Syspeace manual

Syspeace v3.1.5

Treetop Innovation AB

For more information, see https://www.syspeace.com/

Contents

Welcome to this manual!

This manual can be read cover-to-cover, but it is also arranged so that it is an effective reference of Syspeace.

This manual will cover, in order:

- Syspeace's footprint
- Prerequisites
- Installation
- Syspeace's basis of operation
- Syspeace's licensing
- Remote Status and deploying Syspeace
- Configuring Syspeace after installation
- Syspeace Settings
- Troubleshooting
- How to contact us

Footprint

By default, Syspeace is installed inside the folder C:\Program Files\Treetop\Syspeace.

Shortcut icons to the Syspeace application are placed on the desktop and inside the Start menu's Program folder.

The Windows Service "SyspeaceService" is created on first start of application and removed when Syspeace is removed from the system.

No files are placed in any other folders/places than mentioned above.

The event log "SyspeaceLog" is created and viewable through the standard Windows Event Viewer.

The registry is not used to keep settings. To accomplish some tasks, the registry is used transiently.

Settings and operational data are maintained in databases in the Syspeace folder and are kept even when Syspeace is uninstalled.

Prerequisites

There are a number of prerequisites that have to be in place in order for Syspeace to work.

System requirements

Syspeace requires a 32-bit or 64-bit version of Windows Server 2003, Windows Server 2008, Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2, Windows Server 2016 or Windows Server 2019. Syspeace is not available for Itanium or ARM. Syspeace does not run on Server Core or Nano Server.

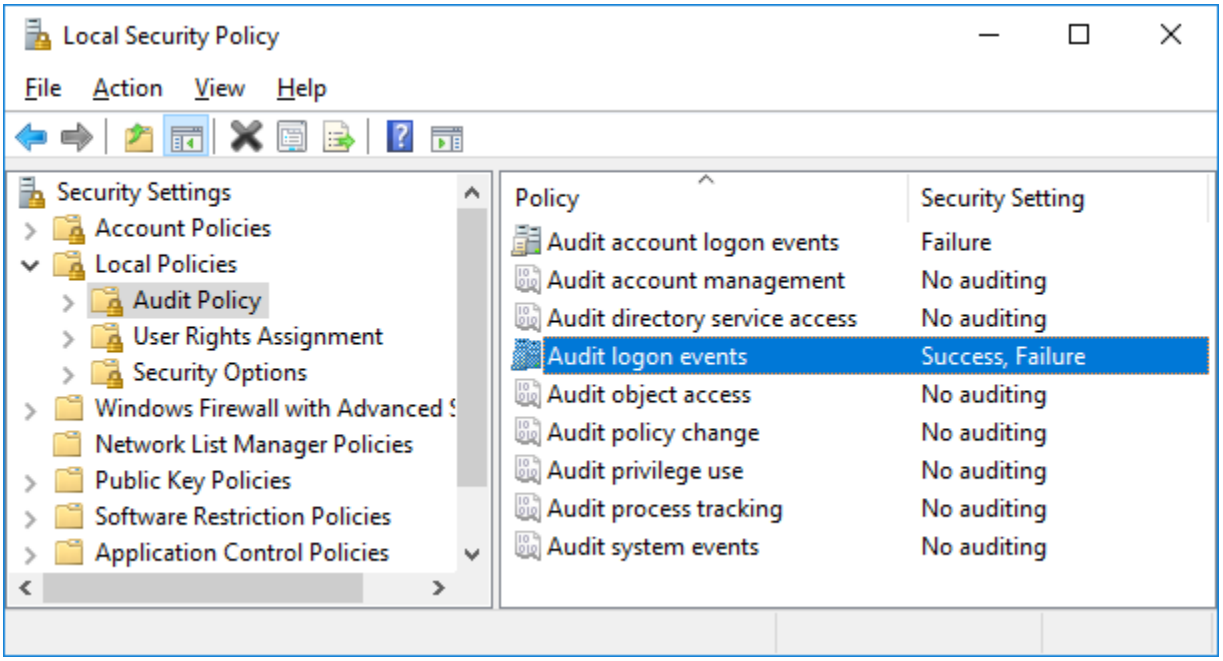
Syspeace requires 1GB of free disk space and a minimum of 500 MB RAM.

Syspeace for Windows Server 2003 requires the special Windows Server 2003 version of Syspeace.

Windows login detection prerequisites

For Windows login attempt detection, Syspeace requires auditing for failed login and successful login to be enabled in the local security policy or in the group policy for the domain. If this is not properly set up, the Syspeace client will attempt to detect this state and warn when starting the Syspeace service.

To set this up in the local security policy:



1. Open the **Control Panel**.
2. Open **Administrative Tools**.
3. Open **Local Security Policy**.
4. In the tree to the left, select **Security Settings** → **Local Policies** → **Audit Policy**.
5. In the list to the right, double click **Audit logon events**.
6. Check the **Success** and **Failure** checkboxes.

To set this up in a group security policy, edit the domain policy using **Active Directory Users and Computers** and follow the steps above starting at step 4.

SQL Server login detection prerequisites

For SQL Server login attempt detection, Syspeace requires auditing for failed login and successful login to be enabled in SQL Server. Note that Syspeace must be installed on the database server itself. To set this up:

1. Open **SQL Server Management Studio** and connect to the database with a user that has administrative privileges.
2. In **Object Explorer** or the **Object Explorer Details** tab, right-click the database server (the node that has SQL Server version information) and select **Properties**.
3. Select the **Security** page in the page list to the left.
4. Under **Login auditing**, select **Both failed and successful logins**.
5. Click **OK**.

Manual configuration of SQL Server login detection after installation

SQL Server login detection is not enabled out of the box.

Under very common scenarios in hosting or hosting-like environments, many different users have access to a shared database server from a shared web hosting server. Blocking an entire shared web hosting server would also shut out access for other customers. Since Syspeace cannot validate that it is not being used in this sort of scenarios and since these scenarios are prevalent, Syspeace has to be configured manually after installation.

Enabling Remote Desktop/Terminal Services detection

Remote Desktop/Terminal Services login detection may require enabling an extra setting.

Failures and successes in Remote Desktop/Terminal Services sessions are picked up using the same log as the Windows login detector. In Windows Server 2003 and 2016, this works without issue.

In Windows Server 2008, 2008 R2, 2012 and 2012 R2, when using Negotiate/SSL/TLS security (and not the so-called RDP Security Layer), the IP address is missing. Syspeace can use other strategies to fill in the IP address.

Windows Server version	Detection solely with Windows login event log	Traffic-based IP detection helps	RDP event log helps partially
Any, using RDP Security Layer	●		
Windows Server 2003	●		
Windows Server 2008/2008 R2		●	
Windows Server 2012/2012 R2		●	●
Windows Server 2016 and later	●		

For Windows Server 2008 through 2012 R2, traffic-based IP detection can be used to detect the IP address from a combination of packet metadata and traffic patterns. To enable this, turn on the setting **Traffic-based Remote Desktop/Terminal Services IP detection** under ***Rules → General***.

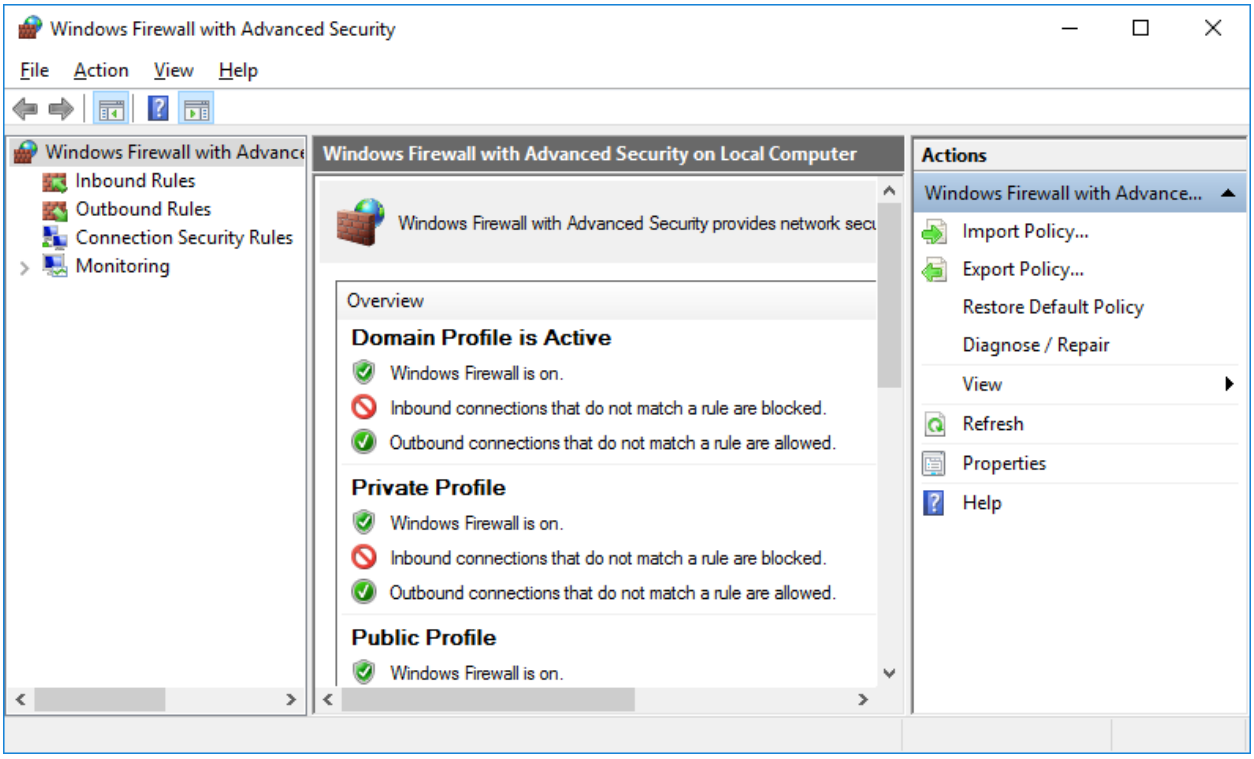
For Windows Server 2012 and 2012 R2, Syspeace can pick up events logged to a separate RDP event log to partially fill in login failures without enabling traffic-based IP detection. This approach catches all login failures that are logged to the RDP event log (not all login failures will generate such an event), but no successful logins since there is not enough information to correctly associate them with an IP address. If the setting mentioned above is not enabled, this approach is used instead.

Firewall

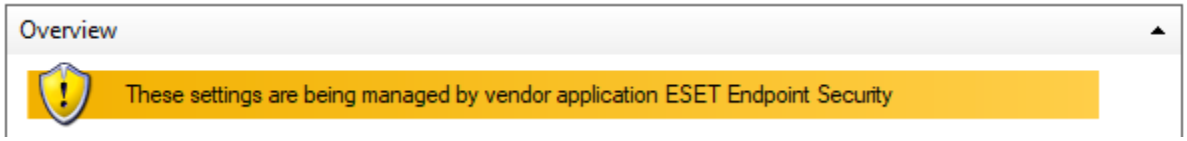
Syspeace can work with the **Windows Firewall with Advanced Security** (for Windows Server 2008 and later) or the **IP Security Policy**, a Windows component that can also block network traffic. Syspeace uses one of the two as its *blocking provider*. By default, Syspeace uses the blocking provider **Automatic**, which attempts to use the Windows Firewall but falls back to IP Security Policy if it is not available.

Windows Server 2008 and later

The built-in firewall in Windows – Windows Firewall with Advanced Security – must be running for the current network profile.



If the Windows Firewall is managed by a third-party software, as shown below, this third-party software is free to ignore Syspeace's rules.



Syspeace will attempt to detect this situation, warn and, if using the Automatic Blocking provider setting, fall back to IP Security Policy.

Windows Server 2003

Due to limitations in the version of the Windows Firewall present in Windows Server 2003, Syspeace uses the IP Security Policy to implement blocking in Windows Server 2003. The IP Security Policy subsystem must be running. Additionally, no other IP Security Policy must be assigned locally or through an Active Directory group policy.

To verify this:

1. Run "`mmc`" to open an empty instance of Microsoft Management Console.
2. Go to File → Add/Remove Snap-in…
3. Click Add…
4. Select IP Security Policy Management and click Add.
5. In the Select Computer or Domain wizard, make sure Local computer is selected and then click Finish.
6. Click Close and OK to get back to the Console Root window.
7. Select IP Security Policies on Local Computer in the tree to the left.
8. From the View menu, make sure Detail is selected.
9. If a policy named `$SYSPEACE$policy` is "assigned" (its icon has a green checkmark badge and the Policy Assigned column says "Yes"), Syspeace is already set-up.
10. If any other policy is assigned, you must first right-click and "un-assign" the policy for Syspeace to be able to work.
11. If a policy says "Policy is assigned, but it is being overridden by Active Directory-assigned policy.", you must first ensure that the group policy assigning the IP Security Policy is made not to apply to this computer.

A note about changing the IP Security Policy

As always, follow your organization's IT policy and exercise common sense. Please consult with your system administrator to make changes in the group policy or before you un-assign a local IP Security policy. If a local policy has to exist, the rules and filters can be added alongside Syspeace's rules and filters inside the `$SYSPEACE$policy`, as long as these rules and filters do not clash with the `$SYSPEACE$` prefix naming convention.

Installation

1. Download the Syspeace zip archive from the Syspeace website and unpack the two files **Setup.exe** and **Syspeace.msi**.
2. Double-click "Setup.exe" (which may show as just "Setup") to start the installation.
3. Syspeace Setup may need to install a number of dependencies before starting the Syspeace Setup Wizard. These dependencies include the Visual C++ 9.0 Redistributable, Microsoft .NET Framework 4.0 and Windows Imaging Component. *If Syspeace Setup needs to install Microsoft .NET Framework 4.0 (common among Windows Server 2003 users), you may need to reboot your server before continuing installation.*
4. Follow the Syspeace Setup Wizard to its conclusion to install Syspeace. For a detailed step-by-step, see ***Appendix A: Syspeace Setup Wizard step by step***. Please note that installation to a network drive is not supported.
5. After installing Syspeace, please launch it from the desktop or from the Start menu.

6. If you have used previous versions of Syspeace, your settings may need to be migrated. This will happen automatically and may take a few minutes.

How Syspeace works

Before we get to the settings, it may be useful to know how Syspeace works. Syspeace works by watching for evidence of intrusion attempts or attacks in various ways and then blocking the offending IP addresses.

Detectors

Syspeace has three built-in detectors: Windows login, Exchange SMTP Connector and SQL Server login.

The Windows login detector checks for Windows authentication attempts. This can be an attempt to log into a computer using Remote Desktop, an attempt to mount a shared folder or an attempt to log into Outlook Web Access or Exchange using a domain account.

The Exchange SMTP Connector detector checks for login failures in the Exchange SMTP Connector.

The SQL Server login detector checks for login failures in SQL Server.

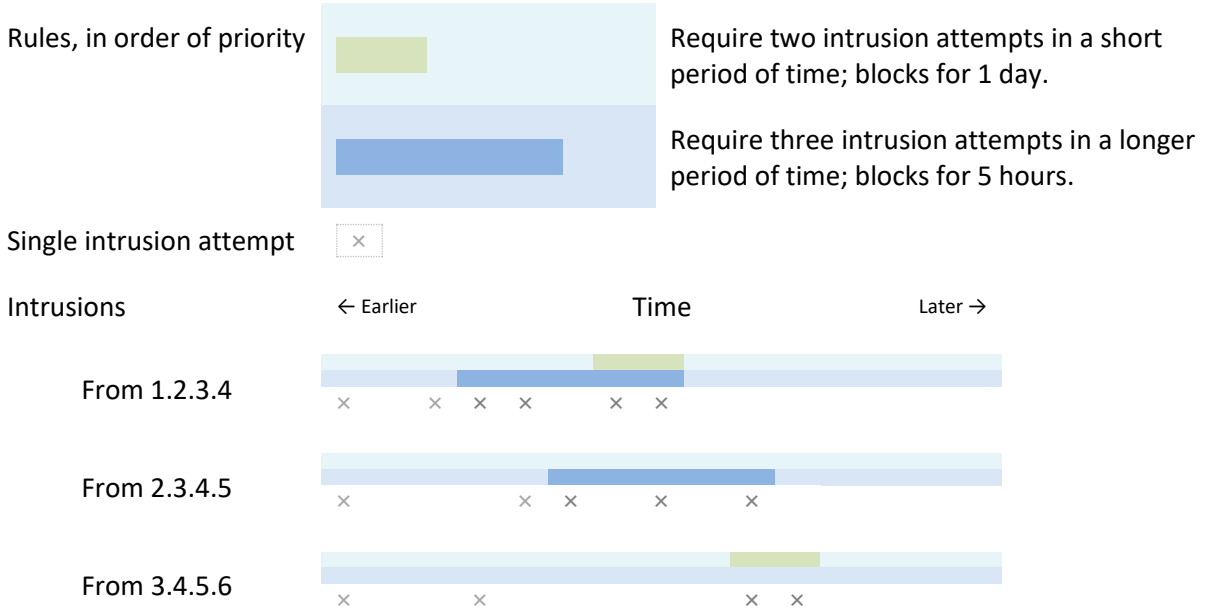
Additional detectors checking for login failures in additional places can be added to Syspeace by installing detector providers. For more information, see "Detector Provider API/SDK" on the Syspeace web site.

Each detector works similarly: based on accumulated evidence of login failures, the offending IP address is blocked for an amount of time.[1] But what decides which IP address and for how long?

Rules

Each detector has a rule system. A rule determines how many login failures are required to happen in which time period for a ban of certain duration to be issued. Additionally, the rule can be narrowed down to certain conditions. For example, a login attempt on a domain which does not exist is far less likely to be legitimate and may be punished more strictly.

Rules in action



In the example above, the attacks from 1.2.3.4 are matched by both the short rule and the long rule, while the attacks from 2.3.4.5 are only matched by the long rule. 1.2.3.4 will be blocked for a day since the short rule is higher priority than the long rule, starting from the last of the detected intrusions. 2.3.4.5 will be blocked for five hours. 3.4.5.6 is only matched by the short rule and will be blocked for a day.

Geographical blocking

Syspeace can also take the IP address's country[2] into consideration and trigger an automatic block when a login attempt is detected by one of the detectors. Syspeace uses country rules to determine which countries to block.

[1] Please note that on Windows Server 2003, the event log – the source of most detector information – has a latency of up to six seconds. This may introduce a brief delay in detecting attempts.

[2] Syspeace uses the geographical IP lookup database GeoLite2 from MaxMind, Inc. Geographical matching is subject to the accuracy of the underlying database. Known authoritative data can be entered into the "GeoIP data overrides" settings pane. Syspeace uses geographical names from the Unicode Common Locale Data Repository, which in turn uses territory containment information from the UN Statistics Division M49 standard.

Country rules are very similar to detector rules (see above). Each country rule describes which countries should be blocked, whether the block should happen on any kind of login attempt or only failed login attempts and for how long the block should last. One country rule can also be set to be an inverse rule, where the countries that should not be blocked are listed, and all other countries are blocked. Like detector rules, country rules are evaluated in order of priority and the highest priority rule is followed.

Other kinds of incoming network traffic from a country with a country rule will not trigger a country rule. However, if the country rule has been triggered, all network traffic from the blocked IP address is stopped.

Blacklists

Repeated culprits may be blocked persistently by adding their IP addresses to the local blacklist. These IP addresses will be blocked by Syspeace as long as they're on the local blacklist.

There is also a global blacklist. Every time an IP address is ordinarily blocked by Syspeace, this is reported to a Syspeace server. (No personally identifying information is sent to Syspeace.) When the Syspeace server knows that a particular IP address has been blocked by many Syspeace installations, Syspeace adds the IP address to the global blacklist. This global blacklist is distributed to all paying Syspeace users and you may opt to follow the global blacklist, thus automatically blocking these IP addresses even before you get hit.

Since attackers come and go, IP addresses change owners regularly and space is limited, the global blacklist rules are transient. The global blacklist is intended to protect against current attacks, so global blacklist entries expire within a few days to make room for new entries.

Whitelist

Syspeace also has a whitelist. You can enter IP addresses that should never be blocked into the whitelist. Even if an IP address is explicitly blocked in a global or local blacklist, including if it is contained in an IP range, it will be excused if it is whitelisted.

The loopback address 127.0.0.1 and every local IP address in every available network interface is automatically whitelisted. However, other computers within the same local network range/subnet are not.

Rule matching database

To speed up the work of the rule matching engine, Syspeace pre-calculates and keeps some information about login attempts in a database. This database will need to be set up with current data when upgrading from a pre-3.1 version of Syspeace, and the database may need to be optimized from time to time or be updated as rules are changed. When this happens, an indicator is shown in the main window and in the ***Rules → General*** pane.

Syspeace licensing

Syspeace requires every server it runs on to be licensed. To use Syspeace, you must register a Syspeace account with your email address and a password.

Once your account has been set up, you will receive a license key, which will not change as long as you keep the same account. One or more individual licenses may be associated with your account, giving one or more servers the right to run Syspeace during a period of time. Licenses are purchased from your reseller or the Syspeace Licenses site.

One account…	…can contain many and different licenses	
Account	**License**	**License**
syspeacecustomer@example.org	4 servers	2 servers
License key: XABC	From 2020-09-01 to 2020-12-31	From 2021-01-01 to 2021-12-31

When you give Syspeace your license key, you are telling it from which account it should attempt to find a license for the server. (For this reason, you should keep your license key private, or risk other Syspeace users using your license key and depleting your licenses.) Syspeace will continuously attempt to "check out" the right to use a license for the server. This means that you will not need to reconfigure Syspeace with a new license key after purchasing licenses.

One license…	…can be used by many servers	
License	**License right**	**License right**
4 servers	Server: SERVER-EMAIL	Server: SERVER-WEB
From 2020-09-01 to 2020-12-31	From 2020-09-01 to 2020-09-04	From 2020-09-01 to 2020-09-04

As license rights are only checked out for a brief period of time and not the duration of the entire license, you may swap servers during the license duration – the license is "floating". You can manually revoke a license right to free it up for another server by logging into the Syspeace Licenses site at https://license.syspeace.com/ with your Syspeace account.

If Syspeace at any point is unable to find a current license, the server gets a 30 day trial and grace period. Once this period is over, Syspeace will stop. If the correct report has been set up, Syspeace will warn in the days before license expiration.

Current information about the license status of a particular server is always visible in the Syspeace client's status bar. Information about all licenses in an account is available from the Syspeace Licenses site.

Remote Status

Remote Status is a way to view the status of one or more Syspeace services with another application called **Syspeace Remote Status Console**. For this to work, Syspeace needs to report its current status.

Remote Status is optional and needs to be enabled in Syspeace. (See the ***Management → System settings*** pane.) It provides a way of viewing remote status; it does not provide full management capabilities.

Remote Status information is sent to a Relay server, a server which relays information from Syspeace services to any currently running Consoles. The information is encrypted and not visible to the host of the server. By default, this server is a common server hosted by Treetop Innovation AB, the makers of Syspeace. Remote Status supports using another Relay server than the default server. Please contact Syspeace support for information about setting up your own Relay server.

For more information about Remote Status, see these separate documents, available on the Syspeace web site:

- **Getting Started with Remote Status** for information about using Remote Status.
- **Syspeace Remote Status Architecture** for detailed technical information (not required to use Remote Status).

Deploying Syspeace

Syspeace can be automatically and remotely deployed by using a deployment tool to run the .msi Windows Installer package. Combined with settings files, Syspeace can be deployed and configured without manual intervention.

For more information and detailed instructions, see:

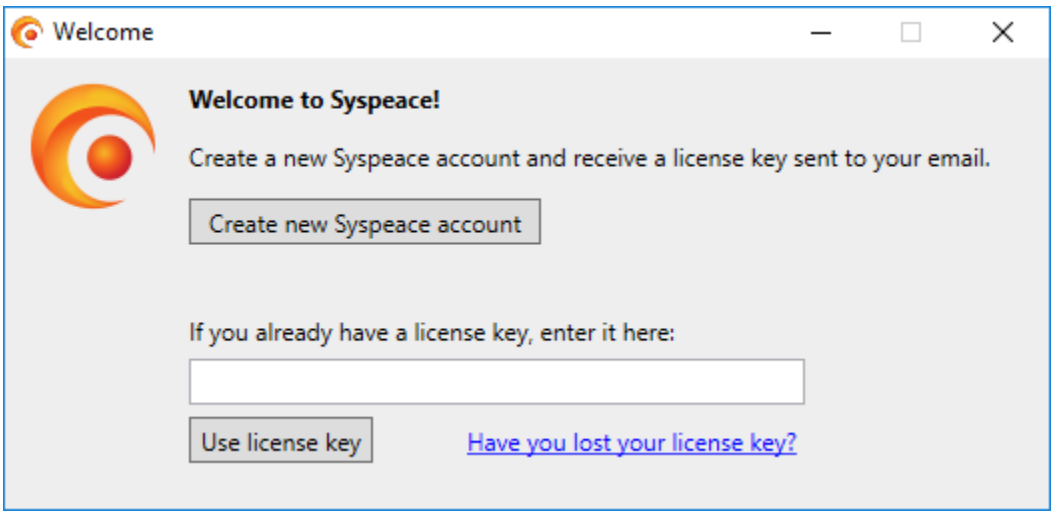
- The separate **Deploying Syspeace** document, available on the Syspeace web site.

Configure Syspeace

Before using Syspeace, you will need to configure it.

Licensing and the Welcome window

Syspeace needs an appropriate *license* to run on a server. These licenses are purchased online and grouped together in an account with a common license key. (The license key itself does not confer one or more licenses; it is just a way to specify a Syspeace account which may have active licenses.) Every new server gets a free 30 day trial.



The welcome screen lets you create a Syspeace account or enter a license key.

Using an existing account and license key

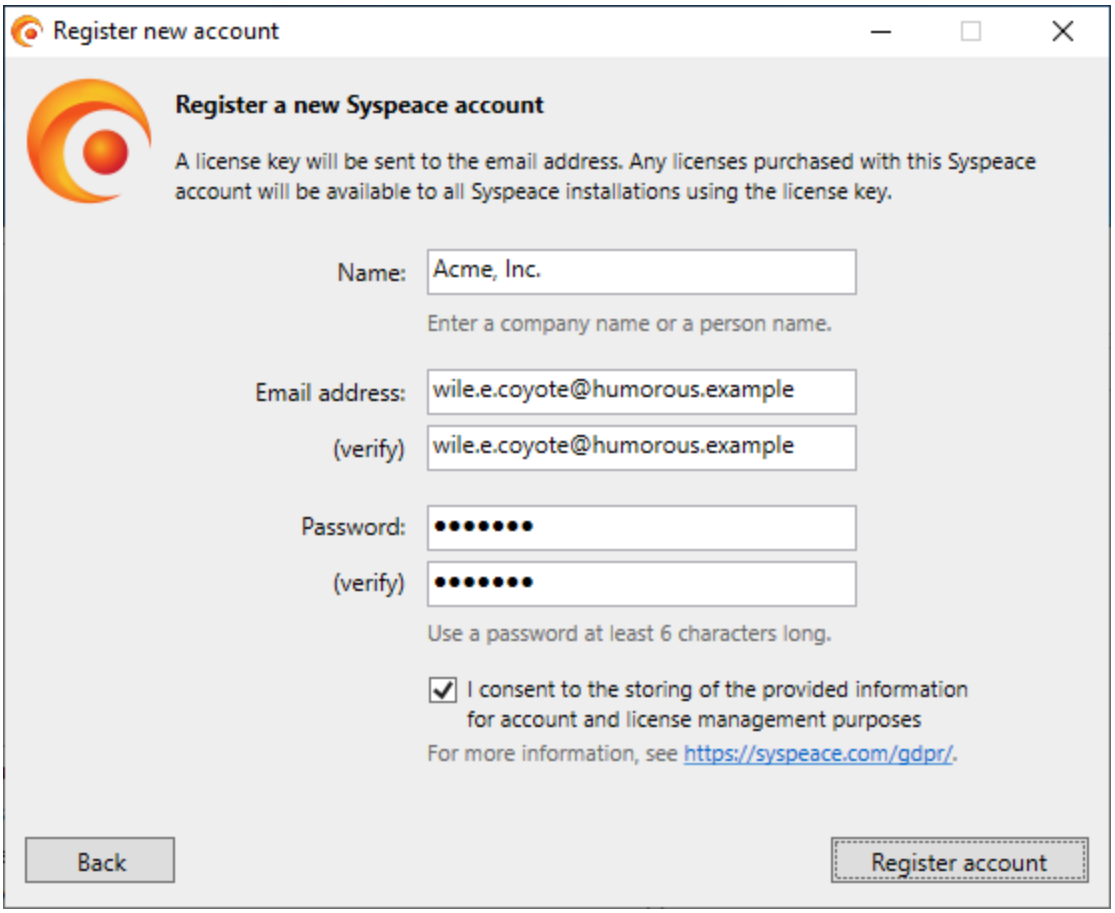
Locate your account's license key. You may click the **Have you lost your license key?** link to have it sent to your Syspeace account email. When you have your license key, paste it or enter it manually into the text box and click **Use license key** to continue.

Registering a new account and license key

Push the **Create new Syspeace account** button. Fill out the form with the appropriate details, then click **Register account**.

The **Name** field should be filled out with your company name or your own name, as is appropriate.
The license key will be sent to the **email address** you enter.
The **password** will be used, along with the email address, to log in to the Syspeace Licenses web. It must be at least six characters long.

All fields are required. Your email address cannot be re-used for another Syspeace account.



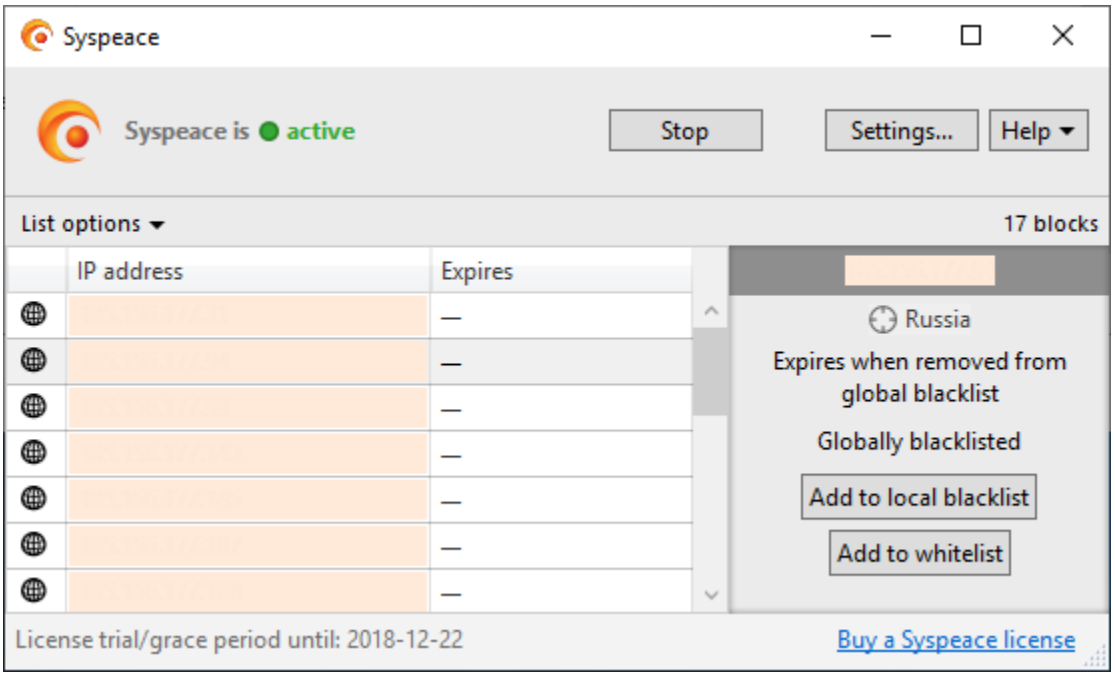
You must also check the checkbox to consent to the storing of the provided information for account and license management purposes. For more information, see https://syspeace.com/gdpr/.

Receiving the license key

After registering, you will receive an email message with the license key. Enter this into the text box in the welcome window and push **Use license key**.

Main window

When the license key has been activated, the main window will appear. The main window shows a few important pieces of information.



The main window and the Settings window reachable from the **Settings** button make up the visible part of Syspeace, the **Syspeace client**. This is where you observe the current status and make changes to the configuration.

The other part of Syspeace is a **service** that continuously runs in the background. This part is the one that actually detects attacks and intrusion attempts. It needs to be running for Syspeace to work.

After configuring Syspeace the first time, the service will start automatically. However, if the service is stopped manually, you must start Syspeace from the main window by pushing **Start** or from the Services control panel.

When Syspeace is active, the Start button changes to a **Stop** button. Exiting the Syspeace client will not stop the service and stopping the service will not exit the client.

The first time you start Syspeace up, it will immediately add blocks from the Global blacklist. For more information, see the section on *IP lists → Global Blacklist*.

The current Syspeace status is visible to the left of the Start/Stop button.

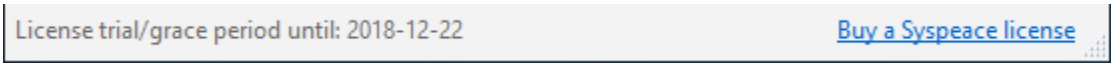
Syspeace status	What it means
Inactive	The Syspeace service is not running. Syspeace is not protecting your server.
Starting up	The Syspeace service is running and is getting ready.
Active	The Syspeace service is running and protecting your server.

Help, including this manual and the About box, is reachable from the **Help** button.

When Syspeace blocks an IP address or when it is blocked due to its inclusion in the Global blacklist or your own Local blacklist, it will appear in the list in the main window. Syspeace's blocks will always show up, but you can hide blacklist-based blocks or Country rule blocks using the menu **List options** above the list. Select an IP address to see more information or to add to a whitelist or blacklist, remove a blacklist block from the blacklist or forgive a block.

If Syspeace is busy updating the rule matching database, the "Updating rule matching database" link will be shown above the list to indicate this.

License information is shown in the status bar at the bottom of the window.



You may click the link to navigate to the Syspeace Licenses site to purchase licenses.

Main window notices

The main window may show two notices in the area to the left of the Stop button.

Notice	What it means
Dry run	Syspeace is currently set to use the blocking provider "Dry run", which runs Syspeace as usual except for setting the blocks in a firewall. This is meant for evaluating what Syspeace would block, and the notice is to remind you to not leave it on. For more information, see the ***Management → System settings*** pane.
RDP IP	Syspeace is running on a version of Windows Server where you could benefit from turning on enhanced detection of Remote Desktop/Terminal Services login failures. If this is not necessary, this notice can be hidden. For more information, see the ***Rules → General*** pane.

IP links

In many places across Syspeace where an IP is presented, it is shown in green text with a dashed underline, like so. Clicking this link shows basic information about the IP as well as actions to add to/remove from the local blacklist and add to the whitelist.

Using a settings file to configure Syspeace

Syspeace can use a settings file to configure settings and which Syspeace license to use. To produce the settings file, use the ***Management → Export settings*** pane.

Using the settings file

The following steps all require a **defaultSettings.syspeaceSettings** file produced by the Export Settings pane.

To use the settings file to configure initial settings and/or set a license key:

- To adopt the license key, Syspeace must not have a current license (the Welcome window shows up when it starts). Syspeace must either be…
    - …freshly installed and not have a license yet, or
    - …the Reset license button in the License settings pane must just have been used.

1. Install Syspeace, if needed.
2. Exit Syspeace if it is running.
3. Place the defaultSettings.syspeaceSettings file in the folder Syspeace was installed into (by default **C:\Program Files\Treetop\Syspeace**).
4. Start the Syspeace client (not the service).
5. Syspeace will automatically be configured to use the license key.
6. Syspeace will adopt the settings in the settings file.

To use the settings file to reconfigure settings:

1. Stop the Syspeace service using the Stop button.
2. Place the defaultSettings.syspeaceSettings file in the folder Syspeace was installed into (by default **C:\Program Files\Treetop\Syspeace**).
3. Start Syspeace using the Start button.
4. Syspeace will adopt the settings in the settings file.

- Syspeace will not change to the license key contained in the settings file.

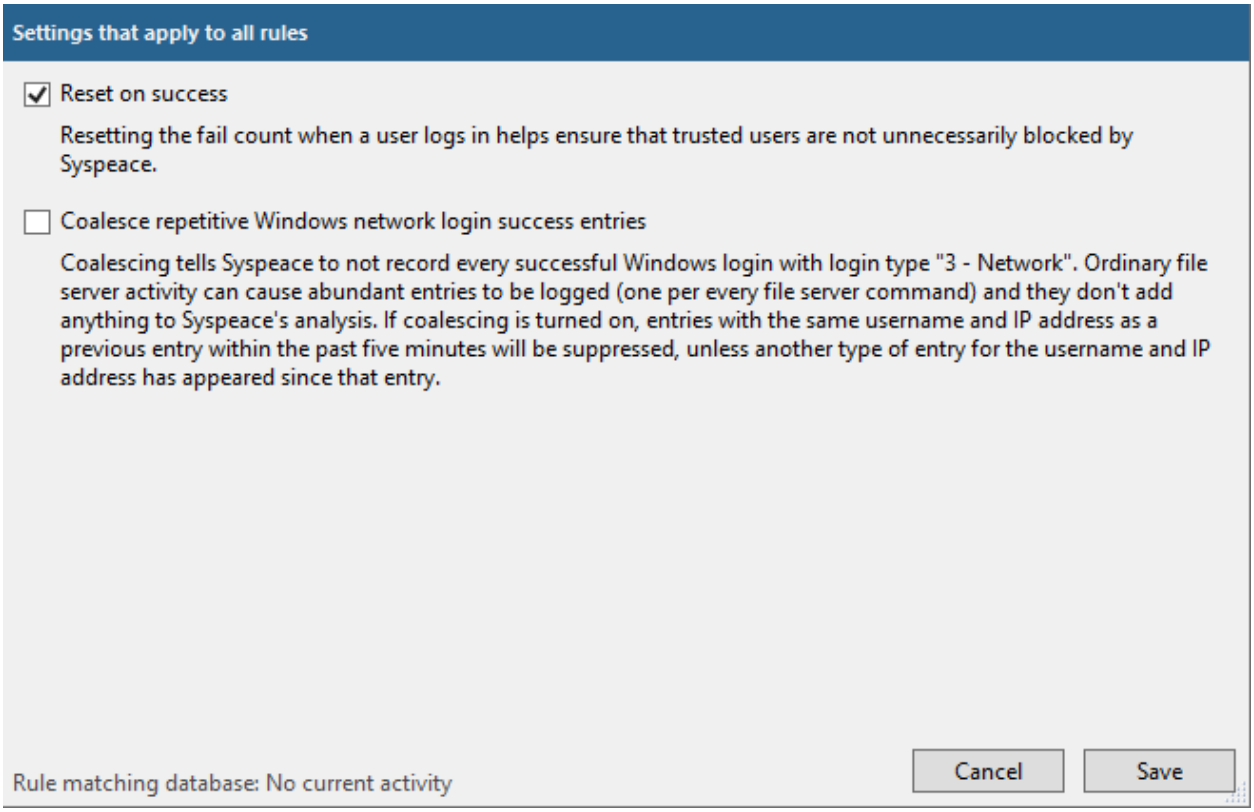
If settings are changed manually after the settings file is applied, the changes will persist. If a new settings file is provided, the settings will be reset to the settings in the new settings file.

Syspeace settings

The left side of the Settings window consists of a list of panels. Each panel has one or more settings that can be tweaked in order to specify the behavior of the service.

Some panels have colored badges with numbers in them. The dark badges signal how many rules are currently enabled; if there are no rules (0), the protection is currently not in effect and the badge is gray. The bright badges signal the number of entries in an IP list, or how many blocks are in effect. If a panel name is struck through (~~like so~~), it is not supported on the current Windows Server version.

Rules → General



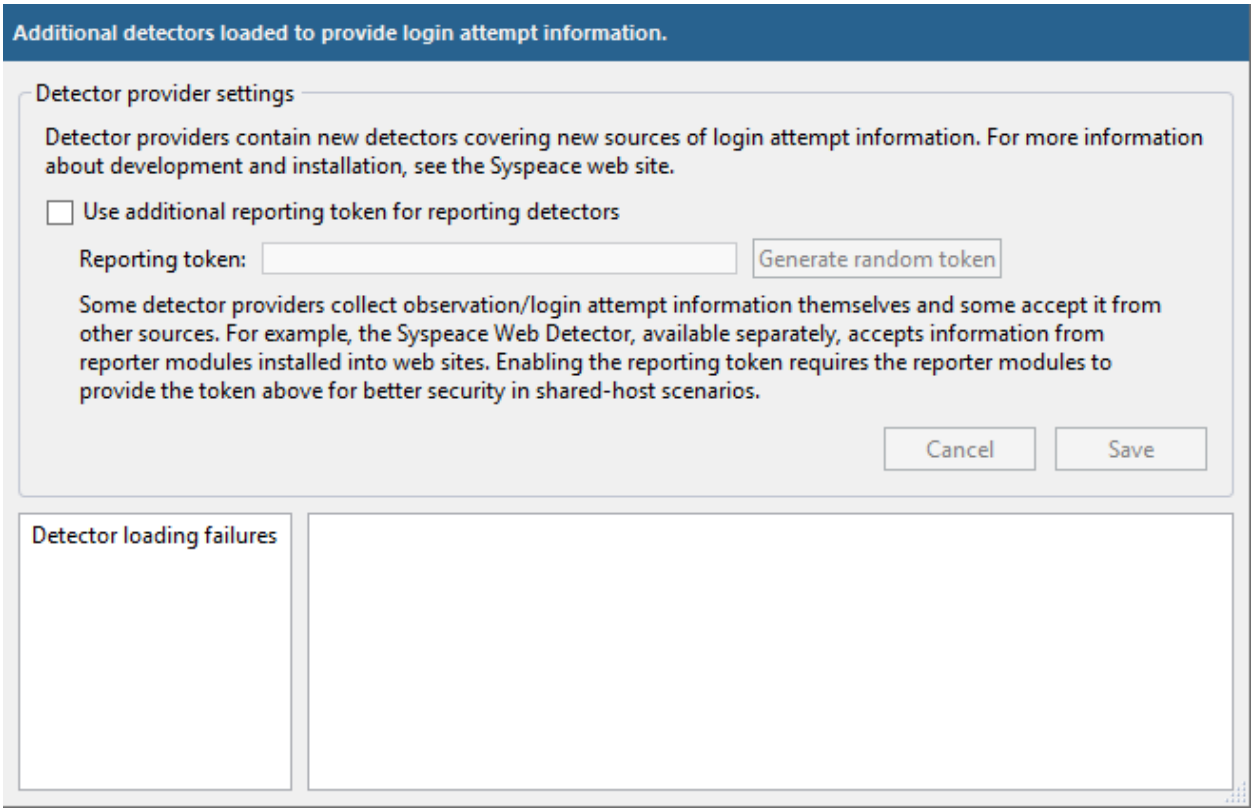
The **Reset on success** setting changes how rule matching works. If an IP address with failed logins makes a successful login, the failed logins are stricken from the record as if the failed logins were never attempted.

The **Coalesce repetitive Windows network login success entries** setting filters out repetitive "success" login entries issued by file servers on every file operation. Enable this if there are a lot of successful logins when users browse the file shares on this server.

The **Traffic-based Remote Desktop/Terminal Services IP detection** setting turns on enhanced detection to make sure the IP address is recorded for Remote Desktop/Terminal Services login failures. This detection affects network throughput and should not be enabled if the server does not host Remote Desktop/Terminal Services traffic. It requires the port used for RDP to be correctly configured in the **RDP port** field. If this setting is available but not enabled, Syspeace shows a notice in the main window. If it does not need to be enabled, you can check the Don't show checkbox to acknowledge and hide the notice.

> *This setting is only available on Windows Server 2008, 2008 R2, 2012 or 2012 R2.* For more information about this issue, please see the section ***Enabling Remote Desktop/Terminal Services detection***.

Rules → Detectors

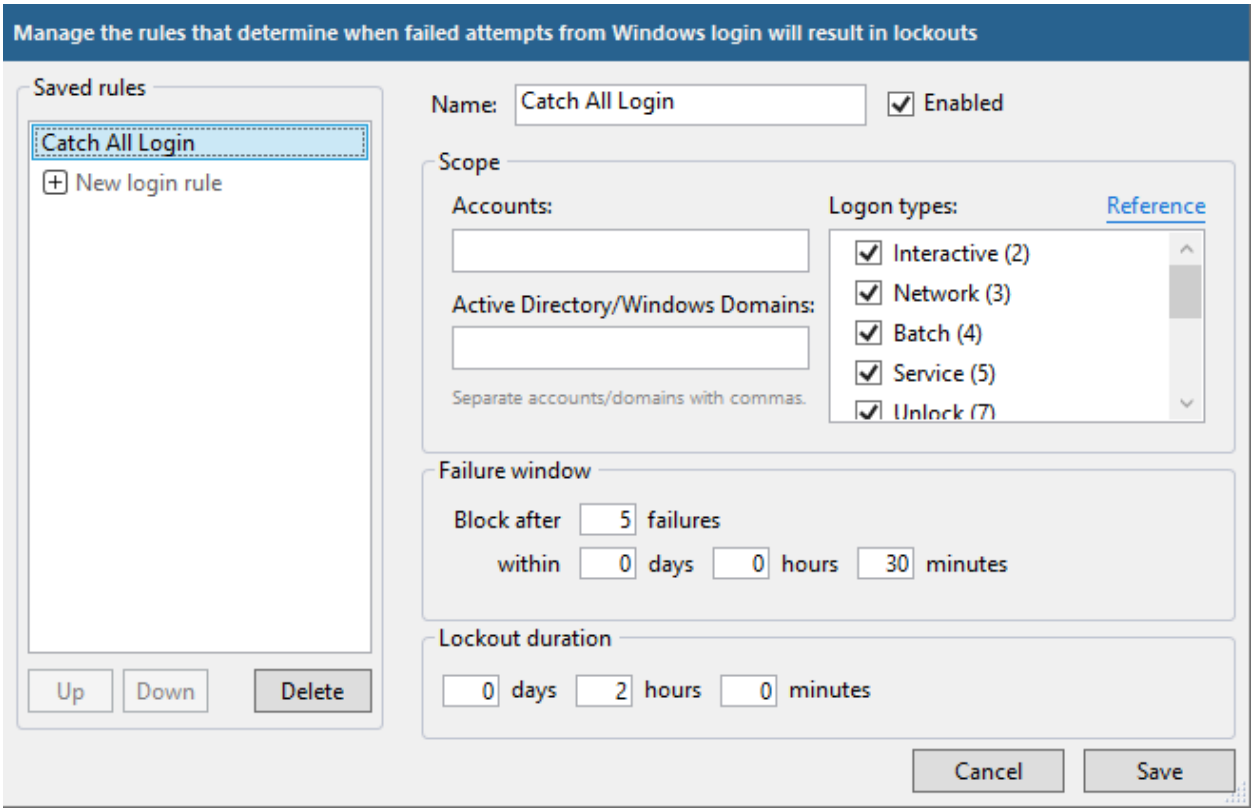


The Detectors panel lists the additional detectors loaded by Syspeace from detector providers, beyond the built-in detectors. For more information about detector providers, please see the Syspeace web site.

Logs from the detector providers, as well as logs regarding failures loading a detector, are shown in the bottom half of this panel.

Detector providers may require cooperation with “reporters” installed into other software to receive information about login attempts. If other unrelated software is running on the same server, it would be able to report incorrect information through the same channel. A **reporting token** may be enabled and required of the reporters by checking the box **Use additional reporting token for reporting detectors** and filling out the **Reporting token** text field, or clicking the **Generate random token** button. Login attempt information reported with an incorrect reporting token will be silently ignored.

Rules → Rules settings panels for detectors



These rules govern how failed logins will be treated. (For more information, see ***How Syspeace works***.) One panel appears for every detector available. If detector providers load additional detectors besides the detectors built into Syspeace, every built-in detector will have a small Syspeace logo next to it in the settings panel list for identification.

By default, a "Catch All Login" rule will block intruders that fail to log in after a small number of attempts within a short amount of time and block them for two hours. (The exact settings will depend on the detector.) This rule is not a special rule and may be deleted or changed like any other rule. *Note that if all rules are removed, Syspeace will no longer offer any protection, since there is nothing left to define when to start blocking an intruder and for how long.*

To edit a rule, select it in the **Saved rules** list to the left. Then change the properties of the rule to the right and click **Save**. To discard changes made to the rule, click **Cancel**.

The following properties are available:

Property	Description	Default value
Name	The rule's name.	Nothing
Enabled	Whether the rule is enabled.	Yes
Failure window	How many failures to require within what period of time.	5 failures within 30 minutes
Lockout duration	For how long to block the intruder.	2 hours

Scope	Options for Windows login rules	
Accounts	If not empty, the login names of one or more Windows accounts to match. (Separate many names with commas.) For example: “Administrator,Economy”	Empty
Active Directory/Windows Domains	If not empty, the names of one or more Windows domains to match. (Separate many domain names with commas.)	Empty
Logon types	The login method used. Click the adjacent Reference link to see an explanation.	All logon types
Scope	**Options for Exchange SMTP rules**	
Limit to receive connectors	If not empty, the names of the SMTP connectors to match. Add connectors with the text field and the Add button. Remove connectors with the Remove button.	No connectors
Scope	**Options for SQL Server rules**	
Accounts	If not empty, the login names of one or more Windows or SQL Server accounts to match. (Separate many names with commas.) For example: “Administrator,Economy”	Empty

Rules are evaluated from top to bottom. The first rule to match will determine the lockout duration. Rules can be reordered by selecting one rule and using the **Up** and **Down** buttons.

To delete a rule, select the rule and use the **Delete** button.

To create a new rule, select the **New login rule** row in the **Saved rules** list and edit the rule as usual. Click **Save** to finish creating the rule.

The Exchange SMTP detector

Running an Exchange server, you might have Connectors that enable relaying. With this enabled, you must certainly require an account for the SMTP connection so that the applications that need to send mail have to log in.

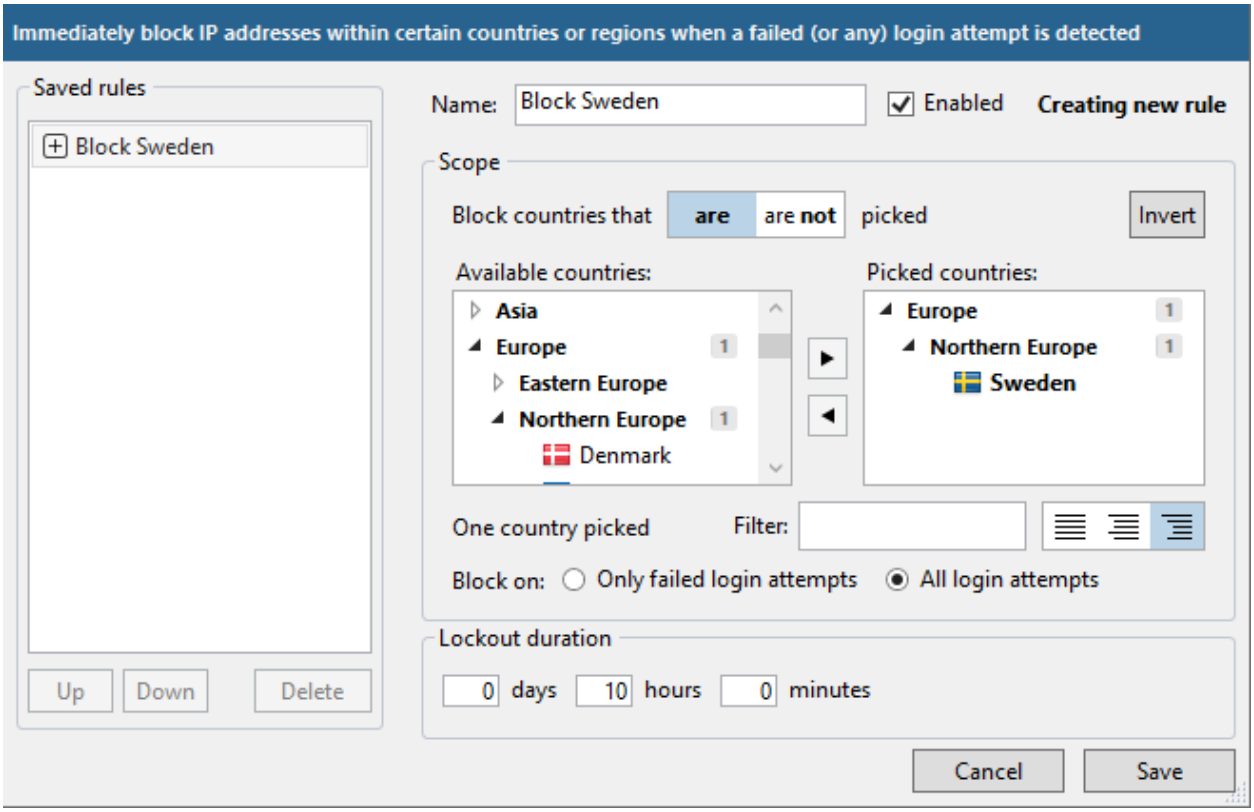
As is the case with Windows authentication, others may try to gain access to the connector to send email. Syspeace offers similar protections. Support for Exchange SMTP connectors is unavailable in Windows Server 2003.

The SQL Server detector

SQL Server login failures can be detected just like Windows login failures.

A default “catch all” rule is created during installation but is disabled. Out of the box, SQL Server login blocking may be counter-productive for reasons outlined in the earlier section ***Manual configuration of SQL Server login detection after installation***, which you should review before enabling SQL Server support by creating a rule manually or enabling the default rule.

Rules → Country rules



These rules govern Syspeace's geographical blocking. If a rule includes a country, users determined to be from that country will be blocked as soon as soon a failed or successful login attempt is detected. (For more information, see ***How Syspeace works***.) By default, Syspeace provides no such rules.

To edit a rule, select it in the **Saved rules** list to the left. Then change the properties of the rule to the right and click **Save**. To discard changes made to the rule, click **Cancel**.

A rule can be inclusive (block the countries listed) or exclusive (block every country not listed). Use the mode button to choose between "Block countries that **are** picked" (inclusive) or "Block countries that are **not** picked" (exclusive). Only one exclusive rule is allowed at any given time since the consequence of two exclusive rules that are not identical is to block all countries.

Using the lists **Available countries** and **Picked countries**, pick the countries to include in the rule. To pick a country, select it in **Available countries** and use the ▸ button to transfer it to the **Picked countries** list.

Both lists can be shown as flat lists, grouped by continents or grouped by continents and subgroups (the default). Change this mode by using the mode button below the Picked countries list. In any mode with groups, a grey badge to the right of a group name shows how many countries contained in the group are picked. The badge is progressively filled towards the right with a darker grey as more and more countries are picked.

Use the **Filter** text box to filter both lists to more easily find a country.

Use the **Invert** button, if necessary, to pick every country that isn't currently picked, and vice versa.

Apart from the list of countries and the rule mode, the following properties are available:

Property	Description	Default value
Name	The rule's name.	Nothing
Enabled	Whether the rule is enabled.	Yes
Block on	Whether to block immediately on any kind of login attempt or only failed login attempts.	Only failed
Lockout duration	For how long to block the intruder.	2 hours

Rules are evaluated from top to bottom. The first rule to match will determine the lockout duration. Rules can be reordered by selecting one rule and using the **Up** and **Down** buttons.

To delete a rule, select the rule and use the **Delete** button.

To create a new rule, select the **New rule** row in the **Saved rules** list and edit the rule as usual. Click **Save** to finish creating the rule.

IP lists

The local blacklist and local whitelist accept these IP address/range syntaxes:

Variant	Example	Contains
Single IP address	1.2.3.4	The single IP address 1.2.3.4.
IP range	1.2.3.4-1.2.3.80	Every IP address in-between 1.2.3.4 and 1.2.3.80 inclusive. Backwards ranges (2.2.2.2-1.1.1.1) are not valid since they may be indicative of typing errors. They can be entered by simply placing the numerically larger IP address last.
IP mask, CIDR notation	1.2.3.0/24	Every IP address with the first 24 bits equal to the first 24 bits of 1.2.3.0 (1.2.3.0-1.2.3.255)

IP address import text format

This format is used to import into the local blacklist.

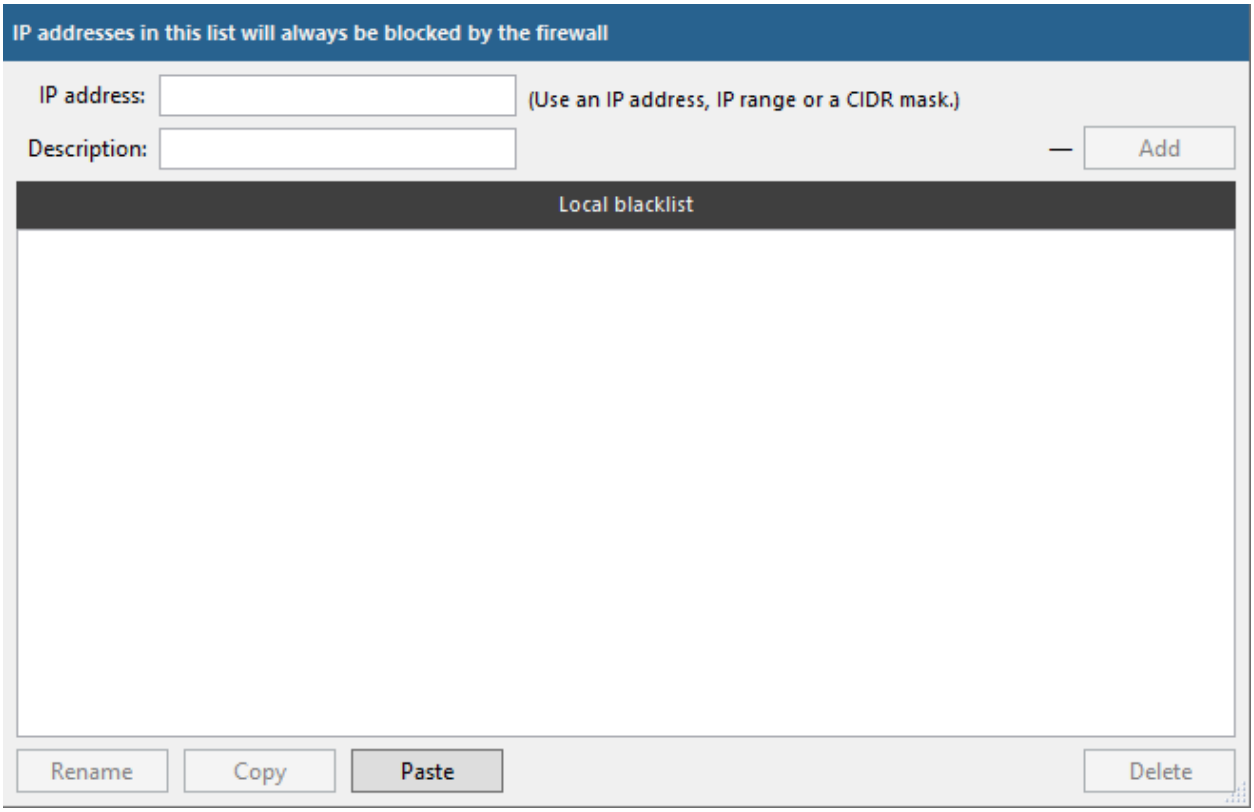
- One IP address/range (with the above syntax) per line.
- Optionally, at the end of each line, a separator followed by a description of the address/range.
  - The separator may be either:
    - a tab
    - a semicolon “**;**”
    - a comma “**,**”
    - or a space.
  - The separator must be the same for all lines.
- Lines that are empty, contain only whitespace or start with a “#” are ignored.

For example:

```
# blacklist for import
# updated 2020-..-..

1.2.3.4
2.2.2.2-2.2.2.8;Range
2.4.8.16/28;CIDR range
```

IP lists → Local Blacklist



Every IP address entered in the local blacklist will be blocked indefinitely. (For more information, see ***How Syspeace works***.)

Enter an IP address or range, add a description if necessary and click **Add** to add it to the blacklist.

Select an IP address or range in the list and click **Delete** to remove it from the blacklist, or click **Rename** to change its description.

Exporting from the local blacklist by copying

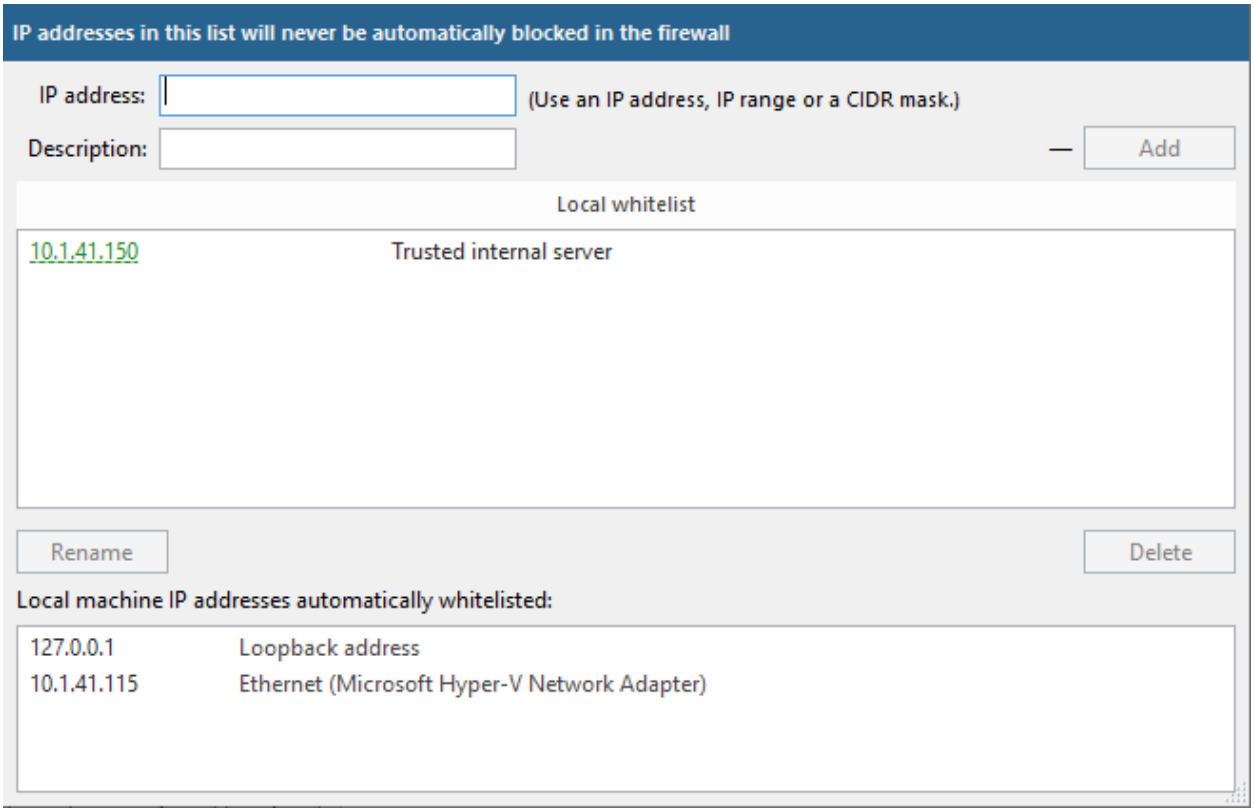
You can export the entire local blacklist with ***Management → Export settings***.

You can also select one or more items and copy them using **Ctrl+C** or the **Copy** button. They are exported in a tab-separated format that is compatible with the ***IP address import text format***.

Importing to the local blacklist by pasting

You can import new local blacklist entries by copying text in the ***IP address import text format*** and using the **Paste** button.

IP lists → Local Whitelist



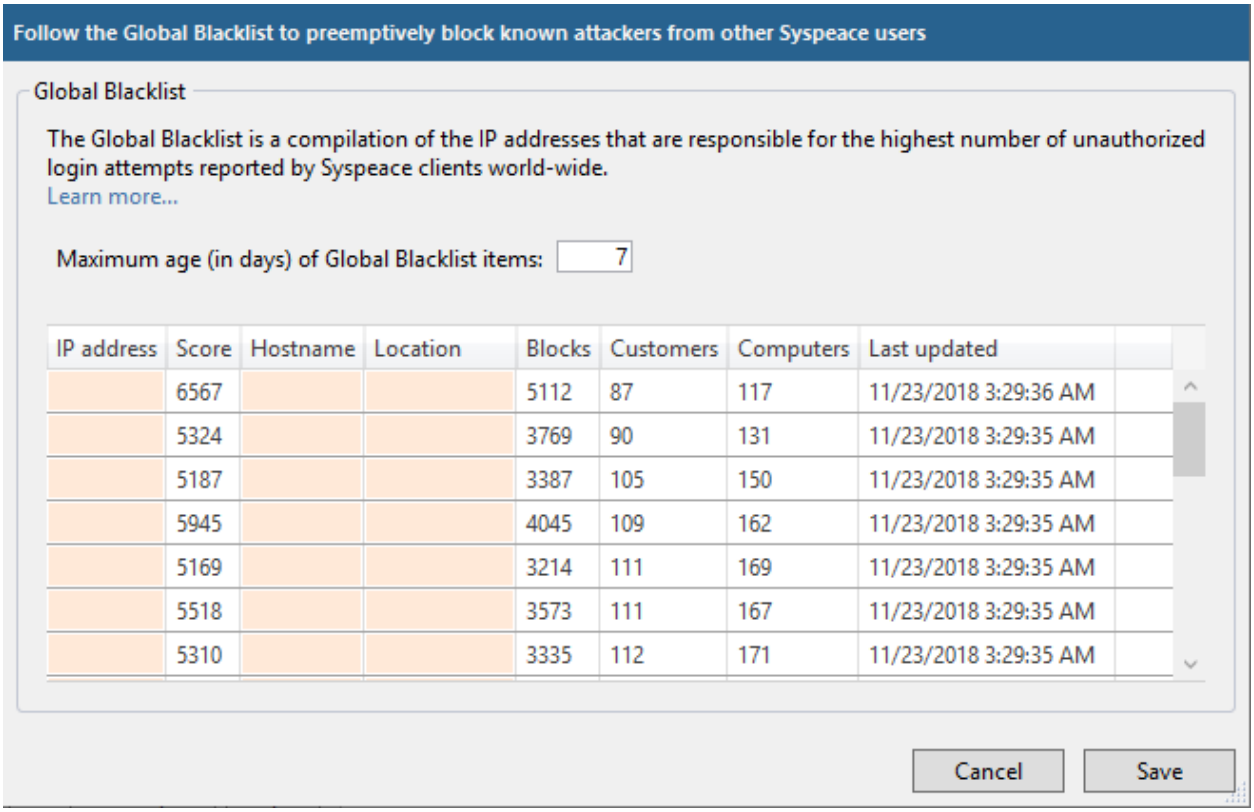
Every IP address entered in the local whitelist will be exempt from blocks, even from being in a blacklist. (For more information, see ***How Syspeace works***.)

Enter an IP address or range, add a description if necessary and click **Add** to add it to the whitelist.

Select an IP address or range in the list and click **Delete** to remove it from the whitelist, or click **Rename** to change its description.

The loopback/local machine IP addresses for every active network interface will be whitelisted at all times. They are listed in the **Local machine IP addresses automatically whitelisted** list along with the corresponding network interface.

IP lists → Global Blacklist



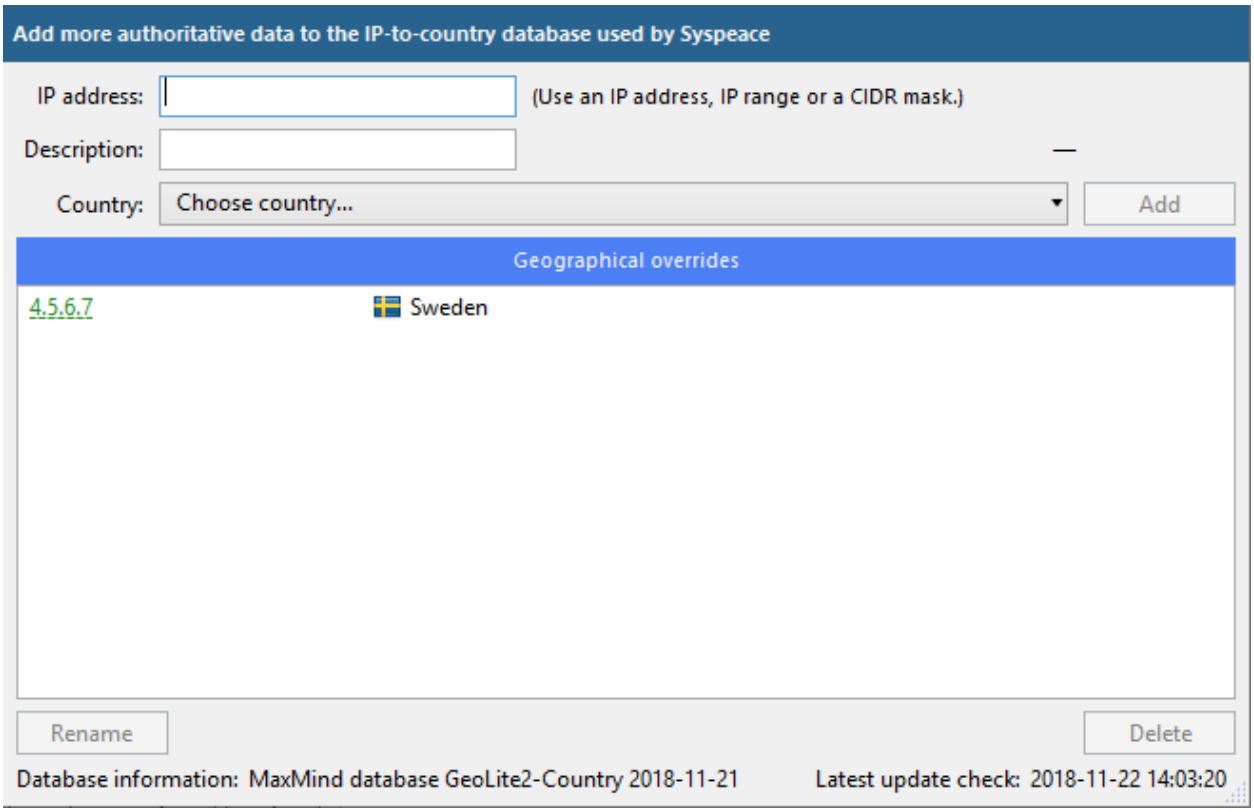
The Global Blacklist is maintained by Syspeace servers and tracks the most common, widespread or insistent recent attackers across every Syspeace installation worldwide. When an IP address enters the Global Blacklist, it will preemptively be blocked by Syspeace if Syspeace is set to follow the Global Blacklist. Syspeace updates the Global Blacklist daily. (For more information, see ***How Syspeace works***.)

The Global Blacklist is effective against current attacks as they happen. For this reason, you can keep a number of days of Global Blacklist items to follow. Set this number to 0 to disable the Global Blacklist. As you change the number of days, the table listing the current known Global Blacklist will dim, showing which items will not be included. When you are done, click **Save** to save the setting or **Cancel** to revert.

Column	Description
IP address	The IP address that will be blocked.
Score	A severity indicator. Calculated as: *number of affected customers* × 10 + *number of computers* × 5 + *number of blocks*
Hostname	The hostname, as determined by a reverse DNS lookup on the IP address.
Location	The geographic location of the IP address, if known.
Blocks	The total number of times this IP address has been blocked across all of Syspeace's customers.
Customers	The total number of customers (Syspeace accounts) that have blocked this IP address.

Computers	The total number of computers that have blocked this IP address.
Last updated	When this item was last updated.

IP lists → GeoIP data overrides



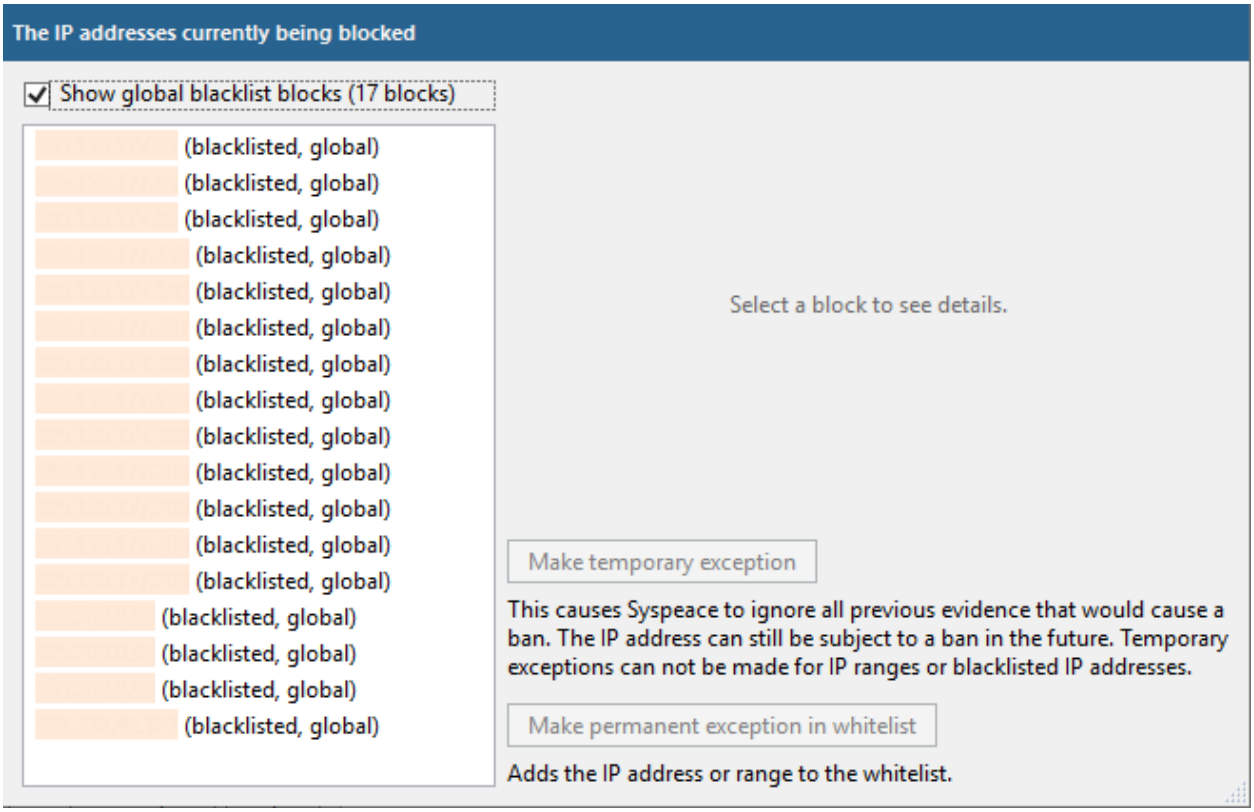
GeoIP data is used to map an IP address to a country. If you have authoritative data for where an IP address or IP range is located, you can enter it here. (Note that overrides are not effective retroactively and will not undo any blocks resulting from Country rules.)

Enter an IP address or range, add a description if necessary, choose a country by clicking **Choose country…**, selecting a country and clicking **Choose**, and click **Add** to add this data to the overrides.

Select an IP address or range in the list and click **Delete** to remove it from the overrides, or click **Rename** to change its description.

At the bottom, the current version of the IP address-to-country database and the date of the latest update check are listed. Syspeace automatically performs a recurring check for updates to the database and upgrades to a new database when necessary.

Blocks and Analysis → Live blocks



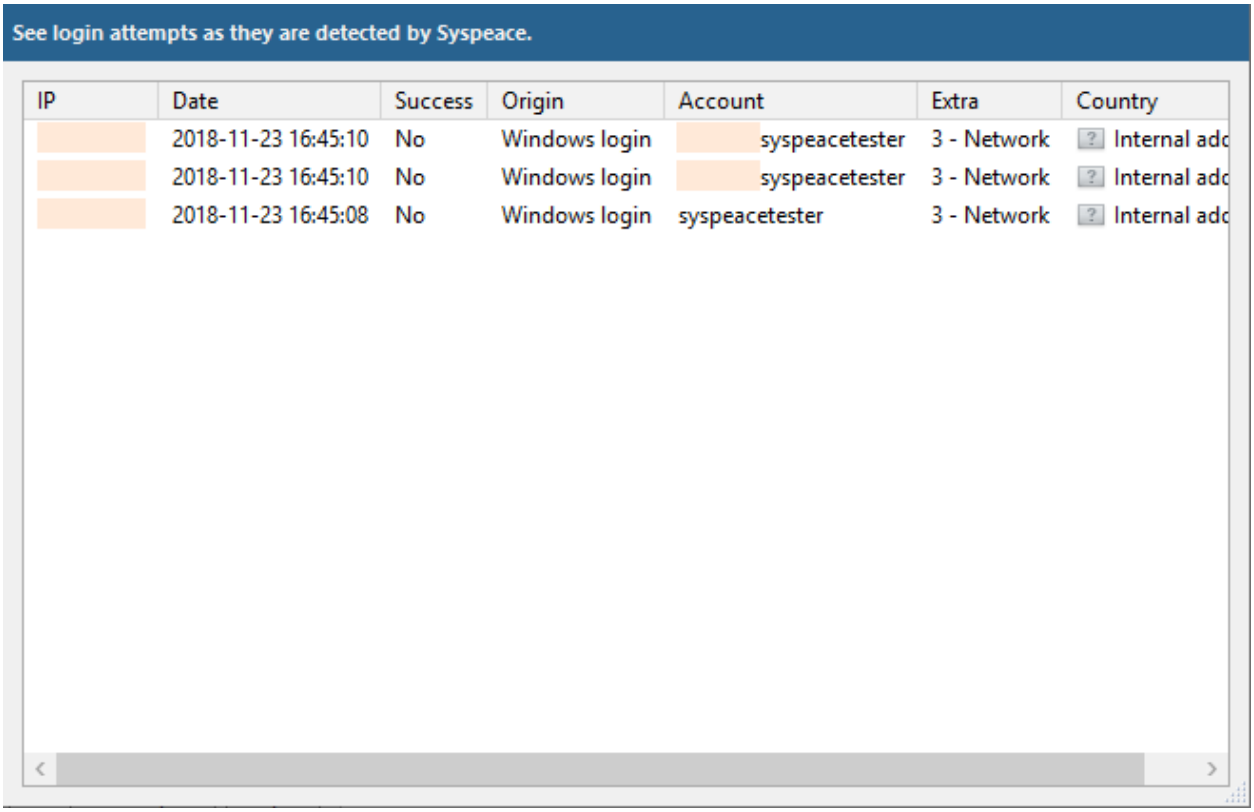
The live blocks panel shows the currently active blocks. (The screenshot has been altered to remove any addresses.)

When a block is selected, the reason for the block is shown to the right, including detected intrusion attempts. Global blacklist blocks are hidden by default, but may be shown by checking **Show global blacklist blocks**.

Non-blacklisted blocks can be temporarily reset by selecting a block and pushing **Make temporary exception**. This makes Syspeace disregard all previous evidence to a block. If the IP address “earns” a block again, it will be blocked again.

Any block can be added to the whitelist by selecting it and pushing **Make permanent exception in whitelist**. This should be used with caution as this exception does not expire and as the affected IP addresses will be unable to be blocked until removed from the whitelist.

Blocks and Analysis → Live observations

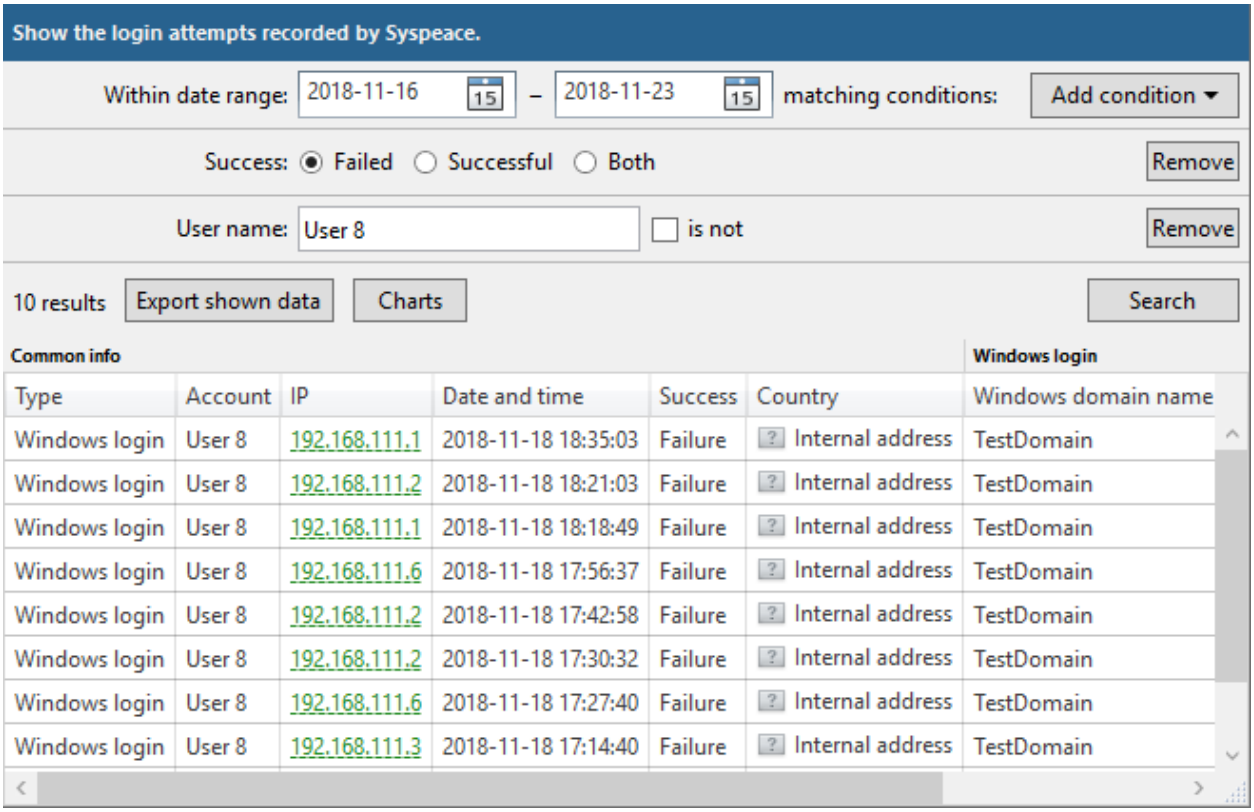


The live observations panel shows login attempts as they are detected by Syspeace.

The login attempts shown are only the login attempts that have arrived in Syspeace since the settings window was opened. Login attempts detected by Syspeace before the settings window was opened are not listed.

At most 35 login attempts are shown. When more login attempts arrive, older login attempts are dropped.

Blocks and Analysis → Access log



Access log shows the login attempts recorded by Syspeace. These attempts are stored as part of Syspeace's operation and may be informative to understand why a block has been made. Login attempts will not be retained for more than six months, so this is not an archival system.

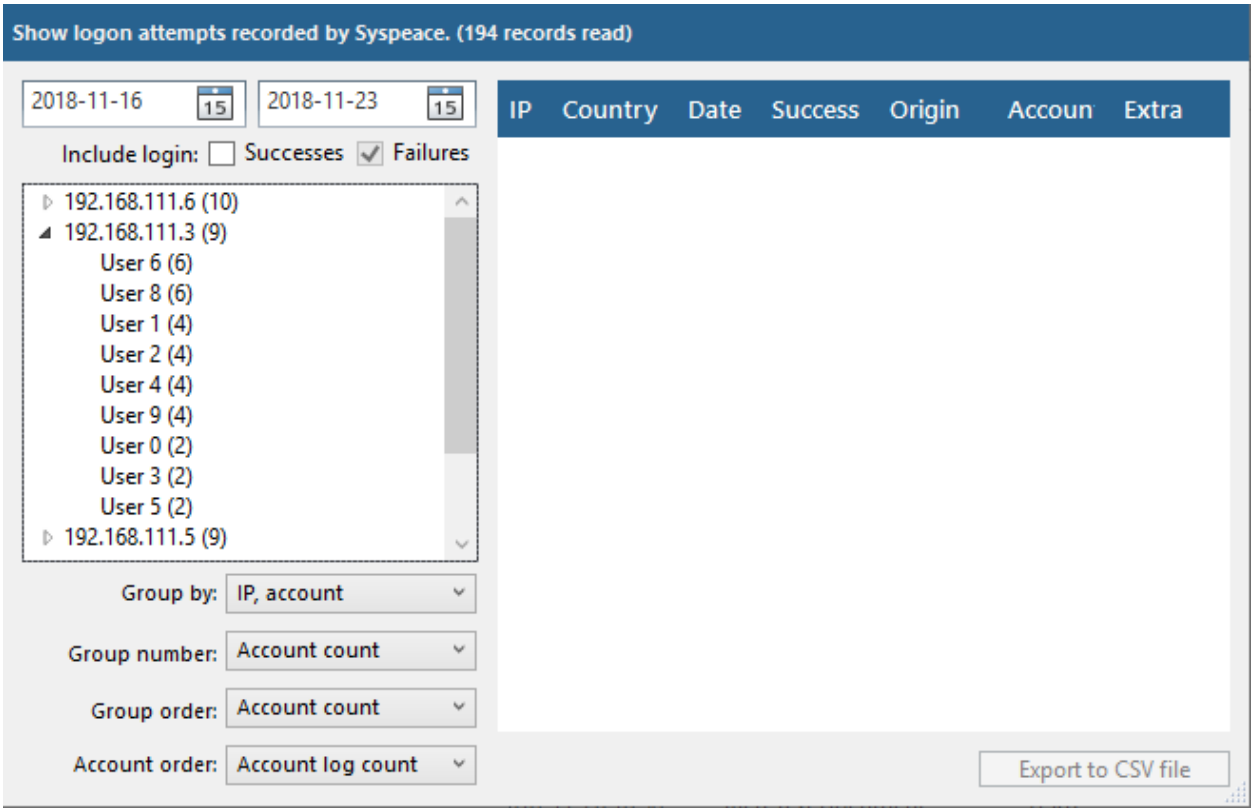
Beyond choosing a date range and clicking **Search** to show the login attempts in that range, conditions can be added to narrow down the search. For example, the screenshot shows a Success condition (provided by default to narrow the search down to failed logins). More conditions can be added from the **Add condition** button's menu. For example, the User name condition has been added in the screenshot and set up to match users that do not have the user name "User 8". Individual conditions can be removed with their respective **Remove** button.

Syspeace disables adding conditions that will be incompatible, such as searching for a Windows logon type and also for an SMTP connector, since no login attempt will have both of these filled in.

The login attempts shown in the list can be exported to a CSV file by clicking Export shown data.

Histograms describing the distribution across days in the month, weekdays and hours of the day can be shown by clicking **Charts**. When viewing the charts, click **Back to the data** to return to the list.

Blocks and Analysis → Access report



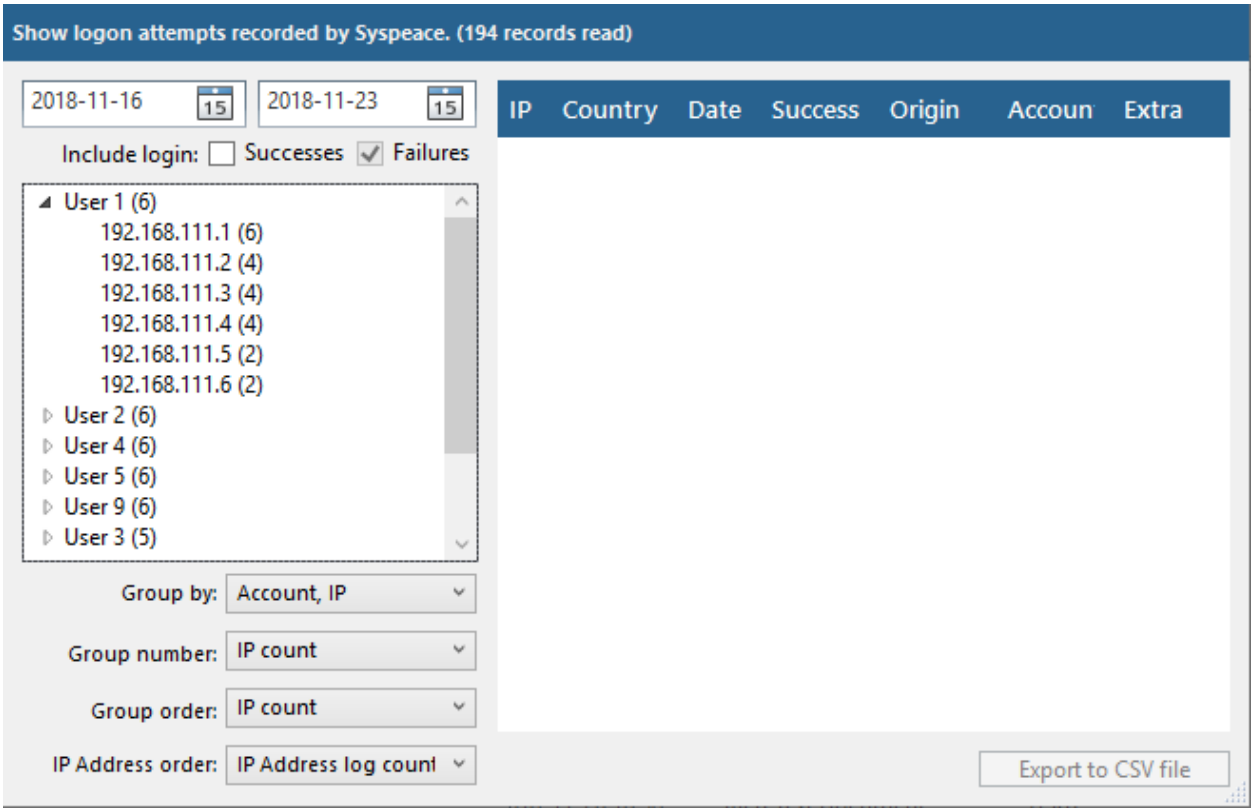
The Access report tab is another tool to use in order to get information about who is accessing your system.

In order to fully understand the advantages and possibilities of this tool, we must master the selection area, the left column with the IP addresses that is shown in the example above and the selection boxes below that. For the purposes of illustrations, we will use fake account names and local IP addresses.

Let's go through the settings:

Group by: describes how the information (IP addresses and Accounts) are shown in the table. It can be either "IP, account" or "Account, IP". With the settings in the above example, we see a main list of IP addresses that have failed to login to our system and if we open that IP address, we see all accounts that that IP address tried to log in to.

By changing the Group By to read "Account, IP" instead, we get the following result:



It is now possible to analyze which accounts are getting hits from what IP addresses instead.

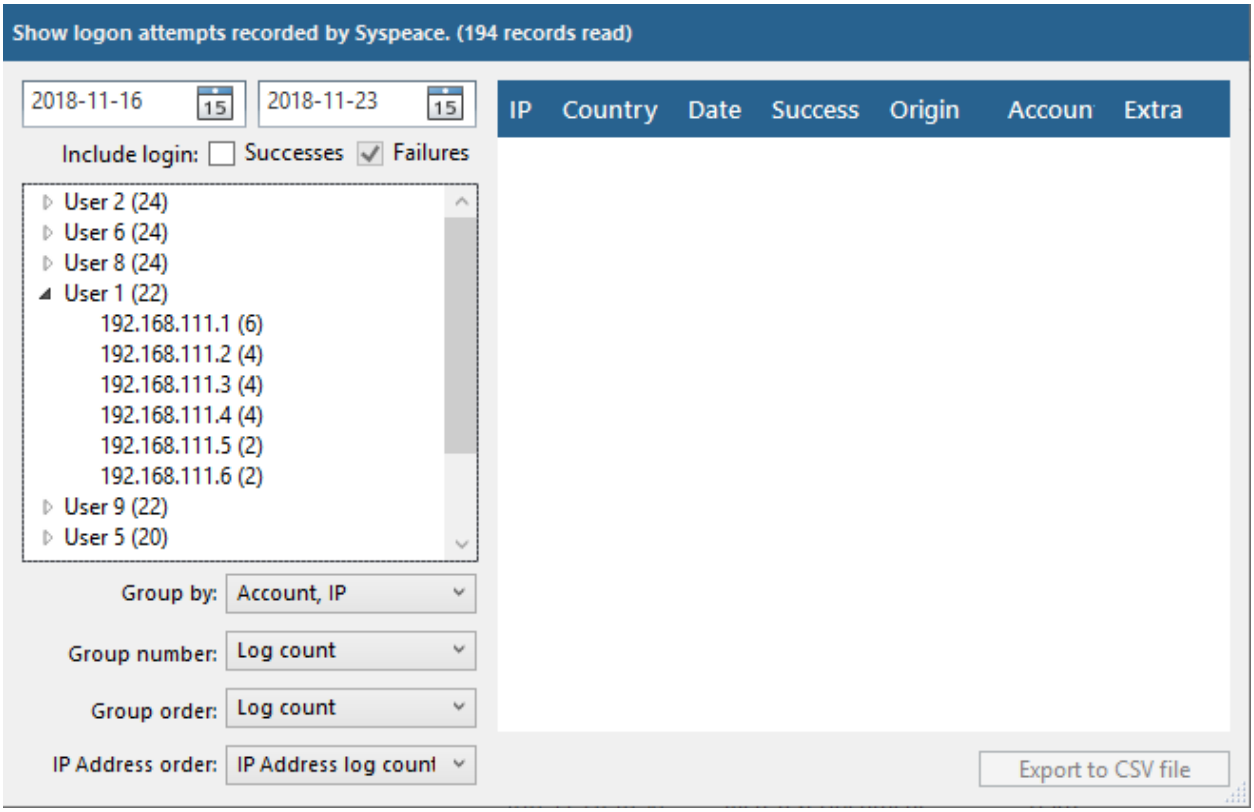
The next settings "Group number:" reads "IP Count". That means that the number after the account (6 after the account "User 1" in the above list) represent the number of IP addresses that you find when you open the account and see the IP addresses, as in the example.

All IP addresses also have numbers after them, that is the number of attempts that that specific IP address have tried to access the system using the account "User 1". From the example above, note that IP address "192.168.111.1" have tried to log in to our system using "User 1" as a user name 6 times.

If an IP address is in the global blacklist, there is also a number in brackets (like "[41]") telling us that this specific IP address has been visiting, and been blocked by, 41 computers in total running Syspeace.

With this setting, you can find out how many IP addresses that have tried to log in using the same account. There are 6 IP addresses that have tried to login to the account "User 1" at the top of the list.

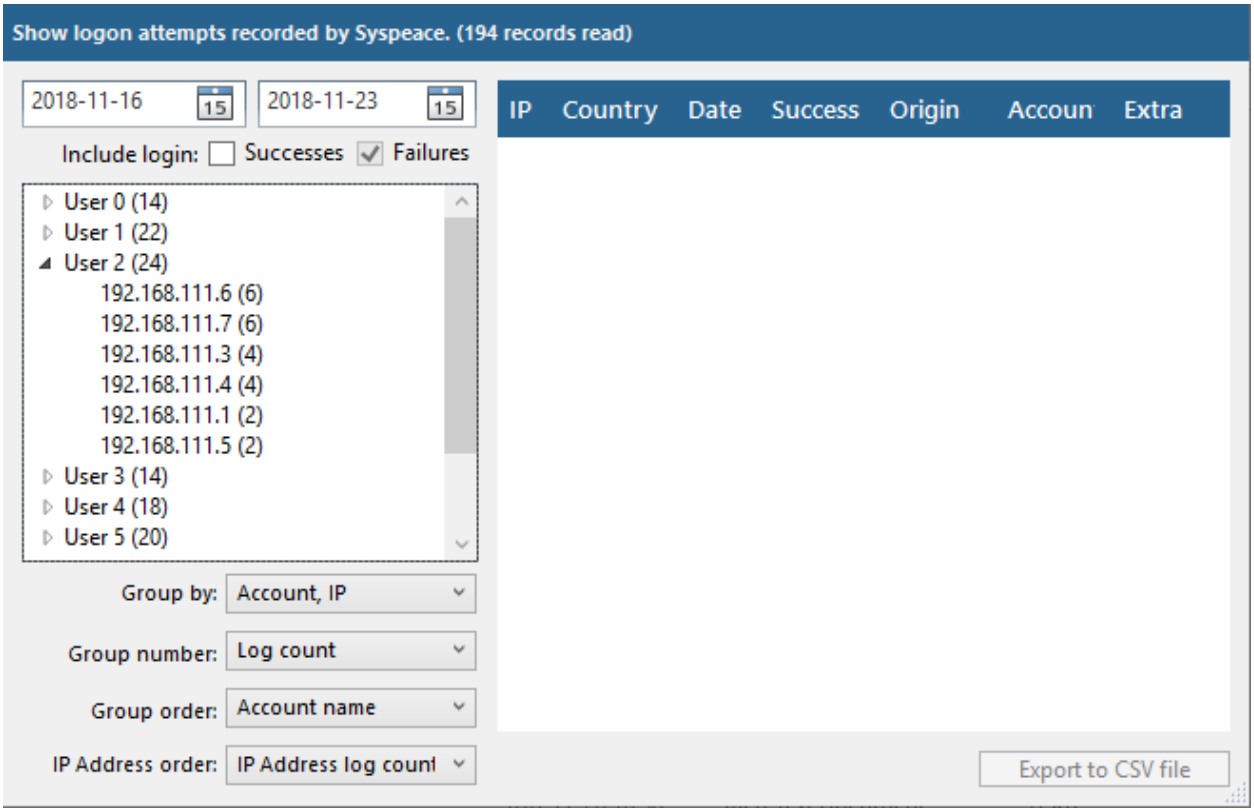
If we change "Group number:" to read "Log count" instead, we get the following result:



Note that the account list is sorted not after the number of IP addresses, but rather after the number of times that account have been accessed from the IP addresses. The number 22 is the sum of 6+4+4+4+2+2.

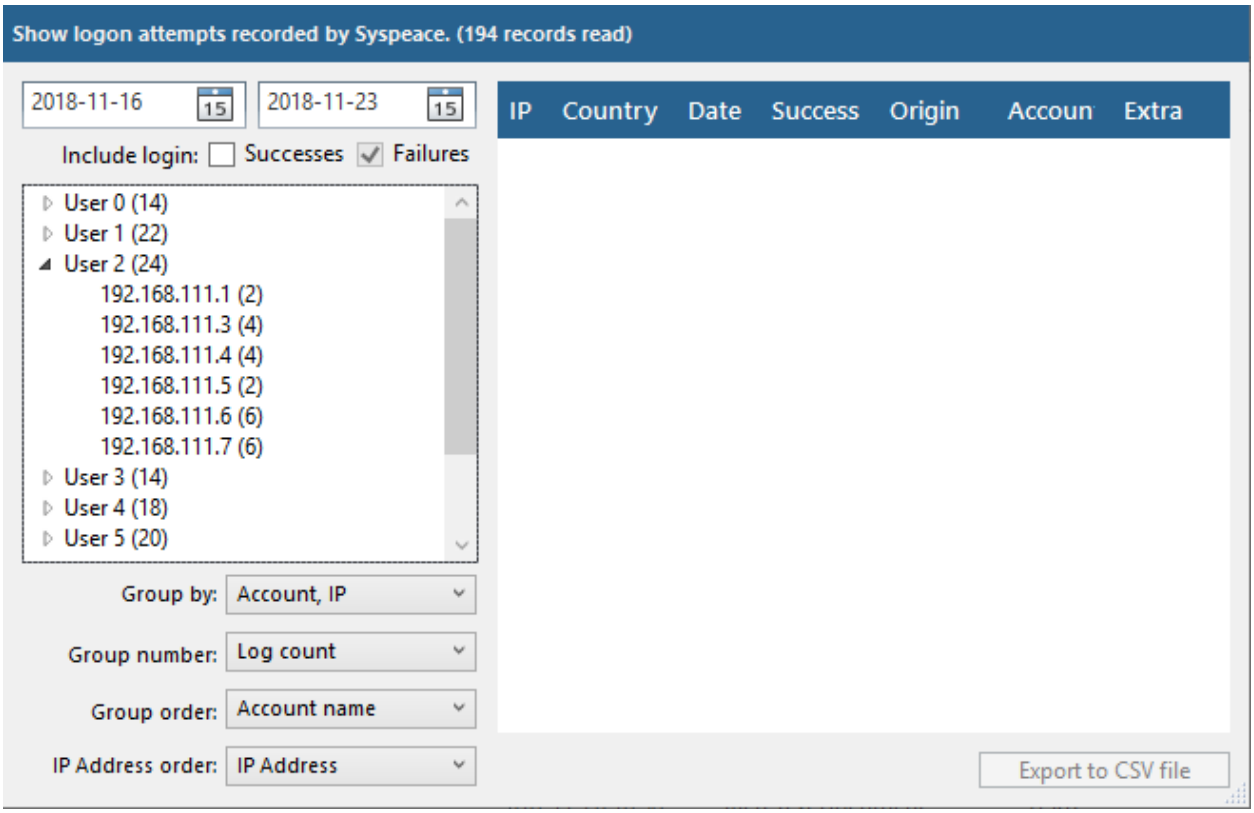
With these settings you can find out how many attacks each account has been the target of.

Change Group order to "Account name" and the main list is sorted by account name.

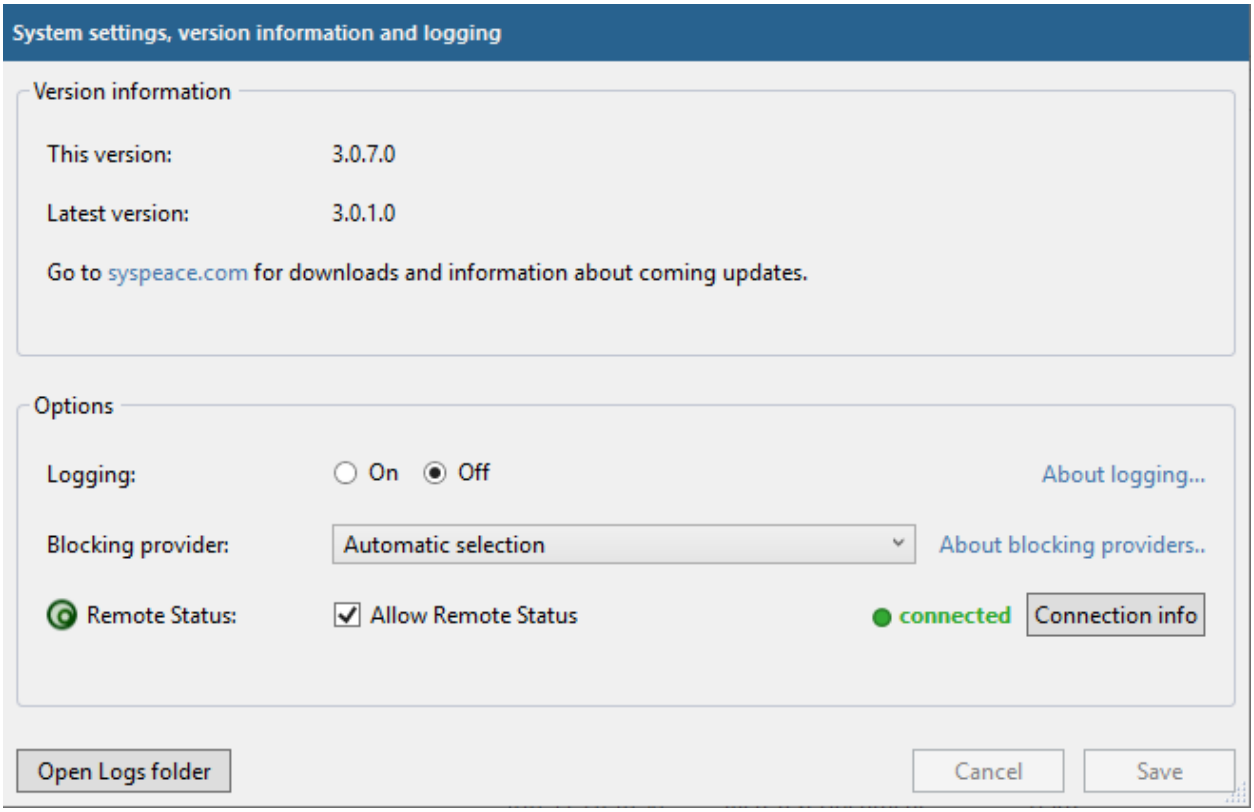


With this setting you will easily find a specific account.

Account order tells us how the list of IP addresses under the account is sorted. Currently, the list of IP addresses is sorted by the number of login tries each IP address have done on that account. Changing "IP Address order:" to "IP Address" will sort the list in order of IP address and present the following result:



Management → System settings



The System settings panel shows the current version number, the version number of the latest downloadable version and the logging setting.

Logging saves debug information about what Syspeace is doing to a log text file. The only reason to enable logging is if you are having problems. The log file can be useful to Syspeace support in the support process.

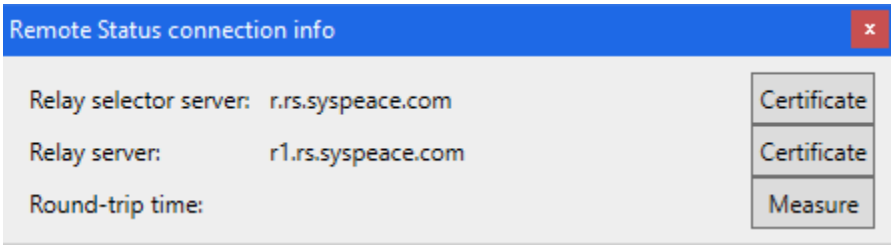
In System settings, you can also control the blocking provider. The blocking provider is the part that turns Syspeace's blocks into actual blocks. There are three blocking providers:

- The Windows Firewall with Advanced Security blocking provider uses the Windows Firewall in Windows Server 2008 and later. This is recommended in most cases.
- The IP Security Policy blocking provider uses the IP Security Policy in Windows Server 2003 and later. If other security software manages the Windows Firewall and ignores Syspeace's blocks, this option can still work.
- The Dry run provider does not actually do anything to turn the blocks Syspeace produces into actual blocks. This can be handy during evaluation to see which blocks Syspeace would have made, but should not be left running. For this reason, prominent Dry run badges will be shown in the Settings and Main windows.

We recommend the default setting Automatic selection, which uses the best choice available.

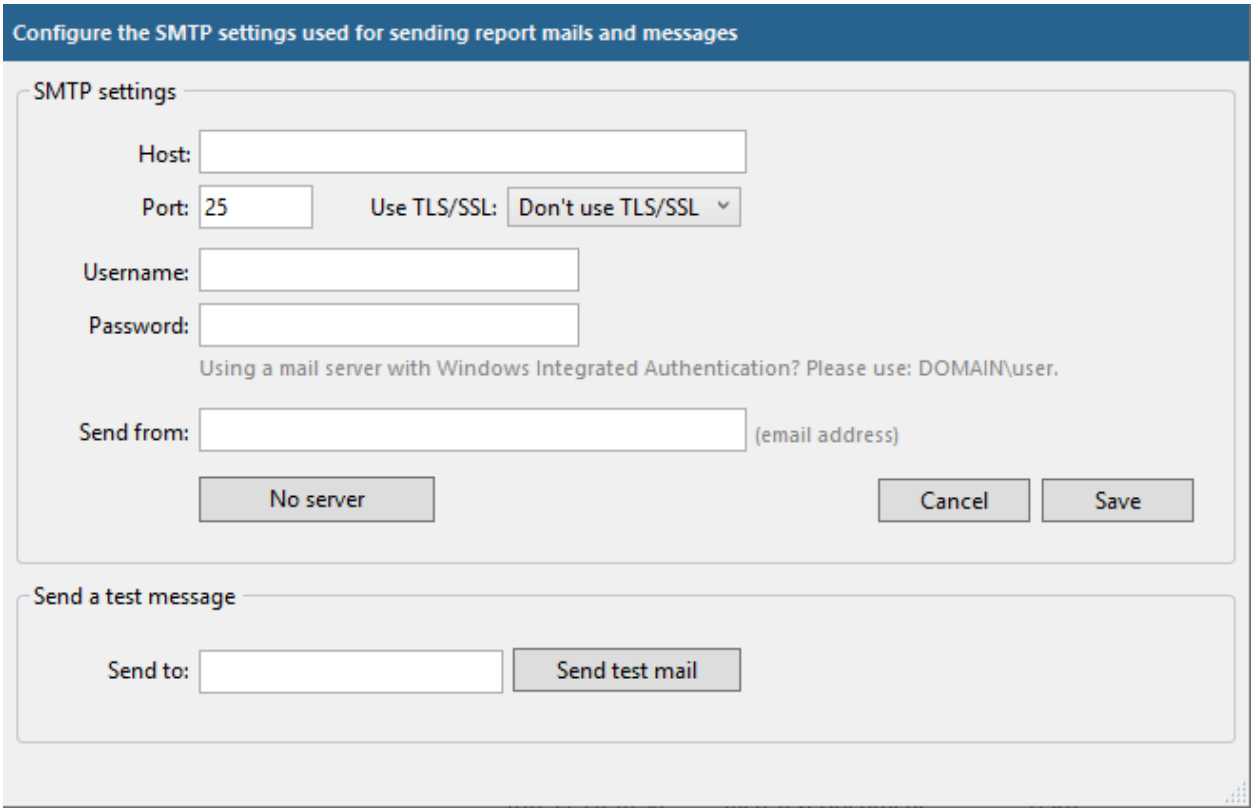
Remote Status

You can enable Remote Status by checking the box **Allow Remote Status** and restarting the Syspeace service. If Remote Status is enabled, you can see the status connecting to the server to the right and see more detailed information about the connection by clicking **Connection info**.



In the connection info window, the Relay selector server and Relay server hostnames are shown and their certificates can be shown by clicking the corresponding **Certificate** button. The round-trip time (the time it takes to send a message to itself and receive it via the Relay server) is also measured and displayed, and can be re-measured by clicking the **Measure** button.

Management → Mail settings



The Mail settings panel is used to configure the SMTP server used by Syspeace to send messages.

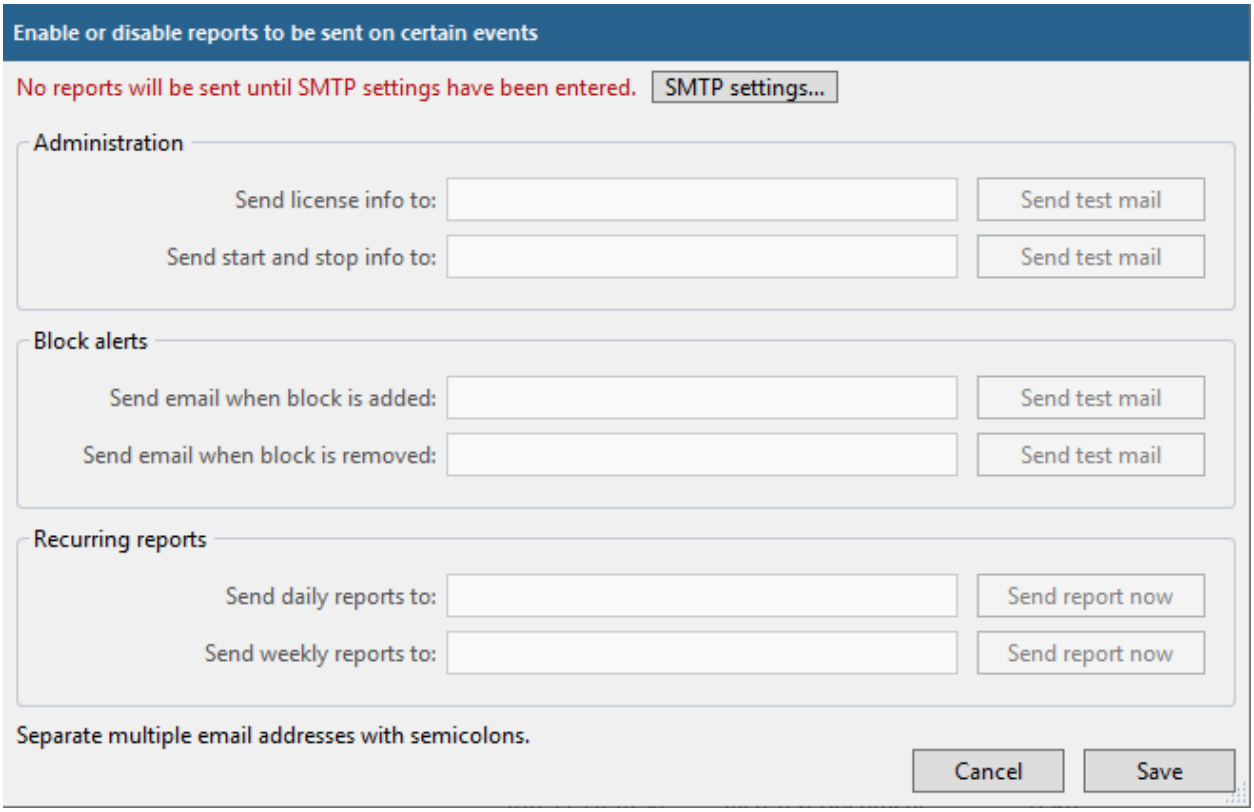
Supply the details of your SMTP server in the text fields. “Sent from” will be the address that the messages are all sent from. Depending on your SMTP server configuration, you may need to pick an address in your domain for the SMTP server to allow the messages. If using an Exchange Server with Windows Integrated Authentication, you may need to provide the Windows domain name in the Username field, in the form “DOMAIN\user”.

Click **Save** to save the SMTP server settings or **Cancel** to discard the changes. Click **No server** to reset the SMTP settings to not point to an SMTP server.

Use the **Send a test message** group to send a test mail message. The mail will be sent using the currently entered SMTP settings, which may not correspond to the saved SMTP settings.

Once you’ve entered the SMTP server details, you may configure which messages to send using ***Management → Messages***.

Management → Messages



Configure which reports to send by entering the recipients of a report in its text field. Click **Send test mail** to send test mails to the recipients currently entered. In the case of daily and weekly reports, click **Send report now** to send an actual report.

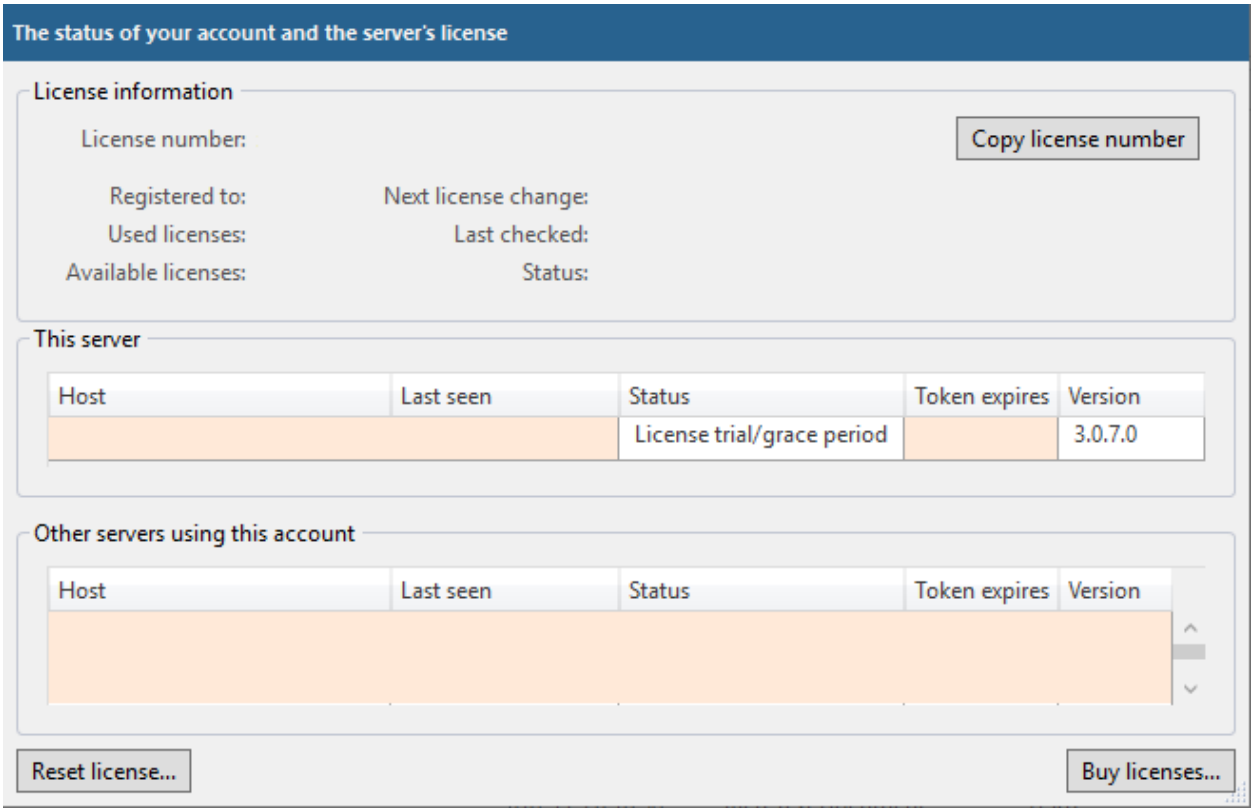
This panel will be disabled if no SMTP mail server is configured in ***Management → Mail settings***.

You may enter multiple email addresses for each report. Click **Save** to save the report settings.

Syspeace will send mail under the following circumstances

- Syspeace is started or stopped
- Syspeace has a problem contacting the license server
- License is about to expire
- Syspeace will add or remove blocks
- Daily and weekly reports

Management → License



The License panel shows information about the server's license status and the other servers on this account, as of the last time the license was validated with Syspeace. This is not a real-time display.

For more information about how Syspeace licenses and accounts work, see ***Syspeace licensing***.

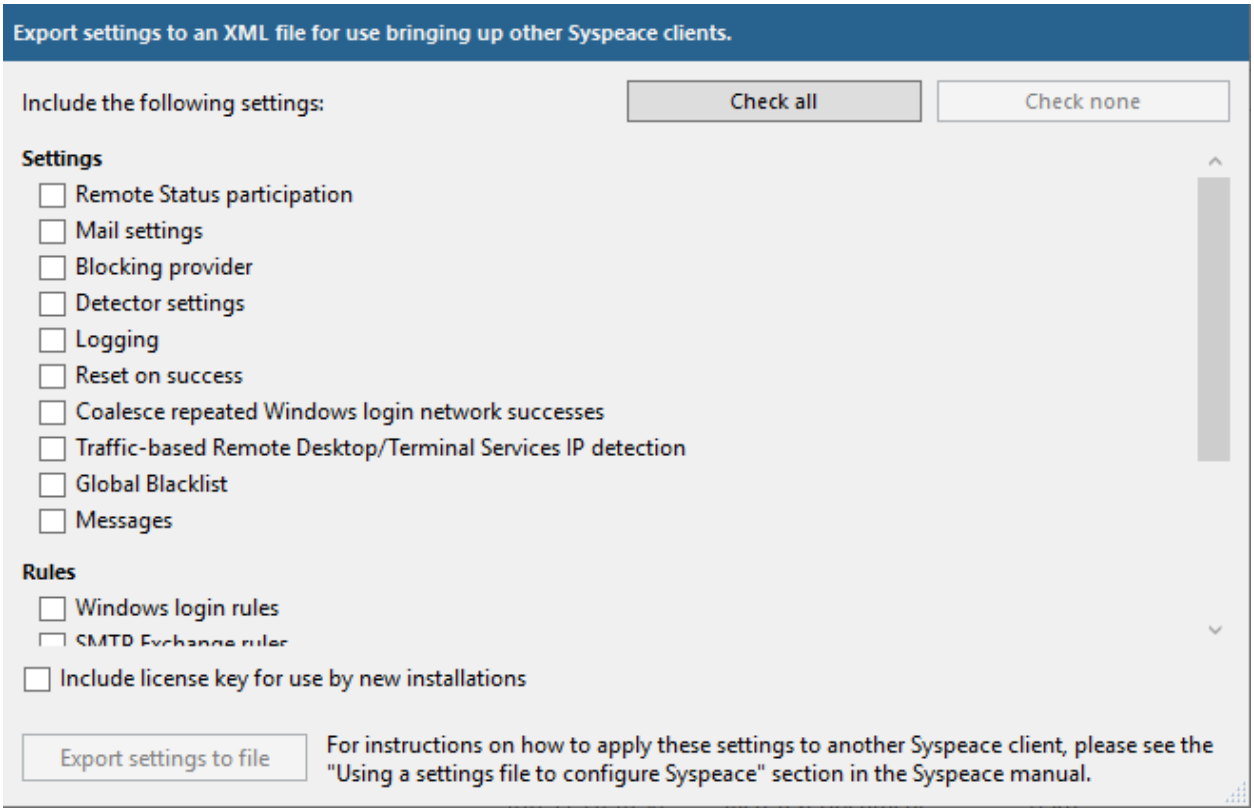
This information is present in the server tables: (the screenshot has been altered to remove any addresses)

Column	Description
Host	The name of the server.
Last seen	When the server last validated its license with Syspeace.
Status	The server's current license status.
Token expires	When the license right will be renewed next time.
Version	The version of Syspeace running on the server.

To buy licenses from your reseller's license site or from the Syspeace Licenses site, click **Buy licenses**.

To disassociate your server from the current Syspeace account, click **Reset license**. The Syspeace service must be stopped and you will be asked to confirm this. You will need to restart Syspeace after this happens. Your server's license use right will not be automatically revoked; it can be manually revoked in the Syspeace Licenses site.

Management → Export settings



The Export settings pane is used to export all or some settings to a file which can be used to reconfigure Syspeace. For more information on this process, see ***Using a settings file to configure Syspeace***.

The settings that are included (checked) will overwrite the corresponding settings on the target Syspeace installation completely, such that the corresponding setting or settings pane will look exactly as it looks on the source Syspeace installation when the settings were exported.

Block or login attempt history are not settings and will not be exported.

The following is exported:

Remote Status participation	The state of Remote Status participation. See the ***Management → System settings*** pane.
Mail settings	The settings required to send mail messages. See the ***Management → Mail settings*** pane.
Blocking provider	Which blocking provider to use. See the ***Management → System settings*** pane.
Logging	Whether or not logging is turned on. See the ***Management → System settings*** pane.
Reset on success, **Coalesce repeated Windows login network successes**, **Traffic-based Remote**	Whether or not the corresponding settings is turned on. See the ***Rules → General*** pane.

Desktop/Terminal Services IP detection	
Global Blacklist	For how many days the Global Blacklist is tracked. The Global Blacklist entries are not exported since they change continuously. See the ***IP lists → Global Blacklist*** pane.
Messages	The recipients of the various messages. See the ***Management → Messages*** pane.
Detector rules (Windows login rules etc.) Country rules	The rules for the various detectors or country rules. The rules on the target Syspeace installation will be removed in favor of any rules in the source Syspeace installation.
Local blacklist	All local blacklist entries. See the ***IP lists → Local Blacklist*** pane.
Whitelist	All whitelist entries. See the ***IP lists → Local Whitelist*** pane.
GeoIP data overrides	All GeoIP data overrides. See the ***IP lists → GeoIP data overrides*** pane.
Include license key for use by new installations	The license key for the Syspeace license. Will not be adopted by Syspeace installations that are already using another license key.

When you have checked the settings you want to export, push **Export settings to file** to produce a **defaultSettings.syspeaceSettings** file.

Troubleshooting

If Syspeace seems to be malfunctioning or you believe there is an error somewhere, please start with these steps:

1. Make sure the Windows Firewall is enabled (as described in ***Firewall***). If the Windows Firewall has been disabled and enabling it is not an option, or if it is managed by other software, go to ***Management → System settings*** and change the Blocking provider to IP Security Policy to use an alternative way of blocking.

   (If Syspeace can detect that the Windows Firewall is managed by other software, it will automatically use IP Security Policy if the Blocking provider is set to Automatic selection; if not, the Blocking provider will need to be changed manually.)

2. Make sure you've enabled the auditing (as described in ***Windows login detection prerequisites***). Syspeace will warn when you start the Syspeace service from the client, there are enabled Windows login detection rules and it can't verify that the auditing is enabled.

3. Verify that the server can reach https://s.syspeace.com/. (You can try this by browsing to https://s.syspeace.com/Ping.) If not, allow Syspeace access to https://s.syspeace.com/ (port 443) in any applicable firewall or antivirus software.

4. In some instances, when running Terminal Server or Remote Desktop Services, Windows Server itself fails to log the source IP address of the login attempt (you can verify this by checking the Windows event log and look for **Source Network Address** in events with event ID 4625). This happens in Windows Server 2008, 2008 R2, 2012 and 2012 R2 when using Negotiate/SSL security and not RDP Security Layer.

   Syspeace will attempt to pick up the IP address from other relevant logs automatically in Windows Server 2012 and 2012 R2, and in Windows Server 2008 and 2008 R2, the setting **Traffic-based Remote Desktop/Terminal Services IP detection** needs to be enabled in ***Rules → General*** and the RDP port configured to the correct port. If no IP address is found, there's no way to tell what to block.

5. Verify any proxy settings, if applicable.

   The Syspeace service runs as the local System account; Group policy objects setting a proxy server where each account is intended to authenticate as itself with a domain identity will be problematic and an exception should be made.

6. Some methods of Windows authentication attempt to log in several times. Two failures may be part of one log in attempt. Syspeace has no way of knowing how many attempts were intended and has to work with the actual failures. Due to counting failures instead of attempts, rules may be triggered seemingly ahead of time.

7. One way of quickly verifying functionality is to use a workstation (not whitelisted) and attack your server with the **net use** command from the command prompt. Login attempts should show in ***Blocks and Analysis → Live observations*** in Settings as they happen. After the number of

tries defined in the current rules, the workstation should be blocked from communicating with the server.

Example of the command:
net use * *server name or server IP address*\anyshare /user:syspeacetester "anypassword"

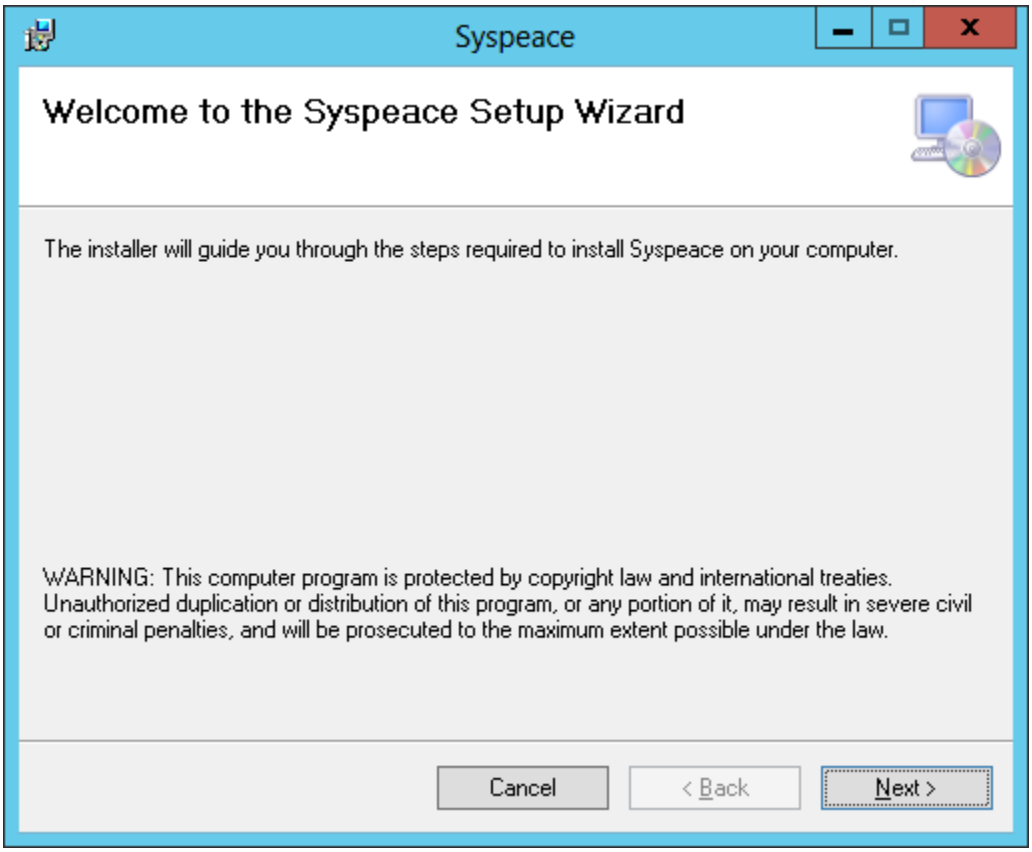
8. If you want to submit logs to us, start Syspeace, go to ***Management → System settings***, enable logging and start the service.
   The log file is created in a subfolder of the Syspeace installation folder.

Contact

Please send any questions or thoughts to support@syspeace.com.

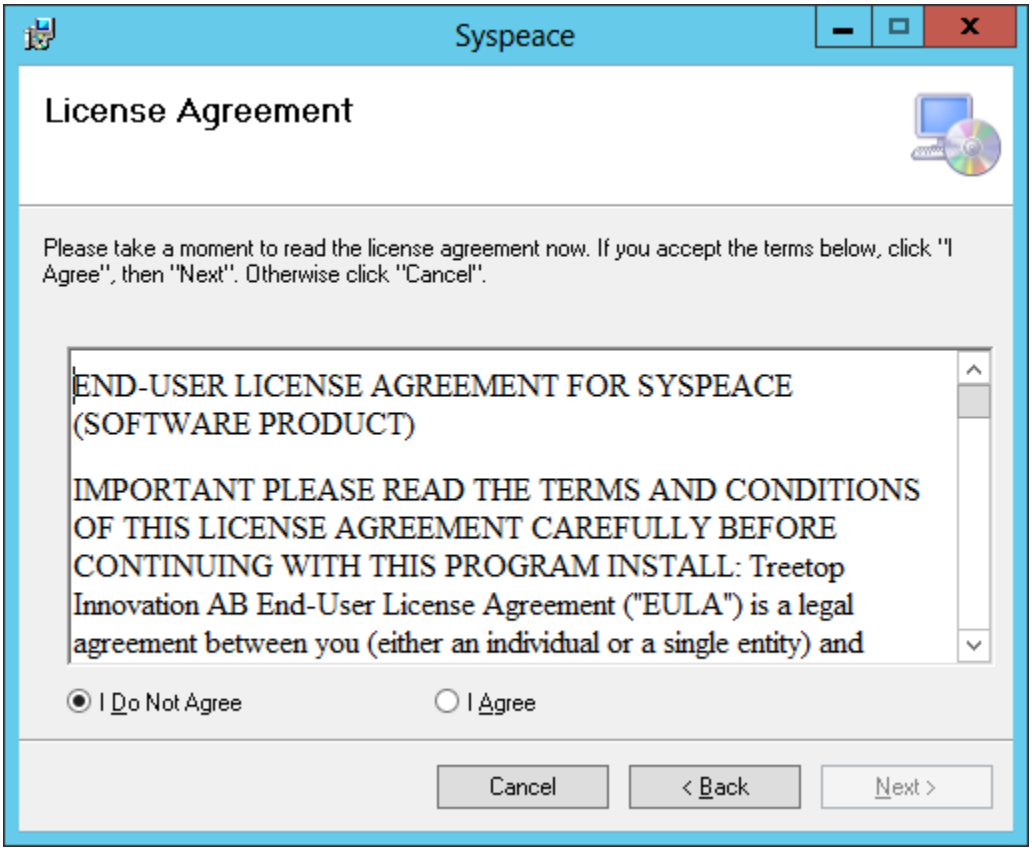
Appendix A: Syspeace Setup Wizard step by step

Welcome



Press **Next** to continue.

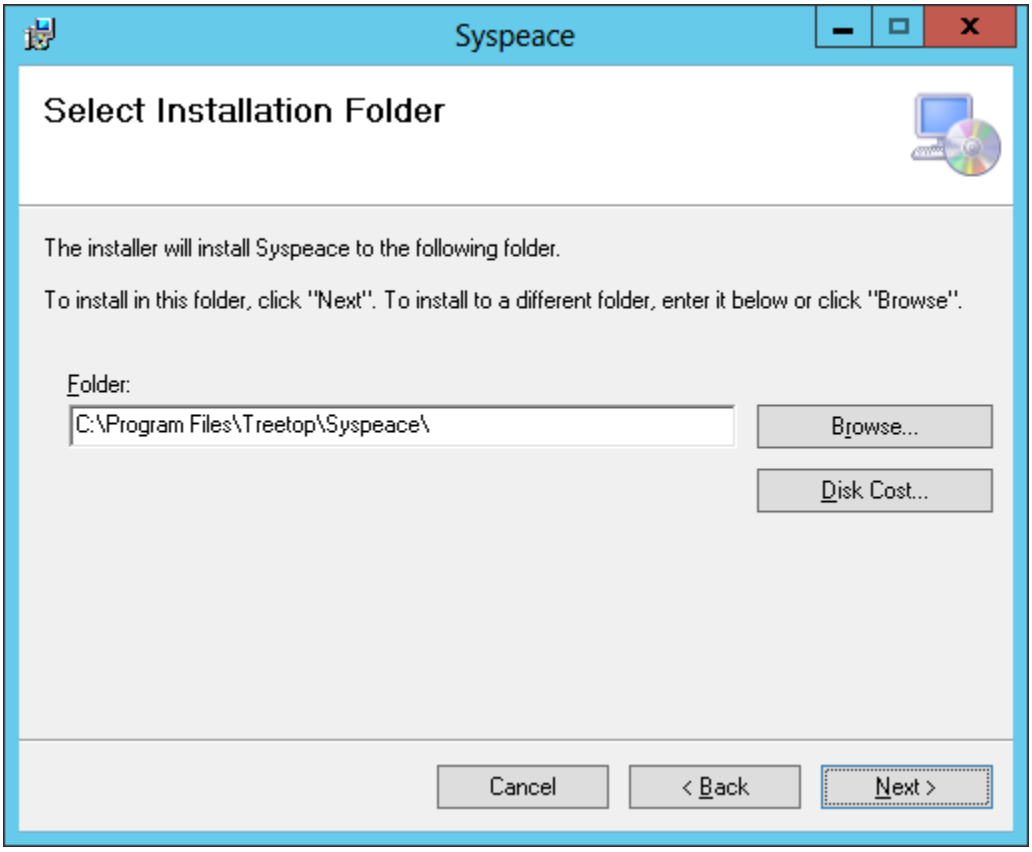
License Agreement



Press **Cancel** if you do not agree with the license agreement. Syspeace will not be installed.

Press **Next** if you agree with the license agreement.

Select Installation Folder

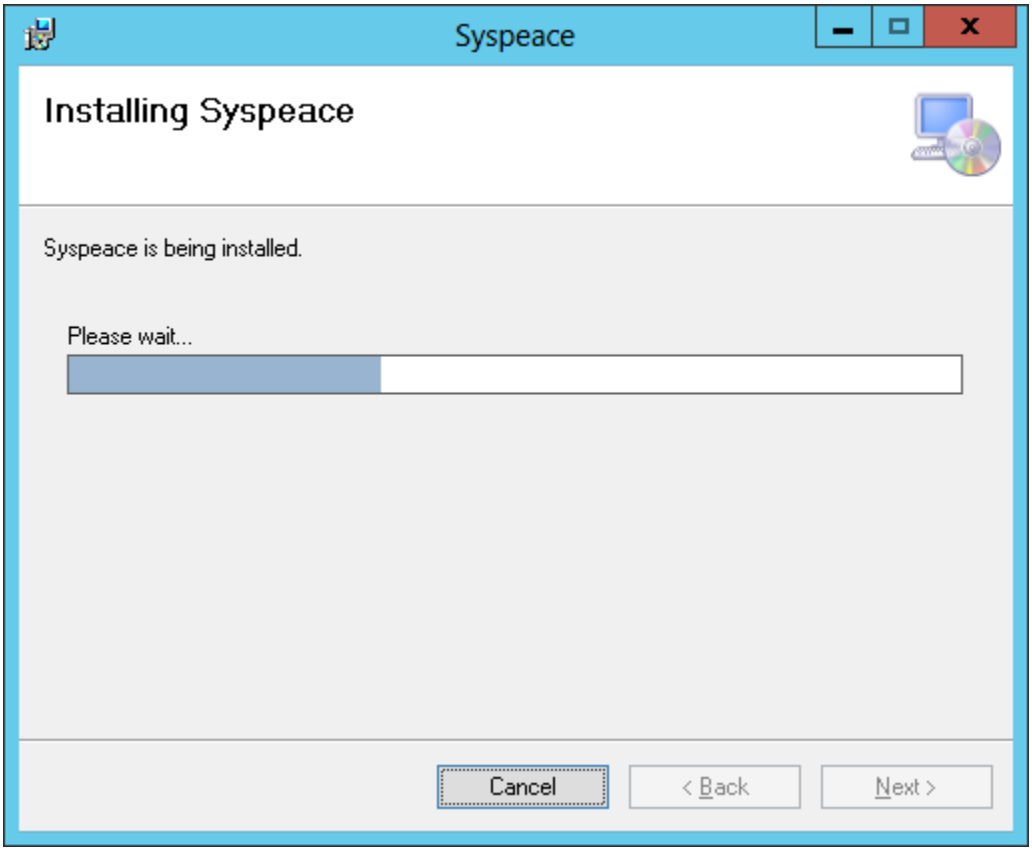


Select the folder to install Syspeace into using the **Browse** button, or by manually entering the path to a folder.

You may not use a folder based in a network share or a drive hosted on the network.

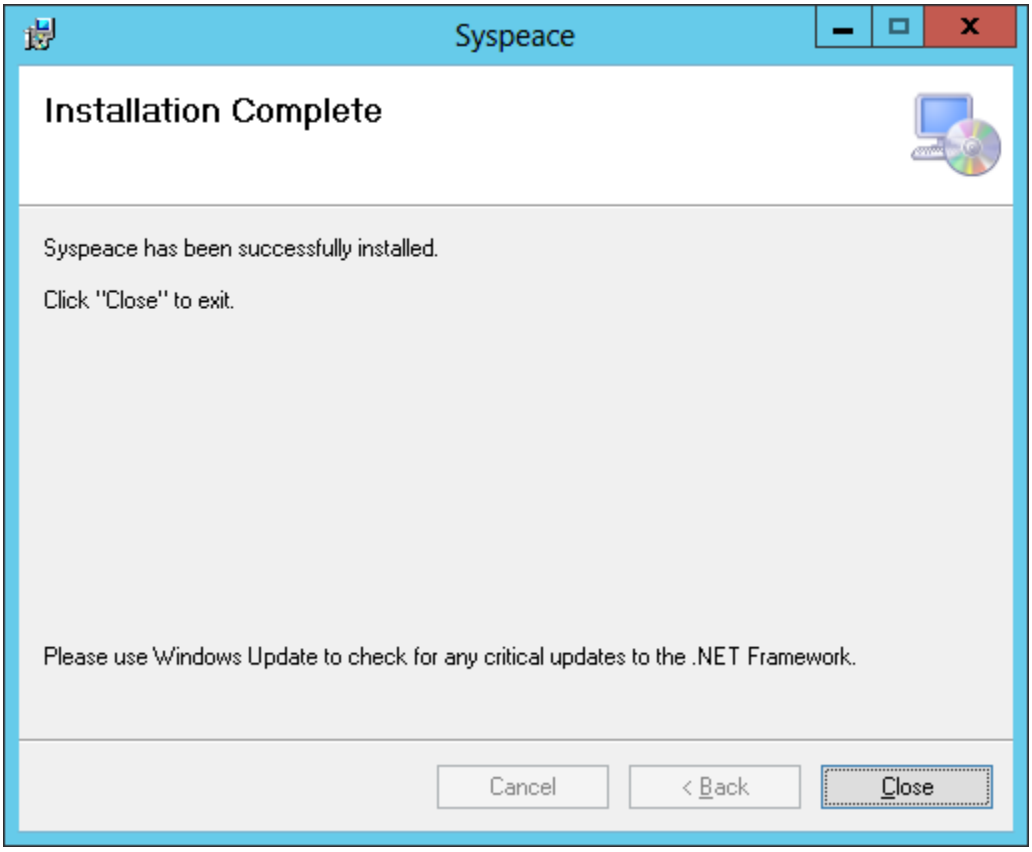
Press **Next** to start the installation.

Installing Syspeace



Wait until Syspeace is installed or press **Cancel** to abort the installation.

Installation Complete



Press **Close** to exit the installer.