

RDS-Knight Documentation





Quick Start

Just installed RDS-Knight? [Get Started!](#)
See [RDS-Knight Changelog](#).

Documentation

Planning and Managing RDS-Knight

- [Pre-requisites](#)
- [Installation](#)
- [Activating your license](#)
- [Updating RDS-Knight](#)
- [System Audit](#)

Using RDS-Knight

- [User Interface Overview](#)
- [Events Viewer](#)
- [Restrict access from other countries](#)
- [Protect your server against brute-force attacks](#)
- [IP Addresses](#)
- [Permissions](#)
- [Restrict connection hours](#)
- [Security Level](#)
- [Endpoint Protection and Device Control](#)
- [Ransomware Protection](#)
- [Settings](#)



Get Started with RDS-Knight

Step 1: Installing RDS-Knight on your computer

Installing RDS-Knight is an easy process.

Just download it from our web site, run the Setup-RDS-Knight.exe and follow the steps detailed here.

Files are decompressed and copied into:

"C:\Program Files (x86)\RDS-Tools\RDS-Knight" folder. The trial version is a full featured version limited to 2 weeks.

After the installation, there will be a new icon on your Desktop:



Step 2: Using RDS-Knight

You can now launch the [RDS-Knight interface](#) and begin to set RDS-Knight security features and prevent your server from both internal and external threats. The dashboard proposes an immediate access to the five last security events. Moreover, the version tile allows administrators to directly update RDS-Knight to the latest version directly from there.

- You can begin by [defining a security level](#) for your group of users, and customize it for a specific user.
- Then, you can set specific [working hours](#) in order for your users to connect only during their working time.
- You can protect your server from foreign cyber-attacks by allowing the access to the countries of your choice, with the [Homeland access protection](#).

Don't forget to [activate your license](#) and to [update to the latest version](#) if you wish to be fully protected by RDS-Knight!

Look at our documentation for all security features [here](#).



Pre-requisites

Hardware Requirements

RDS-Knight can only work on 32 and 64-bit editions of OS servers.

Operating System

RDS-Knight is compatible with the following OS:

- Windows 7 SP2
- Windows 8.1
- Windows 10
- Windows Server 2008 R2
- Windows Server 2012 / 2012 R2
- Windows Server 2016
- Windows Server 2019

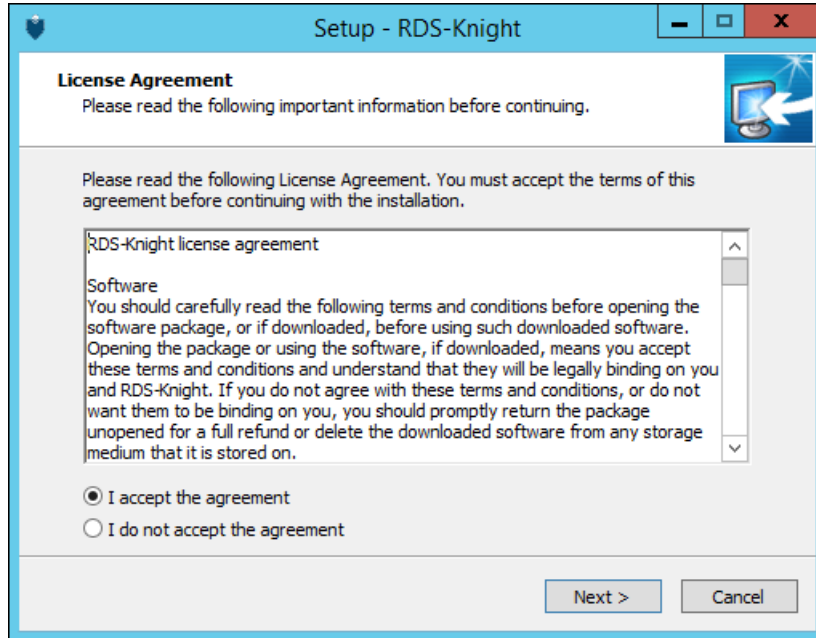
The required framework is .NET version 3.5.



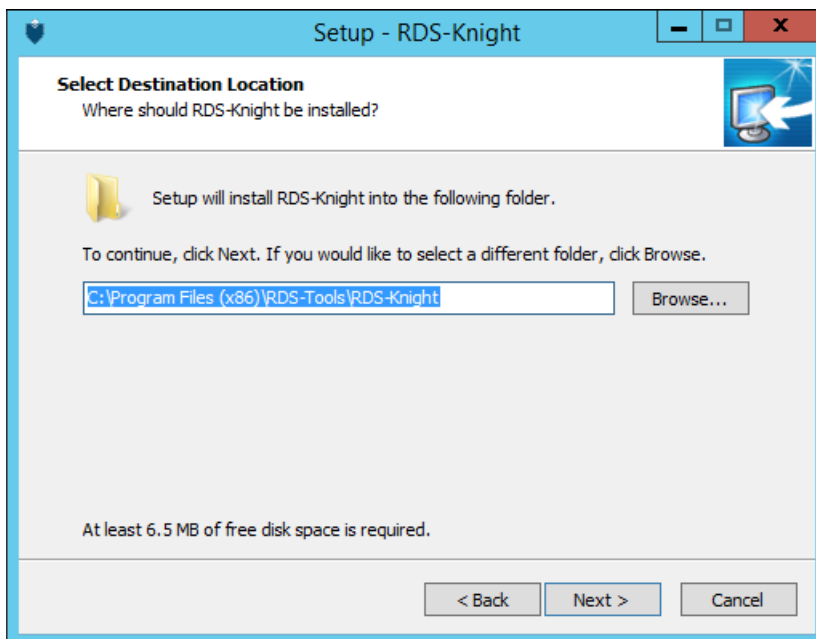
Installation

Run the RDS-Knight setup program and then **follow the installation steps**.

Please note that you must run this Setup as an Administrator, but don't worry, Windows will automatically require it.



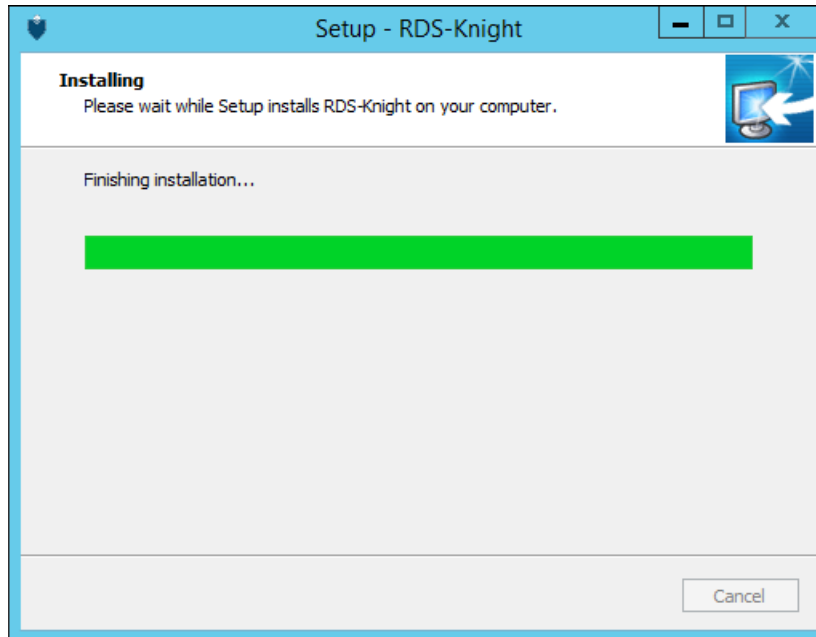
Click on "Next" if you agree to the license.



The Setup is now ready to install RDS-Knight on your computer.

Click on "next" to start the actual installation.

A progress bar is displayed and allows you to follow the installation progress.



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

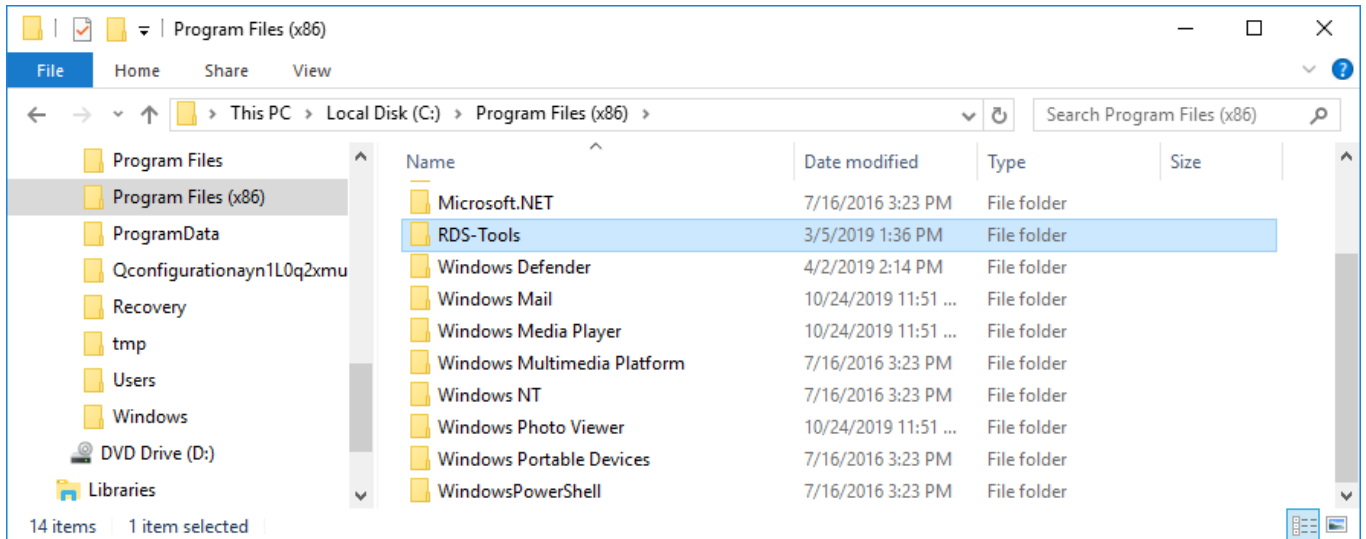


The installation is now finished, you can now start using RDS-Knight!

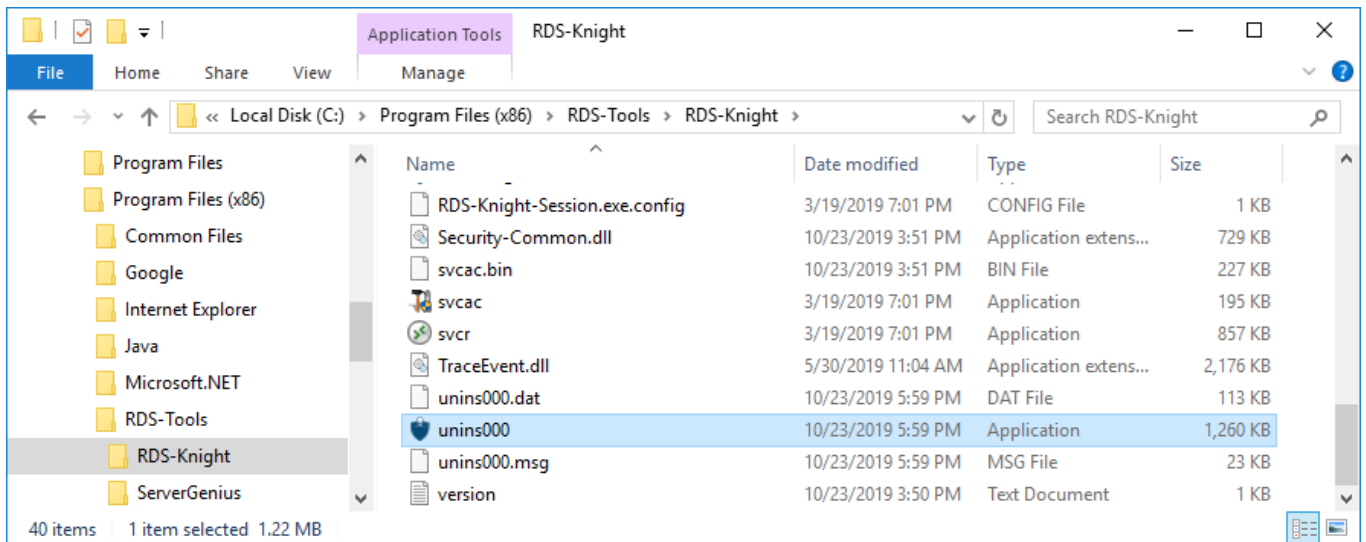
The free trial version is fully featured for 2 weeks.

Uninstall RDS-Knight

In order to completely uninstall RDS-Knight, go to C:\Program Files (x86)\RDS-Tools\RDS-Knight\ :



Then, double-click on the "unins000" application:



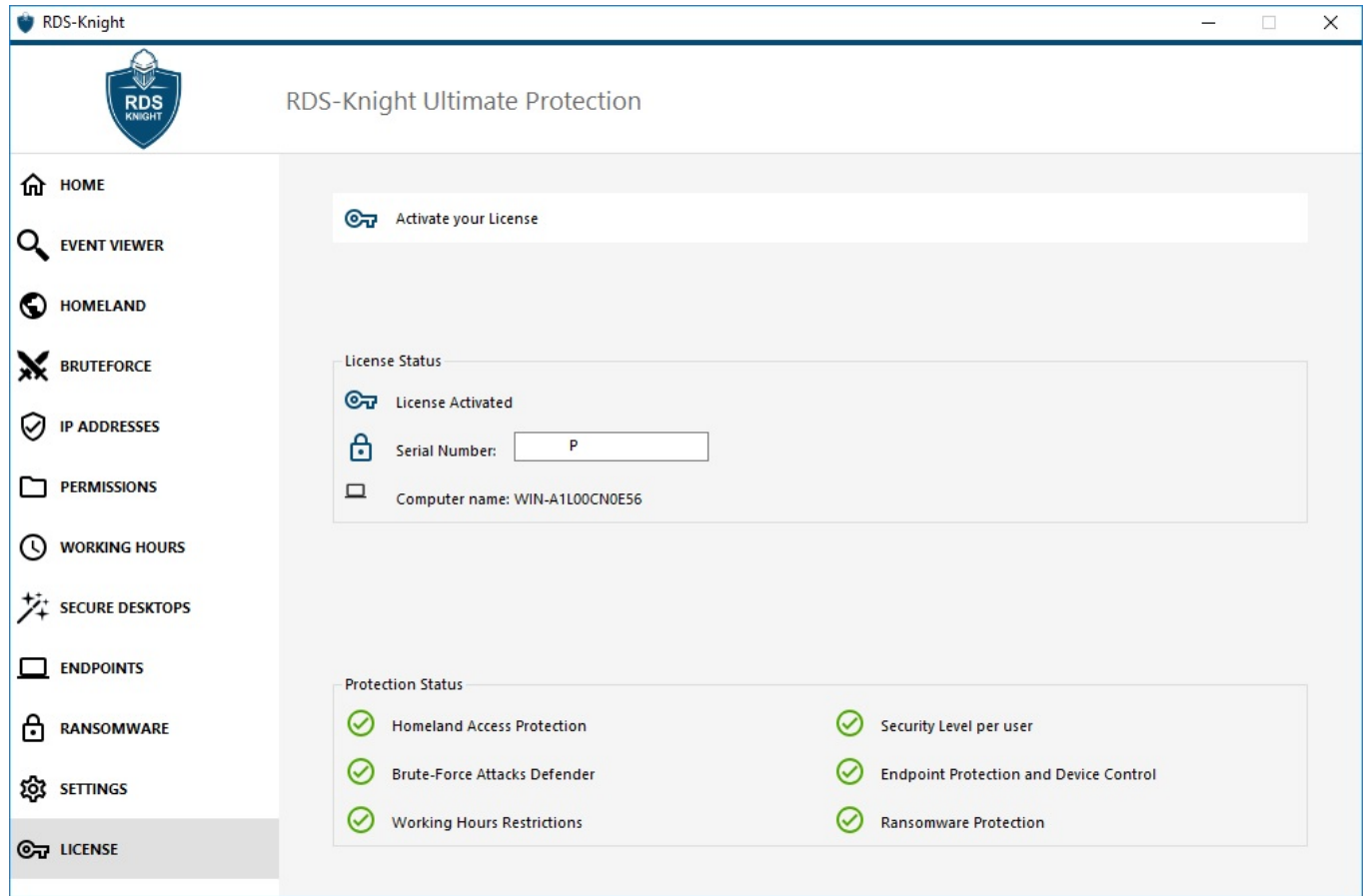
Click on yes on the next window to completely remove RDS-Knight and all of its components.

The software will be completely uninstalled from your machine.

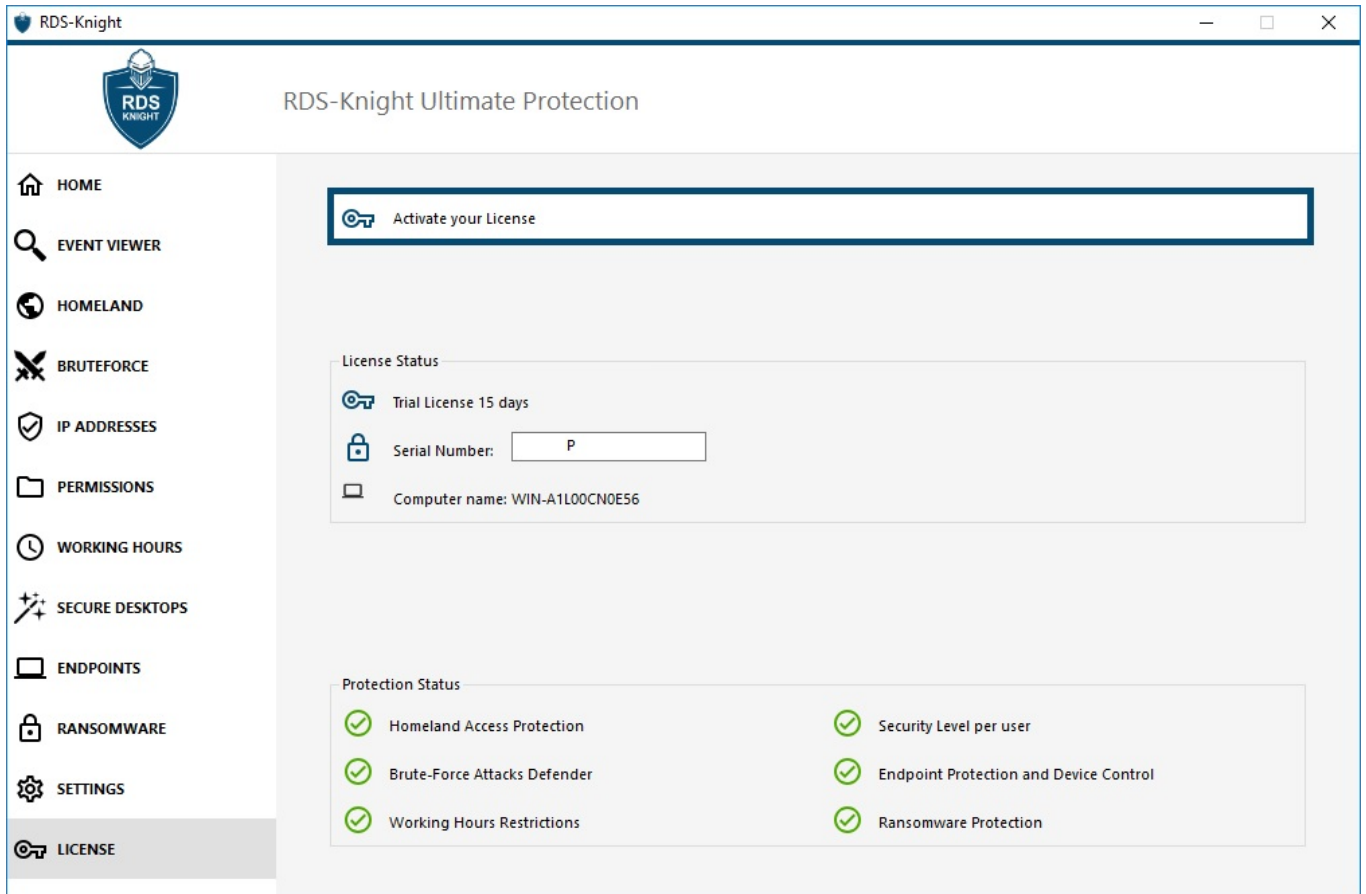


Activating your license

Open the RDS-Knight interface and click on the License tab:

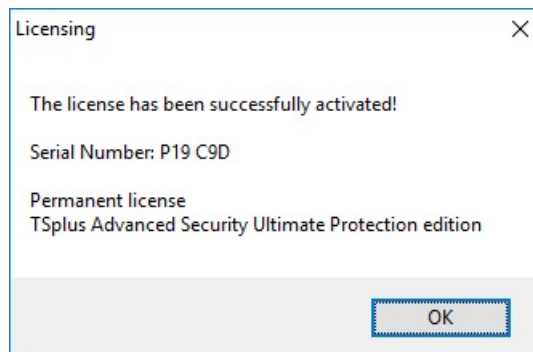


Then, click on the "Activate your License" button:



Click on the "Activate License" button, and select the license.lic file you have been given by your reseller or the license.lic file that you have downloaded from our [Licensing Web Portal](#).

When your license is activated, the following confirmation message will be displayed:



From now on, your License window will look like the one below, to confirm that you have indeed an activated license:



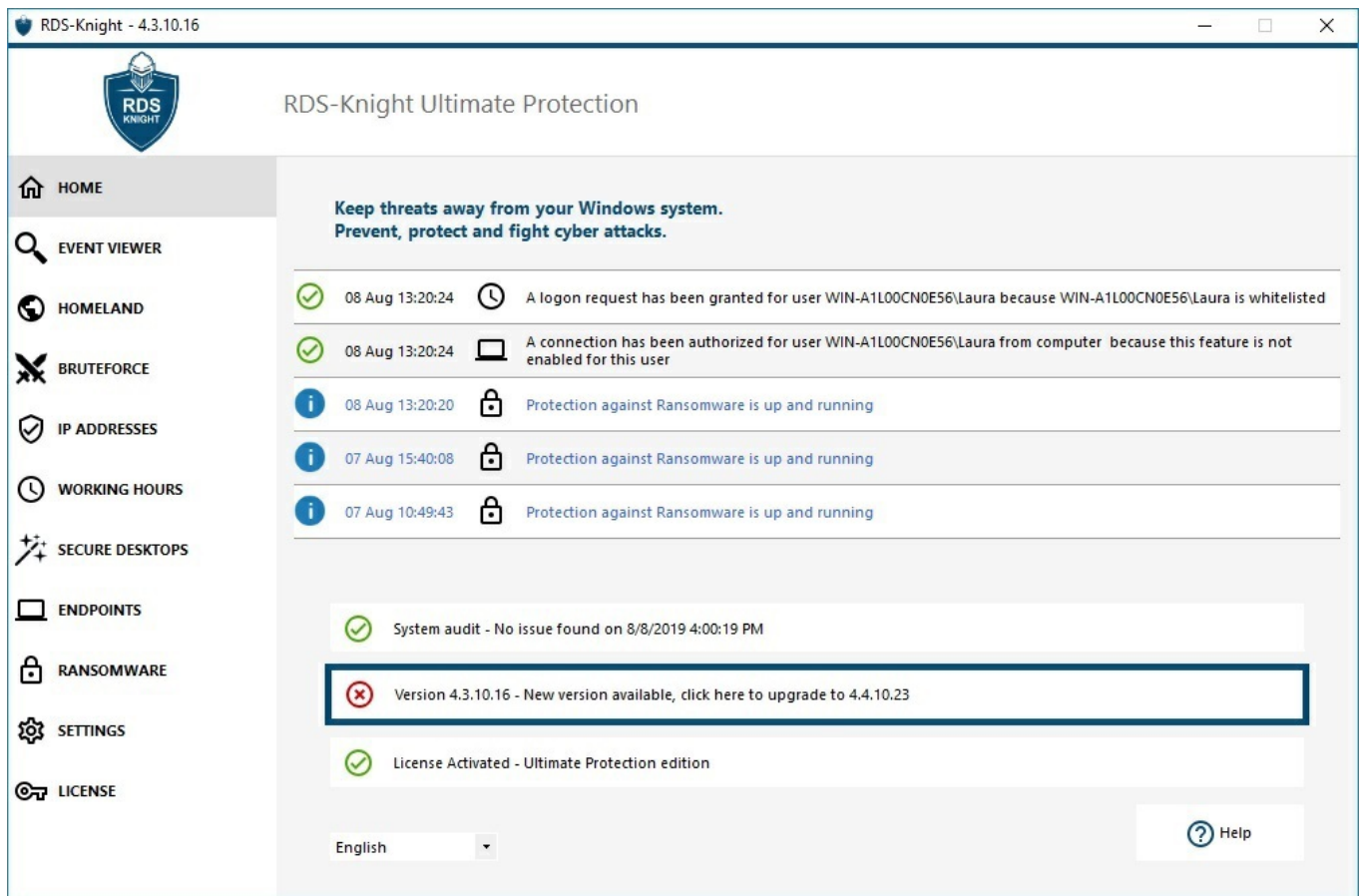
The screenshot displays the RDS-Knight Ultimate Protection web interface. On the left is a navigation sidebar with icons and labels for: HOME, EVENT VIEWER, HOMELAND, BRUTEFORCE, IP ADDRESSES, PERMISSIONS, WORKING HOURS, SECURE DESKTOPS, ENDPOINTS, RANSOMWARE, SETTINGS, and LICENSE (which is highlighted). The main content area is titled "RDS-Knight Ultimate Protection" and contains a "License Status" section. At the top of this section is a button labeled "Activate your License". Below it, the "License Status" is shown as "License Activated" with a key icon, which is highlighted by a blue box. Underneath, the "Serial Number" is displayed as "P" and the "Computer name" is "WIN-A1L00CN0E56". A "Protection Status" section below shows six features, each with a green checkmark icon: Homeland Access Protection, Security Level per user, Brute-Force Attacks Defender, Endpoint Protection and Device Control, Working Hours Restrictions, and Ransomware Protection.

Thank you for choosing RDS-Knight!



Updating RDS-Knight

Updating RDS-Knight is easy and can be done by clicking on the corresponding tile, on the Home Dashboard:



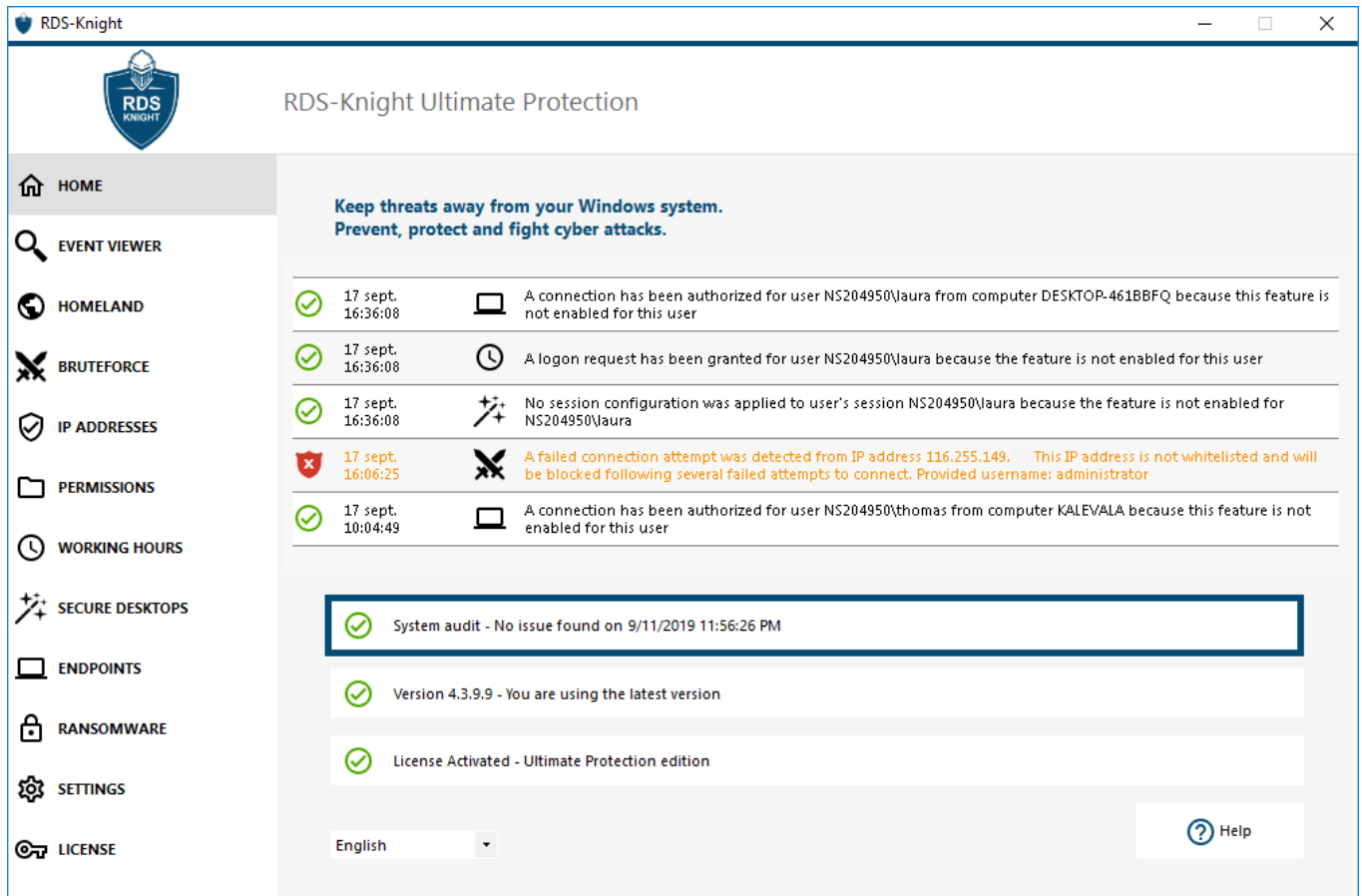
RDS-Knight automatically downloads and applies Update Release program when requested.

The Update Release program is designed to continuously improve all RDS-Knight functionalities and keep your current RDS-Knight settings safe.



System Audit

RDS-Knight offers a System Audit located on the AdminTool dashboard. The tick on the System Audit button turns red when an issue has been found.



When you click on it, you can see that it monitors :

- If the RDS-Knight service is running.
- If you allowed RDS-Knight to access Internet to check for updates.
- If RDS-Knight main programs exist.
- If the Windows Firewall is enabled.
- If the Logging is disabled in production use.
- If the Windows minimum password length is greater than zero.
- If the Guest account is disabled.



RDS-Knight - System audit

- ✓ Success - Service RDS-Knight should be running
- ✓ Success - You should allow RDS-Knight to access Internet to check for updates
- ✓ Success - RDS-Knight main programs should all exist
- ✓ Success - Windows Firewall should be enabled
- ✓ Success - Logging should be disabled in production use
- ✓ Success - Minimum Password Length must be greater than zero
- ✓ Success - Guest account should be disabled

System audit - Latest check on 9/17/2019 11:09:35 AM

Run system audit

Warnings

If you see the Windows password length error, like on the screenshot below:

RDS-Knight - System audit

- ✓ Success - Service RDS-Knight should be running
- ✓ Success - You should allow RDS-Knight to access Internet to check for updates
- ✓ Success - RDS-Knight main programs should all exist
- ✓ Success - Windows Firewall should be enabled
- ✓ Success - Logging should be disabled in production use
- ⚠ Warning - Minimum Password Length must be greater than zero
- ✓ Success - Guest account should be disabled

System audit - Latest check on 9/11/2019 2:45:24 PM

Run system audit

It is because you need to modify the minimum password length on your server, under Local Policy/Account Policies/Password Policy:



The screenshot shows the Windows Local Security Policy console. The left-hand navigation pane is expanded to 'Account Policies' > 'Password Policy'. The right-hand pane displays a list of password-related policies. The 'Minimum password length' policy is highlighted with a red rectangular box, showing its current value as '0 characters'.

Policy	Security Setting
Enforce password history	0 passwords remembered
Maximum password age	0
Minimum password age	0 days
Minimum password length	0 characters
Password must meet complexity requirements	Enabled
Store passwords using reversible encryption	Disabled



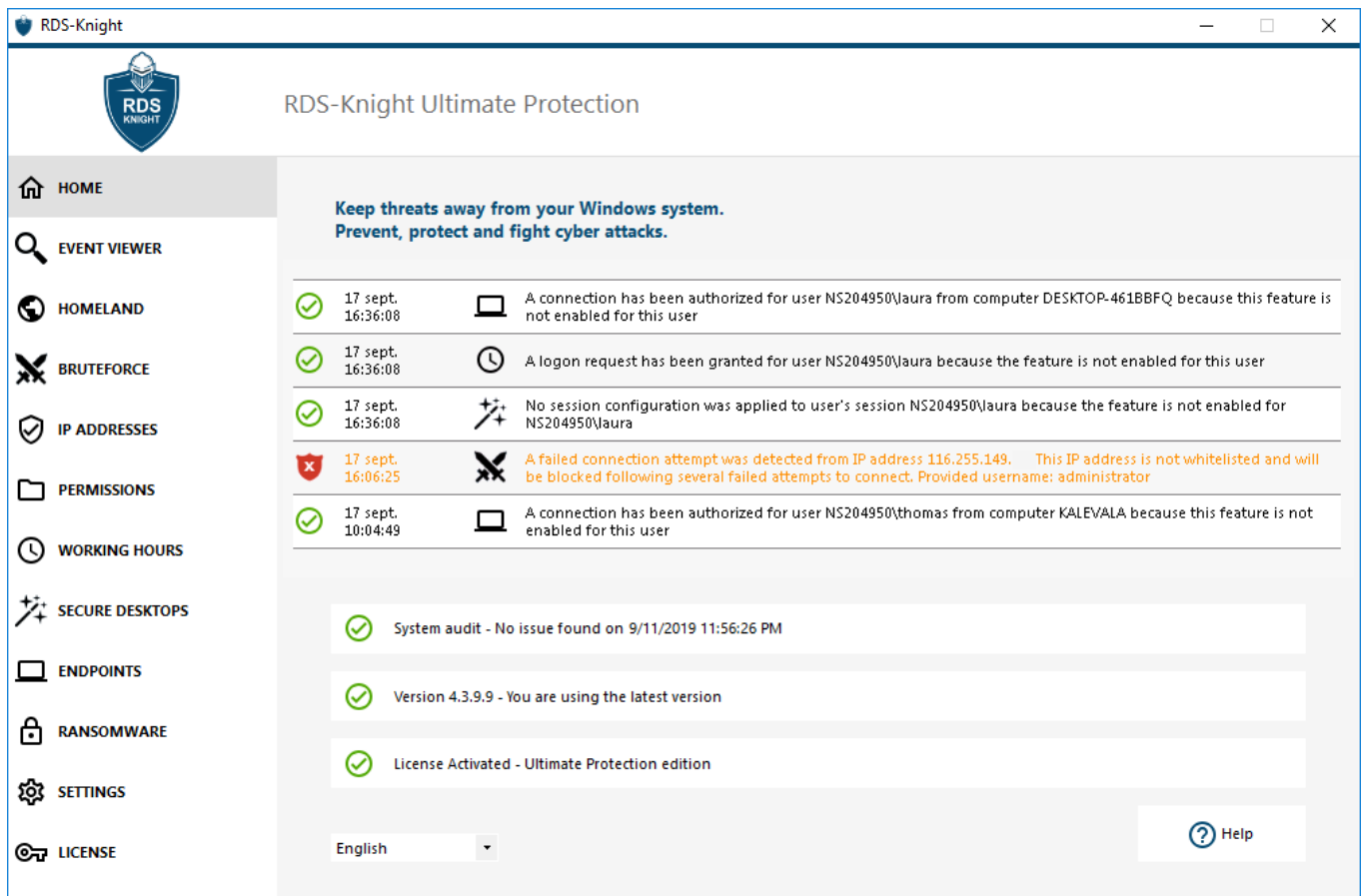
User Interface Overview

Overview

To launch the RDS-Knight interface, just click on the RDS-Knight **AdminTool icon** on your desktop:



There are several tiles on the main window, each tile giving you access to the various features and settings offered by RDS-Knight. The Dashboard proposes an immediate access to the **five last Security Events**. Moreover, the version tile allows administrators to directly run a System Audit and [update RDS-Knight](#) to the latest version directly from there.



Click on each tile to know more about each feature.



Events viewer

RDS-Knight is not a security audit solution. However, we pushed further the security events logs by allowing to trace the last two thousand and five hundred events, which should offer a more relevant alternative to a full audit solution.

The security events are a great source of information as they display the operations performed by RDS-Knight to protect your computer.

The Events Viewer window can be opened from the RDS-Knight main window, by clicking directly on the last 5 events displayed or on the Events tab. The information displayed on the Events Viewer window are refreshed automatically every few seconds.

Date	Feature	Message
08 Mar 12:02:18		A failed login attempt was detected from Web portal for user NS204950\BENJAMIN. 1 failed login attempts were detected for this user since 08 Mar 11:02:18.
08 Mar 12:01:14		A remote connection has been authorized from IP address 62.210. because 62.210.99.241 is associated with the authorized country France
08 Mar 11:58:33		A failed login attempt was detected from Web portal for user NS204950\BENJAMIN. 1 failed login attempts were detected for this user since 08 Mar 10:58:33.
08 Mar 11:48:40		A failed login attempt was detected from Web portal for user NS204950\BENJAMIN. 1 failed login attempts were detected for this user since 08 Mar 10:48:40.
08 Mar 11:45:28		A remote connection has been denied from IP address 125.212. because 125.212. is associated with the unauthorized country Vietnam
08 Mar 11:37:05		A failed login attempt was detected from Web portal for user NS204950\BENJAMIN. 1 failed login attempts were detected for this user since 08 Mar 10:37:05.
08 Mar 11:35:58		A logon request has been granted for user NS204950\benjamin because the feature is not enabled for this user
08 Mar 11:35:58		A connection has been authorized for user NS204950\benjamin from computer DESKTOP-L6QS37C because this feature is not enabled for this user
08 Mar 11:35:58		No session configuration was applied to user's session NS204950\benjamin because the feature is not enabled for NS204950\benjamin
08 Mar 11:35:34		A failed login attempt was detected from Web portal for user NS204950\BENJAMIN. 1 failed login attempts were detected for this user since 08 Mar 10:35:34.
08 Mar 11:31:48		A failed connection attempt was detected from IP address 94.23. This IP address is not whitelisted and will be blocked following several failed attempts to connect.
08 Mar 11:31:15		A connection has been authorized for user NS204950\benjamin from computer DESKTOP-L6QS37C because this feature is not enabled for this user

Note that the example above illustrates real life bruteforce attacks attempts managed by RDS-Knight. The description often explains why the action was performed or not.

As illustrated, retaliatory actions are often written in red and highlighted with a red shield icon. The list of security events presents four columns, which describes the severity, the date of the check or performed operation, the associated feature icon and the description.

Note: The RDS-Knight Events Viewer window can be moved around and does not prevent you from using the other RDS-Knight feature.

The five tiles at the top of the window displays a status for each RDS-Knight features.



RDS-Knight - Events Viewer - Events since 23 juil. 08:49:38

Working Hours Restrictions 0 logon attempt denied	Homeland Access Protection 0 remote access denied	One click to Secure Desktops 5 sessions configured	Endpoint Protection and Device This feature is not enabled	Brute-Force Attacks Defender 0 IP address blocked
--	--	---	---	--

In the example above, the *One Click to Secure Desktops* status shows 5 user session configured. Also, the example warn that the *Endpoint Protection and Device Control* feature is not enabled. The status are displayed according to the security events recorded. The window title highlights the oldest security events.

Plus, a deep global search is now available in order to find specific events quickly. It is also possible to copy the event message and the IP Address, unblock an IP address, OR unblock and add to IP Addresses Whitelist by right-clicking on it:

RDS-Knight - Security Event Log - Events since 10 juil. 12:26:00

Working Hours Restrictions 0 logon attempt denied	Homeland Access Protection 471 remote accesses denied since 10 juil. 12:26:27	One click to Secure Desktops 15 sessions configured since 10 juil. 13:00:51	Endpoint Protection and Device This feature is not enabled	Brute-Force Attacks Defender 22 IP addresses blocked since 10 juil. 12:37:23
--	--	--	---	---

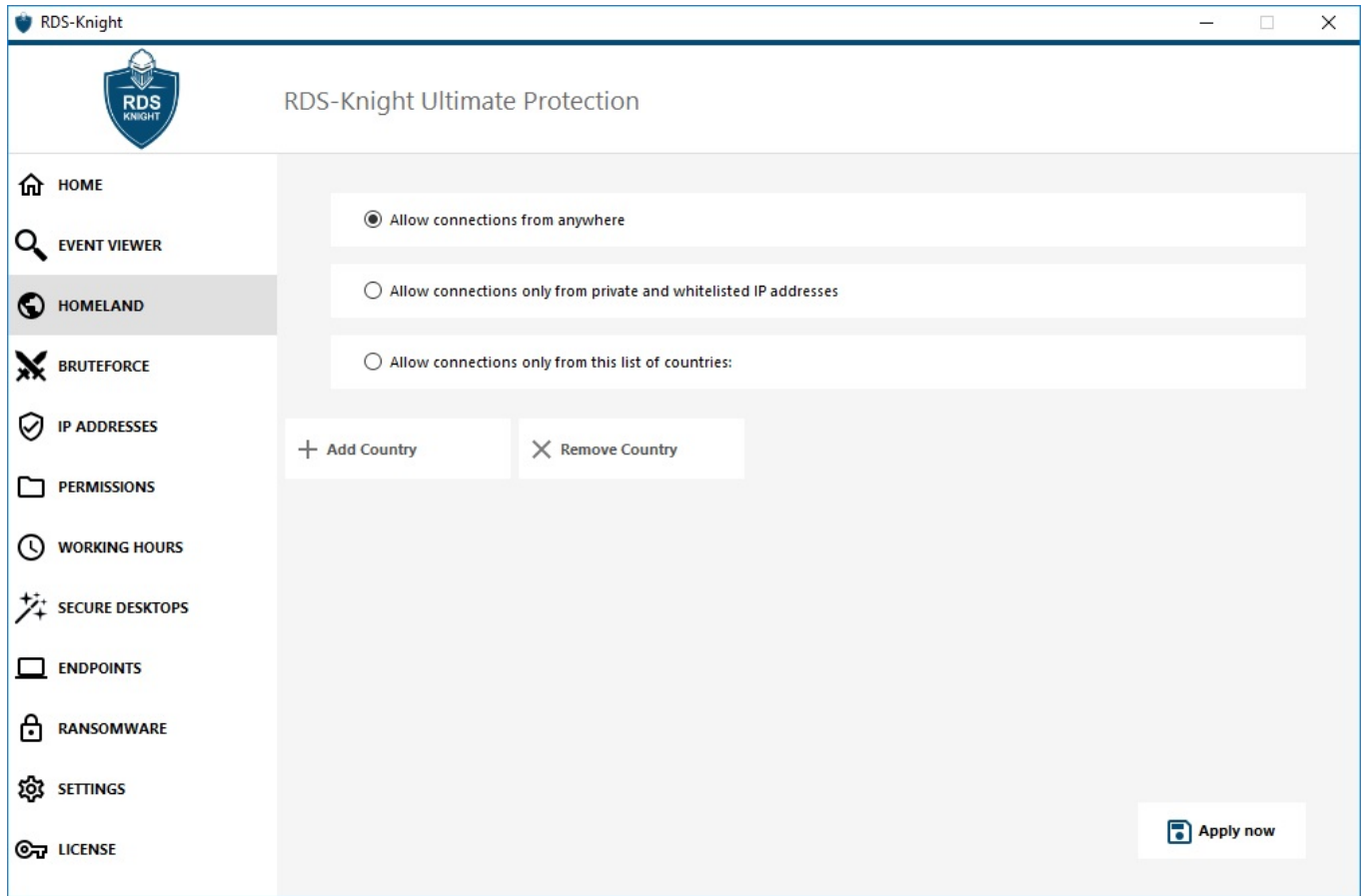
Date	Feature	Message
02 août 04:45:20		A failed connection attempt was detected from IP address 110.77. This IP address is not whitelisted and will be blocked following several failed attempts to connect. Provided username: administrator
02 août 04:45:18		A failed connection attempt was detected from IP address 110.77. This IP address is not whitelisted and will be blocked following several failed attempts to connect. Provided username: administrator
01 août 13:40:01		Next connection attempts from IP address 122.114.26.50 will be denied following several failed attempts to connect. Provided username: administrator
01 août 13:40:00		A failed connection attempt was detected from IP address and will be blocked following several failed attempts to c
01 août 13:39:36		A failed connection attempt was detected from IP address and will be blocked following several failed attempts to c
01 août 13:38:32		A failed connection attempt was detected from IP address 122. This IP address is not whitelisted and will be blocked following several failed attempts to connect. Provided username: administrator
01 août 13:37:56		A failed connection attempt was detected from IP address 122. This IP address is not whitelisted and will be blocked following several failed attempts to connect. Provided username: administrator
01 août 12:21:30		A failed connection attempt was detected from IP address 122. This IP address is not whitelisted and will be blocked following several failed attempts to connect. Provided username: administrator
01 août 11:09:20		A failed connection attempt was detected from IP address 122. This IP address is not whitelisted and will be blocked following several failed attempts to connect. Provided username: administrator

Search



Homeland Access Protection

On this tile, you can allow access for users connecting from all countries by letting this feature by default:



Or decide to restrict the access to only private and [whitelisted IP addresses](#):



The screenshot shows the RDS-Knight Ultimate Protection interface. On the left is a navigation menu with items: HOME, EVENT VIEWER, HOMELAND (highlighted), BRUTEFORCE, IP ADDRESSES, PERMISSIONS, WORKING HOURS, SECURE DESKTOPS, ENDPOINTS, RANSOMWARE, SETTINGS, and LICENSE. The main content area has three radio button options: "Allow connections from anywhere", "Allow connections only from private and whitelisted IP addresses" (selected), and "Allow connections only from this list of countries:". Below these are two buttons: "+ Add Country" and "X Remove Country". An "Apply now" button is in the bottom right corner.

You can allow access only to specific countries by selecting the "Allow connections only from this list of countries" button and by clicking on the "Add country" button:

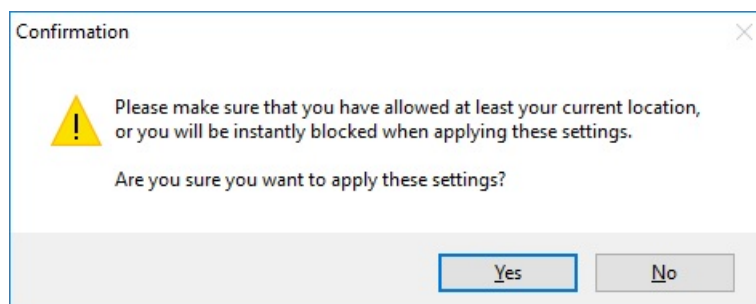
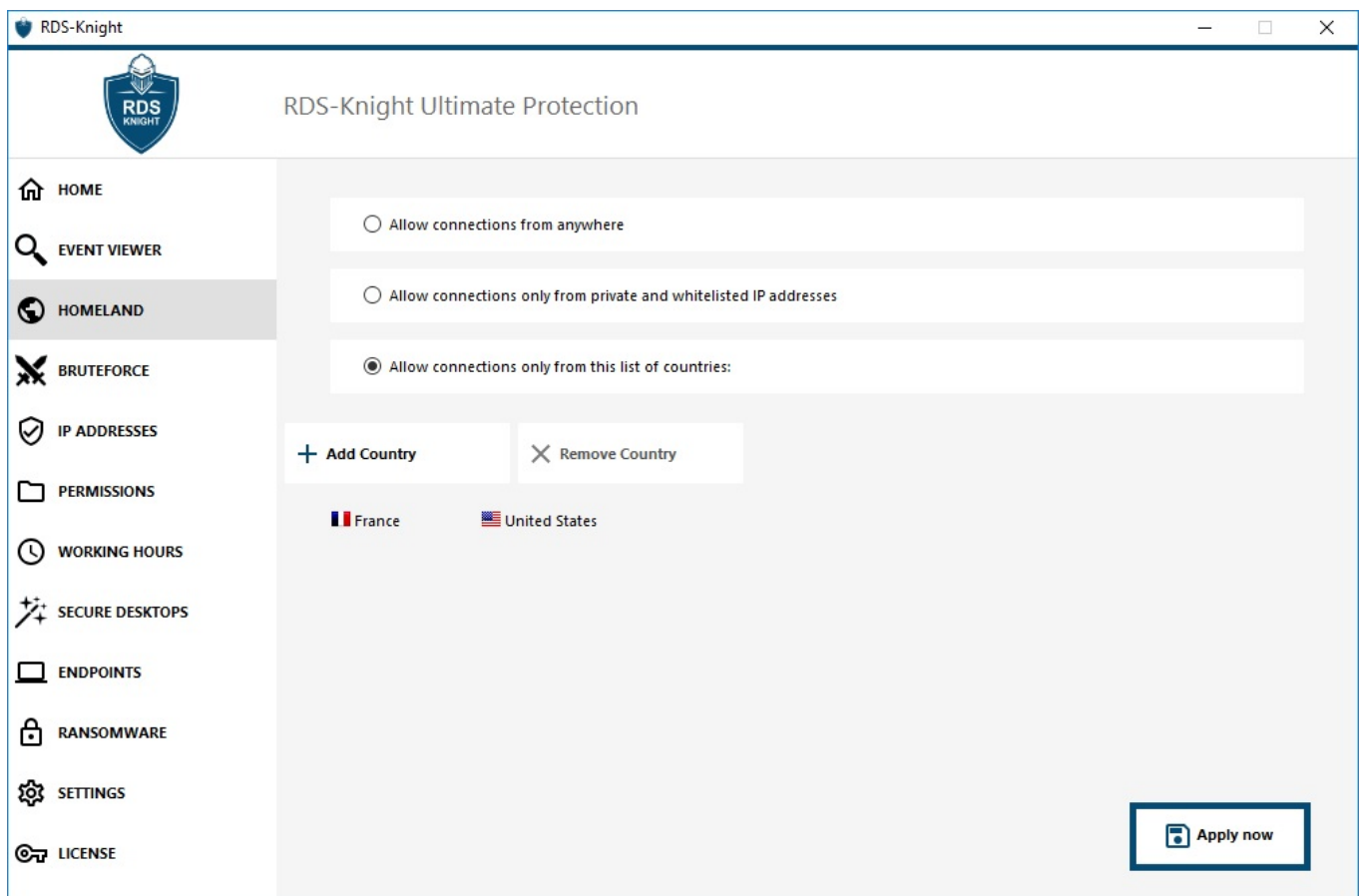
This screenshot is identical to the one above, but the "+ Add Country" button is highlighted with a red rectangular box to indicate the next step in the process.



Select the country you wish to add on the list. (on this example, access is allowed for users connecting from United States, Ireland and France.)

– You also have the choice to check the box below to unblock all IP addresses from the selected country.

When you selected the countries you wish to allow, click on the apply button:



When an IP address gets blocked, it appears on the [Ip Addresses](#) list, and you have the possibility to unblock it.

– By default, the HTML5 service is the watched process. If you wish to disable its monitoring or check connections on other processes, go to the [Settings - Advanced](#) tab.



Warning: please triple-check that you have at least included the country where you are currently connected from. Otherwise, your IP address will be blocked quite quickly after applying the settings, more precisely as soon as a new user session will be opened on the server, thus disconnecting you without any hope of connecting back again from the same IP. If you get blocked, we recommend that you try connecting from any country you allowed on RDS-Knight, for instance by connecting from another remote server. You can also use your console session to fix the settings, as this connection is not using Remote Desktop Services or any non-local network and will not be blocked by RDS-Knight.

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

In order to block an IP address, this feature add 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 to develop these "connectors" for the firewall.

[Contact us.](#)

VPN: In case the remote client uses a VPN, Homeland Access 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 Homeland Access 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 Homeland Access Protection. However, a proxy would definitively change the originating IP address to use a private network address, which will always be allowed by Homeland Access 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.

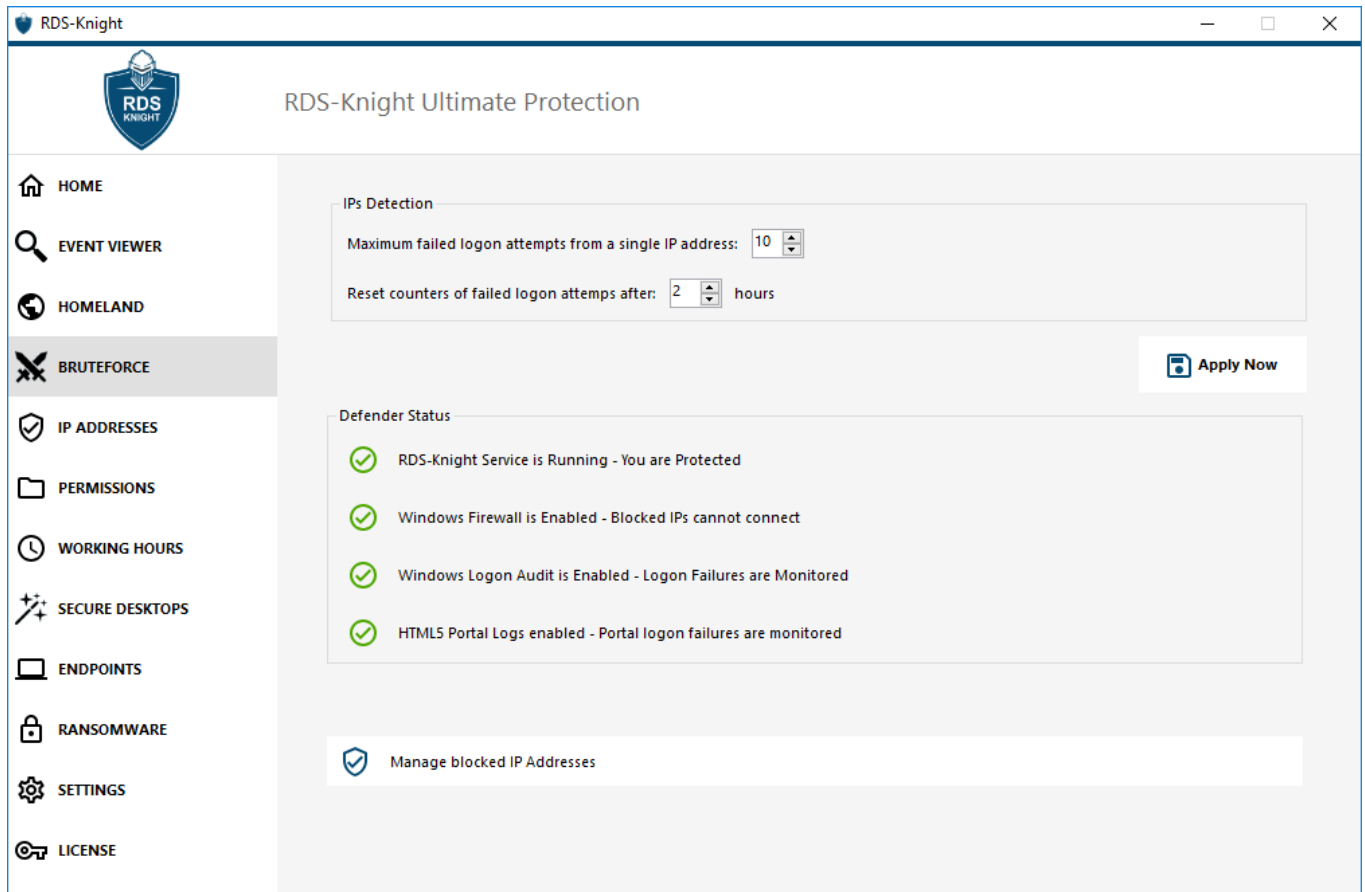
This product includes GeoLite data created by MaxMind, available from <http://www.maxmind.com>. If you find that some IP address is not registered in its real country, please contact MaxMind directly.



Brute-Force Attacks Defender

The Brute-Force Attacks Defender 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.



– 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 RDS-Knight 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 brute-force attacks defender.

– You can **ignore Local and Private IP Addresses** by changing the default setting on the [Settings - Advanced - Brute-force tab](#)

Note: If you ever notice that the Brute-Force Attacks Defender 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 RDS-Knight 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 RDS-Knight, these robots are progressively being blocked, so that one day:

- Most of the active robots are already blocked and are not interested by the server, even the new ones.
- Also, the server does not appear anymore on the list of publicly known servers.



IP Addresses

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

RDS-Knight Ultimate Protection

[+ Add IP Address](#) [Edit IP Address](#) [Remove IP Address\(es\)](#) [WHOIS](#)

IPs in the whitelist will be ignored by RDS-Knight and will not be blocked by Homeland Access Protection or Bruteforce Attacks Defender features.

7 IP address(es) blocked

IP Address	Status	Date	Description
93.184.221.240	Blocked - Homeland Protection	23 Oct 2019 18:06:05	
95.101.180.88	Blocked - Homeland Protection	23 Oct 2019 18:05:34	
192.168.133.12	Whitelisted	23 Oct 2019 17:59:54	localhost
125.212.233.172	Blocked from RDS-Knight	13 Mar 2019 19:35:02	
127.0.0.1	Blocked from RDS-Knight	13 Mar 2019 19:18:46	localhost
::1	Blocked from RDS-Knight	13 Mar 2019 17:34:53	localhost
192.168.247.128	Blocked from RDS-Knight	13 Mar 2019 17:34:53	localhost
fe80::e4c6:34e4:c48e:b9e2	Blocked from RDS-Knight	13 Mar 2019 17:34:53	localhost

Search

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

A convenient search bar provide search capabilities based on all information provided. For example, if we searched for blocked addresses, by entering the word "blocked" on the search bar, all the blocked IPs will be visible:



The screenshot shows the RDS-Knight Ultimate Protection interface. On the left is a navigation menu with options: HOME, EVENT VIEWER, HOMELAND, BRUTEFORCE, IP ADDRESSES (selected), PERMISSIONS, WORKING HOURS, SECURE DESKTOPS, ENDPOINTS, RANSOMWARE, SETTINGS, and LICENSE. The main area has a header with the RDS-Knight logo and the title "RDS-Knight Ultimate Protection". Below the header are three buttons: "+ Add IP Address", "Edit IP Address", and "Remove IP Address(es)", along with a "WHOIS" search button. A note states: "IPs in the whitelist will be ignored by RDS-Knight and will not be blocked by Homeland Access Protection or Bruteforce Attacks Defender features." Below this is a table of IP addresses with columns for IP Address, Status, Date, and Description. At the bottom of the table is a search box containing the text "blocked".

IP Address	Status	Date	Description
213.148.201.59	Blocked - BruteForce Defender	14 Mar 2019 04:01:11	
178.34.152.180	Blocked - BruteForce Defender	11 Mar 2019 21:38:55	
58.244.117.214	Blocked - Homeland Protection	11 Mar 2019 04:26:57	
49.14.98.70	Blocked - Homeland Protection	11 Mar 2019 03:10:33	
105.14.32.99	Blocked - Homeland Protection	11 Mar 2019 00:50:07	
202.133.54.73	Blocked - Homeland Protection	10 Mar 2019 23:43:50	
42.51.217.61	Blocked - Homeland Protection	10 Mar 2019 20:37:56	
201.158.104.100	Blocked - Homeland Protection	10 Mar 2019 17:35:18	
2.182.5.87	Blocked - Homeland Protection	10 Mar 2019 17:20:58	
196.189.44.50	Blocked - Homeland Protection	10 Mar 2019 17:19:15	
42.202.33.232	Blocked - Homeland Protection	10 Mar 2019 15:16:59	
117.224.202.156	Blocked - Homeland Protection	10 Mar 2019 14:18:03	
125.227.29.199	Blocked - Homeland Protection	10 Mar 2019 08:13:40	
124.226.216.77	Blocked - Homeland Protection	10 Mar 2019 07:56:32	
109.188.131.204	Blocked - Homeland Protection	10 Mar 2019 06:18:58	
190.60.108.18	Blocked - Homeland Protection	10 Mar 2019 05:46:16	
68.145.140.120	Blocked - Homeland Protection	10 Mar 2019 02:23:04	
101.230.201.89	Blocked - Homeland Protection	10 Mar 2019 00:50:43	
93.113.125.89	Blocked - Homeland Protection	09 Mar 2019 18:55:01	
31.220.43.113	Blocked - Homeland Protection	09 Mar 2019 18:07:53	

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:

The screenshot shows the "Edit Description" dialog box. It has a title bar with the RDS-Knight logo and the text "Edit Description". Inside the dialog, there are two input fields: "IP Address" with the value "125.212.233.172" and "Description" with the value "Accountancy-Server". At the bottom right of the dialog is a button with a pencil icon and the text "Edit Description".

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.

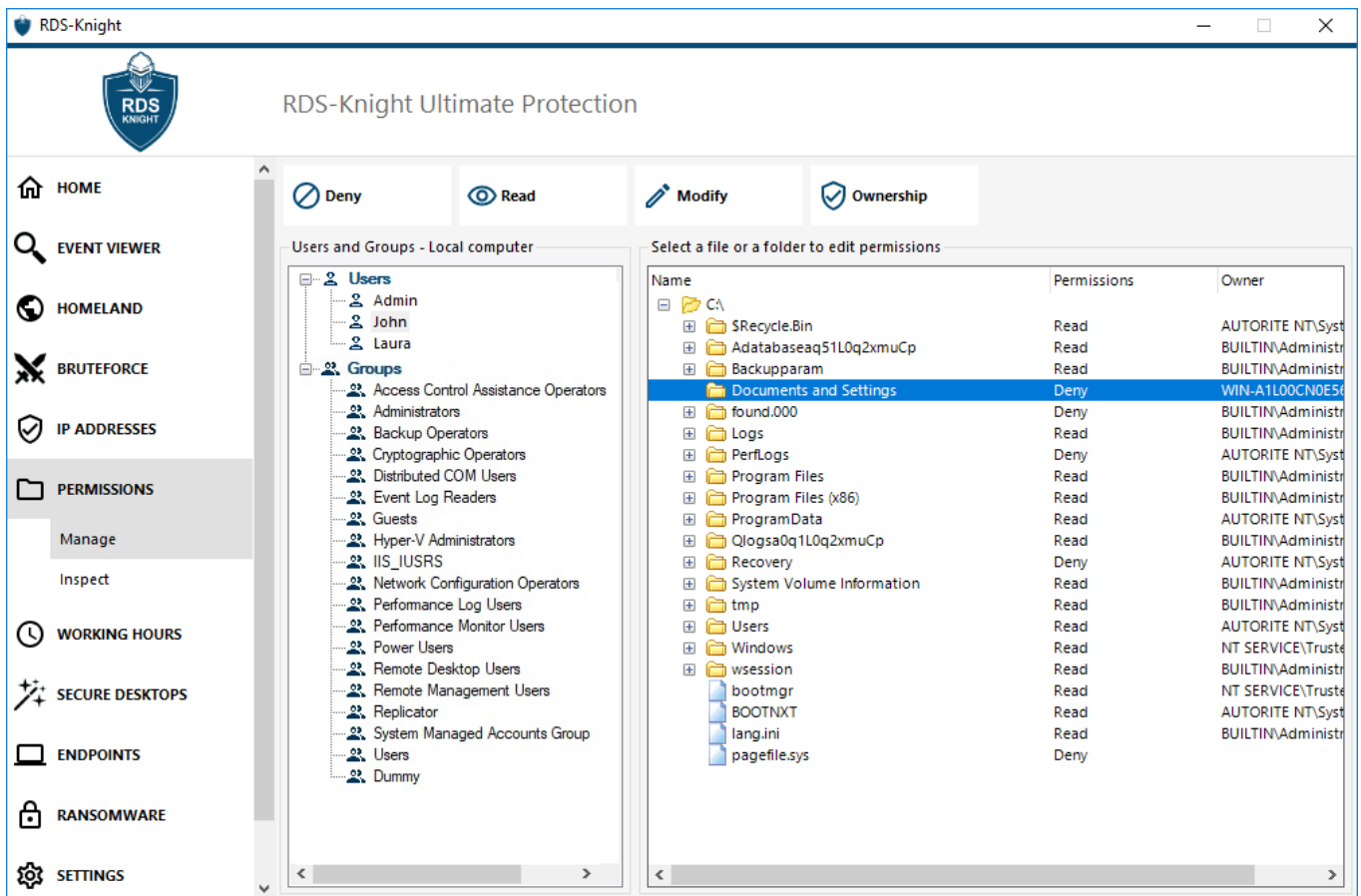
Permissions

Since version 4.3, RDS-Knight offers a Permissions functionality, that allows 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 folders are shown side-by-side. Everything is visible at one sight, which makes it super easy to Inspect (RDS-Knight Essentials) and edit (RDS-Knight Ultimate) privileges for one user at a time and therefore to increase the accuracy of the restrictions.

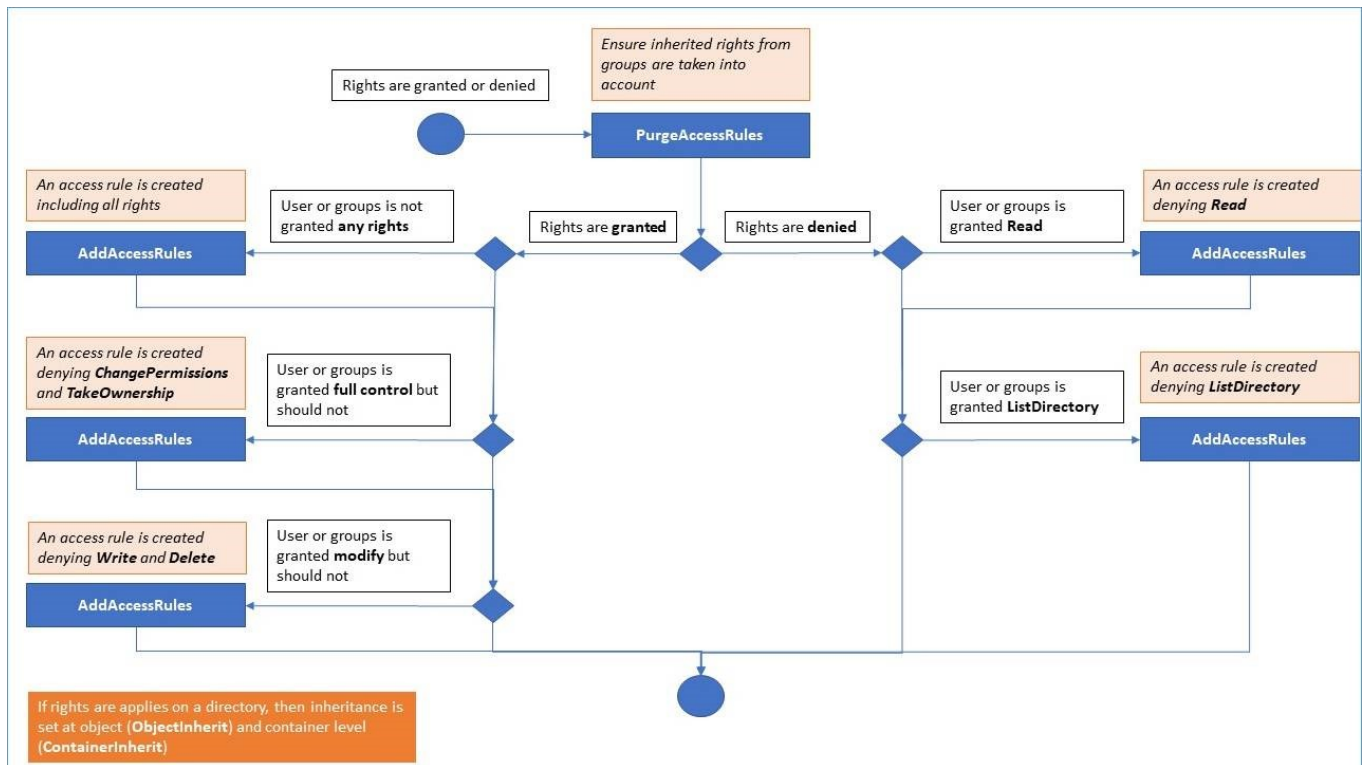
Manage

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



- **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).

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:

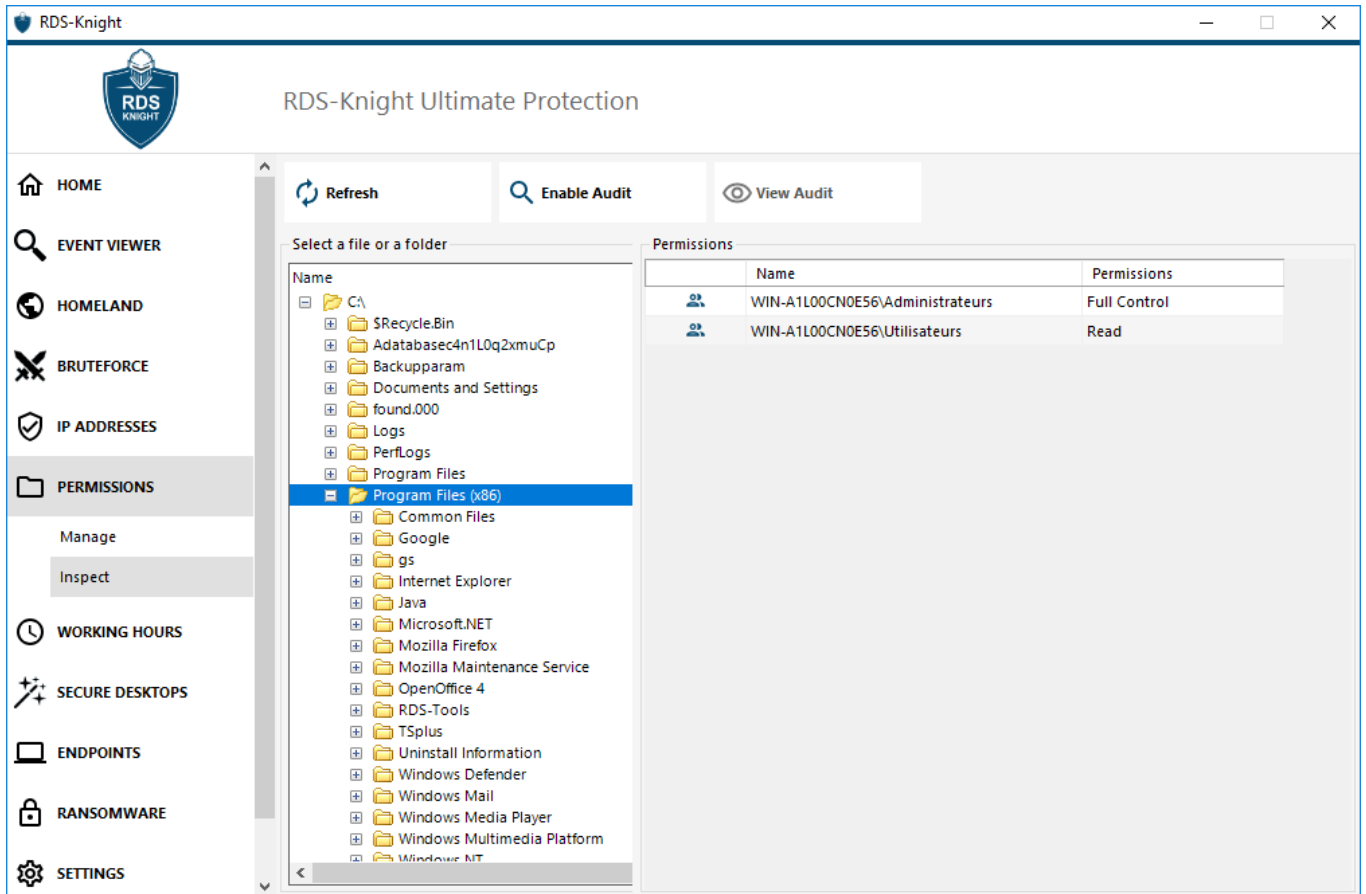


Documentation:

- Object Security: <https://docs.microsoft.com/en-us/dotnet/api/system.security.accesscontrol.objectsecurity?view=netframework-3.5>
- FileSystemRights: <https://docs.microsoft.com/en-us/dotnet/api/system.security.accesscontrol.filesystemrights?view=netframework-3.5>

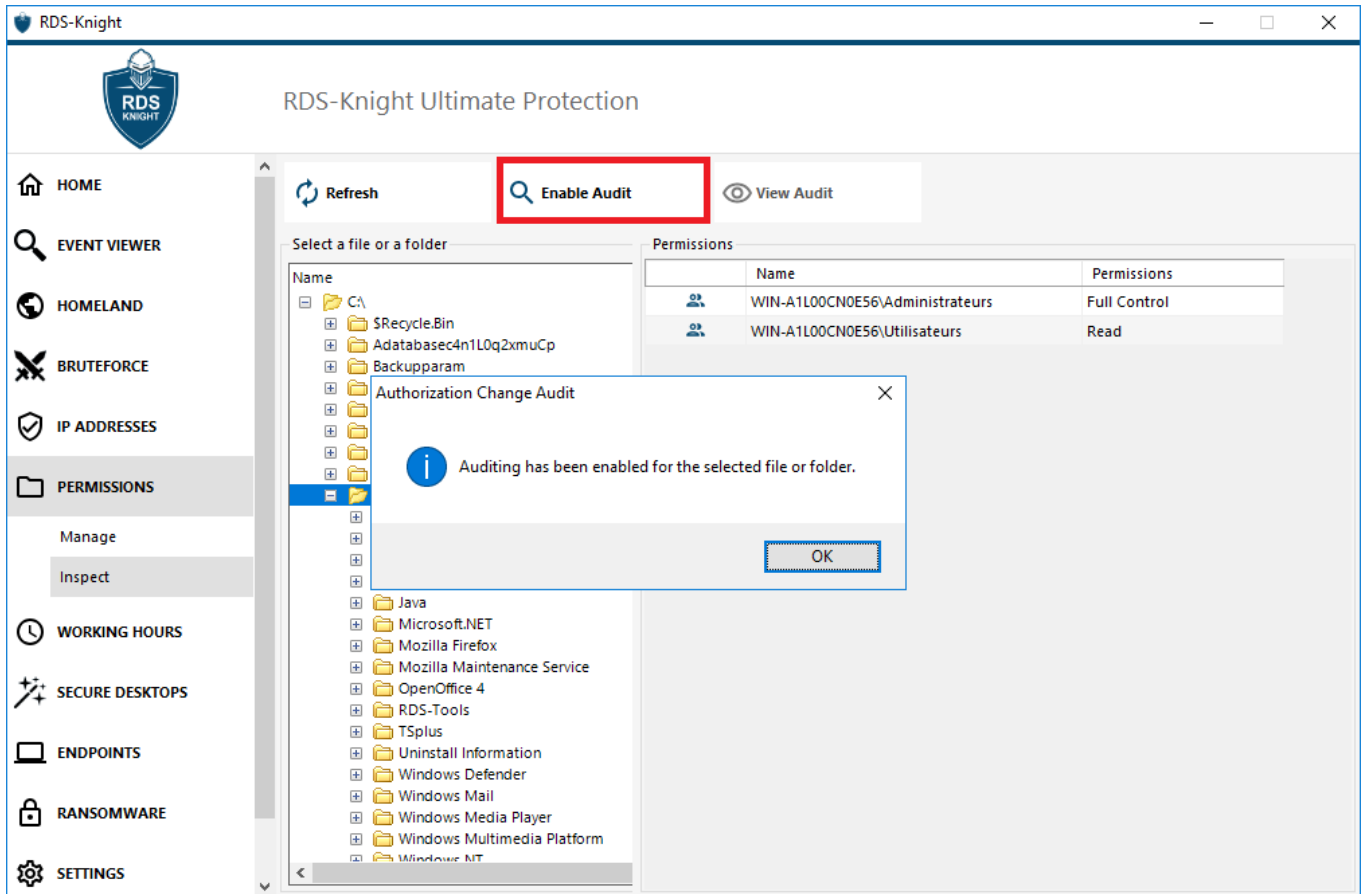
Inspect

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.

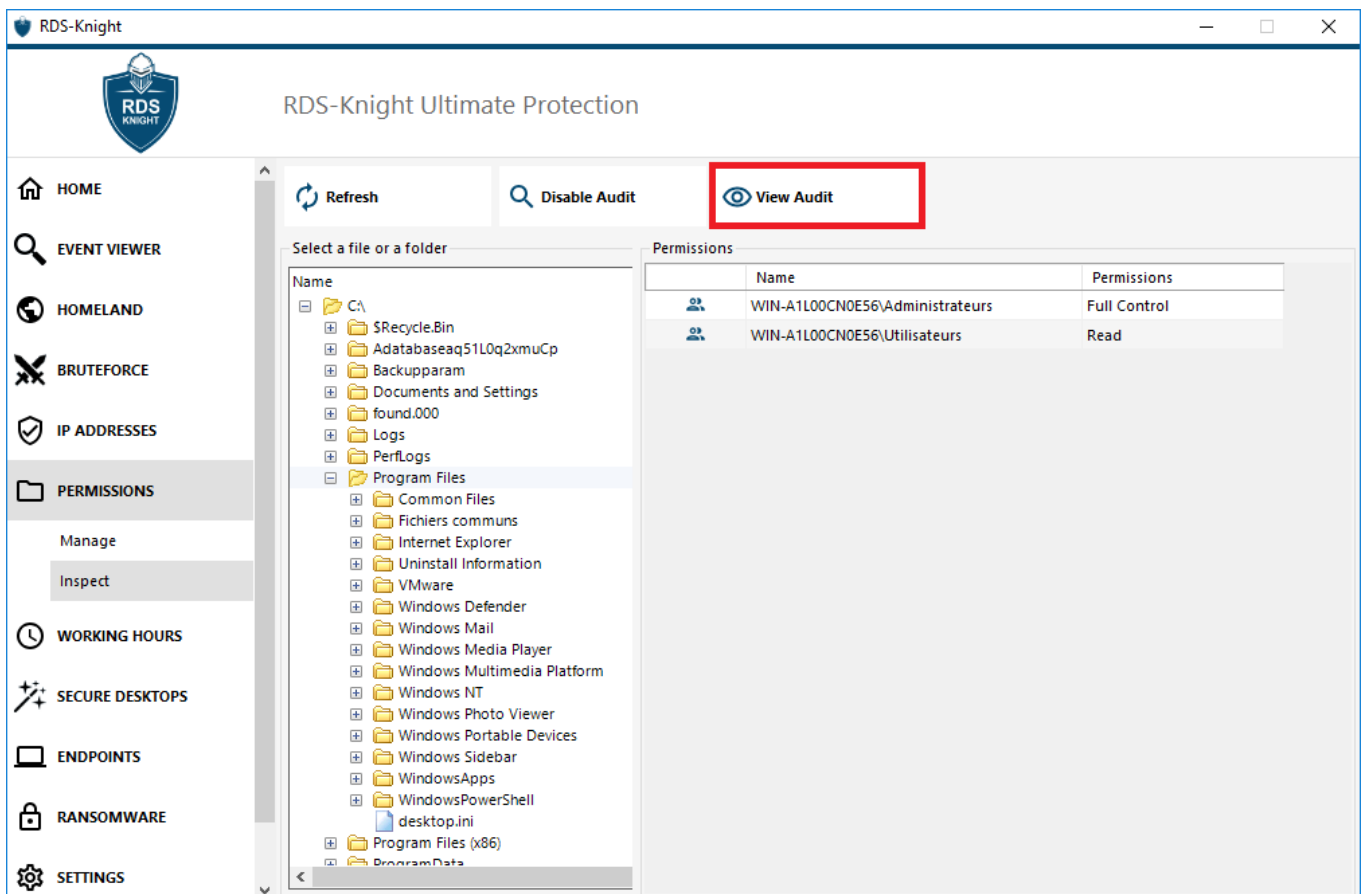


You can refresh the status of the folders for them to be updated in real-time.

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:





Working Hours Restriction

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:

The screenshot shows the RDS-Knight Ultimate Protection interface. On the left is a navigation menu with options: HOME, EVENT VIEWER, HOMELAND, BRUTEFORCE, IP ADDRESSES, PERMISSIONS, WORKING HOURS (selected), SECURE DESKTOPS, ENDPOINTS, RANSOMWARE, SETTINGS, and LICENSE. The main area is titled 'Users and Groups - Local computer' and displays a tree view of users and groups. The 'Users' section includes Admin, John, and Laura (whitelisted). The 'Groups' section includes Access Control Assistance Operators, Administrators, Backup Operators, Cryptographic Operators, Distributed COM Users, Event Log Readers, Guests, Hyper-V Administrators, IIS_IUSRS, Network Configuration Operators, Performance Log Users, Performance Monitor Users, Power Users, Remote Desktop Users, Remote Management Users, Replicator, System Managed Accounts Group, Users, and Dummy. On the right, there are radio buttons for 'Not configured for this user/group', 'Always authorize', 'Always block', and 'Authorize only during these time ranges:'. The 'Authorize only during these time ranges' option is selected. Below this, there are checkboxes for each day of the week (Monday through Sunday) and time range selectors (09:00 to 17:30). A dropdown menu for 'Select timezone for user or group ((UTC+01:00) Brussels, Copenhagen, Madrid, Paris is applied by default):' is set to '(UTC-08:00) Pacific Time (US & Canada)'. At the bottom, there are two informational notes: 'Whitelisted users will always be able to connect.' and '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.'

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 on the [Settings - Advanced - Working Hours tab of the AdminTool](#).

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 RDS-Knight 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.



Security Level

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 Desktop 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.

The screenshot displays the RDS-Knight Ultimate Protection interface. On the left is a navigation menu with options: HOME, EVENT VIEWER, HOMELAND, BRUTEFORCE, IP ADDRESSES, PERMISSIONS, WORKING HOURS, SECURE DESKTOPS (highlighted), ENDPOINTS, RANSOMWARE, SETTINGS, and LICENSE. The main area is titled 'Users and Groups - Local computer' and shows a tree view of users and groups. Under 'Users', 'John' is selected. Under 'Groups', several groups are listed, including 'Accès DCOM service de certificats', 'Administrateurs', 'Administrateurs Hyper-V', 'Duplicateurs', 'IIS_IUSRS', 'Invités', 'Lecteurs des journaux d'événements', 'Opérateurs d'impression', 'Opérateurs d'assistance de contrôle', 'Opérateurs de chiffrement', 'Opérateurs de configuration réseau', 'Opérateurs de sauvegarde', 'Serveurs Accès Distant RDS', 'Serveurs Gestion RDS', 'Serveurs RDS Endpoint', 'Storage Replica Administrators', 'System Managed Accounts Group', 'Utilisateurs', 'Utilisateurs avec pouvoir', 'Utilisateurs de gestion à distance', 'Utilisateurs de l'Analyseur de perfor', 'Utilisateurs du Bureau à distance', and 'Utilisateurs du journal de perform'. To the right of the tree view, there are radio buttons for 'Not configured for this user/group' and 'Configured for this user/group'. The 'Configured for this user/group' option is selected. Below this, a vertical slider allows selecting a security level: 'Kiosk Mode' (top), 'Secured Desktop Mode' (middle), and 'Windows Mode' (bottom). The slider is currently positioned at 'Secured Desktop Mode'. A 'Customize Security Level...' button is located at the bottom right, with a note below it: 'Whitelisted users will always use "Windows Mode".'

Customization

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

Desktop Security:



RDS-Knight - Security Level Customization

Security Level Customization

Desktop Security | Disks Control | Applications Control

- Remove Recycle Bin
- Remove My Documents
- Remove My Recent Documents
- Remove My Music
- Remove My Pictures
- Remove Frequently Used Programs
- Remove Programs
- Remove Help and Support
- Remove Control Panel
- Remove Printers
- Remove Network
- 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
ADMIN-PC\john

Currently based on
Secured Desktop Mode

Disks Control:



RDS-Knight - Security Level Customization

Security Level Customization

Desktop Security | **Disks Control** | Applications Control

Hide Selected Disks

<input checked="" type="checkbox"/> A	<input checked="" type="checkbox"/> B	<input checked="" type="checkbox"/> C	<input checked="" type="checkbox"/> D	<input checked="" type="checkbox"/> E	<input checked="" type="checkbox"/> F	<input checked="" type="checkbox"/> G
<input checked="" type="checkbox"/> H	<input checked="" type="checkbox"/> I	<input checked="" type="checkbox"/> J	<input checked="" type="checkbox"/> K	<input checked="" type="checkbox"/> L	<input checked="" type="checkbox"/> M	<input checked="" type="checkbox"/> N
<input checked="" type="checkbox"/> O	<input checked="" type="checkbox"/> P	<input checked="" type="checkbox"/> Q	<input checked="" type="checkbox"/> R	<input checked="" type="checkbox"/> S	<input checked="" type="checkbox"/> T	<input checked="" type="checkbox"/> U
<input checked="" type="checkbox"/> V	<input checked="" type="checkbox"/> W	<input checked="" type="checkbox"/> X	<input checked="" type="checkbox"/> Y	<input checked="" type="checkbox"/> Z		

Select all Unselect all

Deny Access to Selected Disks

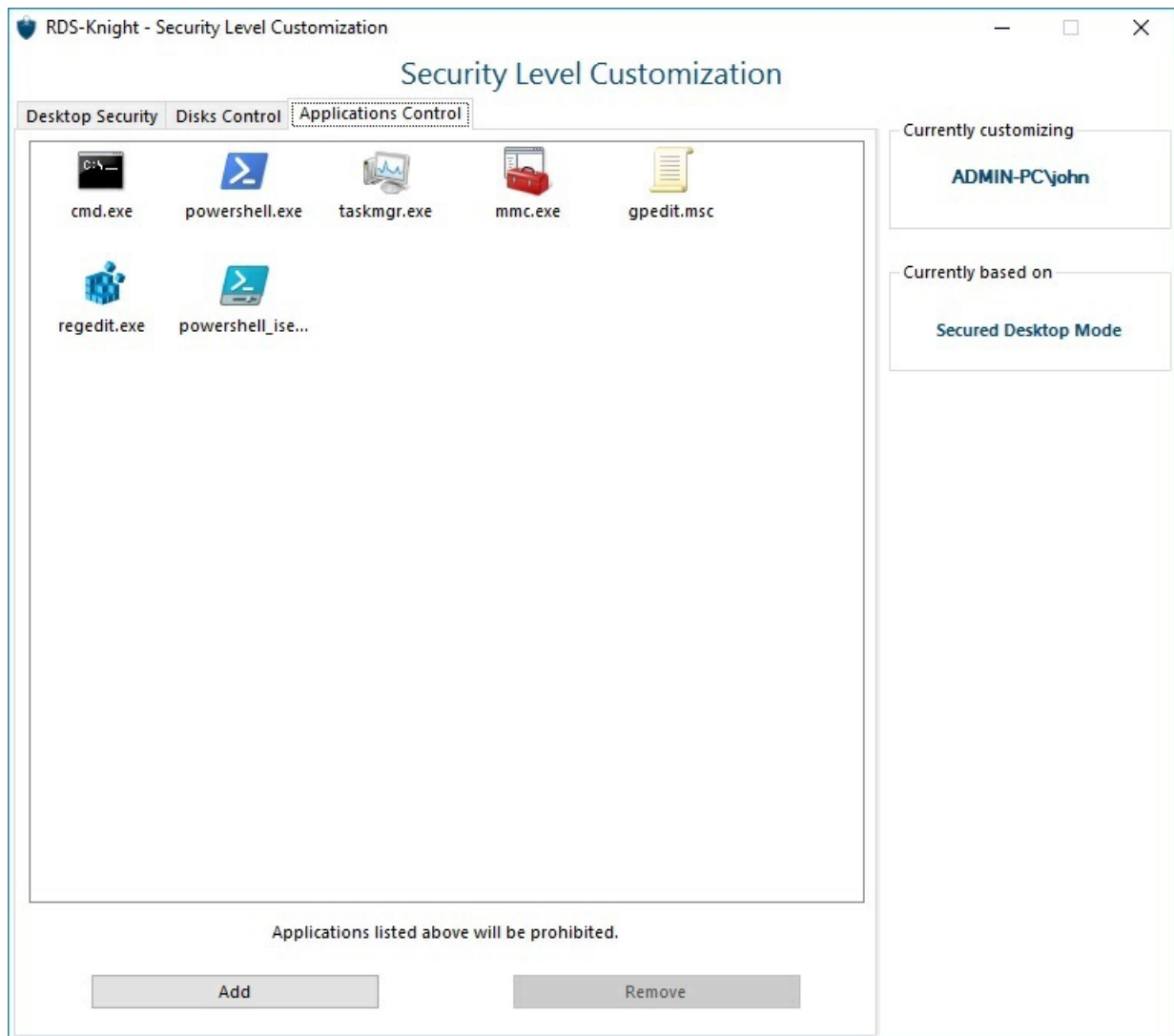
<input checked="" type="checkbox"/> A	<input checked="" type="checkbox"/> B	<input checked="" type="checkbox"/> C	<input checked="" type="checkbox"/> D	<input checked="" type="checkbox"/> E	<input checked="" type="checkbox"/> F	<input checked="" type="checkbox"/> G
<input checked="" type="checkbox"/> H	<input checked="" type="checkbox"/> I	<input checked="" type="checkbox"/> J	<input checked="" type="checkbox"/> K	<input checked="" type="checkbox"/> L	<input checked="" type="checkbox"/> M	<input checked="" type="checkbox"/> N
<input checked="" type="checkbox"/> O	<input checked="" type="checkbox"/> P	<input checked="" type="checkbox"/> Q	<input checked="" type="checkbox"/> R	<input checked="" type="checkbox"/> S	<input checked="" type="checkbox"/> T	<input checked="" type="checkbox"/> U
<input checked="" type="checkbox"/> V	<input checked="" type="checkbox"/> W	<input checked="" type="checkbox"/> X	<input checked="" type="checkbox"/> Y	<input checked="" type="checkbox"/> Z		

Select all Unselect all

Currently customizing
ADMIN-PC\john

Currently based on
Secured Desktop Mode

Applications Control:



Users/Groups rules priorities

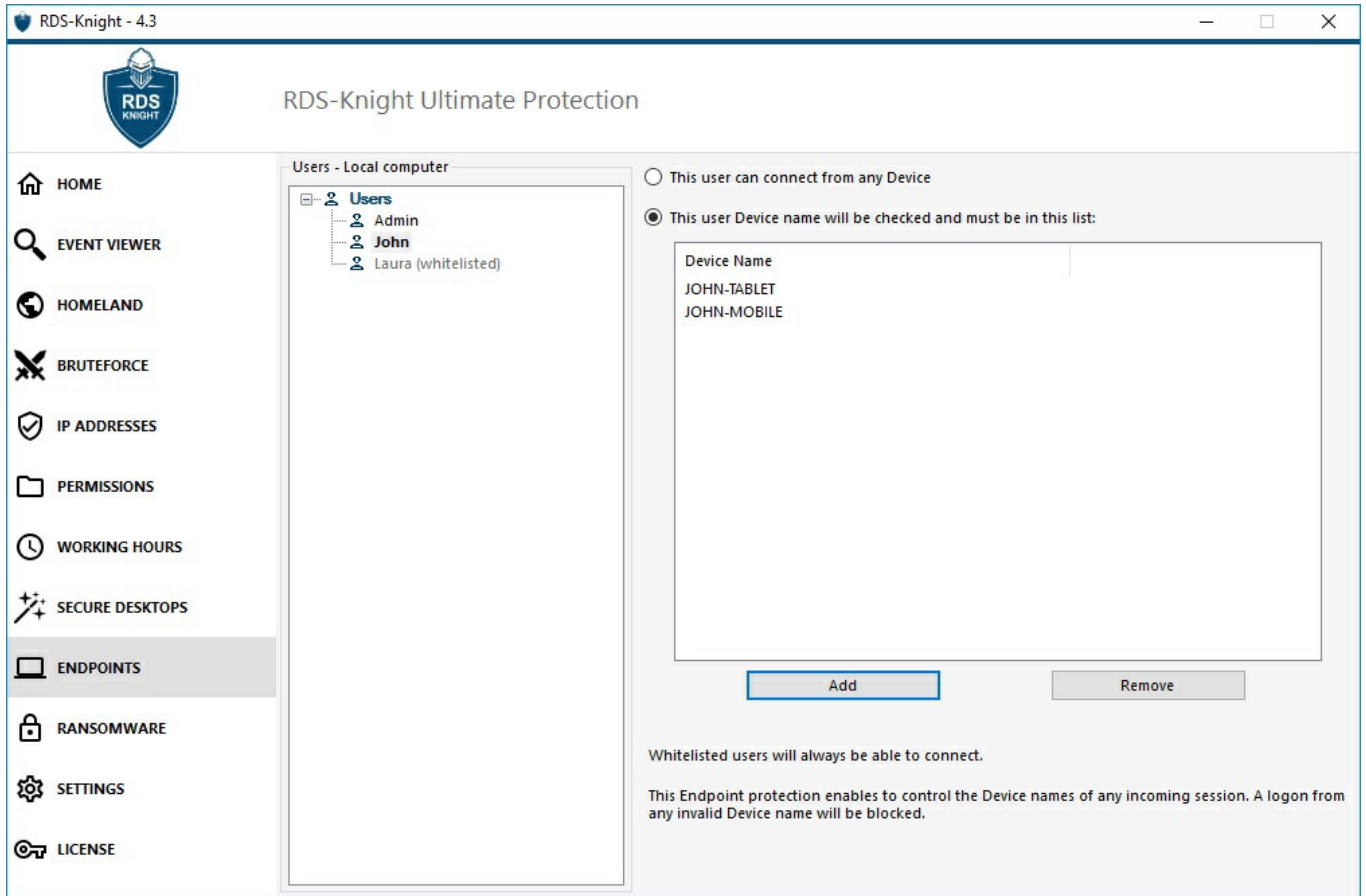
When a user opens a new session on the server:

- 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 RDS-Knight 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).

Endpoint Protection and Device Control

The endpoint protection and device control 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.



On this example, John will be using the device names John-PC and John-Tablet.

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, RDS-Knight will automatically save the name of the latest device used to connect to the server by any user who does not have the Endpoint Protection and Device Control feature enabled. After one working day, the device name of most users will be known by RDS-Knight, thus allowing you to quickly enable the Endpoint Protection feature without having to check every user's workstation name.

Note: Endpoint Protection is not compatible with HTML5 connections.



Ransomware Protection

Since **RDS-Knight 3.0 version**, the Ransomware Protection enables you to efficiently DETECT, BLOCK and PREVENT ransomware attacks. RDS-Knight reacts as soon as it detects ransomware on your session.

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

The screenshot shows the RDS-Knight Ultimate Protection interface. On the left is a navigation menu with items: HOME, EVENT VIEWER, HOMELAND, BRUTEFORCE, IP ADDRESSES, PERMISSIONS, WORKING HOURS, SECURE DESKTOPS, ENDPOINTS, RANSOMWARE (highlighted), SETTINGS, and LICENSE. The main content area displays two error messages: "Ransomware Protection is disabled. Click here to enable Ransomware Protection." and "Email alerts are not configured yet. Click here to configure email alerts." Below these is a section titled "The programs interrupted by Ransomware Protection are listed below:" containing a table with columns "Date", "Interrupted Program", and "Review & Act". At the bottom of the main area is a "Manage programs whitelist" button.

The dialog box is titled "RDS-Knight - About Ransomware Protection" and contains the following text:

RDS-Knight

About Ransomware Protection

RDS-Knight Ransomware Protection observes in real time how programs interact with system and personal files.

To ensure a greater level of protection, RDS-Knight Ransomware Protection creates bait files in key folders where ransomware often begins its attack.

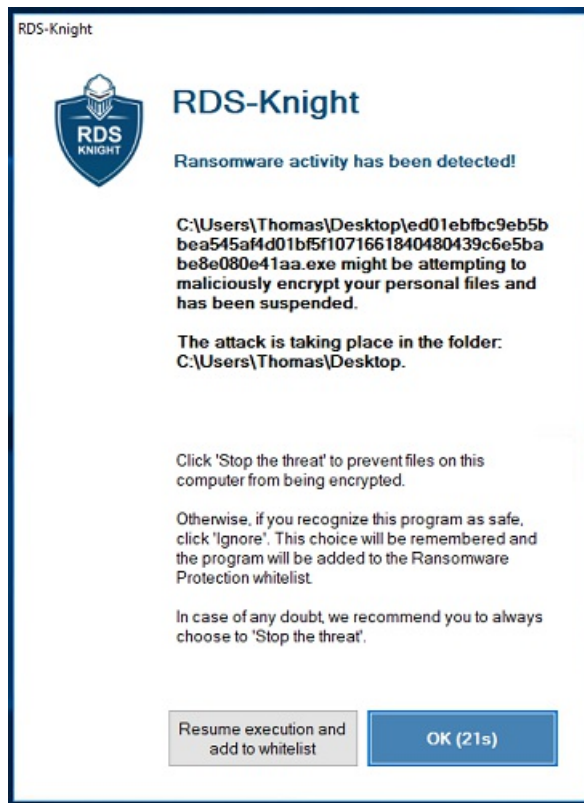
Therefore, a few hidden files may appear in the users' desktop and documents folders, as well as in other locations. We suggest to hide hidden files to regular users through your server settings or Group Policy.

At the bottom, there are two buttons: "Cancel" and "Enable Ransomware Protection".



RDS-Knight - Documentation

It quickly scans your disk(s) and displays the file(s) or program(s) responsible, in addition to providing a list of the infected items. RDS-Knight automatically stops the attack and quarantines the program(s) along with the file(s) encrypted before its intervention.



Only the administrator can whitelist them, by entering the path of the desired program on the bottom line and by clicking on "Add":



RDS-Knight - Ransomware Protection

Ransomware Protection

✔ Ransomware Protection is enabled Disable Ransomware Protection Configure Email Alerts

Ransomware Protection Summary

Date	Interrupted Program	Review & Act
vendredi 5 octobre 2018 16:19:59	C:\Users\Thomas\Desktop\DEMO\Ransomware\ransomware.exe	!

Whitelisted programs will be ignored by Ransomware Protection

Program File Path	Remove
C:\Program Files (x86)\Notepad++\notepad++.exe	×
C:\Program Files (x86)\RDS-Tools\RDS-Knight\RDS-Knight.exe	×

+ Add

Enter a program file path to add a program to the Ransomware Protection program whitelist. This executable will be able to create, change and delete your personal files without triggering Ransomware Protection.

Apply now

Ransomware Protection Report

RDS-Knight 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.



RDS-Knight Ultimate Protection

RDS-Knight - Ransomware Protection Report

Ransomware Protection Report

Ransomware Protection has detected a ransomware attack on computer WIN-COK62P4JGT7 at Tuesday, March 12, 2019 10:56:02 AM in session WIN-COK62P4JGT7\Thomas. The malicious program C:\Users\Thomas\Desktop\mail_attachment.exe has been terminated. Please review the report to take further action.

Details

Event Date: Tuesday, March 12, 2019 10:56:02 AM

The attack took place in user session: WIN-COK62P4JGT7\Thomas

Executable File Path:
C:\Users\Thomas\Desktop\mail_attachment.exe

The executable file has not been moved into quarantine

A memory dump is available here:
C:\Program Files (x86)\RDS-Tools\RDS-Knight\dumps\MiniDump_2019-12-3--10-57-03.mdump

Review the files created during the attack and put into quarantine the dangerous ones:

File Name	Put Into Quarantine
C:\Users\Thomas\Desktop\TurboCryptoEngine.conf	<input type="checkbox"/>
C:\Users\Thomas\Desktop\TurboCryptoEngine.dat	<input type="checkbox"/>
C:\tmp\TurboCryptoEngine.xyz	<input type="checkbox"/>
C:\tmp\TurboCryptoEngine\Download\3bc6d5a4702eb90277ddb74a3372a9fa\30808e9f7418e0	<input type="checkbox"/>
C:\Temp\TurboCryptoEngine\Download\3bc6d5a4702eb90277ddb74a3372a9fa\2860a934b91d7d77	<input type="checkbox"/>


Review the sensitive registry keys modified during the attack and edit the dangerous ones:

Registry Key	Name	Value	Old Value
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\...	P4wn3d	C:\Users\Thomas\Desкто...	

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.

Add an SMTP configuration - Email Alerts

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

 Email alerts are not configured yet. [Click here to configure email alerts.](#)



RDS-Knight - Emails Settings

Emails Settings

SMTP configuration allows RDS-Knight to send an email to administrators in order to highlight important security events.

SMTP Hostname

SMTP Port

Use SSL

SMTP Username

SMTP Password

Send Email From

Send Email To

Apply and Test now

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.



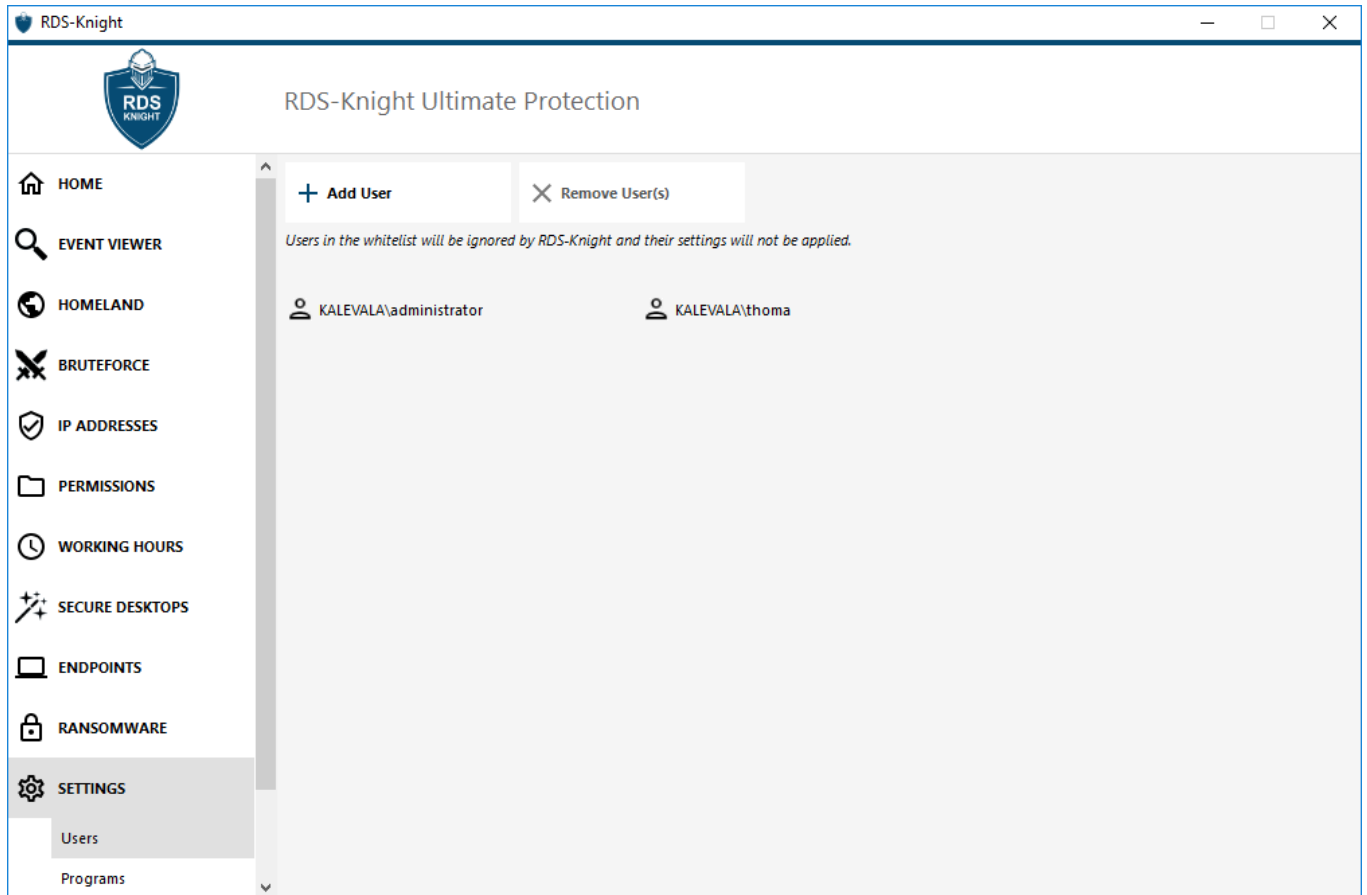
Settings

For information about RDS-Knight System Audit and Database, see these documentations: [System Audit](#) and [RDS-Knight Database](#).

Users Whitelist

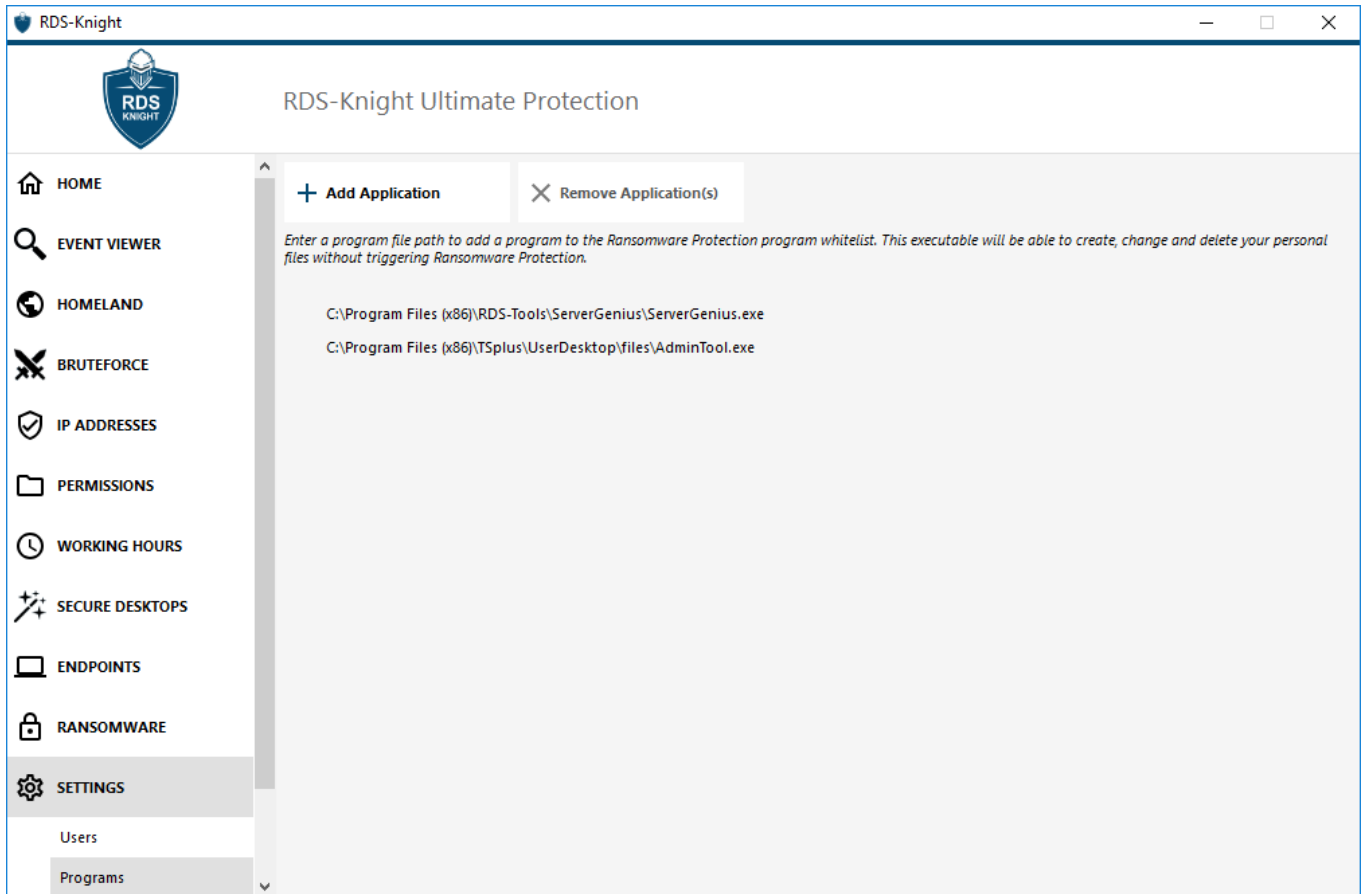
The **Users Whitelist tab** gives the Administrator the possibility to *add/remove users from the whitelist*. Users on the whitelist are ignored by RDS-Knight and their settings will not be applied.

The user who downloaded RDS-Knight is automatically added to the Whitelist:



Programs

On the **Programs tab**, you can *add programs to the list of allowed programs, that won't be checked by RDS-Knight Ransomware Protection*.

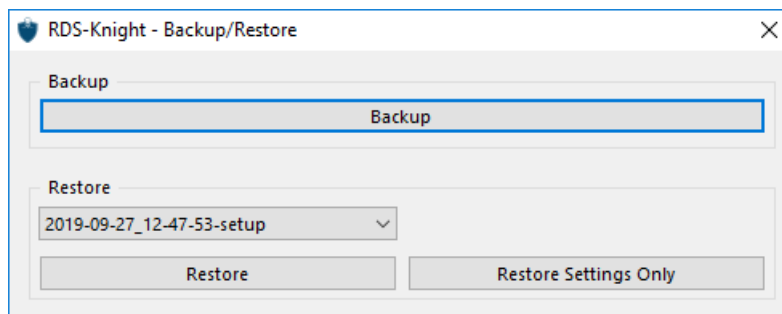
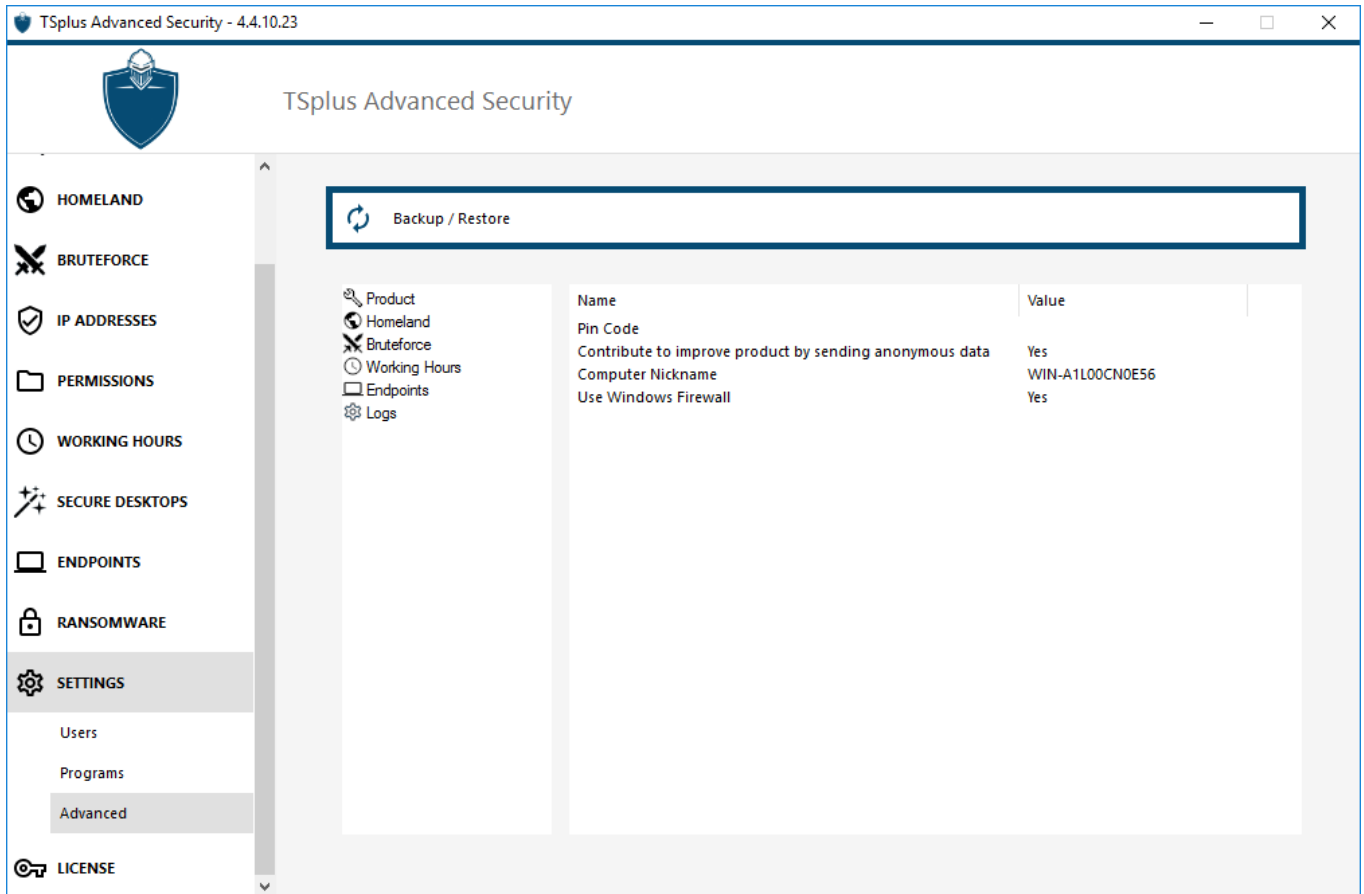


Click on the "Add Application" button to add a program. You can also remove them by selecting application(s) and clicking on the Remove Application(s) button.

Advanced

On the Advanced tab, you can configure RDS-Knight settings.

You can Backup or Restore RDS-Knight data and settings by clicking on the button "Backup/Restore" on the top:



Please follow the steps below to migrate RDS-Knight 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 RDS-Knight setup directory (typically C:\Program Files (x86)\RDS-Tools\RDS-Knight\archives).
2. Copy the newly created backup folder (e.g. named backup-2019-09-11_14-37-31), including 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 RDS-Knight on computer A.
5. Please wait at most 2 minutes for the settings to be reloaded by RDS-Knight features.

- The **Product tab** allows you to add a PIN code to the Administration Tool.



RDS-Knight Ultimate Protection

Backup / Restore

Product	Name	Value
Homeland	Pin Code	
Bruteforce	Contribute to improve product by sending anonymous data	Yes
Working Hours	Computer Nickname	WIN-A1L00CN0E56
Endpoints	Use Windows Firewall	Yes
Logs		

Navigation menu: HOMELAND, BRUTEFORCE, IP ADDRESSES, PERMISSIONS, WORKING HOURS, SECURE DESKTOPS, ENDPOINTS, RANSOMWARE, SETTINGS (Users, Programs, Advanced), LICENSE

RDS-Knight - Edit Setting

Pin Code

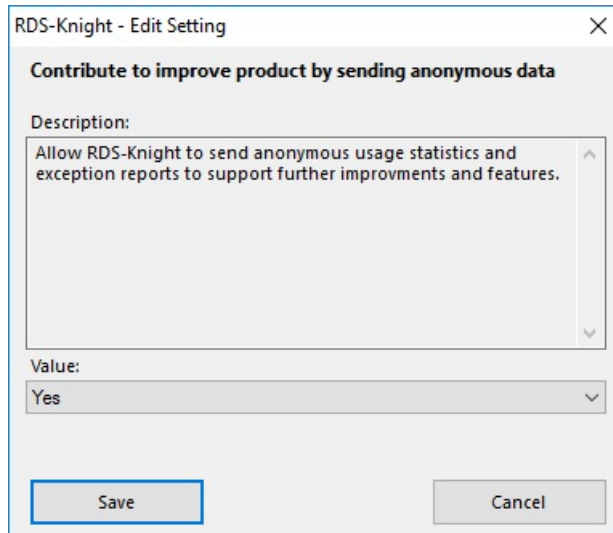
Description:
RDS-Knight will ask for a password if this value is not empty.

Value:
1234

Buttons: Save, Cancel

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

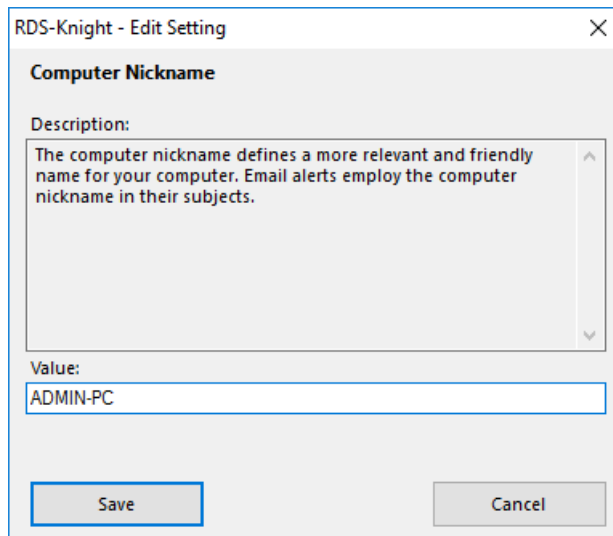
You can also **contribute to improve the product**, by sending anonymous data (enabled by default):



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

- RDS-Knight Version.
- Windows Version.
- Suspected files'paths that lead to the ransomware attack.

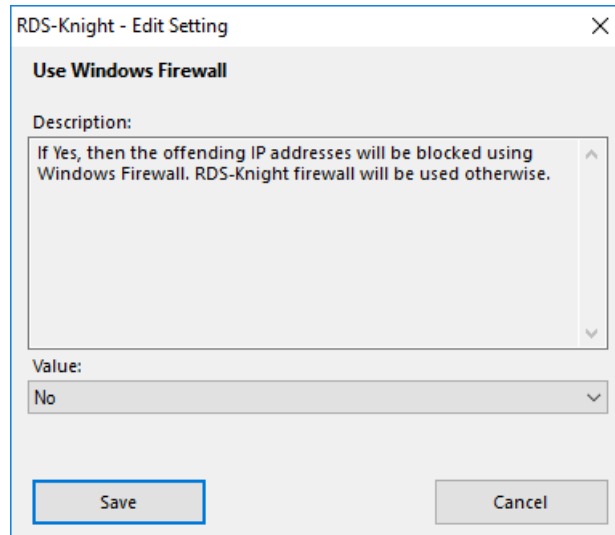
Modifying the **Computer nickname** is also possible:



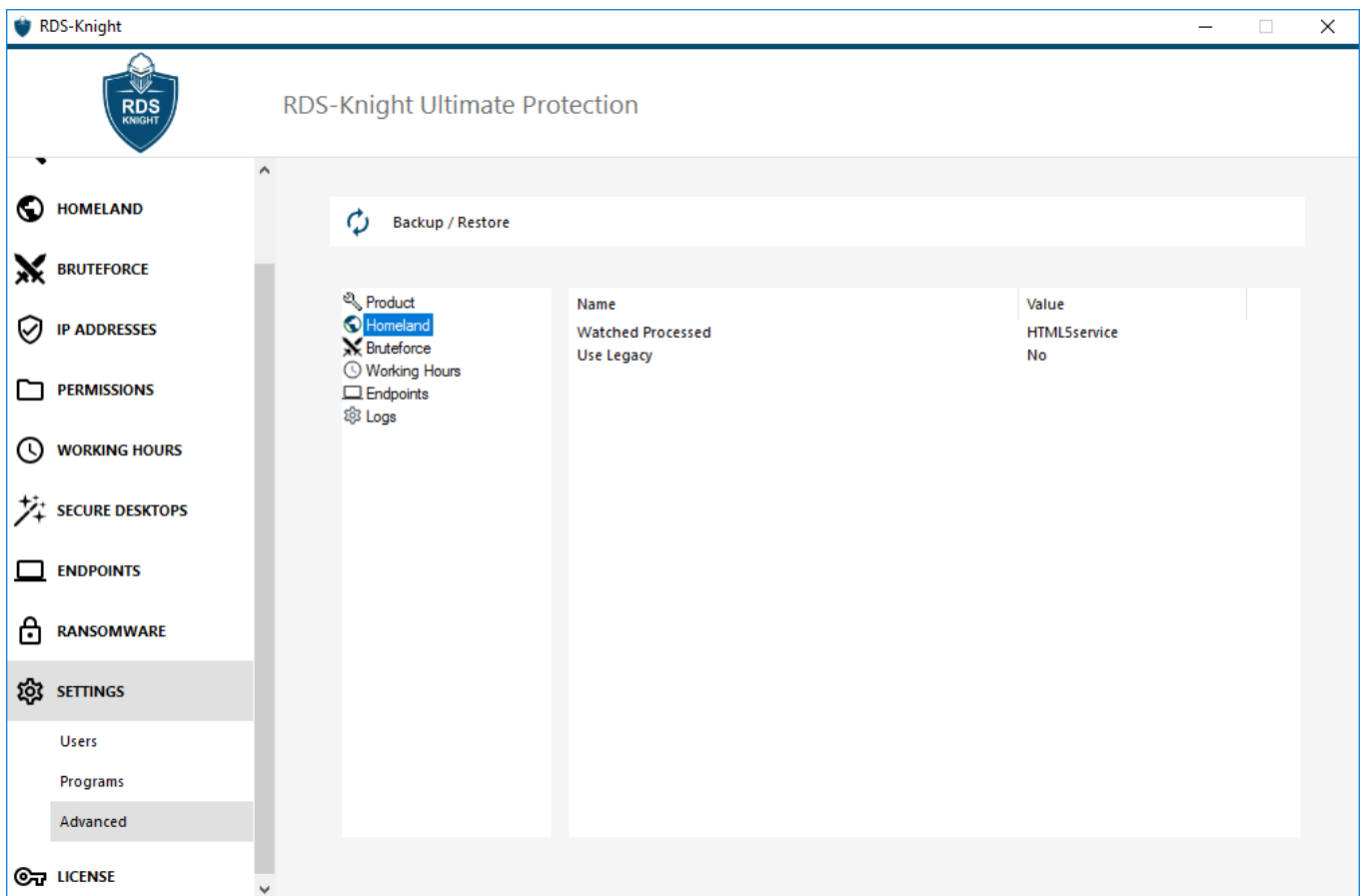
Since version 4.4, a built-in firewall is included in RDS-Knight.

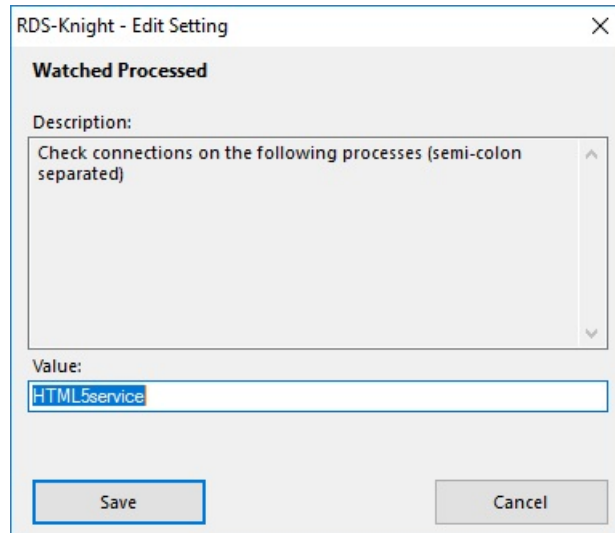
As a general guidance, if Windows Firewall is activated on your server, then you should use it to enforce RDS-Knight rules (default). If you installed another firewall, then you must activate RDS-Knight built-in firewall.

In order to activate the built-in firewall, go to Settings > Advanced > Product > Use Windows Firewall and set the value to No:



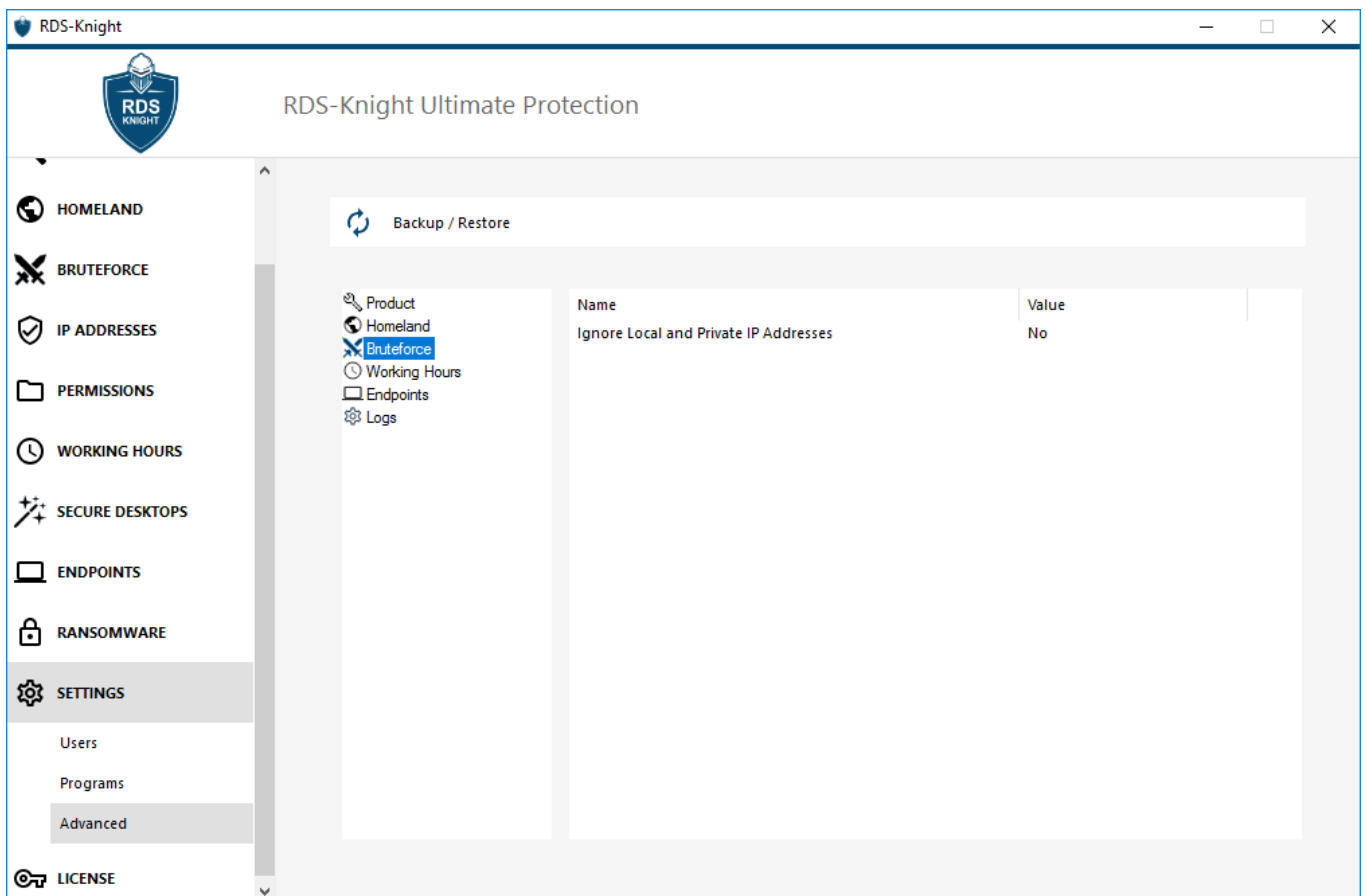
- The **Homeland** tab allows you to *add or remove Processes that are watched by the Homeland Protection feature.*

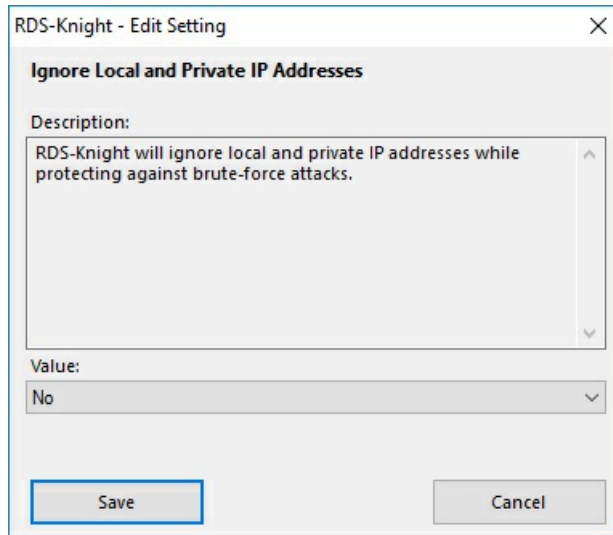




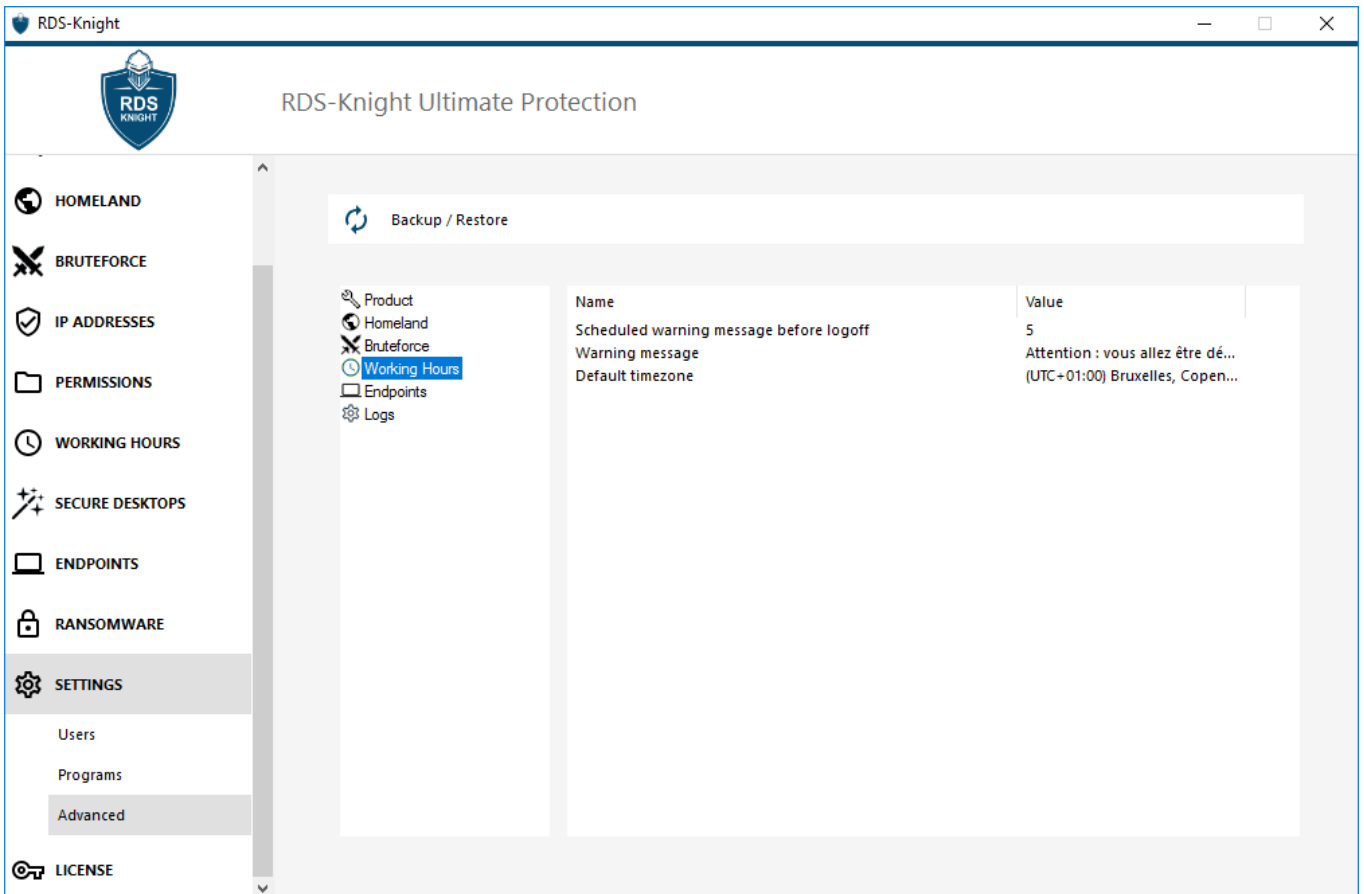
By default, the HTML5 service is watched.

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

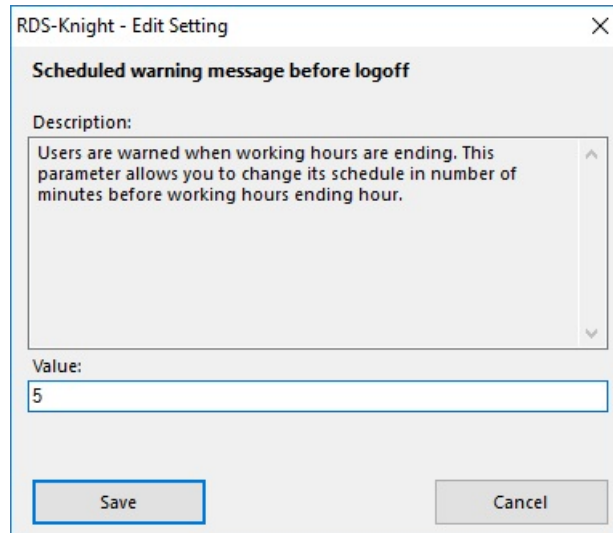




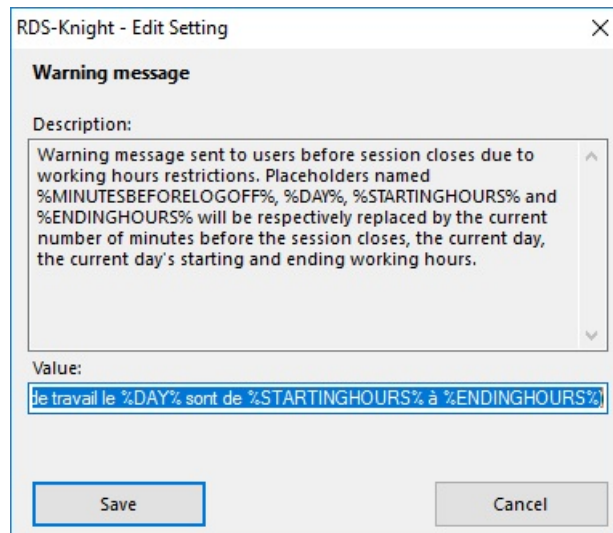
- The **Working Hours** tab allows you to schedule and modify a warning message before the user is logged off.



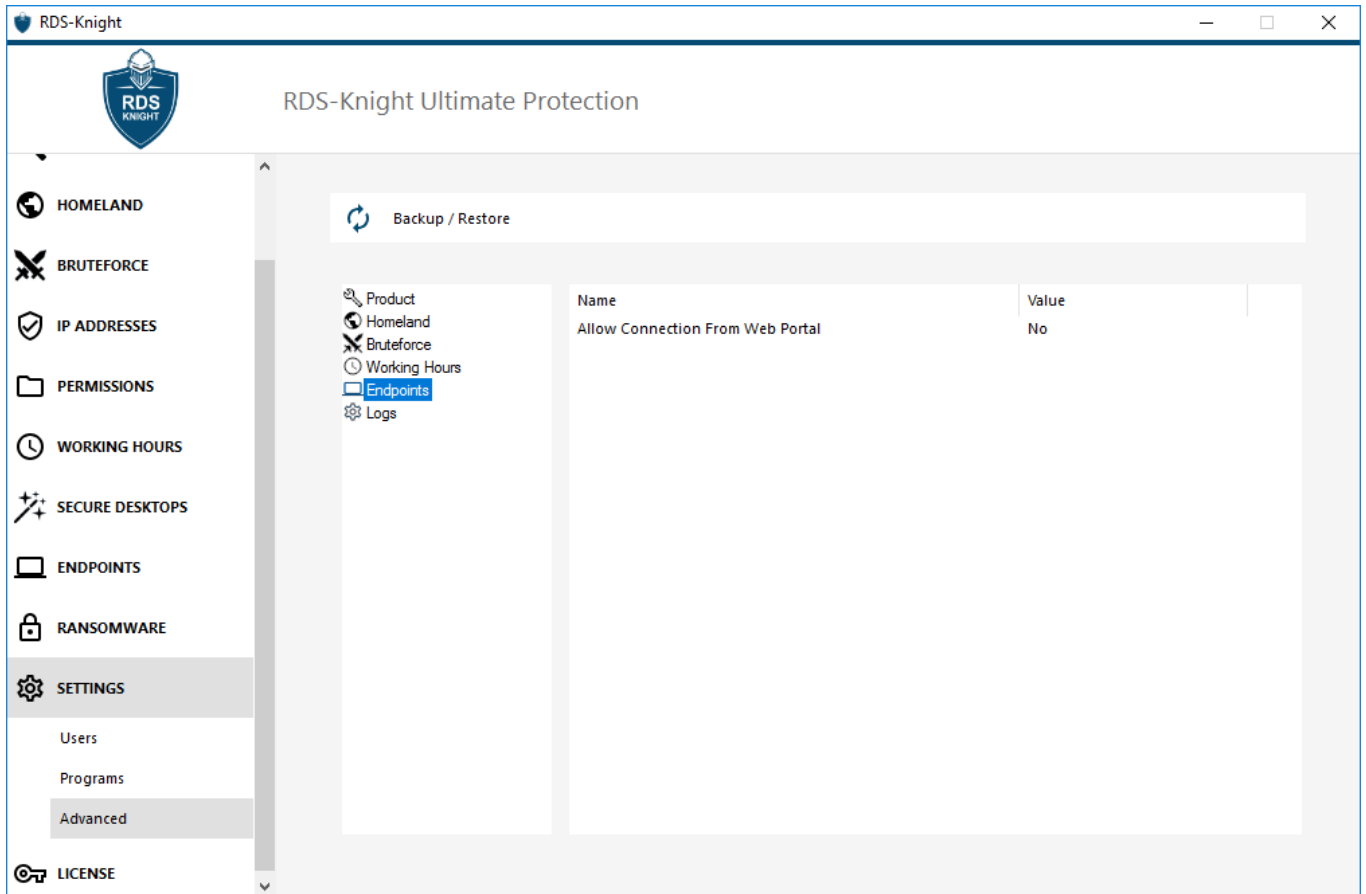
You can configure the warning message schedule in number of minutes before the user is automatically disconnected. By default, it is set to 5 minutes.



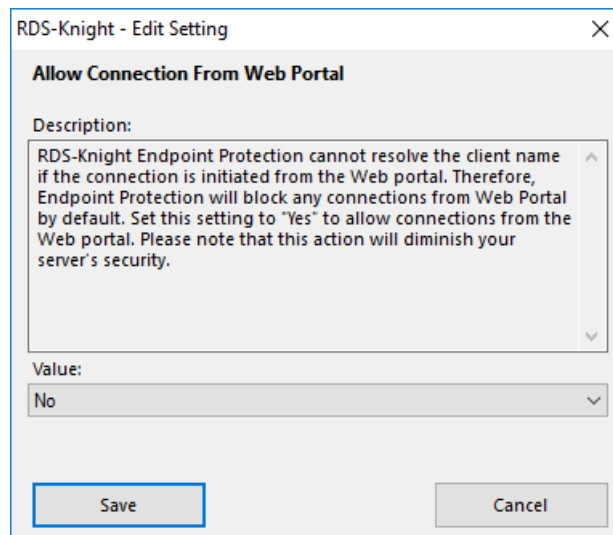
Modify the Warning message at your convenience, with placeholders named %MINUTESBEFORELOGOFF%, %DAY%, %STARTINGHOURS% and %ENDINGHOURS%, which will be respectively replaced by the current number of minutes before the session closes, the current day, the current day's starting and ending working hours.



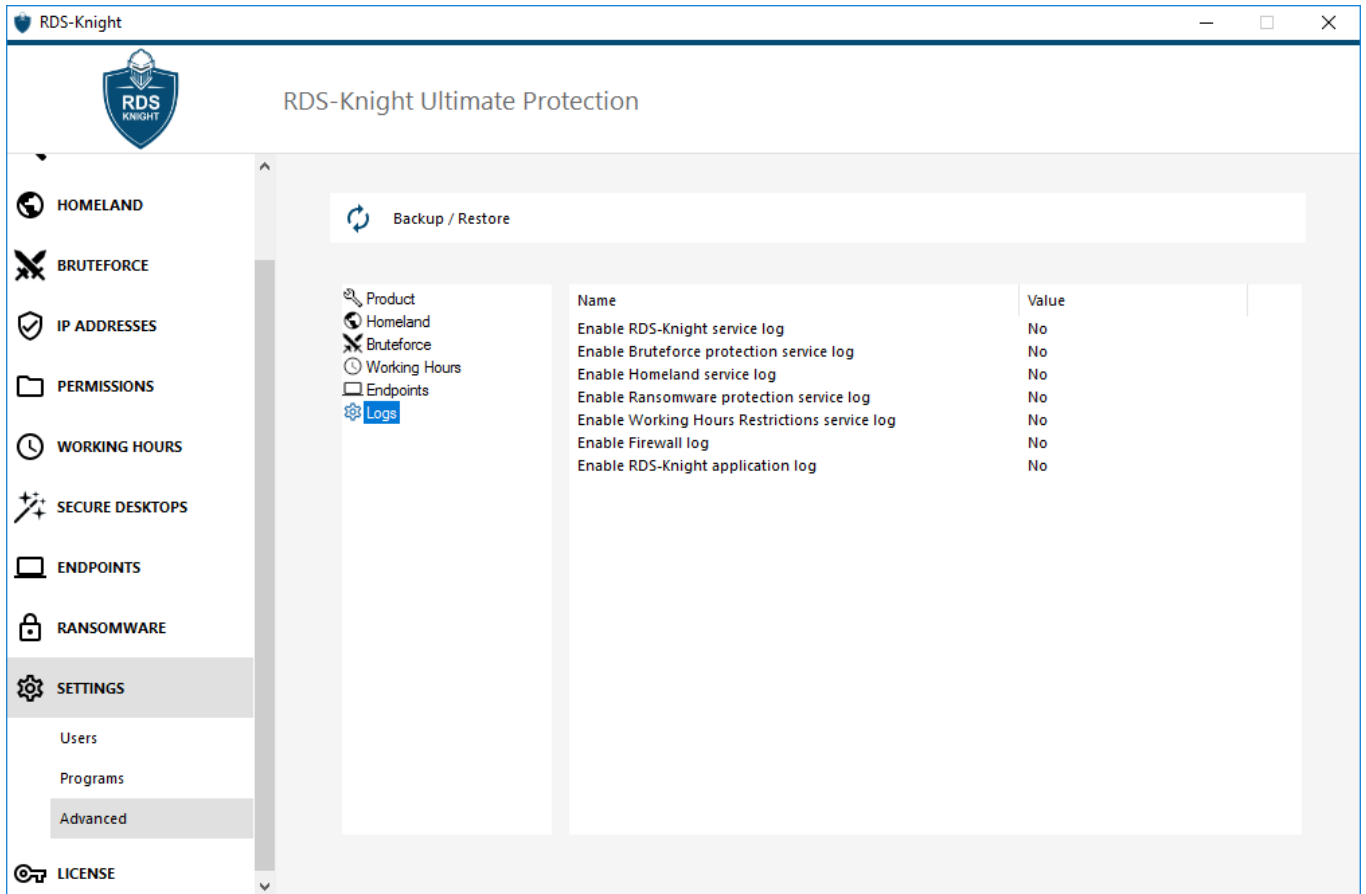
- The **Endpoints** tab allows you to enable connections from the Web Portal for Endpoints Protection users.



RDS-Knight Endpoint Protection cannot resolve the client name if the connection is initiated from the Web portal. Therefore, Endpoint Protection will block any connections from Web Portal by default. Set this setting to "Yes" to allow connections from the Web portal. Please note that this action will diminish your server's security.



- The **Logs tab** allows you to *enable or disable service and functionalities logs*. Logs exist to find more easily the origin of the errors encountered on RDS-Knight.



Enable or disable *RDS-Knight 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 RDS-Knight features : *Bruteforce Protection, Homeland and Ransomware protection services logs*. They are disabled by default.

Logs correspond to different components, our support team will tell you what value to put according to the problem encountered.

Database

Since version 4.3, a **database stores Events, IP addresses, Ransomware attacks reports and programs whitelists**. This database is stored in `.\data` and this is a [LiteDB DataBase](#):

