını sınırlayabilirsiniz.

- **IntelliScan "gerçek dosya türü" tanımlamasını kullanır**: Gerçek dosya türünü temel alarak dosyaları tarar. Bkz. *IntelliScan sayfa D-2*.

- **Aşağıdaki uzantılara sahip dosyaları tara**: Uzantılarına göre taranacak dosyaları manuel olarak belirtin. Birden fazla girdiyi virgüllerle ayırın.

Tarama başlatıcı seç:

- **Oku**: İçeriği okunan dosyaları tarar; dosyalar açıldığında, yürütüldüğünde, kopyalandığında veya taşındığında okunur.

- **Yaz**: İçeriği yazılmakta olan dosyaları tarar; bir dosyanın içeriği, dosya değiştirildiğinde, kaydedildiğinde, indirildiğinde veya başka bir konumdan kopyalandığında yazılır.

- **Okuma veya yazma**

Tarama Dışlamaları

Aşağıdaki ayarlar yapılandırılabilir:

- Dışlamaları etkinleştir veya devre dışı bırak
- Trend Micro ürün dizinlerini taramaların dışında tut
- Diğer dizinleri taramaların dışında tut

  Belirttiğiniz dizin yolundaki tüm alt dizinler de dışlanır
- Dosya adlarını veya tam yol ile dosya adlarını taramaların dışında tut
- Dosya uzantılarını dışla

  Dosya uzantılarında "*" gibi joker karakterler kabul edilmez

Nota

(Yalnızca Advanced) Microsoft Exchange Server istemcide çalıştırılıyorsa, Trend Micro tüm Microsoft Exchange Server klasörlerinin taramadan dışlamasını önermektedir. Microsoft Exchange sunucusu klasörlerini genel olarak taramadan dışlamak için, **Tercihler** > **Genel Ayarlar** > **Masaüstü/Sunucu {sekme}** > **Genel Tarama Ayarları**'na gidin ve **Microsoft Exchange sunucusuna yüklendiğinde Microsoft Exchange sunucusu klasörlerini dışla** seçeneğini işaretleyin.

Gelişmiş Ayarlar

Tarama Türü	Seçenek
Gerçek Zamanlı Tarama	**POP3 iletilerini tara**: Varsayılan olarak Posta Taraması yalnız Gelen Kutusu ve Önemsiz Posta klasörlerine bağlantı noktası 110 aracılığıyla gönderilen yeni iletileri tarar. Güvenli POP3'ü (SSL-POP3) desteklemez. • Outlook Express™ 6.0, Service Pack 2 ile (yalnız Windows XP için) • Windows Mail™ (yalnızca Microsoft Vista'da) • Microsoft Outlook 2000, 2002 (XP), 2003, 2007, 2010 veya 2013 • Mozilla Thunderbird 1.5 veya üzeri Posta Taraması IMAP iletilerindeki güvenlik risklerini algılayamaz. IMAP iletilerindeki güvenlik risklerini ve spam'i algılamak için Messaging Security Agent'ı (yalnızca Advanced) kullanın.
Gerçek Zamanlı Tarama, Manuel Tarama	**Ağdaki eşlenmiş sürücüleri ve paylaşılan klasörleri tara**: Fiziksel olarak diğer bilgisayarlarda bulunan ancak yerel bilgisayara eşlenen dizinleri taramak için seçin.
Gerçek Zamanlı Tarama	**Sistem kapanması sırasında disketleri tara**
Gerçek Zamanlı Tarama	**IntelliTrap'i etkinleştir**: IntelliTrap, sıkıştırılmış dosyalarda botlar gibi zararlı kodu algılar. Bkz. *IntelliTrap sayfa D-2*.
Gerçek Zamanlı Tarama	**Bellekte tespit edilen kötü amaçlı varyantları karantinaya al**: Gerçek Zamanlı Tarama veya Davranış İzleme etkinleştirilmişse ve bu seçenek seçilmişse, paketlenmiş kötü amaçlı yazılım için çalışan bir işlem belleği taranır. Behavior Monitoring tarafından tespit edilen paketlenmiş kötü amaçlı yazılımlar karantinaya alınır.
Gerçek Zamanlı Tarama, Manuel Tarama, Zamanlanmış Tarama	**Sıkıştırılmış dosyaları katmana kadar tara __**: Sıkıştırılmış bir dosya her sıkıştırma işlemi için bir katman edinir. Etkilenmiş bir dosya birden fazla katman şeklinde sıkıştırılmışsa, etkilenmenin algılanması için belirtilen katman sayısı boyunca taranması gerekir. Ancak, birden fazla katmanı taramak daha fazla zaman ve kaynak gerektirir.

TARAMA TÜRÜ	SEÇENEK
Gerçek Zamanlı Tarama, Manuel Tarama, Zamanlanmış Tarama	**Casus Yazılım/Grayware Onaylanan Listesini Değiştir**: Bu ayar, aracı konsolundan yapılamaz.
Manuel Tarama, Zamanlanmış Tarama	**CPU Kullanımı/Tarama Hızı**: Security Agent, bir dosyayı taradıktan sonra ve sonraki dosyayı taramadan önce duraklayabilir. Aşağıdaki seçeneklerden birini belirleyin: • **Yüksek**: Taramalar arasında duraklama yok • **Orta**: CPU kullanımı % 50'den fazlaysa dosya taramaları arasında duraklat, %50 veya daha azsa duraklatma • **Düşük**: CPU kullanımı % 20'den fazlaysa dosya taramaları arasında duraklat, %20 veya daha azsa duraklatma
Manuel Tarama, Zamanlanmış Tarama	**Gelişmiş temizlemeyi çalıştır**: Security Agent'in etkinlikleri, FakeAV olarak da bilinen sahte güvenlik yazılımı tarafından durdurulur. Aracı ayrıca FakeAV davranışı gösteren uygulamaları etkin bir şekilde algılamak ve durdurmak için gelişmiş temizleme kuralları kullanır. **Nota** Gelişmiş temizleme, etkin koruma sağlarken, yüksek sayıda yanlış pozitifle de sonuçlanır.

Casus Yazılım/Grayware Onaylanan Listesi

Bazı uygulamaların Trend Micro tarafından casus yazılım/grayware olarak sınıflandırılmasının nedeni, yüklü oldukları sisteme zarar verebilmeleri değil, istemciyi veya ağı kötü amaçlı yazılım veya korsan saldırılarına maruz bırakma potansiyeline sahip olmalarıdır.

Worry-Free Business Security potansiyel olarak riskli uygulamaların bir listesini içerir ve varsayılan olarak, bu uygulamaların İstemciler üzerinde yürütülmesini önler.

İstemcilerin Trend Micro tarafından casus yazılım/grayware olarak sınıflandırılan bir uygulamayı çalıştırması gerektiği takdirde, uygulama adını casus yazılım/grayware onaylanan listesine eklemeniz gerekir.

Eylem Sekmesi

Security Agent'ların virüslere/kötü amaçlı yazılımlara karşı gerçekleştirebileceği eylemler şunlardır:

TABLO 7-1. Virüs/Kötü Amaçlı Yazılım Tarama Eylemleri

EYLEM	AÇIKLAMA
Sil	Etkilenen dosyayı siler.
Karantinaya Al	Etkilenen dosyayı yeniden adlandırır ve istemci üzerinde geçici bir karantina dizinine taşır. Ardından Security Agent'lar karantinaya alınmış dosyaları, varsayılan olarak Security Server üzerinde yer alan belirlenmiş karantina dizinine gönderir. Security Agent, bu dizine gönderilen karantinaya alınmış dosyaları şifreler. Karantinaya alınmış dosyalardan herhangi birini geri yüklemeniz gerekirse, VSEncrypt aracını kullanın.
Temizle	Dosyaya tam erişime izin vermeden önce etkilenen dosyayı temizler. Dosya temizlenemiyorsa, Security Agent ikinci bir eylem olarak aşağıdaki eylemlerden birini gerçekleştirir: Karantinaya Al, Sil, Yeniden Adlandır ve Geçiş Bu işlem, olası virüs/kötü amaçlı yazılım haricinde tüm kötü amaçlı yazılım türlerinde gerçekleştirilebilir. **Nota** Bazı dosyalar temizlenebilir değildir. Ayrıntılar için, bkz. *Temizlenemeyen Dosyalar sayfa D-25*.

EYLEM	AÇIKLAMA
Yeniden Adlandır	Etkilenen dosyanın uzantısını "vir" olarak değiştirir. Kullanıcılar yeniden adlandırılmış dosyayı önce açamazlar, ancak dosyayı belirli bir uygulamayla ilişkilendirirlerse açabilirler. Yeniden adlandırılmış olan etkilenen dosya açılırken bir virüs/kötü amaçlı yazılım çalışabilir.
Atla	Sadece Manuel Tarama ve Zamanlanmış Tarama sırasında gerçekleştirilir. Security Agent bu tarama eylemini Gerçek Zamanlı Tarama sırasında kullanamaz, çünkü etkilenmiş bir dosyayı açma veya yürütme denemesi algılandığında bir eylem gerçekleştirilmemesi, virüsün/kötü amaçlı yazılımın yürütülmesine izin verecektir. Diğer tüm tarama eylemleri Gerçek Zamanlı Tarama sırasında kullanılabilir.
Erişimi Reddet	Sadece Gerçek Zamanlı Tarama sırasında gerçekleştirilir. Security Agent, etkilenmiş bir dosyayı açma veya yürütme denemesi algıladığında, derhal işlemi engeller. Kullanıcılar etkilenen dosyayı manuel olarak silebilir.

Security Agent'ın gerçekleştirdiği tarama işlemi, casus yazılımı/grayware'i algılayan tarama türüne bağlıdır. Her bir virüs/kötü amaçlı yazılım türü için belirli eylemler yapılandırılabiliyor olsa da, tüm casus yazılım/grayware türleri için sadece bir eylem yapılandırılabilir. Örneğin, Manuel Tarama (tarama türü) sırasında Security Agent herhangi bir türde casus yazılım/grayware algılarsa, etkilenen sistem kaynaklarını temizler (eylemde bulunur).

Security Agent'ın casus/grayware yazılımlara karşı gerçekleştirebileceği eylemler şunlardır:

TABLO 7-2. Casus Yazılım/Grayware Tarama Eylemleri

EYLEM	AÇIKLAMA
Temizle	İşlemleri sonlandırır veya kayıt defterlerini, dosyaları, tanımlama bilgilerini ve kısayolları siler.

EYLEM	AÇIKLAMA
Geçiş	Algılanan casus yazılım/grayware için bir eylem gerçekleştirmez, ancak günlüklerde casus yazılım/grayware tespiti kaydedilir. Bu eylem sadece Manuel Tarama ve Zamanlanmış Tarama sırasında gerçekleştirilebilir. Gerçek Zamanlı Tarama sırasında eylem "Erişimi Reddet" olur. Algılanan casus yazılım/grayware onaylanmış listeye dahil değilse, Security Agent herhangi bir eylem gerçekleştirmeyecektir.
Erişimi Reddet	Algılanan casus yazılım/grayware bileşenlerine erişimi (kopyalama, açma) engeller. Bu eylem sadece Gerçek Zamanlı Tarama sırasında gerçekleştirilebilir. Manuel Tarama ve Zamanlanmış Tarama sırasındaki eylem "Geçiş" olacaktır.

ActiveAction

Farklı virüs/kötü amaçlı yazılım türleri, farklı tarama eylemleri gerektirir. Tarama eylemlerini özelleştirmek, virüsler/kötü amaçlı yazılımlar hakkında bilgi sahibi olmayı gerektirir ve oyalayıcı ve sıkıcı bir iş olabilir. Worry-Free Business Security bu sorunları ortadan kaldırmak için ActiveAction'ı kullanır.

ActiveAction, virüsler/kötü amaçlı yazılımlar için önceden yapılandırılmış tarama eylemleri setidir. Tarama eylemleri hakkında bilgi sahibi değilseniz veya belirli bir virüs/kötü amaçlı yazılım için hangi tarama eyleminin uygun olduğundan emin olamıyorsanız, Trend Micro, ActiveAction'ı kullanmanızı önerir.

ActiveAction'ı kullanmanın yararları şunlardır:

- ActiveAction, Trend Micro tarafından önerilen tarama eylemlerini kullanır. Tarama eylemlerini yapılandırmaya zaman ayırmanız gerekmez.
- Virüs yazarları, virüslerin/kötü amaçlı yazılımların bilgisayarlara saldırma şeklini sürekli olarak değiştirir. ActiveAction ayarları en son tehditlere ve virüs/kötü amaçlı yazılım saldırılarının en son yöntemlerine karşı korumak için güncellenir.

Aşağıdaki tablo, ActiveAction'ın her bir virüs/kötü amaçlı yazılım türünü nasıl işlediğini göstermektedir:

TABLO 7-3. Virüsler ve Kötü Amaçlı Yazılıma Karşı Trend Micro'nun Önerdiği Tarama Eylemleri

VİRÜS/KÖTÜ AMAÇLI YAZILIM TÜRÜ	GERÇEK ZAMANLI TARAMA		MANUEL TARAMA/ ZAMANLANMIŞ TARAMA	
	BİRİNCİ EYLEM	İKİNCİ EYLEM	BİRİNCİ EYLEM	İKİNCİ EYLEM
Şaka programı	Karantinaya Al	Sil	Karantinaya Al	Sil
Truva atı programı/ Solucanlar	Karantinaya Al	Sil	Karantinaya Al	Sil
Paketleyici	Karantinaya Al	Yok	Karantinaya Al	Yok
Olası virüs/kötü amaçlı yazılım	Karantinaya Al	Yok	Geçiş veya kullanıcı tarafından yapılandırılmış eylem	Yok
Virüs	Temizle	Karantinaya Al	Temizle	Karantinaya Al
Test Virüsü	Erişimi Reddet	Yok	Yok	Yok
Diğer kötü amaçlı yazılımlar	Temizle	Karantinaya Al	Temizle	Karantinaya Al

Notlar ve Hatırlatıcılar:

- Olası virüs/kötü amaçlı yazılım için varsayılan eylem, Gerçek Zamanlı Tarama sırasında "Erişimi Reddet" ve Manuel Tarama ve Zamanlanmış Tarama sırasında "Karantina" olur. Bunlar tercih ettiğiniz eylemler değilse, Sil veya Yeniden Adlandır olarak değiştirebilirsiniz.
- Bazı dosyalar temizlenebilir değildir. Ayrıntılar için, bkz. *Temizlenemeyen Dosyalar sayfa D-25*.
- ActiveAction, casus yazılım/grayware taraması için kullanılabilir değildir.
- Yeni kalıp dosyaları bulunduğunda bu ayarların varsayılan değerleri değişebilir.

Gelişmiş Ayarlar

TARAMA TÜRÜ	SEÇENEK
Gerçek Zamanlı Tarama, Zamanlanmış Tarama	**Bir virüs/casus yazılım algılandığında masaüstünde veya sunucuda bir uyarı iletisi görüntüle**
Gerçek Zamanlı Tarama, Zamanlanmış Tarama	**Olası bir virüs/casus yazılım algılandığında masaüstünde veya sunucuda bir uyarı iletisi görüntüle**
Manuel Tarama, Gerçek Zamanlı Tarama, Zamanlanmış Tarama	**Olası virüs/kötü amaçlı yazılım algılandığında temizlemeyi çalıştır**: Yalnızca ActiveAction'ı seçtiyseniz ve olası virüs/kötü amaçlı yazılım için eylemi özelleştirdiyseniz kullanılabilir.

Tarama Hedefleri ve Messaging Security Agent'lar için Eylemler

Her tarama türü (Manuel tarama, Zamanlanmış Tarama ve Gerçek Zamanlı Tarama) için aşağıdaki ayarları yapılandırın:

Hedef Sekmesi

- Tarama Hedefleri
- Ek Tehdit Tarama Ayarları
- Tarama Dışlamaları

Eylem Sekmesi

- Tarama Eylemleri/AktifEylem
- Bildirimler
- Gelişmiş Ayarlar

Tarama Hedefleri

Tarama hedeflerini seçin:

- **Tüm ek dosyalar**: Sadece şifreli veya parola korumalı dosyalar dışarıda bırakılır.

  Nota

  Bu seçenek olası en yüksek güvenliği sağlar. Ancak, her dosyanın taranması çok büyük zaman ve kaynak gerektirir ve bazı durumlarda gereksiz olabilir. Bu nedenle, aracının taramaya dahil edeceği dosyaların miktarını sınırlayabilirsiniz.

- **IntelliScan**: Dosyaları gerçek dosya türüne dayalı olarak tarar. Bkz. *IntelliScan sayfa D-2*.

- **Belirli dosya türleri**: WFBS, seçili türlere ve uzantılara sahip dosyaları tarayacaktır. Birden fazla girişleri noktalı virgülle (;) ayırın.

Diğer seçenekleri seçin:

- **IntelliTrap'i Etkinleştir**: IntelliTrap, sıkıştırılmış dosyalarda botlar gibi zararlı kodu algılar. Bkz. *IntelliTrap sayfa D-2*.

- **İleti gövdesini tara**: Gömülü tehdit içerme olasılığı bulunan e-posta iletisinin gövdesini tarar.

Ek Tehdit Tarama Ayarları

Aracının taraması gereken diğer tehditleri seçin. Bu tehditler hakkında ayrıntılar için, bkz. *Tehditleri Anlama sayfa 1-23*.

İlave seçenekleri seçin:

- **Etkilenen dosyayı temizlemeden önce yedekle**: WFBS, temizlemeden önce, algılanan tehdidin yedeğini oluşturur. Yedeklenen dosya şifrelenir ve istemci üzerinde aşağıdaki dizinde depolanır:

  <Messaging Security Agent installation folder>\storage\backup

  Gelişmiş Seçenekler kısmında **Yedekleme Ayarları** alt kısmında dizin değiştirebilirsiniz.

  Dosyanın şifresini açmak için bkz. *Şifrelenmiş Dosyaları Geri Yükleme sayfa 14-9*

- **Performansı en iyileştirmek için etkilenen sıkıştırılmış dosyaları temizleme**

Tarama Dışlamaları

Hedef sekmesi altından **Dışlamalar** kısmına gidin ve aşağıdaki kriterlerden aracının e-posta iletilerini taramalardan dışlarken kullanacaklarını seçin:

- **İleti gövde boyutu şu sınırı aşıyorsa**: Messaging Security Agent e-posta iletilerini, yalnızca iletinin gövde boyutu belirlenen büyüklüğün altında veya ona eşit olduğu zaman tarar.
- **Ek boyutu şu sınırı aşıyorsa**: Messaging Security Agent e-posta iletilerini, yalnızca ek dosyasının boyutu belirlenen büyüklüğün altında veya ona eşit olduğu zaman tarar.

İpucu

Trend Micro 30 MB'lik bir sınırı önerir.

- **Sıkıştırılmamış dosya sayısı şu sınırı aşıyorsa**: Sıkıştırılmış dosya içindeki açılmış dosyaların miktarı belirlenen sayıyı geçtiğinde, Messaging Security Agent yalnızca bu seçenekle belirlenen sınıra kadar olan dosyaları tarar.
- **Sıkıştırılmış dosya boyutu şu sınırı aşıyorsa**: Messaging Security Agent, yalnızca açıldıktan sonra boyutu belirtilen sınıra eşit veya onun altında olan sıkıştırılmış dosyaları tarar.
- **Sıkıştırma katmanı sayısı şu sınırı aşıyorsa**: Messaging Security Agent, yalnızca belirtilen sıkıştırma katmanına eşit veya daha az katmana sahip sıkıştırılmış dosyaları tarar. Örneğin, sıkıştırma katmanı sınırı 5 olarak ayarlanırsa, Messaging Security Agent sıkıştırılmış dosyaların yalnızca ilk 5 katmanını tarar, 6 veya daha fazla katman şeklinde sıkıştırılmış dosyaları taramaz.
- **Açılmış dosyanın boyutu, sıkıştırılmış dosyanın boyutundan "x" kat büyük**: Messaging Security Agent yalnızca açılmış dosya boyutunun sıkıştırılmış dosya boyutuna oranı bu sayıdan az ise sıkıştırılmış dosyaları tarar. Bu işlev, Servis Reddi (DoS) saldırısına sebep olabilecek bir sıkıştırılmış dosyanın Messaging Security Agent tarafından taranmasını engeller. Bir DoS saldırısı, bir posta sunucusunun kaynaklarının gereksiz görevler ile aşırı yüklenmesi sonucunda ortaya çıkar. Messaging Security Agent'ın çok büyük dosyalar halinde açılacak olan dosyaları taramasını engellemek, bu sorunun ortaya çıkmasını önler.

Örnek: Aşağıdaki tabloda "x" değeri için girilen değer 100'dür.

Dosya boyutu (sıkıştırılmamış)	Dosya boyutu (sıkıştırılmamış)	Sonuç
500 KB	10 KB (oran 50:1)	Tarandı
1.000 KB	10 KB (oran 100:1)	Tarandı
1.001 KB	10 KB (oran 100:1'i aşıyor)	Taranmadı *
2000 KB	10 KB (oran 200:1)	Taranmadı *

* Messaging Security Agent dışlanmış dosyalar için sizin yapılandırdığınız eylemi gerçekleştirir.

Tarama Eylemleri

Yöneticiler, Messaging Security Agent'ı virüs/kötü amaçlı yazılım, Truva Atları ve solucanlar tarafından sunulan tehdidin türüne göre eylemde bulunacak şekilde yapılandırabilirler. Özelleştirilmiş eylemler kullanıyorsanız, her türde tehdit için bir eylem ayarlayın.

Tablo 7-4. Messaging Security Agent Özelleştirilmiş Eylemleri

Eylem	Açıklama
Temizle	Etkilenen ileti gövdelerindeki ve eklerindeki zararlı kodu kaldırır. Kalan e-posta ileti metni, etkilenmemiş dosyalar ve temizlenen dosyalar istenen alıcılara teslim edilir. Trend Micro, virüs/kötü amaçlı yazılım için varsayılan tarama eylemi olan temizle seçeneğini kullanmanızı önerir. Bazı koşullar altında, Messaging Security Agent bir dosyayı temizleyemez. Bir Manuel Tarama veya Zamanlanmış Tarama sırasında Messaging Security Agent, Bilgi Deposunu günceller ve dosyayı temizlenmiş olanı ile değiştirir.

Eylem	Açıklama
Metin/dosya ile değiştir	Etkilenmiş/filtrelenmiş içeriği siler ve onu bir metin veya dosya ile değiştirir. E-posta iletisi, hedeflenen alıcıya gönderilir ancak alıcı orijinal içeriğin etkilendiği ve değiştirildiği ile ilgili metin değiştirme tarafından bilgilendirilir. İçerik Filtreleme ve Veri Kaybını Önleme için, metni yalnızca gövde veya ek alanlarında değiştirebilirsiniz (Kimden, Kime, Cc veya Konu alanlarında değil).
İletinin tamamını karantinaya al	(Yalnızca Gerçek Zamanlı Tarama) Yalnızca etkilenen içeriği karantina dizininde karantinaya alır ve alıcı, iletiyi bu içerik olmadan alır. İçerik Filtreleme, Veri Kaybını Önleme ve Ek Engelleme için, tüm iletiyi karantina dizinine taşır.
İleti bölümünü karantinaya al	(Yalnızca Gerçek Zamanlı Tarama) Yalnızca etkilenen veya filtrelenen içeriği karantina dizininde karantinaya alır ve alıcı iletiyi bu içerik olmadan alır.
İletinin tamamını sil	(Yalnızca Gerçek Zamanlı Tarama) Tüm e-posta iletisini siler. Orijinal alıcı iletiyi almaz.
Geçiş	Virüs günlüklerinin içine zararlı dosyaların virüs bulaşmasını kaydeder ancak eyleme geçmez. Dışlanan, şifrelenen veya parola korumalı dosyalar, günlükler güncellenmeden alıcıya teslim edilir. İçerik Filtrelemesi için, iletiyi olduğu gibi teslim eder.
Arşiv	İletiyi arşiv dizinine taşır ve orijinal alıcısına teslim eder.
İletiyi sunucu tarafındaki spam klasöründe karantinaya al	İletinin tamamını karantina için Security Server'a gönderir.
İletiyi kullanıcının spam klasöründe karantinaya al	İletinin tamamını karantina için kullanıcının spam klasörüne gönderir. Klasör, Bilgi Deposu'nun sunucu tarafında yer alır.
Etiketle ve teslim et	E-posta iletisinin üstbilgisine, spam olarak tanımlandığına ilişkin bir etiket ekler ve hedeflenen alıcıya teslim eder.

Bu eylemlere ek olarak, aşağıdakileri de yapılandırabilirsiniz:

- **Toplu posta gönderme davranışı üzerinde eylemi etkinleştir**: Tehditlerin toplu posta gönderme davranışı türü için; Temizle, Metinle/Dosyayla Değiştir, İletinin Tamamını Sil, Geçir, İleti bölümünü karantinaya al seçenekleri arasından seçim yapın.
- **Temizleme başarısız olduğunda bunu yap**: Başarısız temizleme girişimleri için ikinci eylemi ayarlayın. Temizle, Metinle/Dosyayla Değiştir, İletinin Tamamını Sil, Geçir veya İleti bölümünü karantinaya al seçenekleri arasından seçim yapın.

ActiveAction

Aşağıdaki tablo, ActiveAction'ın her bir virüs/kötü amaçlı yazılım türünü nasıl işlediğini göstermektedir:

TABLO 7-5. Virüsler ve Kötü Amaçlı Yazılıma Karşı Trend Micro'nun Önerdiği Tarama Eylemleri

VİRÜS/KÖTÜ AMAÇLI YAZILIM TÜRÜ	GERÇEK ZAMANLI TARAMA		MANUEL TARAMA/ ZAMANLANMIŞ TARAMA	
	BİRİNCİ EYLEM	İKİNCİ EYLEM	BİRİNCİ EYLEM	İKİNCİ EYLEM
Virüs	Temizle	İletinin tamamını sil	Temizle	Metin/dosya ile değiştir
Truva atı programı/ Solucanlar	Metin/dosya ile değiştir	Yok	Metin/dosya ile değiştir	Yok
Paketleyici	İleti bölümünü karantinaya al	Yok	İleti bölümünü karantinaya al	Yok
Diğer zararlı kod	Temizle	İletinin tamamını sil	Temizle	Metin/dosya ile değiştir
Ek tehditler	İleti bölümünü karantinaya al	Yok	Metin/dosya ile değiştir	Yok
Toplu posta atma davranışı	İletinin tamamını sil	Yok	Metin/dosya ile değiştir	Yok

Tarama Eylemi Bildirimleri

Messaging Security Agent'ı belirli bir e-posta iletisine karşı önlem alırken hedeflenen alıcılarına bildirimde bulunacak şekilde ayarlamak için, **Alıcılara bildir** seçeneğini seçin. Çeşitli nedenlerden ötürü, harici posta alıcılarına hassas bilgiler içeren bir iletinin engellendiğini bildirmek istemeyebilirsiniz. Bildirimleri yalnızca dahili posta alıcılarına göndermek için, **Harici alıcılara bildirme** seçeneğini seçin. **İşlemler** > **Bildirim Ayarları** > **Dahili Posta Tanımı** seçeneklerinden dahili adresleri tanımlayın.

Kimlik sahtekarlığı yapan gönderenlerin harici alıcılarına bildirim göndermeyi de devre dışı bırakabilirsiniz.

Gelişmiş Ayarlar (Tarama Eylemleri)

Ayarlar	Ayrıntılar

Makrolar	Makro virüsler, uygulamalara eşlik eden makro yardımcı programlarını etkileyen uygulamaya özgü virüslerdir. Gelişmiş makrı taraması, makro virüsleri algılamak için sezgisel tarama kullanır veya algılanan tüm makro kodlarını söker. Tahmini tarama, virüsleri algılamanın zararlı makro kod araması yapmak için kalıp tanımayı ve kurallara dayalı teknolojileri kullanan değerlendirme yöntemidir. Bu yöntem, bilinen bir virüs imzası olmayan, keşfedilmemiş virüs ve tehditleri algılamada mükemmel sonuçlara ulaşır.
	
	Messaging Security Agent, yapılandırdığınız eyleme bağlı olarak zararlı makro koda karşı eylem gerçekleştirir.
	
	• **Tahmini düzey**
	  • Düzey 1, en belirli ölçütleri kullanır ama en az makro kodu algılar.
	  • Düzey 4, en çok makro kodu algılar ama en az belirli ölçütü kullanır ve güvenli makro kodu yanlışlıkla zararlı makro kod içeriyor olarak tanımlayabilir.
	
	İpucu
	Trend Micro, 2. sezgisel tarama düzeyini önerir. Bu düzey, bilinmeyen makro virüsleri için yüksek bir algılama düzeyi ve hızlı tarama hızı sağlar ve makro virüs dizelerini denetlemek için yalnızca gereken kuralları kullanır. Ayrıca düzey 2'nin güvenli makro kod içerisindeki zararlı kodu yanlış olarak tanımlama düzeyi düşüktür.
	
	• **Gelişmiş makro tarama tarafından algılanan tüm makroları sil**: Taranan dosyalarda algılanan makro kodlarının tümünü sök

Taranamayan İleti Bölümleri	Şifreli ve/veya parola korumalı dosyalar için eylem ve bildirim koşulunu ayarlayın. Eylem için, Metinle/Dosyayla Değiştir, İletinin tamamını karantinaya al, İletinin tamamını sil, Geçiş veya İleti bölümünü karantinaya al seçenekleri arasından seçim yapın.

AYARLAR	AYRINTILAR
Dışlanan İleti Bölümleri	İletilerin dışlanan bölümleri için eylem ve bildirim koşulunu ayarlayın. Eylem için, Metinle/Dosyayla Değiştir, İletinin tamamını karantinaya al, İletinin tamamını sil, Geçiş veya İleti bölümünü karantinaya al seçenekleri arasından seçim yapın.
Yedekleme Ayarı	Aracı temizlemeden önce etkilenen dosyaların yedeğini kaydetmek için konum.
Değiştirme Ayarları	Değiştirme metni için metni ve dosyayı yapılandırın. Eylem **metinle/dosyayla değiştirme** ise, WFBS tehdidi bu metin dizesi ve dosyasıyla değiştirecektir.

Bölüm 8

Güncellemeleri Yönetme

Bu bölüm, Worry-Free Business Security bileşenlerini ve güncelleme prosedürlerini açıklamaktadır.

Güncellemeye Genel Bakış

Tüm bileşen güncellemeleri Trend Micro ActiveUpdate server'dan kaynaklanır. Güncellemeler mevcut olduğunda, Security Server güncellenmiş bileşenleri indirir ve Security Agent'lara ve Messaging Security Agent'lara (yalnızca Advanced) dağıtır.

Bir Security Server, çok sayıda Security Agent'ı yönetiyorsa, güncelleme oldukça önemli miktarda bilgisayar kaynağı kullanabilir ve sunucunun kararlılığını ve performansını etkileyebilir. Bu sorunu gidermek için, Worry-Free Business Security'de güncellemeleri diğer Security Agent'lara dağıtma görevini paylaştırmak için belirli Security Agent'ların kullanılmasına imkan sağlayan **Update Agent** (Güncelleme Aracısı) özelliği vardır.

Aşağıdaki tablo Security Server ve aracıları için bileşen güncelleme seçeneklerini ve kullanılacakları zaman için önerileri açıklamaktadır:

TABLO 8-1. Güncelleme Seçenekleri

GÜNCELLEME SIRASI	AÇIKLAMA	ÖNERİ
1. ActiveUpdate Server veya özel güncelleme kaynağı 2. Security Server 3. Aracılar	Trend Micro Security Server, güncellenmiş bileşenleri ActiveUpdate sunucusundan veya özel bir güncelleme kaynağından alır ve doğrudan aracılara (Security Agent'lar ve Messaging Security Agent'lar) dağıtır.	Security Server ve aracılar arasında düşük bant genişlikli kesimler yoksa, bu yöntemi kullanın.

Güncelleme Sırası	Açıklama	Öneri
1. ActiveUpdate Server veya özel güncelleme kaynağı 2. Security Server 3. Güncelleme Aracıları, Messaging Security Agent'lar, Güncelleme Aracıları olmadan Security Agent'lar 4. Diğer tüm Security Agent'lar	Trend Micro Security Server, güncellenmiş bileşenleri ActiveUpdate sunucusundan veya özel bir güncelleme kaynağından alır ve doğrudan şunlara dağıtır: • Güncelleme Aracıları • Messaging Security Agent'lar • Güncelleme Aracıları olmadan Security Agent'lar Ardından, Güncelleme Aracıları bileşenleri ilgili Security Agent'lara dağıtır. Bu Security Agent'lar güncelleme yapamıyorsa, doğrudan Security Server'dan güncellenir.	Security Server ve Security Agent'lar arasında düşük bant genişlikli kesimler varsa, ağdaki trafik yükünü dengelemek için bu yöntemi kullanın.
1. ActiveUpdate Server 2. Security Agent'lar	Herhangi bir kaynaktan güncellenemeyen Security Agent'lar doğrudan ActiveUpdate sunucusundan güncellenir. **Nota** Messaging Security Agent'lar asla doğrudan ActiveUpdate sunucusundan güncellenmez. Tüm kaynaklar kullanılmaz ise, Messaging Security Agent güncelleme işleminden çıkar.	Bu mekanizma sadece son seçenek olarak sağlanmaktadır.

Güncellenebilir Bileşenler

Worry-Free Business Security, aracılar için en son tehditlere karşı koruma sağlamak için bileşenlerden yararlanır. Manuel veya zamanlanmış güncellemeler gerçekleştirerek bu bileşenleri güncel tutun.

Salgın Savunması, Antivirüs, casus yazılımlara karşı program ve Ağ Virüsü bileşenlerinin durumunu **Canlı Durum** ekranından görüntüleyin. Eğer Worry-Free Business Security (yalnızca Advanced), Microsoft Exchange sunucularını koruyorsa, Anti-spam bileşenlerinin durumunu da görüntüleyebilirsiniz. Bileşen güncellemeleri gerekli olduğunda Worry-Free Business Security, Yöneticilere bir bildirim gönderebilir.

Aşağıdaki tablolar, Security Server tarafından ActiveUpdate sunucusundan indirilen bileşenleri listelemektedir:

TABLO 8-2. İleti Bileşenleri (Yalnızca Advanced)

BİLEŞEN	DAĞITIM	AÇIKLAMA
Messaging Security Agent Anti-spam Kalıbı	Messaging Security Agent'lar	Anti-spam Kalıbı, e-posta iletilerindeki ve e-posta eklerindeki en son spam'leri tanımlar.
Messaging Security Agent Anti-spam Motoru 32/64-bit	Messaging Security Agent'lar	Anti-spam Motoru, e-posta iletilerindeki ve e-posta eklerindeki spam'leri tanımlar.
Messaging Security Agent Tarama Motoru 32/64-bit	Messaging Security Agent'lar	Tarama Motoru, e-posta iletilerindeki ve e-posta eklerindeki internet solucanlarını, toplu posta atıcıları, truva atlarını, kimlik avı sitelerini, casus yazılımları, yetkisiz ağ programlarını ve virüsleri algılar.
Messaging Security Agent URL Filtreleme Motoru 32/64-bit	Messaging Security Agent'lar	URL Filtreleme Motoru, Worry-Free Business Security ve Trend Micro URL Filtreleme Hizmeti arasındaki iletişimi kolaylaştırır. URL Filtreleme Hizmeti, URL'leri sınıflandıran ve Worry-Free Business Security'ye sınıflandırma bilgisini sağlayan bir sistemdir.

TABLO 8-3. Antivirüs ve Smart Scan

BİLEŞEN	DAĞITIM	AÇIKLAMA
Virüs Tarama Motoru 32/64-bit	Security Agent'lar	Trend Micro ürünlerinin hepsinin merkezinde, eski dosya tabanlı virüslere karşılık olarak orijinal bir biçimde geliştirilmiş bir tarama motoru bulunur. Günümüzde, tarama motoru aşırı ölçüde niteliklidir ve farklı türde virüsleri ve kötü amaçlı yazılımları algılayabilir. Tarama motoru ayrıca, araştırma için geliştirilen ve kullanılan kontrol altındaki virüsleri de algılar. Her dosyanın her bir baytını taramak yerine, motor ve kalıp dosyası birlikte çalışarak şunları tanımlar: • Virüs kodunun gösterge karakteristiklerini • Virüsün bir dosya içinde bulunduğu kesin konum

Bileşen	Dağıtım	Açıklama
Smart Scan Pattern	Security Agent'lar için dağıtımı yapılmaz. Bu kalıp, Security Server içinde kalır ve Security Agent'lar'dan alınan tarama sorgularına yanıt verirken kullanılır.	Smart scan modundayken Security Agent'lar, klasik casus yazılıma karşı ve kötü amaçlı yazılıma karşı kalıplar tarafından sağlanan ile aynı korumayı sağlamak için iki adet daha küçük kalıp kullanır. **Smart Scan Pattern** kalıp tanımlarının çoğunluğunu içerir. **Smart Scan Agent Kalıbı**, Smart Scan Kalıbı'nda bulunmayan diğer tüm kalıp tanımlarını içerir.
Smart Scan Agent Kalıbı	Security Agent'lar smart scan kullanılarak	Security Agent, **Smart Scan Agent Kalıbı**'nı kullanarak güvenlik tehditlerine karşı tarama yapar. Tarama sırasında dosyanın tehlikesini belirleyemeyen Security Agent'lar, Security Server üzerinde yer alan bir hizmet olan Tarama Sunucusu'na bir tarama sorgusu göndererek tehlikeyi doğrular. Tarama Sunucusu, **Smart Scan Kalıbı**'nı kullanarak tehlikeyi doğrular. Security Agent, tarama performansını iyileştirmek için Tarama Sunucusu tarafından sağlanan tarama sorgusu sonucunu "saklar".
Virüs Kalıbı	Security Agent'lar geleneksel tarama kullanılarak	Virüs Kalıbı, Security Agent'lar'nin en son virüs/kötü amaçlı yazılım ve karışık tehdit saldırısını tanımlamasına yardımcı olan bilgileri içerir. Trend Micro, haftada birkaç kez ve çok zararlı bir virüs/kötü amaçlı yazılım keşfedildikten sonra Virüs Kalıbının yeni sürümlerini oluşturur ve yayınlar.
IntelliTrap Kalıbı	Security Agent'lar	IntelliTrap Kalıbı, yürütülebilir dosyalar olarak paketlenmiş gerçek zamanlı sıkıştırılmış dosyaları algılar. Ayrıntılar için, bkz. *IntelliTrap sayfa D-2*.

Bileşen	Dağıtım	Açıklama
IntelliTrap Kural Dışı Durum Kalıbı	Security Agent'lar	IntelliTrap Kural Dışı Durum Kalıbı, "onaylanmış" sıkıştırılmış dosyaların bir listesini içerir.
Hasar Temizleme Motoru 32/64-bit	Security Agent'lar	Hasar Temizleme Motoru, Truva Atları ve işlemleri için tarama yapar ve bunları kaldırır.
Hasar Temizleme Şablonu	Security Agent'lar	Hasar Temizleme Şablonu, Hasar Tarama Motoru tarafından truva atı dosyalarının ve işlemlerinin tanımlanması için kullanılır, böylece motor bunları giderebilir.
Bellek Denetleme Deseni	Security Agent'lar	Bu teknoloji, polimorfik ve mutasyon virüsleri için gelişmiş virüs taraması sağlar ve virüs kalıbı tabanlı taramalarını dosya çalıştırmayı taklit ederek çoğaltır. Ardından, sistem performansına düşük etkisi olan zararlı amacın varlığı için denetimli bir ortamda sonuçlar analiz edilir

Tablo 8-4. Casus yazılımdan koruma

Bileşen	Dağıtım	Açıklama
Casus Yazılım/ Grayware Tarama Motoru v.6 32/64-bit	Security Agent'lar	Casus Yazılım Tarama Motoru, casus yazılım/grayware taraması yapar ve bunlar üzerinde uygun tarama eylemini gerçekleştirir.
Casus Yazılım/ Grayware Kalıbı v.6	Security Agent'lar	Casus Yazılım Kalıbı, dosyalardaki ve programlardaki, bellekteki modüllerdeki, Windows kaydındaki ve URL kısayollarındaki casus yazılımları/ grayware'leri tanımlar.
Casus Yazılım/ Grayware Kalıbı	Security Agent'lar	

TABLO 8-5. Ağ Virüsü

BİLEŞEN	DAĞITIM	AÇIKLAMA
Güvenlik Duvarı Kalıbı	Security Agent'lar	Virüs Kalıbı gibi Güvenlik Duvarı Kalıbı da, aracıların bir ağ virüsünün varlığına işaret eden virüs imzalarını, benzersiz bit ve bayt kalıplarını tanımlamasına yardımcı olur.

TABLO 8-6. Behavior Monitoring ve Aygıt Denetimi

BİLEŞEN	DAĞITIM	AÇIKLAMA
Behavior Monitoring Algılama Kalıbı 32/64-bit	Security Agent'lar	Bu kalıp, şüpheli tehdit davranışını algılama kurallarını içerir.
Behavior Monitoring Core Sürücüsü 32/64-bit	Security Agent'lar	Bu çekirdek modu sürücüsü, sistem olaylarını izler ve bunları ilke uygulaması için Behavior Monitoring Core Hizmetine aktarır.
Behavior Monitoring Core Hizmeti 32/64-bit	Security Agent'lar	Bu kullanıcı modu hizmeti, aşağıdaki işlevlere sahiptir: • Kök kullanıcı takımının tespitini sağlar • Harici aygıtlara erişimi düzenler • Dosyaları, kayıt defteri girişlerini ve hizmetleri korur.
Behavior Monitoring Yapılandırma Kalıbı	Security Agent'lar	Behavior Monitoring Sürücüsü, normal sistem olaylarını tanımlamak ve bunları ilke zorlamalarından dışlamak için bu kalıbı kullanır.
Hasar Kurtarma Motoru	Security Agent'lar	Hasar Kurtarma Motoru, şüpheli tehditler dosyaları değiştiremeden ve başka kötü amaçlı bir davranış gerçekleştiremeden önce sistem olaylarını ve yedekleme dosyalarını alır. Bu motor ayrıca dosya kurtarma isteği aldıktan sonra etkilenen dosyaları geri yükler.

Bileşen	Dağıtım	Açıklama
Hasar Kurtarma Modeli	Security Agent'lar	Hasar Kurtarma Modeli, şüpheli tehdit davranışını izlemek için kullanılan ilkeleri içerir.
Dijital İmza Kalıbı	Security Agent'lar	Bu kalıp, Behavior Monitoring Core Hizmeti tarafından bir sistem olayından sorumlu olan bir programın güvenli olup olmadığının belirlenmesinde kullanılan geçerli dijital imzaların bir listesidir.
İlke Uygulama Kalıbı	Security Agent'lar	Behavior Monitoring Core Service, sistem olaylarını bu kalıptaki ilkelere karşı denetler.
Bellek Taraması Deseni (32/64-bit)	Security Agent'lar	Bellek Taraması Tetikleyicileri hizmeti, bellekteki işlemin paketinin açılmamış olduğunu tespit ettiğinde diğer tarama motorlarını çalıştırır.

Tablo 8-7. Salgın Savunması

Bileşen	Dağıtım	Açıklama
Güvenlik Açığı Değerlendirme Kalıbı 32/64-bit	Security Agent'lar	Tüm güvenlik açıklarını barındıran bir veritabanı içeren dosyadır. Güvenlik Açığı Değerlendirme Kalıbı, tarama motorunun bilinen güvenlik açıklarını taraması için yönergeler sağlar.

Tablo 8-8. Tarayıcı Exploit'leri

Bileşen	Dağıtım	Açıklama
Tarayıcı Exploit Önleme Kalıbı	Security Agent'lar	Bu kalıp, en son web tarayıcısı exploitlerini tanımlar ve exploit'lerin web tarayıcısından ödün vermek üzere kullanılmasını engeller.
Script Analyzer Kalıbı	Security Agent'lar	Bu kalıp, web sayfalarındaki dizgileri kontrol eder ve zararlı dizgileri tanımlar.

Düzeltmeler, Yamalar ve Hizmet Paketleri

Trend Micro resmi bir ürün sürümünden sonra genellikle sorunlara çözüm bulmak, ürün performansını arttırmak veya yeni özellikler eklemek için aşağıdakileri geliştirir:

- *Kritik Yama sayfa D-2*
- *Düzeltme sayfa D-2*
- *Yama sayfa D-9*
- *Hizmet Paketi sayfa D-24*

Bu öğeler mevcut olduğunda satıcınız veya destek sağlayıcınız sizinle irtibat kurabilir. Yeni düzeltme, yama ve service pack sürümleriyle ilgili bilgi için Trend Micro web sitesini inceleyin:

http://downloadcenter.trendmicro.com/index.php?regs=TR

Tüm sürümler yükleme, dağıtım ve yapılandırma bilgilerini içeren bir benioku dosyasına sahiptir. Yüklemeyi gerçekleştirmeden önce benioku dosyasını dikkatle okuyun.

Security Server Güncellemeleri

Otomatik Güncellemeler

Security Server otomatik olarak aşağıdaki güncellemeleri gerçekleştirir:

- Security Server yüklendikten hemen sonra, Trend Micro ActiveUpdate sunucusundan güncellenir.
- Security Server her başlatıldığında, bileşenleri ve Salgın Savunması ilkesini günceller.
- Zamanlanmış güncellemeler varsayılan olarak her saatte bir çalışır (güncelleme sıklığı web konsolundan değiştirilebilir).

Manuel Güncellemeler

Bir güncelleme çok acilse, web konsolundan manuel güncellemeleri çalıştırabilirsiniz.

Sunucu Güncelleme Hatırlatmaları ve İpuçları

- Bir güncelleme sonrasında, Security Server bileşen güncellemelerini otomatik olarak aracılara dağıtır. Aracılara dağıtılan bileşenler hakkında ayrıntılar için, bkz. *Güncellenebilir Bileşenler sayfa 8-3*.

- Salt bir IPv6 Security Server, aşağıdaki görevleri gerçekleştiremez:

  - Trend Micro ActiveUpdate server veya salt bir IPv4 özel güncelleme kaynağından güncellemeleri edinmek.

  - Güncellemeleri doğrudan IPv4 aracılarına dağıtmak.

  Benzer şekilde, salt bir IPv4 Security Server salt bir IPv6 özel güncelleme kaynağından güncellemeleri doğrudan edinemez ve güncellemeleri salt IPv6 aracılara dağıtamaz.

  Bu durumlarda, Security Server'ın güncellemeleri edinmesi ve dağıtması için, DeleGate gibi IP adreslerini dönüştürebilen çift yığınlı proxy sunucu gereklidir.

- Internet'e bağlanmak için proxy sunucusu kullanıyorsanız, güncellemeleri başarıyla indirmek için **Tercihler** > **Genel Ayarlar** > **Proxy** sekmesinden doğru proxy ayarlarını ayarlayın.

Bileşen Çiftlemesi

Trend Micro, istemci korumasını güncel tutmak için düzenli olarak kalıp dosyalarını sunar. Kalıp dosyası güncellemeleri düzenli olarak mevcut olduğundan, Security Server, kalıp dosyalarının daha hızlı indirilmesine imkan sağlayan **bileşen çiftleme** adlı bir mekanizmayı kullanmaktadır.

Trend Micro ActiveUpdate server'da tam kalıp dosyasının en son sürümü mevcut olduğunda, artımlı kalıplar da mevcut olacaktır. Artımlı kalıplar, en son ve önceki tam kalıp dosyası sürümleri arasındaki farkları dikkate alan daha küçük tam kalıp dosyası sürümleridir. Örneğin, son sürüm 175 ise, artımlı kalıp v_173.175, sürüm 175 sürüm 173'te olmayan imzaları içerecektir (kalıp numaraları 2'şer arttırıldığı için sürüm 173 önceki tam kalıp sürümüdür). Artımlı kalıp v_171.175, sürüm 171'de bulunmayan sürüm 175 imzalarını içerir.

En son kalıbı indirirken oluşan ağ trafiğini azaltmak için, Security Server, sunucunun sadece artımlı kalıpları indirdiği bir bileşen güncelleme yöntemi olan bileşen çiftlemesi gerçekleştirir. Bileşen çiftlemesinden faydalanmak için, Security Server'ın düzenli olarak

güncellendiğinden emin olun. Aksi takdirde, sunucu tam kalıp dosyasını indirmeye zorlanacaktır.

Bileşen çiftlemesi aşağıdaki bileşenlere uygulanır:

- Virüs Kalıbı
- Smart Scan Agent Pattern
- Hasar Temizleme Şablonu
- IntelliTrap Kural Dışı Durum Kalıbı
- Casus Yazılım Kalıbı

Security Server Güncelleme Kaynağını Yapılandırılma

Başlamadan önce

Security Server, güncellemeleri varsayılan olarak Trend Micro ActiveUpdate sunucusundan elde eder. Security Server ActiveUpdate sunucusuna doğrudan erişemiyorsa, özel bir güncelleme kaynağı belirtin.

- Kaynak **Trend Micro ActiveUpdate Server** ise, Security Server'da internet bağlantısı olduğundan emin olun ve bir proxy sunucusu kullanıyorsanız, proxy ayarlarını kullanarak Internet bağlantısının sağlanabildiğini test edin. Ayrıntılar için, bkz. *Internet Proxy Ayarlarını Yapılandırma sayfa 11-3*.
- Kaynak özel bir güncelleme kaynağıysa (**Mevcut dosyanın bir kopyasını içeren Intranet konumu** veya **Alternatif güncelleme kaynağı**), bu güncelleme kaynağı için uygun ortamı ve güncelleme kaynaklarını kurun. Ayrıca, Security Server ve bu güncelleme kaynağı arasında işlevsel bir bağlantı olduğundan emin olun. Bir güncelleme kaynağını kurma konusunda yardıma ihtiyacınız varsa, destek sağlayıcınıza başvurun.
- Salt bir IPv6 Security Server, Trend Micro ActiveUpdate sunucusu veya salt bir IPv4 özel güncelleme kaynağından doğrudan güncelleme yapamaz. Benzer şekilde, salt bir IPv4 Security Server, doğrudan IPv6 özel güncelleme kaynaklarından güncelleme yapamaz. Security Server'ın güncelleme kaynaklarına bağlantı kurmasına imkan sağlamak için, DeleGate gibi IP adreslerini dönüştürebilen çift yığınlı proxy sunucu gereklidir.

Prosedür

1. **Güncellemeler** > **Kaynak** kısmına gidin.
2. **Sunucu** sekmesinden bir güncelleme kaynağı seçin.
   - **Trend Micro ActiveUpdate Server**
   - **Mevcut dosyanın bir kopyasını içeren İntranet konumu**: Kaynağa `\\Web\ActiveUpdate` gibi Evrensel Adlandırma Gösterimi (UNC) yolunu girin. Ayrıca Security Server'ın bu kaynağa bağlanırken kullanacağı oturum açma yetkilerini (kullanıcı adı ve parola) belirtin.
   - **Alternatif güncelleme kaynağı**: Bu kaynağın URL'sini yazın. Hedef HTTP sanal dizininin (Web paylaşımı) Security Server tarafından kullanılabilir olduğundan emin olun.
3. **Kaydet** öğesine tıklayın.

Security Server'ı Manuel Olarak Güncelleme

Security Server bileşenlerini, sunucuyu yükledikten veya yükselttikten ve bir salgın olduktan sonra manuel olarak güncelleyin.

Prosedür

1. Manuel bir güncellemeyi iki şekilde başlatabilirsiniz:
   - **Güncellemeler** > **Manuel** kısmına gidin.
   - **Canlı Durum**, **Sistem Durumu** > **Bileşen Güncellemeleri** kısmına gidin ve **Şimdi Güncelle** öğesine tıklayın.
2. Güncellenecek bileşenleri seçin.

   Bileşenler hakkında ayrıntılar için, bkz. *Güncellenebilir Bileşenler sayfa 8-3*.
3. **Güncelle** öğesine tıklayın.

Güncelleme durumunu gösteren yeni bir ekran görüntülenir. Güncelleme başarılıysa, Security Server güncellenen bileşenleri otomatik olarak aracılara dağıtır.

Security Server için Planlı Güncellemeleri Yapılandırma

Güncelleme kaynağını düzenli olarak denetlemek ve kullanılabilir tüm güncellemeleri otomatik olarak indirmek için Security Server'ı yapılandırın. Zamanlanmış güncelleme kullanılması tehditlere karşı korumanın her zaman güncel olmasını sağlamanın kolay ve etkin bir yoludur.

Trend Micro, virüs/kötü amaçlı yazılım salgınları sırasında virüs kalıbı dosyalarını güncellemek için hızlı bir şekilde yanıt verir (güncellemeler her hafta bir defadan fazla dağıtılabilir). Tarama motoru ve diğer bileşenler de düzenli olarak güncellenir. Trend Micro, aracının en güncel bileşenlere sahip olmasını sağlamaya yardımcı olmak için bileşenlerinizi günlük olarak, hatta virüs/kötü amaçlı yazılım salgınları sırasında daha sık bir şekilde güncellemenizi önerir.

Önemli

Bir taramayı ve güncellemeyi aynı anda çalışacak şekilde zamanlamaktan kaçının. Bu, Zamanlanmış Tarama'nın beklenmedik şekilde durmasına neden olabilir.

Prosedür

1. **Güncellemeler** > **Zamanlanmış** kısmına gidin.
2. Güncellenecek bileşenleri seçin.

   Bileşenler hakkında ayrıntılar için, bkz. *Güncellenebilir Bileşenler sayfa 8-3*.
3. **Zamanla** sekmesine tıklayın ve güncelleme zamanlamasını belirtin.
   - **Geleneksel tarama güncellemeleri** Smart Scan Kalıbı ve Akıllı Tarama Grubu hariç tüm bileşenleri içerir. Günlük, haftalık ve aylık güncellemeler arasında seçim yapın ve Security Server'ın güncelleme gerçekleştireceği saat sayısı olan **Güncelleme periyodu** için bir değer belirtin. Security Server, bu zaman periyodu içerisinde verilen herhangi bir zamanda güncellenir.

Nota

Aylık zamanlanmış güncellemeler için (önerilmez); 31, 30 veya 29 gün seçerseniz ve bundan daha az güne sahip bir ay olursa, güncelleme o ay çalışmayacaktır.

- **Smart scan güncellemeleri** sadece Smart Scan Kalıbını ve Akıllı Tarama Grubu'nu içerir. Aracılarınızın hiçbiri smart scan kullanmıyorsa, bu öğeyi dikkate almayın.

4. **Kaydet** öğesine tıklayın.

Bileşenleri Geri Alma

Geri alma Virüs Kalıbı, Akıllı Tarama Grubu ve Virüs Tarama Motoru'nun önceki sürümüne geri alma anlamına gelir. Bu bileşenler düzgün işlev görmüyorsa, önceki sürümlerine geri alın. Security Server, Virus Scan Engine için mevcut ve önceki sürümleri, Virüs Kalıbı ve Smart Scan Agent Kalıbı için son üç sürümü saklamaktadır.

Nota

Sadece yukarıda belirtilen bileşenler geri alınabilmektedir.

Worry-Free Business Security 32-bit ve 64-bit platformlarda farklı tarama motorları kullanmaktadır. Bu tarama motorlarını ayrı olarak geri almanız gerekir. Tüm tarama motoru türleri için geri alma prosedürü aynıdır.

Prosedür

1. **Güncellemeler** > **Geri Al** kısmına gidin.
2. Aracılara belirli bir bileşen için kendi bileşen sürümlerini sunucu üzerindeki sürümle senkronize etmelerini bildirmek için **Senkronize et** öğesine tıklayın.
3. Belirli bir bileşen için, hem Security Server, hem de aracılar üzerindeki bileşeni geri almak için **Geri Al** öğesine tıklayın.

Security Agent ve Messaging Security Agent Güncellemeleri

Otomatik Güncellemeler

Security Agent'lar ve Messaging Security Agent'lar (yalnızca Advanced) otomatik olarak aşağıdaki güncellemeleri gerçekleştirecektir:

- Yüklemeden hemen sonra, aracılar Security Server'dan güncellenir.
- Security Server'ın bir güncellemeyi tamamladığı her seferde, güncellemeleri otomatik olarak aracılara iletecektir.
- Güncelleme Aracısının bir güncellemeyi tamamladığı her seferde, güncellemeleri otomatik olarak Security Agent'lara iletir..
- Zamanlanmış güncellemeler, varsayılan olarak şu zamanlarda gerçekleştirilir:
  - Ofis İçi Security Agent'larda her 8 saatte bir
  - Ofis Dışı Security Agent'larda her 2 saatte bir
- Messaging Security Agent'lar, varsayılan olarak her 24 saatte bir 12:00'da zamanlanmış bir güncelleme gerçekleştirir.

Manuel Güncellemeler

Bir güncelleme çok acilse, web konsolundan manuel güncellemeyi çalıştırın. **Canlı Durum**, **Sistem Durumu** > **Bileşen Güncellemeleri** kısmına gidin ve **Şimdi Dağıt** öğesine tıklayın.

Aracı Güncelleme Hatırlatmaları ve İpuçları

- Security Agent'lar, Security Server'dan, Update Agent'lardan veya doğrudan Trend Micro ActiveUpdate server'dan güncellenir.

  Messaging Security Agent, sadece Security Server'dan güncellenir.

Güncelleme işlemi hakkında ayrıntılar için, bkz. *Güncellemeye Genel Bakış sayfa 8-2*.

- Salt bir IPv6 aracısı, güncellemeleri doğrudan bir salt IPv4 Security Server/ Güncelleme Aracısı ve Trend Micro ActiveUpdate sunucusundan elde edemez.

  Benzer şekilde, salt bir IPv4 aracısı güncellemeleri doğrudan salt bir IPv6 Security Server/Güncelleme Aracısından doğrudan elde edemez.

  Bu durumlarda, aracının güncellemeleri elde etmesi için, DeleGate gibi IP adreslerini dönüştürebilen çift yığınlı proxy sunucu gereklidir.

- Aracıların güncellediği bileşenler hakkında ayrıntılar için, bkz. *Güncellenebilir Bileşenler sayfa 8-3*.

- Bu bileşenlere ek olarak, aracılar Security Server'dan güncellenirken de güncellenmiş yapılandırma dosyalarını alır. Aracılar, yeni ayarları uygulamak için yapılandırma dosyalarına ihtiyaç duyar. Web Konsolu aracılığıyla aracı ayarlarını her değiştirdiğinizde, yapılandırma dosyaları değişir.

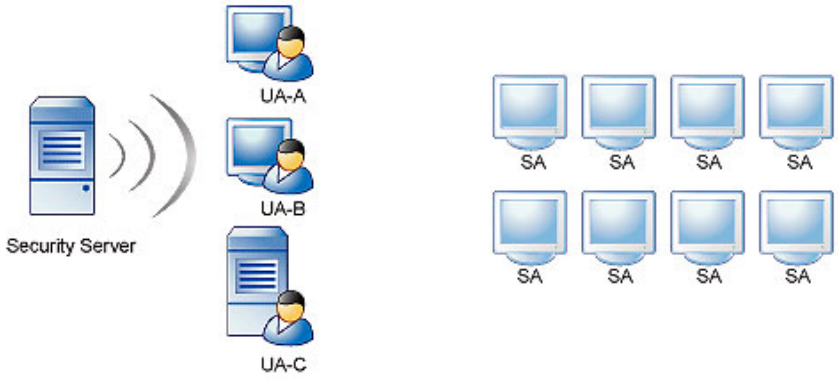
Güncelleme Aracıları

Güncelleme Aracıları, Security Server veya ActiveUpdate Server'dan güncellenmiş bileşenleri alabilen ve bunları diğer Security Agent'lara dağıtan Security Agent'lardır.

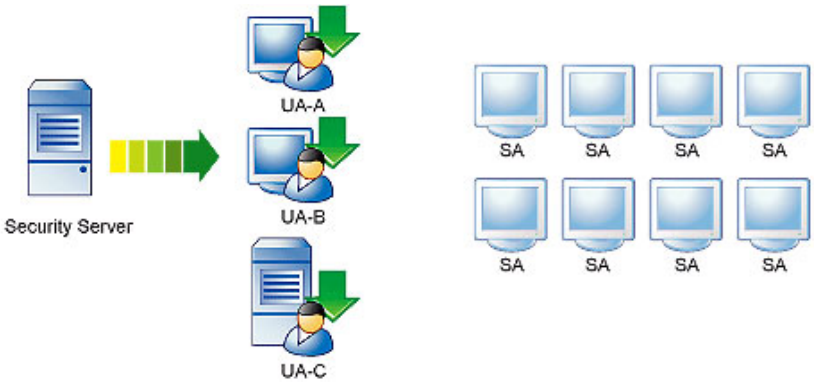
İstemciler ve Trend Micro Security Server arasında ağınızın "düşük bant genişliği" veya "ağır trafik" olarak tanımladığınız kısımları varsa, Security Agent'ları Güncelleme Aracıları olarak belirtebilirsiniz. Güncelleme Aracıları, tüm Security Agent'ların bileşen güncellemeleri için Security Server'a erişmesi gereğini ortadan kaldırarak ağ bant genişliği kullanımını azaltır. Ağınız konuma göre kesimliyse ve kesimler arasındaki ağ bağlantısı sıklıkla ağır trafik yüküyle karşılaşıyorsa, Trend Micro, her kesimde Güncelleme Aracısı görevini üstlenmesi için en az bir Security Agent'a izin vermenizi önerir.

Güncelleme Aracısı güncelleme işlemi aşağıdaki gibi açıklanabilir:

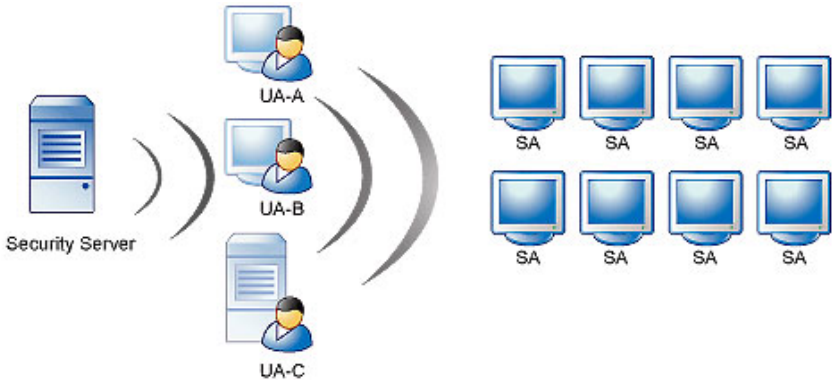
1. Security Server, kullanıma hazır olan yeni güncellemeleri Güncelleme Aracılarına bildirir.



2. Güncelleme Aracıları güncellenen bileşenleri Security Server'dan indirir.



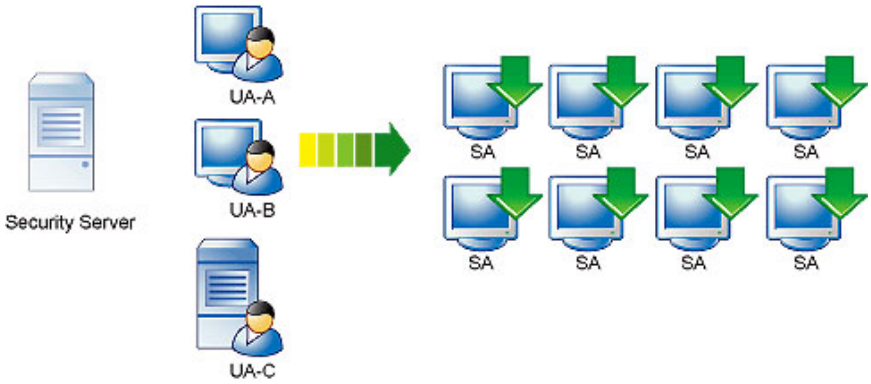
3. Ardından Security Server, güncellenen bileşenler olduğunu Security Agent'lara bildirir.



4. Her Security Agent uygun bir güncelleme kaynağı olup olmadığını belirlemek için Güncelleme Aracısı Sıralama Tablosunun bir kopyasını yükler. Güncelleme Aracısı Sıralama Tablosunda Güncelleme Aracılarının sırası öncelikle, bunların Alternatif Güncelleme Kaynakları olarak web konsoluna eklendikleri sıraya göre belirlenir. Her Security Agent, güncelleme kaynağını tanımlayana kadar ilk girişten başlayarak tablodaki girişlerde bir seferde bir tane olarak ilerler.

Güncelleme Aracısı Sıralama Tablosu	
IP Aralığı	Güncelleme Aracısı
10.1.1.1-10.1.1.10	UA-A
10.2.1.1-10.2.1.10	UA-B
10.3.1.1-10.3.1.10	UA-C

5. Security Agent'lar güncellenen bileşenleri kendi atanan Güncelleme Aracısından indirir. Atanan Güncelleme Aracısı herhangi bir nedenle kullanılamıyorsa, Security Agent güncellenen bileşenleri Security Server'dan indirmeyi dener.



Güncelleme Aracılarını Yapılandırma

Prosedür

1. **Güncellemeler** > **Kaynak** kısmına gidin.
2. **Güncelleme Aracıları** sekmesine tıklayın.
3. Aşağıdaki görevleri gerçekleştirin:

GÖREV	ADIMLAR
Security Agent'ları Güncelleme Aracıları olarak Ata	a. **Güncelleme Aracısı (Aracıları) Ata** bölümünde, **Ekle** öğesine tıklayın. Yeni bir ekran açılır. b. Liste kutusundan, Güncelleme Aracısı görevini üstlenecek bir veya birden fazla aracı seçin. c. **Kaydet** öğesine tıklayın. Ekran kapanır. d. Güncelleme Aracılarının güncellenmiş bileşenleri her zaman başka bir Güncelleme Aracısı yerine Security Server'dan indirmesini istiyorsanız, yine **Güncelleme Aracısı (Aracıları) Ata** bölümünde, **Güncelleme**

GÖREV	ADIMLAR
	Aracılarını her zaman sadece Security Server'dan doğrudan güncelle seçin.
Güncelleme Aracılarını Security Agent'lardan güncelleme için yapılandır	a. **Alternatif Güncelleme Kaynakları** bölümünde, **Security Agent'lar ve Güncelleme Aracıları için alternatif güncelleme kaynaklarını etkinleştir** seçin. **Nota** Bu seçeneğin devre dışı bırakılması, güncelleme kaynağını etkin olarak Security Server'a geri geçirerek Security Agent'ların Güncelleme Aracılarını güncellemesini önler. b. **Ekle** öğesine tıklayın. Yeni bir ekran açılır. c. Güncelleme Aracısından güncellenecek Security Agent'ların IP adreslerini girin. • Bir IPv4 adres aralığı girin. Tek bir Security Agent belirlemek için, Security Agent'ın IP adresini hem **kimden**, hem de **kime** alanlarına girin. • IPv6 için, bir IP öneki ve uzunluğu girin. d. Aşağı açılır listeden bir Güncelleme Aracısı seçin. Aşağı açılır listenin kullanılabilir olmaması, herhangi bir Güncelleme Aracısının yapılandırılmadığı anlamına gelir. e. **Kaydet** öğesine tıklayın. Ekran kapanır. f. Gerektiği şekilde daha fazla IP adresi tanımlayın. Çeşitli IP aralıkları tanımladıysanız, IP aralığı önceliğini ayarlamak için **Yeniden düzenle** seçeneğini kullanabilirsiniz. Security Server, Security Agent'lara güncellemelerin kullanılabilir olduğunu bildirdiğinde, onların doğru güncelleme kaynağını tanımlamak için IP Aralığı listesini tararlar. Security Agent, listedeki ilk öğeyi tarar ve doğru güncelleme kaynağını tanımlayana kadar listede aşağıya doğru devam eder.

GÖREV	ADIMLAR
	İpucu Bir sorun önlemi olarak, aynı IP aralığı için çeşitli Güncelleme Aracıları tanımlayın. Bu, Security Agent'lar bir Güncelleme Aracısından güncellenemiyorsa, diğer Güncelleme Aracılarını deneyecekler anlamına gelmektedir. Bunu yapmak için, aynı IP aralığı ile en az iki (2) girdi oluşturun ve her girdiye farklı bir Güncelleme Aracısı atayın.
Güncelleme Aracılarını Kaldırma	Bir Güncelleme Aracısını kaldırmak ve buna atanmış tüm Security Agent'ların atamasını kaldırmak için, **Güncelleme Aracısı (Aracıları) Ata** bölümüne gidin, Güncelleme Aracısı Bilgisayar Adı'na denk gelen onay kutusunu seçin ve **Kaldır** öğesine tıklayın. Bu eylem, **Alternatif Güncelleme Kaynakları** bölümündeki Security Agent'larının IP adresi aralığını kaldırmayacaktır ve sadece "bağlantısız" kalan Security Agent'ların güncelleme kaynaklarını Security Server olarak değiştirmelerine yol açacaktır. Başka bir Güncelleme Aracınız varsa, bağlantısız Security Agent'lara atayabilirsiniz.
Güncelleme Aracılarından Security Agent'ların Atamasını Kaldır	Bir IP adresi aralığındaki Security Agent'ların artık bir Güncelleme Aracısından güncelleme yapmasını istemiyorsanız, **Alternatif Güncelleme Kaynakları** bölümüne gidin, Security Agent'ların IP adresi aralığındaki ilgili onay kutusunu seçin ve **Kaldır** öğesine tıklayın.

4. **Kaydet** öğesine tıklayın.

Bölüm 9

Bildirimleri Yönetme

Bu bölümde farklı bildirim seçeneklerinin nasıl kullanılacağı açıklanmaktadır.

Bildirimler

Yöneticiler, ağda normal olmayan olaylar olduğunda bildirim alabilir. Worry-Free Business Security e-posta, SNMP veya Windows olay günlükleri kullanarak bildirimler gönderebilir.

Varsayılan olarak **Bildirimler** ekranında listelenen tüm olaylar seçilir ve Security Server'ın sistem Yöneticisi'ne bildirim göndermesini tetikler.

Tehdit Olayları

- **Salgın Savunması**: TrendLabs tarafından bir uyarı bildirildi veya çok kritik güvenlik açıkları algılandı.
- **Antivirüs**: İstemcilerde veya Microsoft Exchange sunucularında (Yalnızca Advanced) algılanan virüs/kötü amaçlı yazılım belirli bir sayıyı aşıyor, virüs/kötü amaçlı yazılıma karşı gerçekleştirilen eylemler başarılı olamadı, Gerçek Zamanlı Tarama istemcilerde veya Microsoft Exchange server'larda devre dışı bırakıldı.
- **Casus Yazılımdan Koruma**: İstemcilerde, casus yazılım/grayware tehdidini tamamen kaldırılması için etkilenen istemcinin yeniden başlatılmasını gerektiren, casus yazılım/grayware algılandı. Casus yazılım/grayware bildirim eşiğini, yani belirlenen bir zaman dönemi (varsayılan olarak bir saat) içindeki casus yazılım/grayware olaylarının sayısını yapılandırabilirsiniz.
- **İstenmeyen E-postadan Koruma** (Yalnızca Advanced): Spam ortaya çıkması, toplam e-posta iletilerinin belirli bir yüzdesini aşıyor.
- **Web Reputation**: URL ihlali sayısı, belirli bir dönemde yapılandırılan sayıyı aşıyor.
- **URL Filtreleme**: URL ihlali sayısı, belirli bir dönemde yapılandırılan sayıyı aşıyor.
- **Davranış İzleme**: İlke ihlali sayısı, belirli bir dönemde yapılandırılan sayıyı aşıyor.
- **Aygıt Denetimi**: Aygıt Denetimi ihlalleri belirli bir sayıyı aştı.
- **Ağ Virüsü**: Algılanan Ağ virüsleri belirli bir sayıyı aşıyor.

Sistem Olayları

- **Smart Scan**: Smart Scan için yapılandırılan istemciler Smart Scan sunucusuna bağlanamıyor veya sunucuya ulaşılamıyor.

- **Bileşen güncelleme**: Bileşenlerin son güncelleme zamanı belirli bir gün sayısını aşıyor veya güncellenen bileşenler Aracılara yeterince hızlı dağıtılmadı.
- **Olağan dışı sistem olayları**: Windows Server işletim sistemi çalıştıran herhangi bir istemcide kalan disk alanı, yapılandırılan miktardan daha düşük; tehlikeli olabilecek düşük düzeylere yaklaşıyor.

Lisans Olayları

- **Lisans**: Ürün lisansının geçerlilik süresi sona ermek üzere veya sona erdi, yer sayısı kullanımı %100'den fazla veya yer sayısı kullanımı %120'den fazla.

Bildirimler için Olayları Yapılandırma

Bildirimleri yapılandırma iki adımdan oluşur. İlk olarak, bildirime gereksiniminiz olan olayları seçin ve daha sonra teslim yöntemlerini yapılandırın.

Worry-Free Business Security, teslim için üç yöntem sunar:

- E-posta bildirimleri
- SNMP bildirimleri
- Windows Olay günlüğü

Prosedür

1. **Tercihler** > **Bildirimler** kısmına gidin.
2. **Olaylar** sekmesinden, aşağıdakileri gerektiği gibi güncelleyin:
   - **E-posta**: Bu olayla ilgili bildirimleri almak için onay kutusunu işaretleyin.
   - **Uyarı Eşiği**: Bu olay için eşiği ve/veya zaman dönemini yapılandırın.
   - **Olay adı**: Bir olay için bildirim içeriğini değiştirmek üzere olay adına tıklayın. İçeriğe simge değişkenleri ekleyebilirsiniz. Ayrıntılar için, bkz. *Sembol Değişkenleri sayfa 9-4*.
3. **Ayarlar** sekmesine tıklayın ve aşağıdakileri gerektiği şekilde güncelleyin:

- **E-Posta Bildirimi**: Gönderen ve alıcıların e-posta adreslerini belirleyin. Alıcılar için, birden fazla e-posta adresini noktalı virgülle (;) ayırın.
- **SNMP Bildirim Alıcısı**: SNMP, ağların yönetiminde kullanılan bilgilerin değişimi için ağ ana makineleri tarafından kullanılan bir protokoldür. Verileri SNMP yakalamadan görüntülemek için Yönetim Bilgi Tabanı tarayıcısı kullanın.
  - **SNMP bildirimlerini etkinleştir**
  - **IP Adresi**: SNMP yakalamanın IP adresi.
  - **Topluluk**: SNMP Topluluğu dizesi.
- **Günlüğe Alma**: Windows Olay günlüğü kullanan bildirimler
- **Windows olay günlüğüne yaz**

4. **Kaydet** öğesine tıklayın.

Sembol Değişkenleri

Olay bildirimlerinin konu satırını ve ileti gövdesini özelleştirmek için sembol değişkenlerini kullanın.

Harici etki alanlarını içeren adreslerden gelen e-postaların spam olarak etiketlenmesini önlemek için, harici e-posta adresini İstenmeyen E-postadan Koruma için Onaylanan Gönderenler listesine ekleyin.

Aşağıdaki simgeler, masaüstü bilgisayarlarda/sunucularda ve Microsoft Exchange sunucularında algılanan tehdit olaylarını temsil eder.

DEĞİŞKEN	AÇIKLAMA
`{$CSM_SERVERNAME}`	Aracıları yöneten Security Server'ın adı
`%CV`	Olayların sayısı
`%CU`	Zaman birimi (dakika, saat)

DEĞİŞKEN	AÇIKLAMA
%CT	%CU sayısı
%CP	Spam olan toplam e-posta iletisinin yüzdesi

Bu bildirimin bir örneği aşağıdadır:

```
Trend Micro, %CT %CU üzerindeki bilgisayarınızda/
bilgisayarlarınızda %CV virüs olayı algıladı. Çok fazla sayıda
veya çok sık görülen virüs olayları beklemede olan bir salgın
durumunu belirtebilir.

Ayrıntılı yönergeler için Security Server'daki Canlı Durum
ekranına bakın.
```

Bölüm 10

Salgın Savunmasını Kullanma

Bu bölümde Worry-Free Business Security Salgın Savunması stratejisi, Salgın Savunması'nın nasıl yapılandırılacağı ve ağların ve istemcilerin korunması için nasıl kullanılacağı anlatılmaktadır.

Salgın Savunması Stratejisi

Salgın Savunması, Worry-Free Business Security çözümünün temel bir bileşenidir ve kurumunuzda bir salgın tediti olması durumunda işletmenizin korunmasını sağlar.

Salgın Savunmasını Yapılandırma

Prosedür

1. **Salgın Savunması**'na gidin.
2. **Salgın Savunması Uygulamasına tabi Aygıtın/ Aygıtların Durumu** bölümünde **Salgın Savunmasını Yapılandır** öğesine tıklayın.
3. Salgın Savunmasını açmak için, **Sarı Uyarılar için Salgın Savunmasını Etkinleştir** öğesini seçin.
4. **Salgın savunması başladığında, istemci kullanıcılarını uyar** seçeneği otomatik olarak seçilir. Kullanıcılara Salgın Savunması bildirimlerini göndermek istemiyorsanız onay kutusundaki işareti kaldırın.
5. Varsaılan olarak, **Salgın Savunmasını Devre Dışı Bırak** 2 gün olarak ayarlıdır. Bu süre 30 güne kadar arttırılabilir.
6. Aşağıdakileri gerektiği gibi güncelleyin:

Seçenek	Açıklama
Paylaşılan klasörlere erişimi kısıtla/ engelle	Salgın Savunması stratejinizin bir parçası olarak paylaşılan ağ klasörlerine erişimi sınırlandırmak veya kısıtlamak için bu seçeneği seçin. Aşağıdakilerden birini seçin: • **Sadece yazma erişimine izin ver** • **Tam erişimi kısıtla**
Bağlantı noktalarını engelleyin	Salgın Savunması stratejinizin bir parçası olarak bağlantı noktalarını engellemek için bu seçeneği seçin. Aşağıdakilerden birini seçin: • **Tüm bağlantı noktaları**

Seçenek	Açıklama
	• **Belirtilen bağlantı noktaları** **Belirtilen bağlantı noktaları** öğesini seçerseniz, **Ekle** öğesine tıklayın ve aşağıdakilerden birini seçin: • **Sık kullanılan bağlantı noktaları**: listeden bağlantı nokta(lar)ı seçin • **Trojan Programları Tarafından Sıklıkla Kullanılan Bağlantı Noktaları**: şu anda Trojan programları tarafından kullanıldığı bilinen 40'dan fazla bağlantı noktası numarası bulunmaktadır. • **1 ve 65535 arasında bir bağlantı noktası numarası veya bağlantı noktası aralığı**: bağlantı noktası veya bağlantı noktası aralığını tanımlayın • **Ping protokolü (ICMP)**
Dosya ve klasörlere yazma erişimini kısıtla	Belirli dosyalara ve klasörlere yazma erişimini reddetmek için bu seçeneği seçin. Aşağıdakilerden seçin: • **Belirli dizinler için korunacak dosyalar**: dizin yolunu girin ve ardından tüm dosyalar veya sadece belirli dosya türleri için yazma erişiminin reddedilip reddedilmeyeceğini belirleyin • **Tüm dizinler için korunacak dosyalar**: korunacak belirli dosyanın (dosyaların) adını girin (dosya uzantısı dahil)
Tüm sıkıştırılmış yürütülebilir dosyalara erişimi reddet	Yürütülebilir sıkıştırılmış dosyalara (paketleyiciler) erişimi reddetmek için bu seçeneği seçin. Desteklenen yürütülebilir paketleyici programları tarafından oluşturulan güvenilen dosyalara erişime izni belirtin.

7. **Kaydet** öğesine tıklayın.

Salgın Savunması Mevcut Durumu

Salgın Savunması durumunu görüntülemek için **Canlı Durum** > **Salgın Savunması** kısmına gidin.

Sarı Uyarı için Salgın Savunması

Sayfanın bu bölümü Salgın Savunması Sarı Uyarıları hakkındaki bilgileri görüntüler.

- **Başlama Zamanı**: Bir Sarı Uyarının yönetici tarafından etkinleştirildiği zaman.
- **Salgın Savunması etkinleştirildi**: Salgın Savunması'nın etkinleştirildiği bilgisayarların sayısı. Salgın Savunması sayfasına gitmek için bağlantılı sayıya tıklayın.
- **Salgın savunması devre dışı bırakıldı**: Salgın Savunması'nın devre dışı bırakıldığı bilgisayarların sayısı. Salgın Savunması sayfasına gitmek için bağlantılı sayıya tıklayın.

Gerekli Eylem

Sayfanın bu bölümü güvenlik açığı olan ve temizleme gerektiren bilgisayarlar hakkındaki bilgileri görüntüler:

- **Güvenlik açığı olan bilgisayarlar**: Güvenlik açığına sahip bilgisayarların sayısı.
- **Temizlenecek bilgisayarlar**: Temizlenmeyi bekleyen bilgisayarların sayısı.

Güvenlik Açığı Değerlendirmesi

Güvenlik Açığı değerlendirmesi sistem yöneticilerine ve diğer ağ güvenlik personeline ağlarındaki güvenlik risklerini değerlendirme olanağı sağlar. Güvenlik Açığı Değerlendirmesi'ni kullanarak elde ettikleri bilgiler, bilinen güvenlik açıklarını nasıl ortadan kaldıracakları ve ağlarının güvenliğini nasıl sağlayacakları konusunda net bir kılavuz sağlar.

Güvenlik Açığı Değerlendirmesi'ni aşağıdaki amaçlarla kullanın:

- Ağınızdaki bilgisayarlarda güvenlik açığı taraması yapın.
- Standart adlandırma kurallarına göre güvenlik açıklarını tanımlama. Güvenlik açığı hakkında daha fazla bilgi ve güvenlik açığı adını tıklatarak nasıl çözüleceğini bulma.
- Güvenlik açıklarını, bilgisayara ve IP adresine göre görüntüler. Sonuçlar, güvenlik açıklarının bilgisayar ve tüm ağ için sergilediği risk düzeyini içerir.
- Güvenlik açıklarını ayrı bilgisayarlara göre görüntüler ve bu bilgisayarların ağın geneli için sergilediği güvenlik risklerini tanımlar.

- Bir ağa bağlı olan bilgisayarların herhangi birini veya tümünü tarayan görevler yapılandırma. Taramalar, bireysel güvenlik açıkları veya bilinen tüm güvenlik açıklarının bir listesi için arama yapabilir.
- Manuel değerlendirme görevleri çalıştırma veya bir zamanlamaya göre çalışacak görevler ayarlama.
- Ağ güvenliği üzerinde kabul edilemeyecek bir risk düzeyi oluşturan bilgisayarlar için engelleme talebinde bulunma.
- Belirli bilgisayarların yarattığı güvenlik açıklarını tanımlayan raporlar oluşturma ve bu bilgisayarların ağ genelinde yarattığı güvenlik risklerini açıklama. Raporlar, Yöneticilerin güvenlik açıklarını ortadan kaldırmak ve ağ güvenliğini sağlamak üzere daha fazla araştırma yapabilmesi için güvenlik açığını standart adlandırma kurallarına göre tanımlar.
- Güvenlik açıklarını ve ağ güvenliğini tehdit eden farklı risk faktörlerini daha iyi anlamak için değerlendirme geçmişlerini görüntüleyin ve raporları karşılaştırın.

Güvenlik Açığı Değerlendirmesini Yapılandırma

Prosedür

1. **Salgın Savunması**'na gidin.
2. **Güvenlik Açığı Olan Bilgisayar(lar)** kısmında, **Zamanlanmış Değerlendirmeleri Yapılandır** öğesini seçin.
3. Zamanlanmış güvenlik açığı değerlendirmelerini açmak için, **Zamanlanmış güvenlik açığı korumasını etkinleştir** öğesini seçin.
4. **Zamanlama** kısmında, güvenlik açığı değerlendirmelerinin sıklığını seçin:
   - **Günlük**
   - **Haftalık**
   - **Aylık**
   - **Başlama Zamanı**

5. **Hedef** kısmında, güvenlik açıkları için değerlendirmek istediğiniz grubu (grupları) seçin:
   - **Tüm gruplar**: Güvenlik Grubu Ağacındaki tüm gruplar
   - **Belirli gruplar**: Güvenlik Grubu Ağacındaki sunucu veya masaüstü grupları
6. **Kaydet** öğesine tıklayın.

Talep Üzerine Güvenlik Açığı Değerlendirmelerinin Çalıştırılması

Prosedür

1. **Salgın Savunması**'na gidin.
2. **Güvenlik Açığı Olan Bilgisayar/Bilgisayarlar** kısmında, **Güvenlik Açıklarını Şimdi Tara** öğesine tıklayın.
3. Güvenlik açığı taramasını çalıştırmak için **Tamam** öğesine tıklayın.

   Güvenlik Açığı Tarama Bildirimi İlerlemesi iletişim kutusu belirir. Tarama tamamlandığında, **Güvenlik Açığı Tarama Bildirim Sonuçları** iletişim kutusu belirir.
4. **Güvenlik Açığı Tarama Bildirim Sonuçları** iletişim kutusunda tarama sonuçlarını gözden geçirin, ardından **Kapat** öğesine tıklayın.

Hasar Temizleme

Security Agent'lar, istemcileri Truva atı programlarına (veya Truva atları) karşı korumak için Hasar Temizleme Hizmetlerini kullanır. Truva atları veya diğer kötü amaçlı yazılımlardan kaynaklanan tehditleri göstermek için Hasar Temizleme Hizmetleri şunları yapar:

- Truva atlarını ve diğer kötü amaçlı yazılım uygulamalarını algılar ve kaldırır

- Truva atlarının ve diğer kötü amaçlı yazılım uygulamalarının oluşturduğu işlemleri sonlandırır
- Truva atlarının ve diğer kötü amaçlı yazılımın değiştirdiği sistem dosyalarını onarır
- Truva atlarının ve diğer kötü amaçlı yazılımın oluşturduğu dosyaları ve uygulamaları siler

Hasar Temizleme Hizmetleri, bu görevleri gerçekleştirmek için aşağıdaki bileşenleri kullanır:

- **Hasar Temizleme Motoru**: Hasar Temizleme Hizmetleri, Truva atlarını ve Truva atı işlemlerini, solucanları ve casus yazılımı taramak ve kaldırmak için kullanılır.
- **Virüs Temizleme Kalıbı**: Hasar Temizleme Motoru tarafından kullanılır. Bu şablon, Truva atlarını ve Truva atı işlemlerini, solucanları ve casus yazılımı tanımlamaya yardımcı olur, bu sayede Hasar Temizleme Motoru bunları ortadan kaldırabilir.

Talep Üzerine Temizlemenin Çalıştırılması

Prosedür

1. **Salgın Savunması**'na gidin.
2. **Temizlenecek Bilgisayar/Bilgisayarlar** kısmında, **Hemen Temizle** öğesine tıklayın.

   Başarısız temizleme sonuçları, Security Agent çevrimdışı olduğunda veya ağ kesintileri gibi beklenmeyen durumlarda ortaya çıkar.
3. Temizlemeyi başlatmak için **Tamam** öğesine tıklayın.

   Temizleme Bildirim İlerlemesi iletişim kutusu belirir. Temizleme tamamlandığında, **Temizleme Bildirim Sonuçları** iletişim kutusu belirir.
4. **Güvenlik Açığı Tarama Bildirim Sonuçları** iletişim kutusunda temizleme sonuçlarını gözden geçirin, ardından **Kapat** öğesine tıklayın.

Bölüm 11

Genel Ayarları Yönetme

Bu bölüm, aracılar için global ayarları ve Security Server için sistem ayarlarını açıklamaktadır.

Genel Ayarlar

Web konsolundan, Security Server ve Security Agent'lar için genel ayarları yapılandırabilirsiniz.

Proxy

Ağ, Internet'e bağlanmak için bir proxy sunucu kullanıyorsa, aşağıdaki hizmetler için proxy sunucu ayarlarını belirtin:

- Bileşen güncellemeleri ve lisans bildirimleri
- Web Reputation, Behavior Monitoring ve Smart Scan

Ayrıntılar için, bkz. *Internet Proxy Ayarlarını Yapılandırma sayfa 11-3*.

SMTP

SMTP Sunucu ayarları, Worry-Free Business Security tarafından oluşturulan tüm bildirimler ve raporlar için geçerlidir.

Ayrıntılar için, bkz. *SMTP Sunucusu Ayarlarını Yapılandırma sayfa 11-4*.

Masaüstü Bilgisayar/Sunucu

Masaüstü Bilgisayar/Sunucu seçenekleri, Worry-Free Business Security genel ayarlarına ilişkindir.

Ayrıntılar için, bkz. *Masaüstü/Sunucu Ayarlarını Yapılandırma sayfa 11-5*.

Sistem

Genel Ayarlar ekranının Sistem bölümü, etkin olmayan aracıları otomatik olarak kaldırmak, aracıların bağlantısını denetlemek ve karantina klasörünü korumak için seçenekler içerir.

Ayrıntılar için, bkz. *Sistem Ayarlarını Yapılandırma sayfa 11-10*.

Internet Proxy Ayarlarını Yapılandırma

Security Server ve aracıları internete bağlanmak için bir proxy server kullanıyorsa, aşağıdaki özelliklerden ve Trend Micro hizmetlerden faydalanmak için proxy server ayarlarını belirtin:

- **Security Server**: Bileşen güncellemeleri ve lisans bakımı
- **Güvenlik Aracıları**: Web Reputation, URL Filtreleme, Behavior Monitoring, Smart Feedback ve Smart Scan
- **Messaging Security Agents'lar** (yalnızca Advanced): Web Reputation ve Anti-spam

---

Prosedür

1. **Tercihler** > **Global Ayarlar** kısmına gidin.
2. **Proxy** sekmesinden, aşağıdakileri gerektiği gibi güncelleyin:
   - Security Server Proxy

     Nota

     Messaging Security Agent'lar ayrıca Security Server proxy ayarlarını kullanır.

     - Güncellemeler ve lisans bildirimleri için bir proxy server kullan
     - SOCKS 4/5 proxy protokolünü kullan
     - Adres: IPv4/IPv6 adresi veya ana makine adı
     - Bağlantı Noktası
     - Proxy server kimlik doğrulama
       - Kullanıcı adı
       - Parola
   - Security Agent Proxy

- Güncellenen proxy için belirtilen kimlik bilgilerini kullanın

Nota

Security Agent'lar internete bağlanmak için Internet Explorer proxy sunucusunu ve bağlantı noktasını kullanır. Bu seçeneği sadece istemciler ve Security Server üzerindeki Internet Explorer aynı kimlik doğrulama yeterliliklerini paylaşıyorsa seçin.

- Kullanıcı adı
- Parola

3. **Kaydet** öğesine tıklayın.

SMTP Sunucusu Ayarlarını Yapılandırma

SMTP Sunucu ayarları, Worry-Free Business Security tarafından oluşturulan tüm bildirimler ve raporlar için geçerlidir.

Prosedür

1. **Tercihler** > **Global Ayarlar** kısmına gidin.
2. **SMTP** sekmesine tıklayın ve aşağıdakileri gerektiği şekilde güncelleyin:
   - **SMTP sunucusu**: SMTP sunucusunun IPv4 adresi veya adı.
   - **Bağlantı Noktası**
   - **SMTP Server Kimlik Doğrulamasını etkinleştir**
     - Kullanıcı Adı
     - Parola
3. Ayarların doğru olduğunu doğrulamak için, **Test E-postası Gönder** öğesine tıklayın. Gönderme başarısız olursa, ayarları değiştirin ve SMTP sunucunun durumunu kontrol edin.

4. **Kaydet** öğesine tıklayın.

Masaüstü/Sunucu Ayarlarını Yapılandırma

Masaüstü Bilgisayar/Sunucu seçenekleri, Worry-Free Business Security genel ayarlarına ilişkindir. Ayrı gruplara ilişkin ayarlar bu ayarları geçersiz kılar. Bir grup için belirli bir seçeneği yapılandırmadıysanız, Masaüstü/Sunucu Seçenekleri kullanılır. Örneğin, belirli bir grup için onaylanmış URL yoksa, bu ekranda onaylanan URL'lerin tümü grup için geçerli olacaktır.

Prosedür

1. **Tercihler** > **Global Ayarlar** kısmına gidin.
2. **Masaüstü/Sunucu** sekmesine tıklayın ve aşağıdakileri gerektiği şekilde güncelleyin:

Ayarlar	Açıklama
Konum Tanıma	Yöneticiler, Konum Tanıma sayesinde istemcinin ağa nasıl bağlı olduğuna dayalı olarak güvenlik ayarlarını kontrol edebilir. Konum Tanıma, Ofis İçi/Ofis Dışı bağlantı ayarlarını denetler. Security Agent, web konsolunda yapılandırılan ağ geçidi bilgilerine dayalı olarak istemcinin konumunu otomatik olarak tanımlar ve kullanıcıların erişebildiği web sitelerini kontrol eder. Kısıtlamalar kullanıcının konumuna göre farklılık gösterir: • **Konum tanımayı etkinleştir**: Bu ayarlar, Güvenlik Duvarı, Web Reputation ve zamanlanmış güncelleme sıklığı için Ofis İçi/Ofis Dışı bağlantı ayarlarını etkiler. • **Ağ Geçidi Bilgileri**: Bu listedeki istemciler ve bağlantılar, ağa uzaktan bağlanırken (VPN kullanarak) ve Konum Tanıma etkinken Dahili Bağlantı ayarlarını kullanacaktır. • Ağ geçidi IP adresi

AYARLAR	AÇIKLAMA
	• MAC adresi: MAC adresinin eklenmesi, yalnızca yapılandırılan aygıtın bağlanmasına izin vererek güvenliği büyük ölçüde pekiştirir. Bir girişi silmek için ilgili çöp kutusu simgesini tıklatın.
Yardım Masası Uyarısı	Yardım Masası Uyarısı, Security Agent'a bildirim yerleştirerek kullanıcıyı yardım için kiminle iletişim kuracağı konusunda bilgilendirir. Aşağıdakileri gerektiği gibi güncelleyin: • **Yardım Masası Etiketi** • **Yardım Masası E-posta Adresi** • **Ek Bilgi**: Kullanıcı, fareyi etiketin üzerine getirdiğinde bu bilgi açılır
Genel Tarama Ayarları	• **Smart Scan servisini Devre Dışı Bırak**: Tüm Security Agent'ları Geleneksel Tarama moduna geçirir. Smart Scan yeniden buradan etkinleştirilinceye kadar kullanılamaz. Bir veya daha çok Security Agent grubunda geçiş yapmak için, **Güvenlik Ayarları** > **{Grup}** > **Yapılandır** > **Tarama Yöntemi** kısmına gidin. **Nota** Security Agent'ları tarama yöntemleri arasında geçirmek hakkında yönergeler için, bkz. *Tarama Yöntemlerini Yapılandırma sayfa 5-5*. • **Dosya işlemleri üzerindeki ertelenmiş taramayı etkinleştir**: Bu ayarı, sistem performansını geçici olarak iyileştirmek için etkinleştirin. **UYARI!** Ertelenmiş taramayı etkinleştirmek güvenlik riskleri oluşturabilir. • **Gölge kopya bölümünü dışlayın**: Gölge Kopyası veya Birim Anlık Görüntü Hizmetleri, belirli bir birimdeki bir dosyanın veya klasörün manuel ya da otomatik yedek kopyalarını veya anlık görüntülerini alır.

Ayarlar	Açıklama
	• **Security Server veritabanı klasörünü hariç tut**: Bu Security Server'da yüklü Aracıların yalnızca Gerçek Zamanlı Taramalar sırasında kendi veritabanını taramasını önler. Varsayılan olarak, WFBS kendi veritabanını taramaz. Trend Micro, tarama sırasında veritabanının bozulmasını önlemek amacıyla bu seçimi korumayı önerir. • **Microsoft Exchange sunucusuna yüklendiği zaman Microsoft Exchange Sunucu klasörlerini dışla**: Microsoft Exchange sunucusunda yüklü Aracıların Microsoft Exchange klasörlerini taramasını engeller. • **Microsoft Etki alanı denetleyicisi klasörlerini dışlayın**: Etki Alanı Denetleyicisi'nde yüklü Aracıların Etki Alanı Denetleyicisi klasörlerini taramasını engeller. Bu klasörlerde kullanıcı bilgileri, kullanıcı adları, parolalar ve diğer önemli bilgiler depolanır.
Virüs Taraması Ayarları	• **Büyük sıkıştırılmış dosyalar için tarama ayarlarını yapılandırın**: Ayıklanan dosyanın maksimum boyutunu ve Aracının taraması gereken sıkıştırılmış dosyadaki dosya sayısını belirtin. • **Sıkıştırılmış dosyaları temizleyin**: Aracılar, sıkıştırılmış bir dosya içindeki etkilenmiş dosyaları temizlemeye çalışır. • **En fazla { } OLE katmanı tara**: Aracılar, belirtilen sayıda Nesne Bağlama ve Katıştırma (OLE) katmanını tarar. OLE, kullanıcıların bir uygulamayla nesne oluşturmasına ve ardından bu nesneleri ikinci bir uygulamaya bağlamasına veya katıştırmasına olanak sağlar. Örneğin, .doc dosyasına katıştırılmış bir .xls dosyası. • **İstemciler üzerindeki Windows kısayol menüsüne Manuel Taramayı ekleyin**: Bu, bağlama duyarlı menüye **Security Agent ile Tara** bağlantısı ekler. Kullanıcılar bu bağlantıyla bir dosyayı veya klasörü sağ tıklatabilir (Masaüstünde veya Windows Explorer'da) ve dosyayı veya klasörü manuel olarak tarayabilir.

AYARLAR	AÇIKLAMA
Casus Yazılım/ Grayware Tarama Ayarları	• **Tanımlama bilgileri için tarama yap**: Security Agent çerezleri taramaktadır. • **Casus yazılım günlüğüne tanımlama bilgisi algılamaları ekle**: Tespit edilen her casus yazılım tanımlama bilgisini casus yazılım günlüğüne ekler.
Güvenlik Duvarı Ayarları	WFBS istemci güvenlik duvarını ve güvenlik duvarıyla ilgili sürücüleri kaldırmak için **Güvenlik Duvarını devre dışı bırak ve sürücüleri kaldır** onay kutusunu işaretleyin. **Nota** Güvenlik duvarını devre dışı bırakırsanız, bununla ilgili ayarlar güvenlik duvarını yeniden etkinleştirene kadar kullanılamaz.
Web Reputation ve URL Filtreleme	• **Onaylanan Listesi**: Web siteleri (ve onların alt etki alanları), Web Reputation ve URL Filtreleme doğrulamalarının dışında bırakılır. **Nota** Onaylanan listesi, engellenen listesinden önceliklidir. Bir URL onaylanan listesindeki girdiyle eşleniyorsa, aracılar engellenen öğeler listesinde olsa dahi URL'ye erişime daima izin verir. Belirli bir grup için İzin Verilen veya Engellenen listelerinin etkinleştirilmesi Global İzin Verilen veya Engellenen ayarları yok sayar. • **Engellenen Öğe Listesi**: URL Filtreleme sırasında daima engellenen Web siteleri (ve onların alt etki alanları). • **İşlem İstisna Listesi**: Web Reputation ve URL Filtreleme doğrulamalarından dışlanan işlemler. Kuruluşunuzun güvenli olarak kabul ettiği kritik işlemleri girin.

AYARLAR	AÇIKLAMA
	İpucu İşlem dışlama listesini güncellediğinizde ve sunucu güncellenmiş listeyi aracılara dağıttığında, istemci bilgisayar üzerindeki aktif tüm HTTP bağlantıları (80, 81 veya 8080 bağlantı noktası üzerinden) birkaç saniye için kesilecektir. İşlem dışlama listesini yoğun olmayan saatlerde güncellemeyi dikkate alın • **IP Kural Dışı Durum Listesi**: Bu IP adresleri (örn: 192.168.0.1) , Web Reputation ve URL Filtreleme doğrulamalarının dışında bırakılır. Kuruluşunuzun güvenilir bulduğu önemli IP adreslerini yazın. • **Web Reputation ve URL Filtreleme günlüklerini Security Server'a gönder**
Uyarı Ayarları	**Virüs kalıbı dosyası {} gün sonra güncellenmediyse Windows görev çubuğundaki uyarı simgesini gösterin**: Belirli sayıda gün sonunda kalıp dosyası güncellenmediyse istemciler üzerinde bir uyarı simgesi görüntüler.
Security Agent Kaldırma Parolası	• **İstemci kullanıcısının Security Agent'ı parolasız kaldırmasına izin ver.** • **İstemci kullanıcısının Security Agent'ı kaldırması için parola iste.**
Security Agent Program Çıkış ve Kilit Açma Parolası	• **İstemci kullanıcılarının parola olmadan bilgisayarlarındaki Security Agent'tan çıkmasına ve kilidi açmasına izin verir.** • **İstemci kullanıcılarının Security Agent'tan çıkmak ve kilidi açmak için parola girmesini gerektirir.** **Nota** Security Agent'ın kilidinin açılması, kullanıcının **Güvenlik Ayarları** > **{grup}** > **Yapılandır** > **İstemci Ayrıcalıkları** altında yapılandırılan tüm ayarları geçersiz kılmasına izin verir.

AYARLAR	AÇIKLAMA
Tercih Edilen IP Adresi	Bu ayar sadece çift yığınlı Security Server'lar üzerinde kullanılabilir ve sadece çift yığınlı aracılar tarafından uygulanır. Aracıları yükledikten veya güncelledikten sonra, aracılar bir IP adresi kullanarak Security Server'a kaydolur. Aşağıdaki seçeneklerden birini seçin: • **Önce IPv4, ardından IPv6**: Aracılar önce IPv4 adreslerini kullanır. Aracı IPv4 adresini kullanarak kaydolamıyorsa, IPv6 adresini kullanır. Her iki IP adresini kullanarak da kayıt başarısız olursa, aracı bu seçim için IP adresi önceliğini kullanmayı tekrar dener. • **önce IPv6, ardından IPv4**: Aracılar önce IPv6 adreslerini kullanır. Aracı IPv6 adresini kullanarak kaydolamıyorsa, IPv4 adresini kullanır. Her iki IP adresini kullanarak da kayıt başarısız olursa, aracı bu seçim için IP adresi önceliğini kullanmayı tekrar dener.

3. **Kaydet** öğesine tıklayın.

Sistem Ayarlarını Yapılandırma

Genel Ayarlar ekranının **Sistem** bölümü, etkin olmayan aracıları otomatik olarak kaldırmak, aracıların bağlantısını denetlemek ve karantina klasörünü korumak için seçenekler içerir.

Prosedür

1. **Tercihler** > **Global Ayarlar** kısmına gidin.
2. **Sistem** sekmesine tıklayın ve aşağıdakileri gerektiği şekilde güncelleyin:

Ayarlar	Açıklama
Etkin Olmayan Security Agent'ın Kaldırılması	Aracıları bir istemciden kaldırmak için istemcide Security Agent kaldırma programını kullandığınızda, program, Security Server'ı otomatik olarak bilgilendirir. Security Server bu bildirimi aldığında, istemcinin artık var olmadığını göstermek için istemci simgesini Güvenlik Grupları Ağacı'ndan kaldırır. Ancak Security Agent, bilgisayarın sabit diskini yeniden biçimlendirme veya istemci dosyalarını manuel olarak silme gibi başka yöntemler kullanılarak kaldırılırsa, Security Server bu kaldırma işleminden habersiz olacak ve Security Agent'ın etkin olmadığını gösterecektir. Bir kullanıcı aracıyı bellekten kaldırır veya uzun süreliğine devre dışı bırakırsa, Security Server, Security Agent'ın da etkin olmadığını gösterir. Güvenlik Grupları Ağacının yalnızca etkin istemcileri görüntülemesini sağlamak için, Security Server'ı etkin olmayan Security Agent'ı Güvenlik Grupları Ağacından otomatik olarak kaldıracak şekilde yapılandırabilirsiniz. • **Etkin olmayan Security Agent'ın otomatik olarak kaldırılmasını etkinleştir**: Belirtilen süre içinde Security Server ile bağlantı kurmayan istemcilerin otomatik olarak kaldırılmasını etkinleştirir. • **{} gün boyunca etkin değilse, Security Agent'ı otomatik olarak kaldır**: Bir istemcinin kaç gün boyunca etkin olmadığında web konsolundan kaldırılacağını belirtir.

Ayarlar	Açıklama

Aracı Bağlantısını Doğrulama	WFBS simgeler kullanarak Güvenlik Grupları Ağacı'nda istemci bağlantı durumunu gösterir. Ancak bazı durumlar Güvenlik Grupları Ağacı'nın doğru aracı bağlantı durumunu görüntülemesini engelleyebilir. Örneğin, bir aracının ağ kablosunun bağlantısı yanlışlıkla kesildiyse, aracının, o sırada çevrimdışı olduğunu Trend Micro Security Server'a bildiremez. Bu aracı, Güvenlik Grupları Ağacı'nda çevrimiçi görünmeye devam eder.
	
	Aracı-sunucu bağlantısını manuel olarak doğrulayabilir veya doğrulamayı web konsolundan zamanlayabilirsiniz.
	
	Nota
	Bağlantı Doğrulama, belirli grupların veya aracıların seçilmesine izin vermez. Security Server'a kayıtlı tüm aracılar için bağlantıyı doğrular.
	
	• **Zamanlanmış doğrulamayı etkinleştir**: Aracı-sunucu bağlantısının zamanlanmış doğrulamasını etkinleştirir.
	  • **Saatlik**
	  • **Günlük**
	  • **Haftalık, sıklık**
	  • **Başlangıç saati**: Doğrulamanın başlaması gereken saat.
	• **Şimdi Doğrula**: Bağlantıyı anında test eder.

AYARLAR	AÇIKLAMA
Karantina Bakımı	Varsayılan olarak, Security Agent'lar karantinaya alınmış etkilenmiş dosyaları Security Server'daki aşağıdaki dizine gönderir: <Security Server yükleme klasörü>\PCCSRV\Virus Dizini değiştirmeniz gerekiyorsa (örneğin yetersiz disk alanı varsa), **Karantina Dizini** alanında D:\Quarantined Files gibi mutlak bir yol girin. Bunu yaparsanız, **Güvenlik Ayarları** > **{Grup}** > **Yapılandır** > **Karantina** kısmında aynı değişiklikleri uyguladığınızdan emin olun, yoksa aracılar dosyaları <Security Server yükleme klasörü>\PCCSRV\Virus adresine göndermeye devam eder. Ek olarak, aşağıdaki bakım ayarlarını yapılandırın: • **Karantina klasörü kapasitesi**: Karantina klasörünün MB olarak boyutu. • **Tek bir dosya için maksimum boyut**: Karantina klasöründe depolanan tek bir dosyanın MB olarak maksimum boyutu. • **Karantina Altına Alınan Tüm Dosyaları Sil**: Karantina klasöründeki tüm dosyaları siler. Klasör doluyken yeni bir dosya yüklenirse, yeni dosya depolanmaz. Aracıların karantinaya alınmış dosyaları Security Server'a göndermesini istemiyorsanız, yeni dizini **Güvenlik Ayarları** > **Yapılandır** > **Karantina** kısmında yapılandırın ve tüm bakım ayarlarını yok sayın. Talimatlar için bkz. *Karantina Dizini sayfa 5-30*.

AYARLAR	AÇIKLAMA
Security Agent Yüklemesi	**Security Agent Yükleme dizini**: Yükleme sırasında, Kurulum'un her Security Agent'ı yüklediği Security Agent yükleme dizinini girmeniz istenir, Gerekirse, mutlak bir yol girerek dizini değiştirin. Sadece ilerideki aracılar bu dizine yüklenecektir; mevcut aracılar güncel dizini muhafaza eder. Yükleme yolunu ayarlamak için aşağıdaki değişkenlerden birini kullanın: • `$BOOTDISK`: Önyükleme diskinin sürücü harfi • `$WINDIR`: Windows'un yüklü olduğu klasör • `$ProgramFiles`: Programlar klasörü

3. **Kaydet** öğesine tıklayın.

Bölüm 12

Günlükleri ve Raporları Kullanma

Bu bölümde sisteminizi izlemek ve korumanızı analiz etmek için günlüklerin ve raporların nasıl kullanılacağı açıklanmaktadır.

Günlükler

Worry-Free Business Security, virüs/kötü amaçlı yazılım ve casus yazılım/grayware olguları, olaylar ve güncellemeler hakkında kapsamlı günlükler tutar. Kuruluşunuzun koruma ilkelerini değerlendirmek, yüksek etkilenme riski taşıyan istemcilerini tanımlamak ve güncellemelerin başarıyla dağıtıldığını doğrulamak için bu günlükleri kullanın.

Nota

CSV günlük dosyalarını görüntülemek için Microsoft Excel gibi elektronik tablo uygulamalarını kullanın.

WFBS aşağıdaki kategoriler altında günlüklerin bakımını yapar:

- Web Konsolu olay günlükleri
- Masaüstü/Sunucu günlükleri
- Microsoft Exchange server günlükleri (Yalnızca Advanced)

TABLO 12-1. Günlük Türü ve İçerik

TÜR (GÜNLÜK GİRİŞİNİ OLUŞTURAN VARLIK)	İÇERİK (İÇERİK KAYNAĞINI ELDE ETMEK İÇİN GÜNLÜK TÜRÜ)
Yönetim konsolu olayları	• Manuel Tarama (web konsolundan çalıştırılır) • Güncelleme (Security Server Güncellemeleri) • Salgın Savunması olayları • Konsol olayları

TÜR (GÜNLÜK GİRİŞİNİ OLUŞTURAN VARLIK)	İÇERİK (İÇERİK KAYNAĞINI ELDE ETMEK İÇİN GÜNLÜK TÜRÜ)

Masaüstü Bilgisayar/ Sunucu	• Virüs günlükleri
	  • Manuel Tarama
	  • Gerçek Zamanlı Tarama
	  • Zamanlanmış Tarama
	  • Temizleme
	• Casus Yazılım/Grayware günlükleri
	  • Manuel Tarama
	  • Gerçek Zamanlı Tarama
	  • Zamanlanmış Tarama
	• Web Reputation günlükleri
	• URL Filtreleme günlükleri
	• Behavior monitoring günlükleri
	• Güncelleme günlükleri
	• Ağ virüsü günlükleri
	• Salgın Savunması günlükleri
	• Olay günlükleri
	• Aygıt Denetim günlükleri
	• Düzeltme Dağıtımı günlükleri

TÜR (GÜNLÜK GİRİŞİNİ OLUŞTURAN VARLIK)	İÇERİK (İÇERİK KAYNAĞINI ELDE ETMEK İÇİN GÜNLÜK TÜRÜ)
Exchange server (Yalnızca Advanced)	• Virüs günlükleri • Ek Engelleme günlükleri • İçerik Filtreleme/Veri Kaybını Önleme günlükleri • Güncelleme günlükleri • Yedekleme günlükleri • Arşiv günlükleri • Salgın Savunması günlükleri • Tarama Olayı günlükleri • Taranamayan İleti Bölümleri günlükleri • Web Reputation günlükleri • Mobil Olay günlükleri

Günlük Sorgusu Kullanma

Günlük veritabanından bilgileri toplamak için günlük sorgularını gerçekleştirir. Sorgularınızı ayarlamak ve çalıştırmak için **Günlük Sorgusu** ekranını kullanabilirsiniz. Sonuçlar .CSV dosyası biçiminde dışa aktarılabilir veya yazdırılabilir.

Messaging Security Agent (yalnızca Advanced) günlüklerini her beş dakikada bir Security Server'a gönderir (günlüğün oluşturulma zamanından bağımsız).

Prosedür

1. **Raporlar** > **Günlük Sorgusu** kısmına gidin.
2. Aşağıdaki seçenekleri gerektiği gibi güncelleyin:
   - **Zaman Aralığı**
     - **Önyapılandırılan aralık**

- **Belirtilen aralık**: Sorguyu belirli tarihlerle sınırlamak için.

- **Tür**: Her bir günlük türünün içeriğini görüntülemek için, bkz. *Günlükler sayfa 12-2*.
  - **Yönetim konsolu olayları**
  - **Masaüstü Bilgisayar/Sunucu**
  - **Exchange server** (yalnızca Advanced)
- **İçerik**: Kullanılabilecek seçenekler günlük **Tür**'üne bağlıdır.

3. **Günlükleri Görüntüle** öğesine tıklayın.
4. Günlüğü virgülle ayrılan değer (CSV) veri dosyası olarak kaydetmek için **Dışa Aktar** öğesine tıklayın. CSV dosyalarını görüntülemek için elektronik tablo uygulamasını kullanın.

Raporlar

Tek seferlik raporları manuel olarak oluşturabilir veya Security Server'ın zamanlanmış raporlar oluşturmasını ayarlayabilirsiniz.

Raporları yazdırabilir veya e-posta ile bir yöneticiye veya diğer kişilere gönderebilirsiniz.

Bir raporda mevcut olan veri, raporun oluşturulduğu zaman Security Server üzerinde yer alan günlüklerin miktarından etkilenir. Yeni günlükler eklendikçe ve eskileri silindikçe, günlüklerin miktarı değişir. **Raporlar** > **Bakım** kısmından, günlükleri manuel olarak silebilir veya bir günlük silme programı oluşturabilirsiniz.

Tek Seferlik Raporlarla Çalışma

Prosedür

1. **Raporlar** > **Tek Seferlik Raporlar** kısmına gidin.
2. Aşağıdaki görevleri gerçekleştirin:

GÖREV	ADIMLAR
Bir rapor oluştur	a. **Ekle** öğesine tıklayın. Yeni bir ekran belirir. b. Aşağıdakileri yapılandırın: • **Rapor adı** • **Zaman Aralığı**: Raporu belirli tarihlerle sınırlar. • **İçerik**: Tüm tehditleri seçmek için, **Tümünü Seç** onay kutusunu seçin. Ayrı tehditleri seçmek için, ilişkili onay kutusuna tıklayın. Seçimi genişletmek için artı (+) simgesine tıklayın. • **Rapor gönder** • **Alıcı**: Noktalı virgülle (;) ayırarak alıcıların e-posta adreslerini girin. • **Biçimlendir**: PDF veya bir HTML rapor bağlantısı seçin. PDF seçerseniz, PDF e-postaya eklenecektir. c. **Ekle** öğesine tıklayın.
Raporu görüntüle	Rapor Adı sütununun altından rapora olan bağlantılara tıklayın. Birinci bağlantı bir PDF rapor açarken, ikinci bağlantı bir HTML rapor açar. Bir raporda mevcut olan veri, raporun oluşturulduğu zaman Security Server üzerinde yer alan günlüklerin miktarından etkilenir. Yeni günlükler eklendikçe ve eskileri silindikçe, günlüklerin miktarı değişir. **Raporlar** > **Bakım** kısmından, günlükleri manuel olarak silebilir veya bir günlük silme zamanlaması oluşturabilirsiniz. Raporun içeriği hakkında ayrıntılar için, bkz. *Raporları Yorumlama sayfa 12-11*.

GÖREV	ADIMLAR
Raporları sil	a. Rapor bağlantılarını içeren satırı seçin. b. **Sil** öğesine tıklayın. **Nota** Raporları otomatik olarka silmek için, **Raporlar** > **Bakım** > **Raporlar** sekmesine gidin ve WFBS tarafından tutulan tek seferlik raporların maksimum sayısını ayarlayın. Varsayılanı, 10 adet tek seferlik rapordur. Bu sayı aşıldığında, Security Server en uzun süre tutulan rapordan başlayarak raporları siler.

Zamanlanmış Raporlarla Çalışma

Prosedür

1. **Raporlar** > **Zamanlanmış Raporlar** kısmına gidin.
2. Aşağıdaki görevleri gerçekleştirin:

GÖREV	ADIMLAR
Zamanlanmış bir rapor şablonu oluşturun	a. **Ekle** öğesine tıklayın. Yeni bir ekran belirir. b. Aşağıdakileri yapılandırın: • **Rapor şablonu adı** • **Zamanla**: Günlük, haftalık veya aylık ve raporu oluşturma zamanı. Aylık raporlar için; 31, 30 veya 29 gün seçerseniz ve bundan daha az güne sahip bir ay olursa, WFBS o ay bir rapor oluşturmayacaktır. • **İçerik**: Tüm tehditleri seçmek için, **Tümünü Seç** onay kutusunu seçin. Ayrı tehditleri seçmek için, ilişkili onay kutusuna tıklayın. Seçimi genişletmek için artı (+) simgesine tıklayın. • **Rapor gönder** • **Alıcı**: Noktalı virgülle (;) ayırarak alıcıların e-posta adreslerini girin. • **Biçimlendir**: PDF veya bir HTML rapor bağlantısı seçin. PDF seçerseniz, PDF e-postaya eklenecektir. c. **Ekle** öğesine tıklayın.

Görev	Adımlar
Zamanlanmış raporları görüntüle	a. Zamanlanmış raporların oluşturulduğu şablonu içeren satırda, **Rapor Geçmişi** öğesine tıklayın. Yeni bir ekran açılır. b. Görünüm sütununun altından rapora olan bağlantılara tıklayın. Birinci bağlantı bir PDF rapor açarken, ikinci bağlantı bir HTML rapor açar. Bir raporda mevcut olan veri, raporun oluşturulduğu zaman Security Server üzerinde yer alan günlüklerin miktarından etkilenir. Yeni günlükler eklendikçe ve eskileri silindikçe, günlüklerin miktarı değişir. **Raporlar** > **Bakım** kısmından, günlükleri manuel olarak silebilir veya bir günlük silme zamanlaması oluşturabilirsiniz. Raporun içeriği hakkında ayrıntılar için, bkz. *Raporları Yorumlama sayfa 12-11*.
Bakım Görevleri Şablonu	
Şablon ayarları düzenle	Şablona tıklayın ve beliren yeni ekranda ayarları düzenleyin. Değişikliklerinizi kaydettikten sonra oluşturulan raporlar, yeni ayarları kullanacaktır.
Bir şablonu Etkinleştir/Devre Dışı Bırak	Etkin sütunu altındaki simgeye tıklayın. Zamanlanmış raporları oluşturmayı geçici olarak durdurmak istiyorsanız bir şablonu devre dışı bırakın ve tekrar raporlara ihtiyacınız olduğunda etkinleştirin.

GÖREV	ADIMLAR
Bir şablonu sil	Bir şablon seçin ve **Sil** öğesine tıklayın. Bir şablonun silinmesi, şablondan oluşturulan zamanlanmış raporları silmez, ancak raporlara olan bağlantılar artık web konsolundan kullanılabilir olmayacaktır. Raporlara doğrudan Security Server bilgisayarından erişebilirsiniz. Raporlar sadece bilgisayardan menuel olarak silerseniz silinecektir veya **Raporlar** > **Bakım** > **Raporlar** sekmesindeki zamanlanmış rapor oto-silme ayarına göre Security Server otomatik olarak siler. Şablonları otomatik olarak silmek için, **Raporlar** > **Bakım** > **Raporlar** sekmesine gidin ve WFBS'nin tutacağı maksimum şablon sayısını ayarlayın. Varsayılan değer 10 şablondur. Bu sayı aşıldığında, Security Server en uzun süre tutulan şablondan başlayarak şablonları siler.
Bakım Görevleri Raporla	
Zamanlanmış raporlara bir bağlantı gönder	Zamanlanmış raporlara e-posta aracılığıyla (PDF biçiminde) bir bağlantı gönder Alıcılar, PDF dosyasına erişmek için e-posta iletisindeki bağlantıya tıklar. Alıcıların Security Server bilgisayarına bağlanabileceğinden emin olun, yoksa dosya görüntülenmeyecektir. **Nota** E-postada sadece PDF dosyasına bir bağlantı verilir. Güncel PDF dosyası eklenmez. a. Zamanlanmış raporların oluşturulduğu şablonu içeren satırda, **Rapor Geçmişi** öğesine tıklayın. Yeni bir ekran açılır. b. Raporları seçin ve **Gönder** öğesine tıklayın. Varsayılan e-posta istemciniz, rapora bağlantı içeren yeni bir e-posta ile açılır.

GÖREV	ADIMLAR
Zamanlanmış raporları sil	a. Zamanlanmış raporların oluşturulduğu şablonu içeren satırda, **Rapor Geçmişi** öğesine tıklayın. Yeni bir ekran açılır. b. Raporları seçin ve **Sil** öğesine tıklayın. **Nota** Raporları otomatik olarak silmek için, **Raporlar** > **Bakım** > **Raporlar** sekmesine gidin ve WFBS'nin her şablonda tutacağı maksimum zamanlanmış rapor sayısını ayarlayın. Varsayılanı, 10 zamanlanmış rapordur. Bu sayı aşıldığında, Security Server en uzun süre tutulan rapordan başlayarak raporları siler.

Raporları Yorumlama

Worry-Free Business Security raporları aşağıdaki bilgileri içerir. Görüntülenen bilgiler işaretlenen seçeneklere bağlı olarak değişiklik gösterebilir.

Tablo 12-2. Rapor İçeriği

Rapor Öğesi	Açıklama
Antivirüs	**Masaüstü/Sunucular Virüs Özeti** Virüs raporları, tarama motorunu algılayan ve onlara karşı önlemler alan virüs/kötü amaçlı yazılım sayısı ve türlerine ilişkin ayrıntılı bilgileri gösterir. Raporda ayrıca En Büyük virüs/kötü amaçlı yazılım adları listelenir. Yeni bir web tarayıcı sayfası açmak için virüs/kötü amaçlı yazılım adlarını tıklatın ve virüs/kötü amaçlı yazılım hakkında daha fazla bilgi edinmek için Trend Micro virüs ansiklopedisine yönlendirin.
	Virüs Algılamaları ile ilk 5 /Masaüstü/Sunucu Virüs/kötü amaçlı yazılım algılamalarını raporlayan ilk beş masaüstü veya sunucuyu görüntüler. Aynı istemci üzerinde en sık virüs/kötü amaçlı yazılım olaylarının gözlenmesi, istemcinin daha fazla araştırma gerektirecek yüksek güvenlik riski taşıdığını gösterebilir
Salgın Savunması Geçmişi	**Salgın Savunması Geçmişi** En yeni salgınları, salgınların derecesini görüntüler ve salgına neden olan virüs/kötü amaçlı yazlımı ve nasıl geldiğini (e-posta veya dosya aracılığıyla) belirler.
Casus yazılımdan koruma	**Masaüstü/Sunucular Casus Yazılım/Grayware Özeti** Casus yazılım/grayware raporu, algılama sayısı ve tehditlere karşı WFBS tarafından alınan önlemleri içeren, istemciler üzerinde algılanan casus yazılım/grayware tehditlerine ilişkin ayrıntılı bilgiyi içerir. Rapor, gerçekleştirilen her bir casus yazılım/grayware eyleminin yüzdesini gösteren bir pasta grafik içerir.
	Casus Yazılım/Grayware Algılamaları ile ilk 5 Masaüstü/ Sunucu Rapor ayrıca algılanan ilk beş casus yazılım/grayware tehdidini ve en yüksek sayıda algılanan casus yazılım/grayware ile beş masaüstü/sunucuyu gösterir. Algılanan casus yazılım/grayware tehditlerine ilişkin daha fazla bilgi almak için, casus yazılım/ grayware adlarını tıklatın. Yeni bir web tarayıcı sayfası açılır ve Trend Micro web sitesindeki casus yazılım/grayware ilişkili bilgileri görüntüler.

Rapor Öğesi	Açıklama
Anti-spam özeti (Yalnızca Advanced)	**Spam Özeti** Anti-spam raporlarında, taranan iletilerin tümünde algılanan spam ve kimlik avı sayısı hakkında bilgi verilir. Bildirilen hatalı pozitifler listelenir.
Web Reputation	**Web Reputation İlkelerini İhlal Eden İlk 10 Bilgisayar**
URL kategorisi	**İhlal Edilen İlk 5 URL Kategori İlkesi** İlkeyi ihlal eden, en çok erişilen web sitesi kategorilerini listeler.
	URL Kategori İlkelerini İhlal Eden İlk 10 Bilgisayar
Behavior Monitoring	**Behavior Monitoring İlkelerini İhlal Eden İlk 5 Program**
	Behavior Monitoring İlkelerini İhlal Eden İlk 10 Bilgisayar
Aygıt Denetimi	**Aygıt Denetimi İlkesini İhlal Eden İlk 10 Bilgisayar**
İçerik filtreleme özeti (Yalnızca Advanced)	**İçerik Filtreleme Özeti** İçerik filtreleme raporlarında, Messaging Security Agent'ın filtrelediği iletilerin toplam sayısı hakkında bilgi verilir.
	İhlal Edilen İlk 10 İçerik Filtreleme Kuralı İhlal edilen ilk 10 içerik filtreleme kuralının listesi. Filtreleme kurallarınızın ince ayarını yapmak için bu geribildirimi kullanın.
Ağ Virüsü	**Algılanan İlk 10 Ağ Virüsü** Ortak güvenlik duvarı sürücüsü tarafından en sık algılanan ilk 10 ağ virüsünü listeler. Yeni bir web tarayıcı sayfası açmak için virüs adlarını tıklatın ve virüs hakkında daha fazla bilgi edinmek için Trend Micro virüs ansiklopedisine yönlendirin.
	Saldırılan İlk 10 Bilgisayar En sık virüs olayı bildiren, ağınızdaki bilgisayarları listeler.

Raporlar ve Günlükler için Bakım Görevlerini Gerçekleştirme

Prosedür

1. **Raporlar** > **Bakım** kısmına gidin.
2. Aşağıdaki görevleri gerçekleştirin:

GÖREV	ADIMLAR
Raporların ve şablonların maksimum sayısını ayarlayın	Security Server üzerindeki tek seferlik raporların, zamanlanmış raporların (şablon başına) ve şablonların sayısını sınırlayabilirsiniz. Bu sayı aşıldığında, Security Server en uzun süre tutulan rapordan/şablondan başlayarak raporları/şablonları siler. a. **Bildirimler** sekmesine tıklayın. b. Tutulacak tek seferlik raporların, zamanlanmış raporların ve rapor şablonlarının maksimum sayısını girin.
Günlüklerin otomatik silinmesini yapılandırın	a. **Otomatik Günlük Silme** sekmesini tıklayın. b. Günlük türlerini seçin ve günlüklerin maksimum süresini belirtin. Bu değerden daha eski günlükler silinecektir.
Günlükleri manuel olarak silme	a. **Manuel Günlük Silme** sekmesini tıklayın. b. Her günlük türü için, günlüklerin maksimum süresini girin. Bu değerden daha eski günlükler silinecektir. Tüm günlükleri silmek için `0` girin. c. **Sil** öğesine tıklayın.

3. **Kaydet** öğesine tıklayın.

Bölüm 13

Yönetici Görevlerinin Gerçekleştirilmesi

Bu bölümde, ürün lisansını görüntüleme, Plug-in Manager ile çalışma ve Security Server'ı kaldırma gibi ek yönetici görevlerinin nasıl gerçekleştirildiği açıklanmaktadır.

Web Konsolu Parolasını Değiştirme

Trend Micro, web konsolu için sağlam parolaların kullanılmasını önerir. Sağlam bir parola, en az sekiz karakter uzunluğundadır ve bir veya birden fazla büyük harf (A-Z), bir veya birden fazla küçük harf (a-z), bir veya birden fazla sayı (0-9) ve bir veya birden fazla özel karakter ya da noktalama işareti (!@#$%^&,.:;?) içerir. Sağlam parolalar, kesinlikle kullanıcının oturum açma adıyla aynı değildir veya oturum açma adını içermez. Kullanıcının adından veya soyadından, doğum tarihinden ya da kullanıcıyla kolaylıkla ilişkilendirilebilecek herhangi bir bilgiden oluşmaz.

Prosedür

1. **Tercihler** > **Parola** kısmına gidin.
2. Aşağıdaki seçenekleri gerektiği gibi güncelleyin:
   - **Eski parola**
   - **Yeni parola**
   - **Parolayı onaylayın**: Onaylamak için yeni parolayı tekrar yazın.
3. **Kaydet** öğesine tıklayın.

Plug-in Manager ile Çalışma

Plug-in Manager hem Security Server hem de web konsolundaki Aracılar için programları kullanılabilir oldukları anda görüntüler. Ardından, istemci eklenti programlarını Aracılara dağıtmak da dahil olmak üzere programları web konsolundan yükleyebilir ve yönetebilirsiniz. Plug-in Manager'ı **Tercihler** > **Eklentiler** kısmından indirebilir ve yükleyebilirsiniz. Yüklemeden sonra, kullanılabilir eklenti programlarını kontrol edebilirsiniz. Daha fazla bilgi için Plug-in Manager belgelerine ve eklenti programlara bakın.

Ürün Lisansını Yönetme

Ürün Lisansı ekranından, ürün lisansı ayrıntılarını yenileyebilir, yükseltebilir veya görüntüleyebilirsiniz.

Ürün Lisansı ekranında, lisansınızla ilgili ayrıntılar görüntülenir. Yükleme sırasında belirlediğiniz seçeneklere bağlı olarak, tam lisanslı bir sürümü veya deneme sürümünü elde etmiş olabilirsiniz. Her iki durumda da, lisansınız size bir bakım sözleşmesi hakkı kazandırır. Bakım sözleşmenizin süresi dolduğunda, ağınızdaki istemciler son derece kısıtlı bir şekilde korunacaktır. Lisansınızın geçerlilik sonu tarihini belirlemek ve süresi dolmadan önce lisansınızı yenilemek için Ürün Lisansı ekranını kullanın.

Nota

Trend Micro ürünlerinin çeşitli bileşenlerinin lisansları bölgeye göre farklılık gösterebilir. Yüklemeden sonra, Kayıt Anahtarınızın/Etkinleştirme Kodunuzun kullanmanıza izin verdiği bileşenlerin bir özetini göreceksiniz. Lisanslarına sahip olduğunuz bileşenleri doğrulamak için satıcınıza veya tedarikçinize başvurun.

Lisans Yenileme

Bir bakım yenilemesi satın alarak WFBS'nin tam lisanslı sürümünü yenileyebilir veya yükseltebilirsiniz. Tam lisanslı sürüm bir Aktivasyon Kodu gerektirmektedir.

Ürün lisansını iki şekilde yenileyebilirsiniz:

- Web konsolu üzerinden Canlı Durum ekranına gidin ve ekran üzerindeki talimatları takip edin. Bu talimatlar, lisansın sona ermesinden 60 gün önce ve sona erdikten 30 gün sonra aralığında belirir.
- Lisans sözleşmenizi yenilemek için Trend Micro satış temsilcinize veya kurumsal tedarikçinize başvurun.

  Satıcılar, Security Server üzerinde bir dosyada kendi iletişim bilgilerini bırakabilirler. Buradaki dosyayı kontrol edin:

  {Security Server installation folder}\PCCSRV\Private\contact_info.ini

Nota

{Güvenlik Sunucusu yükleme klasörü} normalde C:\Program Files\Trend Micro\Security Server konumundadır.

Bir Trend Micro temsilcisi, Trend Micro Ürün Kaydı'nı kullanarak kayıt bilgilerinizi güncelleyecektir.

Security Server, Ürün Kayıt sunucusunu yoklar ve yeni geçerlilik sonu tarihini doğrudan Ürün Kayıt sunucusundan alır. Lisansınızı yenilerken manuel olarak yeni bir Etkinleştirme Kodu girmeniz gerekmez.

Yeni bir Lisansın Etkinleştirilmesi

Lisans türünüz Worry-Free Business Security Etkinleştirme Kodunuzu belirler.

TABLO 13-1. Lisans Türüne Göre Etkinleştirme Kodu

LİSANS TÜRÜ	ETKİNLEŞTİRME KODU
WFBS Standard tam lisanslı sürümü	CS-xxxx-xxxxx-xxxxx-xxxxx-xxxxx
WFBS Gelişmiş tam lisanslı sürümü	CM-xxxx-xxxxx-xxxxx-xxxxx-xxxxx

Nota

Aktivasyon Kodu hakkında sorunuz varsa, lütfen şu Trend Micro destek web sitesini ziyaret edin:

http://esupport.trendmicro.com/support/viewxml.do?ContentID=en-116326

Yeni bir Etkinleştirme Kodu girerek lisans türünüzü değiştirmek için Ürün Lisansı ekranını kullanın.

1. **Tercihler** > **Ürün Lisansı** bölümüne gidin.
2. **Yeni bir kod girin** öğesine tıklayın.
3. Verilen alana yeni Etkinleştirme Kodunuzu girin.
4. **Etkinleştir** öğesine tıklayın.

Smart Feedback Program'ına Katılma

Smart Feedback hakkında ayrıntılar için, bkz. *Smart Feedback sayfa 1-21*.

Prosedür

1. **Tercihler** > **Smart Protection Network** kısmına gidin.
2. **Trend Micro Smart Feedback'i Etkinleştir**'i tıklatın.
3. İstemci bilgisayarlarınızdaki dosyalara ilişkin potansiyel güvenlik tehditleri hakkında bilgi göndermek için **Şüpheli program dosyalarının geribildirimini etkinleştir** onay kutusunu işaretleyin.

   Nota

   Smart Feedback'e gönderilen dosyalar kullanıcı verisi içermez ve yalnızca tehdit analizi için sunulur.

4. Trend Micro'nun kuruluşunuz hakkında bilgi edinmesine yardımcı olmak için **Endüstri** türünü seçin.
5. **Kaydet** öğesine tıklayın.

Aracı Arayüzü Dilini Değiştirme

Aracı arayüzünde kullanılan dil, varsayılan olarak istemci işletim sisteminde yapılandırılmış yerel ayara karşılık gelir. Kullanıcılar, aracı arayüzünden dili değiştirebilir.

Program Ayarlarını Kaydetme ve Geri Yükleme

Security Server'ı geri almak için, Security Server veritabanının ve önemli yapılandırma dosyalarının bir kopyasını kaydedebilirsiniz. Birtakım sorunlarla karşılaşıyorsanız ve Security Server'ı yeniden yüklemek istiyorsanız ya da eski yapılandırmaya geri dönmek istiyorsanız, bunu gerçekleştirebilirsiniz.

Prosedür

1. Trend Micro Security Server Master Service'ı durdurun.
2. Aşağıdaki dosya ve klasörleri klasörden farklı bir konuma manuel olarak kopyalayın:

   UYARI!
   Bu görev için yedekleme araçlarını veya uygulamalarını kullanmayın.

   C:\Program Files\Trend Micro\Security Server\PCCSRV

   - ofcscan.ini:Genel ayarları içerir.
   - ous.ini: Antivirüs bileşen dağıtımı için güncelleme kaynağı tablosunu içerir.
   - Özel klasör: Güvenlik duvarı ve güncelleme kaynağı ayarlarını içerir.

- Web\TmOPP klasörü: Salgın Savunması ayarlarını içerir.
- Pccnt\Common\OfcPfw.dat: Güvenlik duvarı ayarlarını içerir.
- Download\OfcPfw.dat: Güvenlik duvarı dağıtım ayarlarını içerir.
- Log klasörü: Sistem olaylarını ve bağlantı doğrulama günlüğünü içerir.
- Virüs klasörü: WFBS'nin etkilenmiş dosyaları karantinaya aldığı klasör.
- HTTDB klasörü: WFBS veritabanını içerir.

3. Security Server'ı Kaldırma. Bkz. *Security Server'ı Kaldırma sayfa 13-8*.
4. Yüklemeyi yeniden gerçekleştirin. WFBS *Yükleme ve Yükseltme Kılavuzu*'na bakın.
5. Ana yükleyici tamamlandıktan sonra, hedef bilgisayarda Trend Micro Security Server Master Service'ı durdurun.
6. Yedekleme dosyasından virüs kalıbı sürümünü güncelleyin:
   a. Yeni sunucudan geçerli virüs kalıbı sürümünü edinin.

      \Trend Micro\Security Server\PCCSRV\Private\component.ini. [6101]

      ```
      ComponentName=Virüs kalıbı

      Sürüm=xxxxxx 0 0
      ```

   b. Yedeklenen dosyada virüs kalıbının sürümünü güncelleyin:

      \Private\component.ini

      Nota

      Security Server yükleme yolunu değiştirirseniz,ofcscan.ini ve \private\ofcserver.ini yedekleme dosyaları içindeki yol bilgisini güncellemeniz gerekir.

7. Oluşturduğunuz yedeklemeleri, hedef makinede PCCSRV klasöründeki WFBS veritabanının ve ilgili dosya ve klasörlerin üzerine yazın.
8. Trend Micro Security Server Master Service'ı yeniden başlatın.

Security Server'ı Kaldırma

Security Server'ın kaldırılması, ayrıca Tarama Sunucusunu da kaldırır.

Worry-Free Business Security, Trend Micro Security Server'ı bilgisayarınızdan güvenle kaldırmak için bir kaldırma programı kullanır. Security Server'ı kaldırmadan önce Aracıyı tüm istemcilerden kaldırın.

Trend Micro Security Server'ın kaldırılması Aracıların kaldırılmasını sağlamaz. Yöneticilerin, Trend Micro Security Server'ı kaldırmadan önce tüm Aracıları kaldırması veya başka bir Security Server'a taşıması gerekir. Bkz. *Aracıları Kaldırma sayfa 3-39*.

Prosedür

1. Sunucuyu yüklemek için kullandığınız bilgisayarda, **Başlat** > **Denetim Masası** > **Program Ekle veya Kaldır** seçeneklerine tıklayın.
2. Önce **Trend Micro Security Server**'ı, ardından da **Değiştir/Kaldır**'ı tıklatın.

   Bir onay ekranı görünür.
3. **İleri** öğesine tıklayın.

   Ana Kaldırıcı, sunucu kaldırma programı, sizden Yönetici parolasını girmenizi ister.
4. Metin kutusuna Yönetici parolasını girin ve **Tamam**'ı tıklatın.

   Ardından, Ana Kaldırıcı sunucu dosyalarını kaldırmaya başlar. Security Server kaldırıldıktan sonra bir onay iletisi görünür.
5. Kaldırma programını kapatmak için **Tamam**'ı tıklatın.

Bölüm 14

Yönetim Araçlarını Kullanma

Bu bölümde, yönetici ve istemci araçlarının nasıl kullanılacağını ve eklentileri açıklanmaktadır.

Araç Türleri

Worry-Free Business Security, sunucu yapılandırması ve istemci yönetimi dahil çeşitli görevleri kolaylıkla yerine getirebilmenizde size yardımcı olacak bir dizi araç içerir.

Nota

Yönetici ve istemci araçları web konsolundan başlatılamaz. Eklentiler web konsolundan indirilebilir.

Araçların nasıl kullanılacağına ilişkin yönergeler için, aşağıda ilgili bölümlere bakın.

Bu araçlar üç kategoride sınıflandırılır:

- **Yönetici araçları**
  - **Oturum Açma Komut Dosyası Kurulumu** (SetupUsr.exe): Security Agent yüklemesini otomatikleştirir. Bkz. *Oturum Açma Komut Dizesi Kurulumu ile Yükleme sayfa 3-14*.
  - **Güvenlik Açığı Tarayıcısı** (TMVS.exe): Ağdaki korunmasız bilgisayarları konumlandırır. Bkz. *Güvenlik Açığı Tarayıcısıyla Yükleme sayfa 3-23*.
  - **Uzaktan Yönetim Aracısı**: WFBS'yi yönetmek için Tedarikçiler'i merkezi web konsolu aracılığıyla etkinleştirir. Bkz. *Trend Micro Remote Manager Agent'ı Yükleme sayfa 14-3*.
  - **Trend Micro Disk Temizleyici**: Gereksiz WFBS yedekleme dosyalarını, günlük dosyalarını ve kullanılmayan kalıp dosyalarını siler. Bkz. *Disk Alanı Kazanma sayfa 14-5*.
  - **Tarama Sunucusu Veritabanı Taşıma Aracı**: Scan Server veritabanını güvenli bir şekilde başka bir disk sürücüsüne taşır. Bkz. *Scan Server Veritabanının Taşınması sayfa 14-8*.
- **İstemci araçları**
  - **Client Packager** (ClnPack.exe): Security Agent ve bileşenlerini içeren kendiliğinden ayıklanan bir dosya oluşturur. Bkz. *Client Packager ile Yükleme sayfa 3-16*.

- **Restore Encrypted Virus ve Spyware** (VSEncode.exe): WFBS tarafından şifrelenen etkilenmiş dosyaları açar. Bkz. *Şifrelenmiş Dosyaları Geri Yükleme sayfa 14-9*.

- **Client Mover Tool** (IpXfer.exe): Aracıları bir Security Server'dan diğerine aktarır. Bkz. *Aracıları Taşıma sayfa 4-12*.

- **Security Agent İstemci Kimliği'ni yeniden oluştur** (WFBS_WIN_All_ReGenID.exe): Security Agent'ın kopyalanmış bilgisayarda veya sanal makinede olmasına bağlı olarak Security Agent İstemci Kimliği'ni yeniden oluşturmak için ReGenID yardımcı programını kullanın. Bkz. *ReGenID Aracını Kullanma sayfa 14-13*.

- **Security Agent Kaldırma** (SA_Uninstall.exe): İstemci makinesinden tüm Security Agent içeriklerini otomatik olarak kaldırır. Bkz. *SA Kaldırma Aracını Kullanma sayfa 3-43*.

- **Eklentiler**: Yöneticilerin, desteklenen Windows işletim sistemlerinin konsollarından canlı güvenlik ve sistem bilgisini görüntülemesine imkan sağlar. Bu, Canlı Durum ekranında görüntülenebilen aynı yüksek düzeydeki bilgidir. Bkz. *SBS ve EBS Eklentilerini Yönetme sayfa 14-14*.

Nota

WFBS'nin önceki sürümlerinde kullanılabilen bazı araçlar bu sürümde mevcut değildir. Bu araçlar gerekiyorsa, Trend Micro Teknik Destek ile irtibat kurun.

Trend Micro Remote Manager Agent'ı Yükleme

Trend Micro Remote Manager Agent, tedarikçilerin Trend Micro Remote Manager (TMRM) ile WFBS yönetmesini sağlar. TMFRM Agent (sürüm 3.5), Security Server 9.0 SP1 üzerine yüklenir.

Trend Micro sertifikalı iş ortağıysanız, Trend Micro Remote Manager (TMFRM) için aracıyı yükleyebilirsiniz. Security Server yüklemesi tamamlandıktan sonra TMRM Agent'ı yüklememeyi seçtiyseniz, bunu daha sonra yapabilirsiniz.

Kurulum gereksinimleri:

- TMRM Agent GUID

  GUID'u elde etmek için, TMRM Konsolunu açın ve şu yolu takip edin; **Müşteriler (sekme) > Tüm Müşteriler (ağaç üzerinde) > {müşteri} > WFBS/CSM > Server/Agent Ayrıntıları (sağ bölme) > WFRM Agent Ayrıntıları**

- Aktif bir Internet bağlantısı

- 50 MB'lik boş disk alanı

Prosedür

1. Security Server'a gidin ve şu yükleme klasörüne ulaşın: PCCSRV\Admin\Utility \RmAgent ve TMRMAgentforWFBS.exe uygulamasını çalıştırın.

   Örneğin: C:\Program Files\Trend Micro\Security Server\PCCSRV\Admin\Utility \RmAgent\TMRMAgentforWFBS.exe

   ---

   Nota

   Yüklemeyi Security Server Kurulum ekranından başlatıyorsanız, bu adımı atlayın.

   ---

2. Trend Micro Remote Manager Agent Kurulum Sihirbazı'nda lisans sözleşmesini okuyun. Hükümleri kabul ediyorsanız, **Lisans sözleşmesinin hükümlerini kabul ediyorum** seçin ve ardından **İleri** öğesine tıklayın.

3. Sertifikalı iş ortağı olduğunuzu belirtmek için **Evet** öğesine tıklayın.

4. **Trend Micro Remote Manager hesabım zaten var ve aracıyı yüklemek istiyorum**'i seçin. **İleri** öğesine tıklayın.

5. Senaryonuzu belirleyin.

SENARYO	ADIMLAR
Yeni müşteri	a. **Yeni bir müşteriyle ilişkilendir** seçin b. **İleri** öğesine tıklayın. Müşteri bilgilerini girin.

SENARYO	ADIMLAR
	Nota Müşteri TMRM Konsolunda zaten varsa ve yukarıdaki yeni bir müşteriyle ilişkilendirme seçeneğini kullanıyorsanız, bunun sonucunda TMFRM ağ ağacında aynı ada sahip iki kopya müşteri oluşacaktır. Bundan kaçınmak için aşağıdaki yöntemi kullanın.
Mevcut müşteri	a. **Bu ürün Remote Manager'da zaten var** seçeneğini seçin. **Nota** WFBS, TMRM Konsoluna zaten eklenmiş olmalıdır. Yönergeler için TMRM belgelerine bakın. b. GUID'i girin.

6. **İleri** öğesine tıklayın.
7. **Bölge** ve **Protokol** seçin ve gerekirse Proxy bilgilerini girin.
8. **İleri** öğesine tıklayın.

   Yükleme Konumu ekranı açılır.
9. Varsayılan konumu kullanmak için **İleri** öğesine tıklayın.
10. **Son** öğesine tıklayın.

    Yükleme başarılıysa ve ayarlar doğruysa, TMRM Agent otomatik olarak Trend Micro Remote Manager sunucusuna kayıt yaptırmalıdır. Aracı, TMRM Konsolunda Çevrimiçi görünmelidir.

Disk Alanı Kazanma

Disk Temizleyici'yi çalıştırarak Security Server ve istemciler üzerinde disk alanı kazanın.

Security Server üzerinde Disk Temizleyiciyi Çalıştırma

Başlamadan önce

Disk alanı kazanmak için, Disk Temizleyici Aracı (TMDiskCleaner.exe) kullanılmayan yedek, günlük ve kalıp dosyalarını tanımlar ve aşağıdaki dizinlerden siler:

- {Security Agent}\AU_Data\AU_Temp*
- {Security Agent}\Reserve
- {Security Server}\PCCSRV\TEMP* (gizli dosyalar hariç)
- {Security Server}\PCCSRV\Web\Service\AU_Data\AU_Temp*
- {Security Server}\PCCSRV\wss*.log
- {Security Server}\PCCSRV\wss\AU_Data\AU_Temp*
- {Security Server}\PCCSRV\Backup*
- {Security Server}\PCCSRV\Virus* (NOTVIRUS dosyası hariç, karantina altına alınan iki haftadan eski dosyaları siler)
- {Security Server}\PCCSRV\ssaptpn.xxx (yalnızca en son kalıbı saklar)
- {Security Server}\PCCSRV\lpt$vpn.xxx (yalnızca en son üç kalıbı saklar)
- {Security Server}\PCCSRV\icrc$oth.xxx (yalnızca en son üç kalıbı saklar)
- {Security Server}\DBBackup* (yalnızca en son iki alt klasörü saklar)
- {Messaging Security Agent}\AU_Data\AU_Temp*
- {Messaging Security Agent}\Debug*
- {Messaging Security Agent}\engine\vsapi\latest\pattern*

Prosedür

1. Security Server'da, aşağıdaki dizine gidin:

   {Server Yükleme Klasörü}\PCCSRV\Admin\Utility\

2. **TMDiskCleaner.exe** dosyasına çift tıklayın.

   Trend Micro Worry-Free Business Security Disk Temizleyici görünür.

   Nota

   Dosyalar geri yüklenemez.

3. Kullanılmayan yedek, günlük ve kalıp dosyalarını taramak ve silmek için **Dosyaları Sil** seçeneğine tıklayın.

Komut Satırı Arayüzünü Kullanarak Security Server Üzerinde Disk Temizleyiciyi Çalıştırma

Prosedür

1. Security Server'da bir Komut İstemi penceresi açın.
2. Komut isteminde, aşağıdaki komutu çalıştırın:

   ```
   TMDiskCleaner.exe [/hide] [/log] [/allowundo]
   ```

   - `/hide`: Aracı arka plan işlemi olarak çalıştırır.
   - `/log`: Geçerli klasörde bulunan DiskClean.log dosyasına bir işlem günlüğü kaydeder.

     Nota

     `/log` yalnızca `/hide` kullanıldığı sırada kullanılabilir.

   - `/allowundo`: Dosyaları Geri Dönüşüm Kutusu'na taşır ve dosyaları kalıcı olarak silmez.
3. Disk Temizleyici aracını sık olarak çalıştırmak için, Windows Zamanlanmış Görevler'i kullanarak yeni bir görev yapılandırın. Daha fazla bilgi için Windows belgelerine bakın.

İstemciler üzerinde Disk Alanı Kazanma

Prosedür

- Security Agent'lar ile masaüstleri/sunucular üzerinde:
  - Karantina altına alınan dosyaları temizleyin
  - Günlük dosyalarını temizleyin
  - Windows Disk Temizleme Programını çalıştırın
- Messaging Security Agent'lar ile Microsoft Exchange Sunucuları üzerinde:
  - Karantina altına alınan dosyaları temizleyin
  - Günlük dosyalarını temizleyin
  - Windows Disk Temizleme Programını çalıştırın
  - Arşiv günlüklerini temizleyin
  - Yedek dosyalarını temizleyin
  - Microsoft Exchange veritabanı veya işlem günlüklerinin boyutunu kontrol edin

Scan Server Veritabanının Taşınması

Scan Server'ın yüklü bulunduğu disk sürücüsündeki disk alanı yetersizse, Scan Server veritabanını güvenli bir şekilde başka bir disk sürücüye taşımak için Scan Server Database Mover aracını kullanın.

Security Server bilgisayarında 1'den fazla disk sürücüsü bulunduğundan ve yeni disk sürücüsünde en az 3GB kullanılabilir disk alanı olduğundan emin olun. Eşlenmiş sürücüler kabul edilmemektedir. Veritabanını manuel olarak veya başka araçlar kullanarak taşımayın.

Prosedür

1. Security Server bilgisayarında <Security Server yükleme klasörü>\PCCSRV\Admin \Utility'e gidin.
2. ScanServerDBMover.exe öğesini çalıştırın.
3. **Değiştir** öğesine tıklayın.
4. **Gözat** üzerine tıklayın ve ardından diğer disk sürücüsü üzerindeki hedef dizine gözatın.
5. Veritabanı taşındıktan sonra, **Tamam** öğesine ve ardından **Tamamlandı** öğesine tıklayın.

Şifrelenmiş Dosyaları Geri Yükleme

Etkilenmiş dosyaların açılmasını önlemek için, Worry-Free Business Security dosyayı aşağıdaki durumlar sırasında şifreler:

- Bir dosyayı karantinaya almadan önce
- Temizlemeden önce bir dosyayı yedeklerken

WFBS, bir bilgi almanız gerektiğinde dosyanın şifresini açmak ve geri yüklemek için bir araç sağlar. WFBS aşağıdaki dosyaların şifresini açar ve geri yükler:

TABLO 14-1. WFBS'nin Şifresini Açabileceği ve Geri Yükleyebileceği Dosyalar

DOSYA	AÇIKLAMA
İstemci üzerindeki karantina dosyaları	Bu dosyalar şu dizinlerde bulunur: • <Security Agent yükleme klasörü>\SUSPECT\Backup veya <Security Agent yükleme klasörü>\quarantine, hangisi kullanılabilirse. • <Messaging Security Agent installation folder>\storage\quarantine Bu dosyalar, tipik olarak Security Server üzerinde bir dizin olan, belirtilen karantina dizinine karşıya yüklenir.
Belirtilen karantina dizinindeki karantinaya alınmış dosyalar	Varsayılan olarak, bu dizin Security Server bilgisayarında yer alır (<Security Server yükleme klasörü>\PCCSRV\Virus). Dizini değiştirmek için, **Tercihler** > **Genel Ayarlar** > **Sistem** sekmesine gidin ve Karantina Bakım bölümüne gidin.
Yedeklenmiş şifreli dosyalar	Bunlar, aracının temizleyemediği etkilenmiş dosyaların yedekleridir. Bu dosyalar şu klasörlerde bulunur: • <Security Agent yükleme klasörü>\Backup • <Messaging Security Agent yükleme klasörü>\storage\backup Bu dosyaları geri yüklemek için, kullanıcıların bunları istemci üzerindeki karantina dizinine geri yüklemesi gerekir.

UYARI!

Etkilenmiş bir dosyanın geri yüklenmesi virüsün/zararlı yazılımın diğer dosyalara ve istemcilere yayılmasına neden olabilir. Dosyayı geri yüklemeden önce, etkilenmiş istemciyi ayırın ve istemci üzerindeki önemli dosyaları bir yedek konumuna taşıyın.

Security Agent üzerindeki Dosyaların Şifresinin Açılması ve Geri Yüklenmesi

Prosedür

1. Bir komut istemi açın ve <Security Agent yükleme klasörü> kısmına gidin.

2. Aşağıdakileri yazarak VSEncode.exe dosyasını çalıştırın:

   ```
   VSEncode.exe /u
   ```

   Bu parametre <Security Agent yükleme klasörü>\SUSPECT\Backup altında bulunan dosyaların listesiyle bir ekran açacaktır.

   Yöneticiler, Casus Yazılım/Grayware sekmesinden dosyaları casus yazılım/grayware olarak geri yükleyebilir. Ekran, şunun altındaki dosyaların listesini gösterir: <Security Agent yükleme klasörü>\BackupAS.

3. Geri yüklemek için bir dosya seçin ve **Geri yükle** öğesine tıklayın. Bu araç bir seferde sadece bir dosyayı geri yükleyebilir.

4. Açılan ekranda, dosyayı geri yüklemek istediğiniz klasörü seçin.

5. **Tamam** öğesine tıklayın. Dosya belirtilen klasöre geri yüklenir.

   Nota

   Dosya geri yüklenir yüklenmez aracının dosyayı tekrar taraması ve etkilenmiş olarak işlem yapması olasılığı mevcuttur. Dosyanın taranmasını önlemek için, tarama dışlama listesine ekleyin. Bkz. *Security Agent'lar için Tarama Hedefleri ve Eylemler sayfa 7-9*.

6. Dosyaları geri yüklemeyi bitirdiğinizde **Kapat** öğesine tıklayın.

Security Server üzerindeki Dosyaların Şifresini Açma ve Geri Yükleme, Özel Karantina Dizini veya Messaging Security Agent

Prosedür

1. Dosya Security Server bilgisayarındaysa, bir komut istemi açın ve <Sunucu yükleme klasörü>>\PCCSRV\Admin\Utility\VSEncrypt kısmına gidin.

   Dosya bir Messaging Security Agent istemcisinde veya özel bir karantina dizinindeyse, <Sunucu yükleme klasörü>\PCCSRV\Admin\Utility kısmına gidin ve VSEncrypt klasörünü istemciye veya özel karantina dizinine kopyalayın

2. Metin dosyası oluşturun ve şifrelemek veya şifresini açmak istediğiniz dosyaların tam yolunu yazın.

   Örneğin, dosyaları C:\My Documents\Reports içine geri yüklemek için, metin dosyasının içine C:\My Documents\Reports*.* yazın.

   Security Server bilgisayarında karantinaya alınmış dosyalar, <Sunucu yükleme klasörü <>\PCCSRV\Virus altında bulunur.

3. Metin dosyasını INI veya TXT uzantısıyla kaydedin. Örneğin, ForEncryption.ini olarak burada kaydedin: C: .

4. Bir komut istemi açın ve VSEncrypt klasörünün yer aldoığı dizine gidin.

5. Aşağıdakileri yazarak VSEncode.exe dosyasını çalıştırın:

   ```
   VSEncode.exe /d /i < INI veya TXT dosyası konumu>
   ```

   burada:

   <INI veya TXT dosyasının konumu> oluşturduğunuz INI veya TXT dosyasının yoludur (örneğin, C:\ForEncryption.ini).

6. Çeşitli komutları yayınlamak için diğer parametreleri kullanın.

TABLO 14-2. Parametreleri Geri Yükle

PARAMETRE	AÇIKLAMA
Yok (parametre yok)	Dosyaları şifrele
`/d`	Dosya şifrelerini aç
`/debug`	Bir hata ayıklama günlüğü oluşturun ve bilgisayara kaydedin. İstemci üzerinde, VSEncrypt.log hata ayıklama günlüğü, <Agent yükleme klasörü> içerisinde oluşturulur.
`/o`	Şifreli veya şifresi açılan dosya zaten mevcutsa üzerine yazar
`/f <dosya adı>`	Tek bir dosyayı şifreler veya şifresini açar
`/nr`	Orijinal dosya adını geri yükleme
`/v`	Araç hakkındaki bilgileri görüntüle

PARAMETRE	AÇIKLAMA
`/u`	Aracın kullanıcı arayüzünü başlat
`/r <Hedef klasör>`	Bir dosyanın geri yükleneceği klasör
`/s <Orijinal dosya adı>`	Orijinal şifrelenmiş dosyanın dosya adı

Örneğin, VSEncode [/d] [/debug] yazarak dosyaların şifresini Suspect klasöründe açın ve bir hata ayıklama günlüğü oluşturun. Bir dosyayı şifrelediğinizde veya şifresini açtığınızda, WFBS aynı klasör içinde şifresi açılmış veya şifrelenmiş dosyayı oluşturur. Bir dosyanın şifresini açmadan veya şifrelemeden önce, WFBS, aynı klasör içinde şifreli ve şifresi açılmış bir dosya oluşturur.

Transport Neutral Encapsulation Format E-Posta İletilerinin Geri Yüklenmesi

Transport Neutral Encapsulation Format (TNEF), Microsoft Exchange/Outlook tarafından kullanılan bir ileti kuşatmasıdır. Genellikle bu biçim Winmail.dat adıyla bir e-posta eki olarak sıkıştırılır ve Outlook Express tarafından bu ek otomatik olarak gizlenir. Bkz. http://support.microsoft.com/kb/241538/tr-tr.

Messaging Security Agent bu tür e-postayı arşivlerse dosya uzantısı .EML olarak değişir, Outlook Express yalnız e-posta iletisi gövdesini görüntüler.

ReGenID Aracını Kullanma

Her Security Agent yüklemesi, Security Server'ın aracıları ayrı olarak tanımlayabilmesi için eşsiz bir Genel Eşsiz Tanımlayıcı (GUID) gerektirir. Çiftlenmiş GUID'ler tipik olarak klonlanmış istemcilerde veya sanal olarak oluşturulmuş makinelerde bulunur.

İki veya daha fazla aracı aynı GUID'yi bildiriyorsa, her istemci için eşsiz bir GUID oluşturmak için ReGenID aracını çalıştırın.

Prosedür

1. Security Server'da, aşağıdaki dizine gidin: <Server yükleme klasörü>\PCCSRV\Admin \Utility.
2. WFBS_WIN_All_ReGenID.exe dosyasını Security Agent'ın yüklendiği istemci üzerinde geçici bir klasöre kopyalayın.

   Örnek: C:\temp
3. WFBS_WIN_All_ReGenID.exe'yi çift tıklatın.

   Araç Security Agent'ı durdurur ve İstemci GUID'sini kaldırır.
4. Security Agent'ı Yeniden Başlat.

   Security Agent yeni bir İstemci GUID'si oluşturur.

SBS ve EBS Eklentilerini Yönetme

Worry-Free Business Security yöneticilerin aşağıdaki Windows işletim sistemlerinin konsollarından canlı güvenlik ve sistem durumu bilgisini görüntülemesine imkan sağlamak için eklentiler sağlamaktadır:

- Windows Small Business Server (SBS) 2008
- Windows Essential Business (EBS) Server 2008
- Windows SBS 2011 Standard/Essentials
- Windows Server 2012 Essentials
- Windows Server 2012 R2 Essentials

SBS ve EBS Eklentilerini Manuel Yükleme

SBS veya EBS eklentisi; Security Server'ı Windows SBS 2008, EBS 2008, SBS 2011 Standard/Essentials veya Server 2012/2012 R2 Essentials çalıştıran bir bilgisayara

yüklediğinizde otomatik olarak yüklenir. Eklentiyi bu işletim sistemlerini çalıştıran başka bir bilgisayarda kullanmak için manuel olarak yüklemeniz gerekir.

Prosedür

1. Web konsolunda **Tercihler** > **Yönetim Araçları** ve ardından **Eklentiler** sekmesine tıklayın.
2. Yükleyiciyi edinmek için ilgili **İndirme** bağlantısına tıklayın.
3. Yükleyiciyi kopyalayın ve ardından hedef bilgisayarda başlatın.

SBS veya EBS Eklentilerini Kullanma

Prosedür

1. SBS veya EBS konsolunu açın.
2. **Güvenlik** sekmesi altında, durum bilgisini görüntülemek için **Trend Micro Worry-Free Business Security** seçeneğine tıklayın.

Ek A

Security Agent Simgeleri

Bu ekte, istemciler üzerinde görüntülenen farklı Security Agent simgeleri açıklanmaktadır.

Security Agent Durumunu Kontrol Etme

Aşağıdaki resim, Security Agent Konsolunu her şeyin güncel olduğu ve düzgün şekilde çalıştığı halde gösterir:

Aşağıdaki tabloda, Security Agent Konsolu Ana Kullanıcı Arayüzü'ndeki simgeler ve anlamları listelenir:

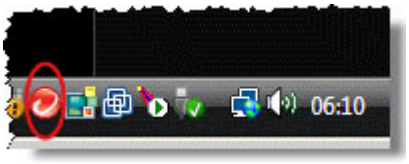
TABLO A-1. Security Agent Konsolu Ana Kullanıcı Arayüzü simgeleri

SİMGE	DURUM	AÇIKLAMA VE EYLEM
	Koruma Etkinleştirildi: Korumanız etkin ve yazılımınız güncel	Yazılım güncel ve düzgün şekilde çalışıyor. Herhangi bir eylem gerekmiyor.
	Bilgisayarı Yeniden Başlat: Güvenlik tehditlerini düzeltme işleminin tamamlanması için bilgisayarı yeniden başlatın.	Security Agent hemen düzeltemeyeceği tehditler buldu. Bu tehditleri düzeltme işleminin tamamlanması için bilgisayarı yeniden başlatın.
	Koruma Risk Altında: Yöneticinize başvurun	Gerçek Zamanlı Tarama devre dışı bırakıldı veya koruma başka bir nedenle risk altında. Gerçek Zamanlı Taramayı etkinleştirin ve bu sorununuzu çözmezse, Destek ile irtibat kurun.
	Şimdi Güncelle: (Sayı) gün içinde güncelleme almadınız.	Virüs kalıbı 3 günden eski. Security Agent'ı derhal güncelleyin.

Simge	Durum	Açıklama ve Eylem
	Smart Scan Kullanılamıyor: Internet bağlantınızı denetleyin	Security Agent 15 dakikadan uzun süredir Scan Server'a erişmedi. En son kalıplarla tarama yapmak için ağınıza bağlı olduğunuzdan emin olun.
	Bilgisayarı Yeniden Başlat: Güncelleme yüklemesini tamamlamak için bilgisayarınızı yeniden başlatın	Bir güncellemeyi tamamlamak için bilgisayarınızı yeniden başlatın.
	Program Güncelleniyor: Güvenlik yazılımınız güncelleniyor	Bir güncelleme devam ediyor. Sonlanana kadar ağ bağlantısını kesmeyin.

Windows Görev Çubuğu üzerindeki Security Agent Simgelerini Görüntüleme

Aşağıdaki Security Agent simgeleri, istemci Windows Görev Çubuğunda görüntülenir:

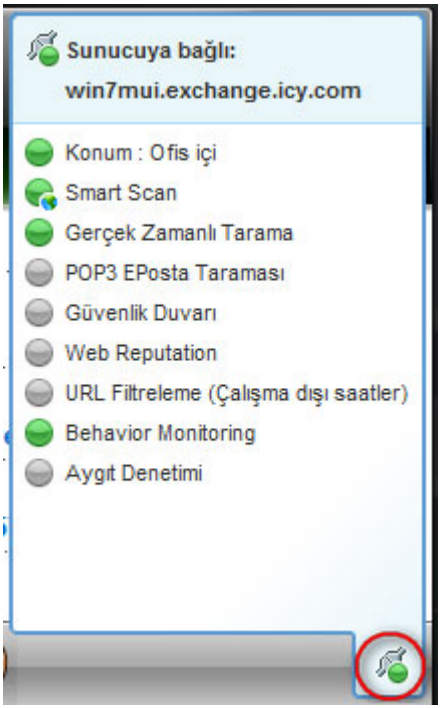


Simge	Anlamı
	Durum normal
	(Animasyonlu) Manuel Tarama veya Zamanlanmış Tarama çalışıyor. Security Agent Geleneksel Tarama veya Smart Scan kullanıyor.
	Security Agent bir güncelleme gerçekleştiriyor.

SİMGE	ANLAMI
	Eylem gerçekleştirilmesi gerekiyor: • Gerçek Zamanlı Tarama devre dışı bırakıldı • Kötü amaçlı yazılımı tamamen temizlemek için yeniden başlatma gereklidir • Güncellenen bir motor nedeniyle yeniden başlatma gereklidir • Güncelleme gerekiyor **Nota** Hangi eylemin gerektiğini görmek için Security Agent Ana Konsolunu açın.

Konsol Geçidine Erişme

Security Agent Konsolu Üst geçidi, fare işaretçisini Security Agent konsolunun sağ altındaki küçük simgenin üzerine tutunca açılır.



Aşağıdaki tabloda, Konsol Üst geçidi simgeleri ve anlamları listelenmektedir:

TABLO A-2. Konsol Üst geçidi Simgeleri

ÖZELLİK	SİMGE	ANLAMI
Bağlantı		Security Server ile bağlantı kuruldu
		Security Server ile bağlantı kurulmadı ancak gerçek zamanlı tarama hala çalışıyor. Kalıp dosyası güncel olmayabilir. Windows Görev Çubuğu'ndaki aracı simgesine sağ tıklayın ve **Şimdi Güncelle** öğesine tıklayın.

Özellik	Simge	Anlamı
Gerçek Zamanlı Tarama		Açık
		Kapalı
Smart Scan		Trend Micro Smart Protection Network'a bağlı
		Smart Protection Network'e bağlanamıyor; Security Agent'lar tarama sorgularını gönderemediği için koruma azalmıştır. **Nota** Smart Scan hizmeti TMiCRCScanService'in çalıştığını ve Security Agent'lar'ın Security Server'a bağlı olduğunu doğrulayın.
		Smart Scan devre dışı bırakıldı. Geleneksel Taramayı kullanıyor
• Güvenlik Duvarı • Web Reputation • URL Filtreleme • Behavior Monitoring • Aygıt Denetimi		Açık
		Kapalı

Ek B

WFBS içinde IPv6 Desteği

Bu eki, WFBS'nin IPv6 adreslemesini destekleyen bir ortamda dağıtımını planlayan kullanıcıların okuması gereklidir. Bu ek, WFBS içindeki IPv6 desteğinin kapsamı hakkında bilgileri içermektedir.

Trend Micro okuyucunun IPv6 kavramlarına ve IPv6 adreslemesini destekleyen bir ağ kurmaya dahil olan görevlere aşina olduğunu varsaymaktadır.

WFBS için IPv6 Desteği ve Security Agent'lar

Worry-Free Business Security için IPv6 desteği, 8.0 sürümüyle başlamıştır. Daha önceki Worry-Free Business Security sürümleri IPv6 adreslemesini desteklememektedir. Security Server, Security Agent ve Messaging Security Agent için IPv6 gereksinimlerini karşılayacak şekilde yükleme veya yükseltme yapıldıktan sonra IPv6 desteği otomatik olarak etkinleştirilir.

Security Server IPv6 Gereksinimleri

Security Server için IPv6 gereksinimleri şu şekildedir:

- Sunucu; Windows Server 2008/2012, SBS 2008/2011, 7, 8 ve Vista üzerine yüklenmelidir. Windows XP veya Server/SBS 2003 üzerine yüklenemez, çünkü bu işletim sistemleri IPv6 adreslemesini sadece kısmen desteklemektedir.
- Sunucu bir IIS web server kullanmalıdır. Apache web server, IPv6 adreslemesini desteklememektedir.
- Sunucu IPv4 vce IPv6 aracıları yönetecekse, IPv4 ve IPv6 adreslerine sahip olmalıdır ve ana makine adı ile tanımlanmalıdır. Bir sunucu IPv4 adresi ile tanımlanıyorsa, salt IPv6 aracıları sunucuya bağlanamaz. Aynı sorun, IPv6 adresi ile tanımlanan bir sunucuya IPv4 istemcilerin bağlanmasında da meydana gelecektir.
- Sunucu sadece IPv6 aracılarını yönetecekse, asgari gereksinim bir IPv6 adresidir. Sunucu, ana makine adı veya IPv6 adresi ile tanımlanabilir. Sunucu ana makine adı ile tanımlandığında, Tam Etki Alanı Adı (FQDN) kullanmak için tercih edilir. Bunun nedeni, salt IPv6 ortamında, WINS sunucusunun bir ana makine adını ilişkili IPv6 adresine çevirememesidir.
- Ana makinenin IPv6 veya IPv4 adresinin örneğin "`ping`" veya "`nslookup`" gibi komutlar kullanılarak alınabildiğini doğrulayın.
- Security Server'ı salt IPv6 bir bilgisayara yüklüyorsanız, IPv4 ve IPv6 adresleri arasında dönüştürme yapabilen bir çift yığınlı proxy sunucusu (DeleGate gibi) kurun. Sunucunun ActiveUpdate sunucusu, Çevrimiçi Kayıt web sayfası ve Smart Protection Network gibi Trend Micro'da konumlandırılan hizmetlere başarıyla

bağlanmasını sağlamak için proxy sunucusunu Security Server ve İnternet arasında konumlandırın.

Security Agent Gereksinimleri

Security Agent aşağıdakiler üzerine yüklenmelidir:

- Windows Vista (tüm sürümler)
- Windows Server 2008 (tüm sürümler)
- Windows 7 (tüm sürümler)
- Windows SBS 2011
- Windows 8 (tüm sürümler)
- Windows Server 2012 (tüm sürümler)

Windows Server/SBS 2003 ve Windows XP üzerine yüklenemez, çünkü bu işletim sistemleri IPv6 adreslemesini sadece kısmen desteklemektedir.

Bir Security Agent'ın hem IPv4, hem de IPv6 adreslerinin olması tercih edilir, çünkü bağlandığı bazı birimler sadece IPv4 adreslemesini desteklemektedir.

Messaging Security Agent Gereksinimleri

Messaging Security Agent (yalnızca Advanced), çift yığınlı veya salt IPv6 Microsoft Exchange sunucu üzerine yüklenmelidir.

Bir Messaging Security Agent'ın hem IPv4, hem de IPv6 adreslerinin olması tercih edilir, çünkü bağlandığı bazı birimler sadece IPv4 adreslemesini desteklemektedir.

Salt IPv6 Sunucu Sınırlamaları

Aşağıdaki tablo, Security Server sadece IPv6 adresine sahip olduğundaki sınırlamaları listelemektedir.

TABLO B-1. Salt IPv6 Sunucu Sınırlamaları

ÖĞE	SINIRLAMA
Aracı yönetimi	Salt bir IPv6 sunucu aşağıdakileri yapamaz: • Aracıları salt IPv4 istemcilere dağıtma • Salt IPv4 aracıları yönetme.
Güncellemeler ve merkezi yönetim	Salt bir IPv6 sunucusu aşağıdaki gibi salt IPv4 güncelleme kaynaklarından güncellenemez: • Trend Micro ActiveUpdate Server • Herhangi salt IPv4 özel güncelleme kaynağı
Ürün kaydı, etkinleştirme ve yenileme	Salt IPv6 sunucusu, ürünü kaydetmek, lisans edinmek ve lisansı etkinleştirmek/yenilemek için Trend Micro Online Registration Server'a bağlanamaz.
Proxy bağlantısı	Salt IPv6 sunucusu salt bir IPv4 proxy sunucusu üzerinden bağlanamaz.
Uyumlu çözümler	Salt IPv6 sunucusunda Plug-in Manager olacaktır, ama uyumlu çözümlerin herhangi birini aşağıdakilere dağıtamayacaktır: • Salt IPv4 aracıları veya salt IPv4 ana makineleri (doğrudan bir bağlantı eksikliğinden) • Salt IPv6 aracıları veya IPv6 ana makineleri çünkü uyumlu çözümlerin hiçbiri IPv6'yı desteklememektedir.

Bu sınırlamaların çoğunun üstesinden, IPv4 ve IPv6 adresleri arasında dönüştürebilmek için ikili yığın proxy sunucu ayarlayarak gelinebilir. Proxy sunucusunu Security Server ve bağlandığı varlıklar veya hizmet verdiği varlıklar arasında konumlandırın.

Salt IPv6 Security Agent Sınırlamaları

Aşağıdaki tablo, Security Agent sadece IPv6 adresine sahip olduğundaki sınırlamaları listelemektedir.

TABLO B-2. Salt IPv6 Security Agent Sınırlamaları

ÖĞE	SINIRLAMA
Ana Security Server	Salt IPv6 aracıları salt IPv4 Security Server tarafından yönetilemez.
Güncellemeler	Salt bir IPv6 Security Agent aşağıdaki gibi salt IPv4 güncelleme kaynaklarından güncellenemez: • Trend Micro ActiveUpdate Server • Salt IPv4 Security Server • Salt IPv4 Güncelleme Aracısı • Herhangi salt IPv4 özel güncelleme kaynağı
Tarama sorguları	Salt bir IPv6 Security Agent, Trend Micro Smart Protection Network'e sorgu gönderemez ve Smart Feedback'i kullanamaz.
Uyumlu çözümler	Salt IPv6 aracıları uyumlu çözümleri yükleyemez, çünkü uyumlu çözümlerin hiçbiri IPv6'yı desteklememektedir.
Proxy bağlantısı	Salt IPv6 Security Agent salt bir IPv4 proxy sunucusu üzerinden bağlanamaz.

Bu sınırlamaların çoğunun üstesinden, IPv4 ve IPv6 adresleri arasında dönüştürebilmek için ikili yığın proxy sunucu ayarlayarak gelinebilir. Security Agent'lar ve bağlanacakları varlıklar arasında proxy sunucuyu konumlandırın.

IPv6 Adreslerini Yapılandırma

Bu web konsolu, bir IPv6 adresi veya bir IPv6 adres aralığını yapılandırmayı imkan sağlar. Aşağıda bazı yapılandırma yönergeleri yer almaktadır.

- WFBS, standart IPv6 adres sunumlarını kabul eder.

  Örneğin:

  `2001:0db7:85a3:0000:0000:8a2e:0370:7334`

  `2001:db7:85a3:0:0:8a2e:370:7334`

```
2001:db7:85a3::8a2e:370:7334
```

```
::ffff:192.0.2.128
```

- Ayrıca, WFBS, şu şekildeki yerel IPv6 adreslerinin bağlantısını kabul eder:

  ```
  fe80::210:5aff:feaa:20a2
  ```

  UYARI!

  Bir yerel bağlantı IPv6 adresini belirtirken dikkat edin, çünkü WFBS adresi kabul etse de, belirli durumlarda beklendiği gibi çalışmayabilir. Örneğin, kaynak başka bir ağ segmanında yer alıyorsa ve yerel IPv6 adresi bağlantısıyla tanımlanıyorsa, Security Agent'lar güncelleme kaynağından güncelleme yapamaz.

- IPv6 adresi bir URL'nin parçasıysa, adresi köşeli parantezle ([]) kapatın.
- IPv6 adres aralıkları için, genellikle bir önek ve önek uzunluğu gereklidir. Sunucunun IP adreslerini sorgulamasını gerektiren yapılandırmalar için, sunucu önemli sayıda IP adresini sorguladığı zaman olabilecek performans sorunlarını önlemek için önek uzunluk sınırlandırmaları uygulanır. Örneğin, Dış Sunucu Yönetimi özelliği, için önek uzunluğu sadece 112 (65.536 IP adresi) ve 128 (2 IP adresi) arasında olabilir.
- IPv6 adreslerini veya adres aralıklarını içeren bazı ayarlar Security Agent'lar'a konuşlandırılacaktır, ancak Security Agent'lar bunları yok sayacaktır. Örneğin, akıllı koruma kaynak listesini yapılandırmış ve IPv6 adresi ile tespit edilmiş bir Smart Protection Server da dahil etmişseniz, salt IPv4 Security Agent'lar sunucuyu görmezden gelir ve diğer akıllı koruma kaynaklarına bağlanır.

IP Adreslerini Gösteren Ekranlar

Bu konu, web konsolunda IP adreslerinin gösterildiği yerleri sıralamaktadır.

- Güvenlik Grupları Ağacı

  Güvenlik Grupları Ağacı görüntülendiğinde, **IP adresi** sütununun altında salt IPv6 aracılarının IPv6 adresleri görüntülenir. İkili yığınlı aracılar için, sunucuya kaydolmak için IPv6 adresini kullanmışlarsa, IPv6 adresleri görüntülenir.

Nota

İkili yığın aracılarının sunucuya kaydolurken kullandıkları IP adresleri, **Tercih Edilen IP Adresi** kısmında, **Tercihler** > **Genel Ayarlar** > **Masaüstü/Sunucu** sekmesinden kontrol edilebilir.

Aracı ayarlarını bir dosyaya dışa aktardığınızda, dış aktarılan dosyada IPv6 adresleri de görüntülenir.

- Günlükler

  İkili yığının ve salt IPv6 aracılarının IPv6 adresleri günlüklerde görüntülenir.

Ek C

Yardım Alma

Bu ekte nasıl yardım alabileceğiniz, ek bilgilere nasıl ulaşabileceğiniz ve Trend Micro ile nasıl bağlantı kurabileceğiniz açıklanmaktadır.

Trend Micro Bilgi Bankası

Trend Micro web sitesinde bulunan Trend Micro Bilgi Bankası, ürünlerle ilgili soruların en güncel yanıtlarını içerir. Bilgi Bankası'nı ayrıca, yanıtını ürün belgelerinde bulamadığınız soruları göndermek için de kullanabilirsiniz. Bilgi Bankası'na şu konumdan erişebilirsiniz:

http://esupport.trendmicro.com/en-us/business/default.aspx

Trend Micro, Bilgi Bankasının içeriğini sürekli güncellemekte ve yeni çözümleri günlük olarak eklemektedir. Bununla birlikte, bir yanıt bulamazsanız, sorunu bir e-postada açıklayabilir ve sorunu araştırıp en kısa zamanda yanıtlayacak olan bir Trend Micro destek mühendisine gönderebilirsiniz.

Trend Micro'ya Başvurma

ABD'de, Trend Micro temsilcilerine telefon veya e-posta aracılığıyla ulaşılabilir:

Adres	Trend Micro, Incorporated 225 E. John Carpenter Freeway, Suite 1500 Irving, Texas 75062 U.S.A.
Telefon	Telefon: +1 (817) 569-8900 Ücretsiz: (888) 762-8736
Web sitesi	http://www.trendmicro.com
E-posta adresi	support@trendmicro.com

- Dünya genelindeki destek ofisleri:

  http://www.trendmicro.com.tr/hakkinda/iletisim/index.html

- Trend Micro ürün belgeleri:

  http://docs.trendmicro.com/tr-tr/home.aspx

Durum Tanı Aracı

Trend Micro Durum Tanı Aracı (CDT), problemler oluştuğunda bir müşterinin ürününden gerekli hata ayıklama bilgisini toplar. Ürünün hata ayıklama durumunu otomatik olarak açık veya kapalı hale getirir ve problem kategorilerine göre gerekli dosyaları toplar. Trend Micro, ürünlerle ilgili problemlerde sorun giderme için bu bilgileri kullanır.

WFBS'nin desteklediği tüm platformlarda bu araç çalıştırılır. Bu aracı ve ilgili belgeleri elde etmek için, destek sağlayıcınıza başvurun.

Destek Çağrısını Hızlandırma

Sorun çözmeyi daha iyi hale getirmek için aşağıdaki bilgilerin hazır olmasını sağlayın:

- Sorunu yeniden üretmek için takip edilecek adımlar
- Cihaz veya ağ bilgileri
- Bilgisayar markası, modeli ve uç noktaya bağlı olan ek donanım (varsa)
- Bellek ve boş sabit disk alanı miktarı
- İşletim sistemi ve hizmet paketi sürümü
- Uç nokta istemci sürümü
- Seri numarası veya etkinleştirme kodu
- Yükleme ortamının ayrıntılı açıklaması
- Alınan her tür hata mesajının tam metni

Şüpheli İçeriği Trend Micro'ya Gönderme

Daha fazla analiz amacıyla şüpheli içeriği Trend Micro'ya göndermek için kullanılabilecek birkaç seçenek vardır.

File Reputation Hizmetleri

Sistem bilgilerini toplayın ve şüpheli dosya içeriğini Trend Micro'ya gönderin:

http://esupport.trendmicro.com/solution/en-us/1059565.aspx

Takip amacıyla olay numarasını kaydedin.

Email Reputation Hizmetleri

Belirli bir IP adresinin geçmişini sorgulayın ve genel onaylanan listesine dahil etmek için bir mesaj aktarma aracısını görevlendirin:

https://ers.trendmicro.com/

Trend Micro'ya mesaj örnekleri göndermek için aşağıdaki Bilgi Bankası girişine bakın:

http://esupport.trendmicro.com/solution/en-US/1112106.aspx

Web Reputation Hizmetleri

Kimlik avı sitesi, ya da başka bir deyişle "hastalık vektörü" (casus yazılım ve kötü amaçlı yazılımlar gibi kasıtlı olarak oluşturulan Internet tehditleri) olduğundan şüphelenilen bir URL'nin güvenlik derecelendirmesini ve içerik türünü sorgulayın:

http://global.sitesafety.trendmicro.com/

Atanan derecelendirme yanlışsa Trend Micro'ya bir yeniden sınıflandırma isteği gönderin.

Tehdit Ansiklopedisi

Günümüzdeki kötü amaçlı yazılımların çoğu "harmanlanmış tehditlerden" oluşur. Bunlar, bilgisayar güvenlik protokollerini atlatmak için iki veya daha fazla teknolojinin birleşmesiyle ortaya çıkan tehditlerdir. Trend Micro, bu karmaşık kötü amaçlı yazılımlarla mücadele etmek için özel bir savunma stratejisi oluşturan ürünler geliştirmiştir. Tehdit Ansiklopedisi; bilinen kötü amaçlı yazılımlar, spam, kötü amaçlı URL'ler ve bilinen

güvenlik açıkları dahil olmak üzere çeşitli harmanlanmış tehditlere ilişkin kapsamlı bir ad ve belirti listesi sağlar.

Şu konular hakkında daha fazla bilgi edinmek için http://about-threats.trendmicro.com/us/threatencyclopedia#malware adresini ziyaret edin:

- Şu anda aktif olan kötü amaçlı yazılım ve kötü amaçlı mobil kod
- Eksiksiz bir web saldırısı hikayesi oluşturmak için korelasyonlu tehdit bilgileri sayfaları
- Hedeflenmiş saldırılar ve güvenlik tehditleri hakkında Internet tehdit önerileri
- Web saldırısı ve çevrimiçi eğilim bilgileri
- Haftalık kötü amaçlı yazılım raporları

TrendLabs

TrendLabs℠, 7/24 tehdit izleme, saldırı önleme ve zamanında ve sorunsuz çözüm sağlama faaliyetlerine odaklanmış araştırma, geliştirme ve eylem merkezlerinden oluşan global bir ağdır. Trend Micro hizmet altyapısının omurgası işlevini gören TrendLabs, çok çeşitli ürün ve teknik destek hizmetleri sunan yüzlerce mühendis ve sertifikalı destek personelinden oluşan bir ekibe sahiptir.

TrendLabs, saldırıları algılamak, önlemek ve ortadan kaldırmak için tasarlanmış etkili güvenlik önlemleri sağlamak amacıyla dünya genelindeki tehdit manzarasını izler. Bu çalışmaların günlük sonucu, sık sık gerçekleştirilen virüs kalıbı dosyası güncellemeleri ve tarama motoru iyileştirmeleri aracılığıyla müşterilerle paylaşılır.

TrendLabs hakkında daha fazla bilgi için şurayı ziyaret edin:

http://www.trendmicro.com.tr/teknoloji-yenilik/teknolojimiz/smart-protection-network/index.html

Belgelerin Geribildirimi

Trend Micro, her zaman belgelerini iyileştirmek için çalışmaktadır. Bu veya herhangi bir Trend Micro belgesi hakkında soru, yorum veya önerileriniz olursa, lütfen aşağıdaki siteye gidin:

http://www.trendmicro.com/download/documentation/rating.asp

Ek D

Ürün Terminolojisi ve Kavramlar

Bu ekte yer alan öğeler, Trend Micro ürünleri ve teknolojileri hakkında daha fazla bilgi sağlamaktadır.

Kritik Yama

Kritik bir yama, tüm müşterilere dağıtım için uygun şekilde güvenlik sorunlarına odaklanır. Kritik Windows yamaları bir Kurulum programı içerirken, Windows olmayan yamalar genellikle bir kurulum dizesine sahiptir.

Düzeltme

Bir düzeltme, müşteri tarafından bildirilen tek bir soruna geçici veya kalıcı bir çözümdür. Düzeltmeler soruna özgüdür, bu nedenle de tüm müşteriler için piyasaya sunulmaz. Windows düzeltmeleri bir Kurulum programı içerirken Windows olmayan düzeltmeler içermez (tipik olarak geri plan programlarını durdurmanız, dosyayı yüklemenizde denk gelen dosyanın yerine kopyalamanız ve geri plan programlarını yeniden başlatmanız gerekir).

IntelliScan

IntelliScan taranacak dosyaları tanımlamak için kullanılan bir yöntemdir. Yürütülebilir dosyalar (örneğin .exe) için, doğru dosya türü, dosya içeriğine bağlı olarak belirlenir. Yürütülemez dosyalar (örneğin .txt) için, doğru dosya türü, dosya başlığına bağlı olarak belirlenir.

IntelliScan'i kullanmanın yararları şunlardır:

- Performans optimizasyonu: IntelliScan, minimum düzeyde sistem kaynaklarından yararlandığı için aracı üzerindeki uygulamaları etkilemez
- Daha kısa tarama süresi: IntelliScan, doğru dosya türü tanımlamasını kullandığı için, yalnızca güvenlik açığı olan dosyaları tarar. Dolayısıyla tarama süresi, tüm dosyaların taranması için gereken süreden çok daha kısadır.

IntelliTrap

IntelliTrap, paketleyiciler gibi diğer kötü amaçlı yazılım özellikleriyle birlikte gerçek zamanlı sıkıştırmayı kullanan tehditleri keşfetmek için kullanılan bir Trend Micro tahmini

teknolojisidir. Bu, virüsleri/kötü amaçlı yazılımları, solucanları, truva atlarını, arka kapıları ve botları kapsar. Virüs yazarları çoğunlukla farklı dosya sıkıştırma düzenleri kullanarak virüs/kötü amaçlı yazılım filtrelemesini atlatmaya çalışırlar. IntelliTrap, 16 popüler sıkıştırma türünden herhangi birini kullanarak altı katman derinliğe kadar sıkıştırılmış dosyalardaki bilinen virüsleri/kötü amaçlı yazılımları algılayan ve temizleyen, gerçek zamanlı, kurala dayalı bir kalıp tanıma tarama motoru teknolojisidir.

Nota

IntelliTrap, virüs tarama ile aynı tarama motorunu kullanır. Sonuç olarak, IntelliTrap için dosya işleme ve tarama kuralları yöneticinin virüs taraması için tanımladıklarıyla aynıdır.

Aracılar, bot ve diğer kötü amaçlı yazılım algılamalarını IntelliTrap günlüğüne yazar. IntelliTrap günlüğü içeriklerini, raporlarda yer alması için dışa aktarır.

IntelliTrap, botları ve diğer kötü amaçlı programları denetlerken aşağıdaki bileşenleri kullanır:

- Virüs Tarama Motoru
- IntelliTrap Kalıbı
- IntelliTrap Kural Dışı Durum Kalıbı

Doğru Dosya Türü

Arama motoru, "doğru dosya türü"nü tarayacak şekilde ayarlandığında, gerçek dosya türünü tespit etmek için dosya adı yerine dosya başlığını inceler. Örneğin, tarama motoru tüm yürütülebilir dosyaları tarayacak şekilde ayarlandıysa ve family.gif" adında bir dosyayla karşılaşırsa, dosyanın bir grafik dosyası olduğunu varsaymaz. Aksine arama motoru, dosyanın gerçekten bir grafik dosyası mı yoksa örneğin, tespit edilememesi için adlandırılmış bir yürütülebilir dosya mı olduğunu belirlemek amacıyla dosya başlığını açar ve dahili kayıtlı veri türünü inceler.

Doğru dosya türü taraması, IntelliScan ile birlikte çalışarak yalnızca potansiyel olarak tehlikeli olduğu bilinen dosya türlerini tarar. Bu teknolojiler tarama motorunun incelemesi gereken dosya sayısını yaklaşık üçte iki oranında azaltabilir; ancak bu azalma ağda izin sağlanan zararlı bir dosya riskini de beraberinde getirir.

Örneğin, web trafiğinin büyük bir bölümünü .gif dosyaları oluşturur, ama bu dosyaların virüs/kötü amaçlı yazılım içerme, yürütülebilir kod başlatma veya bilinen ya da teorik güvenlik açıklarından yararlanma olasılığı düşüktür. Ancak, bu onların tamamen güvenli

olduğu anlamına gelmez. Kötü niyetli bir korsan, tarama motoruna yakalanmadan ağa sızabilmesi için zararlı bir dosyaya "güvenli" bir dosya adı verebilir. Bu dosya yeniden adlandırılır ve çalıştırılırsa zarara yol açabilir.

İpucu

En üst düzeyde güvenlik için, Trend Micro tüm dosyaların taranmasını önerir.

Davetsiz Misafir Algılama Sistemi

WFBS güvenlik duvarı ayrıca Davetsiz Misafir Algılama Sistemi'ni (IDS) de içerir. IDS ekinleştirildiğinde, Security Agent'ye yönelik bir saldırıyı gösterebilen ağ paketlerindeki kalıpları belirlemeye yardımcı olabilir. WFBS güvenlik duvarı, iyi bilinen aşağıdaki davetsiz misafirleri önlemeye yardımcı olabilir:

Davetsiz	Açıklama
Çok Büyük Parça	Bilgisayar korsanının, hedef istemci'e büyük bir TCP/UDP paketi yönlendirdiği bir servis reddi saldırısıdır. Bu saldırı, istemci ara belleğinin taşmasına ve bu sebeple istemci'ın donmasına veya yeniden başlatılmasına neden olabilir.
Ölüm Pingi	Bilgisayar korsanının, hedef istemci'a büyük bir ICMP/ICMPv6 paketi yönlendirdiği bir servis reddi saldırısıdır. Bu saldırı, istemci ara belleğinin taşmasına ve bu sebeple istemci'ın donmasına veya yeniden başlatılmasına neden olabilir.
Çakışan ARP	Bir bilgisayar korsanının, bir hedef istemci'a aynı kaynak ve hedef IP adresi ile Adres Çözümleme Protokolü (ARP) gönderdiği bir saldırı türüdür. Hedef istemci, kendisine sürekli olarak ARP yanıtı (MAC adresi) göndererek, bu sebeple donar veya çöker.
SYN Taşması	Bir programın, bir hedef istemci cihazına birden fazla TCP eşitleme (SYN) paketi göndererek istemci cihazının sürekli olarak eşitleme kabulü (SYN/ACK) yanıtları göndermesine neden olan bir servis reddi saldırısıdır. Bu saldırı, istemci belleğini yorabilir ve sonunda istemci çökmesine neden olabilir.

DAVETSİZ	AÇIKLAMA
Çakışan Parça	Bu servis reddi saldırısı, Teardrop saldırısına benzer şekilde bir istemci cihazına çakışan TCP parçaları gönderir. Bu, ilk TCP parçasındaki başlık bilgisinin üzerine yazar ve bir güvenlik duvarından geçebilir. Ardından güvenlik duvarı, ardışık parçaların hedef istemci'a zararlı kodla geçmesine imkan sağlayabilir.
Gözyaşı	Bu servis reddi saldırısı, çakışan parça saldırısına benzer şekilde IP parçalarıyla ilgilidir. İkinci veya sonraki IP parçasında bulunan karışık bir uzaklık değeri, alıcı istemci'ın işletim sisteminin parçaları yeniden birleştirmeye çalışırken çökmesine neden olabilir.
Küçük Parça Saldırısı	Küçük bir TCP parçasının ilk TCP paketinin üstbilgisini bir sonraki parçaya geçmeye zorladığı bir saldırı türüdür. Bu saldırı, trafiği filtreleyen yönlendiricilerin zararlı veriler içerebilen sonraki parçaları yoksaymasına neden olabilir.
Parçalanmış IGMP	IMGP paketlerini düzgün bir şekilde işleyemeyen hedef istemci'a parçalanmış IGMP paketleri gönderen servis reddi saldırısıdır. Bu, istemci'ın donmasına veya yavaşlamasına neden olabilir.
LAND Saldırısı	Bir hedef istemci cihazına aynı kaynak ve hedef adresle IP eşitleme (SYN) paketleri göndererek bu istemci cihazının ın kendisine eşitleme kabulü (SYN/ACK) yanıtı göndermesine neden olan bir saldırı türüdür. Bu, istemci'ın donmasına veya yavaşlamasına neden olabilir.

Anahtar Sözcükler

WFBS'de, anahtar sözcükler şunları içerir ve iletileri filtrelemek için kullanılır:

- Kelimeler (silahlar, bombalar ve benzeri)
- Sayılar (1,2,3 ve benzeri)
- Özel karakterler (&,#,+, ve benzeri)
- Kısa ifadeler (mavi balık, kırmızı telefon, büyük ev ve benzeri)
- Mantıksal operatörlerle bağlanan kelime veya ifadeler (elmalar .AND. portakallar)

- Kurallı ifadeler kullanan kelime veya ifadeler (.REG. a.*e “ace”, “ate” ve “advance” ile eşleşir, ancak “all”, “any” veya “antivirus” ile eşleşmez)

WFBS, bir metin (.txt) dosyasından var olan bir anahtar sözcük listesini içe aktarabilir. İçe aktarılan anahtar sözcükler, anahtar sözcük listesinde görünür.

Anahtar Sözcüklerde Operatörler

Operatörler, birden fazla anahtar sözcüğü bağlayan komutlardır. Operatörler, ölçütlerin sonuçlarını genişletebilir veya daraltabilir. Noktalı kapama operatörleri (.). Örneğin:

```
elmalar .AND. portakallar ve elmalar .NOT. portakallar
```

Nota

Operatör, kelimenin hemen öncesinde ve sonrasında nokta işaretine sahiptir. Son noktayla anahtar sözcük arasında bir boşluk vardır.

TABLO D-1. Operatörleri Kullanma

OPERATÖR	NASIL ÇALIŞIR	ÖRNEK
herhangi bir anahtar sözcük	Messaging Security Agent, kelimeyle eşleşen içeriği arar	Kelimeyi yazın ve anahtar sözcük listesine ekleyin
OR	Messaging Security Agent, OR ile ayrılmış anahtar sözcüklerden herhangi birini arar Örneğin, elma OR portakal. Aracı, elma veya portakalı arar. İçerik ikisinden birini içeriyorsa, o zaman eşleşme vardır.	Dahil etmek istediğiniz tüm kelimelerin arasına "`.OR.`" yazın Örneğin, "elma .OR. portakal"
AND	Messaging Security Agent, AND ile ayrılmış anahtar sözcüklerden tümünü arar Örneğin, elma AND portakal. Aracı, elma ve portakalın ikisini de arar. İçerik her ikisini de içermiyorsa, o zaman eşleşme yoktur.	Dahil etmek istediğiniz tüm kelimelerin arasına "`.AND.`" yazın Örneğin, "elma .AND. portakal"

OPERATÖR	NASIL ÇALIŞIR	ÖRNEK
NOT	Messaging Security Agent NOT sözcüğünü izleyen anahtar sözcükleri aramanın dışında tutar. Örneğin, .NOT. meyve. Aracı, meyve içermeyen içeriği arar. İleti "portakal soda" içeriyorsa, eşleşme vardır, ancak "portakal meyve" içeriyorsa eşleşme yoktur.	Dışlamak istediğiniz kelimeden önce "`.NOT.`" yazın Örneğin, “.NOT. meyve”
WILD	Joker sembolü kelimenin eksik kısmının yerini alır. Jokerin kalan kısmını kullanarak hecelenen herhangi bir kelimeyle eşleştirilir. **Nota** Messaging Security Agent, joker komutu ".WILD." için "?" kullanmayı desteklemez.	Dahil etmek istediğiniz kelime bölümünden önce "`.WILD.`" yazın Örneğin, "valu" içeren tüm sözcükleri eşleştirmek istiyorsanız “`.WILD.valu`” yazın. Valumart, valucash ve valubucks kelimelerinin tümü eşleşir.
REG	Kurallı ifade belirtmek için, ilgili kalıptan önce ".REG." operatörünü ekleyin (örneğin, .REG. a.*e). Bkz. *Kurallı İfadeler sayfa D-10*.	Algılamak istediğiniz kelime kalıbından önce "`.REG.`" yazın. Örneğin ".REG. a.*e", şunlarla eşleşir: “ace”, “ate” ve “advance”, ama “all”, “any”, veya “antivirus” değil

Anahtar Sözcükleri Verimli Şekilde Kullanma

Messaging Security Agent yüksek düzeyde spesifik filtreler oluşturmak için basit ve güçlü özellikler sunar. İçerik Filtreleme kurallarınızı oluştururken şunları göz önünde bulundurun:

- Messaging Security Agent varsayılan olarak, anahtar kelimelerle tam olarak eşleşen kelimeleri arar. Anahtar kelimelerinizle kısmen eşleşen kelimeleri aramak için kurallı ifadeler kullanın. Bkz. *Kurallı İfadeler sayfa D-10*.

- Messaging Security Agent, bir satırdaki birden fazla anahtar sözcüğü, her kelimesi farklı satırlardaki birden fazla anahtar sözcüğü ve virgüller/noktalar/tireler/ve diğer noktalama işaretleriyle ayrılan birden fazla anahtar sözcüğü farklı şekilde inceler. Anahtar sözcükleri birden fazla satırda kullanma hakkında daha fazla bilgi için aşağıdaki tabloya bakın.
- Messaging Security Agent'ı gerçek anahtar sözcüklerin eşanlamlılarını arayacak şekilde de ayarlayabilirsiniz.

TABLO D-2. Anahtar Sözcükler Nasıl Kullanılır

DURUM	ÖRNEK	EŞLENEN/EŞLENMEYEN
Aynı satırdaki iki kelime	silahlar bombalar	Eşleşmeler: ”Tabancalar bombalar ve diğer silahları satın almak için burayı tıklatın.” Eşleşmez: ”Tabancalar ve bombalar satın almak için burayı tıklatın.”
Virgülle ayrılmış iki kelime	tabancalar, bombalar	Eşleşmeler: "Tabancalar, bombalar ve diğer silahları satın almak için burayı tıklatın.” Eşleşmez: "Kullanılmış tabancalar, yeni bombalar ve diğer silahları satın almak için burayı tıklatın.”

Durum	Örnek	Eşlenen/Eşlenmeyen
Birden çok satırdaki birden çok kelime	tabancalar bombalar silahlar ve cephane	**Belirlenen Herhangi bir anahtar sözcük** seçtiğinizde Eşleşmeler: "Satılık silahlar” Ayrıca şunlarla da eşleşir: "Tabancalar, bombalar ve diğer silahlar" **Belirlenen tüm anahtar sözcükleri** seçtiğinizde Eşleşmeler: ”Tabancalar, bombalar ve cephane satın al” Eşleşmez: "Tabancalar bombalar silahlar mühimmat satın al.” Ayrıca şunlarla da eşleşmez: "Tabancalar, bombalar, silahlar ve cephane satın al”
Aynı satırda birçok anahtar sözcük	tabancalar bombalar silahlar cephane	Eşleşmeler: "Tabancalar, bombalar cephane satın al” Eşleşmez: "Tabancalarınız ve silahlarınız ve yeni bombalarınız için mühimmat satın alın"

Yama

Bir yama, birden fazla program sorununu çözen bir grup düzeltme ve güvenlik yamasıdır. Trend Micro yamaları düzenli bir şekilde kullanıma sunar. Windows yamaları bir Kurulum programı içerirken, Windows olmayan yamalar genellikle bir kurulum dizesine sahiptir.

Kurallı İfadeler

Kurallı ifadeler, dize eşlemesini gerçekleştirmek için kullanılır. Kurallı ifadelere ilişkin yaygın örneklerden bazılarını aşağıdaki tablolarda bulabilirsiniz. Kurallı ifade belirtmek için, ilgili kalıptan önce ".REG." operatörünü ekleyin.

Çeşitli çevrimiçi web siteleri ve öğreticiler mevcuttur. Bu türde bir site olan PerlDoc sitesi şu adreste bulunabilir:

http://www.perl.com/doc/manual/html/pod/perlre.html

UYARI!

Kurallı ifadeler, güçlü bir dize eşleme aracıdır. Bu nedenle, Trend Micro, kurallı ifadeleri kullanmayı seçen Yöneticilerin kurallı ifade söz dizimi hakkında bilgi sahibi ve deneyimli olmasını önerir. Başarıyla yazılmayan kurallı ifadeler, dramatik bir negatif etkiye sahip olabilir. Trend Micro, karmaşık söz dizimi kullanmayan basit kurallı ifadelerle başlamayı önerir. Yeni kurallar oluştururken, arşivleme eylemini kullanın ve Messaging Security Agent'ın kuralınızı kullanarak iletileri nasıl yönettiğini gözlemleyin. Kuralın beklenmedik herhangi bir sonuca neden olmayacağından emin olduğunuzda, eyleminizi değiştirebilirsiniz.

Kurallı İfade Örnekleri

Kurallı ifadelere ilişkin yaygın örneklerden bazılarını aşağıdaki tablolarda bulabilirsiniz. Kurallı ifade belirtmek için, ilgili kalıptan önce ".REG." operatörünü ekleyin.

TABLO D-3. Sayma ve Gruplama

ÖĞE	BUNUN ANLAMI	ÖRNEK
.	Nokta karakteri yeni satır karakteri dışındaki herhangi bir karakteri temsil eder.	do.; doe, dog, don, dos, dot, vb. ile eşleşir. d.r; deer, door, vb. ile eşleşir.
*	Yıldız karakteri, öğenin öncesinde sıfır veya daha fazla birim olduğu anlamına gelir.	do*; d, do, doo, dooo, doooo, vb. ile eşleşir.
+	Artı işareti karakteri, öğenin öncesinde bir veya daha fazla birim olduğu anlamına gelir.	do+; do, do, doo, dooo, doooo, vb. ile eşleşir, d ile değil.

Öğe	Bunun Anlamı	Örnek
?	Soru işareti karakteri, öğenin öncesinde sıfır veya bir birim olduğu anlamına gelir.	do?g; dg veya dog eşleşir ancak doog, dooog, vb. ile değil.
( )	Parantez karakterleri grubu arasındakiler tek bir birim gibi dikkate alınır.	d(eer)+; deer veya deereer veya deereereer, vb. ile eşleşir. + işareti, parantez içindeki alt dizeye uygulanır ve böylece regex, ardından bir veya daha fazla “eer.” grubu gelen d'yi arar.
[ ]	Köşeli parantez karakterleri bir karakter dizisini veya aralığını gösterir.	d[aeiouy]+; da, de, di, do, du, dy, daa, dae, dai, vb. ile eşleşir. + işareti parantez içindeki gruba uygulanır, böylece kurallı ifade d'den sonra gelen gruptaki bir veya daha fazla karakter için arama yapar [aeioy]. d[A-Z]; dA, dB, dC... dZ'ye kadar eşleşir. Köşeli parantez içindeki grup A ve Z arasındaki büyük harf aralığını gösterir.
[^]	Köşeli parantez içindeki ayar karakterleri mantıksal olarak belirtilen aralık grubunu etkisizleştirir, yani regex aralıkta veya grupta bulunmayan herhangi bir karakterle eşleşir.	d[^aeiouy]; kendisinden sonra sesli harf dışında herhangi bir karakter gelen db, dc veya dd, d9, d#--d ile eşleşir.
{ }	Büyük parantez karakterleri, öğenin öncesinde belirli bir olay sayısı belirler. Parantez içindeki tek değer, yalnız o kadar eşleşme olacağı anlamına gelir. Virgülle ayrılmış bir çift sayı, karakterin öncesinde geçerli bir grup sayı olduğunu gösterir. Ardından virgül gelen tek bir rakam, üst sınırın olmadığı anlamına gelir.	da{3}; ardından 3 ve yalnız 3 tane "a" gelen daaa--d ile eşleşir. da{2,4}; ardından 2, 3 veya 4 adet "a" gelen daa, daaa, daaaa ve daaaa (ama daaaaa değil)--d ile eşleşir. da{4,}; ardından 4 veya daha fazla "a" gelen daaaa, daaaaa, daaaaaa, vb. ile eşleşir.

TABLO D-4. Karakter Sınıfları (stenografi)

ÖĞE	BUNUN ANLAMI	ÖRNEK
\d	Herhangi bir rakam karakteri; işlevsel olarak [0-9] or [[:rakam:]] ile eşit	\d; 1, 12, 123 vb. ile eşleşir ancak 1b7 ile eşleşmez--bir veya daha fazla rakam karakteriyle.
\D	Herhangi bir rakam karakteri; işlevsel olarak [^0-9] veya [^[:rakam:]] ile eşit	\D a, ab, ab&, ile eşleşir, ancak 1 ile eşleşmez; bir veya daha fazla karakterle eşleşir ama bu karakterler 0, 1, 2, 3, 4, 5, 6, 7, 8, veya 9 olamaz.
\w	Herhangi bir "sözcük" karakteri--herhangi bir alfasayısal karakter; [_A-Za-z0-9] veya [_[:alnum:]] ile işlevsel olarak eşittir	\w, a, ab, a1 ile eşleşir ancak ! &ile eşleşmez--bir veya daha fazla büyük veya küçük harf veya rakam, ancak noktalama veya diğer özel karakterler değil.
\W	Alfasayısal olmayan herhangi bir karakter; [^_A-Za-z0-9] veya [^_[:alnum:]] ile eşittir	\W, *, & ile eşleşir, ancak ace veya a1 karakteriyle değil--bir veya daha fazla karakter ancak büyük veya küçük harfler ve rakamlar değil.
\s	Herhangi bir alfabe dışı karakter; boşluk, yeni satır, sekme, bölünemez boşluk, vb.; işlevsel olarak [[:space]] ile eşittir	sebze\s, “sebze” ve ardından gelen herhangi bir alfabe dışı karakter ile eşleşir. Böylece "Çorbada sebze severim" ifadesi kurallı ifadeyi tetikler ancak "Sebzeli çorba severim" ifadesi tetiklemez.
\S	Herhangi bir alfabe dışı olmayan karakter; boşluk, yeni satır, sekme, bölünemez boşluk, vb. haricinde; işlevsel olarak [^[:space]] ile eşittir	sebze\S, "sebze" ve ardından gelen herhangi bir alfabe dışı olmayan karakter ile eşleşir. Böylece "Sebzeli çorba severim" ifadesi kurallı ifadeyi tetikler ancak "Çorbada sebze severim" ifadesi tetiklemez.

TABLO D-5. Karakter Sınıfları

ÖĞE	BUNUN ANLAMI	ÖRNEK
[:alpha:]	Herhangi bir alfabe karakteri	.REG. [[:alpha:]] abc, def, xxx ile eşleşir ancak 123 veya @#$ ile değil.
[:digit:]	Herhangi bir rakam karakteri; işlevsel olarak \d ile eşittir	.REG. [[:digit:]] 1,12, 123, vb. ile eşleşir.
[:alnum:]	Herhangi bir "sözcük" karakteri--herhangi bir alfasayısal karakter; işlevsel olarak \w ile eşit	.REG. [[:alnum:]] abc, 123 ile eşleşir ancak ~!@ ile değil.
[:space:]	Herhangi bir alfabe dışı karakter; boşluk, yeni satır, sekme, bölünemez boşluk, vb.; işlevsel olarak \s ile eşittir	.REG. (sebze)[[:space:]] "sebze" ve ardından gelen herhangi bir alfabe dışı karakter ile eşleşir. Böylece "Çorbada sebze severim" ifadesi kurallı ifadeyi tetikler ancak "Sebzeli çorba severim" ifadesi tetiklemez.
[:graph:]	Boşluk dışındaki herhangi bir karakter, kontrol karakterleri veya benzeri	.REG. [[:graph:]] 123, abc, xxx, >< ile eşleşir" ancak boşluk veya kontrol karakterleri ile eşleşmez.
[:print:]	Herhangi bir karakter ([:graph:] ile benzer) ancak boşluk karakteri içerir	.REG. [[:print:]] 123, abc, xxx, ><" ve boşluk karakterleri ile eşleşir.
[:cntrl:]	Herhangi bir kontrol karakteri (örn. CTRL + C, CTRL + X)	.REG. [[:cntrl:]] 0x03, 0x08 ile eşleşir ancak abc, 123, !@# ile değil.
[:blank:]	Boşluk ve sekme karakterleri	.REG. [[:blank:]] boşluk ve sekme karakterleri ile eşleşir ancak 123, abc, !@# ile eşleşmez
[:punct:]	Noktalama karakterleri	.REG. [[:punct:]] şunlarla eşleşir ; : ? ! ~ @ # $ % & * ‘ “ , vb., ancak 123, abc ile eşleşmez

Öğe	Bunun Anlamı	Örnek
[:lower:]	Herhangi bir küçük harfli alfabetik karakter (Not: 'Büyük/küçük harf duyarlı eşleme' etkinleştirilmezse [:alnum:] olarak işlev görecektir.)	.REG. [[:lower:]] abc, Def, bAskı, Yap, vb. ile eşleşir, ABC, DEF, BASKI, YAP, 123, !@# ile eşleşmez.
[:upper:]	Herhangi bir büyük harfli alfabetik karakter (Not: 'Büyük/küçük harf duyarlı eşleme' etkinleştirilmezse [:alnum:] olarak işlev görecektir.)	.REG. [[:upper:]] ABC, DEF, BASKI, YAP vb. ile eşleşir, abc, Def, bAskı, Yap, 123, !@# ile eşleşmez.
[:xdigit:]	Onaltılık sayıda izin verilen basamaklar (0-9a-fA-F)	.REG. [[:xdigit:]] 0a, 7E, 0f, vb. ile eşleşir

Tablo D-6. Kalıp Bağlantıları

Öğe	Bunun Anlamı	Örnek
^	Dizenin başlangıcını gösterir.	^(ancak); "ancak" ile başlayan herhangi bir metin bloku ile eşleşir. Böylece "ancak çorbada sebze sevdiğim bir gerçektir" ifadesi kurallı ifadeyi tetikler ama "Çorbada sebze sevmediğim gerçektir ancak" ifadesi tetiklemez.
$	Dizenin sonunu gösterir.	(ancak)$; "ancak" ile biten herhangi bir metin bloku ile eşleşir. Böylece "Ancak çorbada sebze sevdiğim bir gerçektir" ifadesi kurallı ifadeyi tetiklemez ama "Çorbada sebze sevmediğim gerçektir ancak" ifadesi tetikler.

TABLO D-7. Kaçış Sıraları ve Düz Dizeler

ÖĞE	BUNUN ANLAMI	ÖRNEK
\	Kurallı ifadede özel anlam içeren bazı karakterlerin eşleşmesi için (örneğin "+").	(1) .REG. C\\C\+\+, 'C\C++' ile eşleşir. (2) .REG. *, * ile eşleşir. (3) .REG. \? ? ile eşleşir.
\t	Sekme karakterini gösterir.	(baskı)\t; "baskı" alt dizesi ve hemen ardından gelen bir sekme (ASCII 0x09) karakteri içeren metin bloku ile eşleşir.
\n	Yeni satır karakterini gösterir. **Nota** Farklı platformlar, yeni bir satır karakterini gösterir. Windows üzerinde, yeni bir satır bir karakter çifti, satır başının ardından yeni bir satırdır. Unix ve Linux üzerinde, yeni bir satır sadece yeni satırdır; Macintosh üzerinde yeni bir satır sadece satır başıdır.	(baskı)\n\n; "baskı" alt dizesi ve hemen ardından gelen iki yeni satır (ASCII 0x0A) karakteri içeren metin bloku ile eşleşir.
\r	Satır başı karakterini gösterir.	(baskı)\r; "baskı" alt dizesi ve hemen ardından gelen bir satır başı (ASCII 0x0D) karakteri içeren metin bloku ile eşleşir.

Öğe	Bunun Anlamı	Örnek
\b	Geri alma karakterini gösterir. OR Sınırları gösterir.	(baskı)\b; "baskı" alt dizesi ve hemen ardından gelen bir geri alma (ASCII 0x08) karakteri içeren metin bloku ile eşleşir. Kelime sınırı (\b), \W ile eşleşirken dizenin başında ve sonunda tahmini karakteri atarak bir tarafta \w ve diğer tarafta \W içeren (her iki sırada) iki karakter arasındaki bir nokta olarak tanımlanır. (Karakter sınıfları içinde \b, kelime sınırından çok geri alma karakterini temsil eder.) Örneğin, aşağıdaki kurallı ifade sosyal güvenlik numarasıyla eşleşebilir. .REG. \b\d{3}-\d{2}-\d{4}\b
\xhh	Belirli onaltılı kod ile bir ASCII karakterini gösterir (hh, iki basamaklı herhangi bir onaltılı değeri temsil eder).	\x7E(\w){6}, öncesinde bir ~ (yaklaşık) karakteri ile tam altı alfasayısal karakterli bir "kelime" içeren metin bloku ile eşleşir. Böylece '~ab12cd', '~Pa3499' sözcükleri eşleşebilir ancak '~oops' ile eşleşmez.

Kurallı İfade Oluşturucu

Veri Kaybını Önleme kurallarını nasıl yapılandıracağınıza karar verirken, kurallı ifade oluşturucunun aşağıdaki kurallara ve kısıtlamalara göre yalnızca basit ifadeler oluşturabileceğini göz önünde bulundurun:

- Yalnızca alfasayısal karakterler değişken olabilir.
- Diğer tüm karakterler, örneğin [-], [/], vb. yalnızca sabit olabilir.
- Değişken aralığı yalnızca A-Z ve 0-9 arasında olabilir; örneğin aralığı A-D biçiminde sınırlayamazsınız.
- Bu aracın oluşturduğu kurallı ifadeler küçük/büyük harf duyarlıdır.

- Bu aracın oluşturduğu kurallı ifadeler yalnızca pozitif eşleşme yapabilir, negatif eşleşme yapamaz ("eşleşme olmazsa").
- Örneğinize dayanan ifadeler yalnızca örneğinizle aynı sayıdaki karakterlerle ve boşluklarla eşleşebilir; bu araç belirtilen karakter veya dizenin "bir veya birden fazlası" ile eşleşen kalıplar oluşturamaz.

Karmaşık İfade Söz Dizimi

Anahtar sözcük, ifadeyi içerikle eşleştirmek için kullanılan en küçük birim olan sembollerden oluşur. Sembol; bir operatör, mantıksal bir sembol veya işlenen, yani operatörün üzerinde çalıştığı argüman veya değer olabilir.

.AND., .OR., .NOT., .NEAR., .OCCUR., .WILD., ".(." ve " .)." operatörlerden birkaçıdır. İşlenenle operatörün bir boşlukla ayrılması gerekir. Bir işlenen de çeşitli semboller içerebilir. Bkz. *Anahtar Sözcükler sayfa D-5*.

Çalışmada Kurallı İfadeler

Aşağıdaki örnekte, varsayılan filtrelerden biri olan Sosyal Güvenlik içerik filtresinin nasıl çalıştığı açıklanmaktadır:

[Format] .REG. \b\d{3}-\d{2}-\d{4}\b

Yukarıdaki ifadede; geri alma karakteri olan \b, ardından da herhangi bir basamak olan \d ve basamak sayısını belirten {x}, son olarak da bir tire olan - karakteri kullanılmaktadır. Bu ifadeler sosyal güvenlik numarasıyla eşleşir. Aşağıdaki tabloda, örnek kurallı ifadeyle eşleşen dizeler açıklanmaktadır:

TABLO D-8. Sosyal Güvenlik Kurallı İfadesi ile Eşleşen Sayılar

.REG. \b\d{3}-\d{2}-\d{4}\b	
333-22-4444	Eşleştir
333224444	Bir eşleşme değil
333 22 4444	Bir eşleşme değil
3333-22-4444	Bir eşleşme değil
333-22-44444	Bir eşleşme değil

İfadeyi şu şekilde değiştirirseniz,

[Format] .REG. \b\d{3}\x20\d{2}\x20\d{4}\b

yeni ifade aşağıdaki sırayla eşleşir:

333 22 4444

Tarama Dışlama Listeleri

Security Agent'lar için Tarama Dışlama Listesi

Bu dışlama listesi, tarama işleminden varsayılan olarak dışlanan tüm Trend Micro ürünlerini içerir.

TABLO D-9. Security Agent Dışlama Listesi

ÜRÜN ADI	YÜKLEME YOLU KONUMU
InterScan eManager 3.5x	HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\InterScan eManager \CurrentVersion ProgramDirectory=
ScanMail eManager (ScanMail for Microsoft Exchange eManager) 3.11, 5.1, 5.11, 5.12	HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\ScanMail for Microsoft Exchange eManager\CurrentVersion ProgramDirectory=
ScanMail for Lotus Notes (SMLN) eManager NT	HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\ScanMail for Lotus Notes\CurrentVersion AppDir= DataDir= IniDir=
InterScan Web Security Suite (IWSS)	HKEY_LOCAL_MACHINE\Software\TrendMicro\Interscan Web Security Suite Program Dizini= C:\Program Files\Trend Micro\IWSS

ÜRÜN ADI	YÜKLEME YOLU KONUMU
InterScan WebProtect	HKEY_LOCAL_MACHINE SOFTWARE\TrendMicro\InterScan WebProtect \CurrentVersion ProgramDirectory=
InterScan FTP VirusWall	HKEY_LOCAL_MACHINE SOFTWARE\TrendMicro\ InterScan FTP VirusWall\CurrentVersion ProgramDirectory=
InterScan Web VirusWall	HKEY_LOCAL_MACHINE SOFTWARE\TrendMicro\ InterScan Web VirusWall\CurrentVersion ProgramDirectory=
InterScan E-Mail VirusWall	HKEY_LOCAL_MACHINE SOFTWARE\TrendMicro\ InterScan E-Mail VirusWall\CurrentVersion ProgramDirectory={Installation Drive}:\INTERS~1
InterScan NSAPI Plug-In	HKEY_LOCAL_MACHINE SOFTWARE\TrendMicro\ InterScan NSAPI Plug-In\CurrentVersion ProgramDirectory=
InterScan E-Mail VirusWall	HKEY_LOCAL_MACHINE SOFTWARE\TrendMicro\ InterScan E-Mail VirusWall \CurrentVersion ProgramDirectory=
IM Security (IMS)	HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\IM Security \CurrentVersion HomeDir= VSQuarantineDir= VSBackupDir= FBArchiveDir= FTCFArchiveDir=

ÜRÜN ADI	YÜKLEME YOLU KONUMU
ScanMail for Microsoft Exchange (SMEX)	HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\ScanMail for Microsoft Exchange\CurrentVersion TempDir= DebugDir= HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\ScanMail for Microsoft Exchange\RealTimeScan\ScanOption BackupDir= MoveToQuarantineDir= HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\ScanMail for Microsoft Exchange\RealTimeScan\ScanOption\Advance QuarantineFolder= HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\ScanMail for Microsoft Exchange\RealTimeScan\IMCScan\ScanOption BackupDir= MoveToQuarantineDir= HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\ScanMail for Microsoft Exchange\RealTimeScan\IMCScan\ScanOption\Advance QuarantineFolder=

ÜRÜN ADI	YÜKLEME YOLU KONUMU
ScanMail for Microsoft Exchange (SMEX)	HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\ScanMail for Microsoft Exchange\ManualScan\ScanOption BackupDir= MoveToQuarantineDir= HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\ScanMail for Microsoft Exchange\QuarantineManager QMDir= HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\ScanMail for Microsoft Exchange\CurrentVersion\HomeDir'den exclusion.txt dosyasının yolunu alın HomeDir yoluna (örneğin, C:\Program Files\Trend Micro\Messaging Security Agent\) gidin exclusion.txt dosyasını açın C:\Program Files\Trend Micro\Messaging Security Agent\Temp\ C:\Program Files\Trend Micro\Messaging Security Agent\storage\quarantine\ C:\Program Files\Trend Micro\Messaging Security Agent\storage\backup\ C:\Program Files\Trend Micro\Messaging Security Agent\storage\archive\ C:\Program Files\Trend Micro\Messaging Security Agent\SharedResPool

Messaging Security Agent için Tarama Dışlama Listeleri (Yalnızca Advanced)

Messaging Security Agent, Microsoft Exchange server'a (2000 veya sonrası) yüklendiğinde varsayılan olarak Microsoft Exchange veritabanlarını, Microsoft Exchange günlük dosyalarını, Sanal sunucu klasörlerini veya M:\ sürücüsünü taramayacaktır. Dışlama listesinin kaydedildiği konum:

HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\PC-cillinNTCorp\CurrentVersion\Misc.

ExcludeExchangeStoreFiles=C:\Program Files\Exchsrvr\mdbdata\

priv1.stm|C:\Program Files\Exchsrvr\mdbdata\

priv1.edb|C:\Program Files\Exchsrvr\mdbdata\

pub1.stm|C:\Program Files\Exchsrvr\mdbdata\pub1.edb

ExcludeExchangeStoreFolders=C:\Program Files\Exchsrvr\mdbdata\

|C:\Program Files\Exchsrvr\Mailroot\vsi 1\Queue\

|C:\Program Files\Exchsrvr\Mailroot\vsi 1\PickUp\

|C:\Program Files\Exchsrvr\Mailroot\vsi 1\BadMail\

Microsoft Exchange'in önerdiği diğer klasörleri, lütfen tarama dışlama listesine manuel olarak ekleyin. Bkz. http://support.microsoft.com/kb/245822/.

SBS 2003 Dışlamaları

SBS 2003 için aşağıdakileri manuel olarak ekleyin:

Microsoft Exchange dışlamaları	
Microsoft Exchange Server Veritabanı	C:\Program Files\Exchsrvr\MDBDATA
Microsoft Exchange MTA dosyaları	C:\Program Files\Exchsrvr\Mtadata
Microsoft Exchange İleti izleme günlük dosyaları	C:\Program Files\Exchsrvr\server_name.log
Microsoft Exchange SMTP Mailroot	C:\Program Files\Exchsrvr\Mailroot
Microsoft Exchange çalışma dosyaları	C:\Program Files\Exchsrvr\MDBDATA
Site Çoğaltma Hizmeti	C:\Program Files\Exchsrvr\srsdata C:\Program Files\Exchsrvr\conndata
IIS Dışlamaları	

IIS Sistem Dosyaları	C:\WINDOWS\system32\inetsrv
IIS Sıkıştırma Klasörü	C:\WINDOWS\IIS Geçici Sıkıştırılmış Dosyalar
Etki Alanı Denetleyicisi Dışlamaları	
Active Directory veritabanı dosyaları	C:\WINDOWS\NTDS
SYSVOL	C:\WINDOWS\SYSVOL
NTFRS Veritabanı Dosyaları	C:\WINDOWS\ntfrs
Windows SharePoint Services Dışlamaları	
Geçici SharePoint klasörü	C:\windows\temp\FrontPageTempDir
İstemci Masaüstü Klasör Dışlamaları	
Windows Update Store	C:\WINDOWS\SoftwareDistribution\DataStore
Ek Dışlamalar	
Kaldırılabilir Depolama Veritabanı (SBS Yedeklemesi tarafından kullanılır)	C:\Windows\system32\NtmsData
SBS POP3 bağlayıcısı Hatalı Posta	C:\Program Files\Microsoft Windows Small Business Server \Networking\POP3\Failed Mail
SBS POP3 bağlayıcısı Gelen Posta	C:\Program Files\Microsoft Windows Small Business Server \Networking\POP3\Incoming Mail
Windows Update Store	C:\WINDOWS\SoftwareDistribution\DataStore
DHCP Veritabanı Deposu	C:\WINDOWS\system32\dhcp
WINS Veritabanı Deposu	C:\WINDOWS\system32\wins

Hizmet Paketi

Bir hizmet paketi, ürün yükseltmesi olabilecek ölçüde önemli olan ve düzeltme, yama ve özellik geliştirmelerinden oluşan bir konsolidasyondur. Hem Windows hem de Windows dışındaki hizmet paketleri, bir Kurulum programı ve kurulum komut dosyası içerir.

Truva Atı Bağlantı Noktası

Truva Atı bağlantı noktaları, Truva atı programları tarafından istemcilerbağlanmak için yaygın biçimde kullanılır. Bir salgın sırasında, WFBS Truva Atı programlarının kullanabileceği şu bağlantı noktası numaralarını engeller:

TABLO D-10. Truva Atı Bağlantı Noktaları

BAĞLANTI NOKTASI NUMARASI	TRUVA ATI PROGRAMI	BAĞLANTI NOKTASI NUMARASI	TRUVA ATI PROGRAMI
23432	Asylum	31338	Net Spy
31337	Back Orifice	31339	Net Spy
18006	Back Orifice 2000	139	Nuker
12349	Bionet	44444	Prosiak
6667	Bionet	8012	Ptakks
80	Codered	7597	Qaz
21	DarkFTP	4000	RA
3150	Deep Throat	666	Ripper
2140	Deep Throat	1026	RSM
10048	Delf	64666	RSM
23	EliteWrap	22222	Rux
6969	GateCrash	11000	Senna Spy

Bağlantı Noktası Numarası	Truva Atı Programı	Bağlantı Noktası Numarası	Truva Atı Programı
7626	Gdoor	113	Shiver
10100	Gift	1001	Silencer
21544	Girl Friend	3131	SubSari
7777	GodMsg	1243	Sub Seven
6267	GW Girl	6711	Sub Seven
25	Jesrto	6776	Sub Seven
25685	Moon Pie	27374	Sub Seven
68	Mspy	6400	Thing
1120	Net Bus	12345	Valvo line
7300	Net Spy	1234	Valvo line

Temizlenemeyen Dosyalar

Virüs Tarama Motoru aşağıdaki dosyaları temizleyemedi:

Tablo D-11. Temizlenemeyen Dosya Çözümleri

Temizlenemeyen Dosya	Açıklama ve Çözüm
Truva atı ile etkilenmiş dosyalar	Truva atları, ileti görüntüleme, dosyaları silme veya diskleri biçimlendirme gibi, genellikle kötü amaçlı olan beklenmedik ve yetkisiz eylemler gerçekleştiren programlardır. Truva atları dosyaları etkilemez ve dolayısıyla temizleme işlemi de gerekmez. Çözüm: Hasar Temizleme Motoru ve Hasar Temizleme Şablonu, Truva atlarını kaldırır.
Solucan bulaşan dosyalar	Bilgisayar solucanı, kendisinin veya bir kısmının işlevsel kopyalarını başka istemci sistemlerine yayabilen, kendi içinde bir

Temizlenemeyen Dosya	Açıklama ve Çözüm
	program veya program grubudur. Yayılma genellikle ağ bağlantıları veya e-posta ekleri aracılığıyla gerçekleşir. Solucanlar, dosya kendi içinde bir program olduğundan temizlenemez. Çözüm: Trend Micro solucanların silinmesini önerir.
Yazma korumalı etkilenmiş dosyalar	Çözüm: Dosyanın temizlemesine imkan sağlamak için yazma korumasını kaldırın.
Parola korumalı dosyalar	Parola korumalı dosyalar, parola korumalı sıkıştırılmış dosyaları veya parola korumalı Microsoft Office dosyalarını içerir. Çözüm: Dosyanın temizlemesine imkan sağlamak için parola korumasını kaldırın.
Yedek dosyaları	RB0~RB9 uzantısına sahip dosyalar, etkilenmiş dosyaların yedek kopyasıdır. Temizleme işlemi, temizleme işlemi sırasında virüsün/kötü amaçlı yazılımın dosyaya zarar vermesi olasılığına karşı, etkilenmiş dosyanın yedeğini oluşturur. Çözüm: Etkilenmiş dosyalar başarılı şekilde temizlenirse, yedek kopyayı saklamanız gerekmez. istemci normal şekilde işliyorsa, yedek dosyayı silebilirsiniz.
Geri Dönüşüm Kutusu'ndaki etkilenmiş dosyalar	Sistem çalıştığı için, Geri Dönüşüm Kutusu'ndaki etkilenen dosyaların kaldırılmasına sistem izin vermeyebilir.

	NTFS Dosya Sistemine Sahip Windows XP veya Windows Server 2003 üzerinde Çözüm:
	
	1. istemci'de Yönetici ayrıcalığıyla oturum açın.
	2. Uygulamaların dosyayı kilitlemesini engellemek için, çalışan tüm uygulamaları kapatın; böyle bir durumda Windows dosyayı silemez.
	3. Komut istemini açın.
	4. Dosyaları silmek için şunları yazın:
	
	`cd \`
	
	`cd recycled`

Temizlenemeyen Dosya	Açıklama ve Çözüm
	`del *.* /S` Son komut Geri Dönüşüm Kutusu'ndaki tüm dosyaları siler. 5. Dosyaların kaldırılmış olduğunu kontrol edin.

	Diğer işletim sistemlerindeki çözüm (veya NTFS olmayan):
	1. istemci'i MS-DOS modunda yeniden başlatın.
	2. Komut istemini açın.
	3. Dosyaları silmek için şunları yazın:
	`cd \`
	`cd recycled`
	`del *.* /S`
	Son komut Geri Dönüşüm Kutusu'ndaki tüm dosyaları siler.

Windows Temp klasöründeki veya Internet Explorer geçici klasöründeki etkilenmiş dosyalar	Sistem, istemci tarafından kullanıldığı için Windows Temp klasöründeki veya Internet Explorer geçici klasöründeki etkilenen dosyaların temizlenmesine izin vermeyebilir. Temizlenecek dosyalar, Windows'un çalışması için gerekli olan geçici dosyalar olabilir.
	NTFS Dosya Sistemine Sahip Windows XP veya Windows Server 2003 üzerinde Çözüm: 1. istemci'de Yönetici ayrıcalığıyla oturum açın. 2. Uygulamaların dosyayı kilitlemesini engellemek için, çalışan tüm uygulamaları kapatın; böyle bir durumda Windows dosyayı silemez. 3. Etkilenen dosya Windows Temp klasöründeyse: a. Komut istemini açın ve Windows Temp klasörüne gidin (varsayılan olarak Windows XP veya Windows Server 2003 istemciler için C:\Windows\Temp konumundadır). b. Dosyaları silmek için şunları yazın: `cd temp`

Temizlenemeyen Dosya	Açıklama ve Çözüm

	`attrib -h`
	
	`del *.* /S`
	
	Son komut Windows Temp klasöründeki tüm dosyaları siler.
	
	4. Etkilenen dosya Internet Explorer geçici klasöründeyse:
	
	a. Komut istemini açın ve Internet Explorer Temp klasörüne gidin (varsayılan olarak, Windows XP veya Windows Server 2003 istemciler için C:\Documents and Settings\<Kullanıcı adınız>\Local Settings\Temporary Internet Files konumundadır).
	
	b. Dosyaları silmek için şunları yazın:
	
	`cd tempor~1`
	
	`attrib -h`
	
	`del *.* /S`
	
	Son komut, Internet Explorer geçici klasöründeki tüm dosyaları siler.
	
	c. Dosyaların kaldırılmış olduğunu kontrol edin.

	Diğer işletim sistemlerindeki çözüm (veya NTFS olmayan):
	
	1. istemci'i MS-DOS modunda yeniden başlatın.
	
	2. Etkilenen dosya Windows Temp klasöründeyse:
	
	a. Komut istemini açın ve Windows Temp klasörüne gidin (varsayılan olarak Windows XP veya Windows Server 2003 istemciler için C:\Windows\Temp konumundadır).
	
	b. Dosyaları silmek için şunları yazın:
	
	`cd temp`
	
	`attrib -h`
	
	`del *.* /S`
	
	Son komut Windows Temp klasöründeki tüm dosyaları siler.

Temizlenemeyen Dosya	Açıklama ve Çözüm

	c. istemci makineyi normal modda yeniden başlatın.
	3. Etkilenen dosya Internet Explorer geçici klasöründeyse:
	a. Komut istemini açın ve Internet Explorer Temp klasörüne gidin (varsayılan olarak, Windows XP veya Windows Server 2003 istemciler için C:\Documents and Settings\<Kullanıcı adınız>\Local Settings\Temporary Internet Files konumundadır).
	b. Dosyaları silmek için şunları yazın:
	`cd tempor~1`
	`attrib -h`
	`del *.* /S`
	Son komut, Internet Explorer geçici klasöründeki tüm dosyaları siler.
	c. istemci makineyi normal modda yeniden başlatın.

Desteklenmeyen bir sıkıştırma biçimi kullanılarak sıkıştırılan dosyalar	Çözüm: Sıkıştırılmış dosyaları açın.
Kilitlenmiş dosyalar veya halen çalışan dosyalar	Çözüm: Dosyaların kilidini açın veya dosyalar yürütülene kadar bekleyin.
Bozulmuş dosyalar	Çözüm: Dosyaları silin.

Dizin

A

ActiveAction, 7-15
ActiveX zararlı kodu, 1-24
ağ virüsü, 5-10
akıllı koruma, 1-19
    File Reputation Hizmetleri, 1-19
    Smart Protection Network, 1-19
    Web Reputation Hizmetleri, 1-19
artımlı kalıp, 8-11
AutoPcc.exe, 3-9, 3-10, 3-14

B

Behavior Monitoring Algılama Kalıbı, 8-8
Behavior Monitoring Core Service, 8-8
Behavior Monitoring Driver, 8-8
Behavior Monitoring Yapılandırma Kalıbı, 8-8
belgeler, xii
belgelerin geribildirimi, C-6
bileşen çiftlemesi, 8-11
bileşenler, 8-3
Bilgi Bankası, C-2

C

casus yazılım/grayware, 1-25, 1-26
    casus yazılım, 1-25
    çeviriciler, 1-26
    korsanlık araçları, 1-26
    parola kırma uygulamaları, 1-26
    reklam yazılımı, 1-25
    şaka programları, 1-26
    uzaktan erişim araçları, 1-26
casus yazılım/grayware taraması
    eylemler, 7-14
Casus Yazılım Kalıbı, 8-7
Casus Yazılım Tarama Motoru, 8-7
Client Packager, 3-11, 3-16, 3-17
    ayarlar, 3-17
    dağıtım, 3-18
COM dosyası bulaştırıcısı, 1-24

Ç

Çakışan ARP, D-4
Çakışan Parça, D-5
Çok Büyük Parça, D-4

D

Davetsiz Misafir Algılama Sistemi, D-4
destek
    sorunları daha hızlı çözme, C-3
    TrendLabs, C-5
DHCP ayarları, 3-25
Dijital İmza Kalıbı, 8-9
dosya geçmişi, 1-19
Durum Tanı Aracı, C-3
düzeltmeler, 8-10

E

EICAR test virüsü, 1-25
EXE dosyası bulaştırıcısı, 1-24

G

geleneksel tarama, 5-4
Genel Güvenlik Duvarı Sürücüsü, 8-8
Gözyaşı, D-5
Güncelleme Aracısı, 3-5
Güvenlik Açığı Tarayıcısı, 3-11, 3-23
    bilgisayar açıklamasının alınması, 3-31
    DHCP ayarları, 3-25
    ping ayarları, 3-32

güvenlik duvarı
faydalar, 5-10
güvenlik ilkeleri
parola karmaşıklığı
gereksinimler, 6-56
güvenlik riskleri, 1-25, 1-26
casus yazılım/grayware, 1-25, 1-26
güvenlik yamaları, 8-10

H

harici aygıt koruması, 8-8
Hasar Temizleme Hizmetleri, 3-5
Hasar Temizleme Motoru, 8-7
HTML virüsü, 1-25

I

IDS, D-4
IntelliTrap Kalıbı, 8-6
IntelliTrap Kural Dışı Durum Kalıbı, 8-7
IPv6 desteği, B-2
IPv6 adreslerini görüntüleme, B-6
sınırlamalar, B-3, B-4

İ

iletişim kurma, C-2, C-6
belgelerin geribildirimi, C-6
Bilgi Bankası, C-2
Trend Micro, C-2
İlke Uygulama Kalıbı, 8-9
istemci yükleme
Client Packager, 3-16
Güvenlik Açığı Tarayıcısını kullanma, 3-23
Oturum Açma Komut Dizesi Kurulumu, 3-14
web konsolundan, 3-19

J

JavaScript virüsü, 1-25
Java zararlı kodu, 1-24

K

kaldırma
kaldırma programını kullanmak, 3-42
karantina dizini, 5-30, 14-10
kök kullanıcı takımı algılama, 8-8
Küçük Parça Saldırısı, D-5

L

LAND Saldırısı, D-5

M

makro virüs, 1-24

O

olası virüs/kötü amaçlı yazılım, 1-23
Oturum Açma Komut Dizesi Kurulumu, 3-9, 3-10, 3-14

Ö

Ölüm Pingi, D-4
önyükleme kesimi virüsü, 1-24

P

paketleyici, 1-24
Parçalanmış IGMP, D-5
parola karmaşıklığı, 6-56
Plug-in Manager, 3-5
programlar, 8-3

S

Security Agent yükleme yöntemleri, 3-9
Smart Protection Network, 1-19
smart scan, 5-4
solucan, 1-25
sunucu güncelleme

bileşen çiftlemesi, 8-11
manuel güncelleme, 8-13
zamanlanmış güncelleme, 8-14
SYN Taşması, D-4

Ş

şaka programı, 1-23
şifrelenmiş dosyalar, 14-9

T

tarama eylemleri
casus yazılım/grayware, 7-14
tarama türleri, 3-4
tarama yöntemi, 3-17
test virüsü, 1-25
TrendLabs, C-5
Trend Micro
Bilgi Bankası, C-2
Truva atı programı, 1-24, 8-7

U

uzaktan yükleme, 3-10

V

VBScript virüsü, 1-25
virüs/kötü amaçlı yazılım, 1-23–1-25
ActiveX zararlı kodu, 1-24
COM ve EXE dosyası bulaştırıcısı, 1-24
Java zararlı kodu, 1-24
makro virüs, 1-24
olası virüs/kötü amaçlı yazılım, 1-23
önyükleme kesimi virüsü, 1-24
paketleyici, 1-24
solucan, 1-25
şaka programı, 1-23
test virüsü, 1-25
Truva atı programı, 1-24
türleri, 1-23–1-25
VBScript, JavaScript veya HTML virüsü, 1-25
Virüs Ansiklopedisi, 1-23
Virüs Kalıbı, 8-6, 8-15
Virüs Tarama Motoru, 8-5
Virüs Temizleme Şablonu, 8-7

W

web konsolu, 2-4, 2-5
gereksinimler, 2-5
hakkında, 2-4
web reputation, 1-19, 3-4
web yükleme sayfası, 3-9
WFBS
belgeler, xii

Y

yamalar, 8-10
yeni özellikler, 1-2, 1-7, 1-16
yükleme öncesi görevler, 3-12, 3-20, 3-23

TREND MICRO INCORPORATED

Trend Micro EMEA Ltd. Turkiye Macka Cad. Yeni Macka Han No. 14 Kat. 3 Daire 4 Maçka Istanbul Turkiye

Telefon: +0212 2416100 info@trendmicro.com

www.trendmicro.com

Item Code: WFUM97097/150730