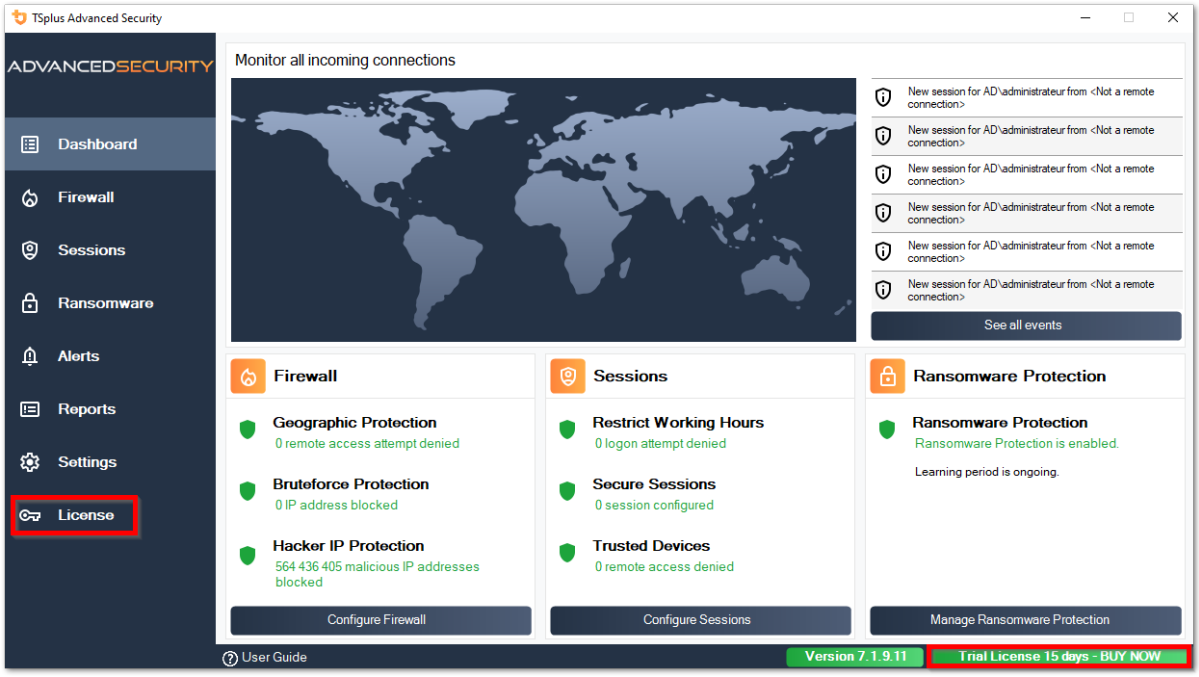
TSplus Advanced Security - 激活您的许可证

步骤 1：从 Lite 模式激活您的许可证

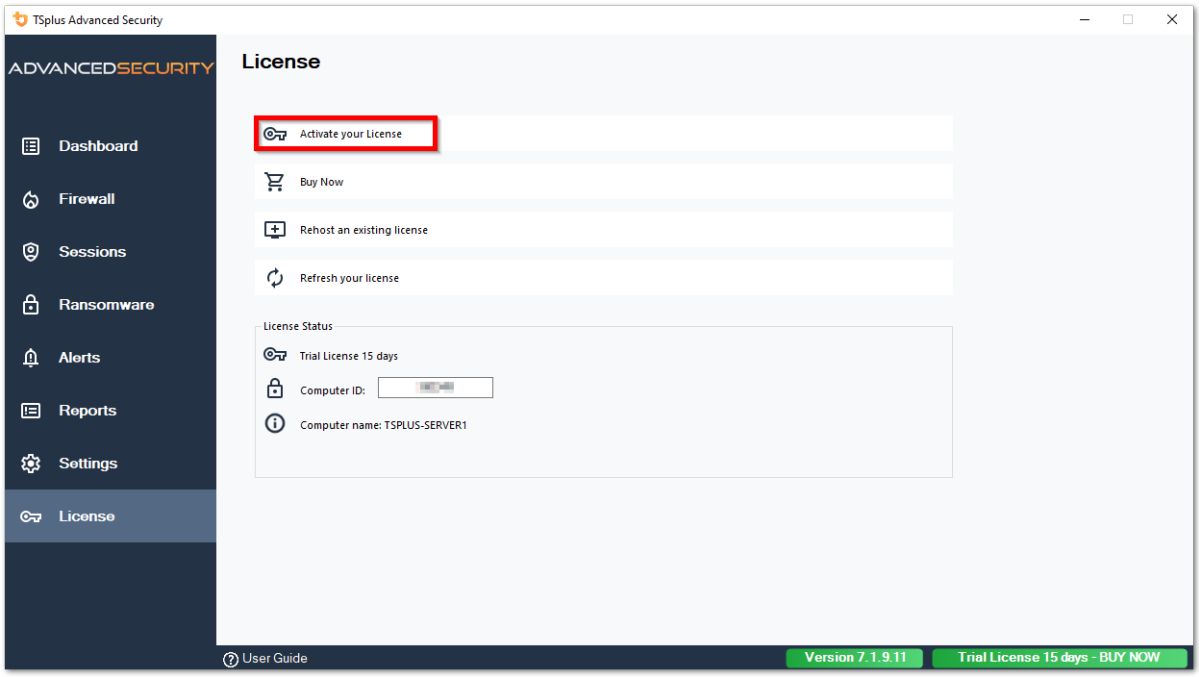
点击“试用许可证”按钮以购买许可证，或者如果您已经拥有许可证和激活密钥，请点击许可证选项卡。



然后，点击“激活您的许可证”按钮。

您将找到您的永久激活密钥 **(XXXX-XXXX-XXXX-XXXX)** 在我们的订单确认电子邮件中。

如果您希望激活您的订阅，请输入您的订阅密钥 **(S-XXXX-XXXX-XXXX-XXXX)** .



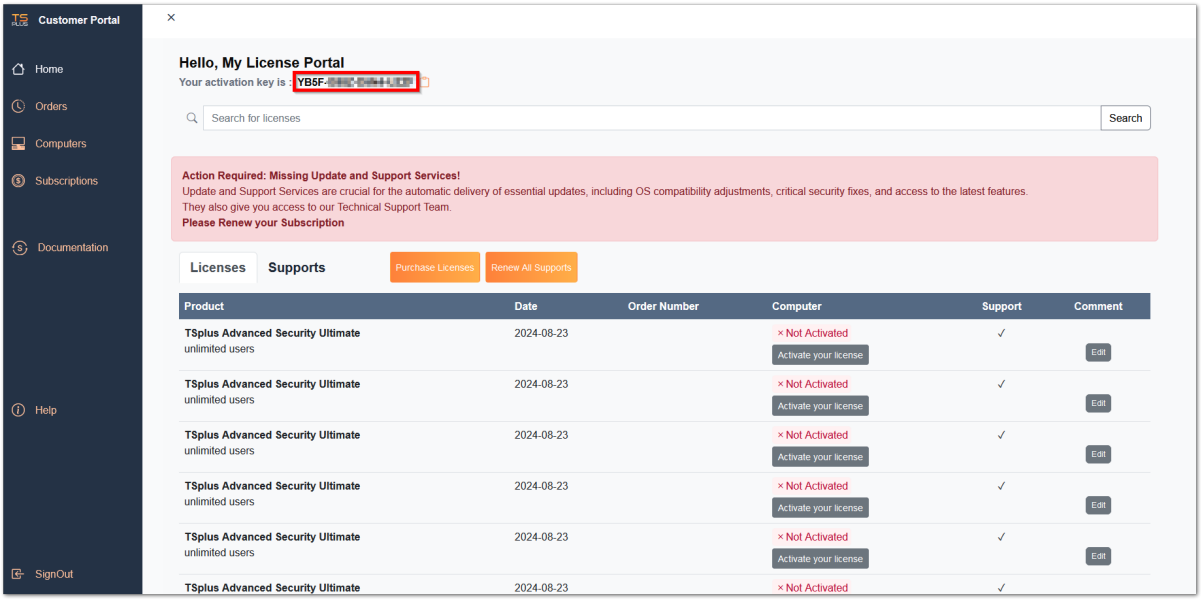
如果您不知道您的激活密钥，请继续进行第2步。否则，请继续进行第3步。

步骤 2：从许可门户获取您的激活密钥

为了获取您的激活密钥，请连接到我们的 许可门户 并输入您的电子邮件地址和订单号：

下载客户门户用户指南 有关您的客户门户的更多信息。

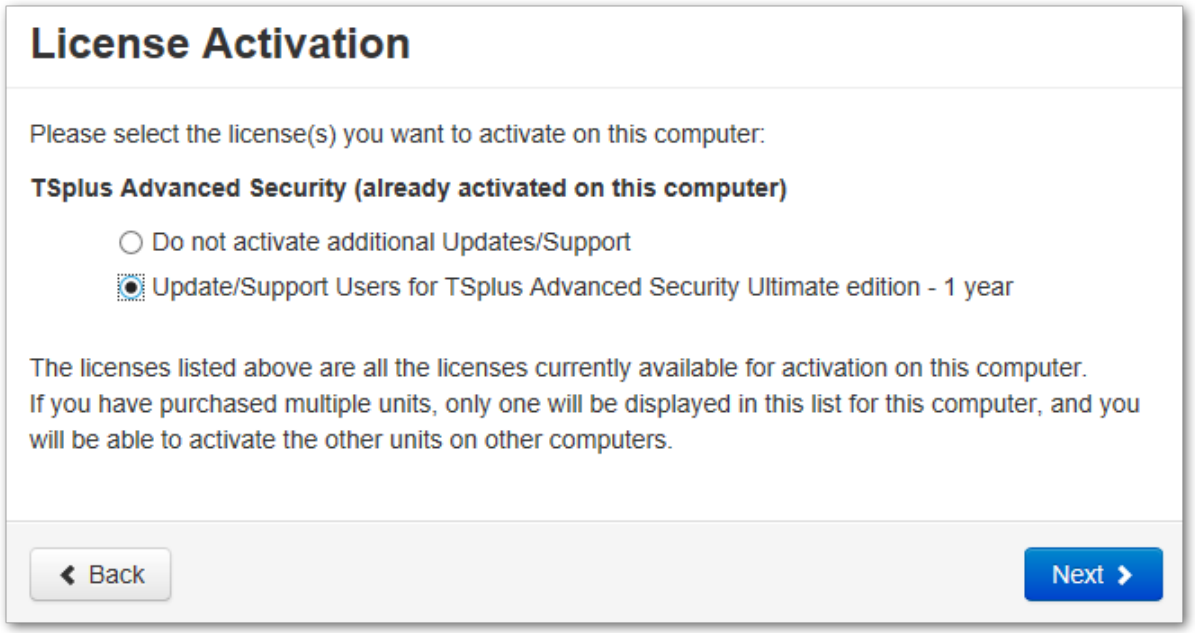
您的激活密钥将在仪表板顶部显示：



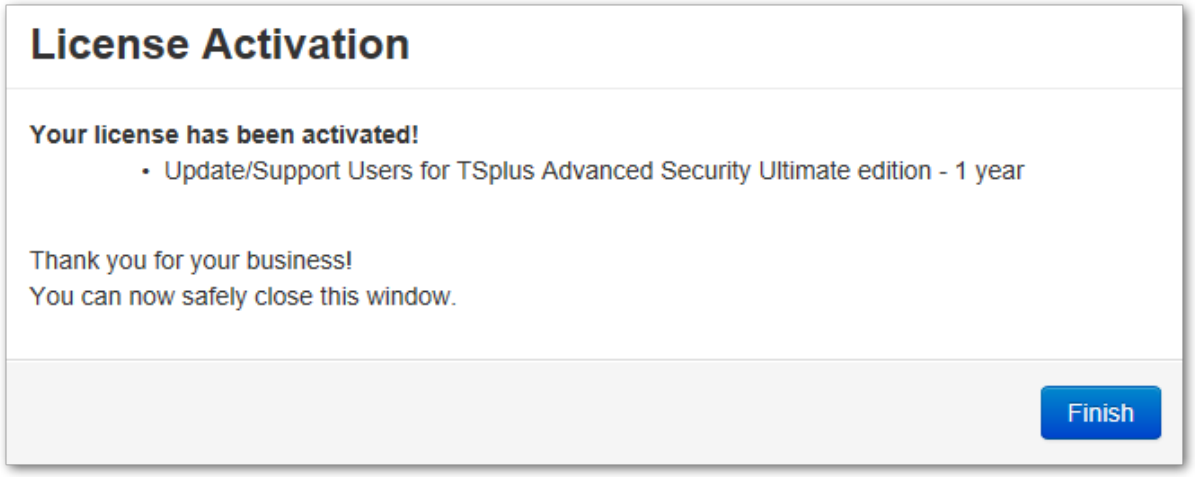
步骤 3：选择所请求的许可证以及已安装产品的更新和支

持服务

输入您的激活密钥，然后单击“下一步”。

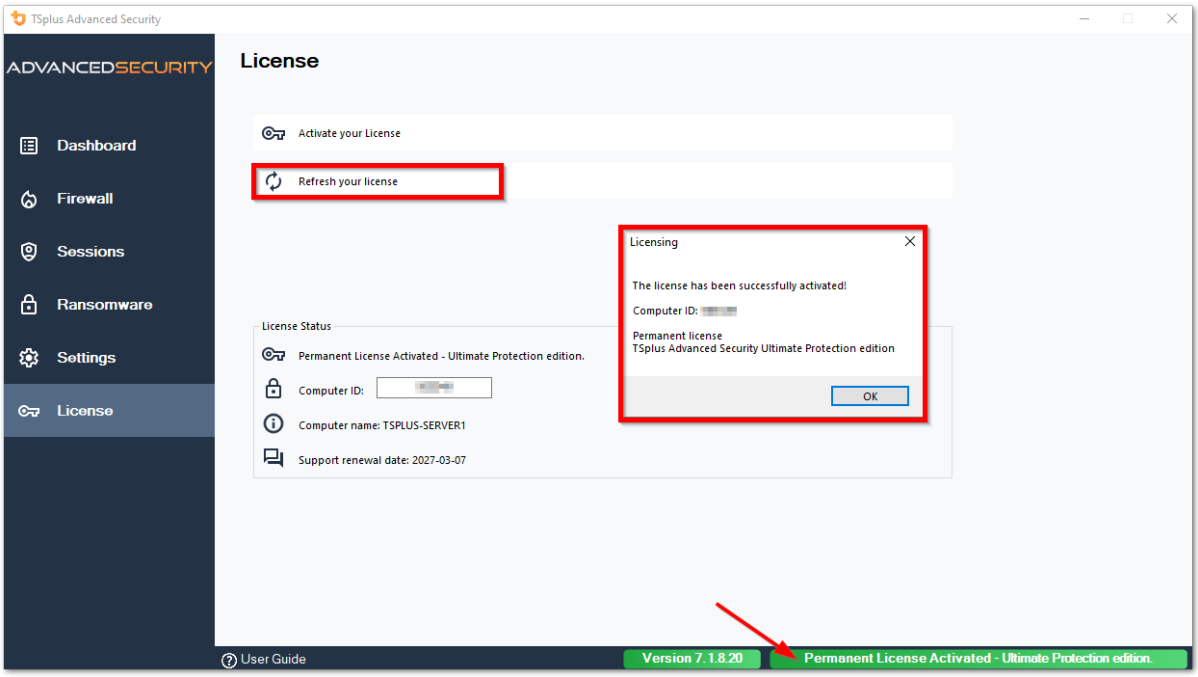


检查一个或多个项目并点击“下一步”按钮。请注意，您可以通过勾选多个产品和/或支持订阅同时激活多个产品。



您所选择的所有产品和支持订阅现在已激活（在此示例中，TSplus 及其支持和 TSplus Advanced Security 已同时激活）。

通过点击相应的按钮刷新您的许可状态。



激活您的许可证（离线）

请参阅为 TSplus Remote Access 描述的程序： 激活您的 TSplus 许可证（离线）

重新托管您的许可证

请参阅为 TSplus Remote Access 描述的程序： 重新托管您的 TSplus 许可证

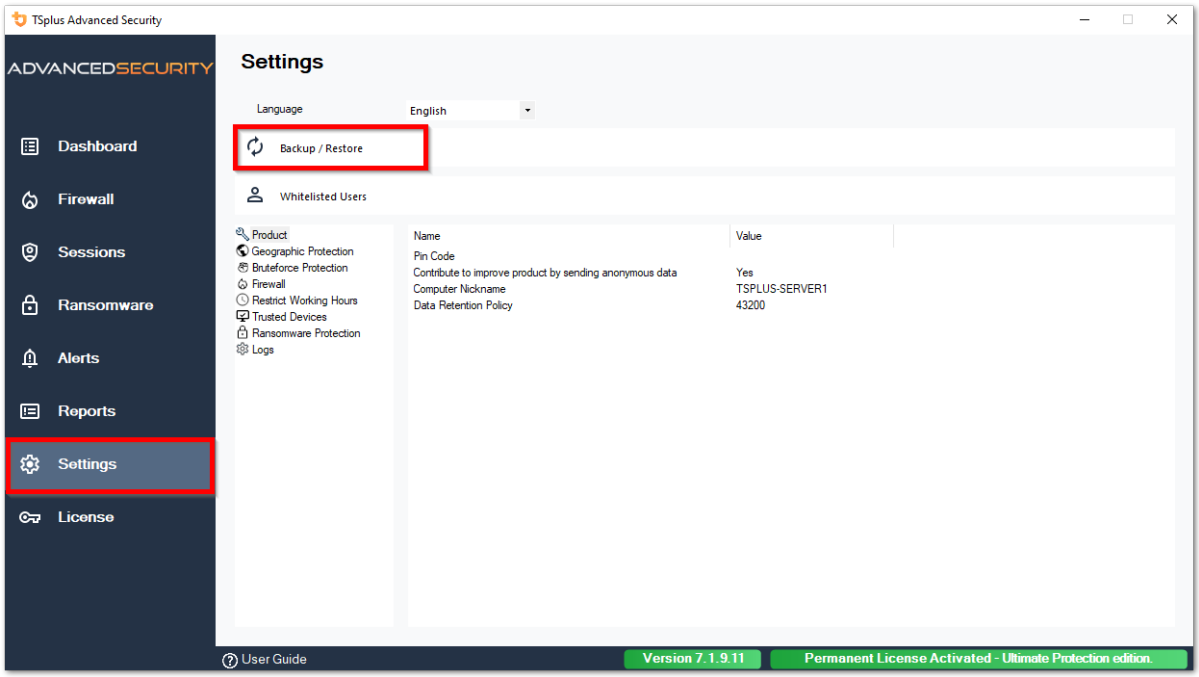
注意： 您可以在许可门户下载适用于以下版本的 TSplus 高级安全的 license.lic 文件。请参阅 客户门户用户指南 有关更多信息。

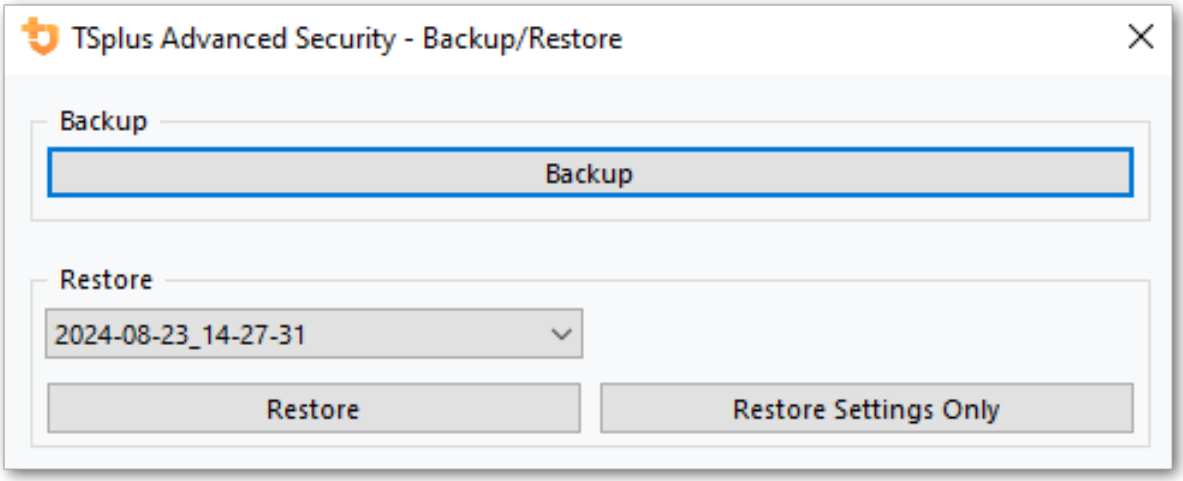
感谢您选择 TSplus Advanced Security!

高级 - 备份和恢复

备份和恢复数据和设置

您可以通过点击顶部的“备份 / 恢复”按钮来备份或恢复 TSplus Advanced Security 的数据和设置：





备份将保存在文件夹中 **档案** 位于 TSplus Advanced Security 的设置目录中。默认情况下， **档案** 文件位于此处：C:\Program Files (x86)\TSplus-Security\archives

使用命令行进行备份和恢复

命令用法如下所述：

- **备份** TSplus-Security.exe /backup [可选的目录路径]

默认情况下，备份将创建在位于 TSplus Advanced Security 设置文件夹中的档案目录中。然而，备份可以保存在指定的文件夹中。允许使用相对路径和绝对路径。

- **恢复** TSplus-Security.exe /restore [备份目录的路径]

指定的备份目录必须包含一个数据文件夹和一个设置文件夹，这些文件夹是通过 /backup 命令创建的。

配置备份

请注意，您可以在注册表中指定以下高级设置：

- 备份目录可以在注册表项中指定 HKEY_LOCAL_MACHINE\SOFTWARE\Digital River\RDS-Tools\knight\archivespath 默认情况下，将使用高级安全设置目录的“archives”目录。

- 可以在注册表项中指定可用的最大备份数量。 HKEY_LOCAL_MACHINE\SOFTWARE\Digital River\RDS-Tools\knight\maxarchives 默认情况下，Advanced Security 保留最后 3 个备份。

将您的数据和设置迁移到另一台计算机

请按照以下步骤将高级安全性从计算机 A 迁移到计算机 B：

1. 在计算机 A 上，请点击备份按钮以创建新的备份。设置和数据将保存在档案目录中，该目录位于高级安全设置目录中（通常为 C:\Program Files (x86)\TSplus-Security\archives）。

2. 将新创建的备份文件夹（例如，命名为 backup-2019-09-11_14-37-31），包括所有内容，从计算机 A 的档案目录复制到计算机 B 的档案目录。

3. 在计算机 B 的备份/恢复窗口中，在“恢复”部分，选择要恢复的相关备份名称。

4. 然后，单击仅恢复设置以恢复设置。或者，可以单击恢复以恢复所有数据和设置，这在迁移时不推荐，但在计算机 A 上恢复高级安全性时很有用。

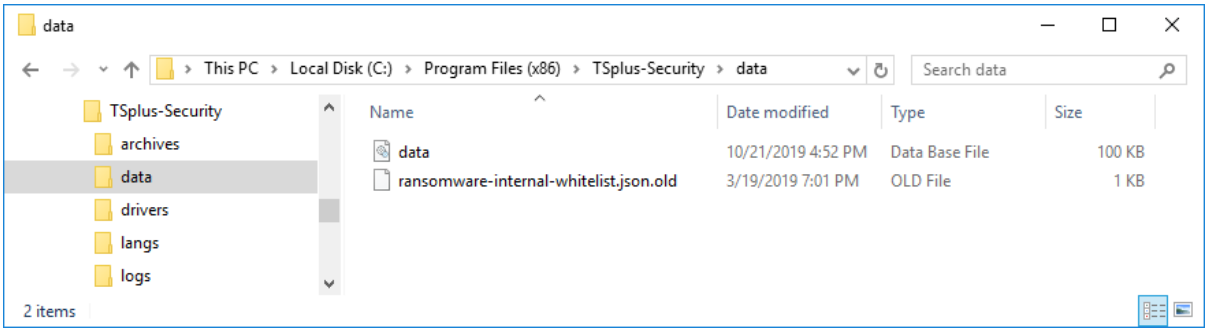
5. 请最多等待 2 分钟，以便通过高级安全功能重新加载设置。

数据库

一个数据库存储事件、IP地址、勒索软件攻击报告和程序白名单。

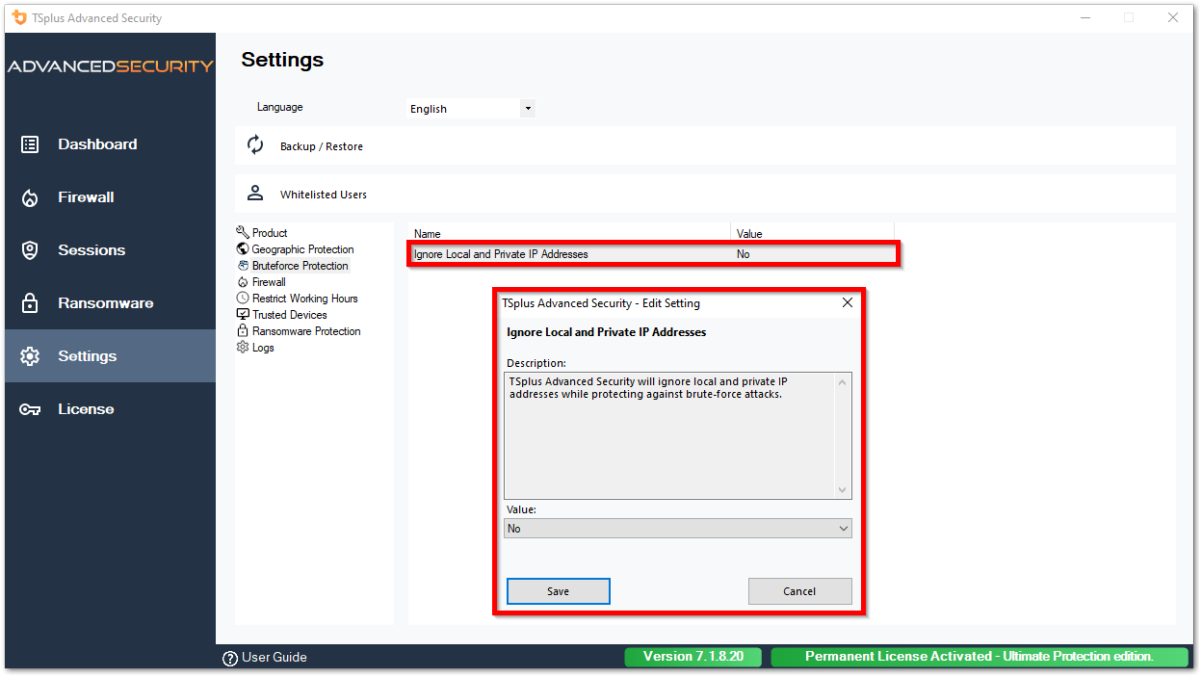
此数据库存储在 **数据** 位于TSplus Advanced Security的安装目录中的文件夹。

- 版本5及之前的Advanced Security使用的是一个 LiteDB数据库引擎 .
- 高级安全性版本 5.3.10.6 以上使用了一个 SQLite 数据库引擎 .



高级 - 暴力破解保护

这 **暴力破解保护** 选项卡允许您 忽略本地和私有IP地址 如果您愿意，可以将默认值从“否”更改为“是”。

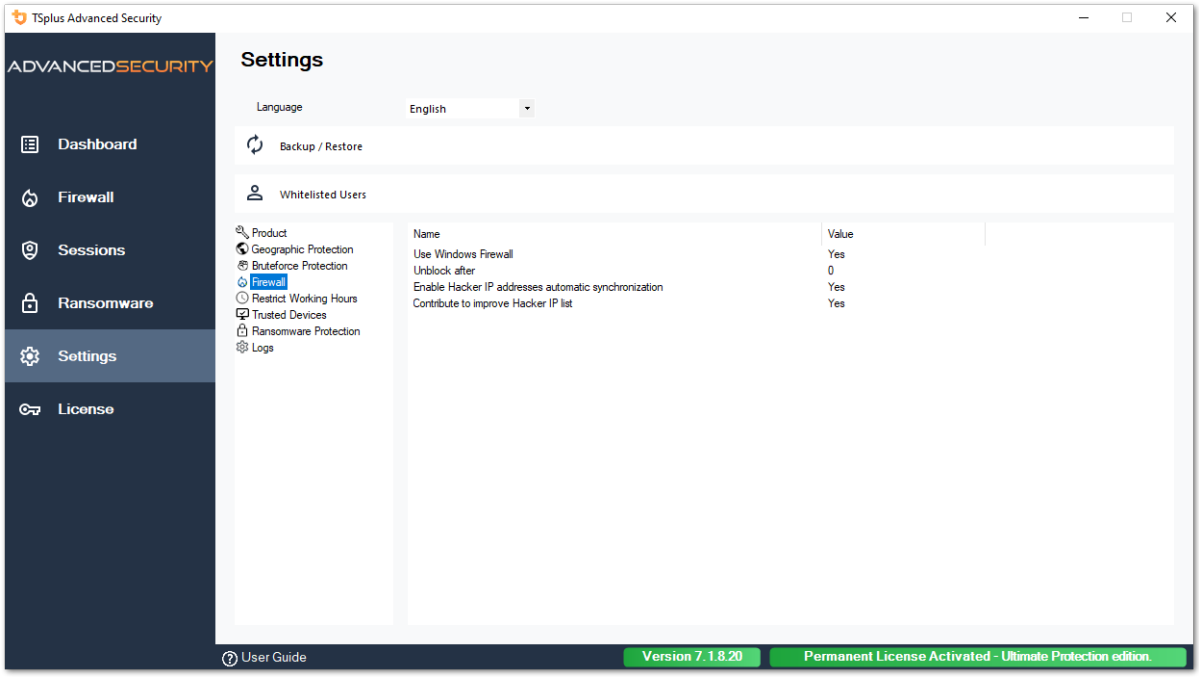


高级 - 防火墙

这 **防火墙** 选项卡允许您激活 **Windows 防火墙或停用它以支持 TSplus Advanced Security 内置防火墙** .

自4.4版本以来，TSplus Advanced Security中包含了内置防火墙。

作为一般指导，如果您的服务器上启用了Windows防火墙，则应使用它来强制执行TSplus Advanced Security规则（默认）。如果您安装了其他防火墙，则必须激活TSplus Advanced Security内置防火墙。



使用Windows防火墙 要激活内置防火墙，请转到设置 > 高级 > 产品 > 使用 Windows 防火墙，并将值设置为：否 如果选择是，则会使用 Windows 防火墙阻止有问题的 IP 地址。否则将使用 TSplus Advanced Security 防火墙。

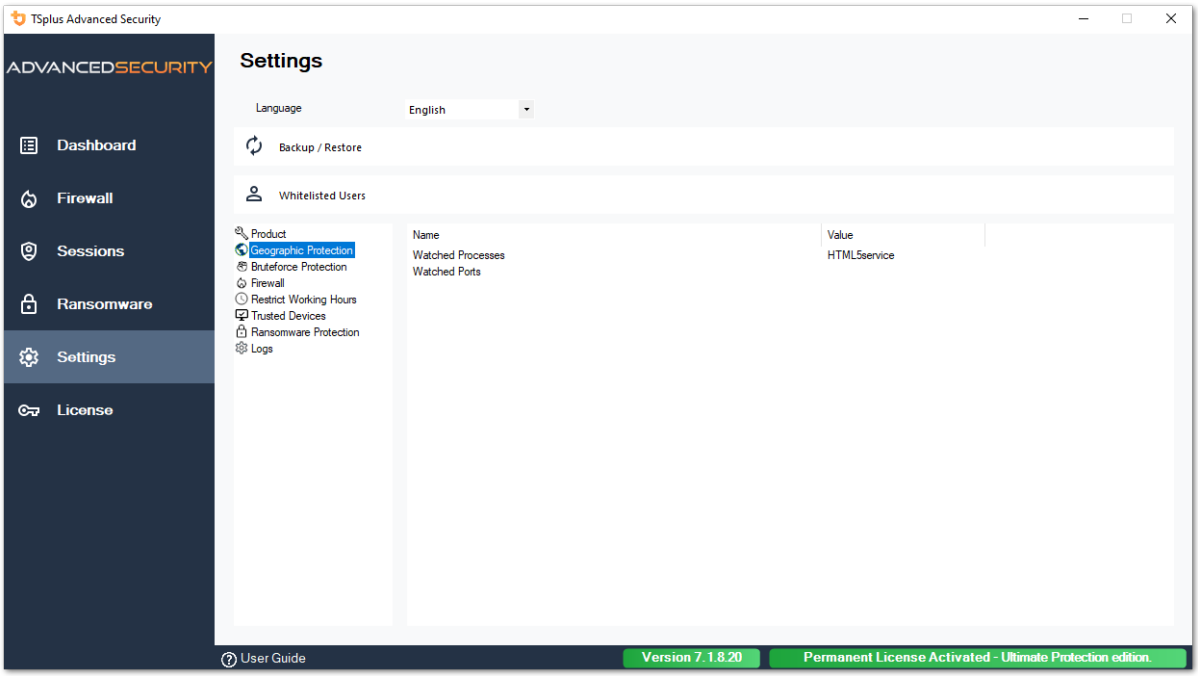
解锁后 更改此设置以在一定时间（以分钟为单位）后自动解锁 IP 地址。默认值为 0，禁用此功能。 值：0

启用黑客IP地址自动同步 保持您的机器免受已知威胁的保护，例如在线攻击、在线服务滥用、恶意软件、僵尸网络和其他电子活动，使用黑客IP保护。 需要订阅支持和更新服务。 价值：是

贡献以改善黑客IP列表 允许 TSplus Advanced Security 发送匿名使用统计数据，以增强对黑客 IP 的保护。
值：是

高级 - 地理保护

这 **地理保护** 选项卡允许您添加或删除被监视的进程。 地理保护 功能。



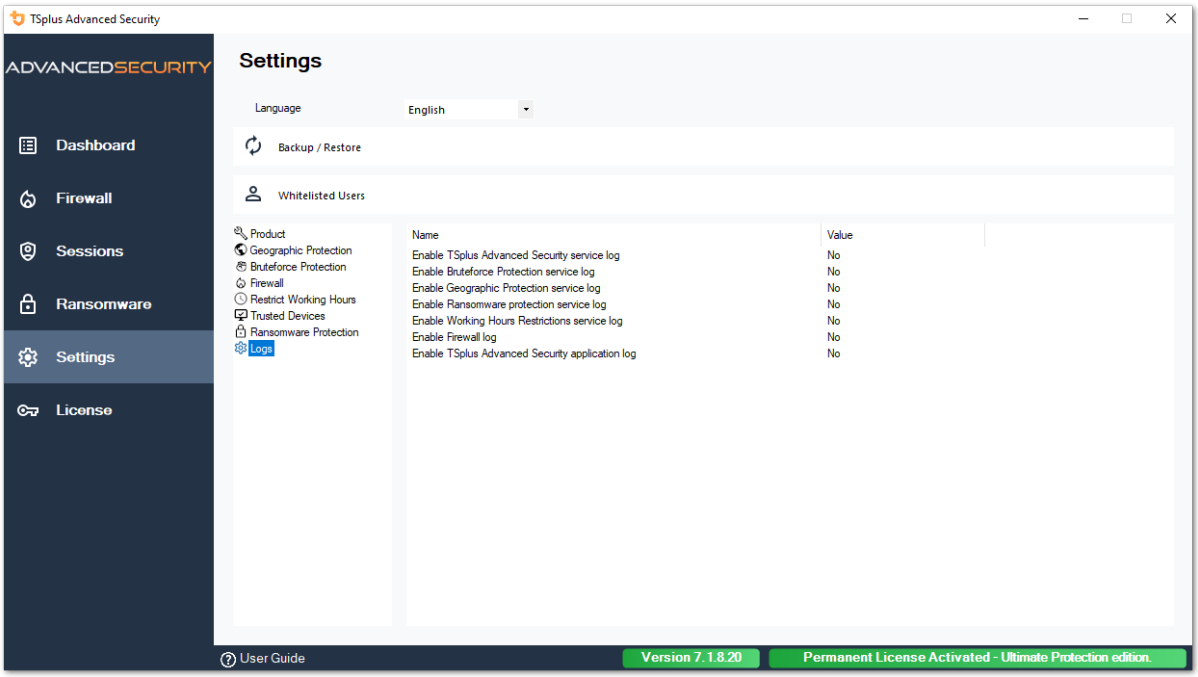
默认情况下，HTML5 服务是被监控的。

这 **监视端口** 设置允许您添加由监视的端口 地理保护 功能。默认情况下，地理保护监听用于远程连接到服务器的默认端口。这些端口包括 RDP（3389）、Telnet（23）和 VNC 端口。地理保护支持以下 VNC 提供商：Tight VNC、Ultra VNC、Tiger VNC 和 Real VNC，这些与 TSplus 完全无关。

高级 - 日志

这 **日志** 选项卡允许您 启用或禁用服务和功能日志 日志存在，以便更容易找到在 TSplus Advanced Security 上遇到的错误的来源。

要检索日志，请打开资源管理器并浏览到 **日志** TSplus Advanced Security的安装目录文件夹。默认情况下，日志将位于此处： **C:\Program Files (x86)\TSplus-Security\logs**



启用或禁用 TSplus Advanced Security 服务和应用程序日志 ，分别是后台运行的全局配置服务和应用程序接口的日志。

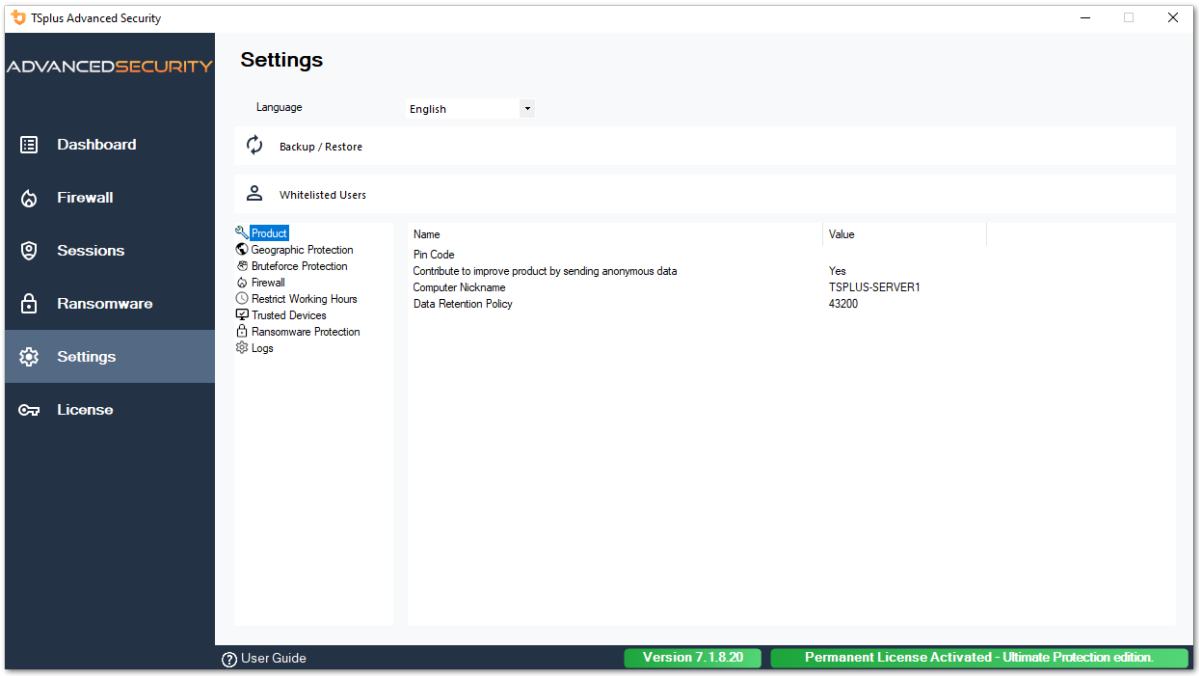
您还可以启用与相应的 TSplus 高级安全功能相对应的日志：

- 服务
- 暴力破解保护
- 地理保护
- 勒索软件保护
- 限制工作时间
- 防火墙..
- 应用程序

所有日志默认情况下都是禁用的。日志对应于不同的组件，我们的支持团队会告诉您根据遇到的问题应该输入什么值。

高级 - 产品

这 **产品** 选项卡允许您 为应用程序添加 PIN 码 ：



点击保存。下次启动应用程序时将需要输入 PIN 码。

您也可以 **贡献以改善产品** 通过发送匿名数据（默认启用）：是

在发生勒索软件攻击的情况下，将收集以下数据：

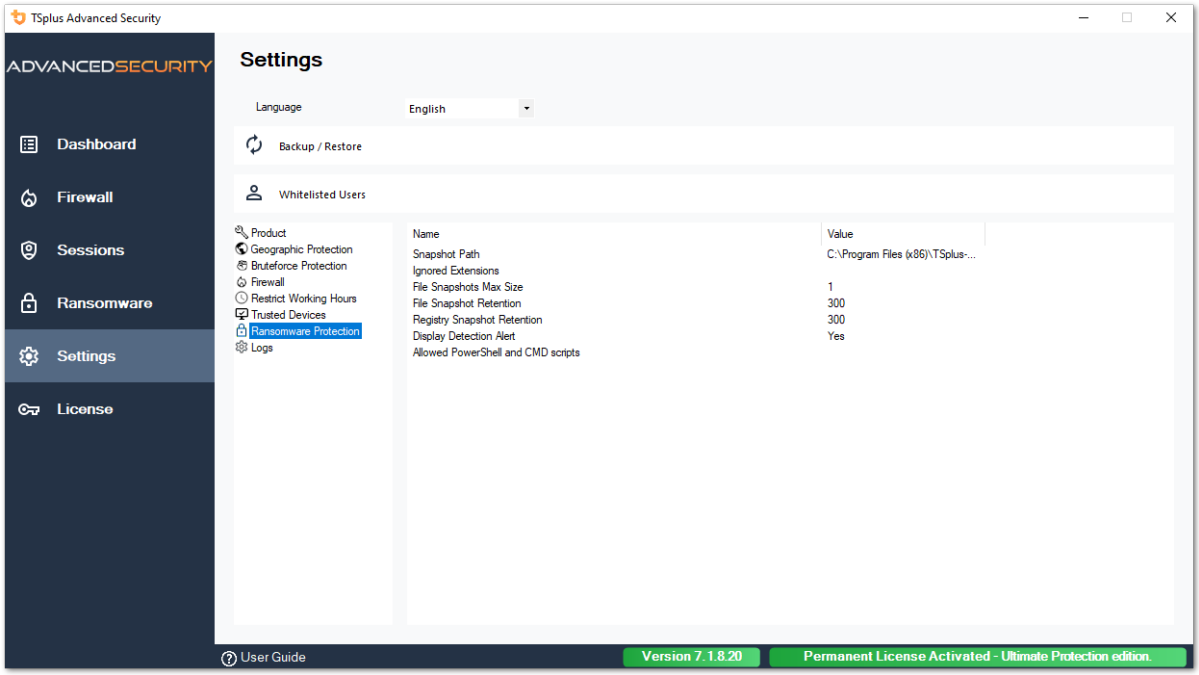
- TSplus Advanced Security的版本。
- Windows 版本。
- 可疑文件路径导致勒索软件攻击。

修改 **计算机昵称** 也可以。

这 **数据保留政策** 定义了从数据库中删除 TSplus Advanced Security 事件的时间段。在每次数据库清理之前都会进行备份。此策略以分钟为单位定义。默认数据保留政策为 259200 分钟，或 6 个月。

高级 - 勒索软件保护

这 **勒索软件保护** 选项卡允许您 配置快照属性并定义被忽略的文件扩展名 针对勒索软件保护功能。



快照路径 定义勒索软件保护存储文件快照的目录。

默认值为：C:\Program Files (x86)\TSplus-Security\snapshots

忽略的扩展名 默认情况下，Ransomware Protection 会忽略与勒索软件活动相关的临时文件的常见扩展名。 在此查看列表 您可以在值字段中定义自定义扩展名（以分号分隔）：

文件快照最大大小 文件快照最大大小定义了保留文件快照所允许的最大空间。

大小以快照路径所在磁盘上可用总空间的百分比表示。

文件快照保留 文件快照保留定义了文件快照的保留策略，以秒为单位。

一旦保留期结束，文件快照将被删除。默认情况下，300秒（即5分钟）

注册表快照保留 注册表快照保留定义为以秒为单位的注册表快照保留策略。保留期结束后，注册表快照将被删除。默认情况下为300秒（即5分钟）。

显示检测警报 在用户的桌面上显示警报消息窗口，当勒索软件保护检测到并阻止攻击时。

允许的 PowerShell 和 CMD 脚本 允许的 PowerShell 和 CMD 脚本列出了可以在机器上执行的 PowerShell 和 CMD 脚本的完整文件路径

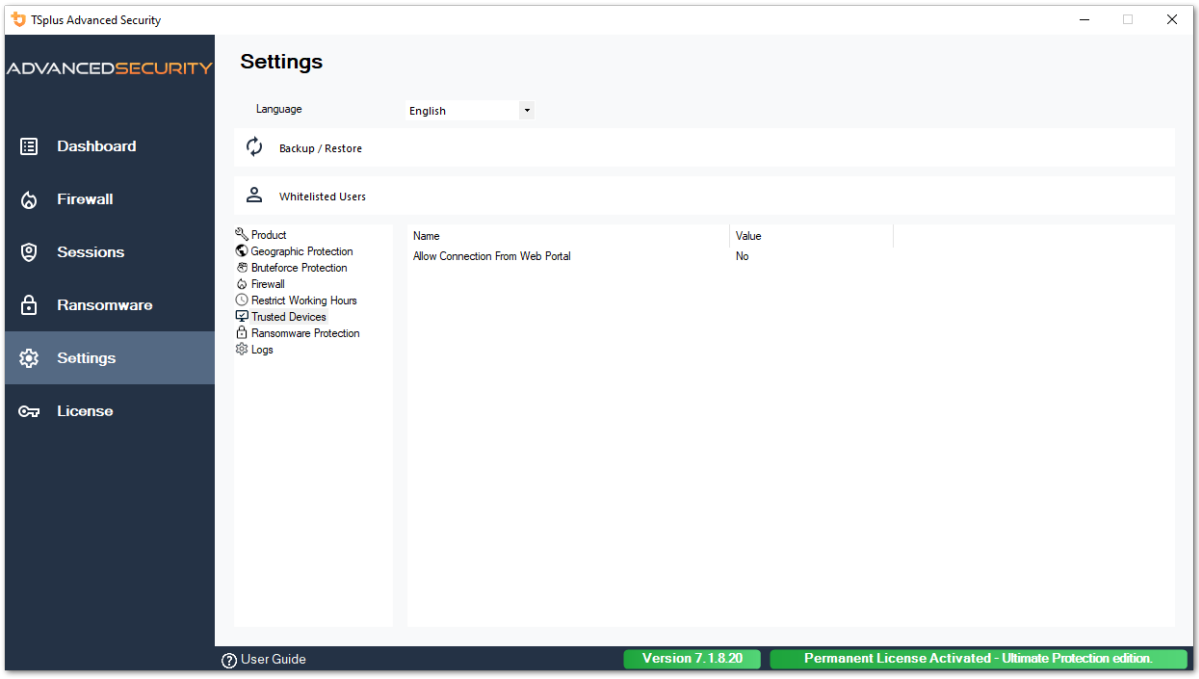
允许的脚本的执行不会触发勒索软件保护（用分号分隔）。

高级 - 受信任的设备

这 **受信任的设备** 选项卡允许您从TSplus Remote Access的Web门户启用连接。

注意 ：

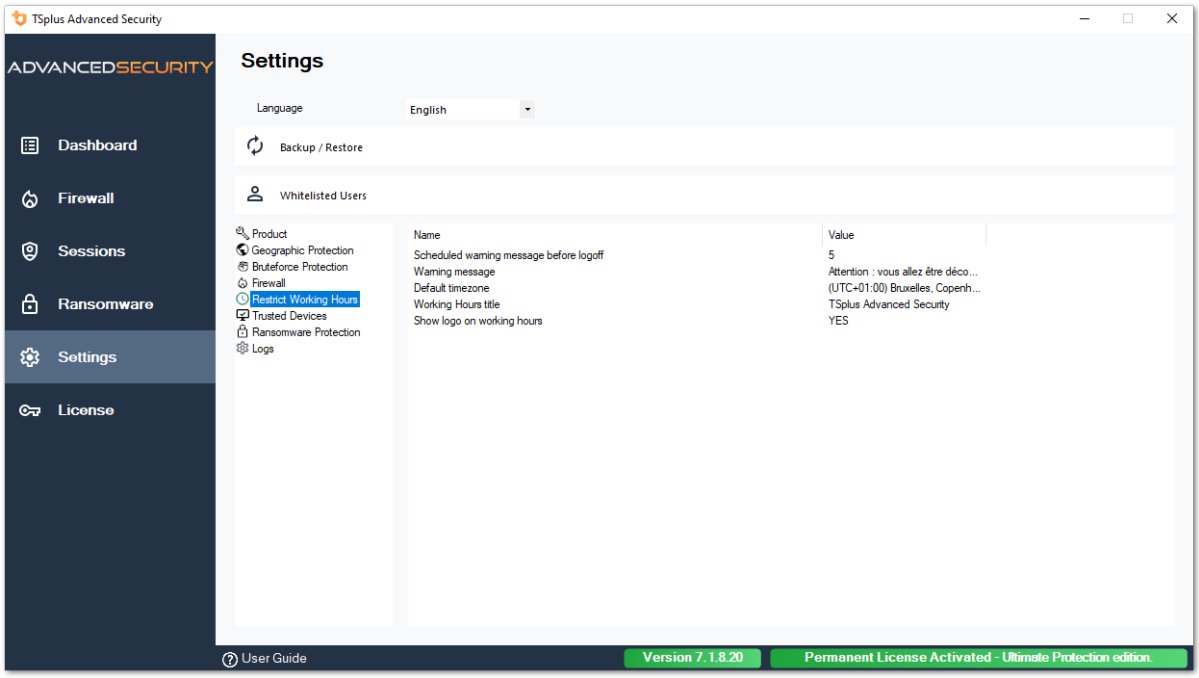
-受信任的设备与HTML5会话不兼容。 -受信任的设备与iOS / Android移动设备不兼容，因为它们隐藏了真实的主机名。 -远程机器的主机名由机器本身定义。该机器可能会根据其配置隐藏或修改主机名。



TSplus Advanced Security的受信任设备无法解析从TSplus Remote Access的Web门户发起的客户端名称。因此，受信任设备默认会阻止来自Web门户的任何连接。将此设置为“是”以允许来自Web门户的连接。请注意，此操作将降低您服务器的安全性。

高级 - 限制工作时间

这 **限制工作时间** 选项卡允许您 在用户注销之前安排警告消息 .



警告消息计划 您可以配置用户在自动断开连接之前的分钟数。默认情况下，它设置为 5 分钟。

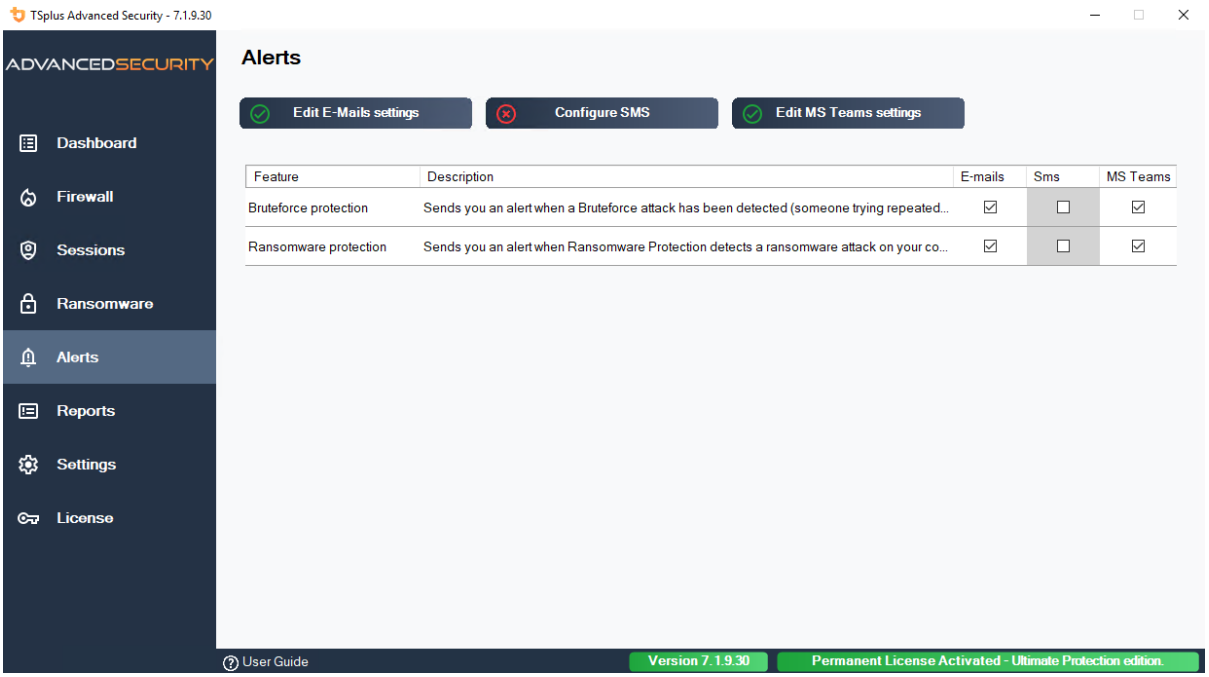
警告信息 您可以根据需要定义警告消息，使用名为 %MINUTESBEFORELOGOFF%、%DAY%、%STARTINGHOURS% 和 %ENDINGHOURS% 的占位符，这些占位符将分别替换为会话关闭前的当前分钟数、当前日期以及当前日期的开始和结束工作时间。

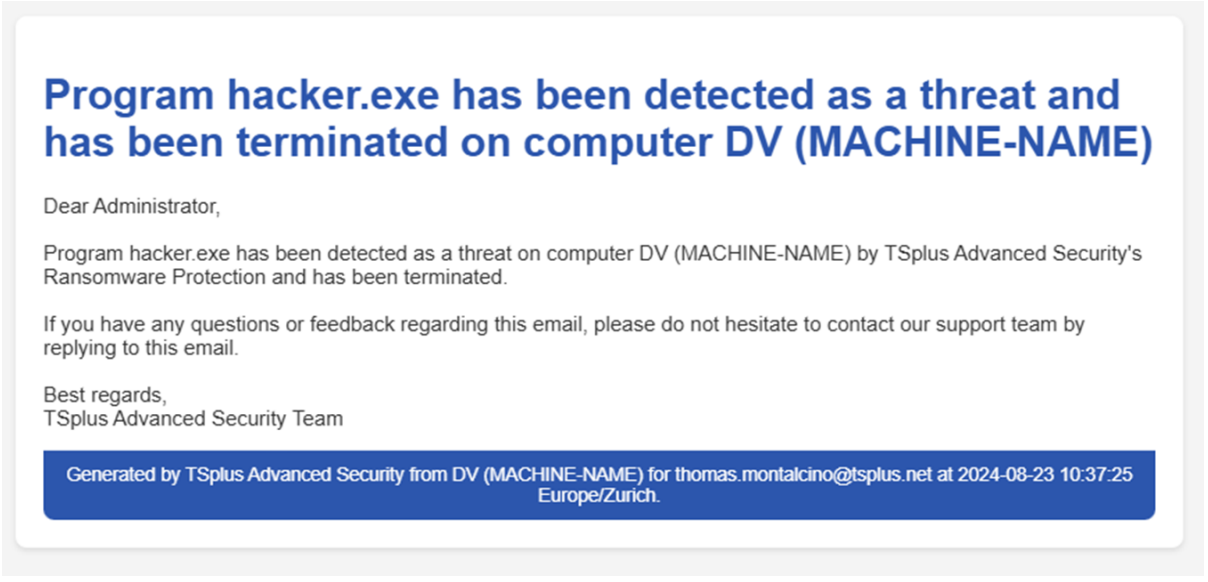
默认服务器时区 可以通过在下拉列表中选择相应的选项来定义默认服务器时区，以便相应地应用工作时间规则。

工作时间标题 当用户的工作时间结束时显示给最终用户的表单标题（默认：TSplus Advanced Security）

在工作时间显示徽标 如果设置为“是”，则在用户的工作时间结束时以显示给最终用户的形式显示徽标（默认：“是”）

警报





Program hacker.exe has been detected as a threat and has been terminated on computer DV (MACHINE-NAME)

Dear Administrator,

Program hacker.exe has been detected as a threat on computer DV (MACHINE-NAME) by TSplus Advanced Security's Ransomware Protection and has been terminated.

If you have any questions or feedback regarding this email, please do not hesitate to contact our support team by replying to this email.

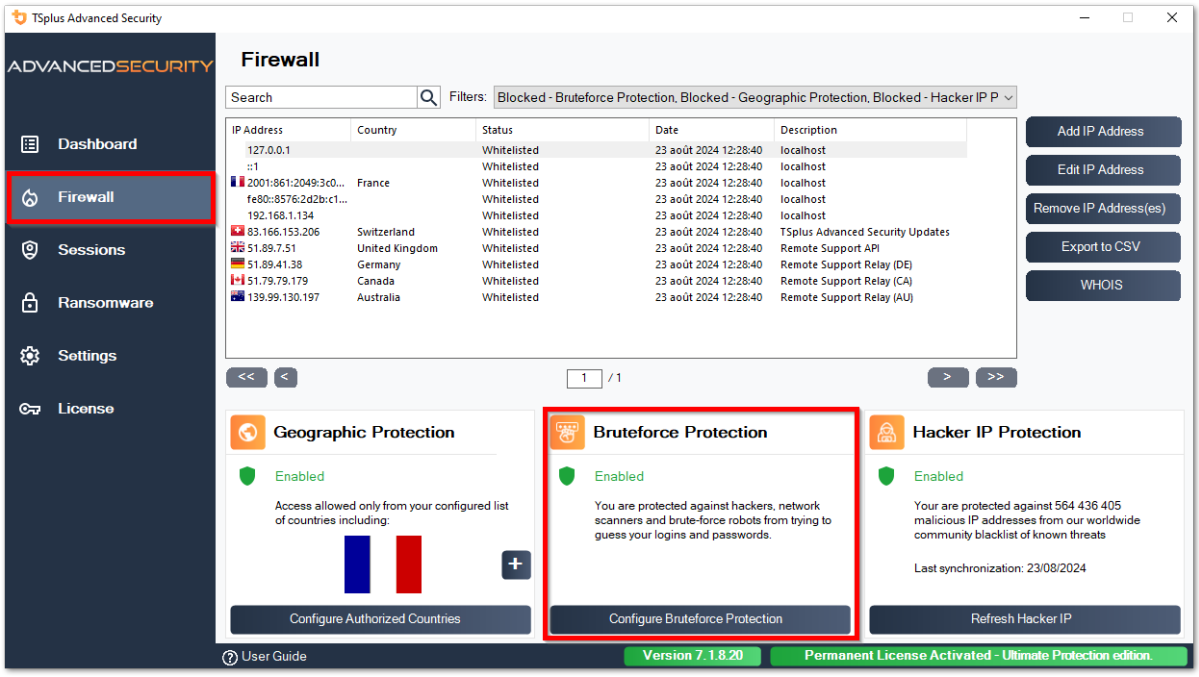
Best regards,
TSplus Advanced Security Team

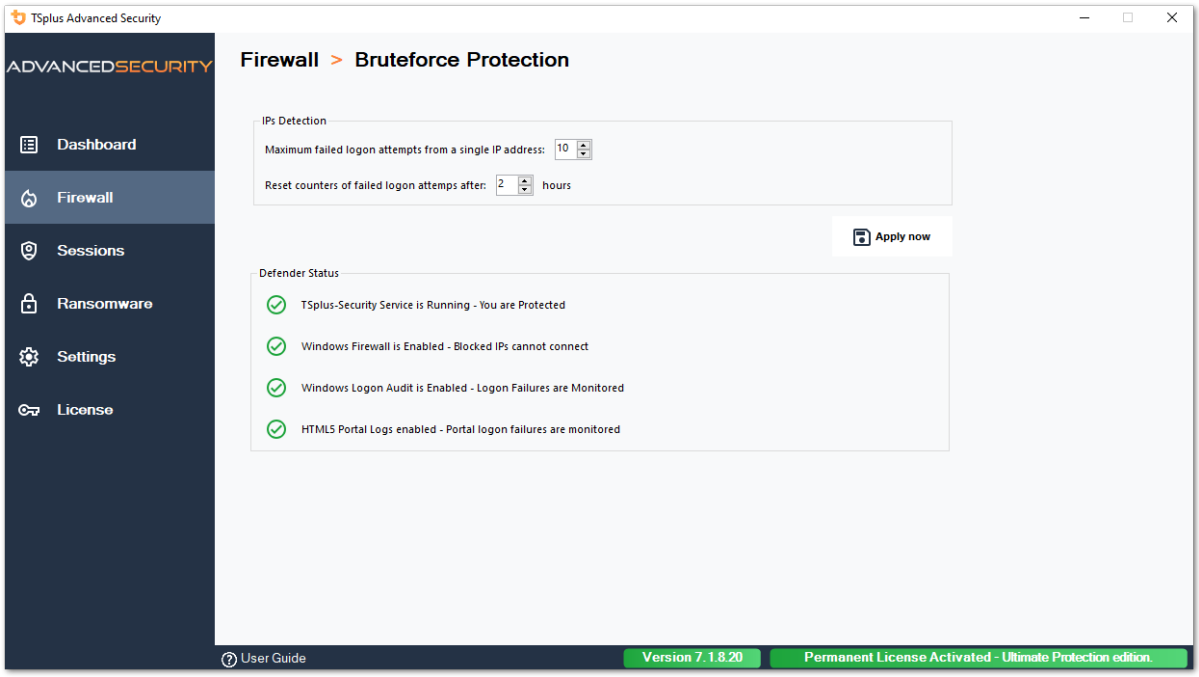
Generated by TSplus Advanced Security from DV (MACHINE-NAME) for thomas.montalcino@tsplus.net at 2024-08-23 10:37:25 Europe/Zurich.

暴力破解保护

暴力破解保护使您能够保护您的公共服务器免受黑客、网络扫描器和试图猜测您的管理员登录和密码的暴力破解机器人攻击。使用当前的登录和密码字典，它们将每分钟自动尝试登录到您的服务器数百到数千次。

通过这个RDP Defender，您可以监控Windows的登录失败尝试，并在多次失败后自动将相关的IP地址列入黑名单。





- 您可以设置该 **来自单个IP地址的最大失败登录尝试次数在IPs检测块内** （默认情况下，它是10），以及失败登录尝试计数器的重置时间（默认情况下是2小时）。

- 在此窗口的底部，您可以看到 **防御者状态** 您可以在此处检查HTML5 Web Portal登录失败，Windows登录失败是否被监控，以及Windows防火墙和高级安全服务是否已启用。

在这种情况下，就像我们的例子一样，所有状态都被勾选。

- **管理被阻止的IP地址** 您当然可以将其配置为满足您的需求，例如通过添加您自己的工作站 IP 地址。 IP 白名单 因此，这个工具永远不会阻止您。您可以在白名单中添加任意数量的IP地址。这些地址将永远不会被暴力攻击保护阻止。

- 您可以 **忽略本地和私有IP地址** 通过更改默认设置上的 设置 > 高级 > 暴力破解选项卡

注意： 如果您注意到Bruteforce Protection每天阻止10个IP地址，而现在不再是这种情况；并且阻止一个、两个，甚至根本不阻止任何地址，这实际上是正常的。确实，在安装advanced-security之前，公开可用的RDP端口的服务器被所有机器人所知，许多机器人尝试当前的密码和来自字典的密码。当您安装advanced-security时，这些机器人会逐渐被阻止，因此有一天：

- 大多数活跃的机器人已经被阻止，并且对服务器不感兴趣，即使是新的机器人。
- 此外，服务器不再出现在公开已知服务器的列表中。

命令行

我们很高兴为您提供一套全面的命令行工具，旨在增强我们软件的灵活性和效率。这些工具使用户能够编写脚本并自动化各种功能，从而根据他们的特定需求和工作流程定制软件。

探索可能性并通过我们的命令行选项优化您的体验。

您只需以提升的管理员身份运行以下命令行。 作为提醒，TSplus-Security.exe 位于以下文件夹中。 **C:\Program Files (x86)\TSplus-Security** 默认情况下。

许可证管理

要对许可证执行操作，请将以下文档中提供的程序 AdminTool.exe 替换为位于 Advanced Security 安装目录中的 TSplus-Security.exe 程序（通常 **C:\Program Files (x86)\TSplus-Security** ）.

- 许可证激活
- 虚拟机克隆后的许可证重置
- 批量许可证激活
- 启用和禁用批量许可证
- 批量许可证更新
- 显示剩余的许可证积分用于批量许可证密钥
- 显示卷许可证密钥的剩余支持积分

配置代理服务器： /proxy /set

语法：

TSplus-Security.exe /proxy /set [参数]

描述：

命令 /proxy /set 用于配置代理服务器以访问互联网。

参数：

- /host 目标主机可以是预定义值（“ie”或“none”）或用户定义值（例如：127.0.0.1或proxy.company.org）。此参数是必需的。
- /port 用于连接到代理服务器的端口号。如果主机名值是自定义用户定义的值，则为必需。
- /username 连接到代理服务器的用户名。此设置是可选的。
- /password 用户的密码必须在定义了用户名的情况下提供。然而，它的值可以为空。

示例：

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

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

有关更多信息，请访问 如何配置代理服务器以进行互联网访问？

备份数据和设置： /backup

语法：

TSplus-Security.exe /backup [目标目录路径]

描述：

命令 /backup 用于备份 TSplus Advanced Security 数据和设置。

默认情况下，备份将创建在位于高级安全设置目录中的档案目录中（例如：C:\Program Files (x86)\TSplus-Security\archives）。

参数：

- DestinationDirectoryPath 在默认目录之外备份到另一个目录。允许使用相对路径和绝对路径。

示例：

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

有关更多信息，请访问 高级 - 备份和恢复

恢复数据和设置： /restore

语法：

TSplus-Security.exe /restore [备份目录路径]

描述：

命令 /restore 用于恢复 TSplus Advanced Security 数据和设置。

指定的备份目录路径必须通过 /backup 命令或通过应用程序中的备份功能创建。

参数：

- Backup Directory Path 备份目录的恢复路径。

示例：

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

有关更多信息，请访问 高级 - 备份和恢复

删除并解锁所有被阻止的IP地址： /unblockall

语法：

TSplus-Security.exe /unblockall

描述：

命令 /unblockall 用于从TSplus Advanced Security的防火墙中移除所有被阻止的IP地址，并在需要时从Microsoft Windows Defender防火墙中解锁它们。

示例：

TSplus-Security.exe /unblockall

有关更多信息，请访问 防火墙

删除和解除指定IP地址的阻止： /unblockips

语法：

TSplus-Security.exe /unblockips [IP 地址]

描述：

命令 /unblockips 用于从TSplus Advanced Security的防火墙中删除所有指定的被阻止的IP地址，并在需要时从Microsoft Windows Defender防火墙中解除阻止。

此命令对已被黑客IP保护阻止的IP地址没有影响。如果您仍然想要解锁其中一个地址，请使用白名单命令。

参数：

- IP addresses 解除封锁的IP地址或IP范围列表（用逗号或分号分隔）。

示例：

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

有关更多信息，请访问 防火墙

阻止指定的IP地址： /blockips

语法：

TSplus-Security.exe /blockips [IP 地址] [可选描述]

描述：

命令 /blockips 用于通过 TSplus Advanced Security 的防火墙阻止所有指定的 IP 地址，并在配置的情况下使用 Microsoft Windows Defender 防火墙阻止它们。

参数：

- IP addresses 要阻止的IP地址或IP范围的列表（用逗号或分号分隔）。
- Optional Description 可选描述，将为每个条目添加。

示例：

TSplus-Security.exe /blockips 1.1.1.1;2.2.2.2;3.3.3.1-3.3.6.12;5.5.5.5 “约翰的工作场所”

有关更多信息，请访问 防火墙

将IP地址添加到白名单： /addwhitelistedip

语法：

TSplus-Security.exe /addwhitelistedip [IP addresses] [可选描述]

描述：

命令 /addwhitelistedip 用于将指定的IP地址添加到TSplus Advanced Security防火墙的授权IP地址中，并在需要时从Microsoft Windows Defender防火墙中解除阻止。

参数：

- IP addresses 要列入白名单的IP地址或IP范围（用逗号或分号分隔）。
- Optional Description 可选描述，将为每个条目添加。

示例：

TSplus-Security.exe /addwhitelistedip 1.1.1.1;2.2.2.2;3.3.3.1-3.3.6.12;5.5.5.5 “约翰的工作场所”

有关更多信息，请访问 防火墙

添加程序或目录到勒索软件保护授权列表： /whitelist

语法：

TSplus-Security.exe /whitelist add [授权路径]

描述：

命令 /whitelist add 用于将指定的程序路径和目录路径添加到TSplus高级安全的勒索软件保护的授权列表中。

参数：

- Authorized Paths 程序路径和目录路径的列表，添加到 TSplus Advanced Security 的 Ransomware Protection 授权列表中（用分号分隔）。

示例：

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

有关更多信息，请访问 勒索软件保护行动

刷新黑客IP保护： /refreshipprotection

语法：

TSplus-Security.exe /refreshipprotection

描述：

命令 /refreshipprotection 用于刷新黑客IP保护功能的被阻止IP范围列表。需要订阅支持和更新服务。

示例：

TSplus-Security.exe /refreshipprotection

有关更多信息，请访问 黑客IP保护

设置日志级别： /setloglevel

语法：

TSplus-Security.exe /setloglevel [日志级别]

描述：

命令 /setloglevel 用于设置所有高级安全组件的日志级别。

参数：

- Log Level 日志级别可选以下值：ALL、DEBUG、INFO、WARN、ERROR、FATAL、OFF

示例：

TSplus-Security.exe /setloglevel ALL

有关更多信息，请访问 高级 > 日志

添加受信任的设备： /addtrusteddevices

语法：

TSplus-Security.exe /addtrusteddevices [受信任设备配置]

描述：

命令 /addtrusteddevices 用于以编程方式添加受信任的设备。需要终极版。

参数：

- Trusted Devices Configuration 该参数由一个受信任设备的列表组成（用分号分隔），结构如下：

用户名和设备由冒号字符（,）分隔。

用户名详情：

用户类型和完整用户名由冒号字符 (:) 分隔。接受的用户类型为“用户”和“组”。

可选关键字“禁用”：如果包含，将创建受信任的设备，但此用户的限制将被禁用。如果未提及，默认情况下启用限制。

设备详情：

设备名称和可选注释：用等号字符（=）分隔。

设备由冒号字符 (:) 分隔。

示例：

TSplus-Security.exe /addtrusteddevices “user:WIN-A1BCDE23FGH\admin:disabled,device1name=这是设备1的评论:device2name:device3name;user:DESKTOP-A1BCDE23FGH\johndoe,device1name=设备4名称=另一个评论;group:DESKTOP-A1BCDE23FGH\Administrators:disabled,device5name”

有关更多信息，请访问 受信任的设备

启用配置的受信任设备： /enabletrusteddevices

语法：

TSplus-Security.exe /enabletrusteddevices [用户或组]

描述：

命令 /enabletrusteddevices 用于启用指定用户和组的所有配置的受信任设备。

参数：

- User or Groups 该参数是一个用户和组的列表（用分号分隔）。在用户名中，用户类型（“user”和“group”是唯一接受的值）与完整用户名之间的分隔由冒号完成。

示例：

TSplus-Security.exe /enabletrusteddevices “user:WIN-A1BCDE23FGH\admin;user:DESKTOP-A1BCDE23FGH\johndoe;group:DESKTOP-A1BCDE23FGH\Administrators”

有关更多信息，请访问 受信任的设备

禁用所有受信任的设备： /disabletrusteddevices

语法：

TSplus-Security.exe /disabletrusteddevices [用户或组]

描述：

命令 /disabletrusteddevices 用于禁用指定用户和组的所有配置的受信任设备。

参数：

- User or Groups 该参数是一个用户和组的列表（用分号分隔）。在用户名中，用户类型（“user”和“group”是唯一接受的值）与完整用户名之间的分隔由冒号完成。

示例：

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

有关更多信息，请访问 受信任的设备

设置勒索软件保护驱动程序： /setup-driver

语法：

TSplus-Security.exe /setup-driver

描述：

命令 /setup-driver 安装勒索软件保护驱动程序。此操作通常在安装过程中执行。

示例：

TSplus-Security.exe /setup-driver

有关更多信息，请访问 勒索软件保护

卸载勒索软件保护驱动程序： /uninstalldriver

语法：

TSplus-Security.exe /uninstalldriver

描述：

命令 /uninstalldriver 卸载Ransomware Protection驱动程序。此操作通常在Advanced Security卸载期间执行。

示例：

TSplus-Security.exe /uninstalldriver

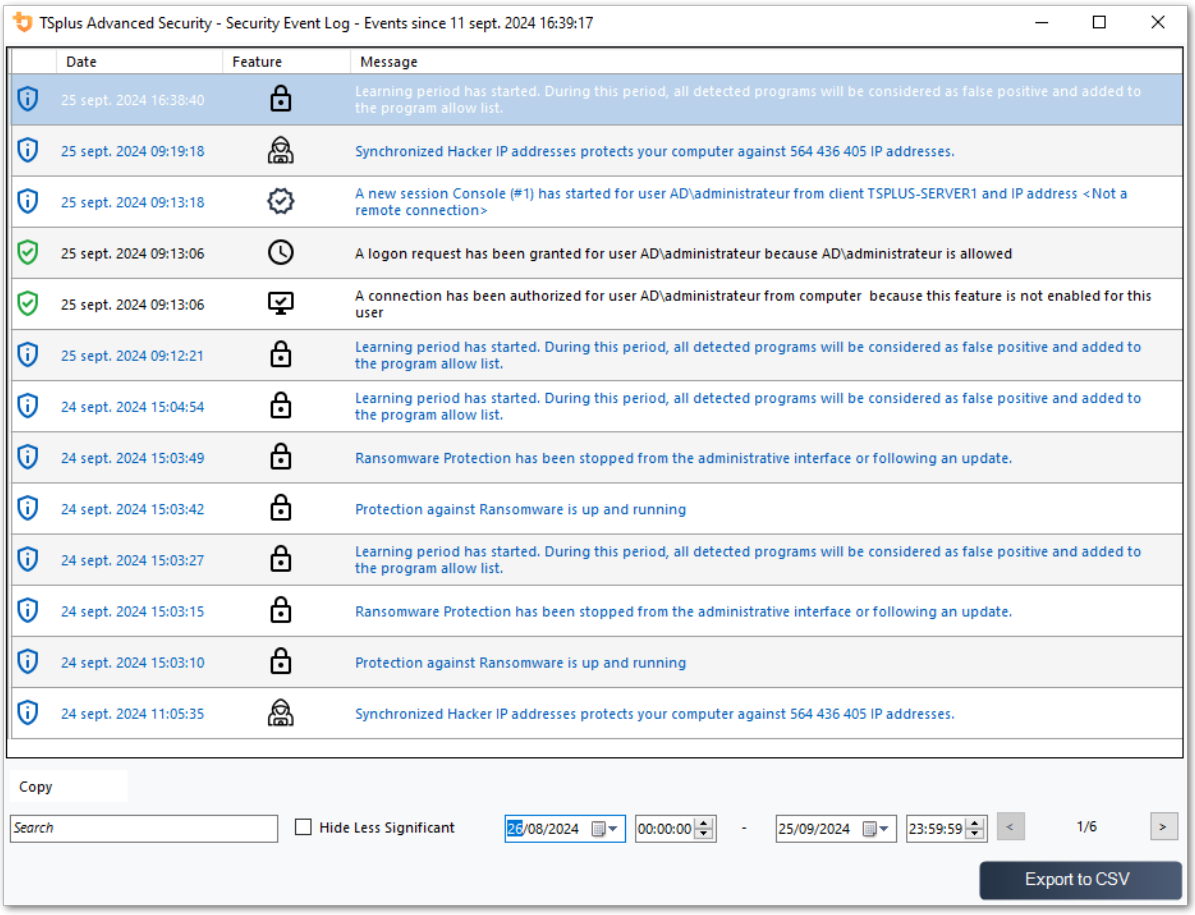
有关更多信息，请访问 勒索软件保护

事件

安全事件是一个重要的信息来源，因为它们显示了TSplus Advanced Security为保护您的计算机所执行的操作。

事件窗口可以从TSplus Advanced Security主窗口打开，方法是直接点击显示的最后5个事件或仪表板选项卡。事件窗口上显示的信息会每隔几秒自动刷新。

安全事件列表包含4列，描述了严重性、检查或执行操作的日期、相关功能图标和描述。



事件的描述通常解释了为什么执行或未执行该操作。报复性行动通常用红色书写，并用红色盾牌图标突出显示。

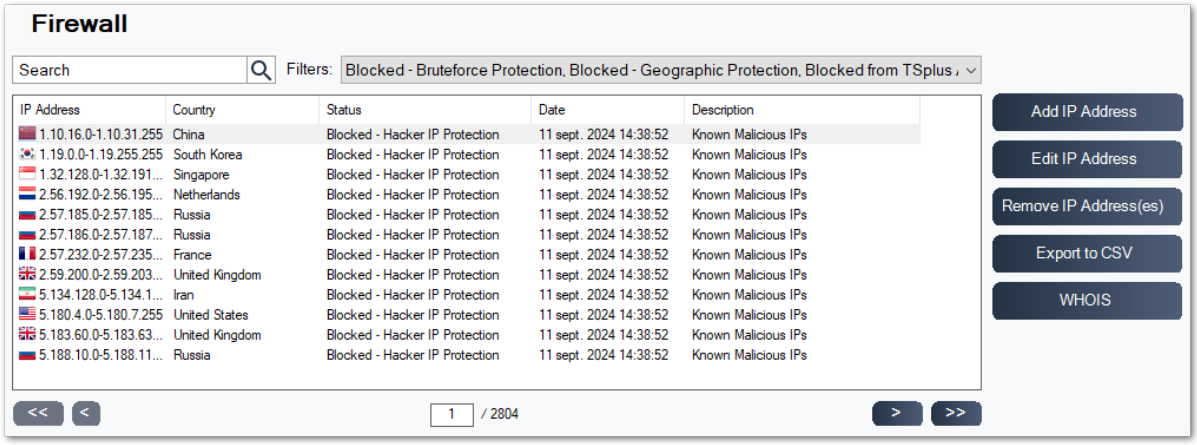
事件窗口可以移动，并且不会妨碍您使用其他 TSplus Advanced Security 功能。

浏览和搜索事件

- 现在可以进行深度全球搜索，以便快速找到特定事件。
- 在全局搜索旁边，两个日期和时间选择器根据事件发生的日期过滤显示的事件。
- 在右侧，箭头允许更改页面并导航以查看较早的事件。

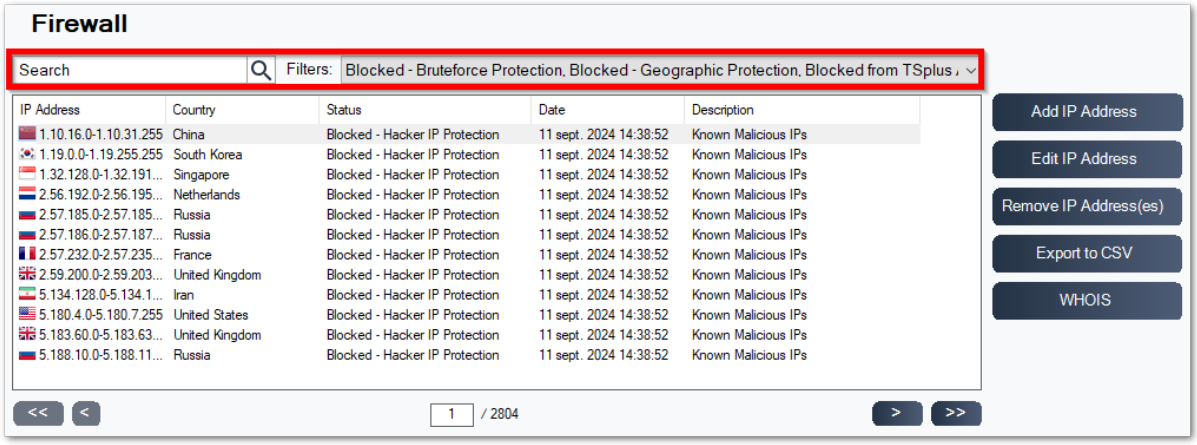
防火墙

IP地址管理很简单，只需一个列表即可管理被阻止和白名单的IP地址：

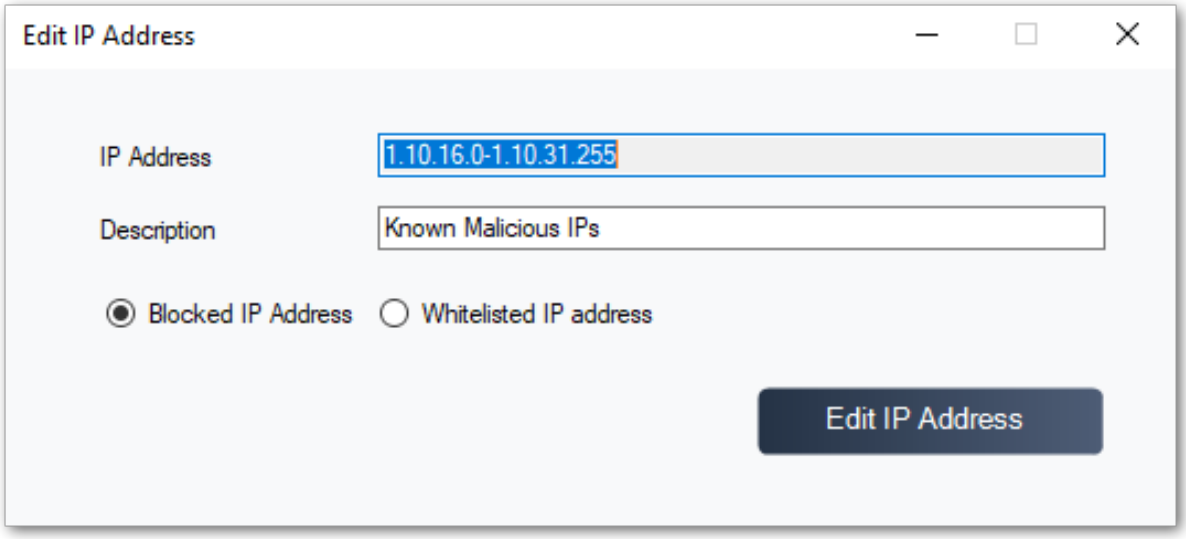


默认情况下，IPV4、IPV6 和所有服务器本地主机地址都在白名单中。

一个方便的搜索栏和过滤器提供基于所有提供的信息的搜索功能。



此外，管理员能够通过单击一次对多个选定的IP地址执行操作。在新引入的IP地址管理功能中，您将发现可以为任何IP地址提供有意义的描述的可能性。



最后但并非最不重要的是，管理员现在可以通过点击“添加现有到白名单”选项卡，在一次操作中解锁并添加多个被阻止的IP地址到白名单。

使用命令行来列入白名单或阻止IP地址和/或IP范围

- 为了 **whitelist** IP 地址或 IP 范围，命令的语法如下：

TSplus-Security.exe 添加白名单IP [ip addresses] [optional description]

您可以将多个IP地址列入白名单，使用一个 **逗号或分号分隔符** 此外，您可以指定IP地址范围，而不是简单的IP地址。语法是： **x.x.x.x-y.y.y.y** 最后，您可以指示白名单规则的可选描述。

这是一个完整命令的示例： 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的工作场所”

- 为了 **区块** IP 地址或 IP 范围，命令具有类似的语法：

TSplus-Security.exe 阻止 IP [ip addresses] [可选描述]

- 为了 **解锁** IP 地址或 IP 范围，命令具有类似的语法：

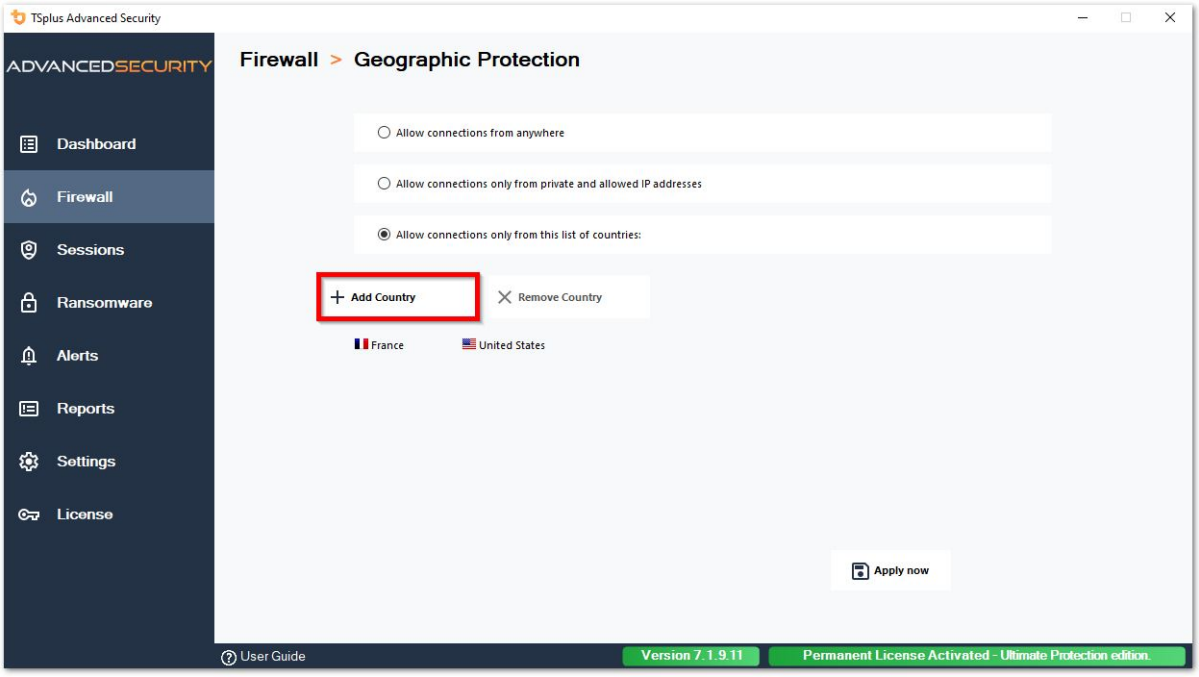
TSplus-Security.exe 解锁 IP 地址 [ip addresses]

此命令对已被黑客IP保护阻止的IP地址没有影响。如果您仍然想要解锁其中一个地址，请使用白名单命令。

地理保护

限制来自其他国家的访问

要仅允许来自特定国家的远程访问，请选择“仅允许来自此国家列表的连接”按钮，然后点击“添加国家”按钮。

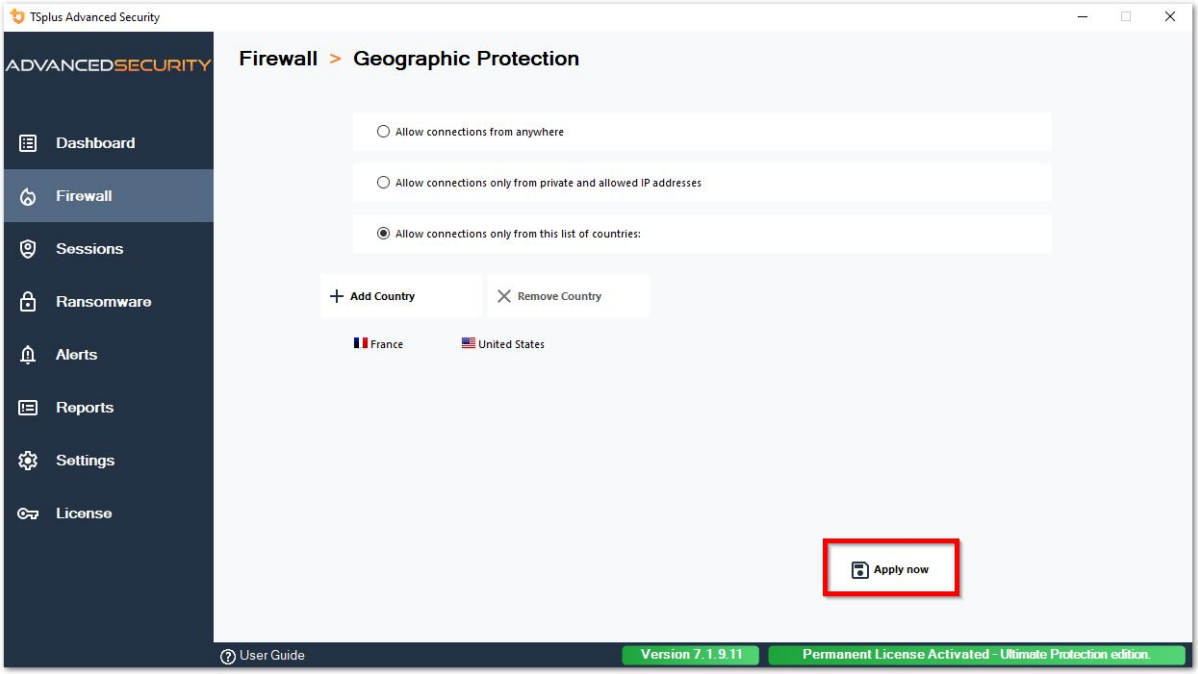


弹出窗口提供国家列表。选择您希望添加到列表中的国家。

您可以选择勾选下面的框，以解除对所选国家/地区所有先前被阻止的IP地址的阻止。

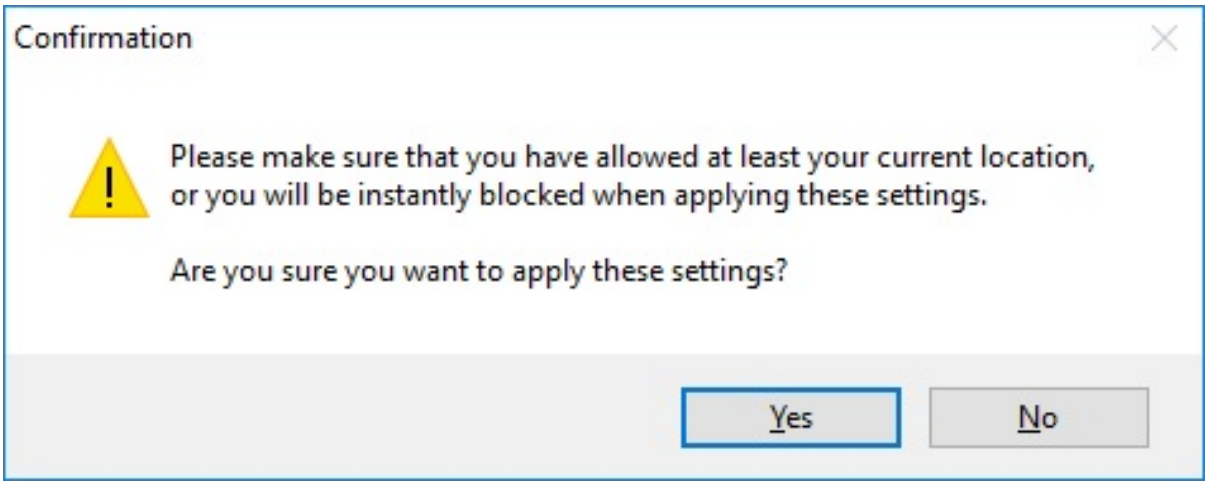
点击“添加国家”按钮以返回功能主屏幕。

重要提示：为了保存您的更改，请点击“应用”按钮。



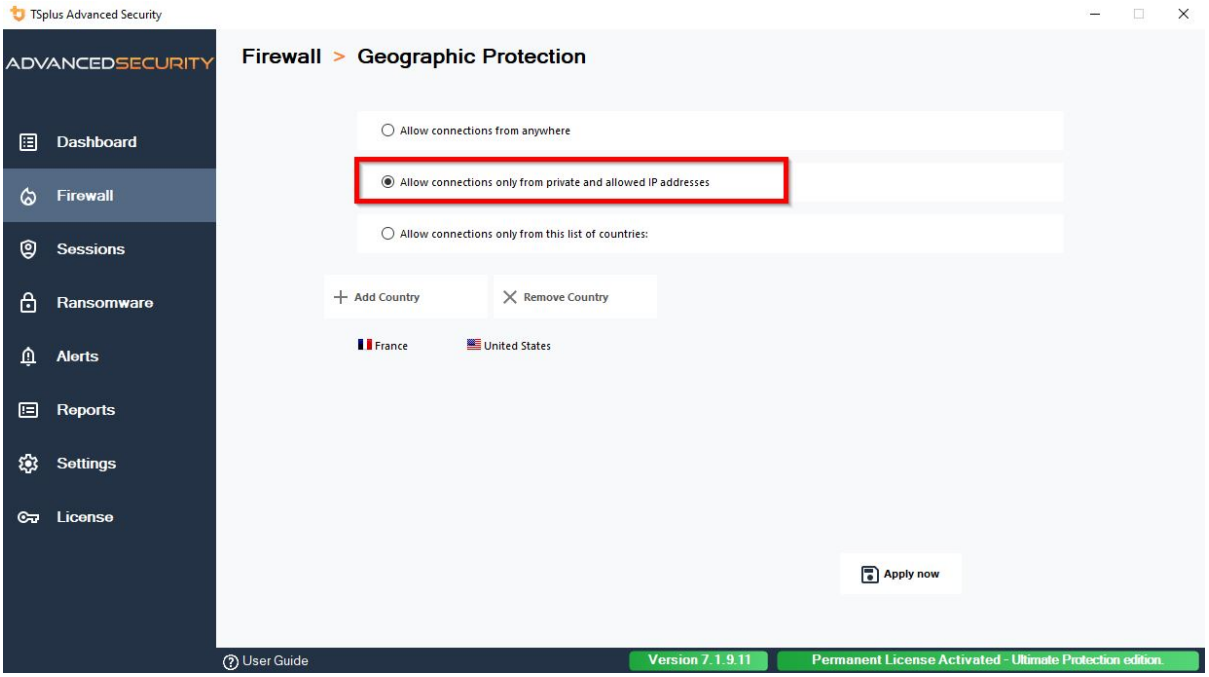
在这个例子中，允许来自美国和法国的用户进行远程访问。

出现确认消息以避免阻止已连接的用户。点击“是”以确认并应用更改。



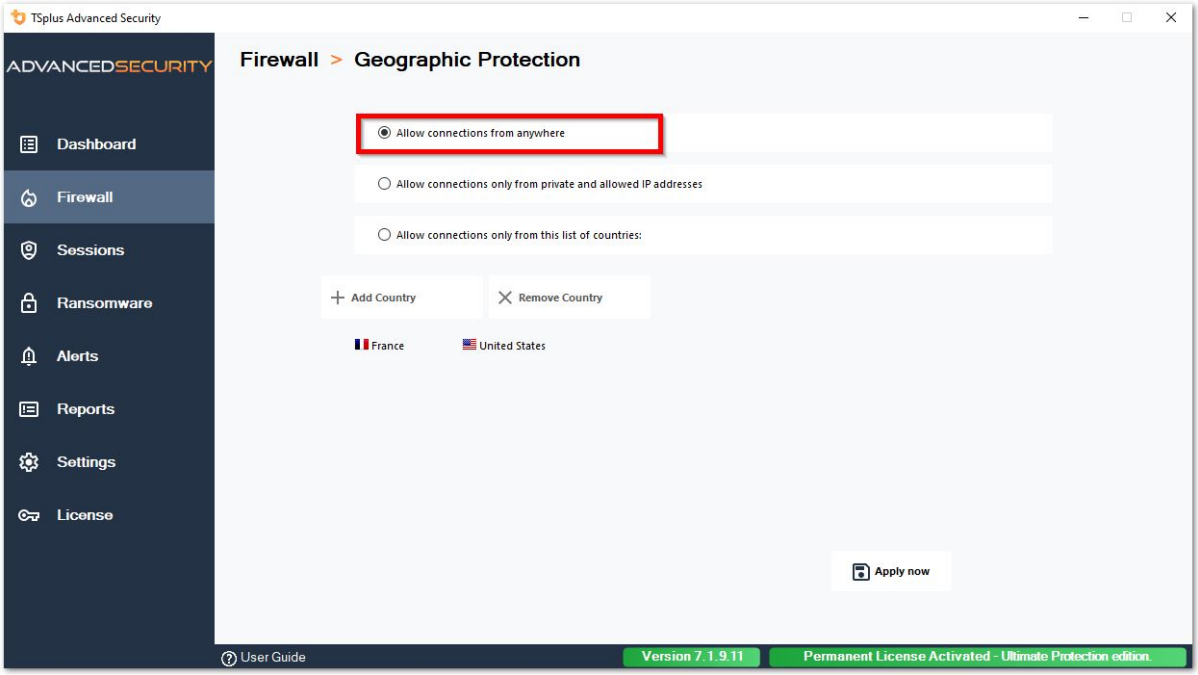
限制来自互联网的访问

地理保护可以配置为限制对您机器的访问，仅限于私人和 白名单IP地址 请提供需要翻译的文本。



禁用地理保护

默认情况下，地理保护允许来自世界各地的用户访问：



解锁被阻止的IP地址

当一个IP地址被阻止时，它会出现在 防火墙选项卡 被阻止的IP地址可以被解锁，并最终添加到允许的IP地址列表中。

如果您被阻止，我们建议您尝试从您在 TSplus Advanced Security 中允许的任何国家进行连接，例如通过从另一个远程服务器连接或使用 VPN 服务。您还可以使用控制台会话进行连接，因为此会话不是远程会话，不会被 TSplus Advanced Security 阻止。

重要：

- 检查您是否选择了您当前连接的国家。如果没有，您的IP地址将在应用设置后迅速被阻止，从而使您断开连接，无法再从同一IP地址重新连接。

- 考虑将您自己的IP地址添加到允许的列表中 IP 地址 避免被地理保护或阻止 暴力破解保护 功能。

理解地理保护

地理保护检查传入的TCP网络连接，包括IPv4和IPV6（除非配置了传统Windows API模式）。

流程： 地理保护默认情况下会监听发送到TSplus Remote Access的Web服务器的连接（如果已安装）。相应进程的名称是HTML5服务。如果您希望禁用其监控或检查发送到其他进程的连接，请前往 设置 > 高级 > 地理保护 .

网络端口： 默认情况下，地理保护监听用于远程连接到服务器的默认端口。这些端口包括RDP（3389）、Telnet（23）和VNC。地理保护支持以下VNC提供商：Tight VNC、Ultra VNC、Tiger VNC和Real VNC，这些与TSplus完全无关。如果您希望禁用其监控或检查指向其他端口的连接，请前往 设置 > 高级 > 地理保护 .

检测机制：

地理保护使用三种不同的检测机制来检测来自未授权国家的入站连接：

- Windows API
- Windows事件追踪
- 内置防火墙

一方面，Windows事件追踪是一个高效的内核级追踪工具，可以实时捕获网络事件。建议在启用Windows防火墙（默认设置）的情况下使用Windows事件追踪。

另一方面，Windows API在任何特定网络配置下都表现良好，但可能会根据活动连接的数量对CPU施加持续压力。请注意，Windows API目前尚不支持IPv6。

内置防火墙允许用户模式捕获和丢弃发送到Windows网络堆栈的网络数据包。当内置防火墙配置为阻止不必要的连接时，建议使用它来执行地理保护的允许国家。

地理位置： 高级安全包括由MaxMind发布的地理位置数据，来自 http://www.maxmind.com 如果您发现一个未在其实际国家注册的IP地址，请直接联系MaxMind以解决此问题。

故障排除

如果您发现地理保护未能阻止来自实际上不在授权国家列表中的国家的连接，这肯定是因为：

杀毒软件： 为了阻止一个IP地址，地理保护在Windows防火墙上添加一个阻止规则。因此，首先，防火墙必须处于活动状态。您还需要检查一些防火墙参数是否被其他程序处理，例如杀毒软件。在这种情况下，您需要停用该程序并重新启动“Windows防火墙”服务。您还可以联系您的第三方程序编辑器，请他们找到一种方法，使他们的程序在添加到Windows防火墙时遵守规则。如果您知道任何软件编辑器的技术联系人，我们准备为防火墙开发这些“连接器”。 联系我们 .

VPN： 如果远程客户端使用VPN，地理保护将获得由VPN提供商选择的IP地址。正如您所知，VPN提供商在全球范围内使用中继，以允许其用户匿名浏览。一些VPN提供商允许用户定义中继的国家。因此，使用VPN提供商的用户可能会通过未经授权的国家进行中继。例如，如果VPN提供商选择了来自斯里兰卡的IP，则该国家必须得到地理保护的授权。此外，如果VPN使用内部企业IP地址，则保护变得无关紧要。

防火墙 / 代理： 硬件防火墙的目的是过滤大型公司的进出连接。由于它仅仅是一个过滤器，因此不应修改源IP地址，因此不应影响地理保护。然而，代理会确实更改源IP地址以使用私有网络地址，这将始终被地理保护允许。此功能的主要目的是阻止对开放给互联网的服务器的访问。如果所有连接都来自企业网络，则保护变得无关紧要。

黑客IP保护

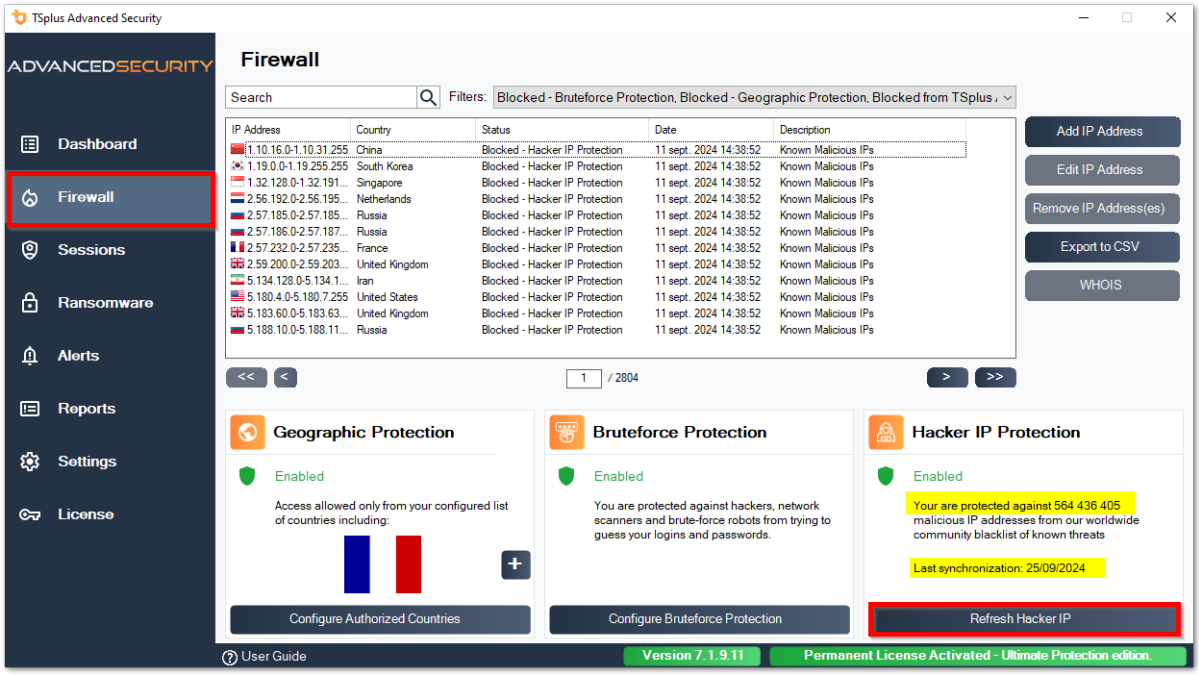
保持您的机器免受已知威胁的保护，例如在线攻击、在线服务滥用、恶意软件、僵尸网络和其他网络犯罪活动，使用黑客IP保护。目标是创建一个足够安全的黑名单，可以在所有系统上使用，配合防火墙，完全阻止对其列出的IP的访问。

支持和更新服务订阅是必需的。

此原因的关键前提是没有误报。所有列出的IP都应为恶意并应被阻止，毫无例外。为此，黑客IP保护利用了高级安全用户社区提供的信息。

黑客IP保护每天自动更新。

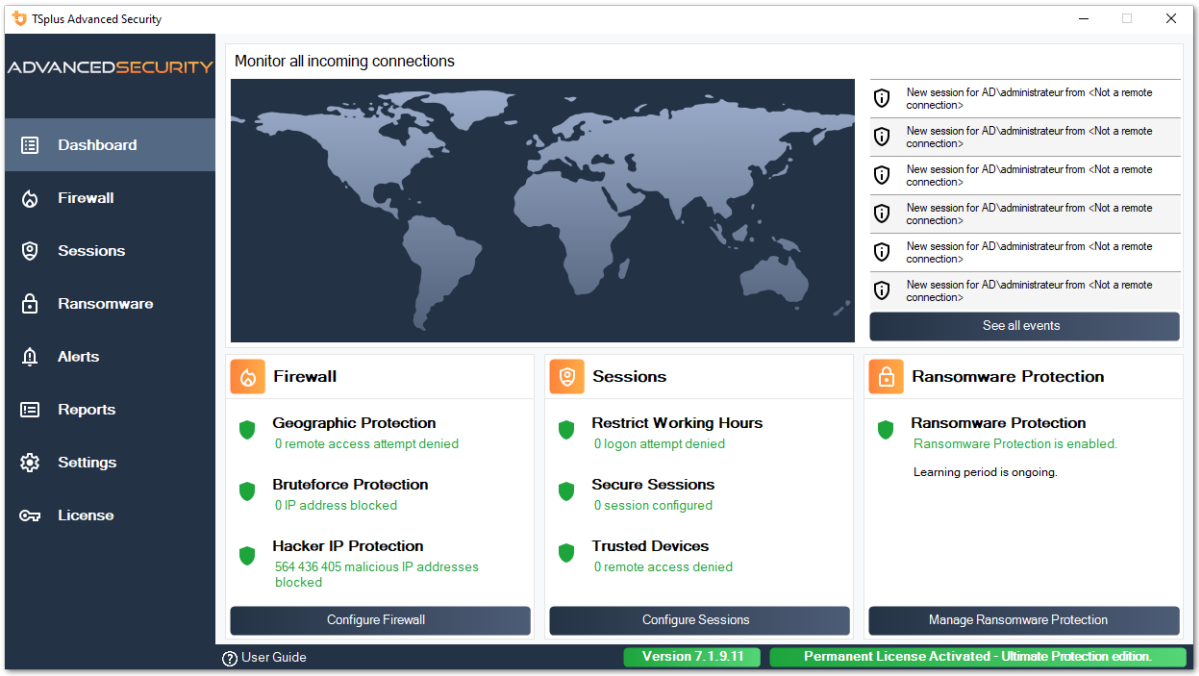
您可以通过点击“刷新黑客 IP”按钮，从“被阻止的 IP 地址”选项卡手动更新：



因此，该功能应在Windows防火墙中创建大约600,000,000个阻止防火墙规则。

仪表板

点击每个图标以了解更多关于每个功能的信息



左侧的菜单栏提供对不同功能的访问。每个图块让您访问 TSplus Advanced Security 提供的各种功能和设置。

高级安全显示最后六个 安全事件 点击任何事件以在单独的窗口中打开完整的事件列表。

在最后的事件下方，三个图块提供快速访问：

1. 防火墙

2. 会话

3. 勒索软件保护

请使用位于右上角的下拉菜单选择您的显示语言，如果应用程序未检测到您的语言。

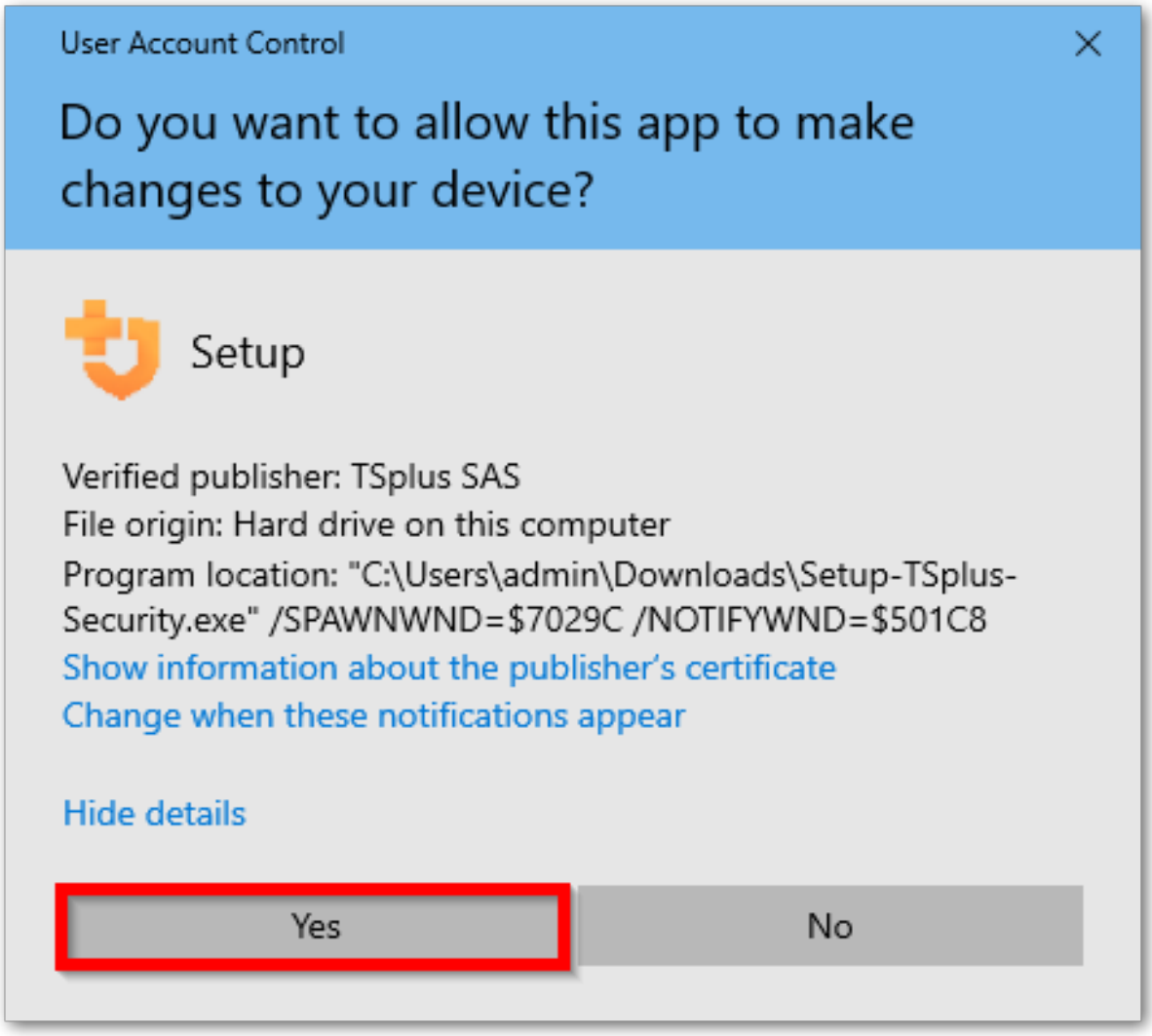
最后，点击“帮助”按钮将会将您重定向到此文档。

安装 TSplus 高级安全性

安装高级安全性

运行 TSplus Advanced Security Setup 程序 **然后** **按照安装步骤** .

您必须以管理员身份运行安装程序并接受软件许可协议。



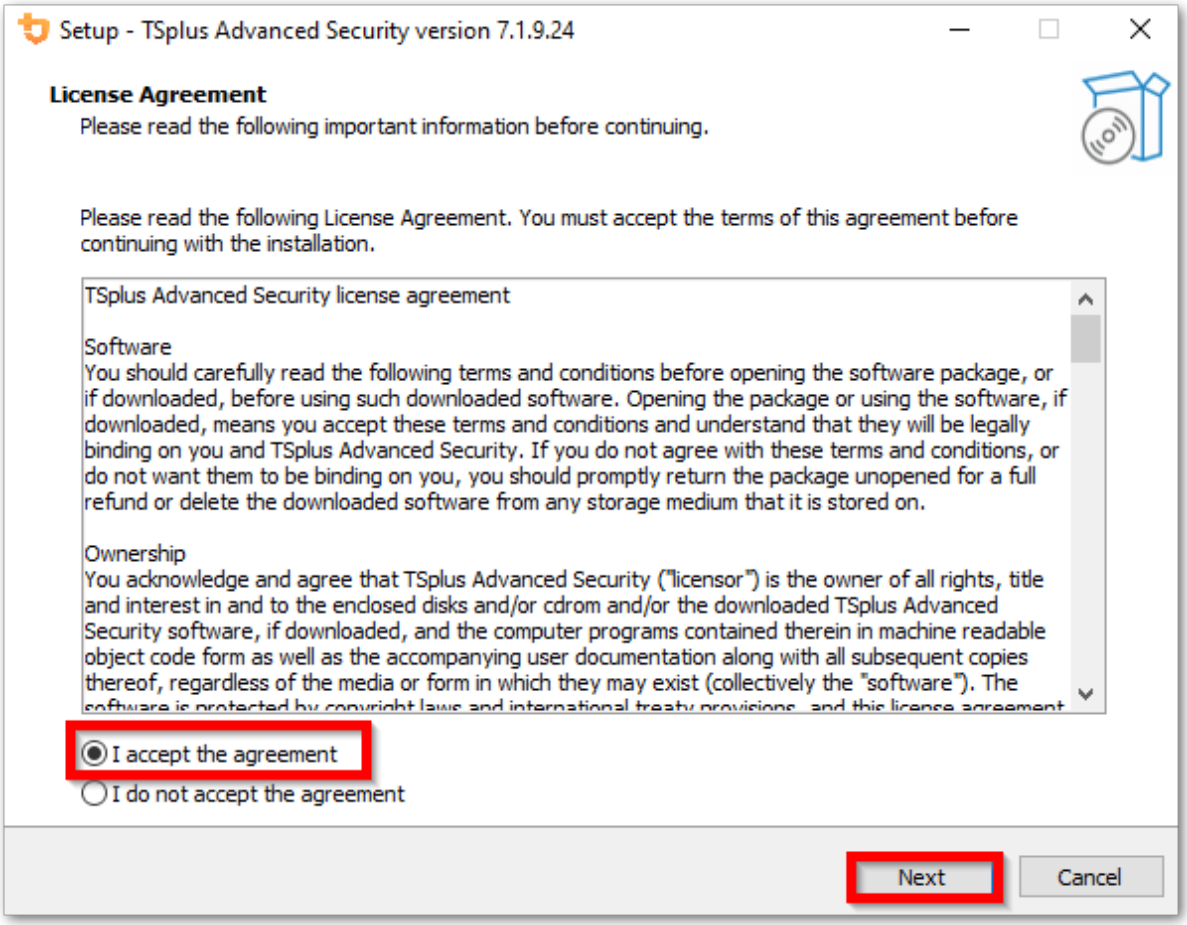
如果未自动检测到，请选择设置助手语言。

然后，选择两个选项之一： **推荐** 或 **高级** 通过点击相应的框。

高级选项增加了额外的步骤，使您能够：

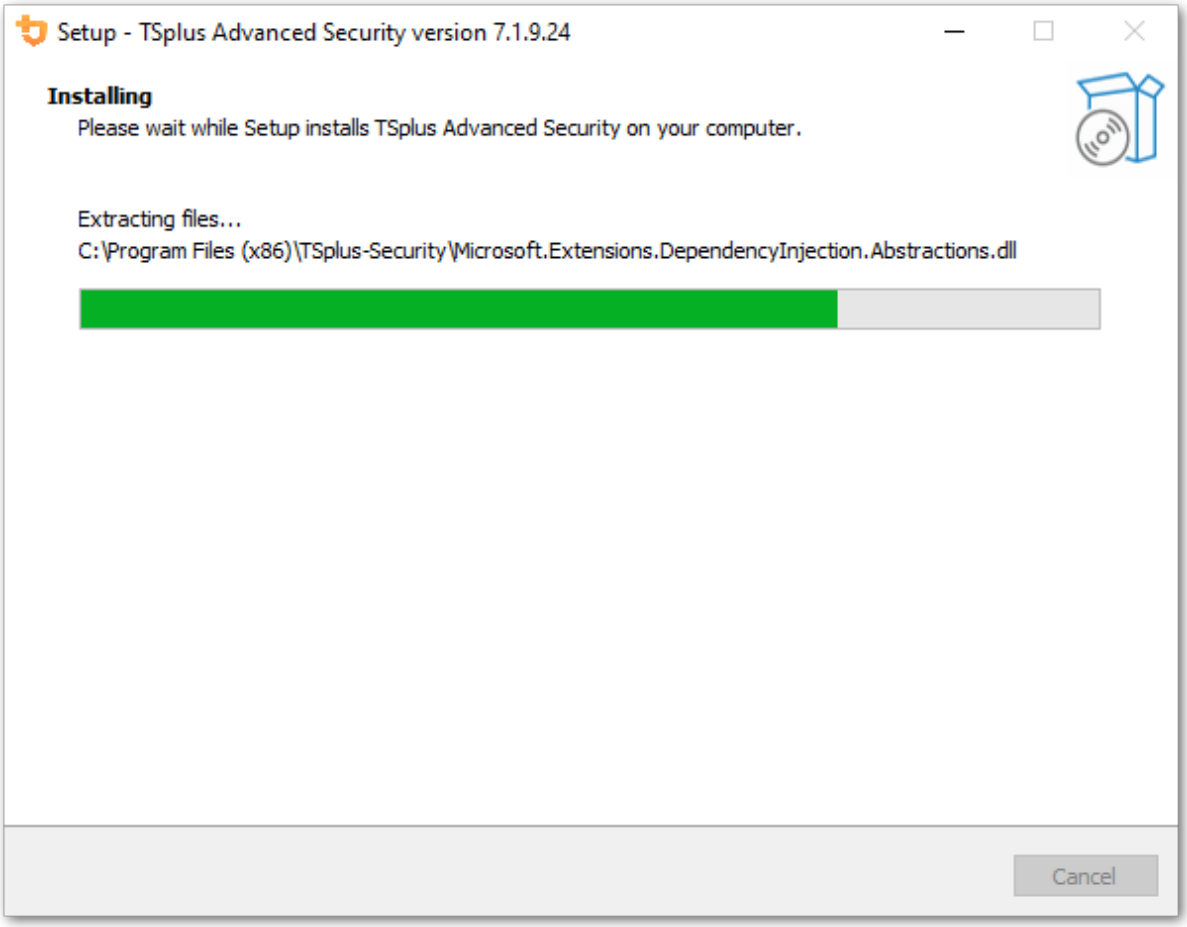
- 仅下载设置（不要安装）
- 使用自定义代理设置

阅读许可协议并点击“我同意”以继续安装。



该程序将安装在您的计算机上。

在底部显示进度条，并报告安装进度。



请耐心等待 有时安装软件可能需要几分钟才能完全完成。

安装完成后，您可以开始使用 TSplus Advanced Security!

免费试用版功能齐全，持续15天。别忘了 激活您的许可证 和到 更新到最新版本 保持高级安全保护处于最佳状态！

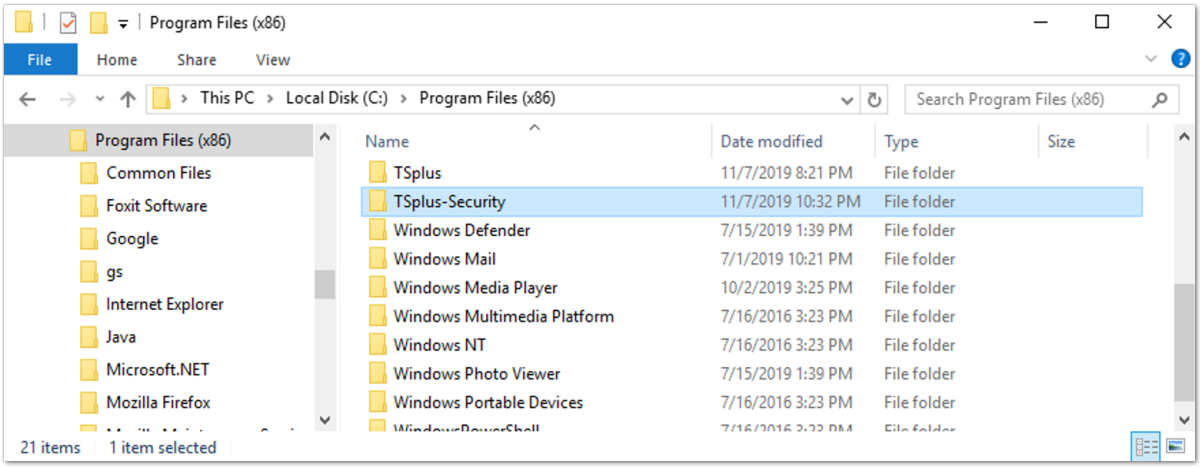
高级安装场景

这 TSplus Advanced Security Classic Setup 程序 处理以下场景，因为它可以从命令行执行：

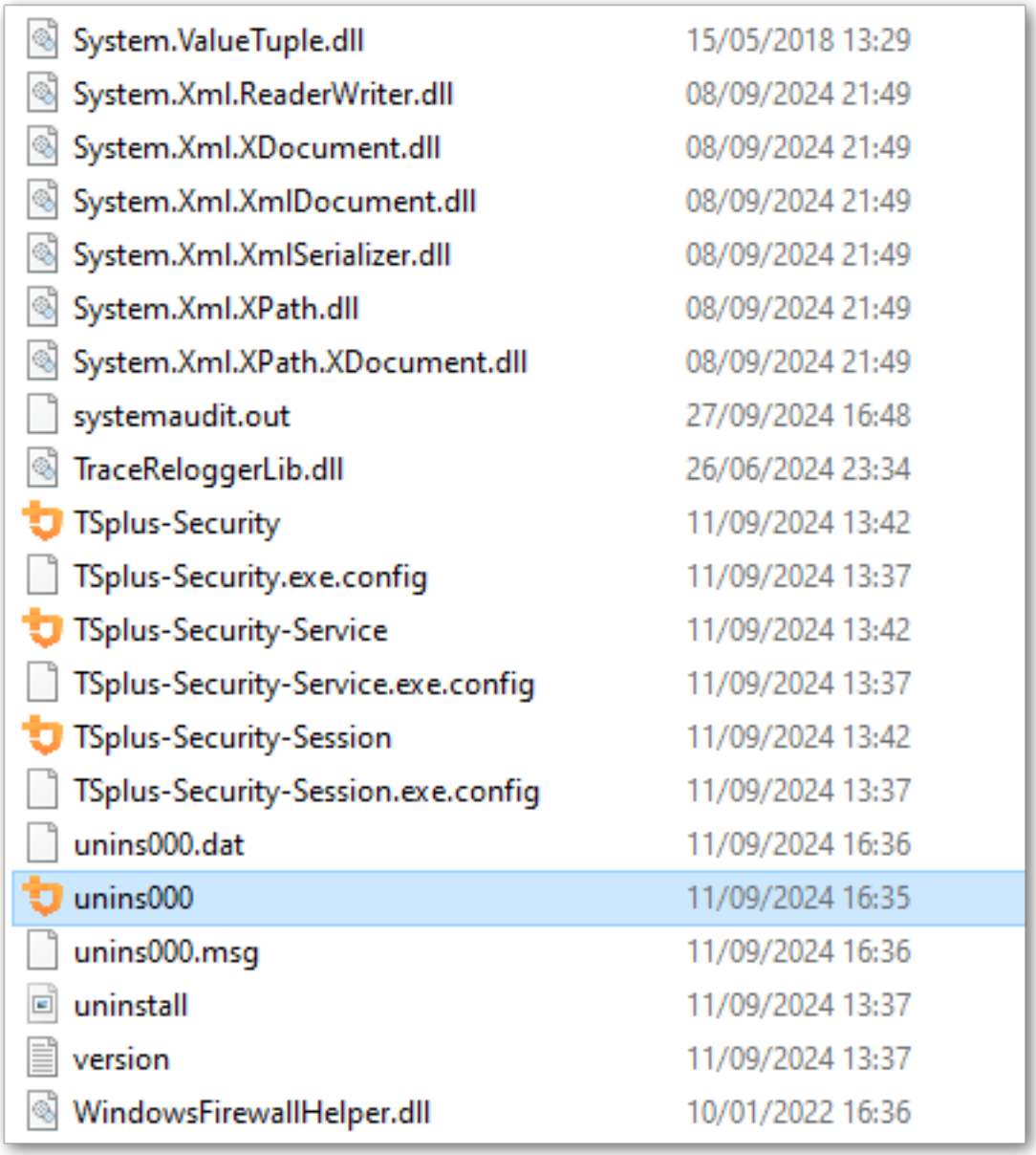
- 静默安装，提供 /VERYSILENT /SUPPRESSMSGBOXES 参数
- 在设置结束时通过提供 /NORESTART 参数来防止重启。此参数通常与上述内容一起使用。
- 在安装时直接激活您的许可证的批量许可（请参阅文档或 联系我们 有关更多信息

卸载 TSplus 高级安全

为了完全卸载 TSplus Advanced Security，请打开目录 C:\Program Files (x86)\TSplus-Security。



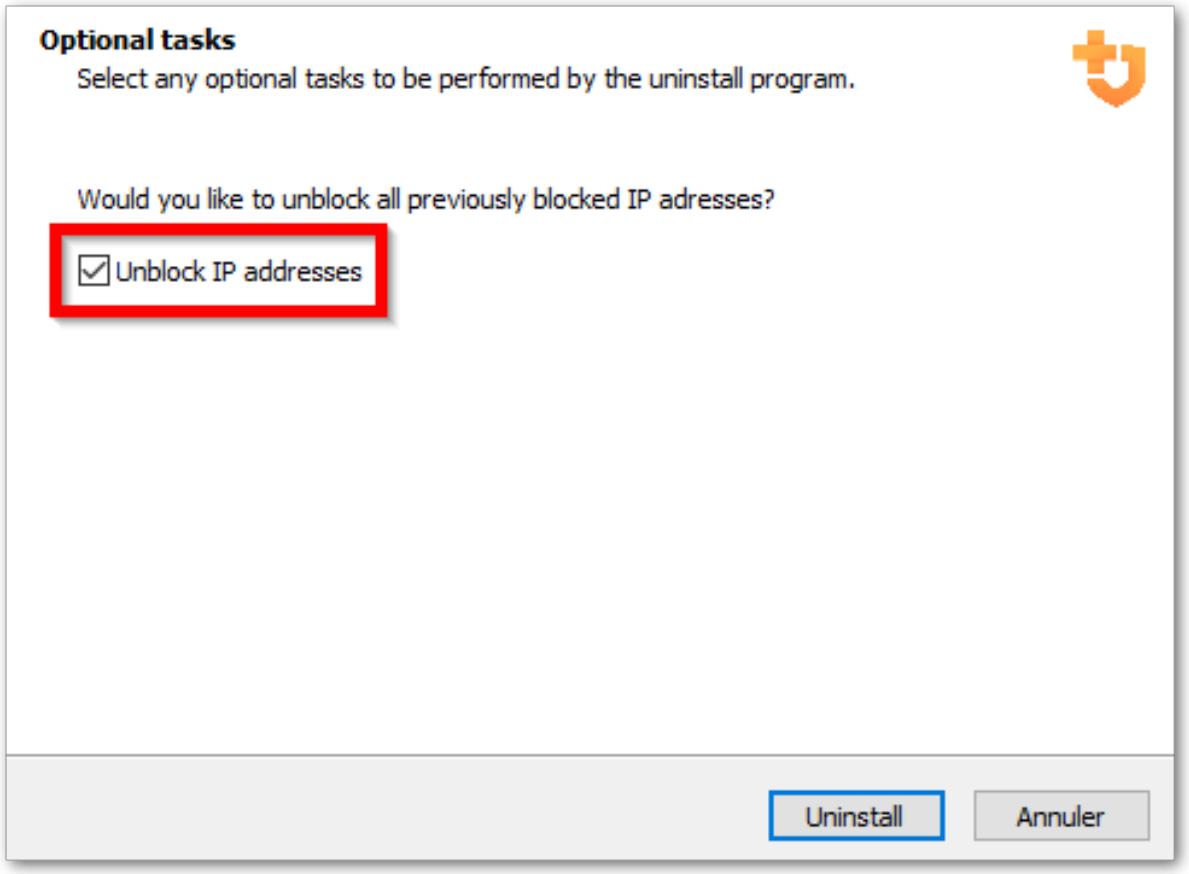
然后，双击“unins000”应用程序以执行卸载程序。



在下一个窗口中点击“是”以完全删除TSplus Advanced Security及其所有组件。

除非另行配置，Advanced Security 会向 Windows 防火墙添加阻止规则。点击“解除阻止 IP 地址”以解除阻止并移除之前被 Advanced Security 阻止的所有 IP 地址。

重要： 请注意，删除所有规则可能需要一个小时。基于此，我们建议直接从Windows防火墙与高级安全控制台中删除规则。



该软件将从您的计算机上完全卸载。

权限管理

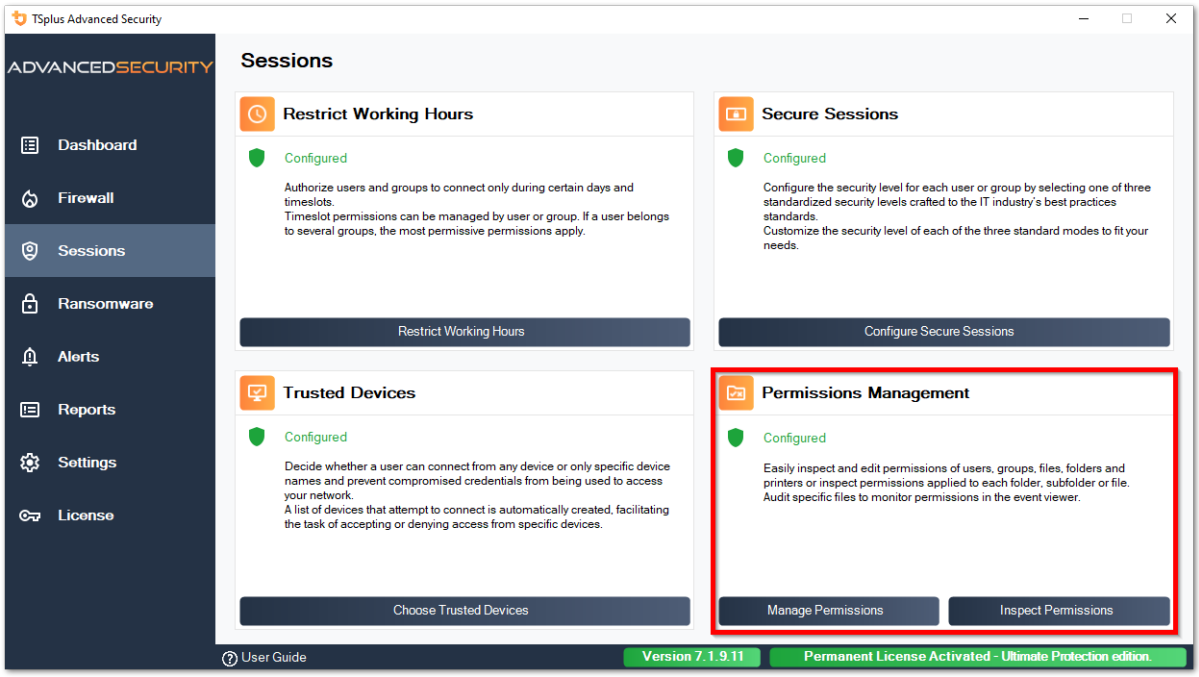
自4.3版本以来，TSplus Advanced Security提供了权限功能，允许管理员管理和/或检查用户/组的权限。

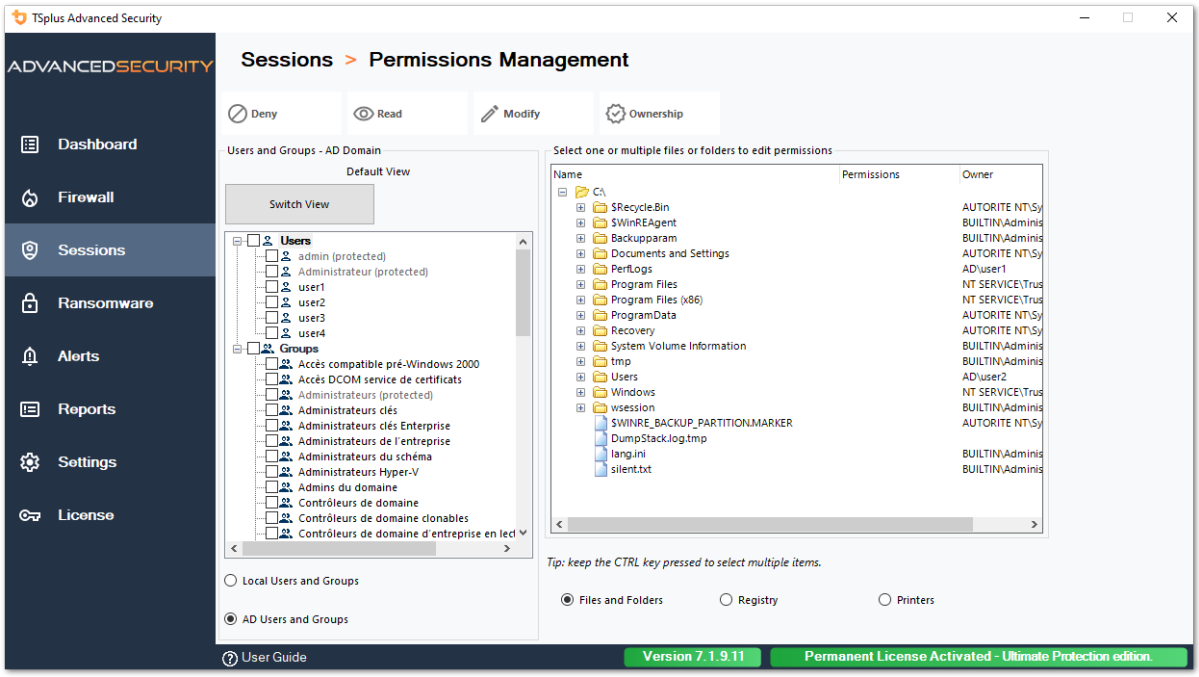
在权限仪表板上，用户和组的列表以及可用的列表 **文件、文件夹、注册表和打印机** 并排显示。

一目了然，这使得它非常容易去 **检查** 和 **管理/编辑** 一次仅为一个用户提供权限，从而提高限制的准确性。

管理权限

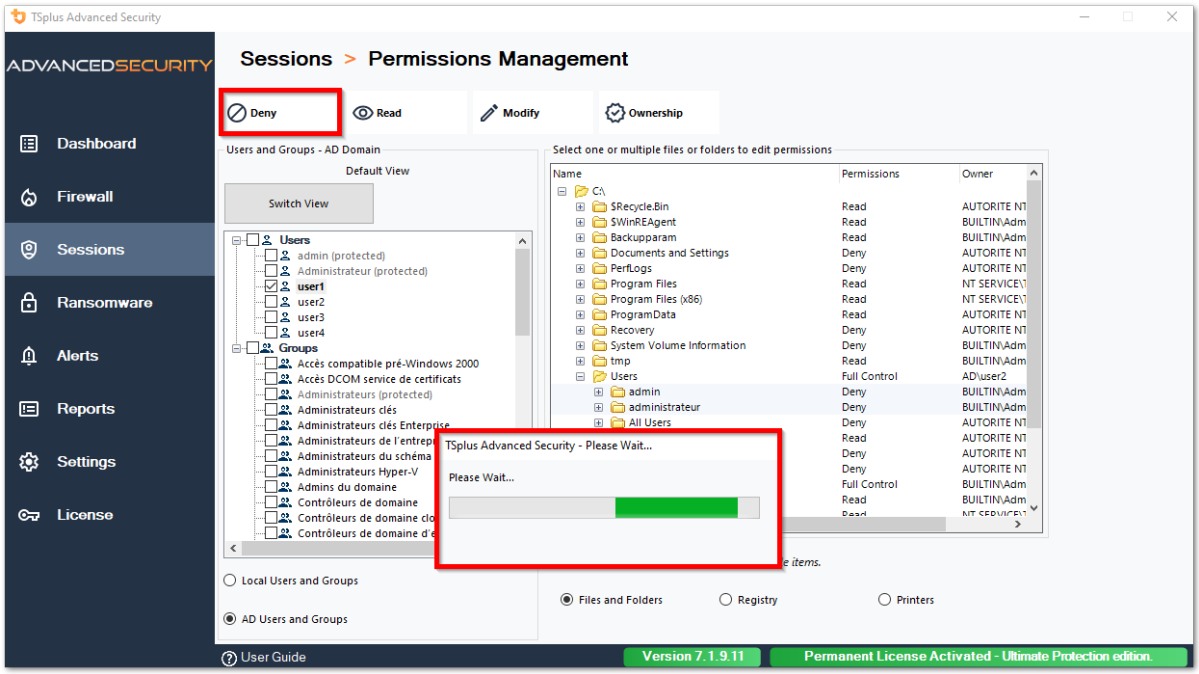
在“管理”选项卡上，对于左侧树视图中选择的每个用户或组，您可以：



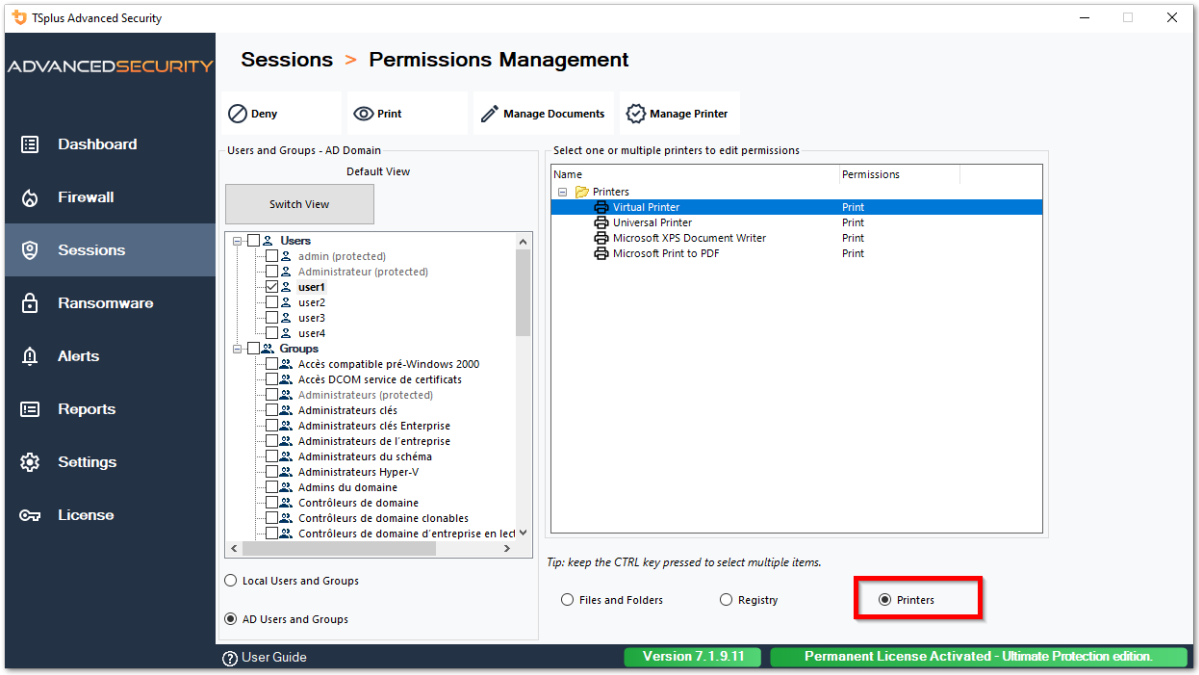


- **拒绝** - 点击拒绝按钮时，所选用户将在所选文件系统对象上被拒绝权限。如果选择了文件，则所选用户被拒绝读取所选文件的权限（FileSystemRights.Read）。如果选择了目录，则所选用户被拒绝读取和列出目录内容的权限（FileSystemRights.Read 和 FileSystemRights.ListDirectory）。
- **阅读** 当点击“读取”按钮时，所选用户将获得对所选文件系统对象的权限。如果选择了一个文件，则所选用户被授予读取所选文件的权限，并在该文件是程序时执行权限（FileSystemRights.ReadAndExecute）。如果选择了一个目录，则所选用户被授予读取和列出或执行目录内容的权限（FileSystemRights.ReadAndExecute 和 FileSystemRights.ListDirectory 和 FileSystemRights.Traverse）。
- **修改** 当点击修改按钮时，所选用户将获得对所选文件系统对象的权限。如果选择了一个文件，则所选用户被授予修改所选文件的权限（FileSystemRights.Modify）。如果选择了一个目录，则所选用户被授予修改和列出目录内容的权限，以及创建新文件或目录的权限（FileSystemRights.Modify 和 FileSystemRights.CreateDirectories 和 FileSystemRights.CreateFiles 和 FileSystemRights.ListDirectory 和 FileSystemRights.Traverse）。
- **所有权** 当点击所有权按钮时，所选用户将获得对所选文件系统对象的完全控制权（FileSystemRights.FullControl）。

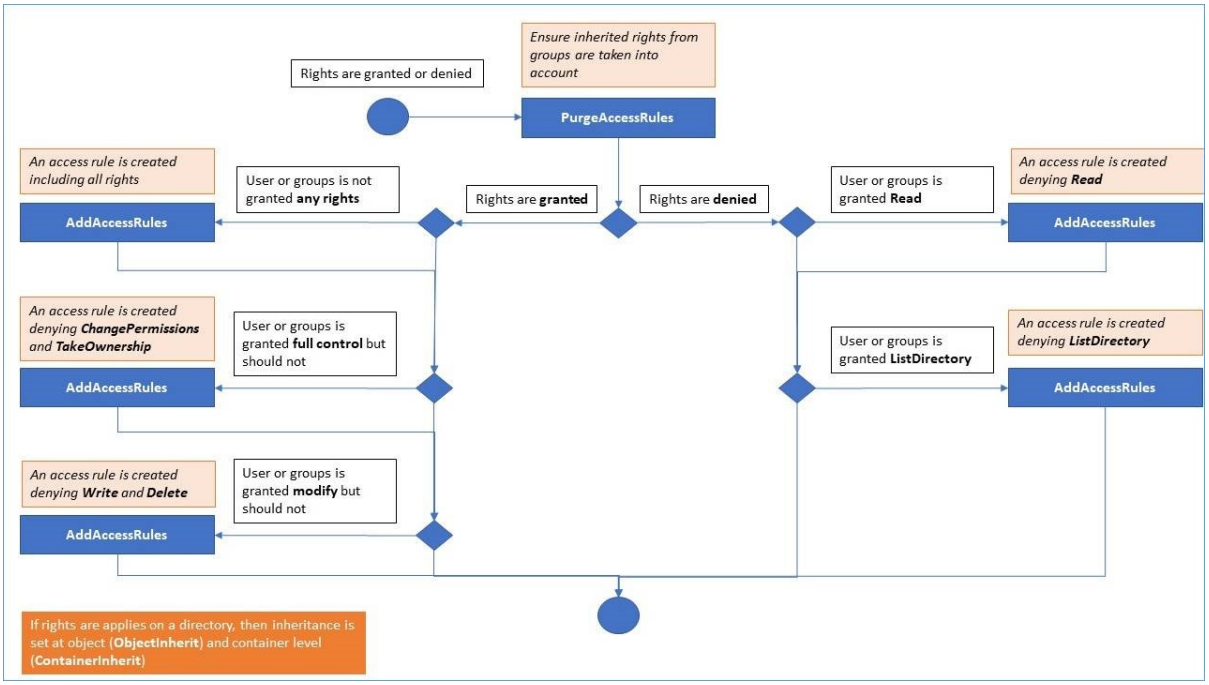
每个注册表的权限选项都是可能的，通过在右侧树视图下选择相应的按钮：



每个打印机：



请注意，所有对目录的权限拒绝或授予都递归地应用于该目录包含的文件系统对象。下面的图表详细说明了在权限应用于文件系统对象时的 API 调用：

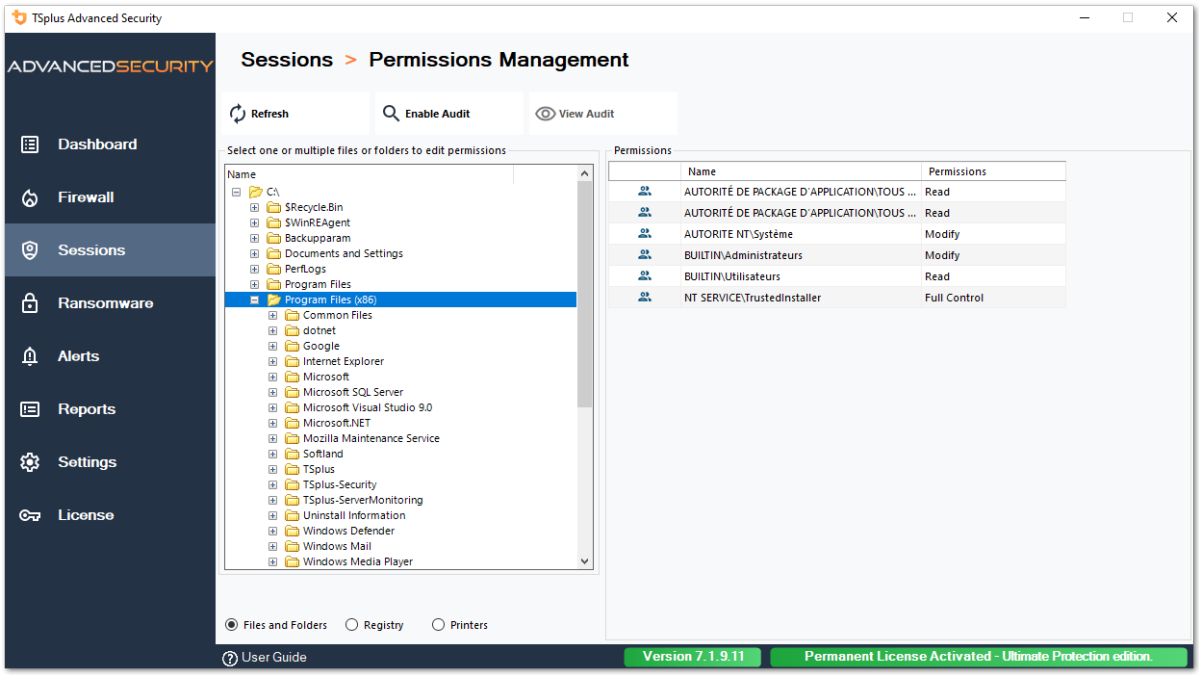


文档：

- 对象安全： https://docs.microsoft.com/zh-cn/dotnet/api/system.security.accesscontrol.objectsecurity?view=netframework-4.5.2
- 文件系统权限： https://docs.microsoft.com/zh-cn/dotnet/api/system.security.accesscontrol.filesystemrights?view=netframework-4.5.2

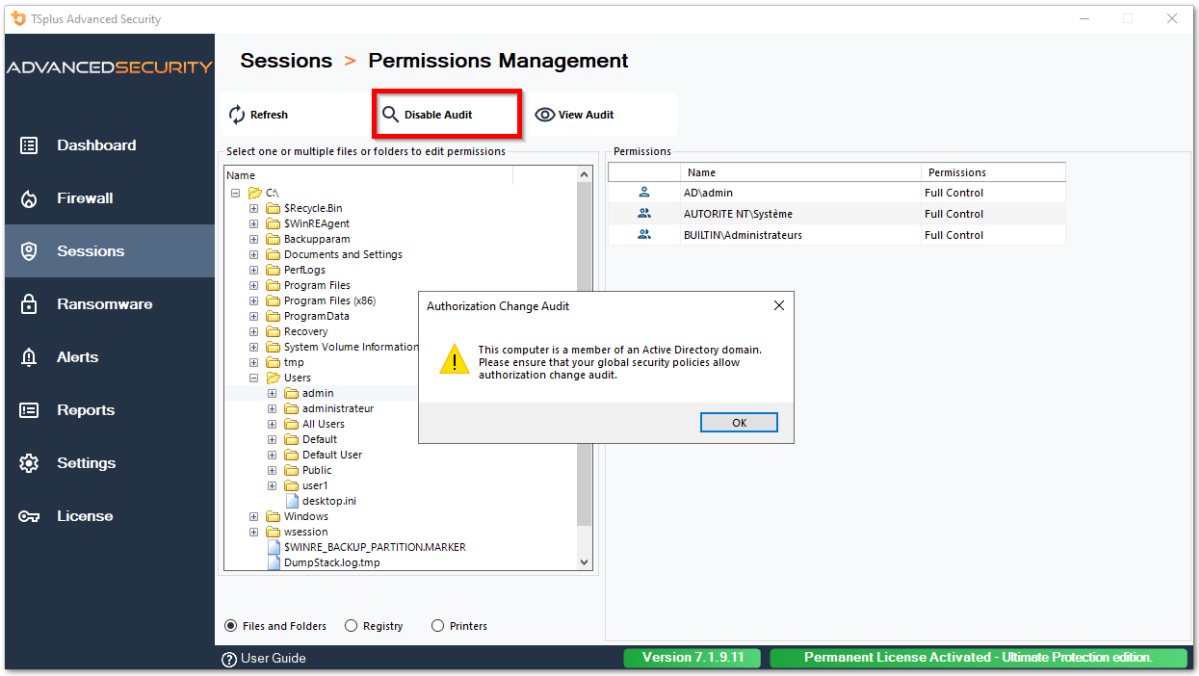
检查权限

在“检查”选项卡中，对于左侧树视图中选定的每个文件夹、子文件夹或文件，您可以在右侧树视图中查看相应的用户或组的权限。

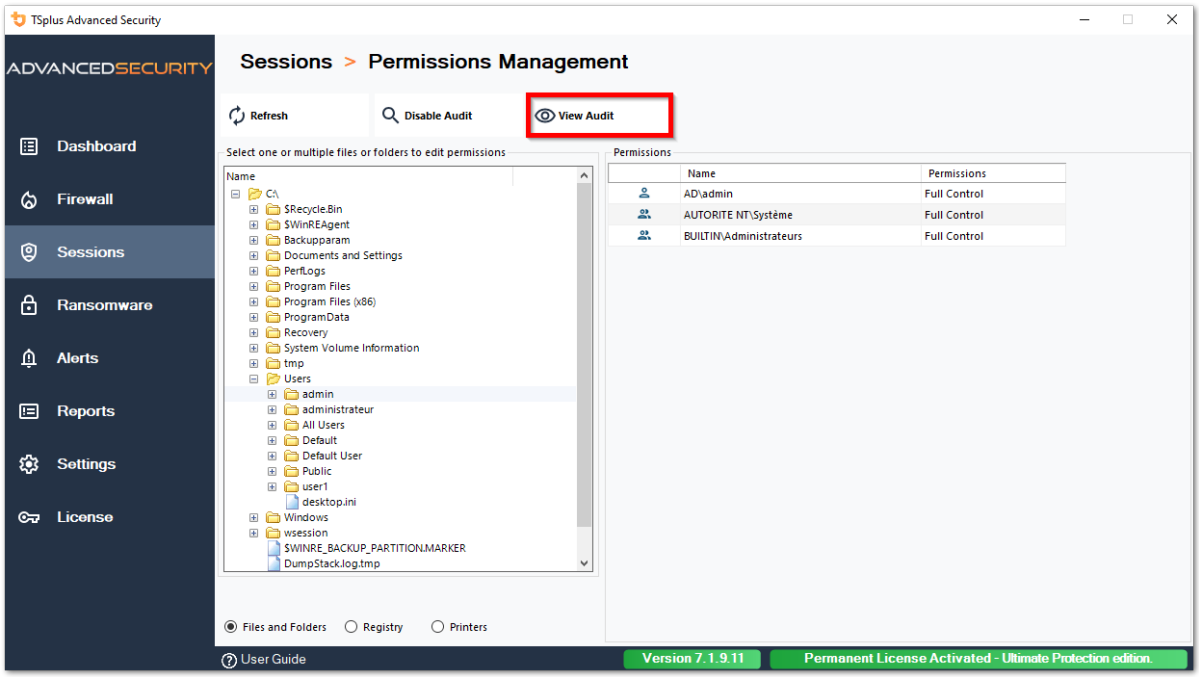


您可以刷新文件夹的状态，以便实时更新。

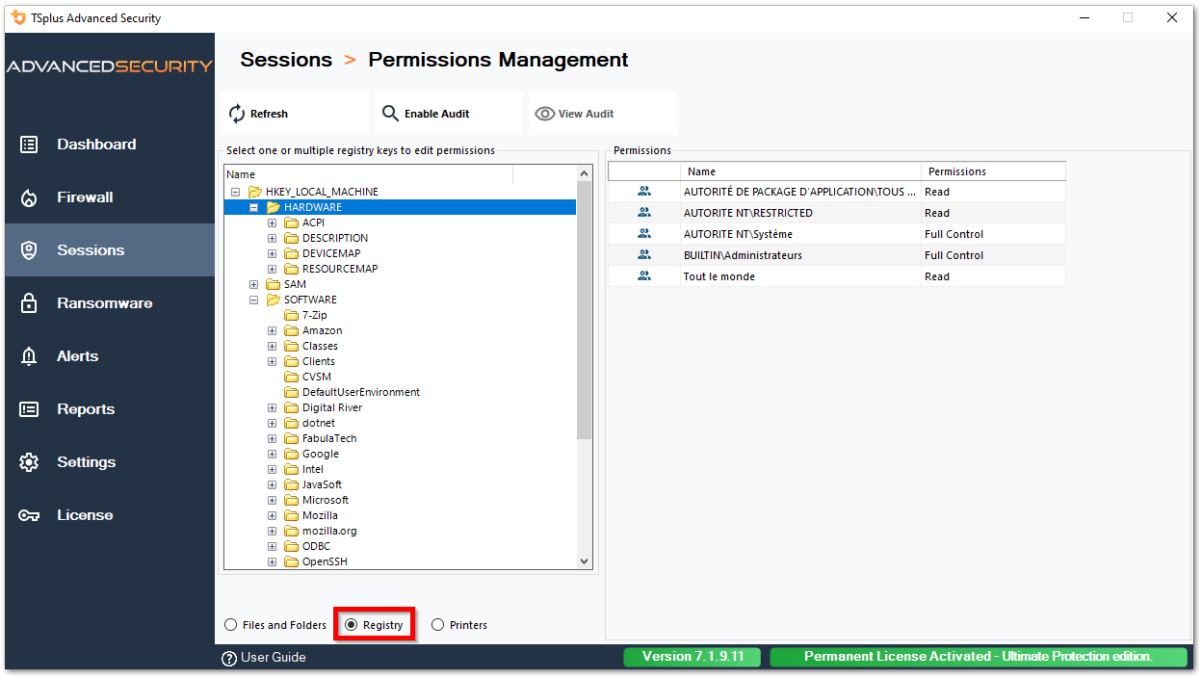
可以通过选择所需的文件夹、子文件夹或文件，然后点击顶部的“启用审计”按钮来启用审计。

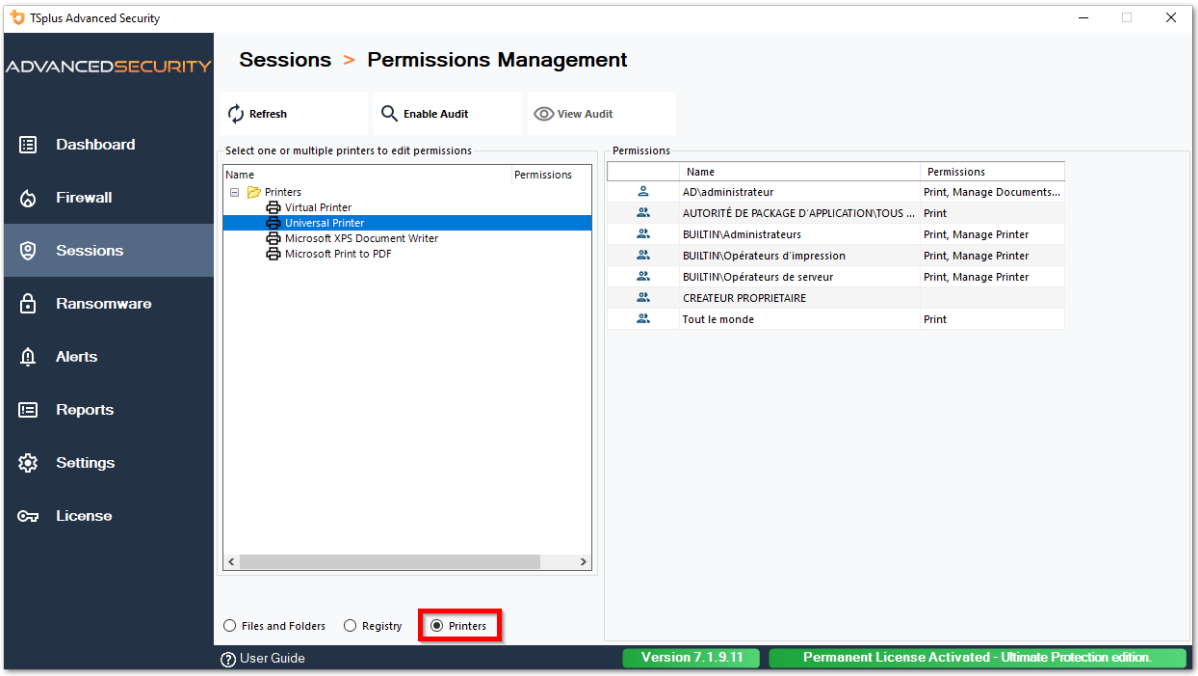


“查看审计”按钮允许您在事件查看器中查看相应的审计：



每个注册表和打印机都有相同的检查选项，可以通过在左侧树视图下选择相应的按钮来实现。




TSplus Advanced Security
ADVANCEDSECURITY
Dashboard
Firewall
Sessions
Ransomware
Alerts
Reports
Settings
License
Sessions > Permissions Management
Refresh
Enable Audit
View Audit
Select one or multiple printers to edit permissions
Name
Permissions
Printers
Virtual Printer
Universal Printer
Microsoft XPS Document Writer
Microsoft Print to PDF
Permissions
Name
Permissions
AD\administrateur
Print, Manage Documents...
AUTORITÉ DE PACKAGE D'APPLICATION\TOUS ...
Print
BUILTIN\Administrateurs
Print, Manage Printer
BUILTIN\Opérateurs d'impression
Print, Manage Printer
BUILTIN\Opérateurs de serveur
Print, Manage Printer
CREATEUR PROPRIETAIRE
Tout le monde
Print
Files and Folders
Registry
Printers
User Guide
Version 7.1.9.11
Permanent License Activated - Ultimate Protection edition.

TSplus高级安全 - 先决条件

硬件要求

TSplus Advanced Security 支持 32 位和 64 位架构。

操作系统

您的硬件必须使用以下操作系统之一：

- Windows **7专业版**
- Windows **8/8.1 专业版**
- Windows **10专业版**
- Windows **11 Pro**
- Windows **Server 2008 SP2/小型企业服务器 SP2 或 2008 R2 SP1**
- Windows **Server 2012 或 2012 R2**
- Windows **Server 2016**
- Windows **Server 2019**
- Windows **服务器 2022**
- Windows **服务器 2025**

同时支持32位和64位架构。

软件要求

TSplus Advanced Security需要以下先决条件：

- 运行时： .NET Framework 4.7.2 或更高版本
- Microsoft Windows 7 SP1 和 Windows 2008 R2 SP1 需要额外的更新以支持 SHA2 交叉签名（ KB4474419 此更新允许TSplus Advanced Security内置防火墙和勒索软件保护正常运行。

注意： 这些先决条件将在系统缺失时由安装程序自动安装。

TSplus高级安全 - 入门指南

先决条件

TSplus Advanced Security需要以下先决条件。

- 操作系统：Microsoft Windows 7 版本，服务包 1（构建 6.1.7601）或 Windows 2008 R2，服务包 1（构建 6.1.7601）或更高版本。

以下 **先决条件将由安装程序自动安装。** 如果缺少：

- 运行时： .NET Framework 4.5.3 或更高版本
- Microsoft Windows 7 SP1 和 Windows 2008 R2 SP1 需要额外的更新以支持 SHA2 交叉签名（ KB4474419 此更新允许TSplus Advanced Security内置防火墙和勒索软件保护正常运行。

请参考该 文档 有关先决条件的更多详细信息。

步骤 1：安装

最新的 TSplus Advanced Security 安装程序始终可以在此处获取： 最新的 TSplus 高级安全设置程序 请下载安装程序并按照安装向导进行操作。

TSplus Advanced Security 安装程序通常不需要重启您的系统以完成安装。

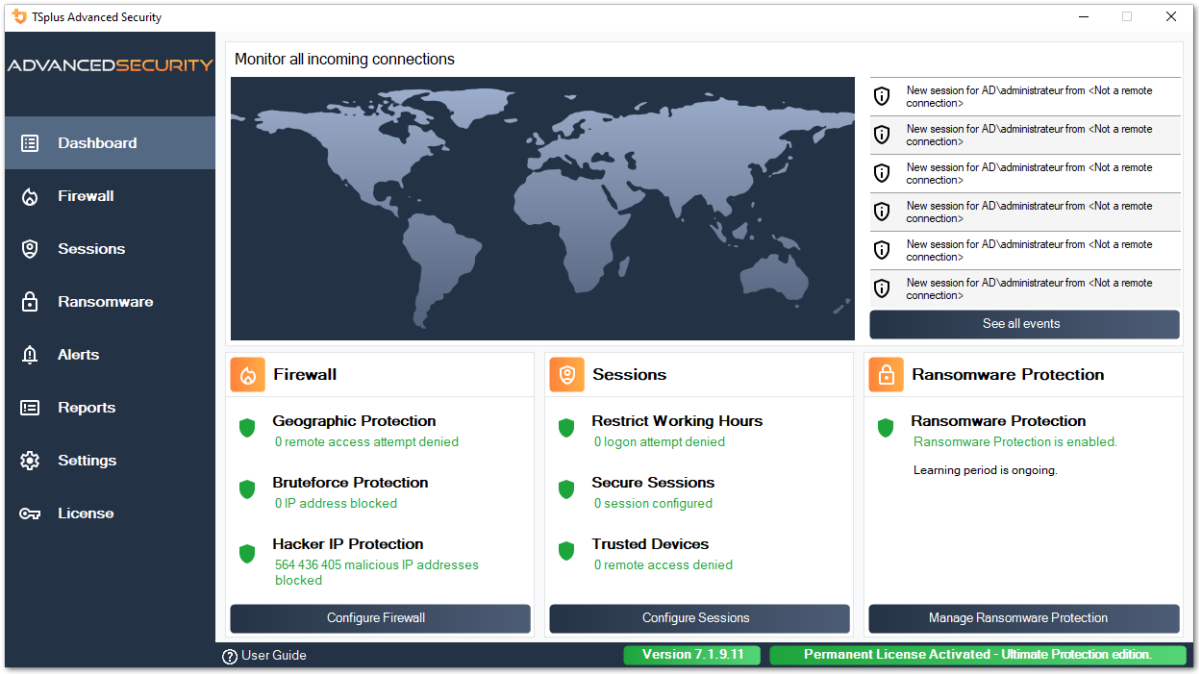
任何新安装都将开始为期 15 天的完整功能试用期。请随时联系 联系我们 如果您在配置 TSplus Advanced Security 时遇到任何障碍或问题。

安装完成后，桌面上会显示一个新图标。双击此图标以打开 TSplus Advanced Security 并开始配置安全功能。

请参考该 文档 完整安装说明。

步骤 2：配置 TSplus 高级安全性

您已启动 TSplus Advanced Security 并开始配置功能，以保护您的服务器免受恶意活动的影响，并实施强大的安全策略。



在左侧栏中，主页允许快速访问配置勒索软件保护、暴力破解保护和地理保护功能。

开始 勒索软件保护 学习期间，以便Advanced Security能够通过点击以下图块识别您系统上的合法应用程序和行为：

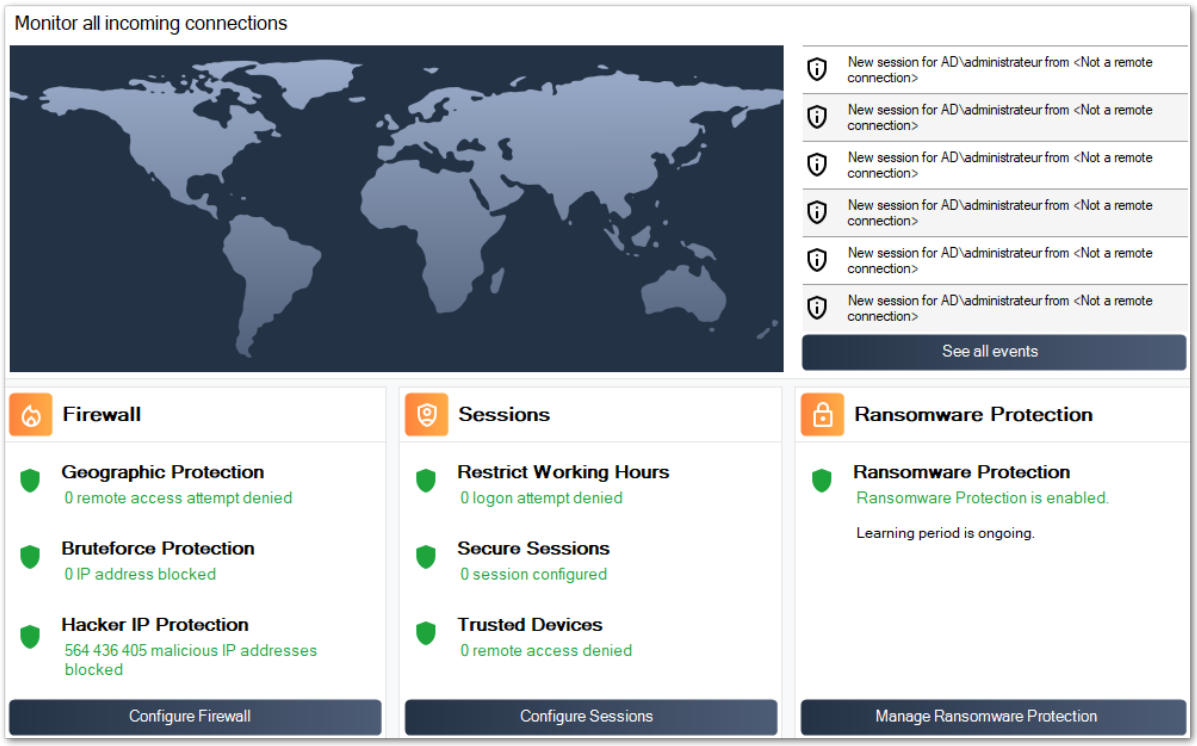
暴力破解保护 通常在安装后即可运行。否则，请单击该 **重复防御暴力攻击** 解决问题并应用所需的系统配置。默认情况下，此功能会在连续 10 次登录失败后阻止攻击者。

最后，将您的国家添加到允许客户连接的授权国家列表中。点击瓷砖 **授权来自其他国家的连接** 并添加您的国家以进行配置 地理保护

您已准备就绪！别忘了 激活您的许可证 和到 更新到最新版本 保持高级安全保护处于最佳状态！

步骤 3：审查被阻止的威胁

现在您已经配置了关键的高级安全功能，避免的威胁将在仪表板中报告。



此外， 黑客 IP 保护使机器免受已知威胁的影响，通过阻止超过 500,000,000 个已知恶意 IP 地址。

所有的 安全事件 可以通过点击显示 **查看所有事件** 瓷砖。

第4步：利用其他安全功能增强保护

在底部，可以访问和配置其他四个安全功能，以增强您机器的保护。

- 调整和监控您本地文件系统、打印机和注册表项上的访问权限，以确保每个用户都能访问相关资源，使用该 权限 功能。
- 定义用户被授权登录的时间段 Working Hours 功能。用户将在允许的工作时间结束后被断开连接。
- 自定义并保护用户会话与TSplus 安全桌面 功能。自定义、隐藏、拒绝本地用户对会话界面项目的访问。
- 验证远程客户端的名称，当用户连接到您的机器时 端点保护 此功能验证每个远程连接用户的客户端计算机名称。

还有更多！切换到高级模式将为您提供更多功能。

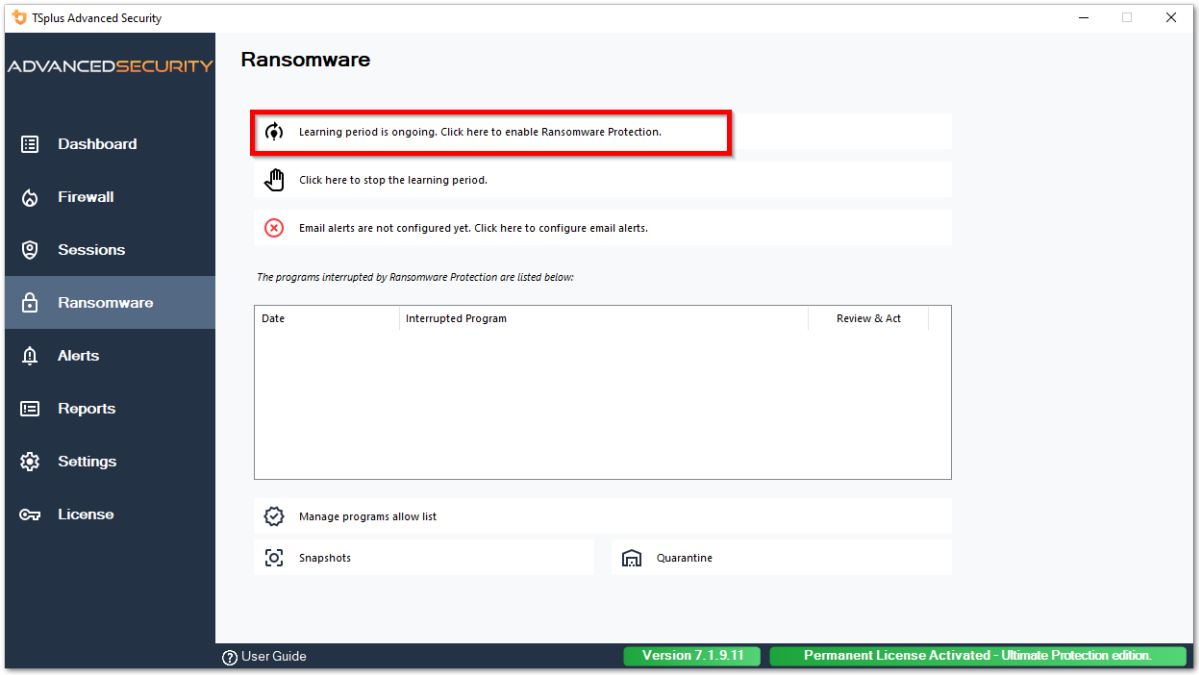
感谢您使用 TSplus Advanced Security!

勒索软件保护

勒索软件保护使您能够有效地检测、阻止和预防勒索软件攻击。TSplus Advanced Security 在检测到您会话中的勒索软件时立即做出反应。它具有两者的功能。 **静态和行为分析** ：

- 这 **静态分析** 使软件在扩展名更改时立即做出反应，
- 这 **行为分析** 查看程序如何与文件交互并检测新型勒索软件。

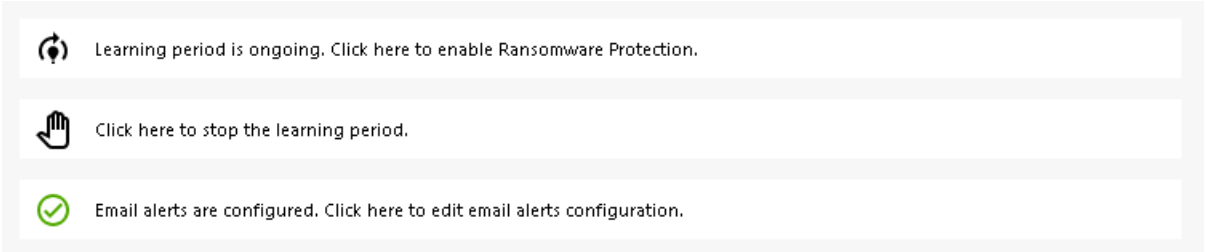
您可以通过点击“启用勒索软件保护”选项卡上的“启用勒索软件保护”来启用它：



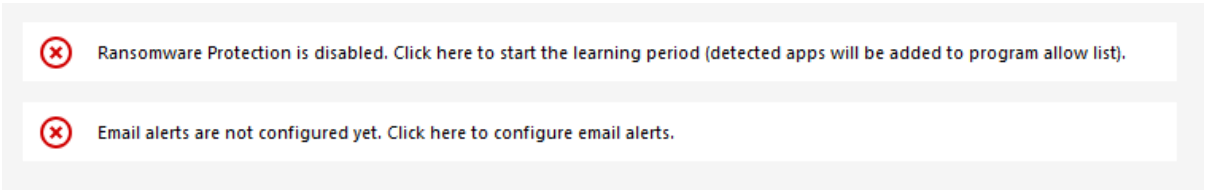
学习期

启用勒索软件保护功能后，学习期会自动激活。在学习期间，勒索软件保护功能检测到的所有程序将被视为误报，并能够恢复其执行。被检测为误报的程序将自动添加到允许程序列表中。

此功能允许在生产服务器上配置勒索软件保护，而不会干扰其活动。我们建议从5天的学习期开始，以识别所有合法的业务应用程序。



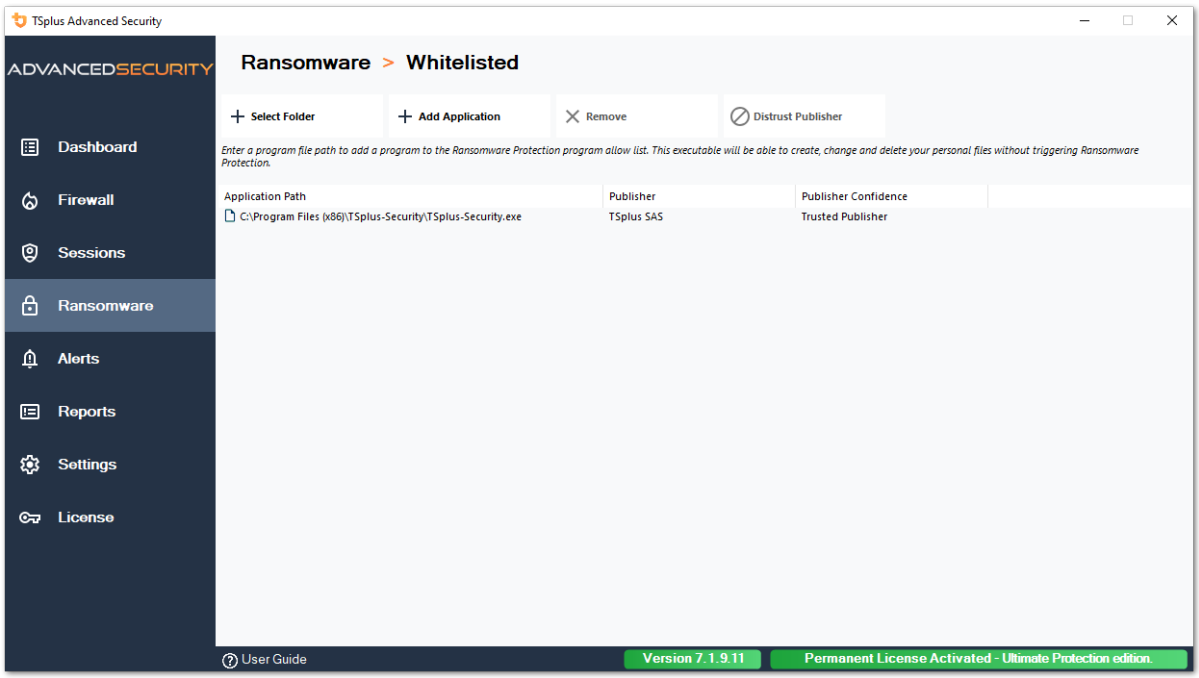
如果您停止学习周期，它将停用勒索软件保护。点击“勒索软件保护已禁用”按钮以重新激活学习周期。



勒索软件保护行动

它快速扫描您的磁盘，并显示负责的文件或程序，并提供受感染项目的列表。TSplus Advanced Security 自动停止攻击并隔离程序以及在其干预之前加密的文件。

只有管理员可以将它们列入白名单，方法是在底部输入所需程序的路径，然后点击“添加”：



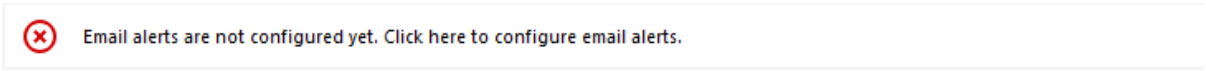
勒索软件保护报告

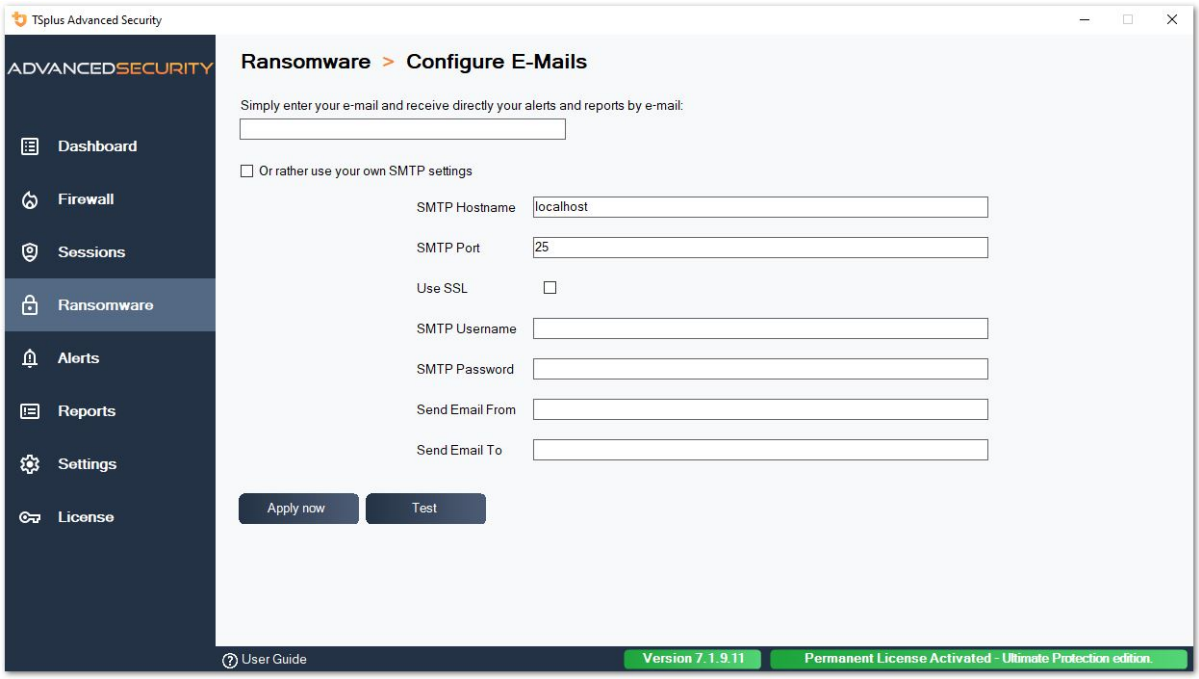
TSplus Advanced Security 通过在早期阶段移除勒索软件，防止企业发生灾难性事件。

管理员可以访问有关攻击来源和正在运行的进程的信息，因此可以了解如何预防这些威胁。

注意 勒索软件保护观察程序如何与系统和个人文件交互。为了确保更高水平的保护，勒索软件保护在勒索软件通常开始攻击的关键文件夹中创建诱饵文件。因此，用户的桌面和文档文件夹以及其他位置可能会出现一些隐藏文件。当它检测到恶意行为时，会立即停止勒索软件（或询问登录用户是否为管理员）。勒索软件保护使用纯行为检测技术，不依赖于恶意软件签名，从而能够捕捉尚不存在的勒索软件。

您可以配置您的SMTP设置，以便TSplus Advanced Security向您发送电子邮件警报，以突出重要的安全事件，方法是点击Ransomware激活按钮下方的按钮：





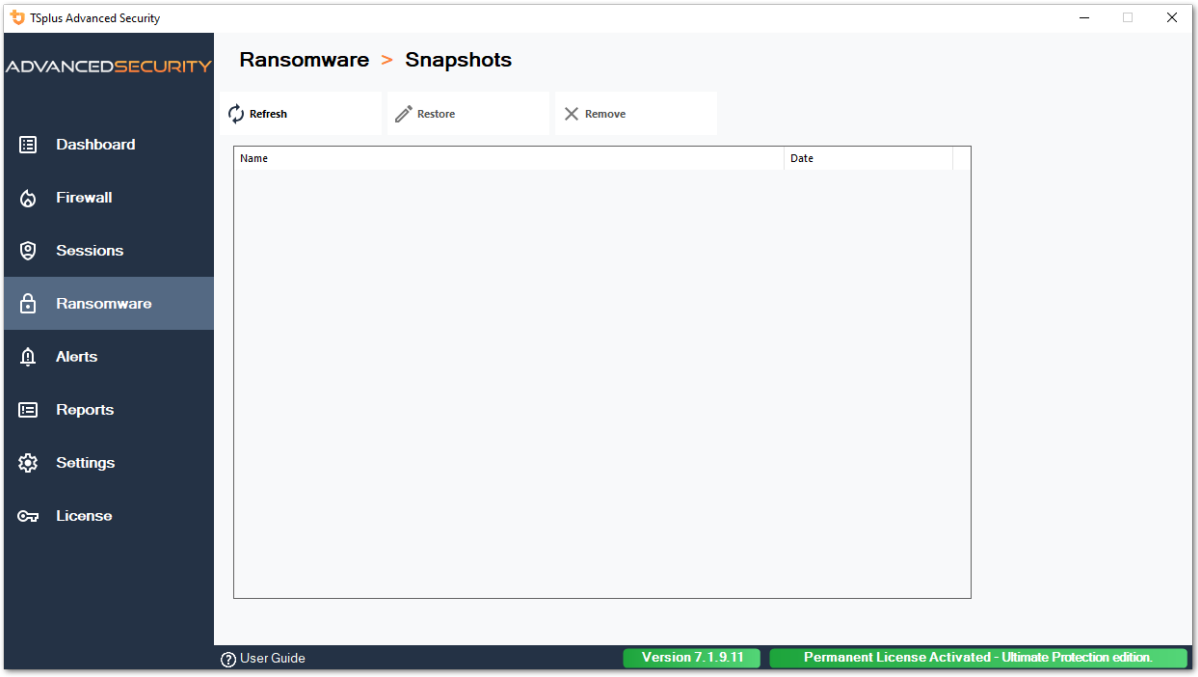
输入您的 SMTP 主机名、端口，并勾选使用 SSL 选项，如果您希望使用 SSL，请将端口从 25 更改为 465。

输入SMTP用户名和密码，以及发件人和收件人地址。

电子邮件设置可以通过在保存SMTP设置时发送测试来验证。

快照

勒索软件保护拍摄的快照可在快照选项卡下查看：

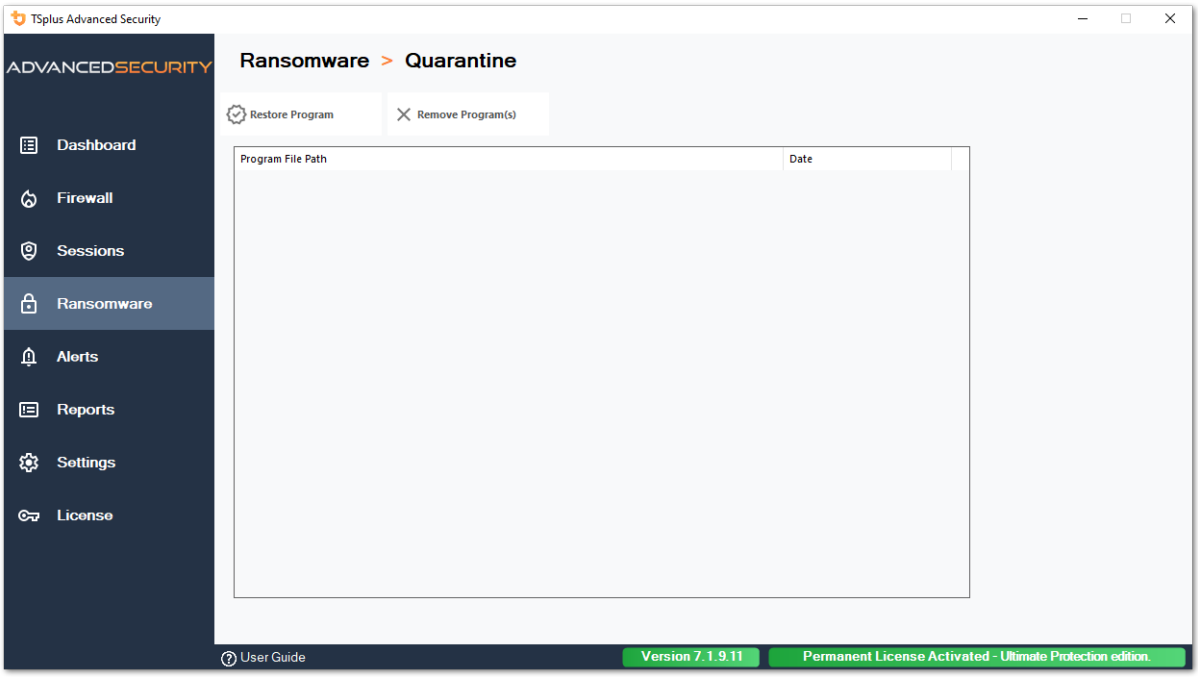


可以通过点击相应的按钮刷新列表。每个元素都可以恢复或删除。

隔离

隔离的程序可以在隔离选项卡下查看：
潜在的不需要程序会被无限期隔离，直到您决定采取行动。

通过这种方式，Advanced Security 确保您的机器安全，同时让您可以根据需要管理隔离项。
这在您需要检索被中和的文件或程序时可能会很有用。 **此决定由您自行承担风险。**
您还可以直接从位于高级安全安装目录中的隔离文件夹中永久删除您选择的任何文件或程序。



每个元素都可以恢复或删除。

忽略的文件不会用于检测可能的恶意行为，并且在修改时不会被保存。这个想法是排除对大型或不相关文件（例如日志文件）的任何操作。

- 系统
- dll
- exe
- 临时
- ~tmp
- 温度
- 缓存
- lnk
- 1
- 2
- 3
- 4
- 5
- 日志1
- LOG2
- customDestinations-ms
- 日志
- wab~
- vmc
- 虚拟硬盘
- vhdx
- 虚拟桌面基础架构
- vo1
- vo2

- vsv
- vud
- iso
- 损坏
- 稀疏图像
- 柜子
- msi
- mui
- 下载_
- 维姆
- 操作系统
- o
- qtch
- ithmb
- vmdk
- 虚拟内存
- vmsd
- vmsn
- vmss
- vmx
- vmxf
- 菜单数据
- 应用图标
- 应用信息
- pva
- pvs
- pvi
- pvm
- fdd
- hds
- 黑暗
- 内存
- 非易失性随机存取存储器
- 硬盘
- pk3
- pf
- trn
- automaticDestinations-ms

备份文件扩展名的注意事项

保存修改文件所用的文件扩展名是： **快照**。 该驱动程序禁止对这些文件进行任何修改或删除操作，除非由TSplus Advanced Security服务执行。停止服务会删除备份的文件。要手动删除这些文件，您必须暂时卸载驱动程序。

备份文件配置

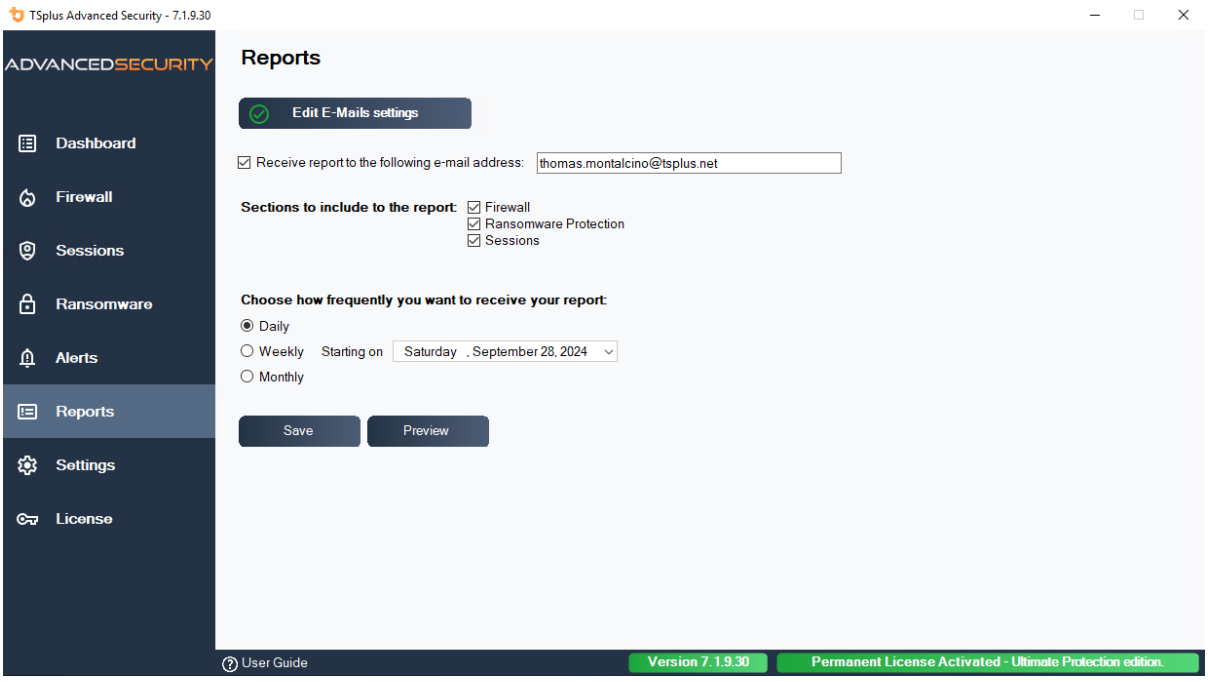
默认情况下，保存文件的目录位于TSplus Advanced Security的安装目录中，称为“快照”。然而，可以为此目录定义另一个位置。这可以允许管理员根据需要定义位于更快的磁盘（SSD）或更大磁盘上的目录。备份目录路径不得为UNC路径，形式为：

\\ \ \

将备份工具添加到白名单

我们建议在白名单中添加备份工具。

报告


TSplus Advanced Security - 7.1.9.30
ADVANCEDSECURITY
Dashboard
Firewall
Sessions
Ransomware
Alerts
Reports
Settings
License
Reports
Edit E-Mails settings
Receive report to the following e-mail address:
thomas.montalcino@tsplus.net
Sections to include to the report:
Firewall
Ransomware Protection
Sessions
Choose how frequently you want to receive your report:
Daily
Weekly
Starting on
Saturday , September 28, 2024
Monthly
Save
Preview
User Guide
Version 7.1.9.30
Permanent License Activated - Ultimate Protection edition.

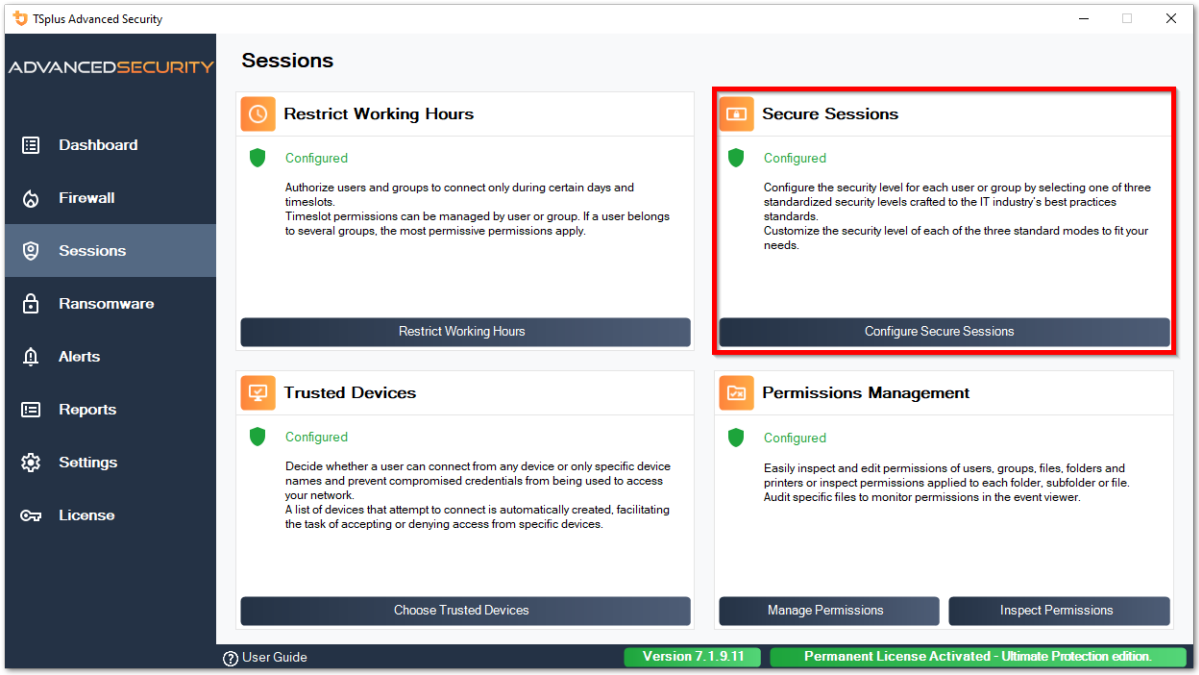
安全会话

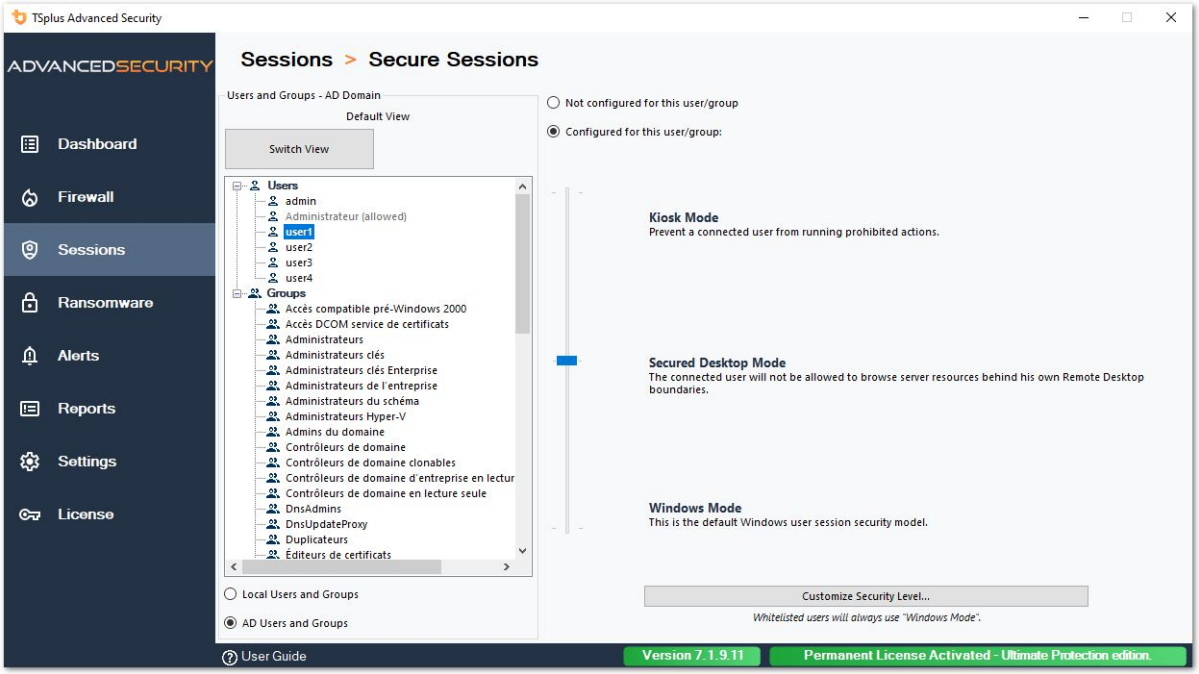
警告

- 安全会话很可能与Active Directory定义的安全策略发生冲突。
- Secure Sessions的主要目的是自定义用户界面，而不是应用访问权限。它的使用应与权限功能结合，以确保对不同驱动器的访问安全。

您可以为每个用户或组配置安全级别。安全级别有三种：

- 这 **Windows模式** 用户可以访问默认的Windows会话。
- 这 **安全会话模式** 用户无法访问控制面板、程序、磁盘、浏览器，无法右键点击……：无法访问服务器资源。他只能访问文档、打印机、Windows 键，并且可以断开他的会话。
- 这 **自助服务模式** 是最安全的，用户在其会话中具有非常有限的操作。

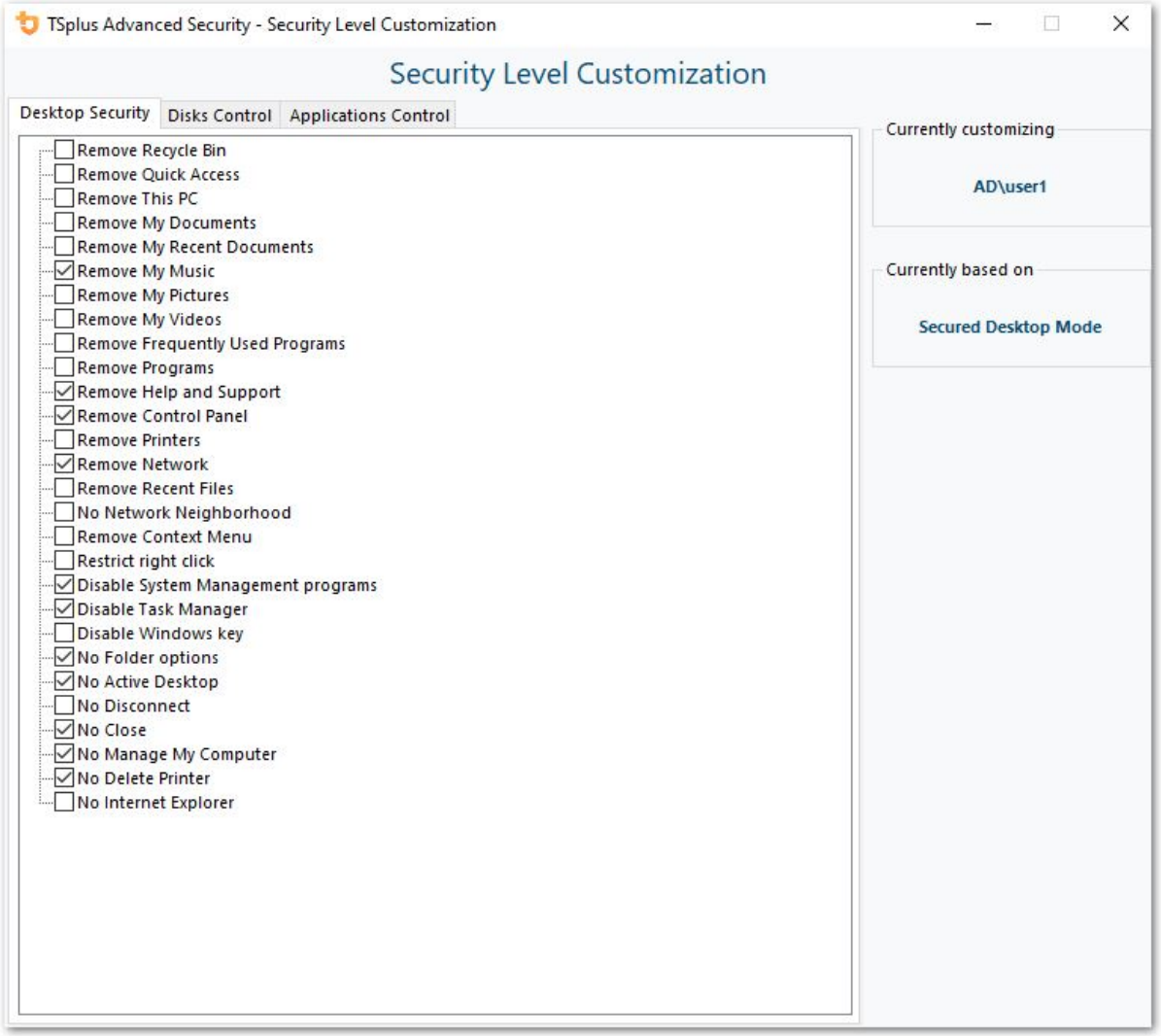




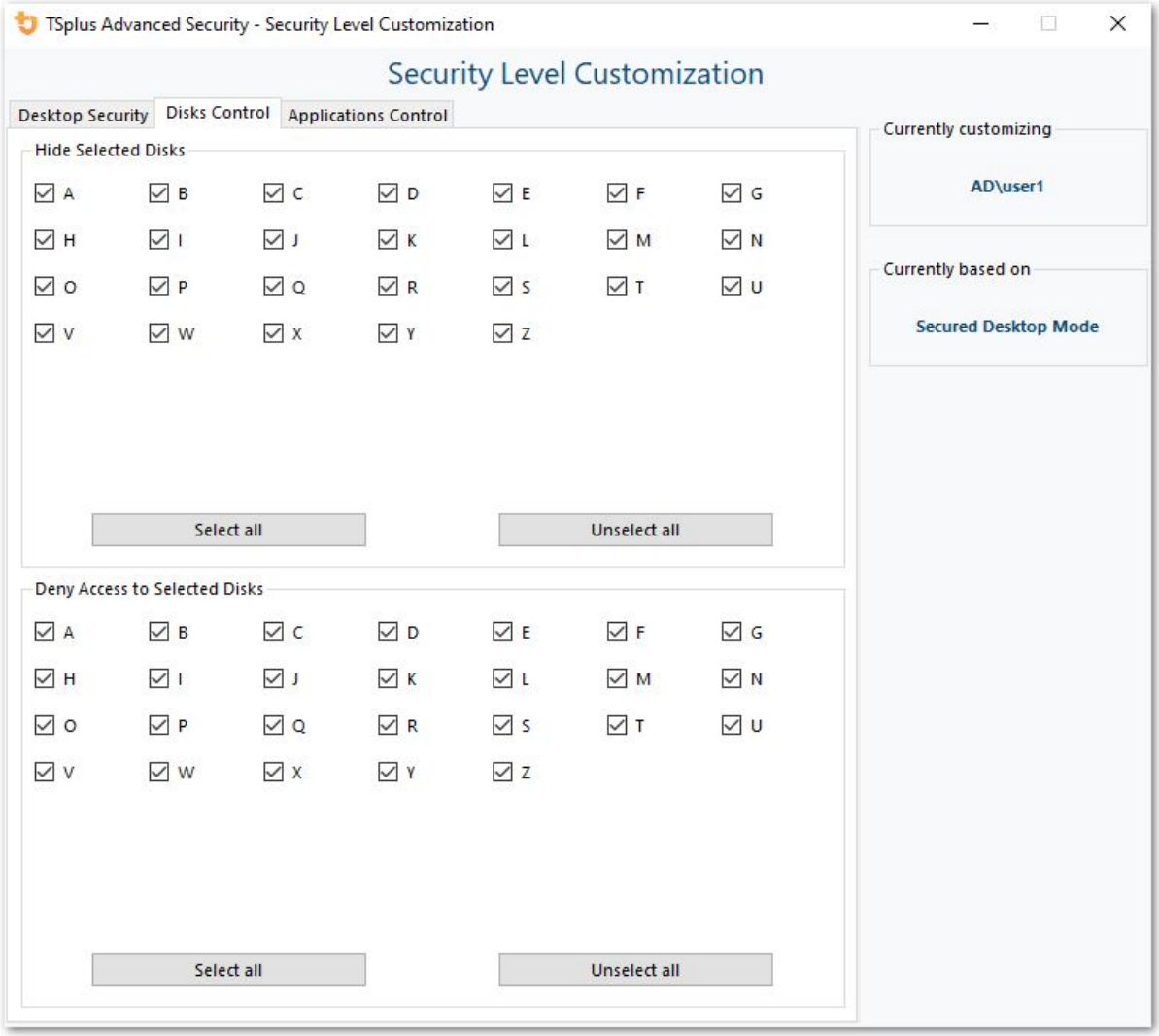
定制化

在任何模式下，您都有可能在三个级别上自定义安全性：

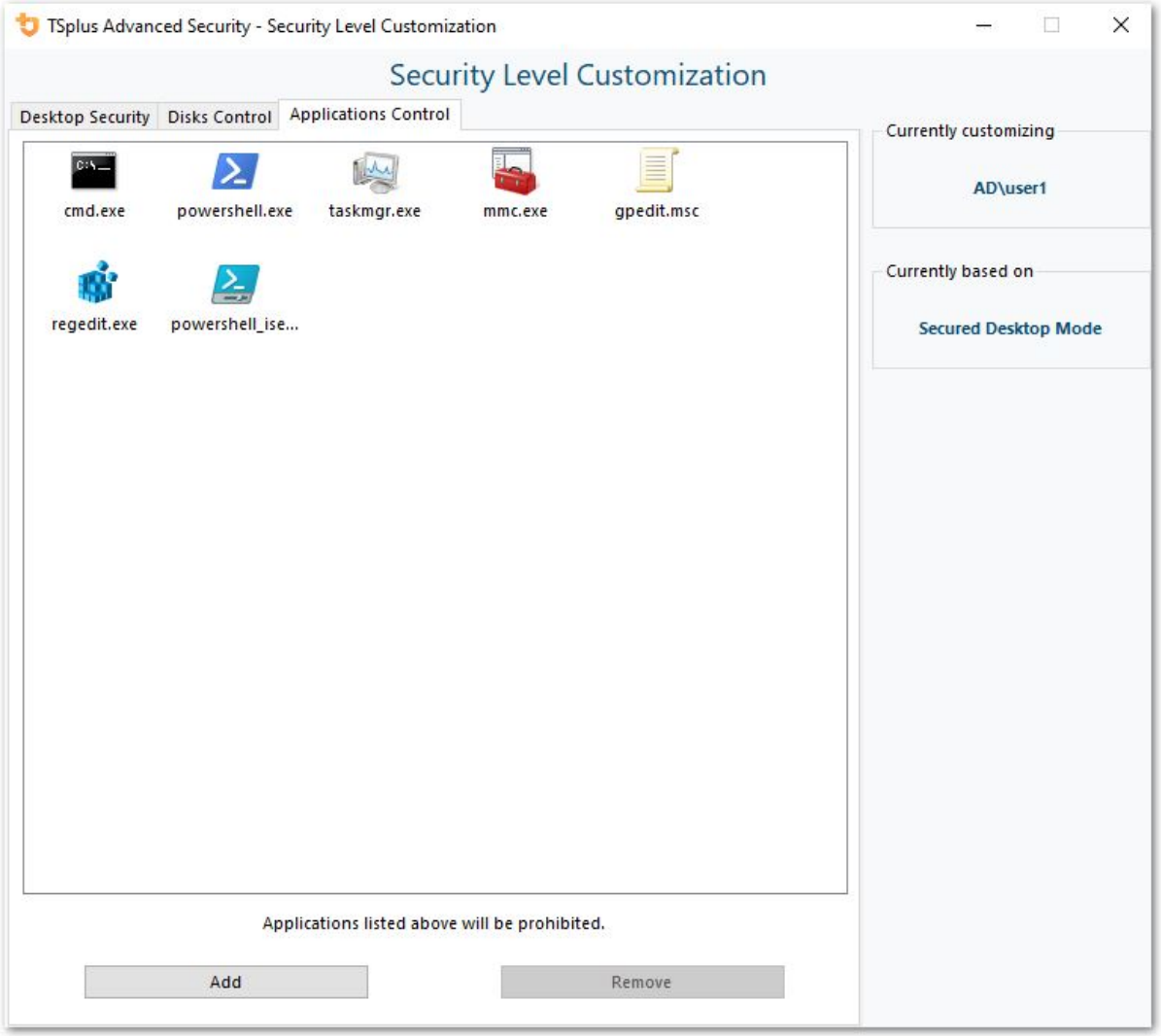
桌面安全：


TSplus Advanced Security - Security Level Customization
Security Level Customization
Desktop Security
Disks Control
Applications Control
Remove Recycle Bin
Remove Quick Access
Remove This PC
Remove My Documents
Remove My Recent Documents
Remove My Music
Remove My Pictures
Remove My Videos
Remove Frequently Used Programs
Remove Programs
Remove Help and Support
Remove Control Panel
Remove Printers
Remove Network
Remove Recent Files
No Network Neighborhood
Remove Context Menu
Restrict right click
Disable System Management programs
Disable Task Manager
Disable Windows key
No Folder options
No Active Desktop
No Disconnect
No Close
No Manage My Computer
No Delete Printer
No Internet Explorer
Currently customizing
AD\user1
Currently based on
Secured Desktop Mode

磁盘控制：


TSplus Advanced Security - Security Level Customization
Security Level Customization
Desktop Security
Disks Control
Applications Control
Hide Selected Disks
A B C D E F G
H I J K L M N
O P Q R S T U
V W X Y Z
Select all
Unselect all
Deny Access to Selected Disks
A B C D E F G
H I J K L M N
O P Q R S T U
V W X Y Z
Select all
Unselect all
Currently customizing
AD\user1
Currently based on
Secured Desktop Mode

应用程序控制：



用户/组规则优先级

当用户在服务器上打开新会话时：

1. 如果该用户为自己直接定义了安全级别，则将强制执行该安全级别。
2. 如果该用户没有为自己直接定义安全级别，则 TSplus Advanced Security 将加载该用户所有组的任何现有安全级别设置，并保留更宽松的规则。

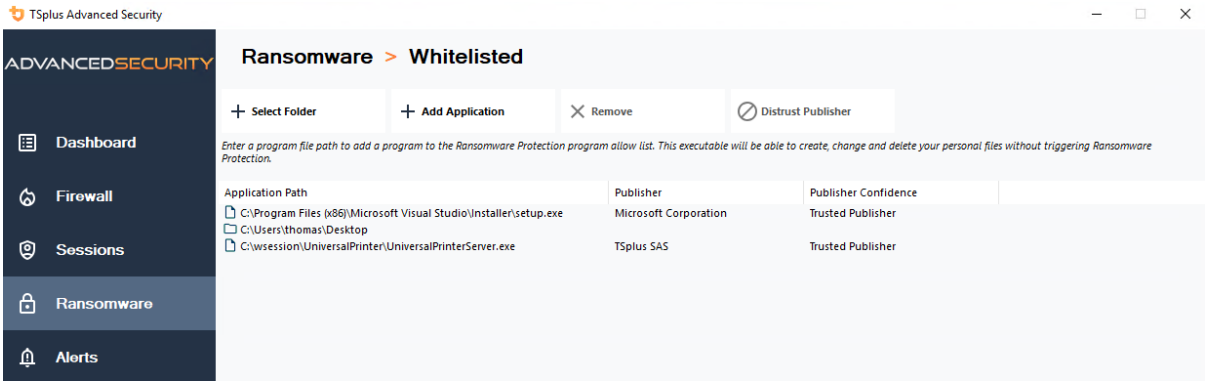
例如，如果第一个组有一个规则来从桌面上删除回收站图标，但该规则对第二个组被禁用，那么用户将在其桌面上看到回收站图标。相同的优先级规则将适用于每个自定义规则（桌面安全、磁盘控制和应用程序控制），以及主要安全级别（Windows模式被认为比安全桌面模式更宽松，而安全桌面模式又被认为比亭模式更宽松）。

请注意：为了在任何地方禁用右键单击，您必须选择以下两个选项：

- 限制右键点击
- 移除上下文菜单

设置 - 程序允许列表

在 **程序选项卡** 你可以 将程序添加到允许程序列表中，这些程序将不会被TSplus Advanced Security的Ransomware Protection检查。 默认情况下，所有 Microsoft 程序都在白名单中。



点击“添加应用程序”按钮以添加程序。您也可以通过选择应用程序并点击“移除应用程序”按钮来删除它们。

设置 - 用户允许列表

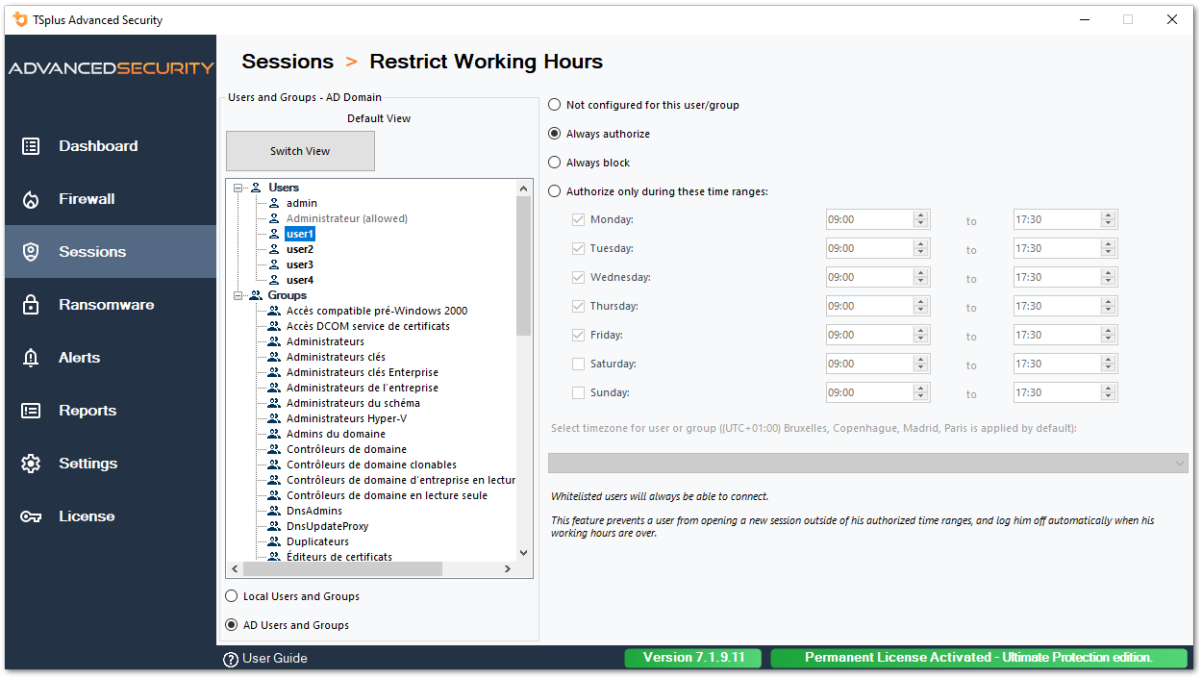
高级视图

使用高级视图，从所有可访问的域中添加和管理用户和组。

您可以使用“切换视图”按钮将视图从默认视图切换到高级视图。

高级视图用于显示和管理当前配置的每个用户和组。它还允许您将新用户和组添加到列表中以进行配置，使用 Windows AD 搜索选择器。您可以通过单击“添加用户/组”按钮来实现。然后，您将能够从服务器上任何可访问的域中添加任何可用用户。

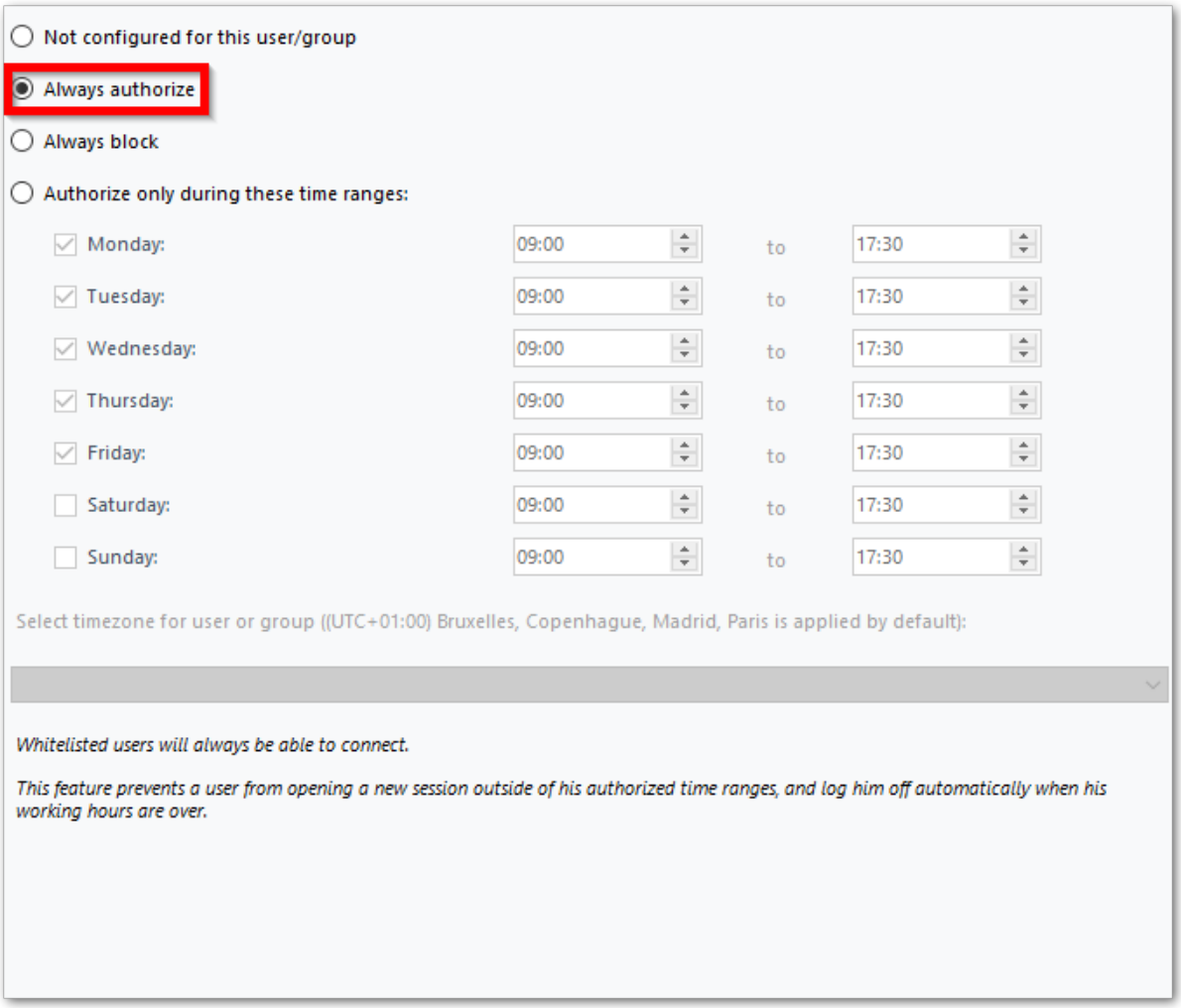
高级视图可用于权限、工作时间、安全桌面功能。示例：



这 **用户白名单** 选项卡使管理员能够 添加/移除用户到白名单 .

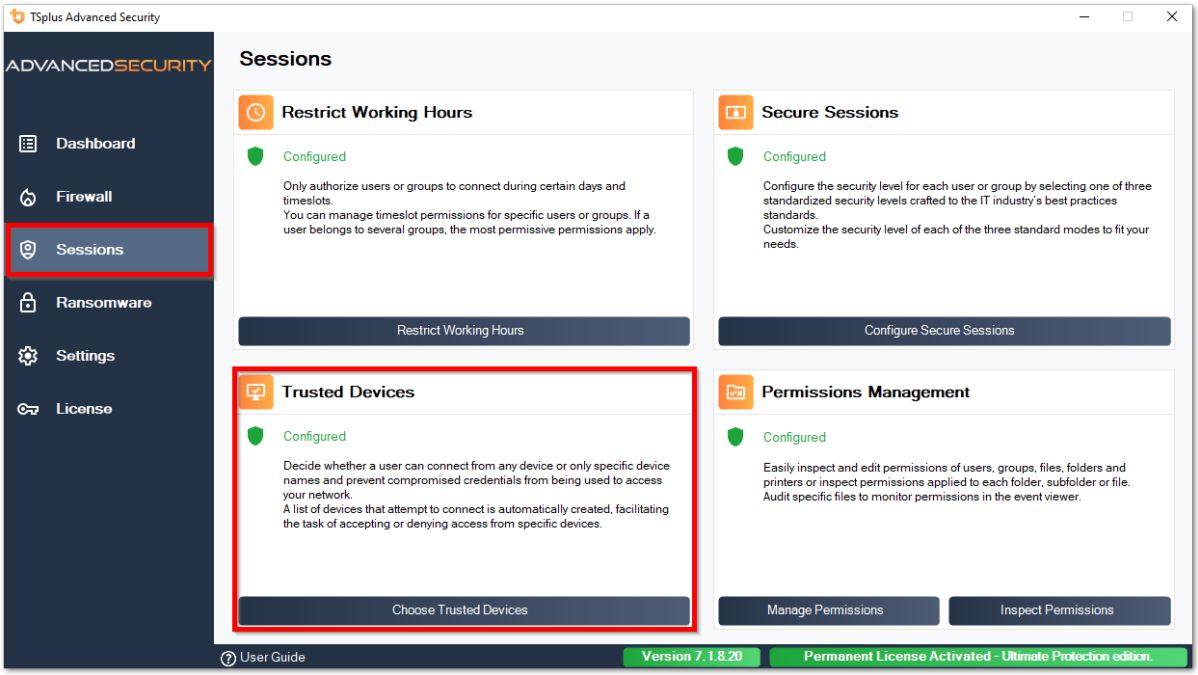
在白名单上的用户将被 TSplus Advanced Security 忽略，他们的设置将不被应用。

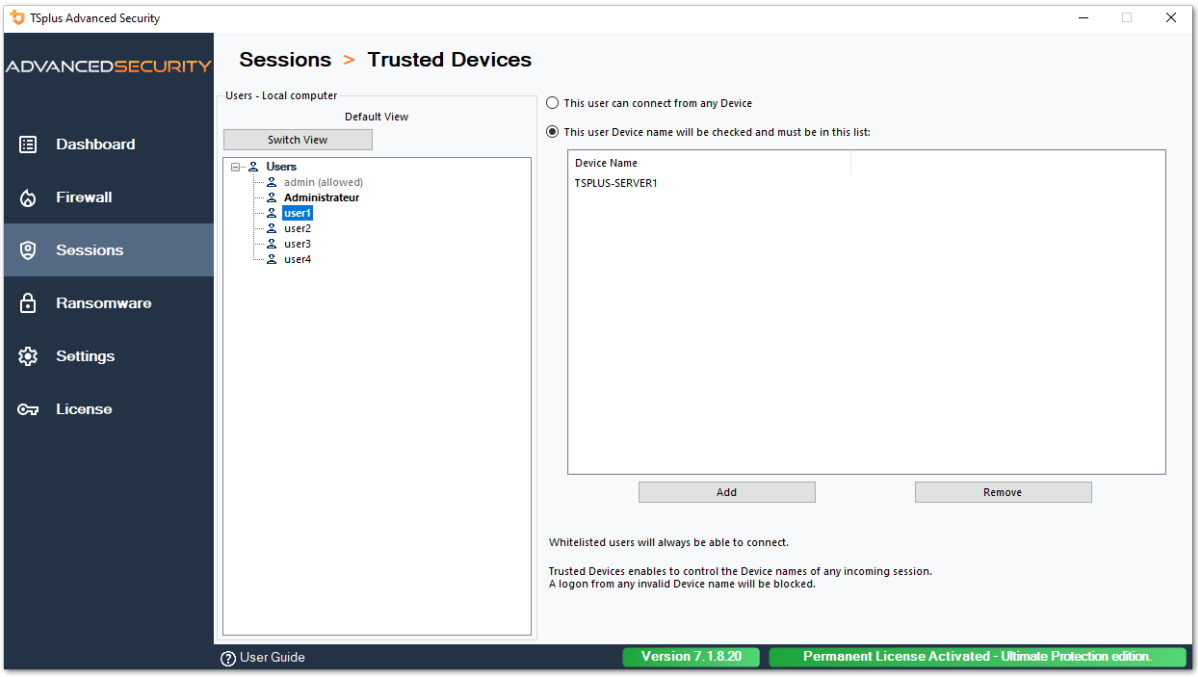
安装了 TSplus Advanced Security 的用户会自动添加到白名单中：


Not configured for this user/group
Always authorize
Always block
Authorize only during these time ranges:
Monday: 09:00 to 17:30
Tuesday: 09:00 to 17:30
Wednesday: 09:00 to 17:30
Thursday: 09:00 to 17:30
Friday: 09:00 to 17:30
Saturday: 09:00 to 17:30
Sunday: 09:00 to 17:30
Select timezone for user or group ((UTC+01:00) Bruxelles, Copenhague, Madrid, Paris is applied by default):
Whitelisted users will always be able to connect.
This feature prevents a user from opening a new session outside of his authorized time ranges, and log him off automatically when his working hours are over.

受信任的设备

受信任的设备允许您通过允许每个用户仅使用一个或多个特定设备来控制用户设备，这些设备将在任何传入会话中进行检查。来自任何无效设备名称的登录将被阻止。





在这个例子中， **用户1** 将使用设备名称 **TSPLUS-SERVER1** 仅。

设备名称字段的自动填充

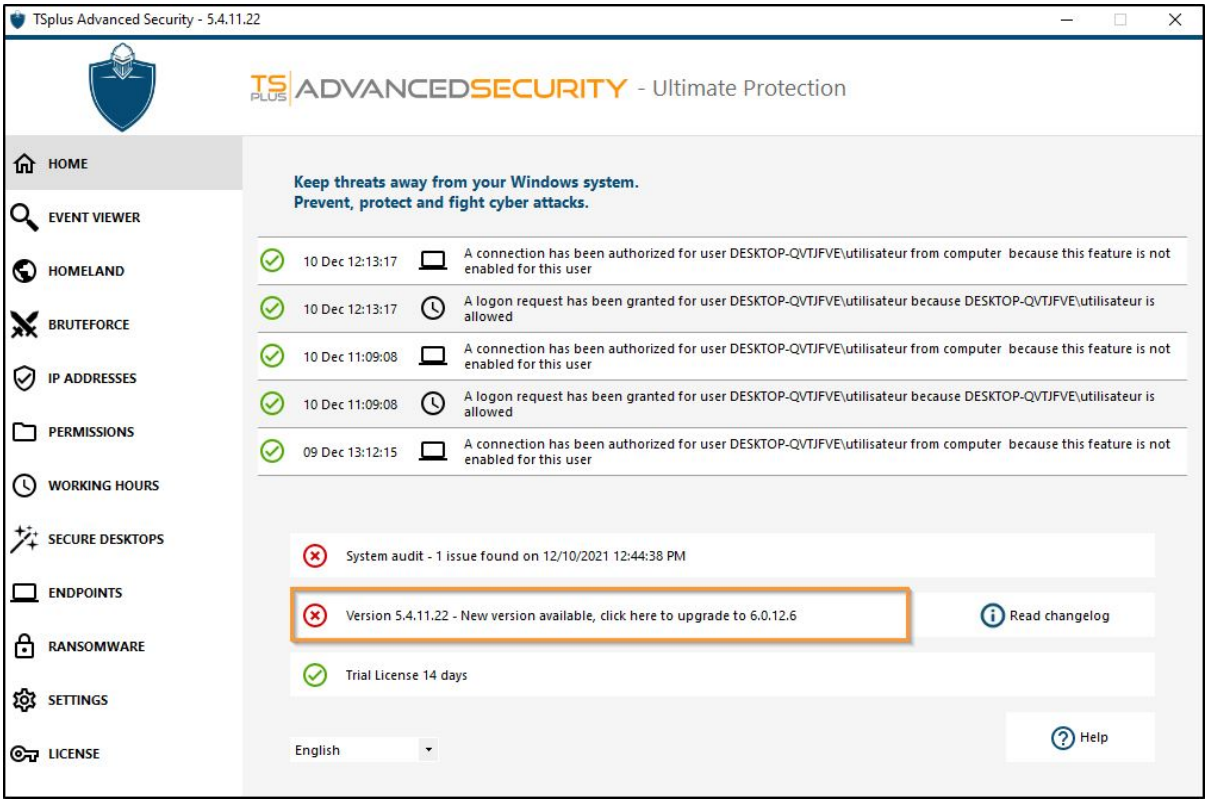
您可能会注意到，对于某些用户，设备名称字段已经填写了设备名称。为了帮助管理员，TSplus Advanced Security 将自动保存任何未启用受信任设备功能的用户连接到服务器时使用的最新设备名称。在一个工作日后，大多数用户的设备名称将被 advanced-security 知道，从而允许您快速启用端点保护功能，而无需检查每个用户的工作站名称。

注意 受信任的设备与HTML5连接不兼容。

更新 TSplus 高级安全性

查看我们的修复和改进，点击此处 更新日志

更新 TSplus 高级安全性很简单，只需点击主页上的相应图块即可：



然后，TSplus Advanced Security 下载并应用更新。

注意： 您的数据和设置在更新之前始终备份，并可以在“archives”目录中找到，位于TSplus Advanced Security设置文件夹中。 备份和恢复您的数据和设置

限制工作时间

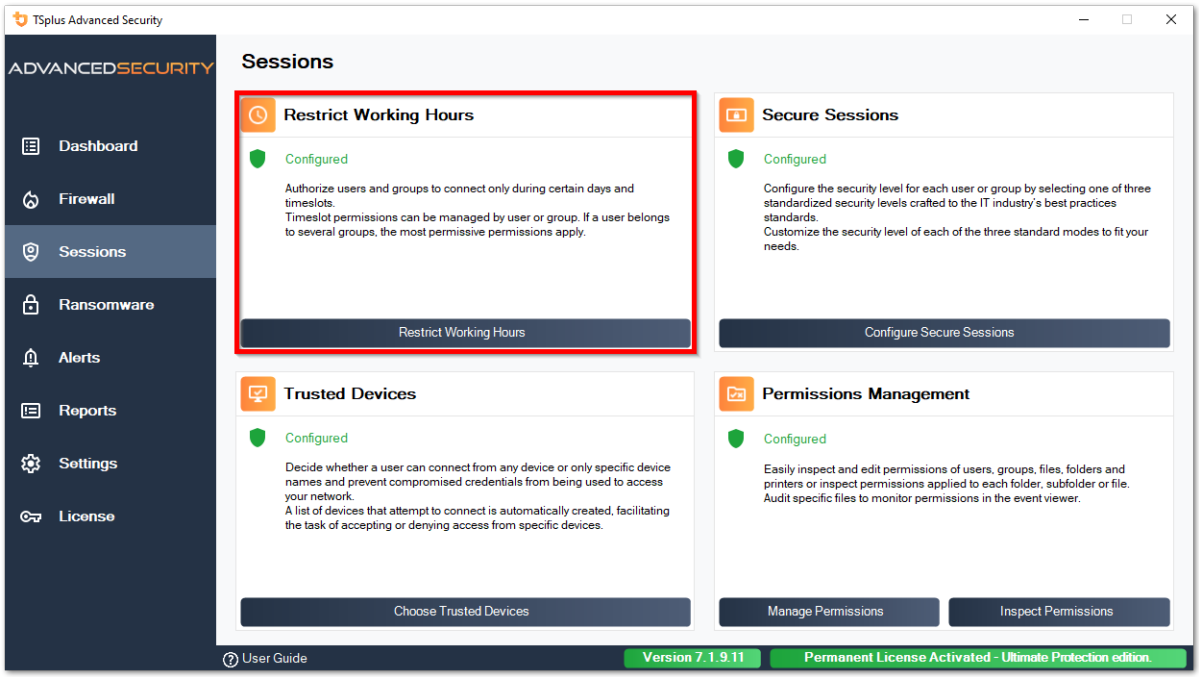
您可以为每个用户或每个组配置工作时间限制。

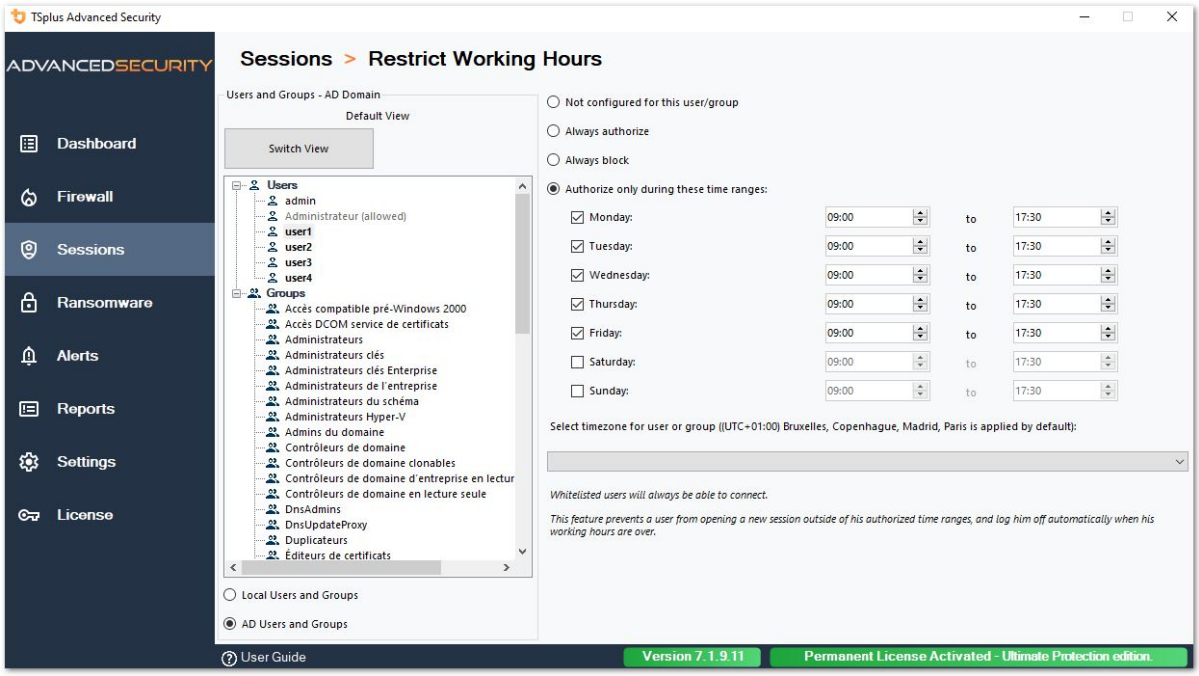
选择您选择的限制：

- 始终授权此用户/组访问
- 始终阻止该用户/组访问

或仅在特定时间范围内授权。

您可以逐日配置并选择您偏好的时间范围：





可以根据用户的办公室位置选择特定的时区。

在配置的工作时间结束时会自动断开连接。

在用户注销之前，可以安排警告消息。 设置 > 高级 > 工作时间 .

###用户/组规则优先级

当用户在服务器上打开新会话时：

1. 如果该用户为自己直接定义了工作时间限制，则这些规则将被执行。

2. 如果该用户没有直接为自己定义工作时间限制，则TSplus高级安全性将加载该用户所有组的任何现有工作时间限制，并保留更宽松的规则。例如，如果第一个组有一个在星期一阻止连接的规则，第二个组有一个在星期一上午9点到下午5点授权连接的规则，第三个组有一个在星期一上午8点到下午3点授权连接的规则，则该用户将能够在星期一上午8点到下午5点之间打开连接。

警告：此功能使用服务器的时间。使用用户的工作站时间和/或时区是没有意义的，因为用户只需更改其时区即可在授权时间之外打开会话。