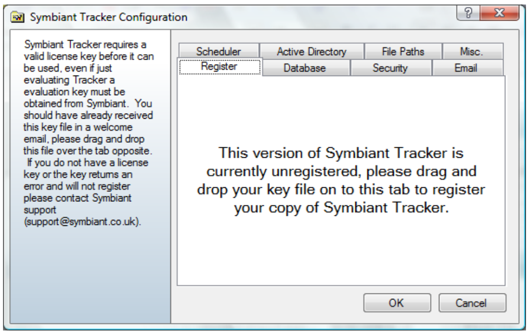
Symbiant Tracker

Configuration Guide

Before you can begin using Tracker you must configure the system. Once Tracker has been installed a Configuration Utility will appear. If this is the first time you have installed Tracker the following screen will be displayed:

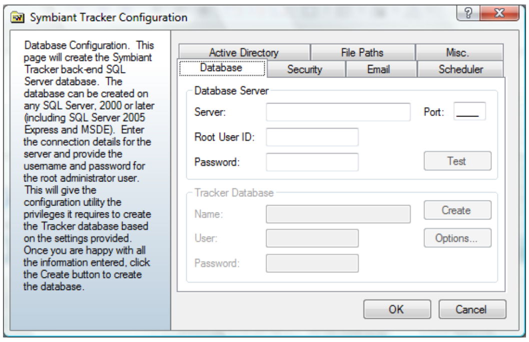


Symbiant Tracker requires a valid license key before it can be used, even if just evaluating Tracker a evaluation key must be obtained from Symbiant. You should have already received this key file in a welcome email, please drag and drop this file over the tab opposite. If you do not have a license key or the key returns an error and will not register please contact Symbiant support (support@symbiant.co.uk).

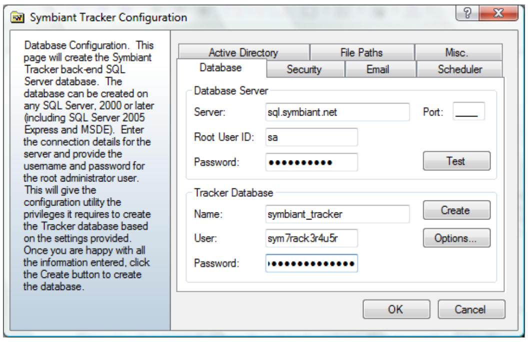
This version of Symbiant Tracker is currently unregistered, please drag and drop your key file on to this tab to register your copy of Symbiant Tracker.

Simply drag and drop the tracker.key file supplied by Symbiant over the tab to register your copy of Tracker. If you do not yet have a key file, please contact your Symbiant Tracker sales representative. They will be able to email you either an evaluation license or a full license if you have already purchased the package.

This done an alert will inform you that you have successfully registered (or provide further instructions) and the register tab will disappear, displaying:



Database Configuration. This page will create the Symbiant Tracker back-end SQL Server database. The database can be created on any SQL Server, 2000 or later (including SQL Server 2005 Express and MSDE). Enter the connection details for the server and provide the username and password for the root administrator user. This will give the configuration utility the privileges it requires to create the Tracker database based on the settings provided. Once you are happy with all the information entered, click the Create button to create the database.



Database Configuration. This page will create the Symbiant Tracker back-end SQL Server database. The database can be created on any SQL Server, 2000 or later (including SQL Server 2005 Express and MSDE). Enter the connection details for the server and provide the username and password for the root administrator user. This will give the configuration utility the privileges it requires to create the Tracker database based on the settings provided. Once you are happy with all the information entered, click the Create button to create the database.

Server: sql.symbiant.net
Port:
Root User ID: sa
Password: ••••••••••
Name: symbiant_tracker
User: sym7rack3r4u5r
Password: ••••••••••••••

Here the Configuration Utility will set-up the database used by Tracker to store the programs data. The database must be installed on a Microsoft SQL Server 2000 or later database. Simply enter the required configuration details and click [Create].

Database Server

Server The SQL Server where the Tracker database should be installed.

Port If the SQL Server uses a different port to the standard for security reasons, enter that otherwise leave port blank.

Root User ID The administrator user for the database, this user should have full sa privileges.

Password The password for the administrator user.

Click the [Test] button to check that the details entered are valid and can be used to create the database.

Tracker Database

Name The name for the new Tracker database, i.e. SymbiantTracker

User The name of the login user to connect to the database, i.e. symtrackusr

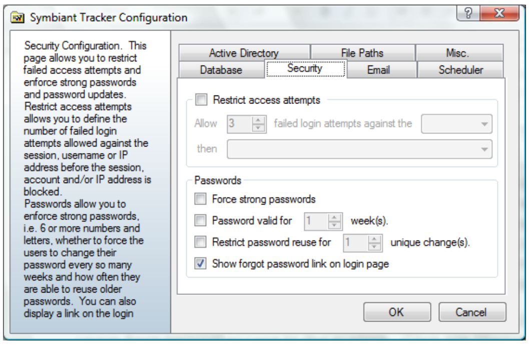
Password The password for the login user, i.e. s9m7rack3r

The password must be a strong and secure password otherwise SQL Server will reject it and you will be forced to enter a stronger password. Strong passwords include both letters and numbers.

Click [Create] and the Configuration Utility will create the Tracker 4 database.

> After creating the database, it is possible to use the [Options] button to rebuild the index for the Tracker database. The index is used by SQL server much like the index of a book allowing the database to quickly find relevant information. Overtime this index can become fragmented, rebuilding the index will tidy this up and can provide significant performance gains. Other options include a quick backup and restore of the complete database as well as an option to delete the database completely.

Next the Security settings should be configured. These allow you to implement measures to prevent unauthorised users from gaining access to the system. Click the [Security] tab to display:



Security Configuration. This page allows you to restrict failed access attempts and enforce strong passwords and password updates. Restrict access attempts allows you to define the number of failed login attempts allowed against the session, username or IP address before the session, account and/or IP address is blocked. Passwords allow you to enforce strong passwords, i.e. 6 or more numbers and letters, whether to force the users to change their password every so many weeks and how often they are able to reuse older passwords. You can also display a link on the login

□ Restrict access attempts

Allow 3 failed login attempts against the

then

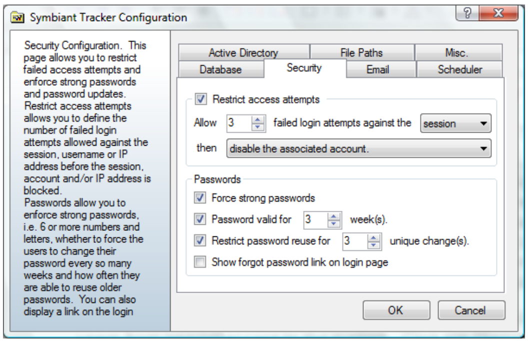
Passwords

□ Force strong passwords

□ Password valid for 1 week(s).

□ Restrict password reuse for 1 unique change(s).

☑ Show forgot password link on login page



Security Configuration. This page allows you to restrict failed access attempts and enforce strong passwords and password updates. Restrict access attempts allows you to define the number of failed login attempts allowed against the session, username or IP address before the session, account and/or IP address is blocked. Passwords allow you to enforce strong passwords, i.e. 6 or more numbers and letters, whether to force the users to change their password every so many weeks and how often they are able to reuse older passwords. You can also display a link on the login

☑ Restrict access attempts

Allow 3 failed login attempts against the session

then disable the associated account.

Passwords

☑ Force strong passwords

☑ Password valid for 3 week(s).

☑ Restrict password reuse for 3 unique change(s).

□ Show forgot password link on login page

Tracker allows you to restrict access attempts by checking the relevant box. Here specify the number of attempts a user can make to access the system before Tracker acts. Attempts can be recorded against:

session A session is a unique identifier created by the server when a user accesses Tracker. A session remains active whilst there is activity, i.e. the users is actively using Tracker or until a set amount of inactivity has transpired (this is defined on the server). Some browsers will also reset the sessions when the browser window is closed and opened again.

username The username is any text entered into the username login box. This basically means that Tracker will only block attempts made against the same entered username, allowing them to try other usernames indefinitely.

IP address Generally the IP address should uniquely identify the computer, however on some networks more than one computer may share the same IP address.

If Tracker records the set number of failed attempts against the defined mechanism it will block the session forcing the user to wait until the session expires (or on some browsers close and re-open the browser) before they can try again. In addition to this it is also possible to:

end the current session. *Basic functionality only.*

disable the associated account. If the account can be ascertained from the details entered, i.e. the username matches a valid username in the Tracker system, that account will be deactivated.

block the IP address. This will in effect ban the current workstation, preventing it from being used to attempt to access Tracker again (note that some networks do not provide unique IP addresses to each computer, if this is the case for your network do not use this function).

disable the account and block the IP address. This basically performs all the above functions.

The password functions allow you to enhance security by ensuring that users choose unique strong passwords:

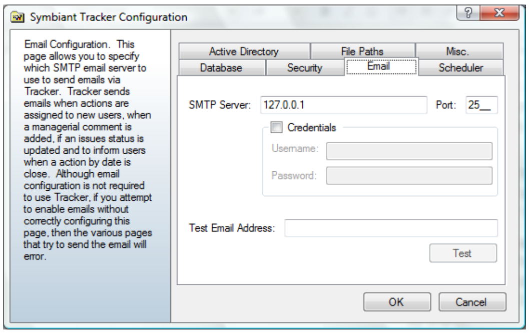
Force strong password Checking this will force the user to enter a strong password, a strong password in Tracker is identified as containing more than 6 characters and using both letters and numbers.

Password valid for ... This will force users to change their password after a defined number of weeks. Users will be warned when the limit of their password is nearing, they can then quickly enter a new password. However if they choose to ignore these warnings when the password expires their account will be locked and an administrator will need to reset it for them.

Restrict password reuse for ... This ensures that users do not simply keep reusing the same few passwords. Tracker will record each password used and ensure they do not reuse if for at least the number of unique changes specified.

Show forgot password link on login page This provides a secure way of allowing users to reset forgotten passwords without needing to contact an administrator. It will not reactivate disabled accounts, but if the user has simply forgotten their password it will allow then to reset it and get the new password emailed to them.

Next the Email settings should be configured. These are required to maker use of the built in email alerts contained in Tracker. Click the [Email] tab to display:



Email Configuration. This page allows you to specify which SMTP email server to use to send emails via Tracker. Tracker sends emails when actions are assigned to new users, when a managerial comment is added, if an issues status is updated and to inform users when a action by date is close. Although email configuration is not required to use Tracker, if you attempt to enable emails without correctly configuring this page, then the various pages that try to send the email will error.

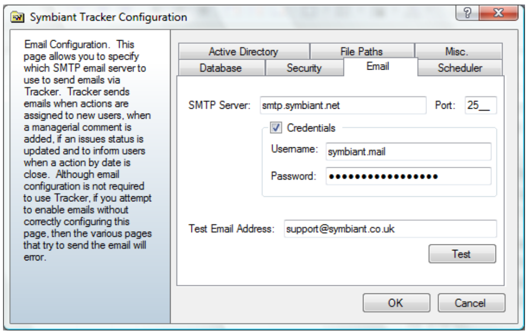
SMTP Server: 127.0.0.1 Port: 25__

□ Credentials

Username:

Password:

Test Email Address:



Email Configuration. This page allows you to specify which SMTP email server to use to send emails via Tracker. Tracker sends emails when actions are assigned to new users, when a managerial comment is added, if an issues status is updated and to inform users when a action by date is close. Although email configuration is not required to use Tracker, if you attempt to enable emails without correctly configuring this page, then the various pages that try to send the email will error.

SMTP Server: smtp.symbiant.net Port: 25__

☑ Credentials

Username: symbiant.mail

Password: ●●●●●●●●●●●●●●●●●

Test Email Address: support@symbiant.co.uk

Here you enter the mail server settings and credentials if required.

SMTP Server The name of the SMTP mail server to connect to.

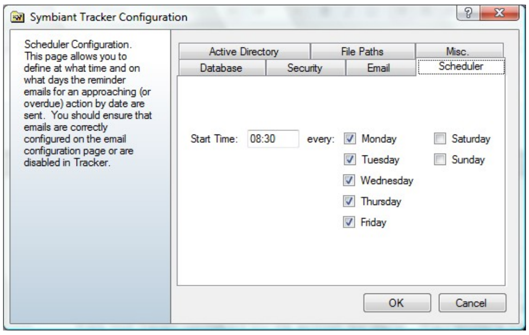
Port Generally the mail server port is 25, if this is different for your server enter the correct value in port.

Username If your SMTP server requires login credentials, check the Credentials box and enter the username to login and send emails.

Password The password for the SMTP user.

To check that the email settings have been entered correctly, you can enter an email address and click the [Test] button. This will send an email to the specified address, if the email arrives then the SMTP configurations are correct.

Next the Scheduler configures when the email reminders are triggered. Email reminders are sent when an action has not been updated by its action by date. Reminders can be sent a defined number of days before the action is due via the main Tracker interface. Here, we configure the days the reminder task will be run and at what time, click the [Scheduler] tab to configure and display:

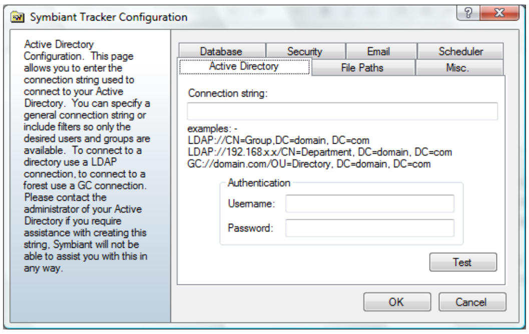


Scheduler Configuration. This page allows you to define at what time and on what days the reminder emails for an approaching (or overdue) action by date are sent. You should ensure that emails are correctly configured on the email configuration page or are disabled in Tracker.

Start Time: 08:30 every: ☑ Monday ☐ Saturday
☑ Tuesday ☐ Sunday
☑ Wednesday
☑ Thursday
☑ Friday

This screen is already preconfigured to run the email reminder every weekday at 8:30 in the morning. This is based on the servers date and time. Note that just because this is set to run every weekday doesn't mean that emails will be sent every day, emails are only sent when action due dates are approaching or have been passed.

The next tab is for Active Directory users only, if you have an Active Directory enabled license and wish to connect to an Active Directory to allow accounts to be created from the directory and network logins, click the [Active Directory] tab to display:

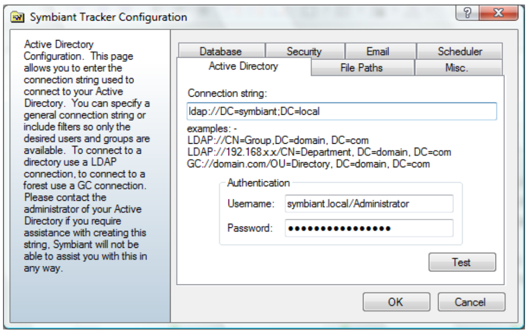


Active Directory Configuration. This page allows you to enter the connection string used to connect to your Active Directory. You can specify a general connection string or include filters so only the desired users and groups are available. To connect to a directory use a LDAP connection, to connect to a forest use a GC connection. Please contact the administrator of your Active Directory if you require assistance with creating this string, Symbiant will not be able to assist you with this in any way.

Connection string:

examples: -
LDAP://CN=Group,DC=domain, DC=com
LDAP://192.168.x.x/CN=Department, DC=domain, DC=com
GC://domain.com/OU=Directory, DC=domain, DC=com

Authentication
Username:
Password:



Active Directory Configuration. This page allows you to enter the connection string used to connect to your Active Directory. You can specify a general connection string or include filters so only the desired users and groups are available. To connect to a directory use a LDAP connection, to connect to a forest use a GC connection. Please contact the administrator of your Active Directory if you require assistance with creating this string, Symbiant will not be able to assist you with this in any way.

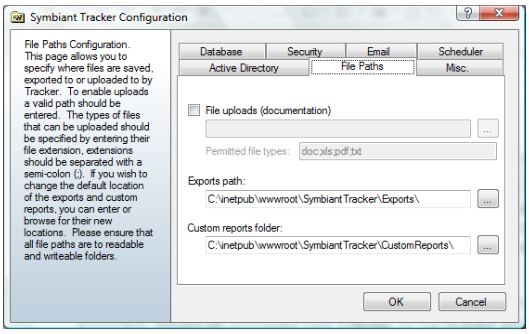
Connection string: ldap://DC=symbiant;DC=local

examples: -
LDAP://CN=Group,DC=domain, DC=com
LDAP://192.168.x.x/CN=Department, DC=domain, DC=com
GC://domain.com/OU=Directory, DC=domain, DC=com

Authentication
Username: symbiant.local/Administrator
Password: ••••••••••••••••

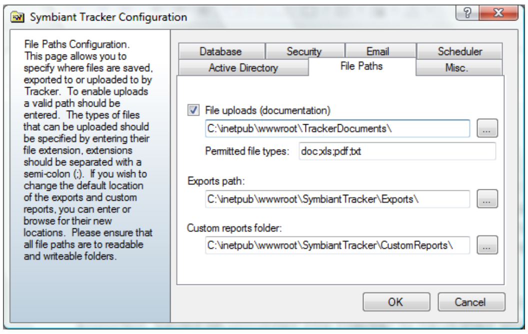
To connect to an Active Directory via Tracker an LDAP or GC connection string is required and any username or password required to authenticate the connection. You can click [Test] to check if the details entered are correct and a connection can be established. Please read the Enabling Active Directory user guide for more details on configuring an Active Directory for Tracker, there are some important account and server changes that must be implemented.

Tracker allows the files that are routinely exported, saved or uploaded into Tracker to have their storage paths defined. Click the [File Paths] tab to display:



File Paths Configuration. This page allows you to specify where files are saved, exported to or uploaded to by Tracker. To enable uploads a valid path should be entered. The types of files that can be uploaded should be specified by entering their file extension, extensions should be separated with a semi-colon (;). If you wish to change the default location of the exports and custom reports, you can enter or browse for their new locations. Please ensure that all file paths are to readable and writeable folders.

☐ File uploads (documentation)
Permitted file types: doc;xls;pdf;txt
Exports path: C:\inetpub\wwwroot\SymbiantTracker\Exports\
Custom reports folder: C:\inetpub\wwwroot\SymbiantTracker\CustomReports\



File Paths Configuration. This page allows you to specify where files are saved, exported to or uploaded to by Tracker. To enable uploads a valid path should be entered. The types of files that can be uploaded should be specified by entering their file extension, extensions should be separated with a semi-colon (;). If you wish to change the default location of the exports and custom reports, you can enter or browse for their new locations. Please ensure that all file paths are to readable and writeable folders.

☑ File uploads (documentation)
C:\inetpub\wwwroot\TrackerDocuments\
Permitted file types: doc;xls;pdf;txt
Exports path: C:\inetpub\wwwroot\SymbiantTracker\Exports\
Custom reports folder: C:\inetpub\wwwroot\SymbiantTracker\CustomReports\

It is important to ensure that all paths entered here are to valid folders that have both read and write privileges available for internet users of the Tracker application.

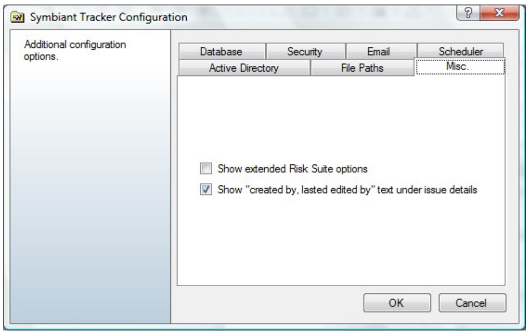
File Uploads Check this to allow users to upload files to Tracker, enter the path to where the files are stored or click the [...] button to browse for the folder.

File Types The permitted file types are the files that are allowed to be uploaded to Tracker, these should be restricted to secure files only, i.e. do not permit executables or potentially harmful files to be uploaded. Separate each type of file that can be uploaded with a semi-colon (;).

Export Path The export path is the location where all XML and CSV files are exported to when exporting reports or exporting archives before they are deleted or for backup purposes. Enter the directory or click the [...] button to browse for the folder.
Note, this directory may become very full over time, the system does not link to any files in here except straight after they are created, so it can be periodically cleared.

Custom Reports This is where the custom report files are stored that are saved by users. Enter the directory or click the [...] button to browse for the folder.

Finally there are a couple of miscellaneous settings that can optionally be enabled under the [Misc.] tab.



□ Show extended Risk Suite options

☑ Show "created by, lasted edited by" text under issue details

If you are also a Symbiant Risk Suite user and wish to track issues migrated from Risk Suite to Tracker, check the [Show extended Risk Suite options] to provide additional functionality specific to Risk Suite users.

Some institutions require that details of who created an issue and who last edited it be displayed for each issue. To display this text at the bottom of each issue in Tracker, check the relevant check box.

That completes all the required configuration settings. Click [OK] to save the setting and begin using Tracker.