TS PLUS TÜRKİYE

ADVANCEDSECURITY

HIZLI BAŞLANGIÇ KILAVUZU

TSplus Advanced Security - Hızlı Başlangıç Kılavuzu

Türkiye pazarına özel Türkçe sürüm · 2026

Sunucunuzu güvenle koruyun.



TSPLUS TÜRKİYE · RESMİ DİJİTAL DOKÜMAN
tsplus.com.tr · sales@tsplus.com.tr

RESMÎ KAYNAK GÖRSELİ

TSplus Advanced Security - Activating your license

Step 1: Activating your license from Lite mode

Click on the "Trial License" button to purchase a license or on the License tab if you already have a license and an Activation Key.



Then, click on the "Activate your License" button .

You will find your permanent activation key **(XXXX-XXXX-XXXX-XXXX)** in our order confirmation email.

If you wish to activate your subscription, please enter your subscription key **(S-XXXX-XXXX-XXXX-XXXX)**.

TÜRKÇE İÇERİK

TSplus Advanced Security - Lisansınızı aktif hale getirmek

Adım 1: Lisansınızı Lite modundan etkinleştirin

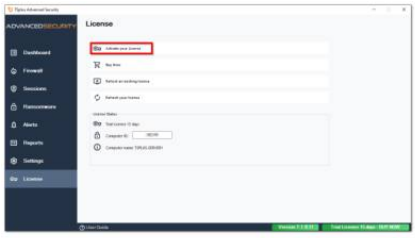
Lisans satın almak için "Deneme Lisansı" düğmesine veya lisansınız ve Aktivasyon Anahtarınız varsa Lisans sekmesine tıklayın.

Ardından, "Lisansını Etkinleştir" düğmesine tıklayın.

Sipariş onay e-postamızda kalıcı etkinleştirme anahtarınızı (XXXX-XXXX-XXXX-XXXX) bulacaksınız.

Aboneliğinizi etkinleştirmek istiyorsanız, lütfen abonelik anahtarınızı girin (S-XXXX-XXXX- XXXX-XXXX).

RESMÎ KAYNAK GÖRSELİ



If you do not know you activation key, please proceed to step 2. Otherwise, proceed to step 3.

Step 2: Retrieve your activation key from the Licensing portal

In order to get your Activation Key, connect to our Licensing Portal and enter your Email Address and your Order Number:

Download the Customer Portal User Guide for more information about your customer portal.

Your activation key will be displayed at the top of the dashboard:



Step 3: Select requested licences and Update &

TÜRKÇE İÇERİK

Etkinleştirme anahtarını bilmiyorsanız, lütfen 2. adıma geçin, aksi takdirde 3. adıma geçin.

Adım 2: Etkinleştirme anahtarınızı Lisanslama portalından alın

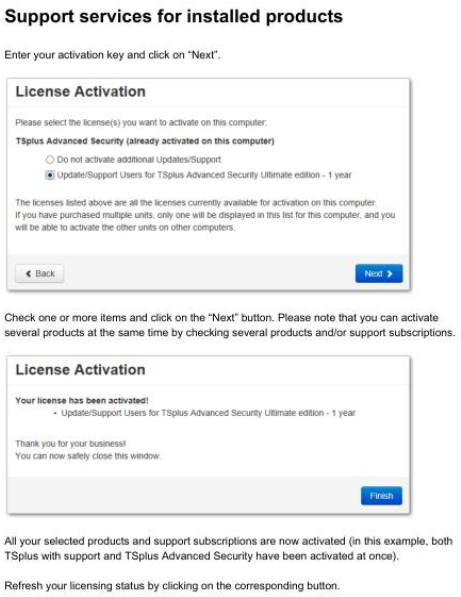
Aktivasyon Anahtarınızı almak için Lisanslama Portalımıza bağlanın ve E-posta Adresinizi ve Sipariş Numaranızı girin:

Müşteri portalınız hakkında daha fazla bilgi için Müşteri Portalı Kullanıcı Kılavuzu'nu indirin.

Etkinleştirme anahtarınız gösterge panelinin üst kısmında görüntülenecektir:

Adım 3: İstenen lisansları seçin ve Güncelle &

RESMÎ KAYNAK GÖRSELİ



TÜRKÇE İÇERİK

Kaynak sayfa 3/99

Kurulan ürünler için destek hizmetleri

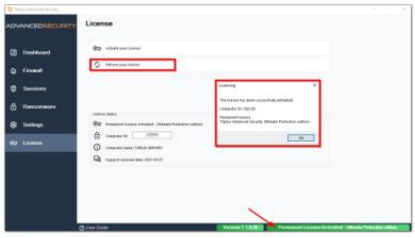
Etkinleştirme anahtarınızı girin ve "Sonraki" ye tıklayın.

Bir veya daha fazla öğeyi kontrol edin ve "Next" düğmesine tıklayın. Birkaç ürünü ve / veya destek aboneliklerini kontrol ederek aynı anda birkaç ürünü etkinleştirebileceğinizi lütfen unutmayın.

Tüm seçili ürünleriniz ve destek abonelikleriniz artık etkinleştirildi (bu örnekte, hem TSplus hem de TSplus Advanced Security bir kerede etkinleştirildi).

Lisanslama durumunuzu ilgili düğmeye tıklayarak yenileyin.

RESMÎ KAYNAK GÖRSELİ



Activating your license (Offline)

Please refer to the procedure described for TSplus Remote Access: Activating your TSplus License (Offline)

Rehosting your license

Please refer to the procedure described for TSplus Remote Access: Rehosting your TSplus License

Note:: You can download a license.lic file on the Licensing Portal for TSplus Advanced Security versions below. Please refer to the Customer Portal User Guide for more information.

Thank you for choosing TSplus Advanced Security!

TÜRKÇE İÇERİK

Lisansını etkinleştirme (Çevrimdışı)

Lütfen TSplus Remote Access için açıklanan prosedüre bakın: TSplus Lisansınızı Etkinleştirme (Çevrimdışı)

Lisansınızı yeniden barındırın

Lütfen TSplus Remote Access için açıklanan prosedüre bakın: TSplus Lisansınızı yeniden barındırın

Not:: Aşağıda TSplus Advanced Security sürümleri için Lisans Portalı'na lisans.lic dosyasını indirebilirsiniz. Daha fazla bilgi için lütfen Müşteri Portalı Kullanıcı Kılavuzu'na bakın.

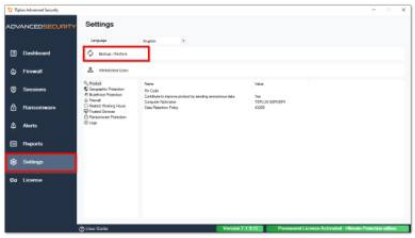
TSplus Advanced Security'ı seçtiğiniz için teşekkür ederiz!

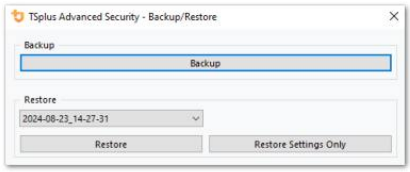
RESMÎ KAYNAK GÖRSELİ

Advanced - Backup and Restore

Backup and Restore Data and Settings

You can backup or restore TSplus Advanced Security's data and settings by clicking on the button "Backup / Restore" on the top:





The backup will be saved in the folder **archives** located in TSplus Advanced Security's setup

TÜRKÇE İÇERİK

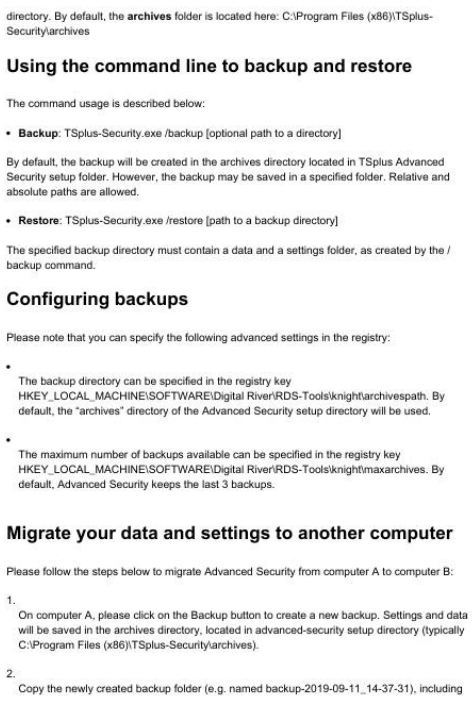
Gelişmiş - Yedekleme ve Geri Yükleme

Veri ve Ayarları Yedekleme ve Geri Yükleme

TSplus Advanced Security'ın verilerini ve ayarlarını, üstteki "Yedekle / Geri Yükle" düğmesine tıklayarak yedekleyebilir veya geri yükleyebilirsiniz:

Yedekleme, TSplus Advanced Security'ın kurulumunda bulunan klasör arşivlerine kaydedilecektir.

RESMÎ KAYNAK GÖRSELİ



directory. By default, the **archives** folder is located here: C:\Program Files (x86)\TSplus-Security\archives

Using the command line to backup and restore

The command usage is described below:

- **Backup**: TSplus-Security.exe /backup [optional path to a directory]

By default, the backup will be created in the archives directory located in TSplus Advanced Security setup folder. However, the backup may be saved in a specified folder. Relative and absolute paths are allowed.

- **Restore**: TSplus-Security.exe /restore [path to a backup directory]

The specified backup directory must contain a data and a settings folder, as created by the / backup command.

Configuring backups

Please note that you can specify the following advanced settings in the registry:

- The backup directory can be specified in the registry key HKEY_LOCAL_MACHINE\SOFTWARE\Digital River\RDS-Tools\knight\archivespath. By default, the "archives" directory of the Advanced Security setup directory will be used.
- The maximum number of backups available can be specified in the registry key HKEY_LOCAL_MACHINE\SOFTWARE\Digital River\RDS-Tools\knight\maxarchives. By default, Advanced Security keeps the last 3 backups.

Migrate your data and settings to another computer

Please follow the steps below to migrate Advanced Security from computer A to computer B:

1. On computer A, please click on the Backup button to create a new backup. Settings and data will be saved in the archives directory, located in advanced-security setup directory (typically C:\Program Files (x86)\TSplus-Security\archives).
2. Copy the newly created backup folder (e.g. named backup-2019-09-11_14-37-31), including

TÜRKÇE İÇERİK

Kaynak sayfa 6/99

directory. By default, the archives folder is located here: C:\Program Files (x86)\TSplus- Security\archives

Yedekleme ve geri yüklemek için komut satırının kullanılması

Komut kullanımı aşağıda açıklanmıştır:

Yedekleme: TSplus-Security.exe /backup [bir dizine isteğe bağlı yol]

Varsayılan olarak, yedekleme TSplus Advanced Security kurulum klasöründe bulunan arşiv dizininde oluşturulacaktır. Ancak, yedekleme belirtilen bir klasöre kaydedilebilir. Bağıl ve mutlak yollara izin verilir.

Geri Yükleme: TSplus-Security.exe /restore [bir yedekleme dizinine giden yol]

Belirtilen yedekleme dizini, / yedekleme komutu tarafından oluşturulduğu gibi bir veri ve ayarlar klasörü içermelidir.

Yedekleri yapılandırma

Kayıt defterinde aşağıdaki gelişmiş ayarları belirtebileceğinizi lütfen unutmayın:

The backup directory can be specified in the registry key HKEY_LOCAL_MACHINE\SOFTWARE\Digital River\RDS-Tools\knight\archivespath. By default, the "archives" directory of the Advanced Security setup directory will be used.

The maximum number of backups available can be specified in the registry key HKEY_LOCAL_MACHINE\SOFTWARE\Digital River\RDS-Tools\knight\maxarchives. By default, Advanced Security keeps the last 3 backups.

Veri ve ayarlarınızı başka bir bilgisayara taşıyın

Gelişmiş Güvenlik'i A bilgisayarından B bilgisayarına taşımak için lütfen aşağıdaki adımları izleyin:

1.

On computer A, please click on the Backup button to create a new backup. Settings and data will be saved in the archives directory, located in advanced-security setup directory (typically C:\Program Files (x86)\TSplus-Security\archives). 2.

Yeni oluşturulan yedekleme klasörünü kopyalayın (örn.: yedeği 2019-09-11_14-37-31), dahil olmak üzere

RESMÎ KAYNAK GÖRSELİ

all content, from the archives directory on computer A to the archives directory on computer B.

3. On computer B, from the Backup / Restore window, in the “Restore” section, select the relevant backup name to be restored.

4. Then, click on Restore Settings Only to restore the settings. Alternatively, it is possible to click on Restore to restore all data and settings, which is not recommended for a migration but useful to restore advanced-security on computer A.

5. Please wait at most 2 minutes for the settings to be reloaded by advanced-security features.

Database

A database stores Events, IP addresses, Ransomware attacks reports and programs whitelists.

This database is stored in **data** folder located in TSplus Advanced Security's setup directory.

- Advanced Security from version 5 and prior to version 5.3.10.6 uses a LiteDB database engine.
- Advanced Security above version 5.3.10.6 uses a SQLite database engine.



TÜRKÇE İÇERİK

Kaynak sayfa 7/99

A bilgisayarındaki arşiv dizininden B bilgisayarındaki arşiv dizine kadar tüm içerikler. 3.

B bilgisayarında, Yedekleme / Geri Yükleme penceresinden, "Geri Yükle" bölümünde, geri yüklenecek ilgili yedekleme adını seçin. 4.

Ardından, ayarları geri yüklemek için yalnızca Geri Yükleme Ayarlarını tıklayın. Alternatif olarak, bir göç için tavsiye edilmeyen ancak bilgisayar A. 5'te gelişmiş güvenliği geri yüklemek için kullanışlı olan tüm veri ve ayarları Geri Yükleme'ye tıklamak mümkündür.

Lütfen ayarların gelişmiş güvenlik özellikleri tarafından yeniden yüklenmesi için en fazla 2 dakika bekleyin.

Veritabanı

Bir veritabanı Olayları, IP adreslerini, Ransomware saldırı raporlarını ve programları beyaz listelerini saklar.

Bu veritabanı, TSplus Advanced Security'ın kurulum dizininde bulunan veri klasöründe saklanır.

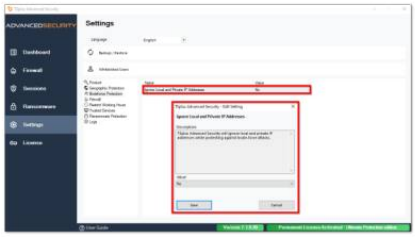
Sürüm 5'ten ve sürüm 5.3.10.6'dan önceki Gelişmiş Güvenlik, LiteDB veritabanı motorunu kullanır.

5.3.10.6 sürümünün üzerindeki Gelişmiş Güvenlik, bir SQLite veritabanı motoru kullanır.

RESMÎ KAYNAK GÖRSELİ

Advanced - Bruteforce Protection

The **Bruteforce Protection** tab allows you to Ignore Local and Private IP Addresses if you wish to, by changing the default value from "No" to "Yes".



TÜRKÇE İÇERİK

Gelişmiş - Bruteforce Koruma

Bruteforce Koruma sekmesi, varsayılan değeri "Hayır"dan "Evet" e değiştirerek, isterseniz Yerel ve Özel IP Adreslerini Görmezden Gelmenizi sağlar.

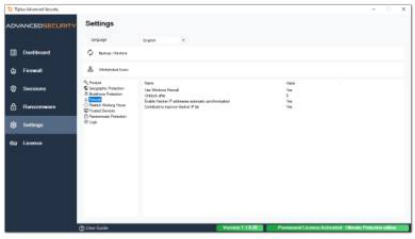
RESMÎ KAYNAK GÖRSELİ

Advanced - Firewall

The **Firewall** tab allows you to activate the **Windows Firewall or deactivate it in favor of the TSplus Advanced Security built-in firewall**.

Since version 4.4, a built-in firewall is included in TSplus Advanced Security.

As a general guidance, if Windows Firewall is activated on your server, then you should use it to enforce TSplus Advanced Security rules (default). If you installed another firewall, then you must activate TSplus Advanced Security built-in firewall.



Use Windows Firewall In order to activate the built-in firewall, go to Settings > Advanced > Product > Use Windows Firewall and set the value to: No If Yes, then the offending IP addresses will be blocked using Windows Firewall. TSplus Advanced Security firewall will be used otherwise.

Unblock after Change this setting to automatically unblock IP addresses after a certain amount of time (in minutes). Default value is 0, disabling this feature. Value: 0

Enable Hacker IP addresses automatic synchronization Keep your machine protected against known threats such as on-line attacks, on-line service abuse, malware, botnets and other electronic activities with the Hacker IP Protection Support and Updates Services subscription is

TÜRKÇE İÇERİK

Gelişmiş - Güvenlik Duvarı

Güvenlik Duvarı sekmesi, Windows Güvenlik Duvarı'nı etkinleştirmenize veya TSplus Advanced Security yerleşik güvenlik duvarı lehine devre dışı bırakmanıza izin verir.

Sürüm 4.4'ten bu yana, TSplus Advanced Security'a yerleşik bir güvenlik duvarı dahildir.

Genel bir kılavuz olarak, Windows Firewall sunucunuzda etkinleştirilirse, bunu TSplus Advanced Security kurallarını uygulamak için kullanmalısınız (varsayılan). Başka bir güvenlik duvarı yüklediyseniz, o zaman TSplus Advanced Security yerleşik güvenlik duvarını etkinleştirmeniz gerekir.

Windows Firewall'ı kullanın Yerleşik güvenlik duvarını etkinleştirmek için Ayarlar> Gelişmiş> Ürün > Windows Güvenlik Duvarı'nı kullanın ve değeri şu şekilde ayarlayın: Hayır Evet ise, rahatsız edici IP adresleri Windows Güvenlik Duvarı kullanılarak engellenecektir. TSplus Advanced Security güvenlik duvarı aksi takdirde kullanılacaktır.

Belirli bir süre sonra (dakikada) IP adreslerinin engelini otomatik olarak kaldırmak için bu ayarı değiştirdikten sonra engellemeyi kaldır. Varsayılan değer 0'dır, bu özelliği devre dışı bırakır. Değer: 0

Hacker IP adreslerini otomatik senkronizasyonu etkinleştir Makinenizi, Hacker IP Koruma Desteği ve Güncellemeleri Hizmetleri aboneliği ile çevrimiçi saldırılar, çevrimiçi hizmet kötüye kullanımı, kötü amaçlı yazılımlar, botnetler ve diğer elektronik faaliyetler gibi bilinen tehditlere karşı korumalı tutun

RESMÎ KAYNAK GÖRSELİ



required. Value: Yes

Contribute to improve Hacker IP list Allow TSplus Advanced Security to send anonymous usage statistics to enhance protection against Hacker IP.
Value: Yes

TÜRKÇE İÇERİK

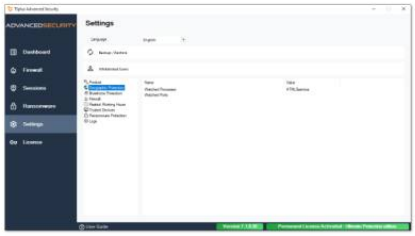
gerekli. Değer: Evet

Hacker IP listesinin geliştirilmesine katkıda bulunun TSplus Advanced Security'ın Hacker IP'ye karşı korumayı artırmak için anonim kullanım istatistikleri göndermesine izin verin. Değer: Evet

RESMÎ KAYNAK GÖRSELİ

Advanced - Geographic Protection

The **Geographic Protection** tab allows you to add or remove processes that are watched by the Geographic Protection feature.



By default, the HTML5 service is watched.

The **Watched Ports** settings allows you to add ports watched by the Geographic Protection feature. By default, Geographic Protection listens to default ports used for connecting remotely to a server. These ports include RDP (3389), Telnet (23) and VNC ports. Geographic Protection supports the following VNC providers: Tight VNC, Ultra VNC, Tiger VNC and Real VNC, which are not related whatsoever with TSplus.

TÜRKÇE İÇERİK

Gelişmiş - Coğrafi Koruma

Coğrafi Koruma sekmesi, Coğrafik Koruma özelliği tarafından izlenen işlemleri eklemenize veya kaldırmanıza olanak tanır.

Varsayılan olarak HTML5 hizmeti izlenir.

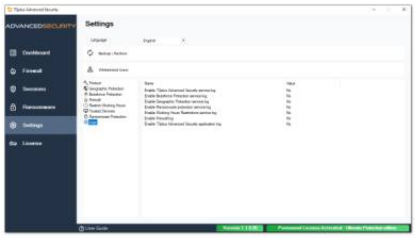
İzlenen Portlar ayarları, Coğrafi Koruma özelliği tarafından izlenen portları eklemenize olanak tanır. Varsayılan olarak, Coğra Koruma, bir sunucuya uzaktan bağlanmak için kullanılan varsayılan portları dinler. Bu portlar arasında RDP (3389), Telnet (23) ve VNC portları bulunur. Coğrafik Koruma, TSplus ile herhangi bir şekilde ilgili olmayan aşağıdaki VNC sağlayıcıları destekler: Sıkı VNC, Ultra VNC, Tiger VNC ve Gerçek VNC.

RESMÎ KAYNAK GÖRSELİ

Advanced - Logs

The **Logs** tab allows you to enable or disable service and features logs. Logs exist to find more easily the origin of the errors encountered on TSplus Advanced Security.

To retrieve the logs, open an Explorer and browse to the **logs** folder of TSplus Advanced Security's setup directory. By default, logs will be located here: **C:\Program Files (x86)\TSplus-Security\logs**



Enable or disable TSplus Advanced Security service and application logs, which are respectively the global configuration service that runs in the background and the log for the application interface.

You can also enable logs corresponding to the respective TSplus Advanced Security's features:

- Service
- Bruteforce Protection
- Geographic Protection
- Ransomware Protection
- Restrict Working Hours
- Firewall..
- Application

TÜRKÇE İÇERİK

Kaynak sayfa 12/99

Gelişmiş - Günlükler

Günlükler sekmesi, hizmet ve özellik günlüklerini etkinleştirmenize veya devre dışı bırakmanıza olanak tanır. Kayıtlar, TSplus Advanced Security'ta karşılaşılan hataların kökenini daha kolay bulmak için mevcuttur.

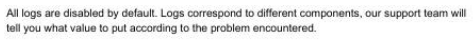
To retrieve the logs, open an Explorer and browse to the logs folder of TSplus Advanced Security's setup directory. By default, logs will be located here: C:\Program Files (x86)\TSplus-Security\logs

TSplus Advanced Security hizmet ve uygulama günlüklerini etkinleştirin veya devre dışı bırakın, bunlar sırasıyla arka planda çalışan küresel yapılandırma hizmeti ve uygulama arayüzü için günlüktür.

Ayrıca, ilgili TSplus Advanced Security'ın özelliklerine karşılık gelen günlükleri etkinleştirebilirsiniz:

Hizmet Bruteforce Koruma Coğrafi Koruma Ransomware Koruma Kısıtlama Çalışma Saatleri Güvenlik Duvarı.. Uygulama

RESMÎ KAYNAK GÖRSELİ



TÜRKÇE İÇERİK

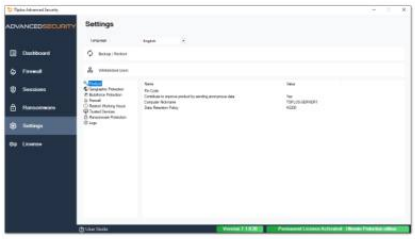
Kaynak sayfa 13/99

Tüm günlükler varsayılan olarak devre dışı bırakılır. Günlükler farklı bileşenlere karşılık gelir, destek ekibimiz karşılaştığı soruna göre hangi değeri koyacağınızı size söyleyecektir.

RESMÎ KAYNAK GÖRSELİ

Advanced - Product

The **Product** tab allows you to add a PIN code to the application:



Click on Save. The PIN code will be required the next time you will start the application.

You can also **contribute to improve the product**, by sending anonymous data (enabled by default): YES

The following data will be collected in case of a Ransomware attack:

- TSplus Advanced Security's version.
- Windows version.
- Suspected files'paths that lead to the ransomware attack.

Modifying the **Computer nickname** is also possible.

The **Data Retention Policy** defines the period of time after which TSplus Advanced Security's events are removed from the database. A backup is performed before each database cleanup. This policy is defined in minutes. Default data retention policy is 259 200 minutes, or 6 months.

TÜRKÇE İÇERİK

Gelişmiş - Ürün

Ürün sekmesi, uygulamaya bir PIN kodu eklemenize izin verir:

Kaydet'e tıklayın. Bir dahaki sefere uygulamayı başlatacağınızda PIN kodu gerekecektir.

Ayrıca, anonim veri göndererek (varsayılan olarak etkinleştirilir): EVET

Aşağıdaki veriler bir Ransomware saldırısı durumunda toplanacaktır:

TSplus Advanced Security'ın sürümü. Windows sürümü. Ransomware saldırısına yol açan şüpheli dosyaların yolları.

Bilgisayar takma adını değiştirmek de mümkündür.

Veri Tutma Politikası, TSplus Advanced Security'ın olaylarının veri tabanından kaldırıldığı süreyi tanımlar. Her veritabanı temizleme işleminden önce bir yedekleme yapılır. Bu politika dakikalar içinde tanımlanır. Varsayılan veri saklama politikası 259 200 dakika veya 6 aydır.

RESMÎ KAYNAK GÖRSELİ

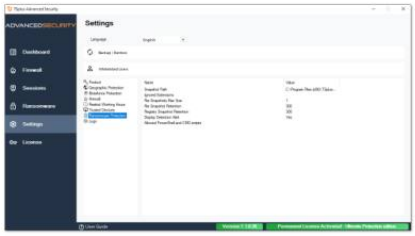
TÜRKÇE İÇERİK

Kaynak sayfa 15/99

RESMÎ KAYNAK GÖRSELİ

Advanced - Ransomware Protection

The **Ransomware Protection** tab allows you to configure the snapshot properties and define ignored file extensions for the Ransomware Protection feature.



Snapshot Path: Define the directory where Ransomware Protection stores file snapshots.

Default value is: C:\Program Files (x86)\TSplus-Security\snapshots

Ignored Extensions: By default, Ransomware Protection ignores well-known extensions of temporary files for ransomware activity. See the list here. You can define custome extension names on the value field (semicolon separated):

File Snapshot Max Size: File Snapshots Max Size defines the maximum space allowed to retain file snapshots.

The size is expressed in percentage of total available space on the disk where Snapshot Path resides.

File Snapshot Retention: File Snapshot Retention defines, in seconds, the retention policy of a file snapshot.

TÜRKÇE İÇERİK

Gelişmiş - Ransomware Koruma

Ransomware Koruma sekmesi, anlık görüntü özelliklerini yapılandırmanıza ve Ransombustan Korunma özelliği için göz ardı edilen dosya uzantılarını tanımlamanıza olanak tanır.

Snapshot Path: Ransomware Protection'ın dosya anlık görüntülerini sakladığı dizini tanımlayın.

Default value is: C:\Program Files (x86)\TSplus-Security\snapshots

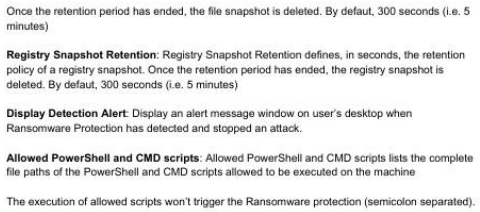
Göz ardı Uzantıları: Varsayılan olarak, Ransomware Koruması fidye yazılımı etkinliği için geçici dosyaların iyi bilinen uzantılarını görmezden gelir. Listeye buradan bakın. Değer alanında özel uzantı adlarını tanımlayabilirsiniz (semicolon ayrılmış):

File Snapshot Max Size: File Snapshots Max Size, dosya anlık görüntülerini saklamak için izin verilen maksimum alanı tanımlar.

Boyut, Snapshot Path'in bulunduğu diskteki toplam kullanılabilir alanın yüzdesiyle ifade edilir.

Dosya Snapshot Tutma: Dosya Snapshot Saklama, saniyeler içinde bir dosya anlık görüntüsünün tutma politikasını tanımlar.

RESMÎ KAYNAK GÖRSELİ



Once the retention period has ended, the file snapshot is deleted. By defaut, 300 seconds (i.e. 5 minutes)

Registry Snapshot Retention: Registry Snapshot Retention defines, in seconds, the retention policy of a registry snapshot. Once the retention period has ended, the registry snapshot is deleted. By defaut, 300 seconds (i.e. 5 minutes)

Display Detection Alert: Display an alert message window on user's desktop when Ransomware Protection has detected and stopped an attack.

Allowed PowerShell and CMD scripts: Allowed PowerShell and CMD scripts lists the complete file paths of the PowerShell and CMD scripts allowed to be executed on the machine

The execution of allowed scripts won't trigger the Ransomware protection (semicolon separated).

TÜRKÇE İÇERİK

Tutma süresi sona erdikten sonra dosya anlık görüntüsü silinir. Defaut ile 300 saniye (yani 5 dakika)

Kayıt Snapshot Tutma: Kayıt Snapshot Saklama, saniyeler içinde bir kayıt defteri anlık görüntüsünün saklama politikasını tanımlar. Tutma süresi sona erdiğinde, kayıt defteri anlık görüntüsü silinir. Defaut tarafından, 300 saniye (yani 5 dakika)

Ekran Algılama Uyarısı: Ransomware Koruması bir saldırı tespit edip durdurduğunda kullanıcının masaüstünde bir uyarı mesajı penceresi görüntüler.

İzin verilen PowerShell ve CMD betikleri: Makinede çalıştırılmasına izin verilen PowerSell ve CMD scriptlerinin tüm dosya yollarını listeler.

İzin verilen betiklerin yürütülmesi Ransomware korumasını tetiklemez (semicolon ayrılmış).

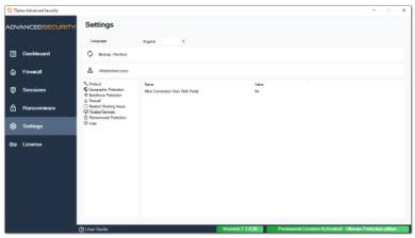
RESMÎ KAYNAK GÖRSELİ

Advanced - Trusted Devices

The **Trusted Devices** tab allows you to enable connections from the TSplus Remote Access' Web Portal.

Note:

-Trusted Devices is not compatible with HTML5 sessions. -Trusted Devices is not compatible with iOS / Android mobile devices as they hide their real hostnames. -The hostname of the remote machine is defined by the machine itself. The machine is likely to conceal or modify it according to its configuration.



TSplus Advanced Security's Trusted Devices cannot resolve the client name if the connection is initiated from TSplus Remote Access' Web portal. Therefore, Trusted Devices will block any connections from Web Portal by default. Set this setting to "Yes" to allow connections from the Web portal. Please be aware that this action will diminish your server's security.

TÜRKÇE İÇERİK

Gelişmiş Güvenilir Cihazlar

Güvenilen Cihazlar sekmesi, TSplus Remote Access' Web Portalı'ndan bağlantıları etkinleştirmenizi sağlar.

Not:

-Güvenilir Cihazlar HTML5 oturumları ile uyumlu değildir. -Güvenilir Aygıtlar, gerçek ana bilgisayar adlarını gizledikleri için iOS / Android mobil cihazlarla uyumlu değildir.-Uzak makinenin ana bilgisayar adı makinenin kendisi tarafından tanımlanır. Makinenin yapılandırmasına göre gizlemesi veya değiştirmesi muhtemeldir.

TSplus Advanced Security'ın Güvenilir Aygıtları, bağlantı TSplus Remote Access'nın Web portalından başlatılırsa istemci adını çözemez. Bu nedenle, Güvenilir Cihazlar varsayılan olarak Web Portalı'ndaki herhangi bir bağlantıyı engeller. Web portalından bağlantılara izin vermek için bu ayarı "Evet" olarak ayarlayın. Lütfen bu eylemin sunucunuzun güvenliğini azaltacağını unutmayın.

RESMÎ KAYNAK GÖRSELİ

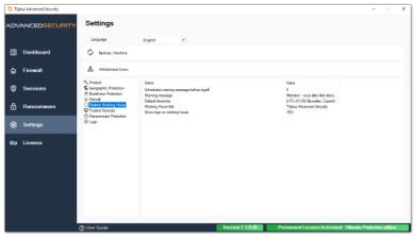
TÜRKÇE İÇERİK

Kaynak sayfa 19/99

RESMÎ KAYNAK GÖRSELİ

Advanced - Restrict Working Hours

The **Restrict Working Hours** tab allows you to Schedule a warning message before the user is logged off.



Warning message schedule You can configure in number of minutes before the user is automatically disconnected. By default, it is set to 5 minutes.

Warning message A warning message may be defined at your convenience, with placeholders named %MINUTESBEFORELOGOFF%, %DAY%, %STARTINGHOURS% and %ENDINGHOURS%, which will be respectively replaced by the current number of minutes before the session closes, the current day, the current day's starting and ending working hours.

Default server timezone A default server timezone may be defined to apply the working hours rules accordingly by selecting the corresponding one on the drop-down list.

Working hours title Title of the form displayed to the end-user, when his/her working hours are ending (default: TSplus Advanced Security)

Show logo on working hours If set to "yes", the logo is shown in the form displayed to the end-user, when his/her working hours are ending (default: "yes")

TÜRKÇE İÇERİK

Gelişmiş - Kısıtlı Çalışma Saatleri

Kısıtlama Çalışma Saatleri sekmesi, kullanıcı oturum açmadan önce bir uyarı mesajı zamanlamanızı sağlar.

Uyarı mesajı zaman çizelgesi Kullanıcı otomatik olarak bağlantısı kesilmeden önce birkaç dakika içinde yapılandırabilirsiniz. Varsayılan olarak, 5 dakikaya ayarlanır.

Uyarı mesajı Bir uyarı mesajı, oturum kapanmadan önce geçerli dakika sayısı ile değiştirilecek olan%MINUTESBEFORELOGOFF%,%DAY% ,%STARTINGHours% ve% ENDINGHours % adlı yer tutucularla, kolaylık içinde tanımlanabilir, geçerli gün, geçerli günün başlangıç ve bitiş çalışma saatleri.

Varsayılan sunucu zaman dilimi Öntanımlı bir sunucu zaman dilimi, açılır listedeki karşılık geleni seçerek çalışma saatleri kurallarını buna göre uygulamak için tanımlanabilir.

Çalışma saatleri başlığı Son kullanıcıya görüntülenen formun başlığı, çalışma saatleri sona erdiğinde (varsayılan: TSplus Advanced Security)

Çalışma saatlerinde logoyu göster "Evet" olarak ayarlanırsa, logo son kullanıcıya gösterilen formda gösterilir, çalışma saatleri sona erdiğinde (varsayılan: "evet")

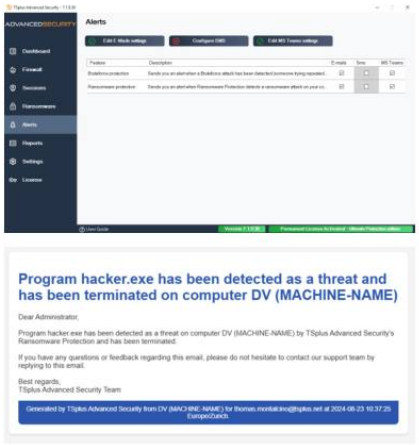
RESMÎ KAYNAK GÖRSELİ

TÜRKÇE İÇERİK

Kaynak sayfa 21/99

RESMÎ KAYNAK GÖRSELİ

Alerts



Create a Alert in Microsoft Teams.

The first thing to do is create a workflow in the Teams channel you want to send alerts to. There are two ways to do this:

TÜRKÇE İÇERİK

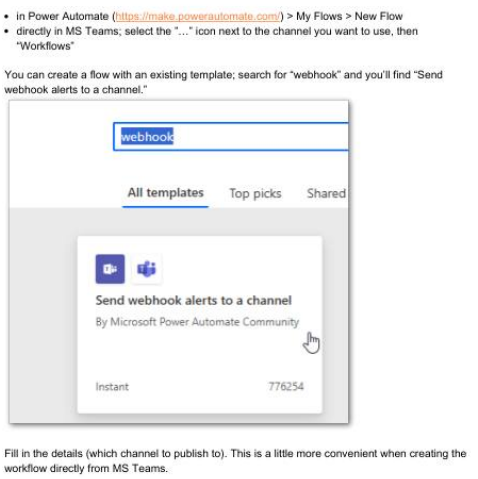
Kaynak sayfa 22/99

Uyarılar

Microsoft Teams'de bir uyarı oluşturun.

Yapılacak ilk şey, uyarıları göndermek istediğiniz Teams kanalında bir iş akışı oluşturmaktır. Bunu yapmanın iki yolu vardır:

RESMÎ KAYNAK GÖRSELİ



TÜRKÇE İÇERİK

Kaynak sayfa 23/99

Power Automate'de (https://make.powerautomate.com/) > Akışlarım > Yeni Akış

doğrudan MS Teams'te; kullanmak istediğiniz kanalın yanındaki "..." simgesini seçin, ardından

"İş Akışları"

Varolan bir şablonla bir akış oluşturabilirsiniz; "webhook" için arama yapın ve "Webhook uyarılarını bir kanala gönderin."

Ayrıntıları doldurun (hangi kanala yayınlanacağını). Bu, iş akışını doğrudan MS Teams'ten oluştururken biraz daha uygundur.

RESMÎ KAYNAK GÖRSELİ





Copy the URL; this is the one you need to provide in Teams settings, in Advanced Security or Server Monitoring.

Finally, edit the flow you just created, remove the "Send every Adaptive Card" option, and replace it with the following component:

(before editing)

TÜRKÇE İÇERİK

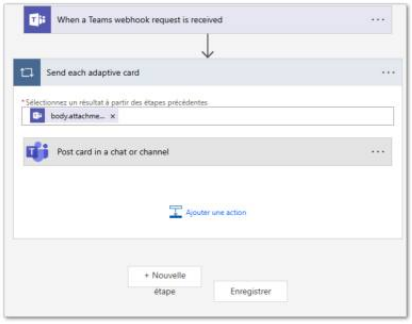
Kaynak sayfa 24/99

URL'yi kopyalayın; Gelişmiş Güvenlik veya Sunucu İzleme'de Teams ayarlarında vermeniz gereken budur.

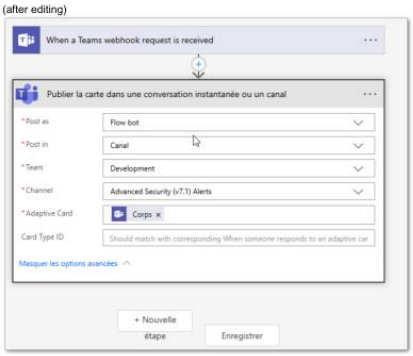
Son olarak, yeni oluşturduğunuz akışı düzenleyin, "Her Adaptif Kartı Gönder" seçeneğini kaldırın ve aşağıdaki bileşenle değiştirin:

(düzenlemeden önce)

RESMÎ KAYNAK GÖRSELİ



(after editing)



TÜRKÇE İÇERİK

Kaynak sayfa 25/99

Bir Teams webhook isteği alındığında +++ Her adaptif kart oe gönderin * S lectionnez un r sultat 4 partir desĞtapes prĞc dentes LJ. Tri Post kartı bir sohbet veya kanal te?

L Ajouter une action + NouvelleĞtape Enregistrer (düzenlemeden sonra) Bir Teams webhook isteği alındığında oo + Ti Publier la carte dans une conversation instantanĞe ou un channel t+ "Kone Kart Tipi Kimliği, biri adaptif bir arabaya cevap verdiğinde karşılık gelmelidir Masquer les options avancĞes "*

RESMÎ KAYNAK GÖRSELİ

TÜRKÇE İÇERİK

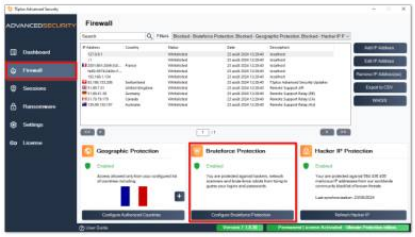
Kaynak sayfa 26/99

RESMÎ KAYNAK GÖRSELİ

Bruteforce Protection

The Bruteforce Protection enables you to protect your public server from hackers, network scanners and brute-force robots that try to guess your Administrator login and password. Using current logins and password dictionaries, they will automatically try to login to your server hundreds to thousands times every minute.

With this RDP Defender, you can monitor Windows failed login attempts and automatically blacklist the offending IP addresses after several failures.



TÜRKÇE İÇERİK

Kaynak sayfa 27/99

Bruteforce Koruma

Bruteforce Koruması, genel sunucunuzu Yönetici girişinizi ve şifrenizi tahmin etmeye çalışan bilgisayar korsanlarından, ağ tarayıcılarından ve kaba kuvvet robotlarından korumanızı sağlar. Mevcut girişleri ve parola sözlüklerini kullanarak, her dakika yüzlerce ila binlerce kez sunucunuza otomatik olarak giriş yapmaya çalışacaklardır.

Bu RDP Defender ile, Windows başarısız giriş denemelerini izleyebilir ve birkaç başarısızlıktan sonra rahatsız edici IP adreslerini otomatik olarak kara listeye alabilirsiniz.

RESMÎ KAYNAK GÖRSELİ



- You can set the **maximum failed logon attempts from a single IP address inside the IPs Detection block** (by default, it is 10), as well as the time of reset for failed logon attempts counters (by default it is 2 hours).
- On the bottom of this window, you can see the **Defender status**, where you can check if the HTML5 Web Portal logon failures, the Windows Logon Failures are monitored and if the Windows Firewall and advanced-security service are enabled.

In this case, like in our example, all the status are ticked.

- **Manage Blocked IP addresses**: You can of course configure it to match your needs, for example by adding your own workstation IP address in the IPs Whitelist, so this tool never block you. You can add as many IP addresses as you want in the whitelist. These addresses will never be blocked by the bruteforce Protection.
- You can **ignore Local and Private IP Addresses** by changing the default setting on the Settings > Advanced > Bruteforce tab

Note: If you ever notice that the Bruteforce Protection blocked 10 IP addresses per day and that now, it is not the case anymore; and blocks one, two or even doesn't block any address, it is actually normal. Indeed, before advanced-security installation, the server having an RDP port publicly available is known by all the robots, and many robots try the current passwords and the ones coming from dictionaries. When you install advanced-security, these robots are progressively being blocked, so that one day:

TÜRKÇE İÇERİK

IPs Detection bloğu içindeki tek bir IP adresinden (varsayılan olarak 10) maksimum başarısız logon denemelerini ve başarısız logon girişimleri sayaçları için sıfırlama süresini ayarlayabilirsiniz (varsayım olarak 2 saattir).

Bu pencerenin alt kısmında, HTML5 Web Portalı oturum açma hatalarının, Windows Oturum Açma Hatalarının izlenip izlenmediğini ve Windows Güvenlik Duvarı ve gelişmiş güvenlik hizmetinin etkin olup olmadığını kontrol edebileceğiniz Defender durumunu görebilirsiniz.

Bu durumda, örneğimizde olduğu gibi, tüm durum işaretlenir.

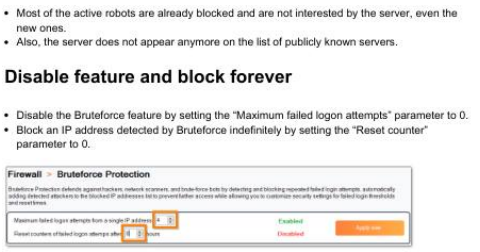
Engellenen IP adreslerini yönetin: Tabii ki ihtiyaçlarınızı karşılayacak şekilde yapılandırabilirsiniz, örneğin IPs Whitelist'e kendi iş istasyonu IP adresinizi ekleyerek, böylece bu araç sizi asla engellemez. Beyaz listede istediğiniz kadar IP adresi ekleyebilirsiniz. Bu adresler kaba kuvvet koruması tarafından hiçbir zaman engellenemez.

Yerel ve Özel IP Adreslerini, Ayarlar> Gelişmiş> Bruteforce sekmesindeki varsayılan ayarı değiştirerek göz ardı edebilirsiniz.

Not: Bruteforce Koruması'nın günde 10 IP adresini engellediğini ve artık böyle olmadığını fark ederseniz; ve bir, iki veya hatta herhangi bir adresi engellemez, aslında normaldir. Gerçekten de, gelişmiş güvenlik kurulumundan önce, halka açık bir RDP portuna sahip olan sunucu tüm robotlar tarafından bilinir ve birçok robot mevcut şifreleri ve sözlüklerden gelenleri dener.

Gelişmiş güvenlik yüklediğinizde, bu robotlar aşamalı olarak engelleniyor, böylece bir gün:

RESMÎ KAYNAK GÖRSELİ



TÜRKÇE İÇERİK

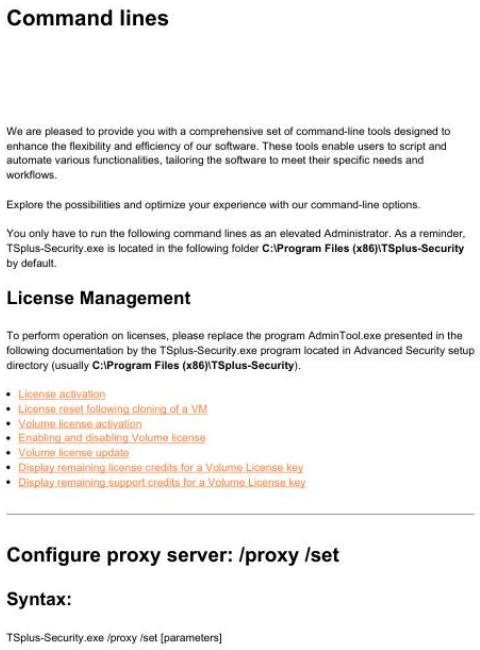
Kaynak sayfa 29/99

Aktif robotların çoğu zaten engellenmiş ve yenileri bile sunucu tarafından ilgilenmiyor. Ayrıca, sunucu artık halka açık olarak bilinen sunucular listesinde görünmüyor.

Özelliği devre dışı bırak ve sonsuza kadar engelle

Bruteforce özelliğini "Maksimum başarısız logon denemeleri" parametresini 0 olarak ayarlayarak devre dışı bırakın. Bruteforse tarafından tespit edilen bir IP adresini, "Reset counter" parametresini sıfıra ayarlayarak süresiz olarak engelleyin.

RESMÎ KAYNAK GÖRSELİ



Command lines

We are pleased to provide you with a comprehensive set of command-line tools designed to enhance the flexibility and efficiency of our software. These tools enable users to script and automate various functionalities, tailoring the software to meet their specific needs and workflows.

Explore the possibilities and optimize your experience with our command-line options.

You only have to run the following command lines as an elevated Administrator. As a reminder, TSplus-Security.exe is located in the following folder **C:\Program Files (x86)\TSplus-Security** by default.

License Management

To perform operation on licenses, please replace the program AdminTool.exe presented in the following documentation by the TSplus-Security.exe program located in Advanced Security setup directory (usually **C:\Program Files (x86)\TSplus-Security**).

- License activation
- License reset following cloning of a VM
- Volume license activation
- Enabling and disabling Volume license
- Volume license update
- Display remaining license credits for a Volume License key
- Display remaining support credits for a Volume License key

Configure proxy server: /proxy /set

Syntax:

TSplus-Security.exe /proxy /set [parameters]

TÜRKÇE İÇERİK

Kaynak sayfa 30/99

Komut satırları

Size yazılımımızın esnekliğini ve verimliliğini artırmak için tasarlanmış kapsamlı bir komut satırı araçları seti sunmaktan memnuniyet duyuyoruz. Bu araçlar, kullanıcıların çeşitli işlevleri komut dosyası oluşturmalarını ve otomatikleştirmelerini sağlar, yazılımı kendi özel ihtiyaçlarını ve iş akışlarını karşılayacak şekilde uyarlar.

Olasılıkları keşfedin ve komut satırı seçeneklerimizle deneyimlerinizi optimize edin.

You only have to run the following command lines as an elevated Administrator. As a reminder, TSplus-Security.exe is located in the following folder C:\Program Files (x86)\TSplus-Security by default.

Lisans Yönetimi

To perform operation on licenses, please replace the program AdminTool.exe presented in the following documentation by the TSplus-Security.exe program located in Advanced Security setup directory (usually C:\Program Files (x86)\TSplus-Security).

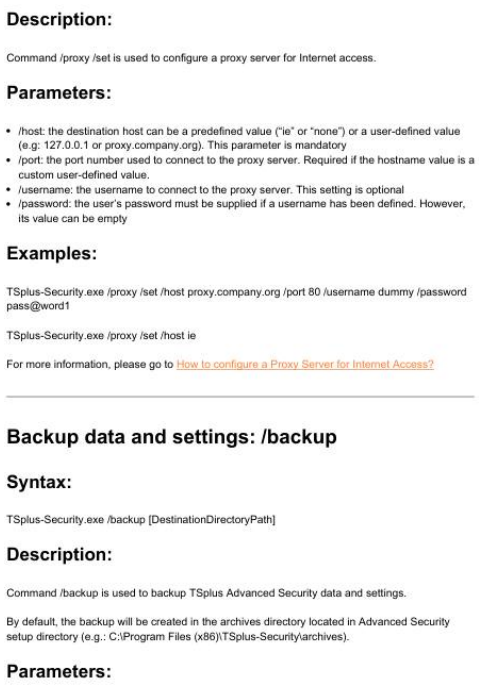
Lisans aktivasyonu Bir VM Volume lisans aktivasyonunun klonlanmasından sonra lisans sıfırlaması, Volume lisansının etkinleştirilmesi ve devre dışı bırakılması Volume Lisansının güncellenmesi Volume Lisans anahtarı için kalan lisans kredilerini göster Volume License anahtarı için kalan destek kredilerini göster

Proxy sunucusunu yapılandır: /proxy /set

Sözdizimi:

TSplus-Security.exe /proxy /set [parametre]

RESMÎ KAYNAK GÖRSELİ



Description:

Command /proxy /set is used to configure a proxy server for Internet access.

Parameters:

- /host: the destination host can be a predefined value ("ie" or "none") or a user-defined value (e.g: 127.0.0.1 or proxy.company.org). This parameter is mandatory
- /port: the port number used to connect to the proxy server. Required if the hostname value is a custom user-defined value.
- /username: the username to connect to the proxy server. This setting is optional
- /password: the user's password must be supplied if a username has been defined. However, its value can be empty

Examples:

TSplus-Security.exe /proxy /set /host proxy.company.org /port 80 /username dummy /password pass@word1

TSplus-Security.exe /proxy /set /host ie

For more information, please go to How to configure a Proxy Server for Internet Access?

Backup data and settings: /backup

Syntax:

TSplus-Security.exe /backup [DestinationDirectoryPath]

Description:

Command /backup is used to backup TSplus Advanced Security data and settings.

By default, the backup will be created in the archives directory located in Advanced Security setup directory (e.g.: C:\Program Files (x86)\TSplus-Security\archives).

Parameters:

TÜRKÇE İÇERİK

Kaynak sayfa 31/99

Açıklama:

Command /proxy /set, Internet erişimi için bir proxy sunucusu yapılandırmak için kullanılır.

Parametreler:

/host: hedef sunucu önceden tanımlanmış bir değer ("ie" veya "none") veya kullanıcı tanımlı bir değer (örneğin: 127.0.0.1 veya proxy.company.org) olabilir. Bu parametre zorunlu /port: vekil sunucuya bağlanmak için kullanılan port numarasıdır. Sunucu adı değeri özel bir kullanıcı tanımlı değerse gereklidir. /username: proxy sunucusuna bağlanmak için kullanıcı adı. Bu ayar isteğe bağlı / paroladır:

Kullanıcı adı tanımlanmışsa kullanıcının parolası sağlanmalıdır. Ancak, değeri boş olabilir

Örnekler:

TSplus-Security.exe /proxy /set /host proxy.company.org /port 80 /username kukla /password

pass@word1

TSplus-Security.exe /proxy /set /host ie

Daha fazla bilgi için lütfen Internet Erişimi için bir Proxy Sunucusu nasıl yapılandırılır? bölümüne gidin.

Yedekleme verileri ve ayarları: /backup

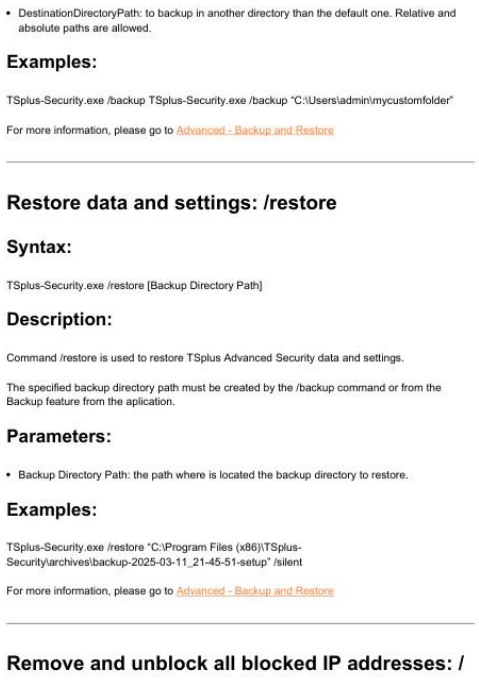
Sözdizimi:

TSplus-Security.exe /backup [DestinationDirectoryPath]

Komut / yedekleme, TSplus Advanced Security verilerini ve ayarlarını yedeklemek için kullanılır.

By default, the backup will be created in the archives directory located in Advanced Security setup directory (e.g.: C:\Program Files (x86)\TSplus-Security\archives).

RESMÎ KAYNAK GÖRSELİ



- DestinationDirectoryPath: to backup in another directory than the default one. Relative and absolute paths are allowed.

Examples:

TSplus-Security.exe /backup TSplus-Security.exe /backup "C:\Users\admin\mycustomfolder"

For more information, please go to Advanced - Backup and Restore

---

Restore data and settings: /restore

Syntax:

TSplus-Security.exe /restore [Backup Directory Path]

Description:

Command /restore is used to restore TSplus Advanced Security data and settings.

The specified backup directory path must be created by the /backup command or from the Backup feature from the aplication.

Parameters:

- Backup Directory Path: the path where is located the backup directory to restore.

Examples:

TSplus-Security.exe /restore "C:\Program Files (x86)\TSplus-Security\archives\backup-2025-03-11_21-45-51-setup" /silent

For more information, please go to Advanced - Backup and Restore

---

Remove and unblock all blocked IP addresses: /

TÜRKÇE İÇERİK

DestinationDirectoryPath: Öntanımlı olandan başka bir dizinde yedekleme yapmak. Bağıl ve mutlak yollara izin verilir.

Örnekler:

TSplus-Security.exe /backup
TSplus-Security.exe /backup "C:\Users\admin\mycustomfolder"

Daha fazla bilgi için lütfen Gelişmiş - Yedekleme ve Geri Yükleme'ye gidin.

Veri ve ayarları geri yükle: /restore

Sözdizimi:

TSplus-Security.exe /restore [Yedekleme Dizini Yolu]

Açıklama:

Command /restore, TSplus Advanced Security veri ve ayarlarını geri yüklemek için kullanılır.

Belirtilen yedekleme dizin yolu /backup komutu tarafından veya uygulamadan Yedekleme özelliğinden oluşturulmalıdır.

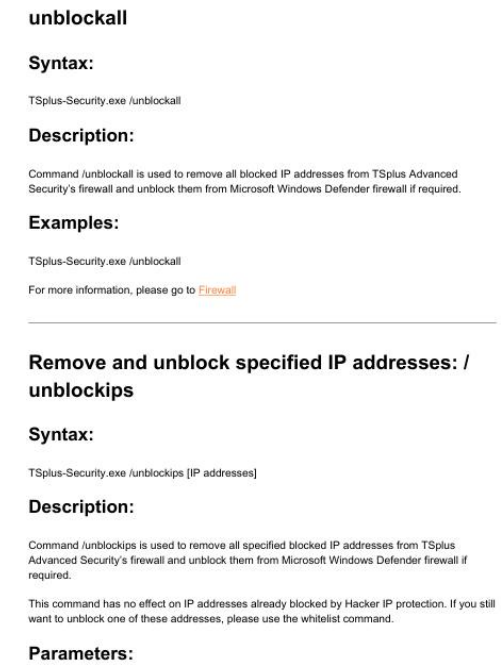
Parametreler:

Yedekleme Dizini Yolu: Geri yüklemek için yedekleme dizininin bulunduğu yol.

TSplus-Security.exe /restore "C:\Program Files (x86)\TSplus-Security\archives\backup-2025-03-11_21-45-51-setup" /silent

Engellenen tüm IP adreslerini kaldır ve engelini kaldır: /

RESMÎ KAYNAK GÖRSELİ



unblockall

Syntax:

TSplus-Security.exe /unblockall

Description:

Command /unblockall is used to remove all blocked IP addresses from TSplus Advanced Security's firewall and unblock them from Microsoft Windows Defender firewall if required.

Examples:

TSplus-Security.exe /unblockall

For more information, please go to Firewall

Remove and unblock specified IP addresses: / unblockips

Syntax:

TSplus-Security.exe /unblockips [IP addresses]

Description:

Command /unblockips is used to remove all specified blocked IP addresses from TSplus Advanced Security's firewall and unblock them from Microsoft Windows Defender firewall if required.

This command has no effect on IP addresses already blocked by Hacker IP protection. If you still want to unblock one of these addresses, please use the whitelist command.

Parameters:

TÜRKÇE İÇERİK

Kaynak sayfa 33/99

engellemeyi kaldır

Sözdizimi:

TSplus-Security.exe /unblockall

Açıklama:

Komut /unblockall, tüm engellenen IP adreslerini TSplus Advanced Security'ın güvenlik duvarından kaldırmak ve gerekirse Microsoft Windows Defender güvenlik duvarından engellemek için kullanılır.

Örnekler:

Daha fazla bilgi için lütfen Firewall'a gidin.

Belirtilen IP adreslerini kaldır ve engelini kaldır: / unblockips

TSplus-Security.exe /unblockips [IP adresleri]

Command / unblockips, TSplus Advanced Security'ın güvenlik duvarından belirtilen tüm engellenmiş IP adreslerini kaldırmak ve gerekirse Microsoft Windows Defender güvenlik duvarından kaldırmak için kullanılır.

Bu komut zaten Hacker IP koruması tarafından engellenen IP adresleri üzerinde bir etkiye sahip değildir. Hala bu adreslerden birinin engelini kaldırmak istiyorsanız, lütfen beyaz liste komutunu kullanın.

Parametreler:

RESMÎ KAYNAK GÖRSELİ



- IP addresses: the list of ip addresses or ip ranges to unblock (coma or semicolon separated).

Examples:

TSplus-Security.exe /unblockips 1.1.1.1;2.2.2.2;3.3.3.1-3.3.6.12;5.5.5.5

For more information, please go to Firewall

Block specified IP addresses: /blockips

Syntax:

TSplus-Security.exe /blockips [IP addresses] [Optional Description]

Description:

Command /blockips is used to block all specified IP addresses using TSplus Advanced Security's firewall and block them using Microsoft Windows Defender firewall if configured.

Parameters:

- IP addresses: the list of ip addresses or ip ranges to block (coma or semicolon separated).
- Optional Description: an optional description which will be added for each entry.

Examples:

TSplus-Security.exe /blockips 1.1.1.1;2.2.2.2;3.3.3.1-3.3.6.12;5.5.5.5 "John's workplaces"

For more information, please go to Firewall

Add IP addresses to whitelist: /addwhitelistedip

Syntax:

TÜRKÇE İÇERİK

Kaynak sayfa 34/99

IP adresleri: Engeli kaldırmak için ip adreslerinin veya ip aralıklarının listesi (coma veya virgül ayrılmış).

Örnekler:

TSplus-Security.exe /unblockips 1.1.1.1;2.2.2.2;3.3.3.1-3.3.6.12;5.5.5.5

Daha fazla bilgi için lütfen Firewall'a gidin.

Belirtilen IP adreslerini engelle: /blockips

Sözdizimi:

TSplus-Security.exe /blockips [IP adresleri] [İsteğe bağlı Açıklama]

Açıklama:

Komut / engellemeler, TSplus Advanced Security'ın güvenlik duvarını kullanarak belirtilen tüm IP adreslerini engellemek ve yapılandırılmışsa Microsoft Windows Defender güvenlik duvarı kullanarak bunları engellemek için kullanılır.

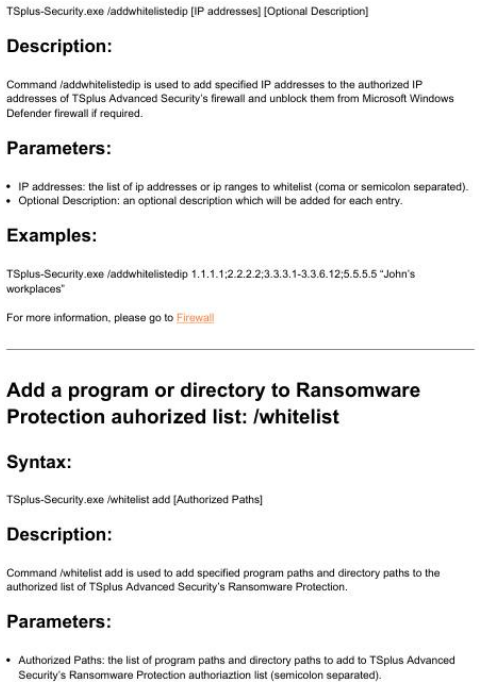
Parametreler:

IP adresleri: Engellenecek ip adreslerinin veya ip aralıklarının listesi (koma veya virgül ayrılmış). İsteğe bağlı Açıklama: Her giriş için eklenecek isteğe bağlı bir açıklama.

TSplus-Security.exe /blockips 1.1.1.1;2.2;3.3.3.1-3.3.6.12;5.5.5.5 "John'un işyerleri"

Beyaz listeye IP adresleri ekle: /addwhitelistip

RESMÎ KAYNAK GÖRSELİ



TSplus-Security.exe /addwhitelistedip [IP addresses] [Optional Description]

Description:

Command /addwhitelistedip is used to add specified IP addresses to the authorized IP addresses of TSplus Advanced Security's firewall and unblock them from Microsoft Windows Defender firewall if required.

Parameters:

- IP addresses: the list of ip addresses or ip ranges to whitelist (coma or semicolon separated).
- Optional Description: an optional description which will be added for each entry.

Examples:

TSplus-Security.exe /addwhitelistedip 1.1.1.1;2.2.2.2;3.3.3.1-3.3.6.12;5.5.5.5 "John's workplaces"

For more information, please go to Firewall

Add a program or directory to Ransomware Protection auhorized list: /whitelist

Syntax:

TSplus-Security.exe /whitelist add [Authorized Paths]

Description:

Command /whitelist add is used to add specified program paths and directory paths to the authorized list of TSplus Advanced Security's Ransomware Protection.

Parameters:

- Authorized Paths: the list of program paths and directory paths to add to TSplus Advanced Security's Ransomware Protection authoriaztion list (semicolon separated).

TÜRKÇE İÇERİK

TSplus-Security.exe /adwhitelistip [IP adresleri] [İsteğe bağlı Açıklama]

Açıklama:

Command /addwhitelistip, TSplus Advanced Security'ın güvenlik duvarının yetkili IP adreslerine belirtilen IP adreslerini eklemek ve gerekirse Microsoft Windows Defender güvenlik duvarından engelini kaldırmak için kullanılır.

Parametreler:

IP adresleri: ip adreslerinin veya ip aralıklarının listesi beyaz listeye (koma veya virgül ayrılmış). İsteğe bağlı Açıklama: Her giriş için eklenecek isteğe bağlı bir açıklama.

Örnekler:

TSplus-Security.exe /addwhitelistip 1.1.1.1;2.2.2.2;3.3.3.1-3.6.6.12;5.5.5.5 "John'un işyerleri"

Daha fazla bilgi için lütfen Firewall'a gidin.

Ransomware Koruma auhorized listesine bir program veya dizin ekleyin: /whitelist

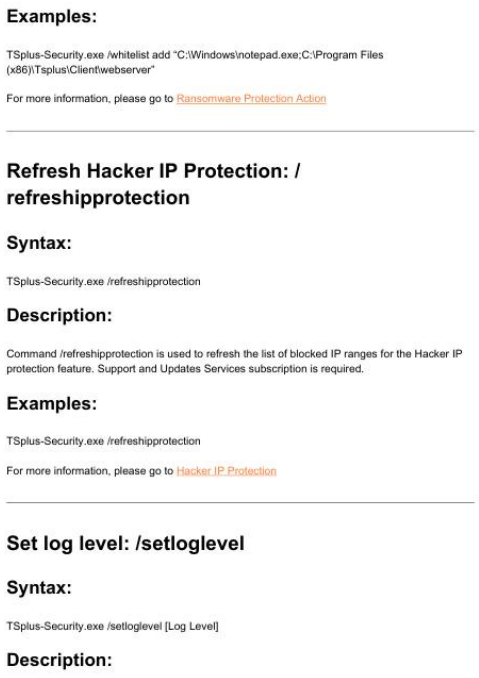
Sözdizimi:

TSplus-Security.exe /whitelist eklentisi [Yetkili Yollar]

Command /whitelist add, TSplus Advanced Security'ın Ransomware Koruması'nın yetkili listesine belirtilen program yolları ve dizin yolları eklemek için kullanılır.

Yetkili Yollar: TSplus Advanced Security'ın Ransomware Koruma yetki listesine eklenecek program yolları ve dizin yollarının listesi (semicolon ayrıldı).

RESMÎ KAYNAK GÖRSELİ



Examples:

TSplus-Security.exe /whitelist add "C:\Windows\notepad.exe;C:\Program Files (x86)\Tsplus\Client\webserver"

For more information, please go to Ransomware Protection Action

---

Refresh Hacker IP Protection: / refreshipprotection

Syntax:

TSplus-Security.exe /refreshipprotection

Description:

Command /refreshipprotection is used to refresh the list of blocked IP ranges for the Hacker IP protection feature. Support and Updates Services subscription is required.

Examples:

TSplus-Security.exe /refreshipprotection

For more information, please go to Hacker IP Protection

Set log level: /setloglevel

Syntax:

TSplus-Security.exe /setloglevel [Log Level]

Description:

TÜRKÇE İÇERİK

Kaynak sayfa 36/99

Örnekler:

TSplus-Security.exe /whitelist add "C:\Windows\notepad.exe;C:\Program Files (x86)\Tsplus\Client\webserver"

Daha fazla bilgi için lütfen Ransomware Protection Action'a gidin.

Hacker IP Korumasını Tazele: / refreipprotection

Sözdizimi:

TSplus-Security.exe /refreshipprotection

Açıklama:

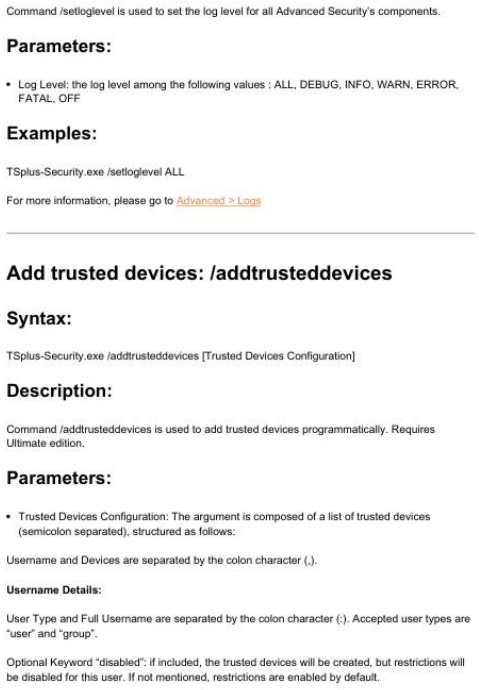
Command /refreshipprotection, Hacker IP koruma özelliği için engellenen IP aralıklarının listesini yenilemek için kullanılır. Destek ve Güncelleme Hizmetleri aboneliği gereklidir.

Daha fazla bilgi için lütfen Hacker IP Protection'a gidin.

Günlük seviyesini ayarla: /setloglevel

TSplus-Security.exe /setloglevel [Giriş Seviyesi]

RESMÎ KAYNAK GÖRSELİ



Command /setloglevel is used to set the log level for all Advanced Security's components.

Parameters:

- Log Level: the log level among the following values : ALL, DEBUG, INFO, WARN, ERROR, FATAL, OFF

Examples:

TSplus-Security.exe /setloglevel ALL

For more information, please go to Advanced > Logs

Add trusted devices: /addtrusteddevices

Syntax:

TSplus-Security.exe /addtrusteddevices [Trusted Devices Configuration]

Description:

Command /addtrusteddevices is used to add trusted devices programmatically. Requires Ultimate edition.

Parameters:

- Trusted Devices Configuration: The argument is composed of a list of trusted devices (semicolon separated), structured as follows:

Username and Devices are separated by the colon character (,).

Username Details:

User Type and Full Username are separated by the colon character (:). Accepted user types are "user" and "group".

Optional Keyword "disabled": if included, the trusted devices will be created, but restrictions will be disabled for this user. If not mentioned, restrictions are enabled by default.

TÜRKÇE İÇERİK

Kaynak sayfa 37/99

Command /setloglevel, Gelişmiş Güvenlik'in tüm bileşenleri için günlük seviyesini ayarlamak için kullanılır.

Parametreler:

Günlük Seviyesi: Aşağıdaki değerler arasındaki günlük seviyesi: ALL, DEBUG, INFO, WARN, ERROR, FATAL, OFF

Örnekler:

TSplus-Security.exe /setloglevel TÜM

Daha fazla bilgi için lütfen Gelişmiş > Günlükler bölümüne gidin

Güvenilir cihazlar ekle: /addtrusteddevices

Sözdizimi:

TSplus-Security.exe / addtrusteddevices [Güvenilir Cihaz Yapılandırması]

Açıklama:

Command /addtrusteddevices, programatik olarak güvenilir cihazlar eklemek için kullanılır. Ultimate sürümü gerektirir.

Güvenilir Cihazlar Yapılandırması: argüman, aşağıdaki gibi yapılandırılmış güvenilir cihazların (semicolon ayrılmış) bir listesinden oluşur:

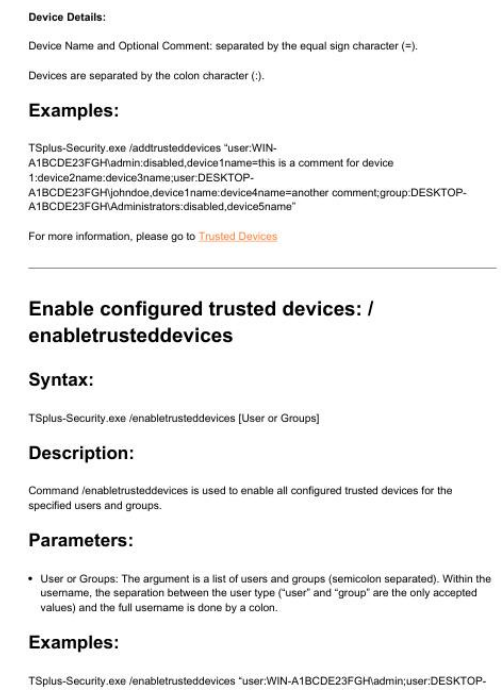
Kullanıcı adı ve cihazlar kolon karakteri (,) ile ayrılır.

Kullanıcı Adı Ayrıntıları:

Kullanıcı Tipi ve Tam Kullanıcı Adı, kolon karakteri (:) ile ayrılır. Kabul edilen kullanıcı türleri "kullanıcı" ve "grup"tur.

İsteğe bağlı anahtar kelime "engelli": dahil edilirse, güvenilir cihazlar oluşturulacak, ancak kısıtlamalar bu kullanıcı için devre dışı bırakılacaktır. Belirtilmemişse, kısıtlamalar varsayılan olarak etkinleştirilir.

RESMÎ KAYNAK GÖRSELİ



Device Details:

Device Name and Optional Comment: separated by the equal sign character (=).

Devices are separated by the colon character (:).

Examples:

TSplus-Security.exe /addtrusteddevices "user:WIN-A1BCDE23FGH\admin:disabled,device1name=this is a comment for device 1:device2name:device3name;user:DESKTOP-A1BCDE23FGH\johndoe,device1name:device4name=another comment;group:DESKTOP-A1BCDE23FGH\Administrators:disabled,device5name"

For more information, please go to Trusted Devices

Enable configured trusted devices: / enabletrusteddevices

Syntax:

TSplus-Security.exe /enabletrusteddevices [User or Groups]

Description:

Command /enabletrusteddevices is used to enable all configured trusted devices for the specified users and groups.

Parameters:

- User or Groups: The argument is a list of users and groups (semicolon separated). Within the username, the separation between the user type ("user" and "group" are the only accepted values) and the full username is done by a colon.

Examples:

TSplus-Security.exe /enabletrusteddevices "user:WIN-A1BCDE23FGH\admin;user:DESKTOP-

TÜRKÇE İÇERİK

Kaynak sayfa 38/99

Aygıt Detayları:

Cihaz Adı ve İsteğe Bağlı Yorum: eşit işaret karakteri (=) ile ayrılır.

Cihazlar kolon karakterine göre ayrılır (:).

Örnekler:

TSplus-Security.exe /addtrusteddevices "user:WIN-A1BCDE23FGH\admin:disabled,device1name=this is a comment for device 1:device2name:device3name;user:DESKTOP-A1BCDE23FGH\johndoe,device1name:device4name=another comment;group:DESKTOP-A1BCDE23FGH\Administrators:disabled,device5name"

Daha fazla bilgi için lütfen Güvenilir Cihazlar'a gidin.

Yapılandırılmış güvenilir cihazları etkinleştir: / enabletrusteddevices

Sözdizimi:

TSplus-Security.exe /enabletrusteddevices [Kullanıcı veya Gruplar]

Açıklama:

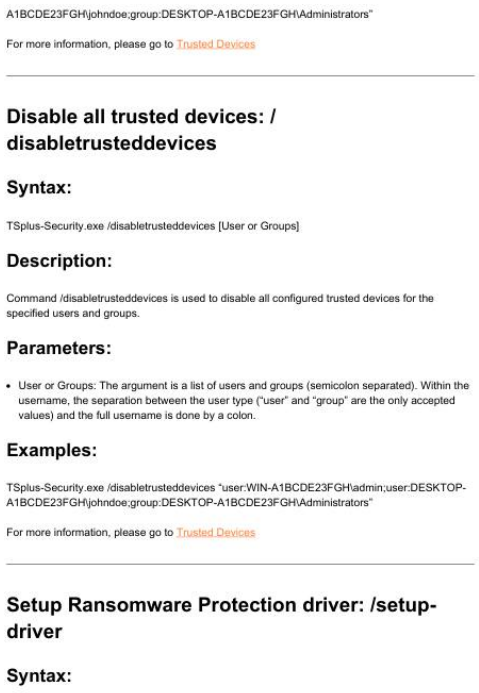
Command /enabletrusteddevices, belirtilen kullanıcı ve gruplar için yapılandırılmış tüm güvenilir cihazları etkinleştirmek için kullanılır.

Parametreler:

Kullanıcı veya Gruplar: Tartışma, kullanıcı ve grupların bir listesidir (semicolon ayrıldı). Kullanıcı adı içinde, kullanıcı türü ("kullanıcı" ve "grup" arasındaki ayrım tek kabul edilen değerlerdir) ve tam kullanıcı adı bir kolon tarafından yapılır.

TSplus-Security.exe /enabletrusteddevices "kullanıcı:WIN-A1BCDE23FGHĞadmin;kullanıcı:DESKTOP-

RESMÎ KAYNAK GÖRSELİ



A1BCDE23FGH\johndoe;group:DESKTOP-A1BCDE23FGH\Administrators"

For more information, please go to Trusted Devices

Disable all trusted devices: / disabletrusteddevices

Syntax:

TSplus-Security.exe /disabletrusteddevices [User or Groups]

Description:

Command /disabletrusteddevices is used to disable all configured trusted devices for the specified users and groups.

Parameters:

- User or Groups: The argument is a list of users and groups (semicolon separated). Within the username, the separation between the user type ("user" and "group" are the only accepted values) and the full username is done by a colon.

Examples:

TSplus-Security.exe /disabletrusteddevices "user:WIN-A1BCDE23FGH\admin;user:DESKTOP-A1BCDE23FGH\johndoe;group:DESKTOP-A1BCDE23FGH\Administrators"

For more information, please go to Trusted Devices

Setup Ransomware Protection driver: /setup-driver

Syntax:

TÜRKÇE İÇERİK

A1BCDE23FGH\johndoe;group:DESKTOP-A1BCDE23FGH\Administrators"

Daha fazla bilgi için lütfen Güvenilir Cihazlar'a gidin.

Tüm güvenilir cihazları devre dışı bırak: / disabletrusteddevices

Sözdizimi:

TSplus-Security.exe /disabletrusteddevices [Kullanıcı veya Gruplar]

Açıklama:

Command /disabletrusteddevices, belirtilen kullanıcı ve gruplar için yapılandırılmış tüm güvenilir cihazları devre dışı bırakmak için kullanılır.

Parametreler:

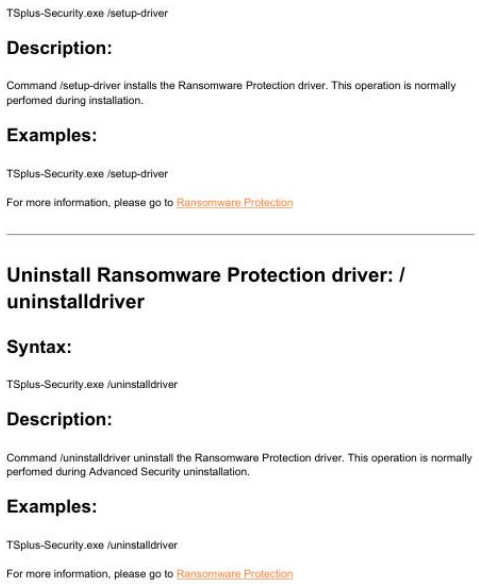
Kullanıcı veya Gruplar: Tartışma, kullanıcı ve grupların bir listesidir (semicolon ayrıldı). Kullanıcı adı içinde, kullanıcı türü ("kullanıcı" ve "grup" arasındaki ayrım tek kabul edilen değerlerdir) ve tam kullanıcı adı bir kolon tarafından yapılır.

Örnekler:

TSplus-Security.exe /disabletrusteddevices "user:WIN-A1BCDE23FGH\admin;user:DESKTOP-A1BCDE23FGH\johndoe;group:DESKTOP-A1BCDE23FGH\Administrators"

Ransomware Koruma sürücüsünü kurun: /setup- sürücü

RESMÎ KAYNAK GÖRSELİ



TSplus-Security.exe /setup-driver

Description:

Command /setup-driver installs the Ransomware Protection driver. This operation is normally perfomed during installation.

Examples:

TSplus-Security.exe /setup-driver

For more information, please go to Ransomware Protection

Uninstall Ransomware Protection driver: / uninstalldriver

Syntax:

TSplus-Security.exe /uninstalldriver

Description:

Command /uninstalldriver uninstall the Ransomware Protection driver. This operation is normally perfomed during Advanced Security uninstallation.

Examples:

TSplus-Security.exe /uninstalldriver

For more information, please go to Ransomware Protection

TÜRKÇE İÇERİK

TSplus-Security.exe /setup-driver

Açıklama:

Komut /setup-driver Ransomware Koruma sürücüsünü yükler. Bu işlem normalde kurulum sırasında perfomed edilir.

Örnekler:

Daha fazla bilgi için lütfen Ransomware Protection'a gidin.

Ransomware Koruma sürücüsünü kaldırmak: / kaldırmadriver

Sözdizimi:

TSplus-Security.exe /uninstalldriver

Command /uninstalldriver Ransomware Koruma sürücüsü kaldırmak. Bu işlem genellikle Gelişmiş Güvenlik kaldırma sırasında perfomed.

RESMÎ KAYNAK GÖRSELİ

TÜRKÇE İÇERİK

Kaynak sayfa 41/99

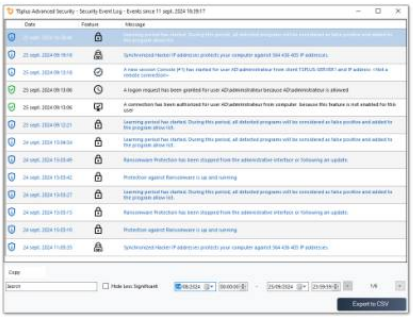
RESMÎ KAYNAK GÖRSELİ

Events

The security events are a great source of information as they display the operations performed by TSplus Advanced Security to protect your computer.

The Events window can be opened from the TSplus Advanced Security main window, by clicking directly on the last 5 events displayed or on the dashbord tab. The information displayed on the Events window are refreshed automatically every few seconds.

The list of security events presents 4 columns, which describes the severity, the date of the check or performed operation, the associated feature icon and the description.



The description of the event often explains why the action was performed or not. Retaliatory actions are often written in red and highlighted with a red shield icon.

Events window can be moved around and does not prevent you from using the other TSplus

TÜRKÇE İÇERİK

Etkinlikler

Güvenlik olayları, bilgisayarınızı korumak için TSplus Advanced Security tarafından gerçekleştirilen işlemleri görüntülerken büyük bir bilgi kaynağıdır.

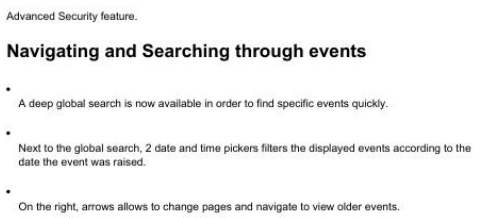
Olaylar penceresi TSplus Advanced Security ana penceresinden, görüntülenen son 5 etkinliğe doğrudan tıklayarak veya dashbord sekmesinde açılabilir. Olaylar penceresinde görüntülenen bilgiler birkaç saniyede bir otomatik olarak yenilenir.

Güvenlik olayları listesi, şiddeti, kontrol tarihini veya gerçekleştirilen işlemi, ilişkili özellik simgesini ve tanımını açıklayan 4 sütun sunar.

Etkinliğin açıklaması genellikle eylemin neden yapıldığını veya yapılmadığını açıklar. Misilleme eylemleri genellikle kırmızı ile yazılır ve kırmızı bir kalkan simgesi ile vurgulanır.

Olay penceresi hareket ettirilebilir ve diğer TSplus'ı kullanmanızı engellemez

RESMÎ KAYNAK GÖRSELİ


Advanced Security feature.

Navigating and Searching through events

- A deep global search is now available in order to find specific events quickly.
- Next to the global search, 2 date and time pickers filters the displayed events according to the date the event was raised.
- On the right, arrows allows to change pages and navigate to view older events.

TÜRKÇE İÇERİK

Kaynak sayfa 43/99

Gelişmiş Güvenlik özelliği.

Etkinlikler aracılığıyla gezinme ve arama

Belirli olayları hızlı bir şekilde bulmak için derin bir küresel arama artık mevcuttur.

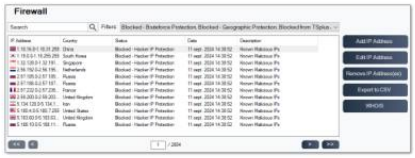
Küresel aramanın yanında, 2 tarih ve saat seçicileri görüntülenen olayları etkinliğin kaldırıldığı tarihe göre filtreler.

Sağda, oklar sayfaları değiştirmek ve eski olayları görüntülemek için gezinmek için izin verir.

RESMÎ KAYNAK GÖRSELİ

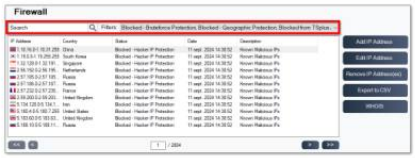
Firewall

IP addresses management is easy with a single list to manage both blocked and whitelisted IP addresses:



By default, IPV4, IPV6 and all server localhosts addresses are whitelisted.

A convenient search bar and filter provides search capabilities based on all the information provided.



Furthermore, administrators are able to perform actions on several selected IP addresses with a single click. Among the new features IP addresses management introduced, you will find the possibility to provide meaningful descriptions to any IP addresses:

TÜRKÇE İÇERİK

Kaynak sayfa 44/99

Güvenlik Duvarı

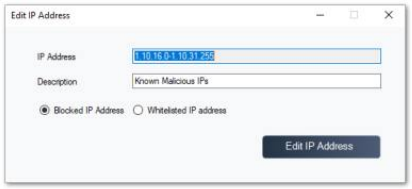
IP adresleri yönetimi, hem engellenmiş hem de beyaz listeye alınmış IP adreslerini yönetmek için tek bir listeyle kolaydır:

Varsayılan olarak, IPV4, IPV6 ve tüm sunucu localhosts adresleri beyaz listeye alınmıştır.

Uygun bir arama çubuğu ve filtre, sağlanan tüm bilgilere dayanarak arama yetenekleri sağlar.

Ayrıca, yöneticiler seçilen birkaç IP adresi üzerinde tek bir tıklama ile eylemler gerçekleştirebilirler. IP adresleri yönetiminin tanıttığı yeni özellikler arasında, herhangi bir IP adresine anlamlı açıklamalar sağlama olanağı bulacaksınız:

RESMÎ KAYNAK GÖRSELİ



Last but not least, administrators are now able to unblock and add to whitelist multiple blocked IP addresses in a single action, by clicking on the "Add Existing to Whitelist" tab.

Using the command line to whitelist or block IP addresses and/or IP ranges

- In order to **whitelist** IP addresses or IP range(s), the command has this syntax :

TSplus-Security.exe addwhitelistedip [ip addresses] [optional description]

You may whitelist several IP addresses, with a **comma or semi-colon delimiter**. Moreover, you can specify IP address ranges, instead of simple IP addresses. The syntax is : **x.x.x.x-y.y.y.y** Finally, you may indicate an optional description of the whitelist rule

Here is an example of a complete command : TSplus-Security.exe addwhitelistedip 1.1.1.1;2.2.2.2;3.3.3.1-3.3.6.12;5.5.5.5 "John's workplaces"

- In order to **block** IP addresses or IP range(s), the command has a similar syntax :

TSplus-Security.exe blockips [ip addresses] [optional description]

- In order to **unblock** IP addresses or IP range(s), the command has a similar syntax :

TSplus-Security.exe unblockips [ip addresses]

This command has no effect on IP addresses already blocked by Hacker IP protection. If you still want to unblock one of these addresses, please use the whitelist command.

TÜRKÇE İÇERİK

Kaynak sayfa 45/99

Son olarak, yöneticiler artık "Beyaz Listeye Var Olanı Ekle" sekmesine tıklayarak tek bir eylemde birden fazla engellenmiş IP adresinin engelini kaldırabilir ve beyaz listeye ekleyebilir.

IP adreslerini ve/veya IP aralıklarını beyaz listeye almak veya engellemek için komut satırının kullanılması

IP adreslerini veya IP aralığını(lar) beyaz listeye almak için, komut şu söz dizimine sahiptir:

TSplus-Security.exe addwhitelistip [ip adresleri] [isteğe bağlı açıklama]

Birkaç IP adresini, virgül veya yarı-kolon sınırlayıcı ile beyaz listeye alabilirsiniz. Ayrıca, basit IP adresleri yerine IP adresi aralıklarını belirtebilirsiniz. Sözdizimi: x.x.x.xy.y.y Son olarak, beyaz liste kuralının isteğe bağlı bir açıklamasını belirtebilirsiniz.

İşte tam bir komut örneği: TSplus-Security.exe addwhitelistip 1.1.1.1;2.2.2.2;3.3.3.1-3.6.6.12;5.5.5.5 "John'un işyerleri"

IP adreslerini veya IP aralığını (s) engellemek için, komut benzer bir sözdizimi içerir:

TSplus-Security.exe engellemeleri [ip adresleri] [isteğe bağlı açıklama]

IP adreslerinin veya IP aralığının (s) engelini kaldırmak için, komut benzer bir sözdizimi içerir:

TSplus-Security.exe engellemeleri [ip adresleri]

Bu komut zaten Hacker IP koruması tarafından engellenen IP adresleri üzerinde bir etkiye sahip değildir. Hala bu adreslerden birinin engelini kaldırmak istiyorsanız, lütfen beyaz liste komutunu kullanın.

RESMÎ KAYNAK GÖRSELİ

TÜRKÇE İÇERİK

Kaynak sayfa 46/99

RESMÎ KAYNAK GÖRSELİ

Geographic Protection

Restrict access from other countries

To allow remote access from only specific countries, select the "Allow connections only from this list of countries" button and then click on the "Add country" button.



A popup offering a country list opens. Select the country you wish to add on the list.

You can choose to check the box below to unblock all previously blocked IP addresses for the selected country.

Click on the button "Add Country" to return to the feature main screen.

TÜRKÇE İÇERİK

Coğrafi Koruma

Diğer ülkelerden erişimi kısıtlama

Yalnızca belirli ülkelerden uzaktan erişime izin vermek için, "Yalnızca bu ülke listesinden bağlantılara izin ver" düğmesini seçin ve ardından "Ülke Ekle" düğmesine tıklayın.

Bir ülke listesi sunan bir açılır pencere açılır. Listeye eklemek istediğiniz ülkeyi seçin.

Seçili ülke için önceden engellenmiş tüm IP adreslerinin engelini kaldırmak için aşağıdaki kutuyu işaretlemeyi seçebilirsiniz.

Özellik ana ekranına dönmek için "Ülke Ekle" düğmesine tıklayın.

RESMÎ KAYNAK GÖRSELİ



Important: In order to save your changes, click on the "Apply" button.



In this example, remote access is allowed for users connecting from United States and France.

A confirmation message appears to avoid blocking the connected user. Click "Yes" to confirm and apply the changes.

TÜRKÇE İÇERİK

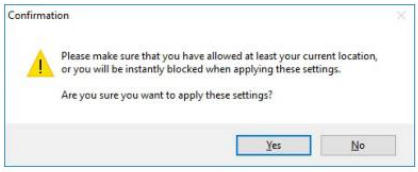
Kaynak sayfa 48/99

Önemli: Değişikliklerinizi kaydetmek için "Uygulama" düğmesine tıklayın.

Bu örnekte, Amerika Birleşik Devletleri ve Fransa'dan bağlanan kullanıcılar için uzaktan erişime izin verilir.

Bağlantılı kullanıcıyı engellemekten kaçınmak için bir onay mesajı görünür. Değişiklikleri onaylamak ve uygulamak için "Evet" i tıklayın.

RESMÎ KAYNAK GÖRSELİ



Restrict access from the internet

Geographic Protection can be configured to restrict the access to your machine to only private and whitelisted IP addresses, as shown below:



Disable Geographic Protection

By default, Geographic Protection allows access for users connecting from all over the world:

TÜRKÇE İÇERİK

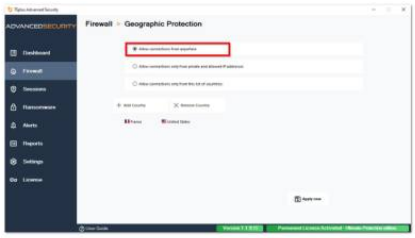
İnternet erişimini kısıtla

Coğrafi Koruma, makinenize erişimi yalnızca aşağıda gösterildiği gibi özel ve beyaz listelenmiş IP adresleriyle kısıtlayacak şekilde yapılandırılabilir:

Coğrafi Korumayı Devre Dışı Bırak

Varsayılan olarak, Coğrafi Koruma dünyanın her yerinden bağlanan kullanıcılar için erişime izin verir:

RESMÎ KAYNAK GÖRSELİ



Unblocking blocked IP addresses

When an IP address gets blocked, it appears on the Firewall tab. Blocked IP addresses can then be unblocked and eventually added to the list of allowed IP addresses.

If you get blocked, we recommend that you try connecting from any country you allowed on TSplus Advanced Security, for instance by connecting from another remote server or using a VPN service. You can also use a console session to connect, as this session is not a remote session and will not be blocked by TSplus Advanced Security.

Important:

- Check that you have selected the country where you are currently connected from. Otherwise, your IP address will be blocked quickly after applying the settings, thus disconnecting you without any hope of connecting back again from the same IP address.
- Consider adding your own IP address to the list of allowed IP Addresses to avoid being blocked by either Geographic Protection or Bruteforce Protection features.

Undestanding Geographic Protection

Geographic Protection checks incoming TCP network connexion, both IPv4 and IPV6 (except when the legacy Windows API mode is configured).

Processes: Geographic Protection listens to connexions sent to the TSplus Remote Access'

TÜRKÇE İÇERİK

Engellenen IP adreslerinin engellenmesi

Bir IP adresi engellendiğinde, Güvenlik Duvarı sekmesinde görünür. Engellenen IP adresleri daha sonra engellenebilir ve sonunda izin verilen IP adresleri listesine eklenebilir.

Engellenirseniz, örneğin başka bir uzak sunucudan bağlanarak veya bir VPN hizmeti kullanarak TSplus Advanced Security'ta izin verdiğiniz herhangi bir ülkeden bağlanmayı denemenizi tavsiye ederiz. Bu oturum uzak bir oturum olmadığı ve TSplus Advanced Security tarafından engellenmeyeceği için bağlanmak için bir konsol oturumu da kullanabilirsiniz.

Önemli:

Şu anda bağlı olduğunuz ülkeyi seçtiğinizi kontrol edin. Aksi takdirde, IP adresiniz ayarları uyguladıktan sonra hızlı bir şekilde engellenir ve böylece aynı IP adresinden tekrar bağlanma umudu olmadan bağlantınız kesilir.

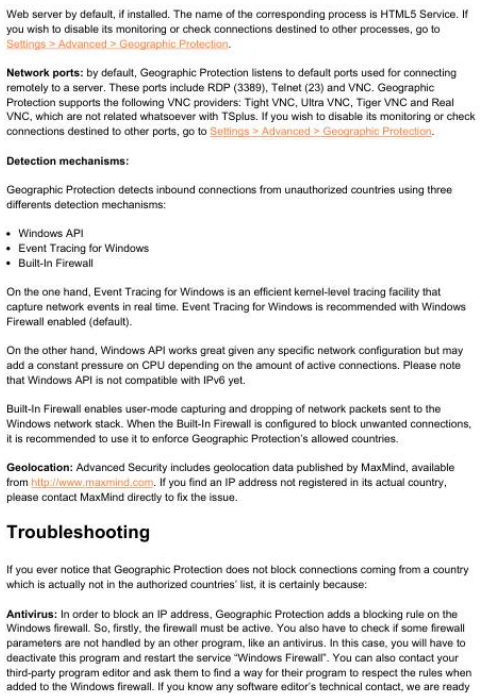
Coğrafi Koruma veya Bruteforce Koruma özellikleri tarafından engellenmemek için izin verilen IP Adresleri listesine kendi IP adresinizi eklemeyi düşünün.

Belirsiz Coğrafi Koruma

Coğrafi Koruma, hem IPv4 hem de IPV6 (eski Windows API modu yapılandırıldığında hariç) gelen TCP ağ bağlantısını kontrol eder.

Süreçler: Coğrafi Koruma, TSplus Remote Access'ya gönderilen bağlantıları dinler

RESMÎ KAYNAK GÖRSELİ



Web server by default, if installed. The name of the corresponding process is HTML5 Service. If you wish to disable its monitoring or check connections destined to other processes, go to Settings > Advanced > Geographic Protection.

Network ports: by default, Geographic Protection listens to default ports used for connecting remotely to a server. These ports include RDP (3389), Telnet (23) and VNC. Geographic Protection supports the following VNC providers: Tight VNC, Ultra VNC, Tiger VNC and Real VNC, which are not related whatsoever with TSplus. If you wish to disable its monitoring or check connections destined to other ports, go to Settings > Advanced > Geographic Protection.

Detection mechanisms:

Geographic Protection detects inbound connections from unauthorized countries using three differents detection mechanisms:

- Windows API
- Event Tracing for Windows
- Built-In Firewall

On the one hand, Event Tracing for Windows is an efficient kernel-level tracing facility that capture network events in real time. Event Tracing for Windows is recommended with Windows Firewall enabled (default).

On the other hand, Windows API works great given any specific network configuration but may add a constant pressure on CPU depending on the amount of active connections. Please note that Windows API is not compatible with IPv6 yet.

Built-In Firewall enables user-mode capturing and dropping of network packets sent to the Windows network stack. When the Built-In Firewall is configured to block unwanted connections, it is recommended to use it to enforce Geographic Protection's allowed countries.

Geolocation: Advanced Security includes geolocation data published by MaxMind, available from http://www.maxmind.com. If you find an IP address not registered in its actual country, please contact MaxMind directly to fix the issue.

Troubleshooting

If you ever notice that Geographic Protection does not block connections coming from a country which is actually not in the authorized countries' list, it is certainly because:

Antivirus: In order to block an IP address, Geographic Protection adds a blocking rule on the Windows firewall. So, firstly, the firewall must be active. You also have to check if some firewall parameters are not handled by an other program, like an antivirus. In this case, you will have to deactivate this program and restart the service "Windows Firewall". You can also contact your third-party program editor and ask them to find a way for their program to respect the rules when added to the Windows firewall. If you know any software editor's technical contact, we are ready

TÜRKÇE İÇERİK

Kaynak sayfa 51/99

Web sunucusu varsayılan olarak yüklüyse. İlgili işlemin adı HTML5 Service'dir. İzlemesini devre dışı bırakmak veya diğer işlemlere yönelik bağlantıları kontrol etmek istiyorsanız, Ayarlar> Gelişmiş> Coğrafi Koruma bölümüne gidin.

Ağ portları: varsayılan olarak, Coğrafi Koruma bir sunucuya uzaktan bağlanmak için kullanılan varsayılan portları dinler. Bu portlar arasında RDP (3389), Telnet (23) ve VNC bulunmaktadır. Coğrafik Koruma aşağıdaki VNC sağlayıcıları destekler: TSplus ile hiçbir şekilde ilişkili olmayan Sıkı VNC, Ultra VNC, Tiger VNC ve Gerçek VNC.

İzlemesini devre dışı bırakmak veya diğer portlara yönlendirilmiş bağlantıları kontrol etmek istiyorsanız, Ayarlar> Gelişmiş> Coğrafi Koruma'ya gidin.

Algılama mekanizmaları:

Coğrafi Koruma, yetkisiz ülkelerden gelen bağlantıları üç farklı algılama mekanizması kullanarak tespit eder:

Windows için Windows API Olay İzleme Yerleşik Güvenlik Duvarı

Bir yandan, Windows için Olay İzleme, ağ olaylarını gerçek zamanlı olarak yakalayan verimli bir çekirdek düzeyinde izleme tesisidir. Windows için Etkinlik İzleme, Windows Güvenlik Duvarı etkin (varsayılan) ile önerilir.

Öte yandan, Windows API herhangi bir özel ağ yapılandırması göz önüne alındığında harika çalışır, ancak aktif bağlantı miktarına bağlı olarak CPU'ya sabit bir basınç ekleyebilir. Windows API'nin henüz IPv6 ile uyumlu olmadığını lütfen unutmayın.

Built-In Firewall, Windows ağ yığınına gönderilen ağ paketlerinin kullanıcı moduyla yakalanmasını ve düşmesini sağlar. Built In Firewall istenmeyen bağlantıları engelleyecek şekilde yapılandırıldığında, Coğrafi Koruma'nın izin verilen ülkelerini uygulamak için kullanılması önerilir.

Geolocation: Advanced Security, MaxMind tarafından yayınlanan coğrafi konum verilerini içerir.

http://www.maxmind.com adresinden. Gerçek ülkesinde kayıtlı olmayan bir IP adresi bulursanız,

Sorunu düzeltmek için lütfen doğrudan MaxMind ile iletişime geçin.

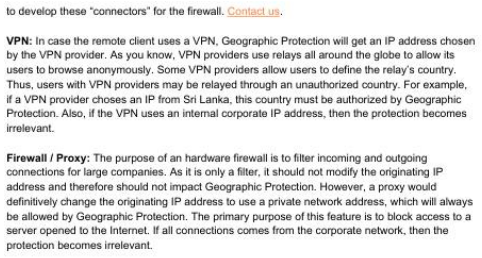
Sorun giderme

Coğrafi Koruma'nın aslında yetkili ülkelerin listesinde olmayan bir ülkeden gelen bağlantıları engellemediğini fark ederseniz, kesinlikle bunun nedeni:

Antivirüs: Bir IP adresini engellemek için, Coğrafi Koruma, Windows güvenlik duvarı üzerinde bir engelleme kuralı ekler. Bu nedenle, öncelikle güvenlik duvarı etkin olmalıdır. Ayrıca, bazı güvenlik duvarı parametrelerinin antivirüs gibi başka bir program tarafından ele alınmadığını kontrol etmeniz gerekir. Bu durumda, bu programı devre dışı bırakmanız ve hizmeti yeniden başlatmanız gerekecektir "Windows Güvenlik Duvarı".

Üçüncü taraf program düzenleyicinizle de iletişime geçebilir ve Windows güvenlik duvarına eklendiğinde programlarına saygı duymaları için bir yol bulmalarını isteyebilirsiniz. Herhangi bir yazılım editörünün teknik temasını biliyorsanız, hazırız

RESMÎ KAYNAK GÖRSELİ



to develop these "connectors" for the firewall. Contact us.

VPN: In case the remote client uses a VPN, Geographic Protection will get an IP address chosen by the VPN provider. As you know, VPN providers use relays all around the globe to allow its users to browse anonymously. Some VPN providers allow users to define the relay's country. Thus, users with VPN providers may be relayed through an unauthorized country. For example, if a VPN provider choses an IP from Sri Lanka, this country must be authorized by Geographic Protection. Also, if the VPN uses an internal corporate IP address, then the protection becomes irrelevant.

Firewall / Proxy: The purpose of an hardware firewall is to filter incoming and outgoing connections for large companies. As it is only a filter, it should not modify the originating IP address and therefore should not impact Geographic Protection. However, a proxy would definitively change the originating IP address to use a private network address, which will always be allowed by Geographic Protection. The primary purpose of this feature is to block access to a server opened to the Internet. If all connections comes from the corporate network, then the protection becomes irrelevant.

TÜRKÇE İÇERİK

Kaynak sayfa 52/99

güvenlik duvarı için bu "bağlayıcıları" geliştirmek. Bize ulaşın.

VPN: Uzak istemcinin VPN kullanması durumunda Coğrafi Koruma, VPN sağlayıcısı tarafından seçilen bir IP adresi alır. Bildiğiniz gibi, VPN sağlayıcıları, kullanıcılarının anonim olarak gezinmelerine izin vermek için dünyanın dört bir yanındaki röleleri kullanır. Bazı VPN sağlayıcıları, kullanıcılara rölenin ülkesini tanımlamalarına izin verir. Böylece, VPN sağlayıcılarına sahip kullanıcılar yetkisiz bir ülke üzerinden aktarılabilir.

Örneğin, bir VPN sağlayıcısı Sri Lanka'dan bir IP seçerse, bu ülkenin Coğrafi Koruma tarafından yetkilendirilmesi gerekir. Ayrıca, VPN dahili bir kurumsal IP adresi kullanırsa, koruma ilgisiz hale gelir.

Firewall / Proxy: Bir donanım güvenlik duvarının amacı, büyük şirketler için gelen ve giden bağlantıları filtrelemektir. Sadece bir filtre olduğu için, kaynak IP adresini değiştirmemeli ve bu nedenle Coğrafi Koruma'yı etkilememelidir. Bununla birlikte, bir proxy, coğrafi koruma tarafından her zaman izin verilen özel bir ağ adresi kullanmak için menşeli IP adresini kesin olarak değiştirecektir.

Bu özelliğin birincil amacı, internete açılan bir sunucuya erişimi engellemektir. Tüm bağlantılar kurumsal ağdan geliyorsa, koruma ilgisiz hale gelir.

RESMÎ KAYNAK GÖRSELİ

Hacker IP Protection

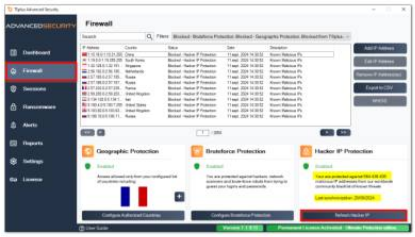
Keep your machine protected against known threats such as on-line attacks, on-line service abuse, malwares, botnets and other cybercrime activities with the Hacker IP Protection. The objective is to create a blacklist that can be safe enough to be used on all systems, with a firewall, to block access entirely, from and to its listed IPs

Support and Updates Services subscription is required.

The key prerequisite for this cause, is to have no false positives. All IPs listed should be bad and should be blocked, without exceptions. To accomplish this, Hacker IP Protection leverages the information provided by the community of Advanced Security's users.

Hacker IP Protection is updated automatically every day.

You can update manually from the "Blocked IP Addresses" tab, by clicking on the "Refresh Hacker IP" button:



As a result, the feature should create approx. 600 000 000 bloxking firewall rules in Windows Firewall.

TÜRKÇE İÇERİK

Kaynak sayfa 53/99

Hacker IP Koruması

Makinenizi, Hacker IP Koruması ile çevrimiçi saldırılar, çevrimiçi hizmet kötüye kullanımı, kötü amaçlı yazılımlar, botnetler ve diğer siber suç faaliyetleri gibi bilinen tehditlere karşı korumalı tutun. Amaç, listelenen IP'lerinden tamamen erişimi engellemek için bir güvenlik duvarıyla tüm sistemlerde kullanılabilecek kadar güvenli olabilecek bir kara liste oluşturmaktır.

Destek ve Güncelleme Hizmetleri aboneliği gereklidir.

Bu neden için en önemli ön koşul, yanlış pozitiflerin olmamasıdır. Listelenen tüm IP'ler kötü olmalı ve istisnasız engellenmelidir. Bunu başarmak için Hacker IP Koruması, Gelişmiş Güvenlik'in kullanıcıları topluluğu tarafından sağlanan bilgilerden yararlanır.

Hacker IP Koruması her gün otomatik olarak güncellenir.

"Kilitli IP Adresleri" sekmesinden manuel olarak güncelleyebilirsiniz, "Hacker IP'yi yenile" düğmesine tıklayarak:

Sonuç olarak, özellik Windows Firewall'da yaklaşık 600 000 000 bloxking güvenlik duvarı kuralları oluşturmalıdır.

RESMÎ KAYNAK GÖRSELİ

TÜRKÇE İÇERİK

Kaynak sayfa 54/99

RESMÎ KAYNAK GÖRSELİ

Dashboard

Click on each tile to know more about each feature



The menu bar on the left provides access to the different features. Each tile gives you access to the various features and settings offered by TSplus Advanced Security.

Advanced Security displays the six last Security Events. Click on any event to open the complete list of events in a separate window.

Below the last events, three tiles provide quick access to:

1. Firewall
2. Sessions
3. Ramsomware Protection

TÜRKÇE İÇERİK

Kaynak sayfa 55/99

GÖSTERGE PANELİ

Her özellik hakkında daha fazla bilgi edinmek için her kiremit üzerine tıklayın

Soldaki menü çubuğu farklı özelliklere erişim sağlar. Her karo, TSplus Advanced Security tarafından sunulan çeşitli özelliklere ve ayarlara erişmenizi sağlar.

Gelişmiş Güvenlik, son altı Güvenlik Olayını görüntüler. Olayların tam listesini ayrı bir pencerede açmak için herhangi bir olaya tıklayın.

Son olayların altında, üç karo aşağıdakilere hızlı erişim sağlar:

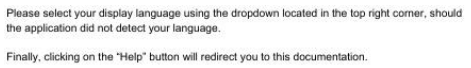
1.

Güvenlik duvarı 2.

Oturumlar 3.

Ramsomware Koruma

RESMÎ KAYNAK GÖRSELİ


Please select your display language using the dropdown located in the top right corner, should the application did not detect your language.

Finally, clicking on the "Help" button will redirect you to this documentation.

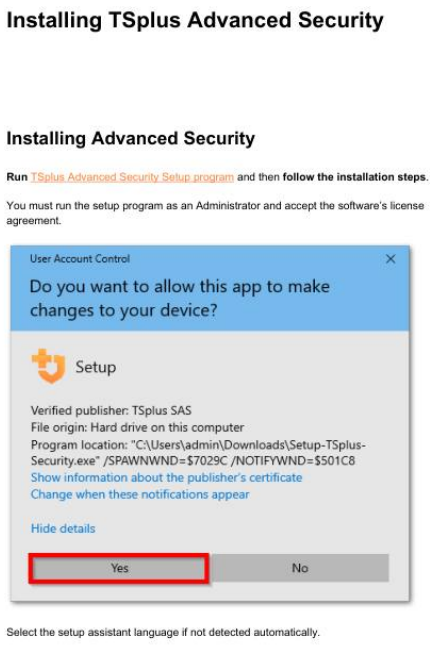
TÜRKÇE İÇERİK

Kaynak sayfa 56/99

Uygulama dilinizi algılamadıysa lütfen sağ üst köşede bulunan açılır menüyü kullanarak ekran dilinizi seçin.

Son olarak, "Yardım" düğmesine tıklamak sizi bu belgeye yönlendirecektir.

RESMÎ KAYNAK GÖRSELİ



TÜRKÇE İÇERİK

Kaynak sayfa 57/99

TSplus Advanced Security kurulumu

Gelişmiş Güvenlik Kurulumu

TSplus Advanced Security Kurulum programını çalıştırın ve ardından kurulum adımlarını izleyin.

Kurulum programını Yönetici olarak çalıştırmanız ve yazılımın lisans anlaşmasını kabul etmeniz gerekir.

Otomatik olarak algılanmazsa kurulum yardımcı dilini seçin.

RESMÎ KAYNAK GÖRSELİ

Then, select one of the two options: **Recommended** or **Advanced** by clicking on the corresponding boxes.

The Advanced option adds aditionnal steps which allows you to:

- Only download setup (do not install)
- Use custom proxy settings

Read the licensing agreement and click "I agree" to resume installation.



The program will install on your computer.

A progress bar is displayed at the bottom and reports the progress of the installation.

TÜRKÇE İÇERİK

Ardından, iki seçenekten birini seçin: İlgili kutulara tıklayarak Önerilen veya Gelişmiş.

Gelişmiş seçenek, aşağıdakileri yapmanıza izin veren aditionnal adımlar ekler:

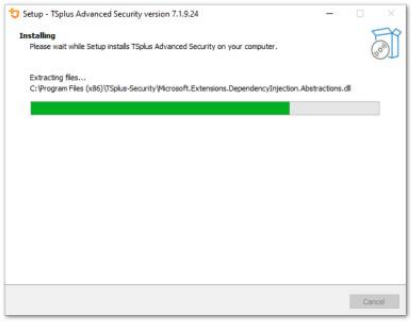
Sadece indirme kurulumu (install etmeyin)
Özel proxy ayarlarını kullanın

Lisans sözleşmesini okuyun ve kuruluma devam etmek için "Kabul ediyorum" ı tıklayın.

Program bilgisayarınıza yüklenecektir.

Alt kısımda bir ilerleme çubuğu görüntülenir ve kurulumun ilerlemesini bildirir.

RESMÎ KAYNAK GÖRSELİ



Please be patient, as it can sometimes take up to a few minutes to fully install the software.



TÜRKÇE İÇERİK

Kaynak sayfa 59/99

Lütfen sabırlı olun, çünkü yazılımın tamamen yüklenmesi bazen birkaç dakika kadar sürebilir.

RESMÎ KAYNAK GÖRSELİ

Once the installation has completed, you can start using TSplus Advanced Security!

The free trial version is fully featured for 15 days. Don't forget to activate your license and to update to the latest version to keep Advanced Security protection at its best!

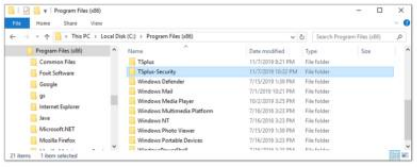
Advanced installation scenarios

The TSplus Advanced Security Classic Setup program handles the following scenarios as it can be executed from the command line:

- Install silently, by providing the /VERYSILENT /SUPPRESSMSGBOXES parameters
- Prevent rebooting at the end of the setup, by providing the /NORESTART parameter. This parameter is usually used along with the above.
- Volume Licensing to activate your license directly while installing (please refer to the documentation or contact us for more information)

Uninstall TSplus Advanced Security

In order to completely uninstall TSplus Advanced Security, open the directory C:\Program Files (x86)\TSplus-Security.



Then, double-click on the "unins000" application to execute the uninstall program.

TÜRKÇE İÇERİK

Kurulum tamamlandıktan sonra TSplus Advanced Security'ı kullanmaya başlayabilirsiniz!

Ücretsiz deneme sürümü 15 gün boyunca tamamen özelliklidir. Lisansınızı etkinleştirmeyi ve Gelişmiş Güvenlik korumasını en iyi şekilde tutmak için en son sürüme güncellemeyi unutmayın!

Gelişmiş kurulum senaryoları

TSplus Advanced Security Classic Setup programı, komut satırından yürütülebileceği gibi aşağıdaki senaryoları ele alır:

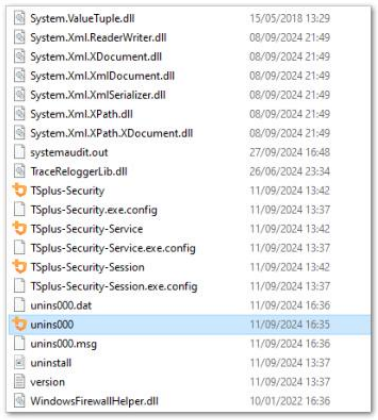
Sessizce yükleyin, /VERYSILENT /SUPSPRESSMSGBOXES parametrelerini sağlayarak Kurulumun sonunda yeniden başlatmayı önleyin, /NORESTART parametresini sağlayarak. Bu parametre genellikle yukarıdakilerle birlikte kullanılır. Yükleme sırasında lisansınızı doğrudan etkinleştirmek için Volume Licensing (lütfen dokümantasyona bakın veya daha fazla bilgi için bizimle iletişime geçin)

TSplus Advanced Security'ı kaldırın

In order to completely uninstall TSplus Advanced Security, open the directory C:\Program Files (x86)\TSplus-Security.

Ardından, kaldırma programını çalıştırmak için "unins000" uygulamasına çift tıklayın.

RESMÎ KAYNAK GÖRSELİ



Click on yes on the next window to completely remove TSplus Advanced Security and all of its components.

Unless configured otherwise, Advanced Security adds blocking rules to the Windows Firewall. Click "Unblock IP addresses" to unblock and remove all the IP addresses previously blocked by Advanced Security.

Important:: Please be mindful that removing all the rules can take up to one hour. Because of this, we would recommend to remove the rules directly from the Windows Firewall with Advanced Security console.

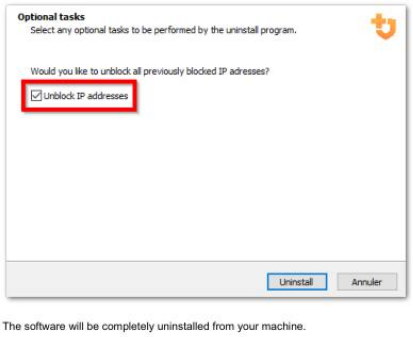
TÜRKÇE İÇERİK

TSplus Advanced Security ve tüm bileşenlerini tamamen kaldırmak için bir sonraki pencereye evet tıklayın.

Aksi yapılandırılmadıkça, Gelişmiş Güvenlik, Windows Güvenlik Duvarı'na engelleme kuralları ekler. Daha önce Gelişmiş Güvenlik tarafından engellenen tüm IP adreslerinin engelini kaldırmak ve kaldırmak için "IP adreslerinin engellenmesini kaldır" ı tıklayın.

Önemli:: Lütfen tüm kuralları kaldırmanın bir saate kadar sürebileceğini unutmayın. Bu nedenle, kuralları Gelişmiş Güvenlik konsoluyla doğrudan Windows Güvenlik Duvarı'ndan kaldırmanızı tavsiye ederiz.

RESMÎ KAYNAK GÖRSELİ



The software will be completely uninstalled from your machine.

TÜRKÇE İÇERİK

Kaynak sayfa 62/99

Yazılım tamamen makinenizden kaldırılacaktır.

RESMÎ KAYNAK GÖRSELİ

Permissions Management

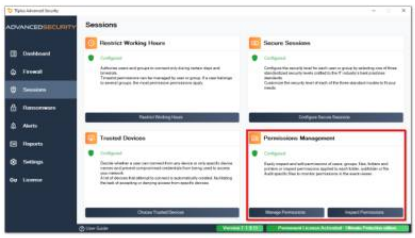
Since version 4.3, TSplus Advanced Security offers a Permissions functionality, allowing the administrator to manage and/or inspect users/groups privileges.

On the Permissions dashboard, the list of users and groups and the list of available **files, folders registries and printers** are showed side-by-side.

Everything is visible at one sight, which makes it super easy to **Inspect** and **Manage/Edit** privileges for one user at a time and therefore to increase the accuracy of the restrictions.

Manage Permissions

On the Manage tab, for each user or group selected on the left tree view, you can:



TÜRKÇE İÇERİK

İzinler Yönetimi

4.3 sürümünden itibaren TSplus Advanced Security, yöneticinin kullanıcı/grup ayrıcalıklarını yönetmesine ve/veya denetlemesine izin veren bir İzinler işlevselliği sunar.

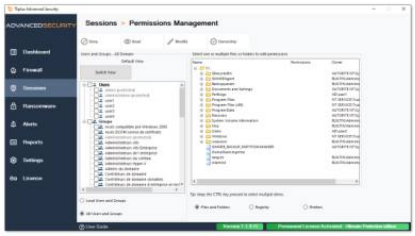
İzinler panosunda, kullanıcıların ve grupların listesi ve mevcut dosyaların, klasörlerin kayıtlarının ve yazıcıların listesi yan yana gösterilir.

Her şey bir bakışta görünür, bu da tek bir kullanıcı için ayrıcalıkları denetlemeyi ve yönetmeyi / düzenlemeyi ve dolayısıyla kısıtlamaların doğruluğunu artırmayı süper kolaylaştırır.

İzinleri Yönet

Yönet sekmesinde, sol ağaç görünümünde seçilen her kullanıcı veya grup için şunları yapabilirsiniz:

RESMÎ KAYNAK GÖRSELİ



- **Deny** - When clicking on the Deny button, the selected user will be denied privilege on the selected filesystem object. If a file is selected, then the selected user is denied the privilege of reading the selected file (FileSystemRights.Read). If a directory is selected, then the selected user is denied the privilege of reading and listing the directory content (FileSystemRights.Read and FileSystemRights.ListDirectory).
- **Read** - When clicking on the Read button, the selected user will be granted privilege on the selected filesystem object. If a file is selected, then the selected user is granted the privilege of reading the selected file and executing if the file is a program (FileSystemRights.ReadAndExecute) . If a directory is selected, then the selected user is granted the privilege of reading and listing or executing the directory content (FileSystemRights.ReadAndExecute and FileSystemRights.ListDirectory and FileSystemRights.Traverse).
- **Modify** - When clicking on the Modify button, the selected user will be granted privilege on the selected filesystem object. If a file is selected, then the selected user is granted the privilege of modifying the selected file (FileSystemRights.Modify) . If a directory is selected, then the selected user is granted the privilege of modifying and listing the directory content, as well as creating new files or directories (FileSystemRights.Modify and FileSystemRights.CreateDirectories and FileSystemRights.CreateFiles and FileSystemRights.ListDirectory and FileSystemRights.Traverse).
- **Ownership** - When clicking on the Ownership button, the selected user will be granted full control over the selected filesystem object (FileSystemRights.FullControl).

Same permissions options are possible for each Registry, by selecting the corresponding button under the right-tree view :

TÜRKÇE İÇERİK

Kaynak sayfa 64/99

Deny - Deny butonuna tıkladığında seçilen kullanıcı seçilen dosya sistemi nesnesinde ayrıcalıktan mahrum kalır. Eğer bir dosya seçilirse, seçilen kullanıcı seçilen dosyayı okuma ayrıcalığı reddedilir (FileSystemRights.Read). Bir dizin seçilirse, o zaman seçilen kullanıcının dizin içeriğini okuma ve listeleme ayrıcalığı reddedilmiştir (FilesystemRights.Read and FileSystemrights.ListDirectory).

Okuma - Oku butonuna tıkladığınızda, seçilen kullanıcıya seçilen dosya sistemi nesnesinde ayrıcalık verilecektir. Bir dosya seçilirse, seçilen kullanıcıya seçili dosyayı okuma ve dosya bir programsa yürütme ayrıcalığı verilir (FileSystemRights.ReadAndExecute).

Bir dizin seçilirse, seçilen kullanıcıya dizin içeriğini okuma ve listeleme veya yürütme ayrıcalığı verilir (FileSystemRights.ReadAndExecute ve FileSystem Rights.ListDirectory and FileSystemyRights.Traverse). Değiştir - Değiştir düğmesine tıkladığında, seçilen kullanıcıya seçilen dosya sistemi nesnesinde ayrıcalık verilecektir.

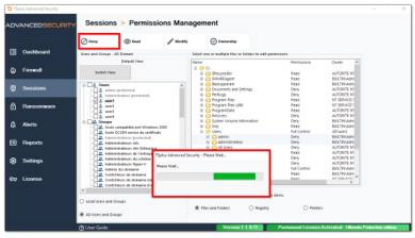
Bir dosya seçilirse, seçilen kullanıcıya seçilen dosyayı değiştirme ayrıcalığı verilir (FileSystemRights.Modify).

Bir dizin seçilirse, seçilen kullanıcıya dizin içeriğini değiştirme ve listeleme ayrıcalığı verilir, ayrıca yeni dosya veya dizinler oluşturma (FileSystemRights.Modify ve FileSystemrights.CreateDirectorys and FileSystemyRights.CreatFiles and FileSistemRrights.ListDirectory and FileStemRight.Traverse).

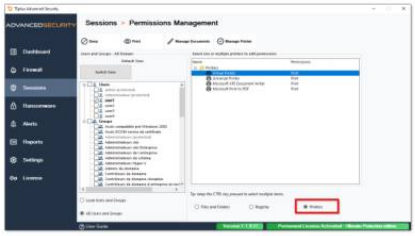
Sahiplik - Sahiplik düğmesine tıkladığınızda, seçilen kullanıcıya seçilen dosya sistemi nesnesi (FileSystemRights.FullControl) üzerinde tam kontrol hakkı verilecektir.

Her Kayıt Defteri için sağ ağaç görünümü altında karşılık gelen düğmeyi seçerek aynı izinler seçenekleri mümkündür:

RESMÎ KAYNAK GÖRSELİ



And for each Printer:



Please note that all permissions denied or granted to a directory are applied recursively to the filesystem objects contained by this directory. The diagram below details the API calls when rights are applied to a filesystem object:

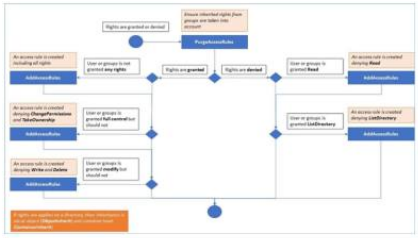
TÜRKÇE İÇERİK

Kaynak sayfa 65/99

Ve her yazıcı için:

Lütfen bir dizine reddedilen veya verilen tüm izinlerin bu dizinin içerdiği dosya sistemi nesnelerine tekrar tekrar uygulandığını unutmayın. Aşağıdaki şema, haklar bir dosya sistemi nesnesine uygulandığında API'nin çağrılarını detaylandırır:

RESMÎ KAYNAK GÖRSELİ

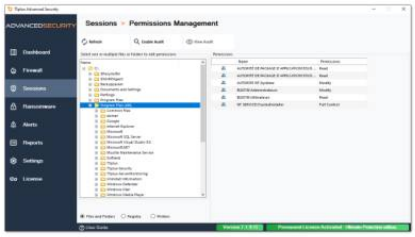


Documentation:

- Object Security: https://docs.microsoft.com/en-us/dotnet/api/system.security.accesscontrol.objectsecurity?view=netframework-4.5.2
- FileSystemRights: https://docs.microsoft.com/en-us/dotnet/api/system.security.accesscontrol.filesystemrights?view=netframework-4.5.2

Inspect Permissions

On the Inspect tab, for each folder, subfolder or file selected on the left tree view, you can see the corresponding attributed permissions to users or groups on the right tree view.



TÜRKÇE İÇERİK

Kaynak sayfa 66/99

Belgelendirme:

Nesne Güvenliği: https://docs.microsoft.com/en-us/dotnet/api/

system.security.accesscontrol.objectsecurity?view=netframework-4.5.2

FileSystemRights: https://docs.microsoft.com/en-us/dotnet/api/

system.security.accesscontrol.filesystemrights?view=netframework-4.5.2

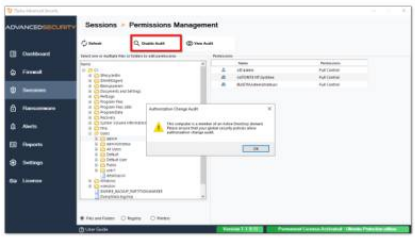
İzinleri İncele

Denetim sekmesinde, sol ağaç görünümünde seçilen her klasör, alt klasör veya dosya için, sağ ağaç görünümünde kullanıcılara veya gruplara karşılık gelen atfedilen izinleri görebilirsiniz.

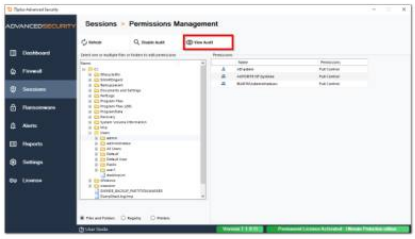
RESMÎ KAYNAK GÖRSELİ

You can refresh the status of the folders for them to be updated in real-time.

An Audit can be enabled by selecting the desired folder, subfolder or file and click on the "Enable Audit" button at the top:



The "View Audit" button allows you to see the corresponding audit on the Event Viewer:



Same Inspections possibilities are available for each registry and printer by selecting the corresponding button under the left-tree view :

TÜRKÇE İÇERİK

Kaynak sayfa 67/99

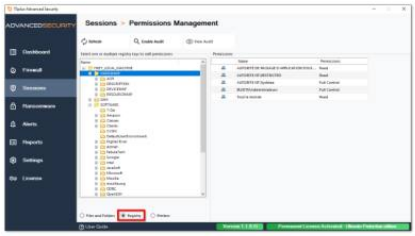
Gerçek zamanlı olarak güncellenmeleri için klasörlerin durumunu yenileyebilirsiniz.

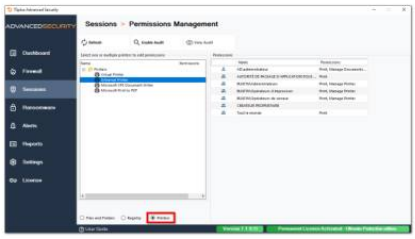
İstenilen klasör, alt klasör veya dosya seçilerek bir Denetim etkinleştirilebilir ve en üstteki "Denetimi Etkinleştir" düğmesine tıklayın:

"Denetlemeyi görüntüle" düğmesi, Olay Görüntüleyicisi'nde ilgili denetimi görmenizi sağlar:

Sol ağaç görünümü altındaki ilgili düğmeyi seçerek her kayıt defteri ve yazıcı için aynı Denetimler olanakları mevcuttur:

RESMÎ KAYNAK GÖRSELİ





TÜRKÇE İÇERİK

Kaynak sayfa 68/99

" Tsplus Gelişmiş Güvenlik - x

İlerleyen Oturumlar > İzin Yönetimi

Retresh Q Enabie DenetimiĞAusit'i görüntüleyin

Dashboard İzinleri düzenlemek için bir veya birden fazla kayıt defteri anahtarı seçin İzinler

İsim x İsim İzinleri

© Firewall (By HKEY_LOCAL_ MACHINE 2 AUTORITE DE PACKAGE D'APPLICATION\TOUS ... Read

cE et 2% OTORITE NTĞRESTRICTED Devamını oku

Gace

& GS AÇIKLAMA SX OTORITE NTĞSyst me Tam Kontrol

Sessions & Devicemap 2 BUILTINAdministrateurs Tam Tartışma

@ Gj RESOURCEMAP e

bir @sM 2 Tout le monde Devamını Oku

@ Ransomware E(B YAZILIM

72

ESĞAmazon

Sınıflar

A Alerts @ @ Clients

Gam

S Defauitusertmvironment

[]_ Raporlar @ Digital River

& GS noktanet

@ G Fabulatech

B @ Google

&3 Ayarlar @ Caitel

GS Javason

Microsok

Gz Lisansı & ES Mozilla

mozillaorg

Kaz

& G5 Açılır y

O Fites ve Klasörler J Registry JO Yazıcılar

@ Kullanıcı Kılavuzu Sürüm 7.1.9.11 Süresiz Lisans Aktif - Nihai Koruma baskısı.

OD Retresh Q Enabie DenetimiĞausit görünümü

Pano İzinleri düzenlemek için bir veya birden fazla yazıcı seçin İzinler

İsim İzinleri İsim İzinleri

FirewallĞYazıcılar tarafından 2 'ADĞadministrateur Yazdır, Belgeleri Yönet...

şişe er 2 OTORITE DE PAKET D'APPLICATIONĞTOUS... Yazdır

' Microsof XPS Belge Yazarı 2 BUILTINAdministrateurs Baskı, Yazıcıyı Yönet

Oturumlar & Microsoft Print to POF 2% BUILTINOpĞrateurs d'impression Baskı, Yazıcıyı Yönet

bir BUILTINĞOp rateurs de serviceur Baskı, Yazıcıyı Yönet

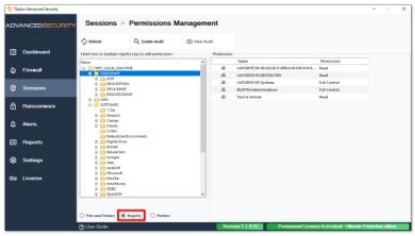
ia) Paseo 2X CREATEUR PROPRIETAIRE

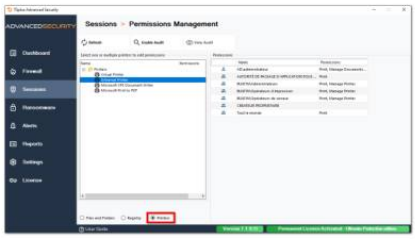
bir Tout le monde baskı

Fi Uyarıları

) Raporlar

RESMÎ KAYNAK GÖRSELİ





TÜRKÇE İÇERİK

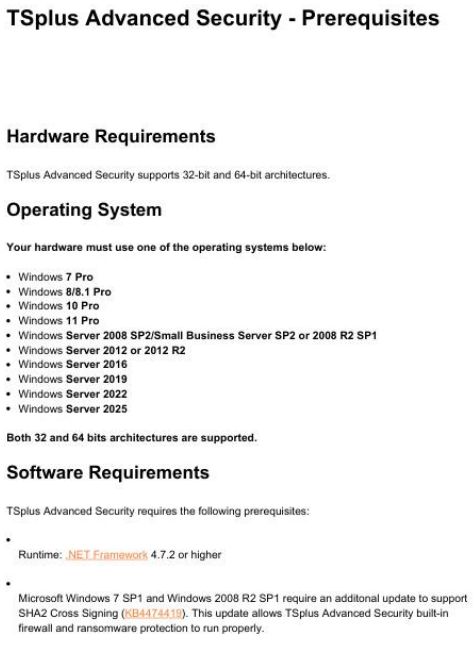
Kaynak sayfa 68/99 • devam 2

3 $ Ayarlar

Gz Lisansı

< >

RESMÎ KAYNAK GÖRSELİ



TSplus Advanced Security - Prerequisites

Hardware Requirements

TSplus Advanced Security supports 32-bit and 64-bit architectures.

Operating System

Your hardware must use one of the operating systems below:

- Windows **7 Pro**
- Windows **8/8.1 Pro**
- Windows **10 Pro**
- Windows **11 Pro**
- Windows **Server 2008 SP2/Small Business Server SP2 or 2008 R2 SP1**
- Windows **Server 2012 or 2012 R2**
- Windows **Server 2016**
- Windows **Server 2019**
- Windows **Server 2022**
- Windows **Server 2025**

Both 32 and 64 bits architectures are supported.

Software Requirements

TSplus Advanced Security requires the following prerequisites:

- Runtime: .NET Framework 4.7.2 or higher
- Microsoft Windows 7 SP1 and Windows 2008 R2 SP1 require an additonal update to support SHA2 Cross Signing (KB4474419). This update allows TSplus Advanced Security built-in firewall and ransomware protection to run properly.

TÜRKÇE İÇERİK

Kaynak sayfa 69/99

TSplus Advanced Security - Ön Koşullar

Donanım Gereksinimleri

TSplus Advanced Security 32-bit ve 64-bit mimarileri destekler.

İşletim Sistemi

Donanımınız aşağıdaki işletim sistemlerinden birini kullanmalıdır:

Windows 7 Pro Windows 8/8.1 Pro Windows 10 Pro Windows 11 Pro Windows Server 2008 SP2/Small Business Server SP2 veya 2008 R2 SP1 Windows Server 2012 veya 2012 R2 Windows Server 2016 Windows Server 2019 Windows Server 2022 Windows Server 2025

32 ve 64 bit mimarileri desteklenmektedir.

Yazılım Gereksinimleri

TSplus Advanced Security aşağıdaki önkoşulları gerektirir:

Çalışma zamanı:.NET Framework 4.7.2 veya daha yüksek

Microsoft Windows 7 SP1 ve Windows 2008 R2 SP1, SHA2 Çapraz İmzalamayı (KB4474419) desteklemek için ek bir güncelleme gerektirir. Bu güncelleştirme, TSplus Advanced Security yerleşik güvenlik duvarı ve ransomware korumasının düzgün çalışmasını sağlar.

RESMÎ KAYNAK GÖRSELİ

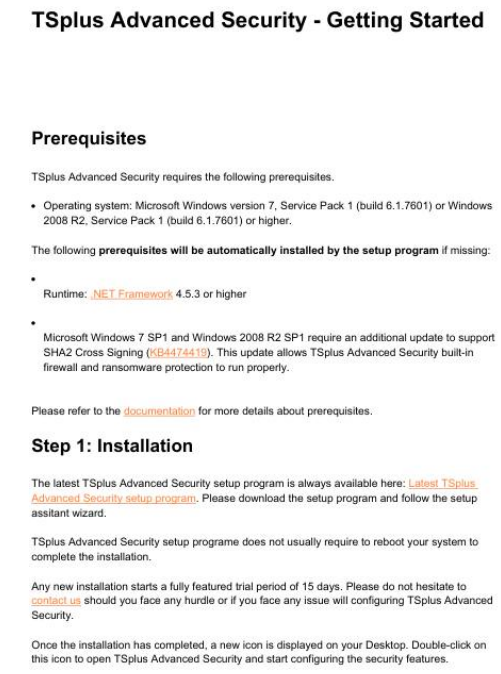


TÜRKÇE İÇERİK

Kaynak sayfa 70/99

Not: Bu önkoşullar, sistemde eksik olmaları durumunda kurulum programı tarafından otomatik olarak yüklenir.

RESMÎ KAYNAK GÖRSELİ



TSplus Advanced Security - Getting Started

Prerequisites

TSplus Advanced Security requires the following prerequisites.

- Operating system: Microsoft Windows version 7, Service Pack 1 (build 6.1.7601) or Windows 2008 R2, Service Pack 1 (build 6.1.7601) or higher.

The following **prerequisites will be automatically installed by the setup program** if missing:

- Runtime: .NET Framework 4.5.3 or higher
- Microsoft Windows 7 SP1 and Windows 2008 R2 SP1 require an additional update to support SHA2 Cross Signing (KB4474419). This update allows TSplus Advanced Security built-in firewall and ransomware protection to run properly.

Please refer to the documentation for more details about prerequisites.

Step 1: Installation

The latest TSplus Advanced Security setup program is always available here: Latest TSplus Advanced Security setup program. Please download the setup program and follow the setup assitant wizard.

TSplus Advanced Security setup programe does not usually require to reboot your system to complete the installation.

Any new installation starts a fully featured trial period of 15 days. Please do not hesitate to contact us should you face any hurdle or if you face any issue will configuring TSplus Advanced Security.

Once the installation has completed, a new icon is displayed on your Desktop. Double-click on this icon to open TSplus Advanced Security and start configuring the security features.

TÜRKÇE İÇERİK

Kaynak sayfa 71/99

TSplus Advanced Security - Başlarken

ÖN KOŞULLAR

TSplus Advanced Security aşağıdaki önkoşulları gerektirir.

İşletim sistemi: Microsoft Windows sürüm 7, Service Pack 1 (yapı 6.1.7601) veya Windows 2008 R2, Service Pack 1. (yapı 6.1.6601) veya daha yüksek.

Aşağıdaki önkoşullar eksik ise kurulum programı tarafından otomatik olarak yüklenecektir:

Çalışma zamanı:.NET Framework 4.5.3 veya daha yüksek

Microsoft Windows 7 SP1 ve Windows 2008 R2 SP1, SHA2 Cross Signing'i (KB4474419) desteklemek için ek bir güncelleme gerektirir. Bu güncelleştirme TSplus Advanced Security yerleşik güvenlik duvarı ve ransomware korumasının düzgün çalışmasını sağlar.

Önkoşullar hakkında daha fazla ayrıntı için lütfen dokümantasyona bakınız.

Adım 1: Kurulum

En son TSplus Advanced Security kurulum programı her zaman burada mevcuttur: Son TSPLUSPROCTAS kurulum programı. Lütfen kurulum programını indirin ve kurulum yardımcı sihirbazını takip edin.

TSplus Advanced Security kurulum programı genellikle kurulumu tamamlamak için sisteminizi yeniden başlatmayı gerektirmez.

Herhangi bir yeni kurulum, 15 günlük tam özellikli bir deneme süresi başlatır. Herhangi bir engelle karşılaşırsanız veya herhangi bir sorunla karşılaşırsanız bizimle iletişime geçmekten çekinmeyin.

Kurulum tamamlandıktan sonra, Masaüstünüzde yeni bir simge görüntülenir. TSplus Advanced Security'ı açmak ve güvenlik özelliklerini yapılandırmaya başlamak için bu simgeye çift tıklayın.

RESMÎ KAYNAK GÖRSELİ



Please refer to the documentation for full installation instructions.

Step 2: Configuring TSplus Advanced Security

You have launch TSplus Advanced Security and begun configuring features to protect your server from malicious activities and enforce strong security policies.



On the left column, the homepage allows a quick access to configure the Ransomware Protection, Bruteforce Protection and Geographic Protection features.

Start Ransomware Protection's learning period to allow Advanced Security to identify legit applications and behaviors on your system by clicking on the following tile:

TÜRKÇE İÇERİK

Kaynak sayfa 72/99

Lütfen tam kurulum talimatları için dokümantasyona bakınız.

Adım 2: TSplus Advanced Security'ı Yapılandırma

TSplus Advanced Security'ı başlattınız ve sunucunuzu kötü niyetli faaliyetlerden korumak ve güçlü güvenlik politikaları uygulamak için özellikleri yapılandırmaya başladınız.

Sol sütunda, ana sayfa Ransomware Koruma, Bruteforce Koruma ve Coğrafi Koruma özelliklerini yapılandırmak için hızlı bir erişim sağlar.

Ransomware Protection'ın öğrenme süresini, Gelişmiş Güvenlik'in aşağıdaki fayansa tıklayarak sisteminizdeki yasal uygulamaları ve davranışları tanımlamasına izin vermek için başlatın:

RESMÎ KAYNAK GÖRSELİ



Bruteforce Protection is usually up-and-running following installation. Otherwise, click on the **Repear defense against bruteforce attacks** tile to resolve issues and applys the required system configuration. By default, this feature blocks attaquants following 10 failed login attempts.



Finally, add your country in the list of authorized countries from where clients are allowed to connect. Click on the tile **Authorize connections from another country** and add your country to configure Geographic Protection

TÜRKÇE İÇERİK

Bruteforce Protection genellikle kurulumdan sonra çalışır ve çalışır. Aksi takdirde, sorunları çözmek için kaba kuvvet saldırılarına karşı Repear savunmasına tıklayın ve gerekli sistem yapılandırmasını uygular. Varsayılan olarak, bu özellik 10 başarısız giriş denemesini takiben attaquants'ı engeller.

Son olarak, ülkenizi müşterilerin bağlanmasına izin verilen yetkili ülkeler listesine ekleyin. Kiremit üzerine tıklayın Başka bir ülkeden bağlantıları yetkilendirin ve coğrafi koruma yapılandırmak için ülkenizi ekleyin

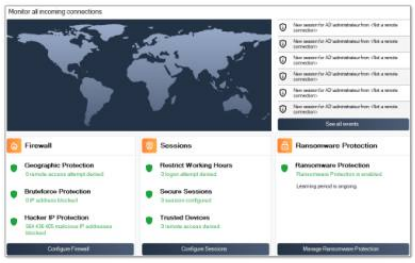
RESMÎ KAYNAK GÖRSELİ



You are all set! Don't forget to activate your license and to update to the latest version to keep Advanced Security protection at its best!

Step 3: Reviewing prevented threats

Now that you have configured the key advanced security features, avoided threats will be reported in the Dashboard.



Also, the Hacker IP protection keeps the machine protected against known threats by blocking more than 500 000 000 known malicious IP addresses.

TÜRKÇE İÇERİK

Kaynak sayfa 74/99

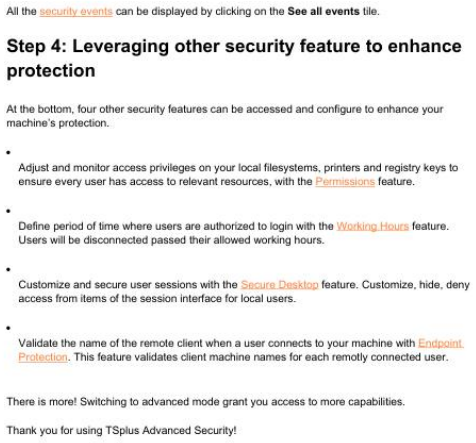
Hepiniz hazırsınız! Lisansınızı etkinleştirmeyi ve Gelişmiş Güvenlik korumasını en iyi şekilde korumak için en son sürüme güncellemeyi unutmayın!

Adım 3: Önlenen tehditleri gözden geçirmek

Artık temel gelişmiş güvenlik özelliklerini yapılandırdığınıza göre, kaçınılan tehditler Dashboard'da bildirilecektir.

Ayrıca, Hacker IP koruması, bilinen 500 000'den fazla kötü niyetli IP adresini engelleyerek makineyi bilinen tehditlere karşı korur.

RESMÎ KAYNAK GÖRSELİ



All the security events can be displayed by clicking on the **See all events** tile.

Step 4: Leveraging other security feature to enhance protection

At the bottom, four other security features can be accessed and configure to enhance your machine's protection.

- Adjust and monitor access privileges on your local filesystems, printers and registry keys to ensure every user has access to relevant resources, with the Permissions feature.
- Define period of time where users are authorized to login with the Working Hours feature. Users will be disconnected passed their allowed working hours.
- Customize and secure user sessions with the Secure Desktop feature. Customize, hide, deny access from items of the session interface for local users.
- Validate the name of the remote client when a user connects to your machine with Endpoint Protection. This feature validates client machine names for each remotly connected user.

There is more! Switching to advanced mode grant you access to more capabilities.

Thank you for using TSplus Advanced Security!

TÜRKÇE İÇERİK

Kaynak sayfa 75/99

Tüm güvenlik olayları, tüm etkinliklerin kiremitini Gör'e tıklayarak görüntülenebilir.

Adım 4: Korumayı artırmak için diğer güvenlik özelliklerinden yararlanmak

Alt kısımda, makinenizin korumasını artırmak için diğer dört güvenlik özelliğine erişilebilir ve yapılandırılabilir.

İzinler özelliği ile her kullanıcının ilgili kaynaklara erişebilmesini sağlamak için yerel dosya sistemlerinizdeki, yazıcılardaki ve kayıt defteri anahtarlarındaki erişim ayrıcalıklarını ayarlayın ve izleyin.

Kullanıcıların Çalışma Saatleri özelliği ile giriş yapmaya yetkili oldukları süreyi belirleyin. Kullanıcılar izin verilen çalışma saatlerini geçtikten sonra bağlantıdan çıkarılacaktır.

Güvenli Masaüstü özelliği ile kullanıcı oturumlarını özelleştirin ve güvenli hale getirin. Yerel kullanıcılar için oturum arayüzünün öğelerinden erişimi özelleştirin, gizleyin, reddedin.

Bir kullanıcı Endpoint Protection ile makinenize bağlandığında uzak istemcinin adını doğrulayın. Bu özellik, her bir remotly bağlı kullanıcı için istemci makine adlarını doğrular.

Daha fazlası var! Gelişmiş moda geçmek daha fazla yeteneğe erişmenizi sağlar.

TSplus Advanced Security kullandığınız için teşekkür ederiz!

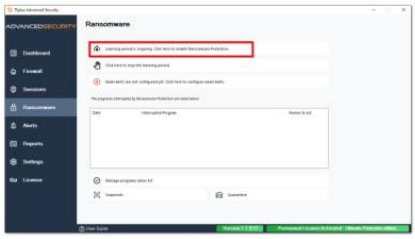
RESMÎ KAYNAK GÖRSELİ

Ransomware Protection

The Ransomware Protection enables you to efficiently DETECT, BLOCK and PREVENT ransomware attacks. TSplus Advanced Security reacts as soon as it detects ransomware on your session. It possesses both **static and behavioral analysis**:

- The **static analysis** enables the software to react immediately when an extension name changed,
- The **behavorial analysis** looks at how a program will interact with files and detect new strain of ransomware.

You can enable it by clicking on the "Enable Ransomware Protection" on the Ransomware Protection tab:



Learning Period

After enabling the Ransomware Protection feature, the Learning Period is automatically activated. During the Learning Period, all programs detected by the Ransomware Protection feature will be considered as false positive and will be able to resume their execution. The programs detected as false positive will be automatically added to the list of allowed programs.

TÜRKÇE İÇERİK

Ransomware Koruması

Ransomware Koruma verimli DETECT, BLOCK ve ÖNCE Ransombus saldırıları sağlar. TSplus Advanced Security oturumunda ransomware algılar gibi en kısa sürede tepki verir. Bu statik ve davranışsal analiz hem sahiptir:

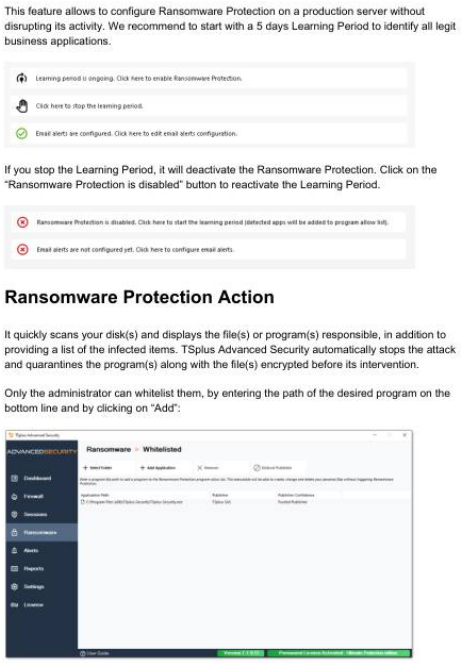
Statik analiz, yazılımın bir uzantı adı değiştiğinde hemen tepki vermesini sağlar, behavorial analiz, bir programın dosyalarla nasıl etkileşime gireceğini ve yeni ransomware türünü nasıl algılayacağını inceler.

Ransomware Koruma sekmesinde "Enable Ransombus Protection" butonuna tıklayarak etkinleştirebilirsiniz:

Öğrenme Dönemi

Ransomware Koruma özelliğini etkinleştirdikten sonra, Öğrenme Süresi otomatik olarak etkinleştirilir. Öğrenme Dönemi boyunca, Ransombus Koruma özelliği tarafından tespit edilen tüm programlar yanlış pozitif olarak kabul edilecek ve yürütmelerine devam edebilecektir. Yanlış pozitif olarak algılanan programlar, izin verilen programların listesine otomatik olarak eklenecektir.

RESMÎ KAYNAK GÖRSELİ



TÜRKÇE İÇERİK

Bu özellik, Ransomware Protection'ı faaliyetlerini bozmadan bir üretim sunucusunda yapılandırmaya izin verir. Tüm yasal iş uygulamalarını tanımlamak için 5 günlük Öğrenme Süresi ile başlamanızı tavsiye ederiz.

Öğrenme Süresini durdurursanız, Ransomware Korumasını devre dışı bırakır. Öğrenme Süresini yeniden etkinleştirmek için "Ransomware Koruması devre dışı" düğmesine tıklayın.

Ransomware Koruma Eylem

Disk(ler)inizi hızlı bir şekilde tarar ve virüslü öğelerin bir listesini sağlamanın yanı sıra sorumlu olan dosya veya programları görüntüler. TSplus Advanced Security, saldırıyı otomatik olarak durdurur ve müdahalesinden önce şifrelenen dosya(lar) ile birlikte programı karantinaya alır.

Alt satırda istenen programın yoluna girerek ve "Ekle" yi tıklatarak yalnızca yönetici bunları beyaz listeye alabilir:

RESMÎ KAYNAK GÖRSELİ

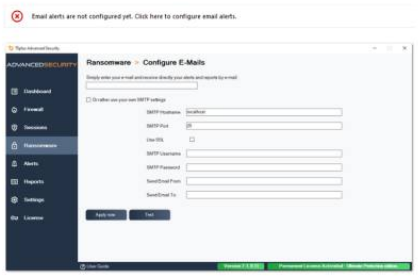
Ransomware Protection Report

TSplus Advanced Security prevents catastrophic events for businesses by removing ransomware at an early stage.

The administrator has access to information regarding the source of the attack and running processes, and therefore learns how to anticipate these threats.

Note: Ransomware Protection observes how programs interact with system and personal files. To ensure a greater level of protection, Ransomware Protection creates bait files in key folders where ransomware often begins its attack. Therefore, a few hidden files may appear in the users' desktop and documents folders, as well as in other locations. When it detects a malicious behaviour, it stops the ransomware immediately (or ask if the logged user is an administrator). Ransomware Protection uses pure behavioural detection techniques and does not rely on malware signatures, allowing it to catch ransomware which does not exist yet.

You can configure your SMTP settings in order for TSplus Advanced Security to send you email alerts to highlight important security events by clicking on the button below the Ransomware activation one:



Enter your SMTP Hostname, Port and check the Use SSL box and change change the port from 25 to 465 if you wish to use SSL.

Enter the SMTP Username and Password, as well as the sender and receiver addresses.

Email Settings can be validated by sending a test when saving SMTP settings.

TÜRKÇE İÇERİK

Ransomware Koruma Raporu

TSplus Advanced Security, erken bir aşamada ransomware kaldırarak işletmeler için felaket olayları önler.

Yönetici, saldırının kaynağı ve işleyen süreçlerle ilgili bilgilere erişebilir ve bu nedenle bu tehditleri nasıl öngöreceğini öğrenir.

Not: Ransomware Koruması programların sistem ve kişisel dosyalarla nasıl etkileşime girdiğini gözlemler. Daha yüksek bir koruma düzeyi sağlamak için Ransombus Protection, ransomware'in genellikle saldırıya başladığı kilit klasörlerde yem dosyaları oluşturur. Bu nedenle, kullanıcıların masaüstünde ve belge klasörlerinde ve diğer yerlerde birkaç gizli dosya görünebilir.

Kötü niyetli bir davranış algıladığında, fidye yazılımı hemen durdurur (veya oturum açmış kullanıcının yönetici olup olmadığını sorun). Ransomware Protection, saf davranış algılama tekniklerini kullanır ve kötü amaçlı yazılım imzalarına güvenmez, henüz mevcut olmayan fidye yazılımlarını yakalamasına izin verir.

TSplus Advanced Security'ın önemli güvenlik olaylarını vurgulamak için size e-posta uyarıları göndermesi için SMTP ayarlarınızı Ransomware aktivasyonunun altındaki düğmeye tıklayarak yapılandırabilirsiniz:

SMTP Hostname, Port'unuzu girin ve SSL kullanmak istiyorsanız SSL kutusunu kullanın ve 25'ten 465'e kadar port değiştirin.

SMTP Kullanıcı Adı ve Şifre'nin yanı sıra gönderen ve alıcı adreslerini girin.

E-posta Ayarları SMTP ayarlarını kaydederken bir test göndererek doğrulanabilir.

RESMÎ KAYNAK GÖRSELİ

Snapshots

Snaphshots taken by Ransomware Protection are visible under the Snapshots tab:



The list can be refreshed by clicking on the corresponding button. Each element can be restored or removed.

Quarantine

Quarantined programs are visible under the Quarantine tab:
Potentially unwanted programs are kept in quarantine indefinitely until you decide on the action to take.

This way, Advanced Security ensures the safety of your machine while giving you the option to manage quarantined items as you choose.
This can be useful if you need to retrieve a file or program that was neutralized. **This decision is made at your own risk.**
You can also permanently delete any files or programs you choose directly from the quarantine folder located in the Advanced Security installation directory.

TÜRKÇE İÇERİK

Snapshots

Ransomware Protection tarafından çekilen Snaphshot'lar Snapshots sekmesi altında görülebilir:

Liste, ilgili düğmeye tıklayarak yenilenebilir. Her eleman geri yüklenebilir veya kaldırılabilir.

Karantina

Karantinalı programlar Karantina sekmesi altında görülebilir: Potansiyel olarak istenmeyen programlar, harekete karar verene kadar süresiz karantinada tutulur.

almak için.

Bu şekilde, Gelişmiş Güvenlik, seçtiğiniz karantinalı öğeleri yönetme seçeneği sunarken makinenizin güvenliğini sağlar. Nötralize edilmiş bir dosyayı veya programı almanız gerekiyorsa bu yararlı olabilir. Bu karar

kendi riskinize göre yapılır. Ayrıca doğrudan karantinadan seçtiğiniz herhangi bir dosyayı veya programı kalıcı olarak silebilirsiniz

Gelişmiş Güvenlik kurulum dizininde bulunan dizin.

RESMÎ KAYNAK GÖRSELİ



Each element can be restored or removed.

Ignored files are not used to detect possible malicious actions and are not saved when they are modified. The idea is to exclude any operation on large or irrelevant files (such as log files).

- sys
- dll
- exe
- tmp
- ~tmp
- temp
- cache
- lnk
- 1
- 2
- 3
- 4
- 5
- LOG1
- LOG2
- customDestinations-ms
- log
- wab~
- vmc
- vhd
- vhdx
- vdi
- vo1
- vo2
- vsv

TÜRKÇE İÇERİK

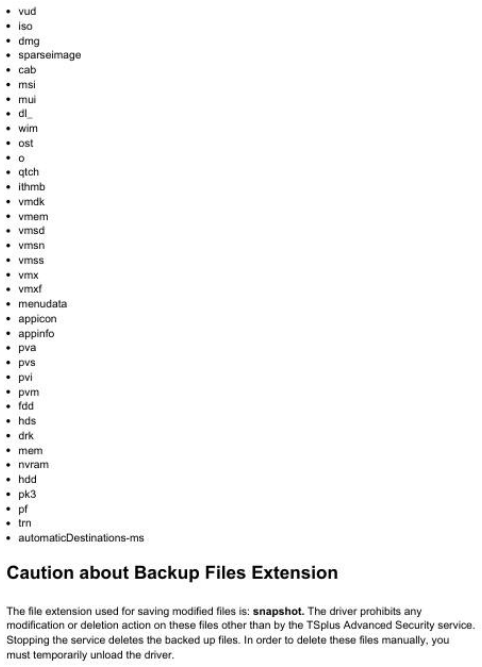
Kaynak sayfa 80/99

Her eleman geri yüklenebilir veya çıkarılabilir.

Göz ardı edilen dosyalar olası kötü niyetli eylemleri tespit etmek için kullanılmaz ve değiştirildiğinde kaydedilmez. Fikir, büyük veya alakasız dosyalardaki (log dosyaları gibi) herhangi bir işlemi dışlamaktır.

sys dll exe tmpĞtmp temp önbellek lnk 1 2 3 4 5 LOG1 LOG2 customDestinations-ms log wabĞvmc vhdx vdi vo1 vo2 vsv

RESMÎ KAYNAK GÖRSELİ



- vud
- iso
- dmg
- sparseimage
- cab
- msi
- mui
- dl_
- wim
- ost
- o
- qtch
- ithmb
- vmdk
- vmem
- vmsd
- vmsn
- vmss
- vmx
- vmxf
- menudata
- appicon
- appinfo
- pva
- pvs
- pvi
- pvm
- fdd
- hds
- drk
- mem
- nvram
- hdd
- pk3
- pf
- trn
- automaticDestinations-ms

Caution about Backup Files Extension

The file extension used for saving modified files is: **snapshot.** The driver prohibits any modification or deletion action on these files other than by the TSplus Advanced Security service. Stopping the service deletes the backed up files. In order to delete these files manually, you must temporarily unload the driver.

TÜRKÇE İÇERİK

vud iso dmg seyrek görüntü taksi msi mui dl_ wim ost o qtch ithmb vmdk vmsd vmsn vmx vmxf menudata appicon appinfo pvs pvi pvm fd hds drk mem nvram hd pk3 pft

Yedekleme Dosyaları Uzantısı Hakkında Uyarı

Değiştirilmiş dosyaları kaydetmek için kullanılan dosya uzantısı şudur: anlık görüntü. Sürücü, TSplus Advanced Security hizmeti dışında bu dosyalarda herhangi bir değişiklik veya silme işlemini yasaklar. Hizmetin durdurulması yedeklenmiş dosyaları siler. Bu dosyaları manuel olarak silmek için sürücüyü geçici olarak boşaltmanız gerekir.

RESMÎ KAYNAK GÖRSELİ



Backup File Configuration

By default, the directory of saved files is located in the installation directory of TSplus Advanced Security and is called "snapshots". However, it is possible to define another location for this directory. This can allow the administrator to define a directory located on a faster disk (SSD) or on a larger disk according to his needs. The backup directory path must not be a UNC path, in the form of:

\\<computer name>\<backup directory>\

Adding Backup Utilities to the Whitelist

We recommend adding backup utilities in the Whitelist.

TÜRKÇE İÇERİK

Yedekleme Dosya Yapılandırması

Varsayılan olarak, kaydedilen dosyaların dizini TSplus Advanced Security'ın kurulum dizininde bulunur ve "snapshots" olarak adlandırılır. Bununla birlikte, bu dizin için başka bir konum tanımlamak mümkündür. Bu, yöneticinin ihtiyaçlarına göre daha hızlı bir diskte (SSD) veya daha büyük bir diskte bulunan bir dizini tanımlamasına izin verebilir. Yedekleme dizini yolu UNC yolu olmamalıdır, şeklinde:

\\<computer name>\<backup directory>\

Whitelist'e Yedekleme Yardımcıları Ekleme

Whitelist'e yedek yardımcı programlar eklemenizi tavsiye ederiz.

RESMÎ KAYNAK GÖRSELİ

Reports



TÜRKÇE İÇERİK

Kaynak sayfa 83/99

“ Tsplus Gelişmiş Güvenlik - 7.1.9.30 - x

İLERİ Raporlar

E-Posta ayarlarını düzenle

GÖSTERGE PANELİ

Aşağıdaki e-posta adresine rapor alın: thomas montalcino@tsplus net

Güvenlik duvarı..

Rapora dahil edilecek bölümler: 7] Firewall

Ransomware Koruması

Oturumlar

Oturumlar

@) Ransomware Raporunuzu ne sıklıkta almak istediğinizi seçin:

@Günlük

i Uyarılar O Haftalık Staringon Cumartesi. Eylül 28,2024 v

- Aylık

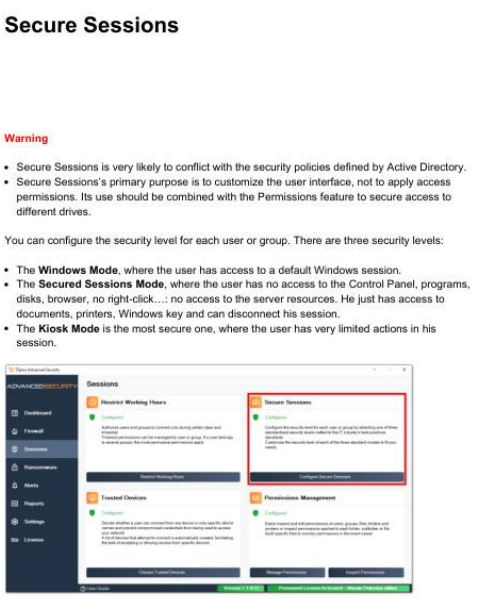
RAPORLAR

3 Ayarlar

G Lisansı

@ Kullanıcı Kılavuzu Sürüm 7.19.30 Süresiz Lisans Aktif - Nihai Koruma baskısı.

RESMÎ KAYNAK GÖRSELİ



Secure Sessions

Warning

- Secure Sessions is very likely to conflict with the security policies defined by Active Directory.
- Secure Sessions's primary purpose is to customize the user interface, not to apply access permissions. Its use should be combined with the Permissions feature to secure access to different drives.

You can configure the security level for each user or group. There are three security levels:

- The **Windows Mode**, where the user has access to a default Windows session.
- The **Secured Sessions Mode**, where the user has no access to the Control Panel, programs, disks, browser, no right-click…: no access to the server resources. He just has access to documents, printers, Windows key and can disconnect his session.
- The **Kiosk Mode** is the most secure one, where the user has very limited actions in his session.

TÜRKÇE İÇERİK

Güvenli Oturumlar

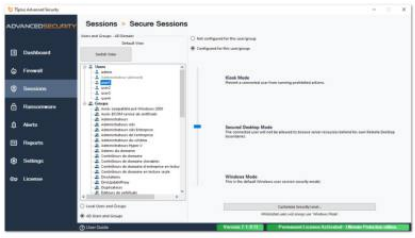
Uyarı

Güvenli Oturumlar, Active Directory tarafından tanımlanan güvenlik politikalarıyla çakışma olasılığı yüksektir. Güvenli Oturumlar'ın birincil amacı, erişim izinlerini uygulamak için değil, kullanıcı arayüzünü özelleştirmektir. Kullanımı, farklı sürücülere erişimi güvence altına almak için İzinler özelliği ile birleştirilmelidir.

Her kullanıcı veya grup için güvenlik seviyesini yapılandırabilirsiniz. Üç güvenlik seviyesi vardır:

Kullanıcının varsayılan bir Windows oturumuna erişebildiği Windows Modu. Kullanıcının Denetim Masası, programlar, diskler, tarayıcı, sağ tıklama olmadan erişemediği Güvenli Oturumlar Modu...: sunucu kaynaklarına erişim yok. Sadece belgelere, yazıcılara, Windows anahtarına erişimi var ve oturumunu devre dışı bırakabilir. Kiosk Modu, kullanıcının oturumunda çok sınırlı eylemleri olduğu en güvenli olanıdır.

RESMÎ KAYNAK GÖRSELİ



Customization

In any mode, you have the possibility to customize the security on three levels:

Desktop Security:

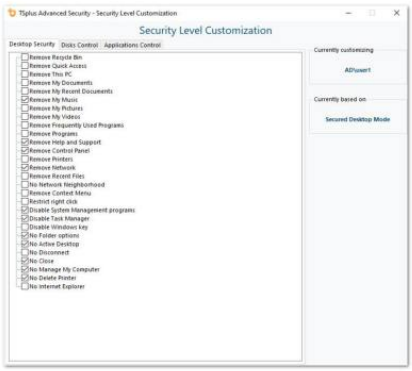
TÜRKÇE İÇERİK

Özelleştirme

Herhangi bir modda, güvenliği üç seviyede özelleştirme olanağınız vardır:

Masaüstü Güvenliği:

RESMÎ KAYNAK GÖRSELİ



Disks Control:

TÜRKÇE İÇERİK

Kaynak sayfa 86/99

» TSplus Advanced Security - Güvenlik Düzeyi Özelleştirme = x Güvenlik Seviyesi Özelleştirme Masaüstü Güvenlik Diskleri Kontrol Uygulamaları Kontrol P Şu anda özelleştirme

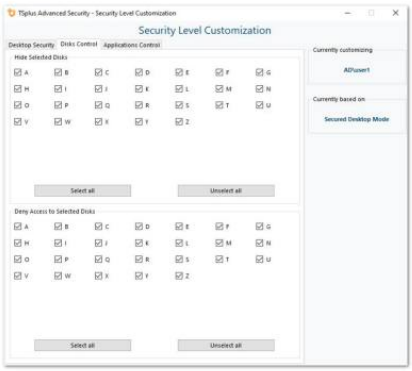
Rl Geri Dönüşüm Kutusunu Kaldır - -[]Hızlı Erişimi Kaldır.

Oo Remove This PC et } Oo Remove My Documents i Remove My Recent Documents ~-fZ]Remove My Music Currently based on ~-{JRemove My Pictures '~{_]Remove My Videos Secured Desktop Mode -~-(_]Remove Frequently Used Programs (J Remove Programs Pe ae Remove Help and Support fw Remove Control Panel -O Remove Printers S| Remove Network } Oo Remove Recent Files ~~-[[JNo Network Neighborhood --[_JRemove Context Menu (Restrict right

) Sistem Yönetimi programlarını devre dışı bırak -[Y] Görev Yöneticisini devre dışı bırak ' (L) Windows tuşunu devre dışı bırak A No Klasör seçenekleri S No Active Desktop Oo No Disconnect S No Close No Manage My Computer - -Z]No Delete Printer '[_]No Internet Explorer

Diskler Kontrolü:

RESMÎ KAYNAK GÖRSELİ



Applications Control:

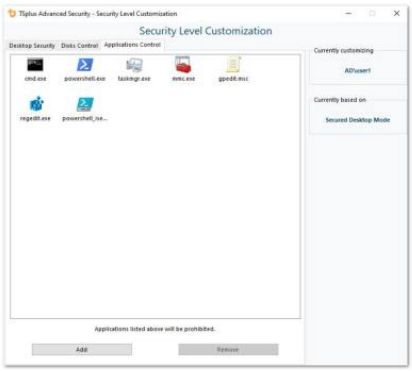
TÜRKÇE İÇERİK

Kaynak sayfa 87/99

vo TSplus Advanced Security - Güvenlik Düzeyi Özelleştirme 4 x Güvenlik Seviyesi Özelleştirme Masaüstü Güvenlik Diskleri Kontrol Uygulamaları Denetimi Şu anda Özelleştirme Hide Selected Disks Ma Me Mc Mo Me Mc ives MH Mt M3 Mk Mt Mu N Şu anda Mo Me'ye dayalı M Ms Mt u Mv Mw Mx My Mz Mz Mq Secured Desktop Mode (Unsetectath Deny Access to Selected Diskes A Me Me Me Ms Mn c D Me)

Uygulamalar Kontrolü:

RESMÎ KAYNAK GÖRSELİ



Users/Groups rules priorities

When a user opens a new session on the server:

1. If this user has a Security Level directly defined for himself, then this Security Level is enforced.
2. If this user does not have a Security Level directly defined for himself, then TSplus Advanced Security will load any existing Security Level settings for all the groups of this user, and keep the more permissive rules.

For instance if a first group has a rule to remove the Recycle Bin icon from the desktop, but this rule is disabled for a second group, then the user will have the Recycle Bin icon on his desktop. The same priority rules will apply on every custom rule (Desktop Security, Disks Control and Applications Control) as well as for the principal Security Level (the Windows Mode being considered more permissive than the Secured Desktop Mode, which is considered more permissive than the Kiosk Mode).

N.B : In order to disable the right click everywhere, you must select the following two options:

- Restrict Right Click

TÜRKÇE İÇERİK

Kullanıcılar/Gruplar öncelikleri belirler

Bir kullanıcı sunucuda yeni bir oturum açtığında:

Bu kullanıcının kendisi için doğrudan tanımlanmış bir Güvenlik Seviyesi varsa, bu Güvenlik Seviyesi 1'dir.

zorla. Bu kullanıcının kendisi için doğrudan tanımlanmış bir Güvenlik Seviyesi yoksa, o zaman TSplus Advanced 2.

Güvenlik, bu kullanıcının tüm grupları için mevcut herhangi bir Güvenlik Seviyesi ayarını yükleyecek ve daha izin verici kuralları koruyacaktır.

Örneğin, bir ilk grubun masaüstünden Geri Dönüşüm Kutusu simgesini kaldırma kuralı varsa, ancak bu kural ikinci bir grup için devre dışı bırakılırsa, kullanıcı masaüstünde Geri Dönüşüm Kutusu ikonuna sahip olacaktır.

Aynı öncelik kuralları, her özel kuralda (Desktop Security, Disks Control and Applications Control) ve ana Güvenlik Seviyesinde (Windows Modu, Kiosk Modundan daha müsamahakar olarak kabul edilen Masaüstü Masaüstü Modundan daha izinli olarak kabul edilir) geçerli olacaktır.

N.B: Her yerde sağ tıklamayı devre dışı bırakmak için aşağıdaki iki seçeneği seçmeniz gerekir:

Sağ Tıklamayı Kısıtla

RESMÎ KAYNAK GÖRSELİ

TÜRKÇE İÇERİK

Kaynak sayfa 89/99

e Bağlam Menüsünü Kaldır

RESMÎ KAYNAK GÖRSELİ

Settings - Programs Allow List

On the **Programs tab**, you can add programs to the list of allowed programs, that won't be checked by TSplus Advanced Security's Ransomware Protection. By default, all Microsoft programs are whitelisted.



Click on the "Add Application" button to add a program. You can also remove them by selecting application(s) and clicking on the Remove Application(s) button.

TÜRKÇE İÇERİK

Ayarlar - Programlar Listeye İzin Veriyor

Programlar sekmesinde, izin verilen programlar listesine TSplus Advanced Security'ın Ransomware Koruması tarafından kontrol edilmeyecek programlar ekleyebilirsiniz. Varsayılan olarak, tüm Microsoft programları beyaz listeye alınmıştır.

Bir program eklemek için "Uygulama Ekle" düğmesine tıklayın. Uygulama(lar)ı seçerek ve Uygulamayı Kaldır(lar) düğmesine tıklayarak bunları da kaldırabilirsiniz.

RESMÎ KAYNAK GÖRSELİ

Settings - Users Allow List

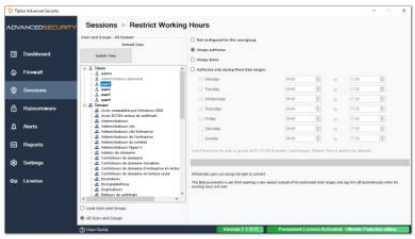
Advanced View

With the Advanced view, add and manage users and groups from every accessible domains.

You can switch view from the Default view to the Advanced View using the "Switch View" button.

The Advanced view is used to display and manage every current configured user and groups. It also allows you to add new user and group to the list to configure them as well, using the windows AD search picker. You can do so by clicking on the "Add user/group" button.You will then be able to add any user available from any accessible domains from your server.

The Advanced View is available on the Permissions, Working Hours, Secure Desktops features. Example:



The **Users Whitelist** tab gives the Administrator the possibility to add/remove users from the whitelist.

Users on the whitelist are ignored by TSplus Advanced Security and their settings will not be applied.

TÜRKÇE İÇERİK

Ayarlar - Kullanıcılar Listeye İzin Verebilir

Gelişmiş Görünüm

Gelişmiş görünümle, her erişilebilir etki alanından kullanıcıları ve grupları ekleyin ve yönetin.

Öntanımlı görünümden Gelişmiş Görünüm'e "Görünüm Değiştir" düğmesini kullanarak geçiş yapabilirsiniz.

Gelişmiş görünüm, her güncel yapılandırılmış kullanıcı ve grubu görüntülemek ve yönetmek için kullanılır. Ayrıca, Windows AD arama seçicisini kullanarak bunları yapılandırmak için listeye yeni kullanıcı ve grup eklemenize izin verir. Bunu "Kullanıcı/grup ekle" düğmesine tıklayarak yapabilirsiniz. Daha sonra sunucunuzdan erişilebilen herhangi bir etki alanından mevcut olan herhangi bir kullanıcıyı ekleyebilirsiniz.

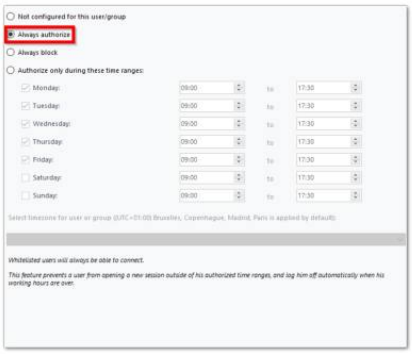
Gelişmiş Görünüm, İzinler, Çalışma Saatleri, Güvenli Masaüstü özelliklerinde mevcuttur. Örnek:

Kullanıcılar Beyaz Liste sekmesi, Yöneticiye kullanıcıları beyaz listeden ekleme / kaldırma olanağı verir.

Beyaz listedeki kullanıcılar TSplus Advanced Security tarafından göz ardı edilir ve ayarları uygulanmaz.

RESMÎ KAYNAK GÖRSELİ

The user who installed TSplus Advanced Security is automatically added to the Whitelist:



TÜRKÇE İÇERİK

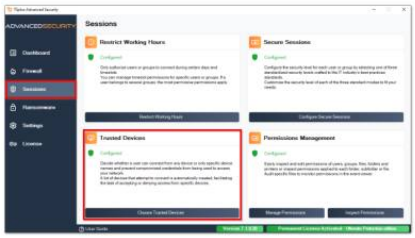
Kaynak sayfa 92/99

TSplus Advanced Security'ı yükleyen kullanıcı otomatik olarak Whitelist'e eklenir:

RESMÎ KAYNAK GÖRSELİ

Trusted Devices

Trusted Devices allows you to control users device by allowing each user to use only one or multiple specific device(s), which will be checked on any incoming session. A logon from any invalid device name will be blocked.





TÜRKÇE İÇERİK

Güvenilir Cihazlar

Güvenilir Cihazlar, her kullanıcının herhangi bir gelen oturumda kontrol edilecek yalnızca bir veya birden fazla belirli cihaz(lar) kullanmasına izin vererek kullanıcı cihazını kontrol etmenizi sağlar. Herhangi bir geçersiz aygıt adından bir logo engellenecektir.

RESMÎ KAYNAK GÖRSELİ



On this example, **User1** will be using the device name **TSPLUS-SERVER1** only.

Auto-fill of device name field

You might notice that the Device Name field is already filled with a device name for some users. In order to help the administrator, TSplus Advanced Security will automatically save the name of the latest device used to connect to the server by any user who does not have Trusted Devices feature enabled. After one working day, the device name of most users will be known by advanced-security, thus allowing you to quickly enable the Endpoint Protection feature without having to check every user's workstation name.

Note: Trusted Devices is not compatible with HTML5 connections.

TÜRKÇE İÇERİK

Kaynak sayfa 94/99

Bu örnekte, User1 yalnızca TSPLUS-SERVER1 aygıt adını kullanacak.

Cihaz adı alanının otomatik doldurulması

Aygıt Adı alanının bazı kullanıcılar için zaten bir aygıt adı ile doldurulduğunu fark edebilirsiniz. Yöneticiye yardımcı olmak için TSplus Advanced Security, Güvenilir Cihazlar özelliği etkin olmayan herhangi bir kullanıcı tarafından sunucuya bağlanmak için kullanılan en son cihazın adını otomatik olarak kaydeder.

Bir iş gününden sonra, çoğu kullanıcının cihaz adı gelişmiş güvenlik tarafından bilinecek ve böylece her kullanıcının iş istasyonu adını kontrol etmek zorunda kalmadan Endpoint Protection özelliğini hızlı bir şekilde etkinleştirmenizi sağlayacaktır.

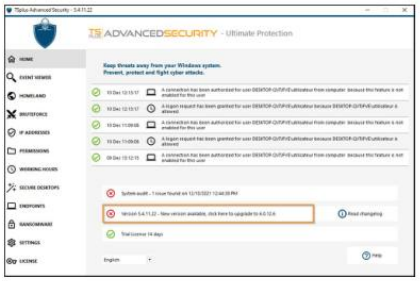
Not: Güvenilir Cihazlar HTML5 bağlantıları ile uyumlu değildir.

RESMÎ KAYNAK GÖRSELİ

Updating TSplus Advanced Security

Check out our fixes and improvements by clicking on Changelog

Updating TSplus Advanced Security is easy and can be done by clicking on the corresponding tile, from the Homepage:



Then, TSplus Advanced Security downloads and applies the update.

Note: your data and settings are always backup before an update and can be found in the "archives" directory, in TSplus Advanced Security setup folder. See Backup and restore your data and settings

TÜRKÇE İÇERİK

Kaynak sayfa 95/99

TSplus Advanced Security güncelleniyor

Changelog'a tıklayarak düzeltme ve geliştirmelerimize göz atın

TSplus Advanced Security'ın güncellenmesi kolaydır ve ilgili fayansa tıklayarak yapılabilir, Ana Sayfadan:

Ardından, TSplus Advanced Security güncellemeyi indirir ve uygular.

Not: Verileriniz ve ayarlarınız her zaman bir güncellemeden önce yedeklenir ve TSplus Advanced Security kurulum klasöründe "arşivler" dizininde bulunabilir. Yedekleme'ye bakın ve verilerinizi ve ayarlarınızı geri yükleyin

RESMÎ KAYNAK GÖRSELİ

TÜRKÇE İÇERİK

Kaynak sayfa 96/99

RESMÎ KAYNAK GÖRSELİ

Restrict Working Hours

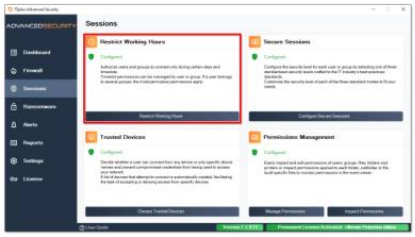
You can configure working hours restrictions per user or per group.

Choose the restriction of your choice:

- Always authorize this user/group access
- Always block this user/group access

or Authorize only during specific time ranges.

You can configure it day by day and select the time range of your preference:



TÜRKÇE İÇERİK

Çalışma Saatlerini Kısıtlama

Kullanıcı başına veya grup başına çalışma saatleri kısıtlamalarını yapılandırabilirsiniz.

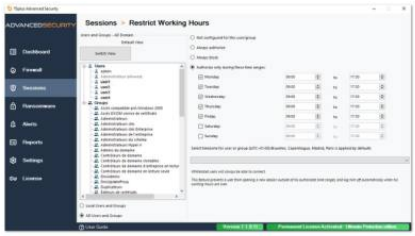
Seçiminizin kısıtlamasını seçin:

Her zaman bu kullanıcı/grup erişimine izin ver Bu kullanıcı/grub erişimini her zaman engelle

veya sadece belirli zaman aralıklarında yetkilendirin.

Gün geçtikçe yapılandırabilir ve tercih ettiğiniz zaman aralığını seçebilirsiniz:

RESMÎ KAYNAK GÖRSELİ



It is possible to select a specific timezone depending on your user's office location.

An automatic disconnection at the end of the configured work time is made.

It is possible to schedule a warning message before the user is logged off from Settings > Advanced > Working Hours.

###Users/Groups rules priorities

When a user opens a new session on the server:

1. if this user has Working Hours restrictions directly defined for himself, then these rules are enforced.

2. if this user does not have Working Hours restrictions directly defined for himself, then TSplus Advanced Security will load any existing Working Hours restrictions for all the groups of this user, and keep the more permissive rules. For instance if a first group has a rule to block the connection on Monday, a second group has a rule to authorize the connection on Monday from 9 AM to 5 PM and a third group has a rule to authorize the connection on Monday from 8AM to 3PM, then the user will be able to open a connection on Monday from 8AM to 5PM.

Warning: This feature uses server's time. Using the user's workstation time and/or time-zone would be pointless, as all the user would only have to change its time-zone to open a session outside his authorized hours.

TÜRKÇE İÇERİK

Kullanıcınızın ofis konumuna bağlı olarak belirli bir saat dilimi seçmek mümkündür.

Yapılandırılmış çalışma süresinin sonunda otomatik bir kopukluk yapılır.

Kullanıcı Ayarlar> Gelişmiş> Çalışma Saatlerinden çıkış yapmadan önce bir uyarı mesajı planlamak mümkündür.

###Kullanıcılar/Gruplar öncelikleri belirler

Bir kullanıcı sunucuda yeni bir oturum açtığında:

1.

Bu kullanıcının kendisi için doğrudan tanımlanmış Çalışma Saatleri kısıtlamaları varsa, bu kurallar uygulanır. 2.

Bu kullanıcının kendisi için doğrudan tanımlanmış Çalışma Saatleri kısıtlamaları yoksa, TSplus Advanced Security bu kullanıcının tüm grupları için mevcut Çalışma Saatleri kısıtlamalarını yükleyecek ve daha izinli kuralları koruyacaktır.

Örneğin, bir ilk grubun Pazartesi günü bağlantıyı engelleme kuralı varsa, ikinci bir grubun Pazartesi günü saat 9'dan 5'e kadar bağlantıya yetki verme kuralı vardır ve üçüncü bir grubun da Pazartesi günü saat 8'den 3'e kadar bağlantıyı yetkilendirme kuralı vardır, ardından kullanıcı Pazartesi günü 8'den 5'e bağlantı açabilecektir.

Uyarı: Bu özellik sunucunun zamanını kullanır. Kullanıcının iş istasyonu saatini ve/veya zaman dilimini kullanmak anlamsız olacaktır, çünkü tüm kullanıcı yetkili saatleri dışında bir oturum açmak için yalnızca zaman dilimini değiştirmek zorunda kalacaktır.

RESMÎ KAYNAK GÖRSELİ

TÜRKÇE İÇERİK

Kaynak sayfa 99/99