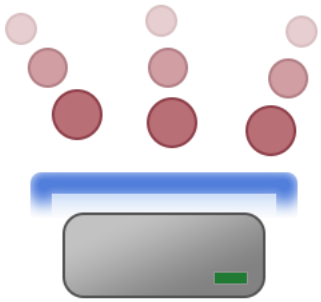


Syspeace manual

Syspeace v2.0.0

Treetop Innovation AB

For more information, see http://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
- Configuring Syspeace after installation
- Syspeace Settings
- Troubleshooting
- How to contact us

Footprint

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" are 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.

Prerequisites

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

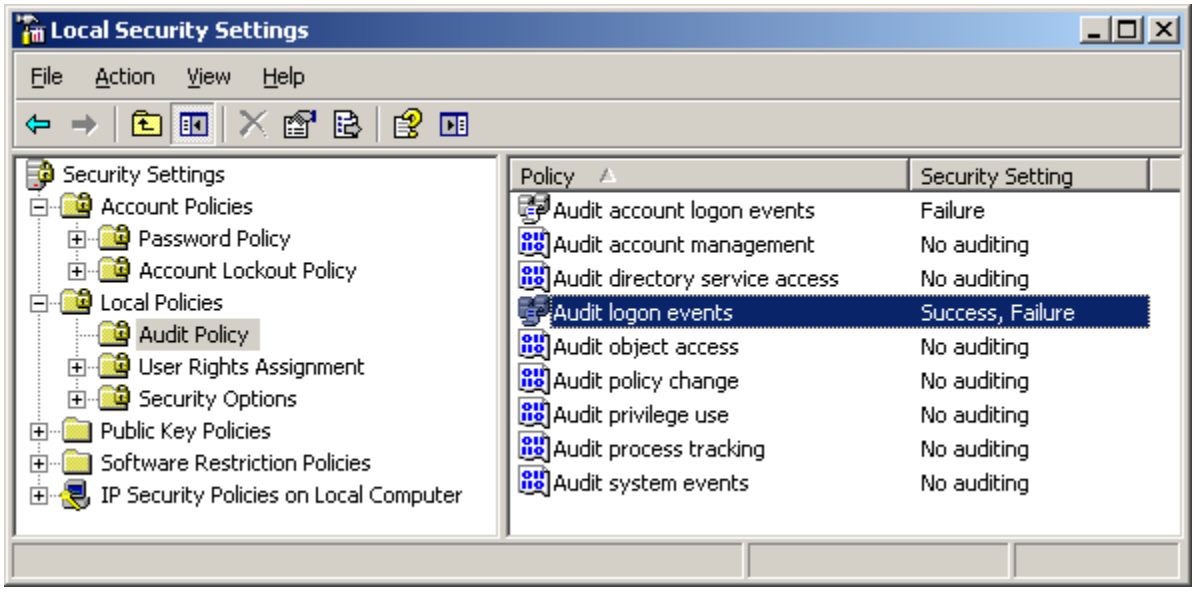
System requirements

Syspeace requires a 32-bit or 64-bit version of Windows 7, Windows Server 2003, Windows Server 2008 or Windows Server 2008 R2. Syspeace is not available for Itanium. 1GB free disk, minimum 500 MB RAM.

Auditing

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.

To set this up in the local security policy:



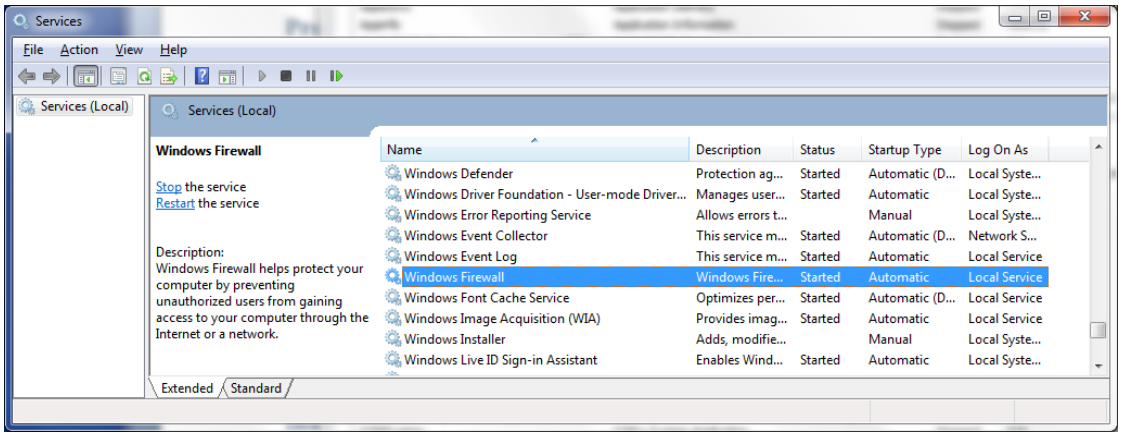
1. Open the **Control Panel**.
2. Open **Administrative Tools**.
3. Open **Local Security Policy**.
4. In the tree to the left, select **Security Settings** → **Local Policies** → **Audit Policy**.
5. In the list to the right, double click **Audit logon events**.
6. Check the **Success** and **Failure**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

Firewall

Windows Server 2008 and later

The built-in firewall in Windows – Windows Firewall with Advanced Security – must be up and running.



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:

- Run “mmc” to open an empty instance of Microsoft Management Console.
- Go to File → Add/Remove Snap-in…
- Click Add…
- Select IP Security Policy Management and click Add.
- In the Select Computer or Domain wizard, make sure Local computer is selected and then click Finish.
- Click Close and OK to get back to the Console Root window.
- Select IP Security Policies on Local Computer in the tree to the left.
- From the View menu, make sure Detail is selected.
- 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.
- If any other policy is assigned, you must first right-click and “un-assign” the policy for Syspeace to be able to work.
- If a policy says “Policy is assigned, but it is being overridden by Active Directory-assigned policy.” [sic], 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" (or 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 Imagining 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 two detectors: Windows login and Exchange SMTP Connector.

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.

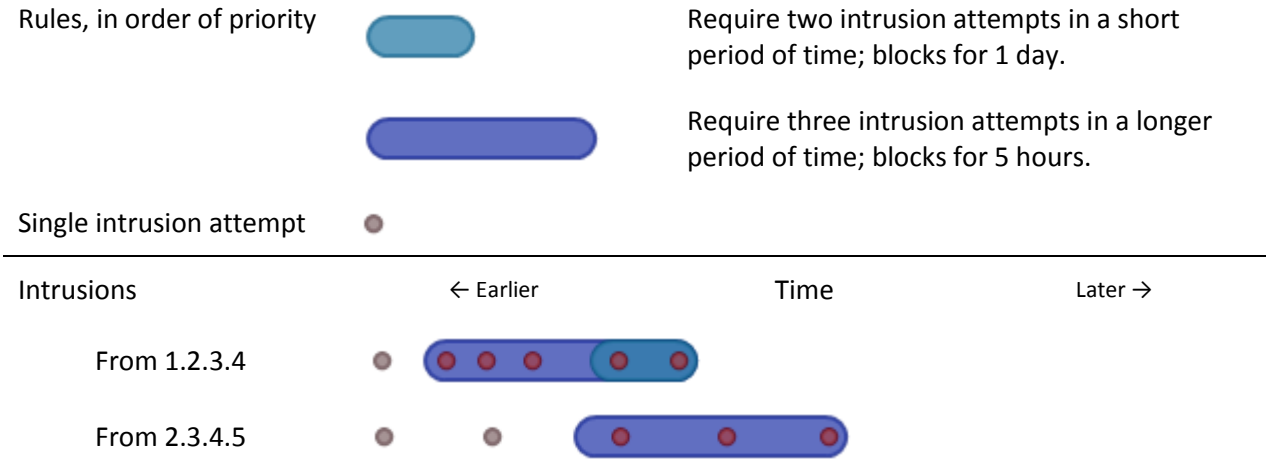
The Exchange SMTP Connector detector checks for login failures in the Exchange SMTP Connector.

Each detector works similarly: based on accumulated evidence of login failures, the offending IP address is blocked for an amount of time. 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.

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, it will be excused if it is whitelisted.

Every loopback address in every available network interface is automatically whitelisted. However, other computers within the same local network range are not.

Syspeace licensing

Syspeace requires every computer 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. One or more individual licenses may be associated with your account, giving one or more computers the right to run Syspeace during a period of time. Licenses are purchased from the Syspeace Licenses site.

One account…	…can contain many and different licenses	
Account	**License**	**License**
syspeacecustomer@example.org	4 computers	2 computers
License key: XABC	From 2013-09-01 to 2013-12-31	From 2014-01-01 to 2014-12-31

When you give Syspeace your license key, you are telling it from which account it should attempt to find a license for the computer. (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 computer.

One license…	…can be used by many computers	
License	**License right**	**License right**
4 computers	Computer: SERVER-EMAIL	Computer: SERVER-WEB
From 2013-09-01 to 2013-12-31	From 2013-09-01 to 2013-09-04	From 2013-09-01 to 2013-09-04

As license rights are only checked out for a brief period of time and not the duration of the entire license, you may swap computers during the license duration – the license is "floating".

If Syspeace at any point is unable to find a current license, the computer 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.

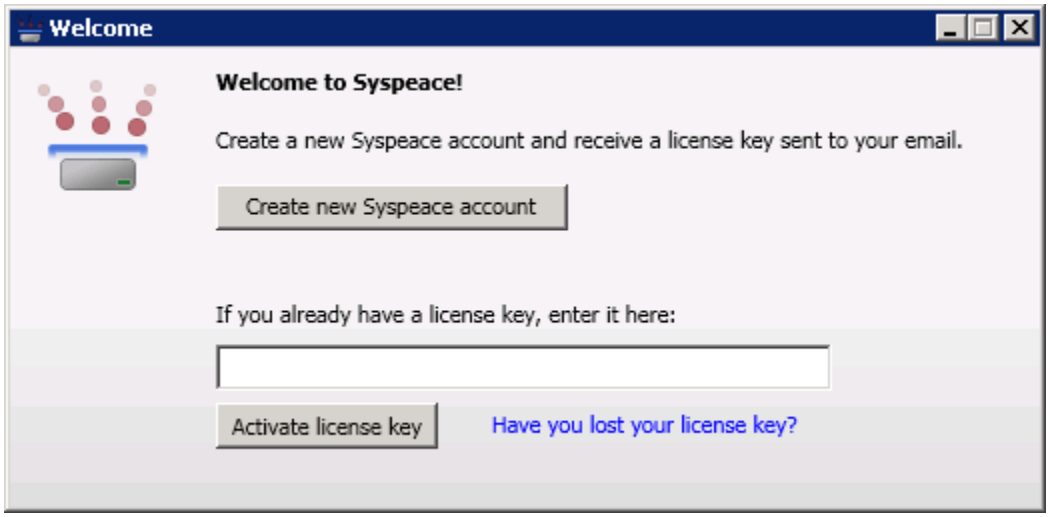
Current information about the license status of a particular computer is always visible in the Syspeace client's status bar. Information about all licenses in an account is available from the Syspeace Licenses site.

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 computer. 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 computer 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

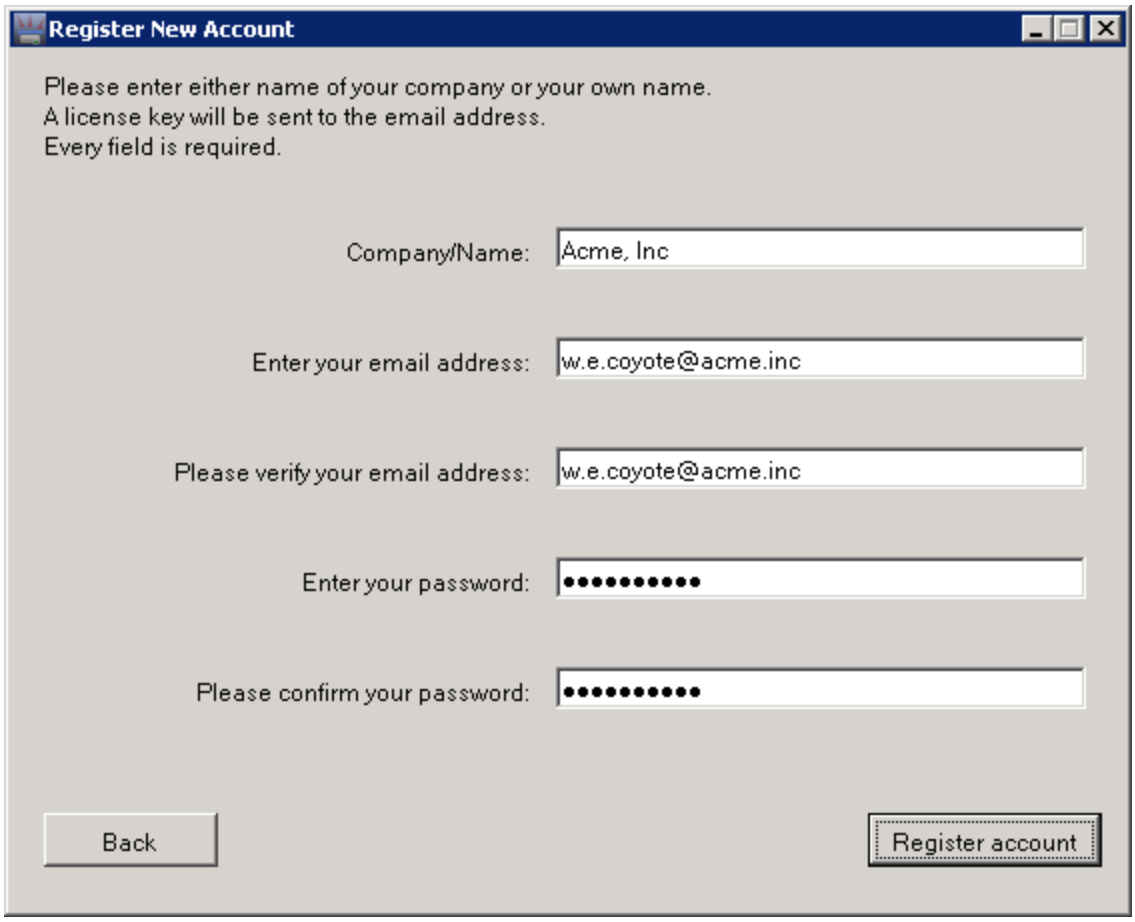
Locate your account's license key. You may click the **Have you lost your license key?** link to have it sent to your Syspeace account email. When you have your license key, paste it or enter it manually into the text box and click **Activate license key** to continue.

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 **Company/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.

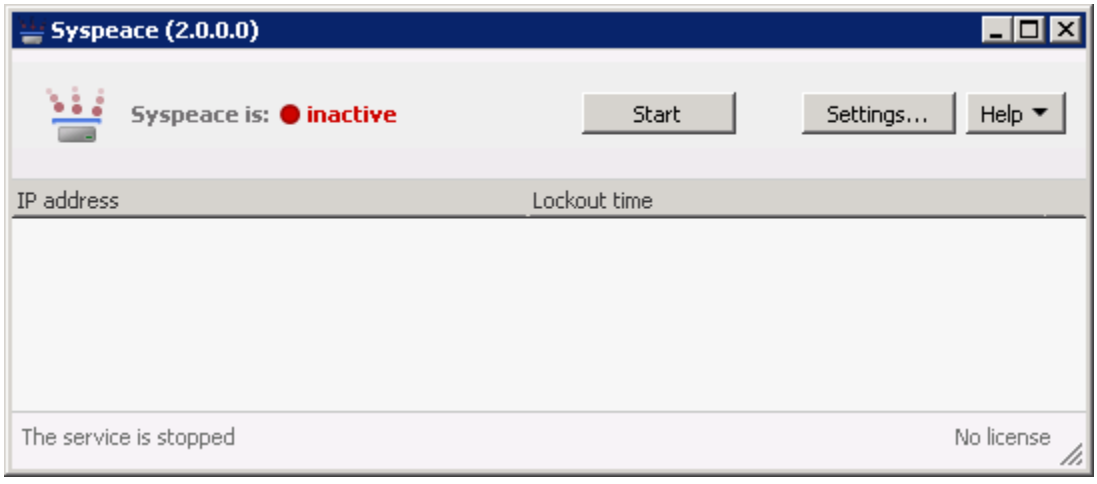


Receiving the license key

After registering, you will receive an email message with the license key. Enter this into the text box in the welcome window and push **Activate 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. For example, the list in the middle shows the currently active blocks.



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.

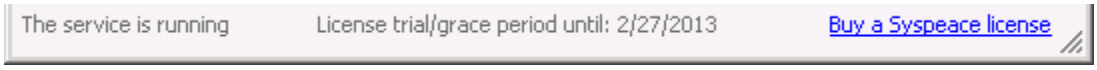
When Syspeace is active, the Start button changes to a **Stop** button. Exiting the Syspeace client will not stop the service and stopping the service will not exit the client.

The 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 computer.
Starting up	The Syspeace service is running and is getting ready.
Active	The Syspeace service is running and protecting your computer.

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

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

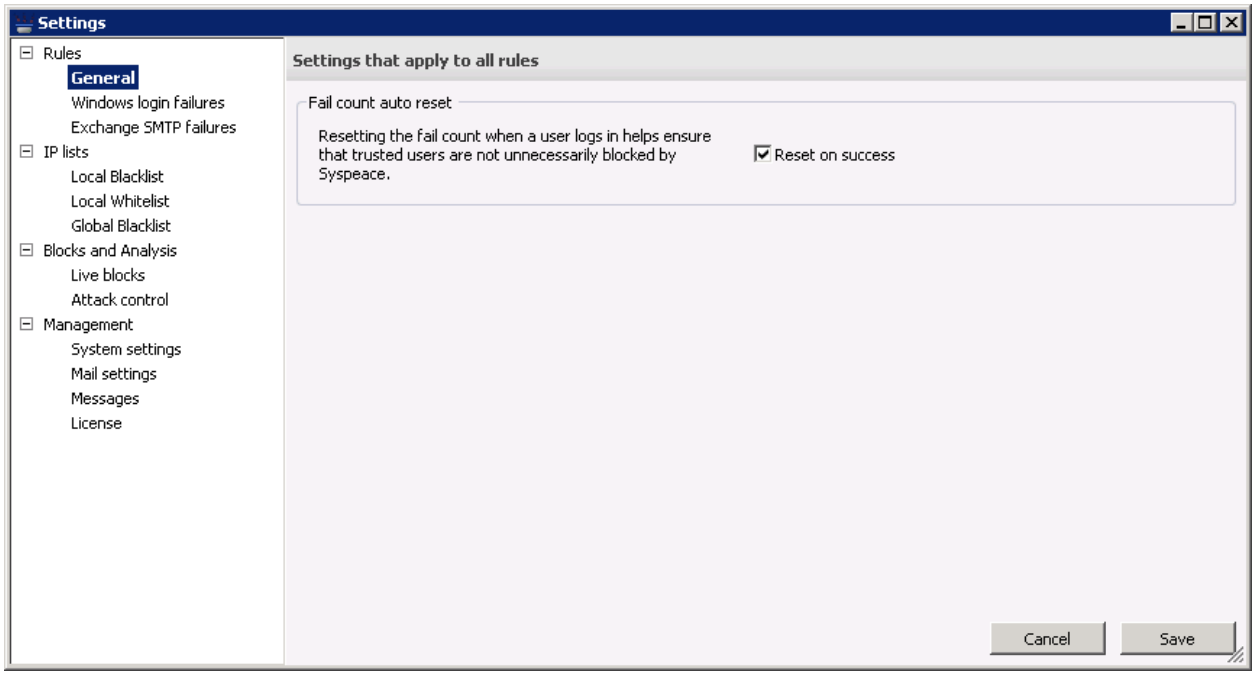


You may click the link to navigate to the Syspeace Licenses site to purchase licenses.

Syspeace settings

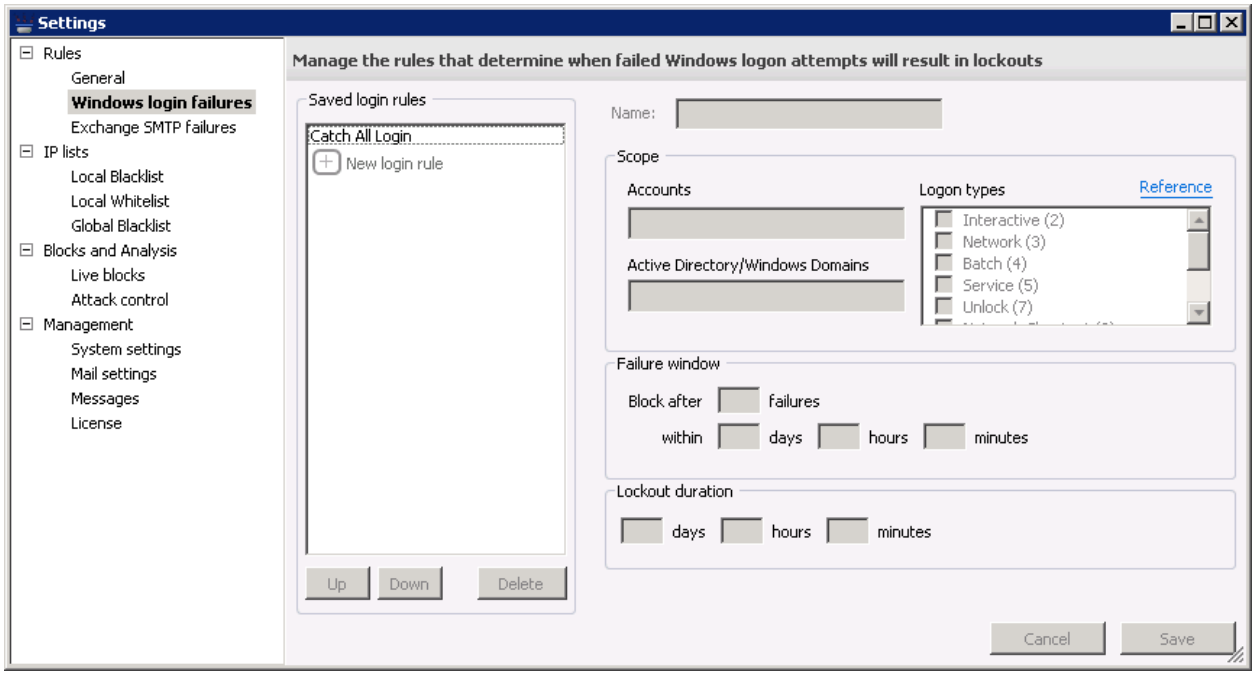
The left side of the Settings window consists of a list of panels. Each panel has one or more settings that can be tweaked in order to specify the behavior of the service. Most of the settings

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.

Rules → Windows login failures



These rules govern how failed logins will be treated. (For more information, see ***How Syspeace works***.)

By default, the rule "Catch All Login" blocks intruders that fail to log in after five attempts within 30 minutes. They will be blocked for two hours. 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 login 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**.

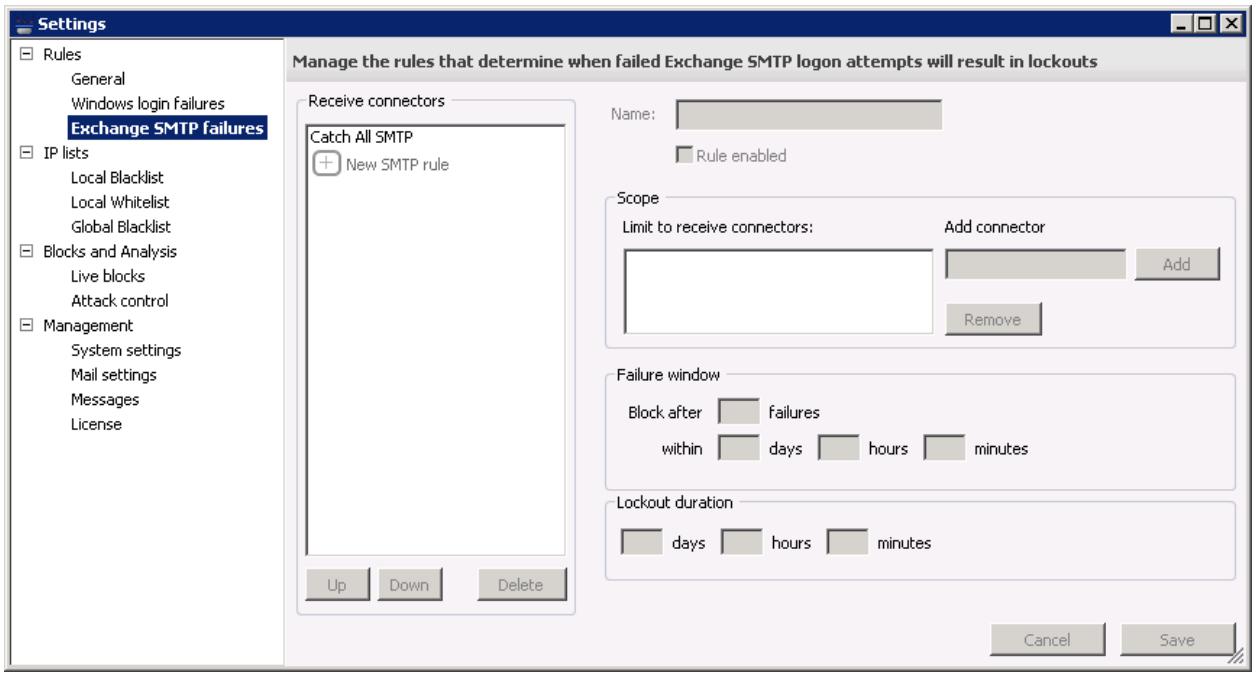
Property	Description	Default value
Name	The rule's name.	Nothing
Scope	Narrow the Windows login circumstances.	
Accounts	If not empty, the login names of one or more Windows accounts to match. (Separate many names with commas.) For example: "Administrator,Economy"	Empty
Active Directory/Windows Domains	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
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

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 **Saves login rules** list and edit the rule as usual. Click **Save** to finish creating the rule.

Rules → Exchange SMTP failures



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.

This panel works just like the Rules → Windows login failures panel, except for the following properties:

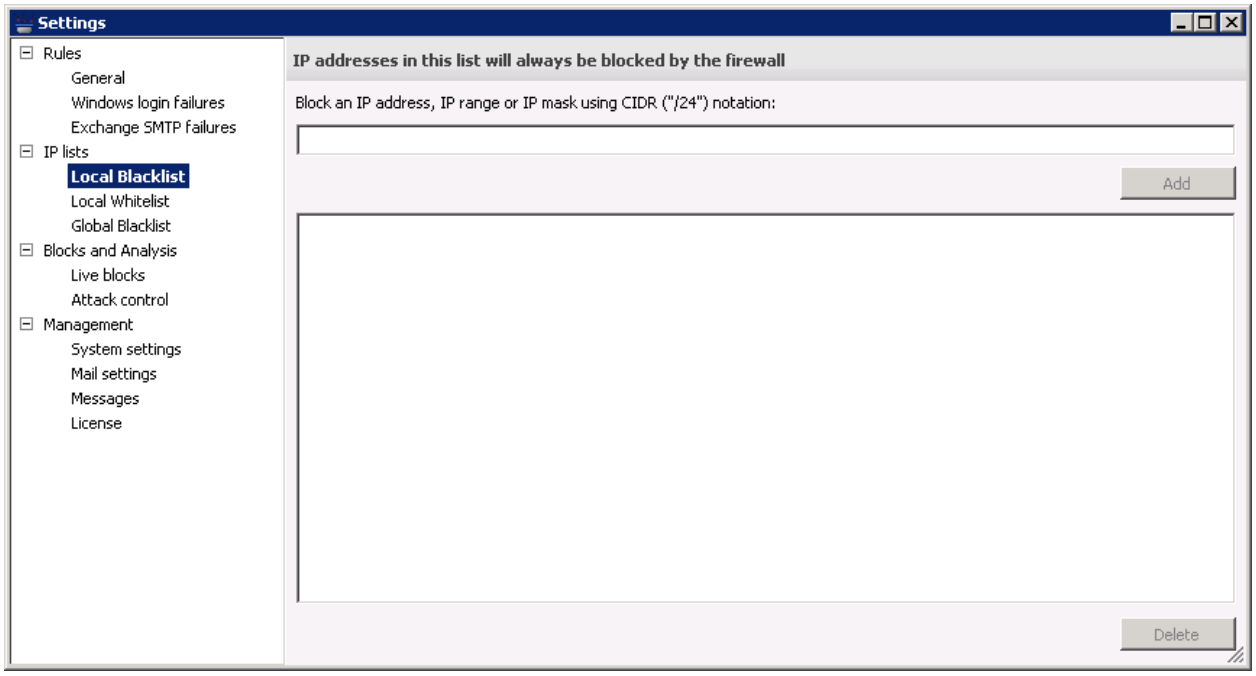
Property	Description	Default value
Rule enabled	Whether the rule is enabled	Yes
Scope	Narrow the Windows login circumstances.	
Limit to receive connectors	If not empty, the names of the SMTP connectors to match.	Empty

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 "larger" IP address last.
IP mask, CIDR notation	1.2.3.0/24	Every IP address with the first 24 bytes equal to the first 24 bytes of 1.2.3.0 (1.2.3.0-1.2.3.255)

IP lists → Local Blacklist

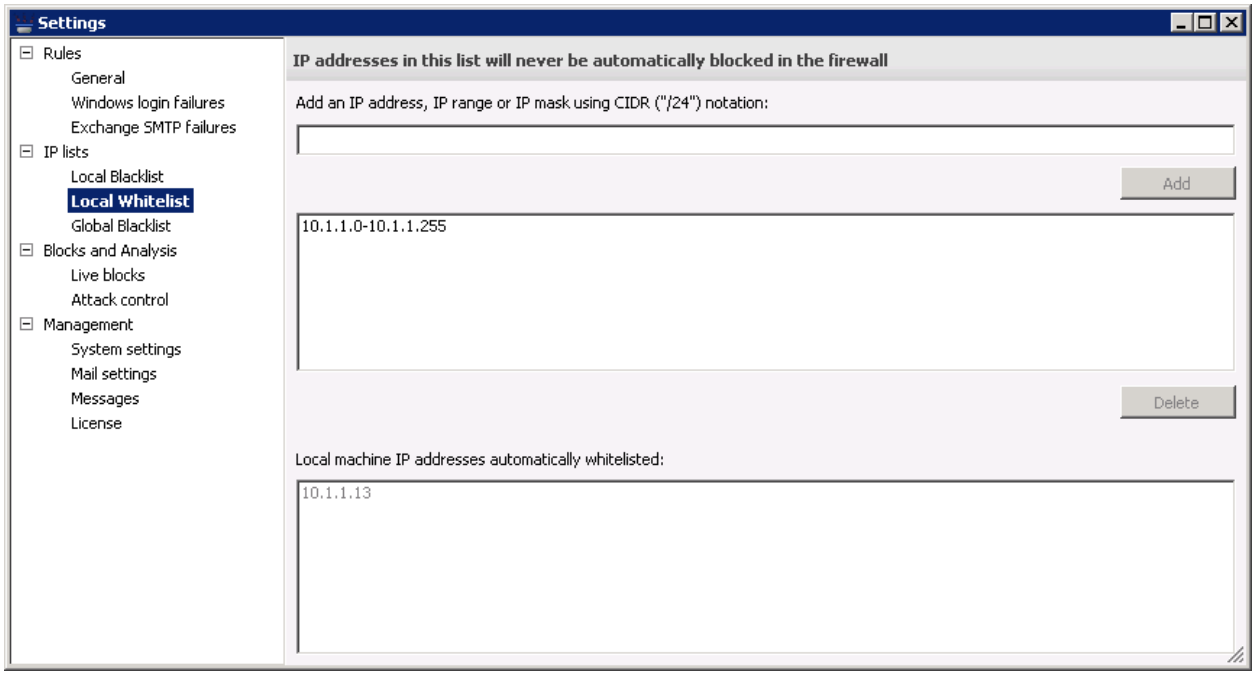


Every IP address entered in the local blacklist will be blocked indefinitely. (For more information, see ***How Syspeace works***.)

Enter an IP address or range 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.

IP lists → Local Whitelist



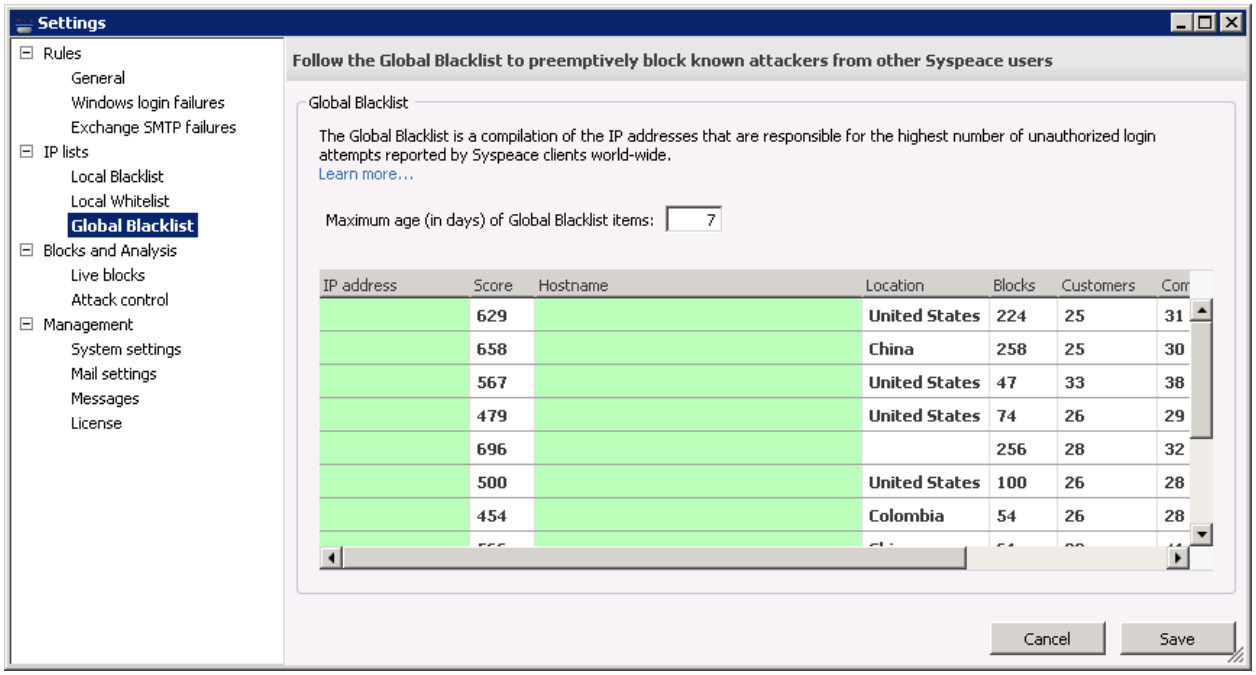
Every IP address entered in the local whitelist will be exempt from blocks, even from being in a blacklist. (For more information, see *How Syspeace works*.)

Enter an IP address or range 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.

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.

IP lists → Global Blacklist



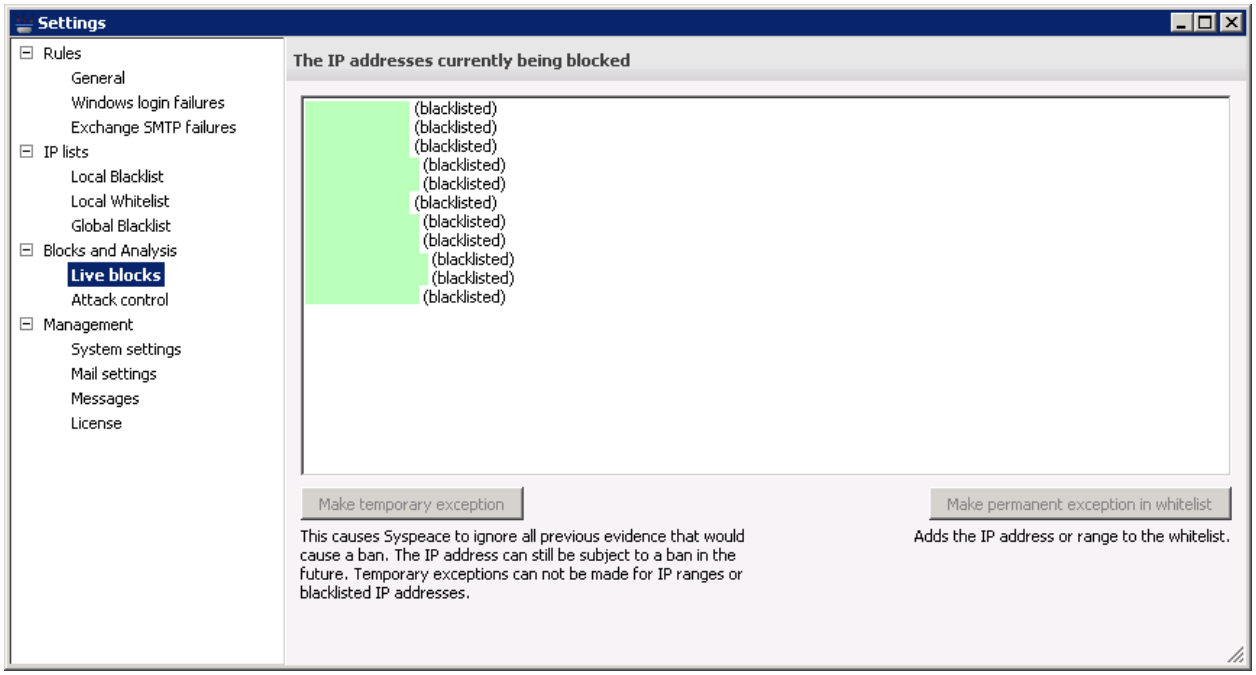
The Global Blacklist is maintained by Syspeace servers and tracks the most common, widespread or insistent recent attackers across every Syspeace installation worldwide. When an IP address enters the Global Blacklist, it will preemptively be blocked by Syspeace if Syspeace is set to follow the Global 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.

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

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.

Blocks and Analysis → Live blocks



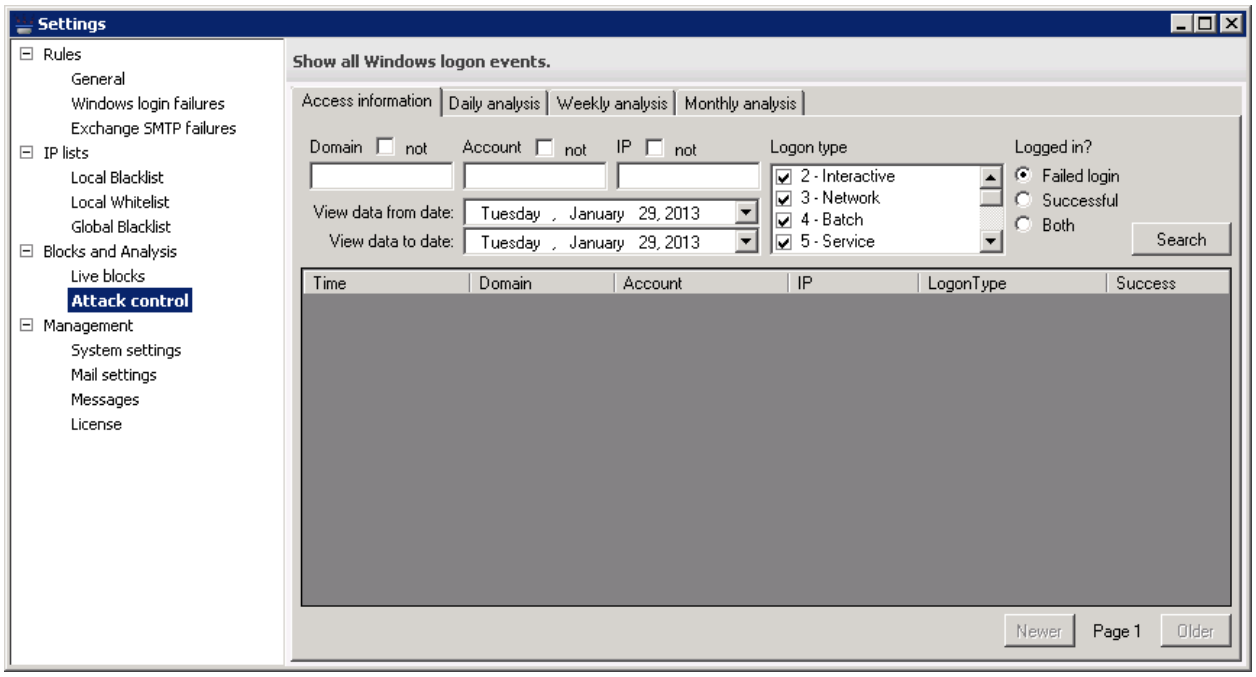
The live blocks panel shows the currently active blocks. (The screenshot has been altered to remove any addresses.)

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 → Attack control

The Access information tab

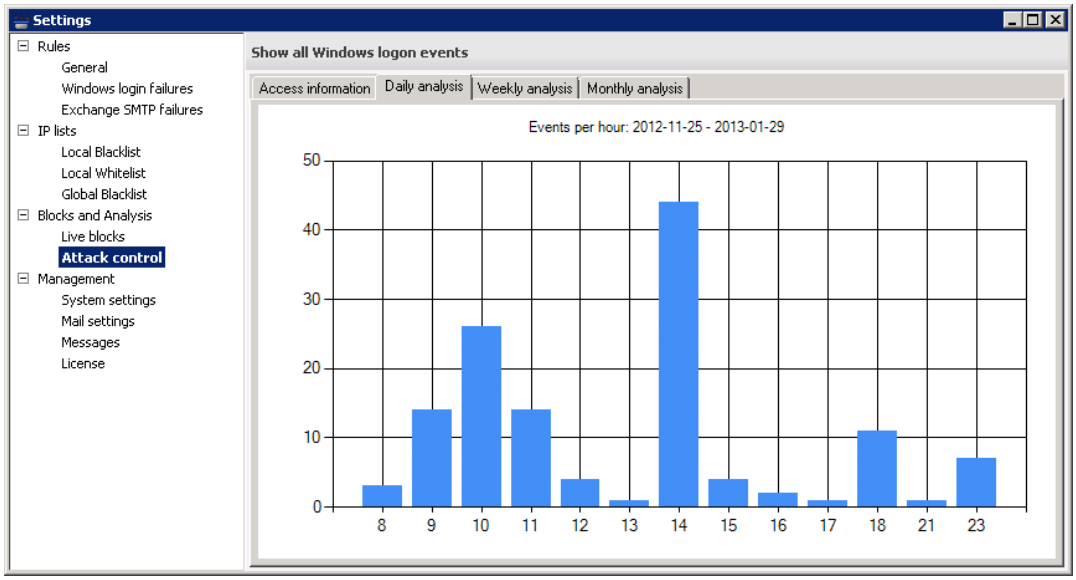


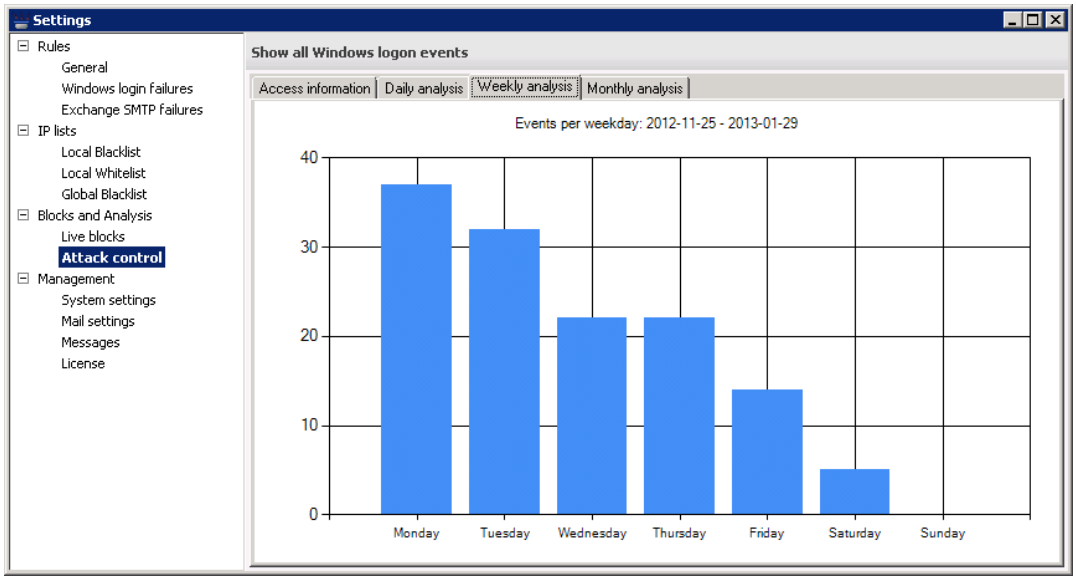
The access information tab has a list of all login attempts on your computer. Syspeace records this information and keeps it for two months. This information is meant to be used to understand why a block was made; not as a complete archive of the login history of the computer.

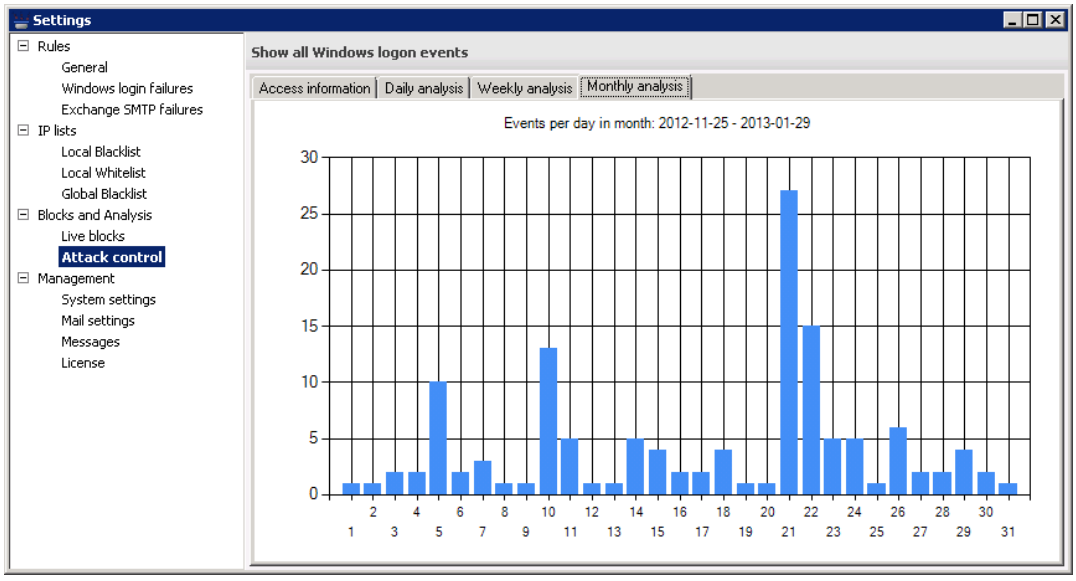
You can filter the data on domain, account, IP address, logon types and whether the login attempts were successful or not. You can also select a range of dates from which to select data. The list shows the last 1000 records by default. In order see more results (if any), you can click the “Older” and “Newer”-buttons.

The analysis tabs

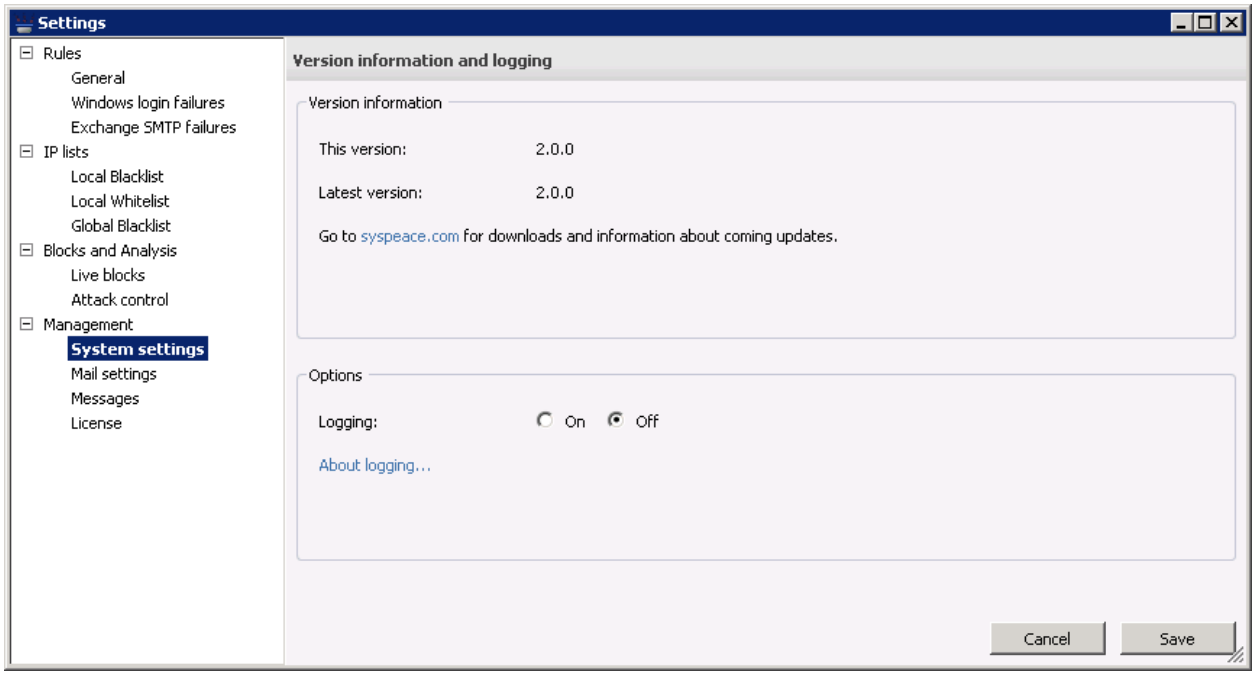
On these screens you will see how login attempts on your computer are distributed over the course of a day, over the course of a week and over the course of a month, respectively. The underlying data is filtered according to the settings you chose on the previous “Access information” tab.


Settings
Rules
General
Windows login failures
Exchange SMTP failures
IP lists
Local Blacklist
Local Whitelist
Global Blacklist
Blocks and Analysis
Live blocks
Attack control
Management
System settings
Mail settings
Messages
License
Show all Windows logon events
Access information
Daily analysis
Weekly analysis
Monthly analysis
Events per hour: 2012-11-25 - 2013-01-29
50
40
30
20
10
0
8 9 10 11 12 13 14 15 16 17 18 21 23


Settings
Rules
General
Windows login failures
Exchange SMTP failures
IP lists
Local Blacklist
Local Whitelist
Global Blacklist
Blocks and Analysis
Live blocks
Attack control
Management
System settings
Mail settings
Messages
License
Show all Windows logon events
Access information
Daily analysis
Weekly analysis
Monthly analysis
Events per weekday: 2012-11-25 - 2013-01-29
40
30
20
10
0
Monday
Tuesday
Wednesday
Thursday
Friday
Saturday
Sunday


Settings
Rules
General
Windows login failures
Exchange SMTP failures
IP lists
Local Blacklist
Local Whitelist
Global Blacklist
Blocks and Analysis
Live blocks
Attack control
Management
System settings
Mail settings
Messages
License
Show all Windows logon events
Access information
Daily analysis
Weekly analysis
Monthly analysis
Events per day in month: 2012-11-25 - 2013-01-29
30
25
20
15
10
5
0
2 4 6 8 10 12 14 16 18 20 22 24 26 28 30
1 3 5 7 9 11 13 15 17 19 21 23 25 27 29 31

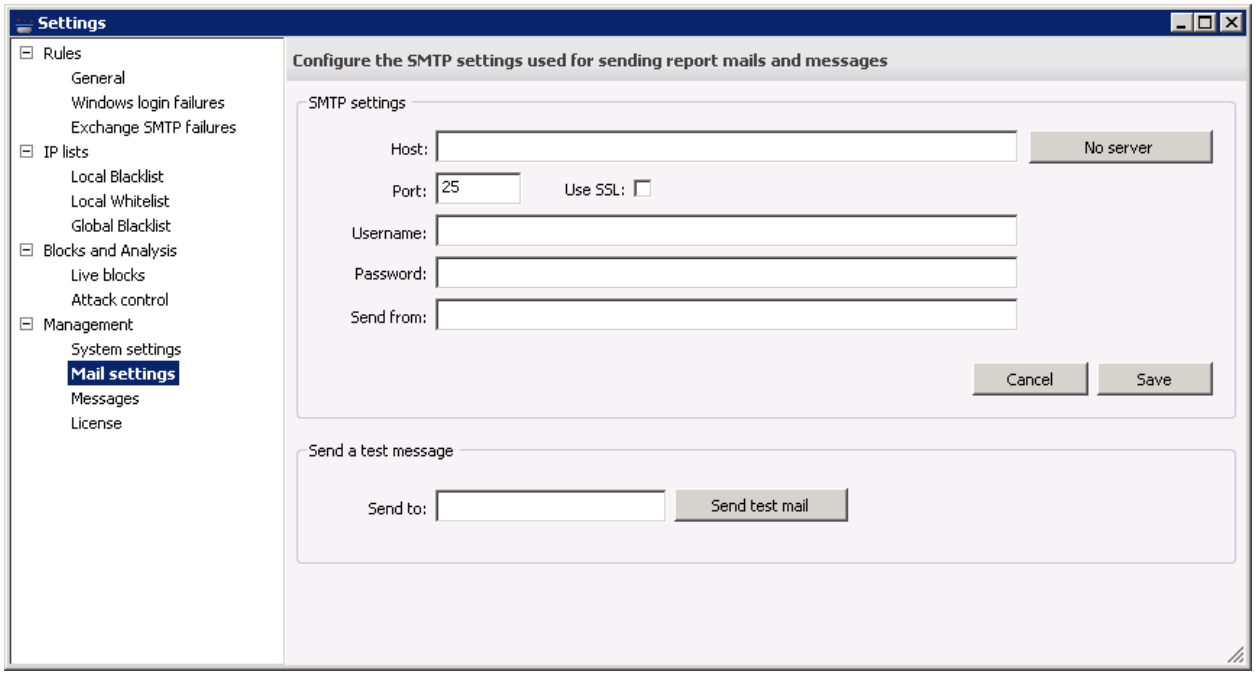
Management → System settings



System settings 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 us in the support process.

Management → Mail settings



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

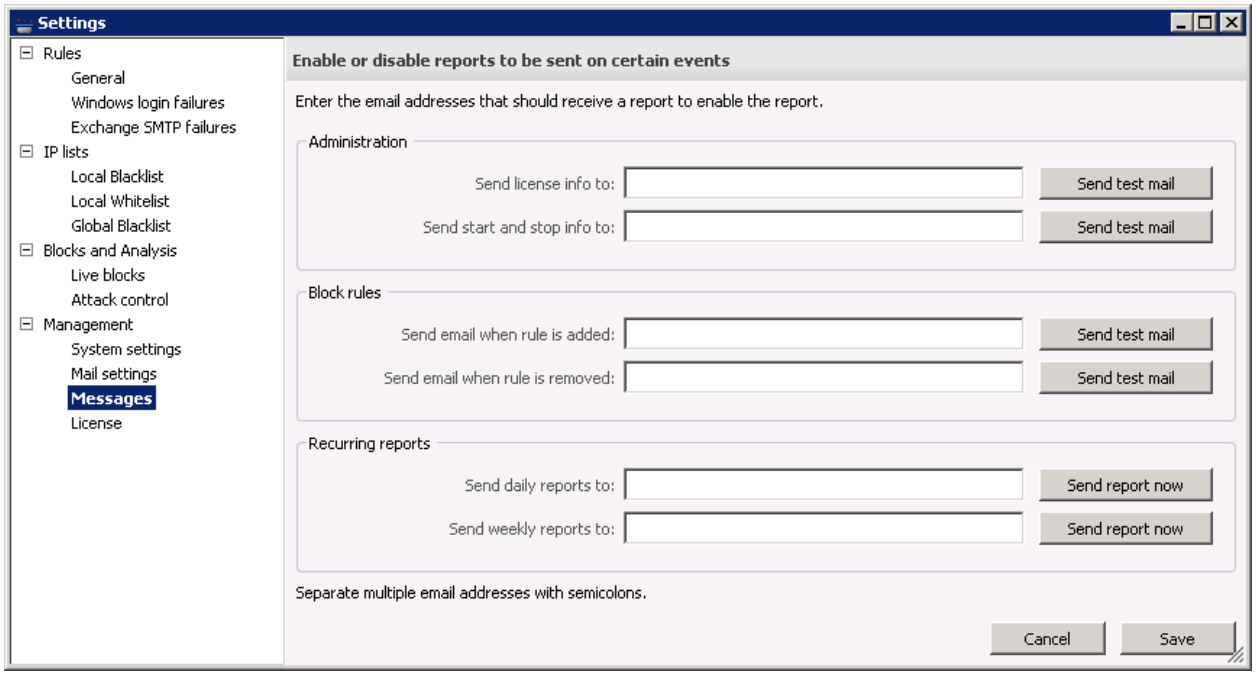
Supply the details of your SMTP server in the text fields. “Sent from” will be the address that the messages are all sent from. Depending on your SMTP server configuration, you may need to pick an address in your domain for the SMTP server to allow the messages.

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.

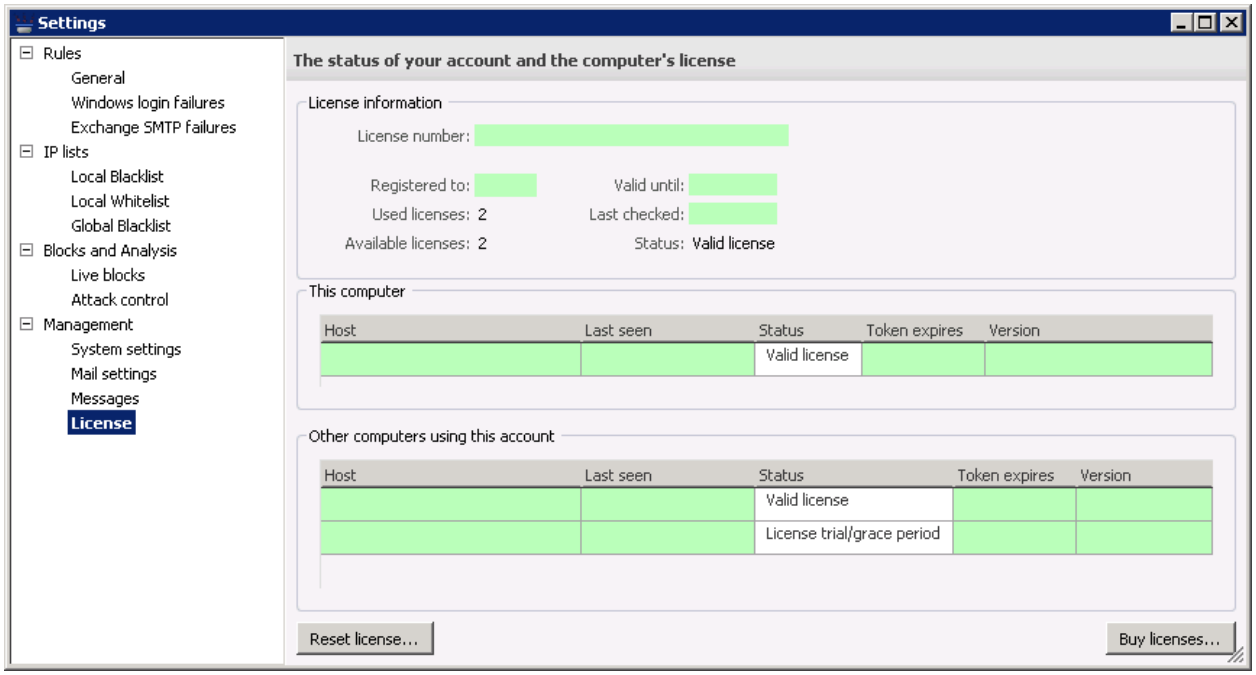
This panel will be disabled if no SMTP server is configured in Management → Mail settings.

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 computer's license status and the other computers 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 computer tables: (the screenshot has been altered to remove any addresses)

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

To buy licenses from the Syspeace Licenses site, click **Buy licenses**.

To disassociate your computer 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.

Troubleshooting

Here's a list on what to check for if Syspeace seems to be malfunctioning or you believe there is an error somewhere

1. Make sure you've enabled the firewall (as described in ***Firewall***)

2. Make sure you've enabled the auditing (as described in ***Auditing***)

3. Verify that the server can reach https://s.syspeace.com/. (If you go to this link in a web browser, you should be redirected to the main Syspeace web site.)

4. In some instances, when running Terminal Server there's actually the scenario where the Windows server itself fails to obtain the source IP address of the login attempt (you can verify this by checking the Windows event log and look for **Source Network Address:**) Sometimes, that entry is empty, thus disabling Syspeace from actually having anything to block. In that case, it is not much that Syspeace can do.

5. In any applicable firewall or antivirus software, allow Syspeace access to https://s.syspeace.com/ (port 443).

6. Verify any proxy settings, if applicable.

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. 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"

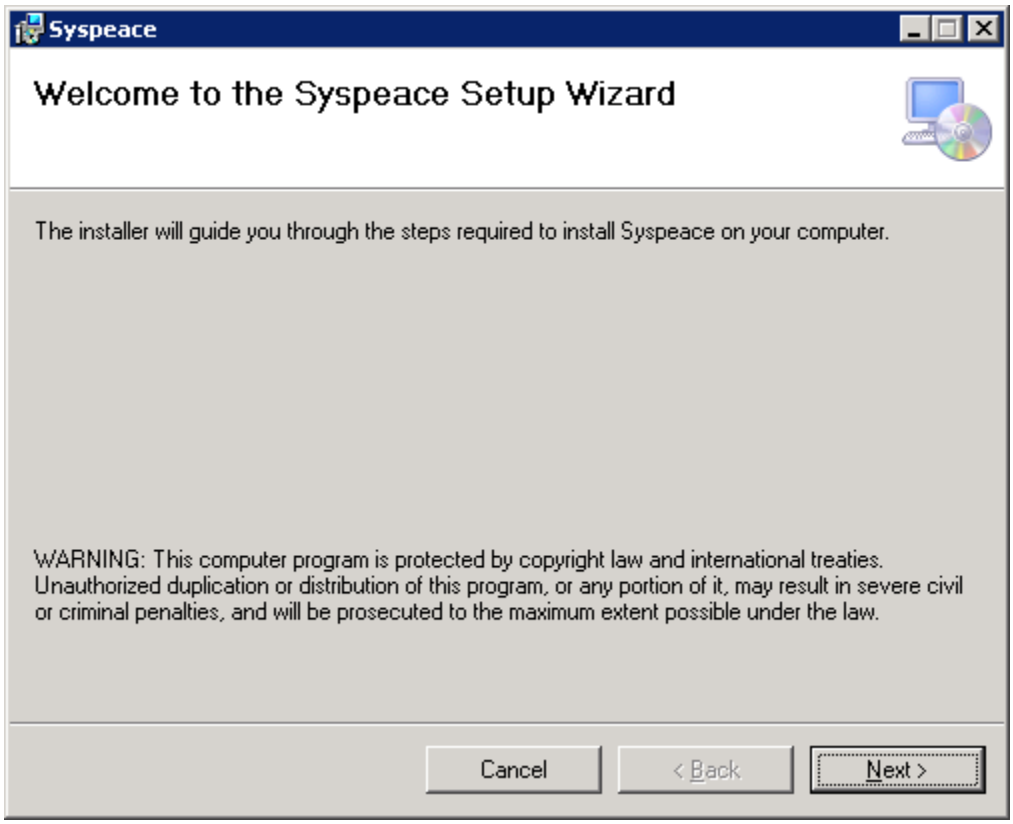
8. If you want to submit logs to us, start Syspeace, go to ***Management → System settings***, enable logging and start the service.
   The log file is created in a subfolder of the Syspeace installation folder.

Contact

Please send any questions or thoughts to syspeace@treetop.se.

Appendix A: Syspeace Setup Wizard step by step

Welcome



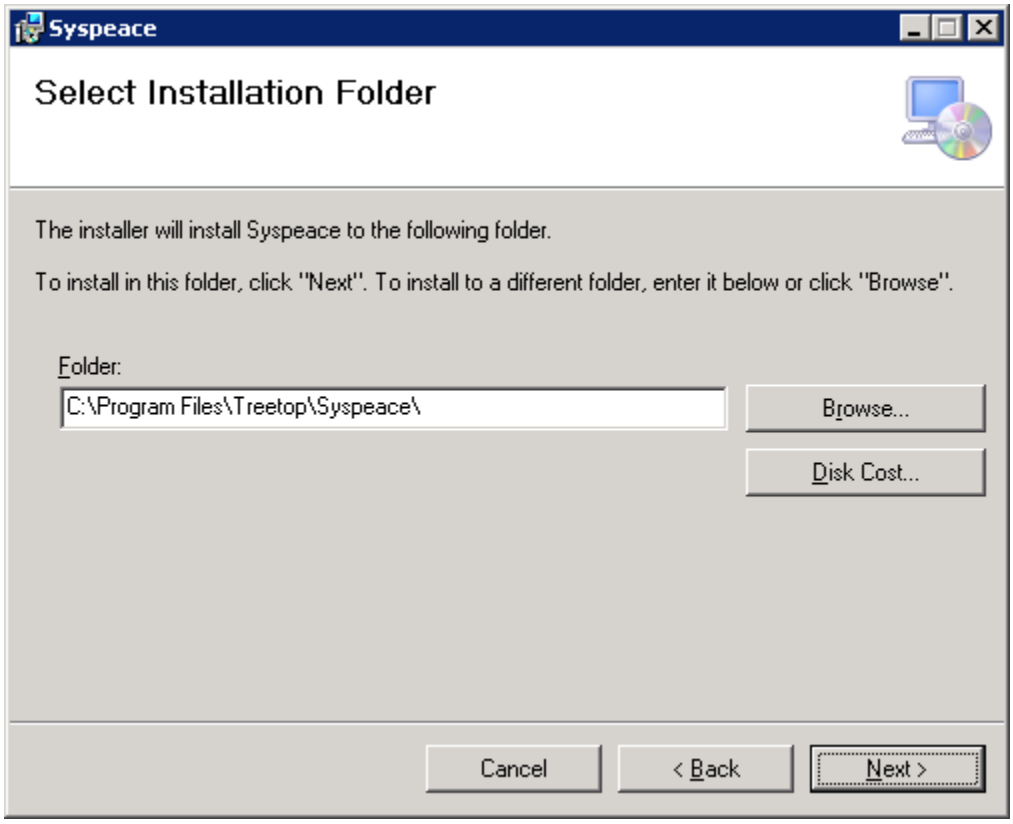
Press **Next** to continue.

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

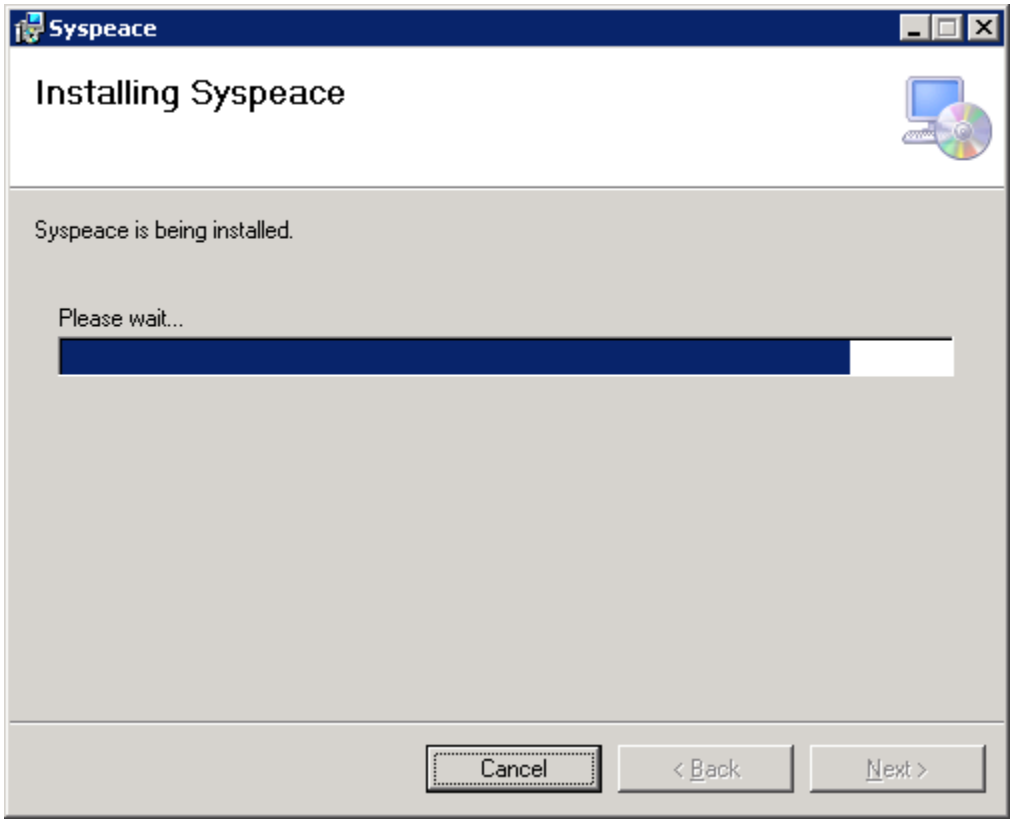


Select the folder to install Syspeace into using the **Browse** button, or by manually entering the path to a folder.

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

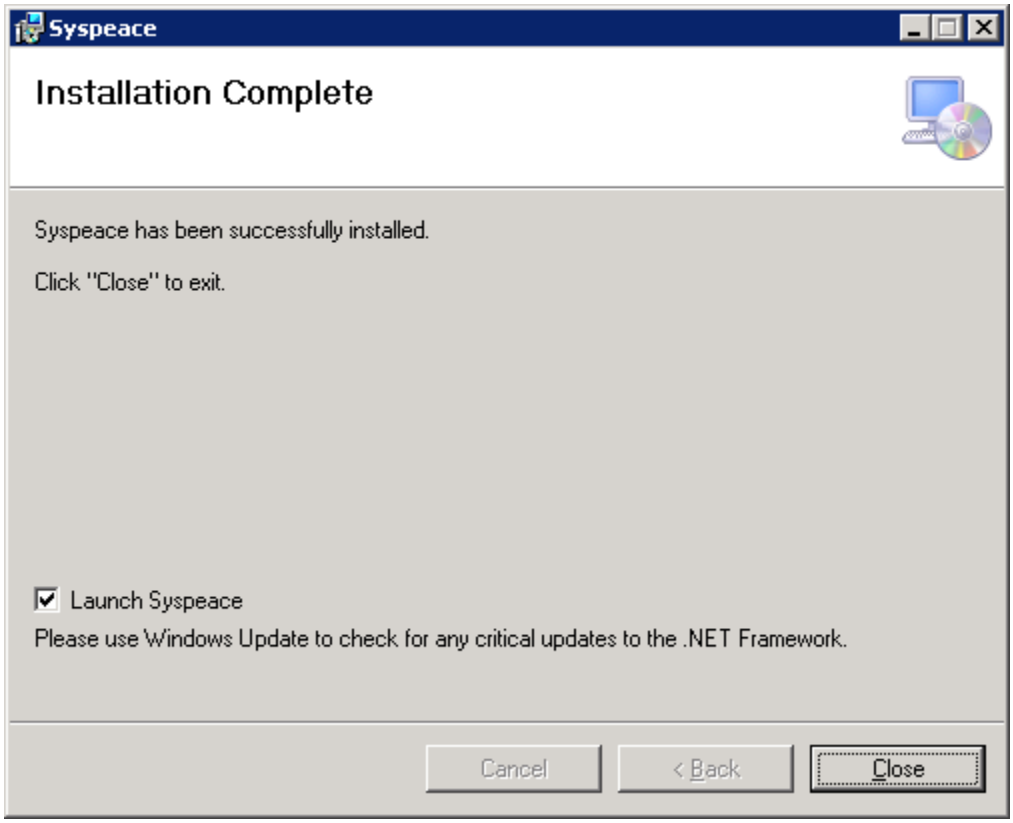
Press **Next** to start the installation.

Installing Syspeace



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

Installation Complete



Uncheck the **Launch Syspeace** check box if you do not want to launch Syspeace immediately.

Press **Close** to exit the installer.