

SecureAware®

SecureAware SA Manual

- for system administrators

Applies to SecureAware version 3.7.0 and later versions

Document date: February 2010

About this document

A system administrator is a special role within SecureAware, and the primary tasks involve general system management tasks. In a default installation the system administrator has limited access to the SecureAware content and user database, these administration tasks are the super users responsibility.

Table of contents	
Installation	3
Upgrade	5
Changing location of the database	6
Procedure	6
MS SQL / MySQL database.....	10
Security	12
License key system	12
Secure Communication	13
Backup – Restore	20
Portals	23
Creating a new portal	23
Installing the license	24
Log in to the new portal	25
General settings	27
Date formats	29
Mail server settings	30
System Administrators	32
LDAP (AD connection)	33
Setting up LDAP.....	33
Internet Information Server	37
Single sign on.....	39
Microsoft SQL Server 7, 2000 or 2005	41
Installation and upgrade on a Linux server	46
SecureAware Support	50
Automatic log off	52
SecureAware logging capabilities	53
Contact Information	55

Installation

Before you start the installation

Be sure that you have administrator access rights to the computer where SecureAware will be installed. On newer Windows installation you need to start the installer with the option “Run as administrator”.

Special SecureAware settings

If you have special requirements about the SecureAware installation, you need to apply these after the installation.

Installing SecureAware from a download

When the SecureAware installer is downloaded from the Internet, it will be either a single file installation application, or the compressed zip file with all the files from the installation CD (includes all setup files and manuals)

To start the installer you need to locate and execute the **sainstall.exe** file.

Installing SecureAware from a CD

The SecureAware installer will automatically start when the SecureAware CD is inserted into the computer. If auto start is disabled, you will need to locate and execute the **sainstall.exe** file on the CD.



The installation procedure

The SecureAware installation application should guide you through the full installation which includes:

- Accepting the End user license agreement
- Checking the Java version
 - Downloading the java installer if not present locally
 - Running the java installer
- Checking Tomcat web server
 - Downloading tomcat installer if not present locally
 - Running the SecureAware tomcat web server installer
- Downloading the SecureAware application installer if not present locally

- Running the SecureAware application installer
- Registering the SecureAware service and installation cleanup
- Starting a local browser to finish the installation online

When the browser opens at <http://localhost:8080>, you will see a screen displaying “Welcome to SecureAware. The application is currently in management mode....”

- Click  ‘Continue the installation or the upgrade’
- Database initialization will begin . Wait for the message: “The Database was successfully upgraded. Click ‘Return to SecureAware’ (this will log you in as System Administrator)
- Upload the license file that you received from Neupart and click ‘Upload’
- Log out and in as superuser (Login: su password: snRt!32w) and accept the End User License Agreement.

Note:

The license files are named with a combination of the client company name, the product modules and limitations in the license, expiration date and a “.lic” files extension.

Note that the license validation code and signature will be broken if any information within the file is changed, so special care should be used when handling the license file. E-Mail servers are known to change attached documents, so when transporting the license with emails, we will wrap the file in a container – like a zip compress archive.

Note that zip wrapped license files need to be unpacked before they are uploaded to SecureAware.

Upgrade

Backup your installation before doing the upgrade

Before upgrading a SecureAware installation, please ensure that you have the option to roll-back the upgrade and continue with your current SecureAware version. In a standard installation SecureAware files are located in two folders:

Application and configuration in C:\Program Files\Neupart\SecureAware3

Database in C:\Windows\Database

Before making a full copy of these folders, you need to stop the SecureAware3 service. This will ensure that the database files are closed and not used by the SecureAware application.

Upgrade from earlier versions than 2.0.2 –please contact Neupart at support@neupart.com for upgrade instructions

Upgrade to version 3.7.0

Please use this guide to upgrade SecureAware to version 3.7.0.

- Stop the SecureAware service and backup your database.
- Stop the IIS (if this is used).
- Download SecureAware version 3.7.0 following the link you received in the release mail from Neupart.
- Execute the installation program
- When you click "Finish" at the end of the installation process, SecureAware will open in your browser.
- Click "Continue the installation or upgrade".
- Type the upgrade password **snRt!32w** and click OK
- When the database upgrade has ended, click "Return to SecureAware".
- Start the IIS (if this is used).

Changing location of the database

In some situations it can be useful to change the location of the SecureAware database. For example, when you want to locate the database separate from the application installation. To do so, you must have administration privileges on the computer where SecureAware is installed.

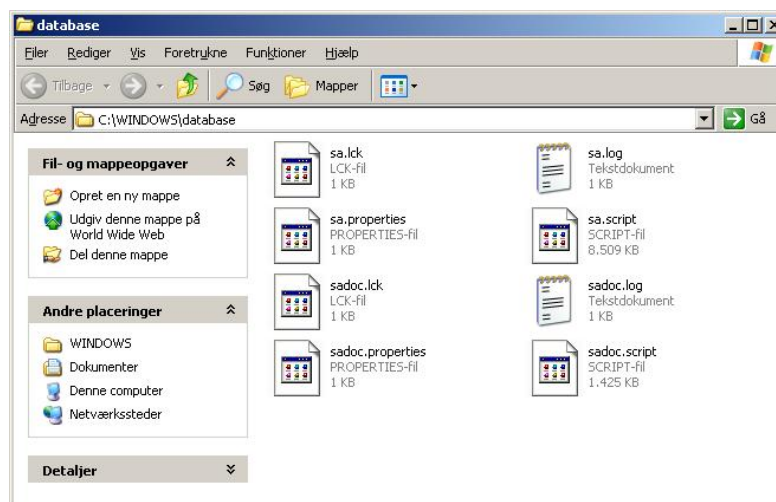
Procedure

To change the location of the SecureAware database, do as follows:

1. Confirm that the SecureAware Service is stopped. If the Service is running, it has to be stopped before going any further.

When the 'Secure Aware Service' is stopped, you should make a database backup, before proceeding.

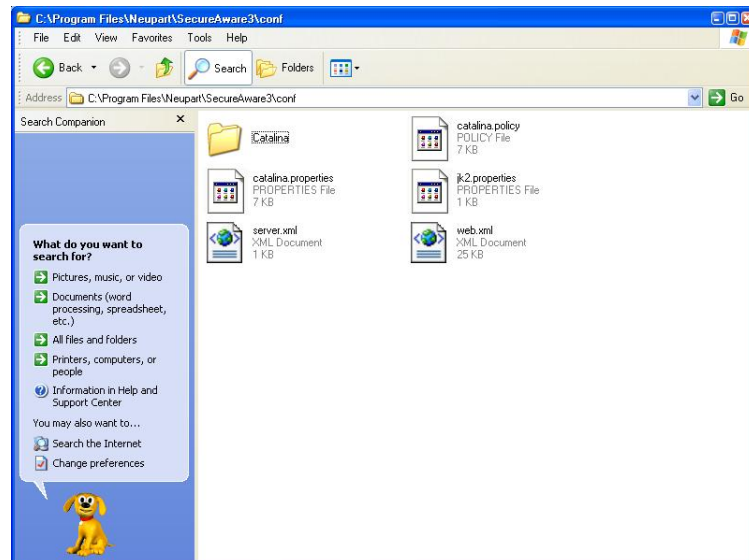
The SecureAware database contains 8 files, and is placed in the folder C:\Windows\Database



After you have made your backup, you can move the destination of the database.

Move the 8 files to a location of your choice, and then write down the path to the files.

SecureAware needs to know where the database is located, so you have to manually make a few changes in one of the SecureAware configuration file named ‘*catalina.properties*’. It is located in *C:\Program Files\Neupart\SecureAware3\conf* as shown below.



Before you make any changes in the configuration file ‘*catalina.properties*’ you should make a backup of the original file. Open the ‘*catalina.properties*’ file in a text editor.

```

catalina.properties - Notepad
File Edit Format View Help
# SecureAware database connection settings

## HypersonicSQL
hibernate.dialect org.hibernate.dialect.HSQLDialect
hibernate.connection.driver_class org.hsqldb.jdbcDriver
hibernate.connection.username sa
hibernate.connection.password
hibernate.connection.url jdbc:hsqldb:../database/sa

document.dialect org.hibernate.dialect.HSQLDialect
document.connection.driver_class org.hsqldb.jdbcDriver
document.connection.username sa
document.connection.password
document.connection.url jdbc:hsqldb:../database/sadoc

## MS SQL Server
#hibernate.dialect org.hibernate.dialect.SQLServerDialect
#hibernate.connection.driver_class net.sourceforge.jtds.jdbc.Driver
#hibernate.connection.username secureaware
#hibernate.connection.password secureaware
#hibernate.default_schema dbo
#hibernate.default_catalog secureaware
#hibernate.connection.url
jdbc:jtds:sqlserver://localhost:1433/secureaware;tds=8.0;lastupdatecount=true

#document.dialect org.hibernate.dialect.SQLServerDialect
#document.connection.driver_class net.sourceforge.jtds.jdbc.Driver
#document.connection.username secureaware
#document.connection.password secureaware
#document.default_schema dbo
#document.default_catalog secureaware
#document.connection.url
jdbc:jtds:sqlserver://localhost:1433/secureaware;tds=8.0;lastupdatecount=true

## MySQL
#hibernate.dialect org.hibernate.dialect.MySQLInnoDBDialect
#hibernate.connection.driver_class com.mysql.jdbc.Driver

```

In the `'catalina.properties'` file, are there two lines there point to the location of the database. Those two lines are shown below in red, and the database is highlighted with yellow.

```
## HypersonicSQL
hibernate.dialect org.hibernate.dialect.HSQLDialect
hibernate.connection.driver_class org.hsqldb.jdbcDriver
hibernate.connection.username sa
hibernate.connection.password
hibernate.connection.url jdbc:hsqldb:../database/sa
```

```
## HypersonicSQL Document Database
document.dialect org.hibernate.dialect.HSQLDialect
document.connection.driver_class org.hsqldb.jdbcDriver
document.connection.username sa
document.connection.password
document.connection.url jdbc:hsqldb:../database/sadoc
```

It's optional to use relative or absolute paths.

If you chose to use relative paths, the start in folder `'system32'` under `'Windows'`. In both cases you have to use the forward slashes (`/`).

One example: if you want to place your database in the following directory and want to use absolute paths:

```
C:\newmap\secureaware3\
```

Below you can see the changes in the two lines in the `'catalina.properties'` file. Note the change from back slash (`\`) to forward slash (`/`).

First line:

hibernate.connection.url jdbc:hsqldb:./database/sa

- change to

hibernate.connection.url jdbc:hsqldb:c:/nymappe/secureaware3/sa

Second line:

document.connection.url jdbc:hsqldb:./database/sadoc

- change to

document.connection.url jdbc:hsqldb:c:/nymappe/secureaware3/sadoc

When the changes are made, save the '*catalina.properties*' configurations file and close the file.

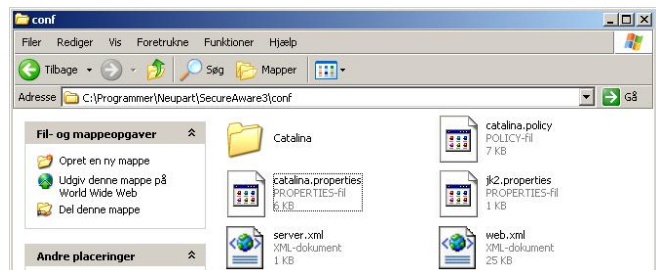
Star the SecureAware service again. You can now connect to SecureAware with the browser.

MS SQL / MySQL database

SecureAwares uses as default a HypersonicSQL database . If you want to use MS SQL or MySQL instead, please follow this guide.

When SecureAware is installed, stop the service and find the configuration file **catalina.properties** in `C:\Programs\Neupart\SecureAware3\conf`

This file is the one SecureAware uses to communicate with the database. Open the file in a text editor.



Below the content of the file is shown. Start with commenting out (put # in front of each line) the 10 lines referring to the native Hypersonic SQL database. Now remove the # in front of the lines referring to the database you want to use. Below you will see which information you will have to add (explained in blue to the right of each line).

```
# SecureAware database connection settings
```

```
## HypersonicSQL
```

```
hibernate.dialect org.hibernate.dialect.HSQLDialect
hibernate.connection.driver_class org.hsqldb.jdbcDriver
hibernate.connection.username sa
hibernate.connection.password
hibernate.connection.url jdbc:hsqldb:./database/sa
```

```
document.dialect org.hibernate.dialect.HSQLDialect
document.connection.driver_class org.hsqldb.jdbcDriver
document.connection.username sa
document.connection.password
document.connection.url jdbc:hsqldb:./database/sadoc
```

```
## MS SQL Server
```

```
#hibernate.dialect org.hibernate.dialect.SQLServerDialect
#hibernate.connection.driver_class net.sourceforge.jtds.jdbc.Driver
#hibernate.connection.username secureaware (database username)
#hibernate.connection.password secureaware (database password)
#hibernate.default_schema dbo
#hibernate.default_catalog secureaware (database name)
```

```
#hibernate.connection.url jdbc:jtds:sqlserver://localhost:1433/secureaware;tds=8.0;lastupdatecount=true (url for the database)

#document.dialect org.hibernate.dialect.SQLServerDialect
#document.connection.driver_class net.sourceforge.jtds.jdbc.Driver
#document.connection.username secureaware (database username)
#document.connection.password secureaware (database password)
#document.default_schema dbo
#document.default_catalog secureaware (database name)
#document.connection.url jdbc:jtds:sqlserver://localhost:1433/secureaware;tds=8.0;lastupdatecount=true (url for the database)

## MySQL
#hibernate.dialect org.hibernate.dialect.MySQLInnoDBDialect
#hibernate.connection.driver_class com.mysql.jdbc.Driver
#hibernate.connection.url jdbc:mysql://localhost:3306/secureaware (url for the database)
#hibernate.connection.username secureaware (database username)
#hibernate.connection.password secureaware (database password)

#document.dialect org.hibernate.dialect.MySQLInnoDBDialect
#document.connection.driver_class com.mysql.jdbc.Driver
#document.connection.url jdbc:mysql://localhost:3306/secureaware (url for the database)
#document.connection.username secureaware (database username)
#document.connection.password secureaware (database password)
```

Save your changes and start the SecureAware service again. Remember to back up the configuration files. You will need them for future upgrades of SecureAware.

Security

The SecureAware application implements different security features that, combined, provide a service to hold both private and publicly available information. The security system in SecureAware was designed to be highly configurable, so the application can meet requirements in the different environments where it is used.

The SecureAware application operates in a standard java servlet container within a web server and, in the standard installation, uses unencrypted http communication between the clients and the server.

If required the communication can be wrapped in certificate driven SSL encryption and will also operate over VPN tunnels.

Each portal in a SecureAware server can be configured to operate in different security modes from public systems with anonymous access to a fully private system that requires authentication before any content can be accessed.

This document will describe all the different parts that make up the SecureAware security system.

Customer License

The SecureAware application contains a license system, where most of the functionality requires an installed license “key”. The license also controls the available languages, number of users, and the number of separate portals.

The different modules in SecureAware are enabled by uploading a valid license, which is an XML text file. The file contains information about the activation period, to whom the license is issued, the user and portal limitations, and which modules and languages the license grants access to. The file must also be signed with both the SecureAware product key, and a key that is generated for each customer.

License key system

The key system is based on a secure private-public key system, where only the public keys are present in a customer installation. The public keys can be used to unencrypt and verify a license, but cannot be used to change, generate or sign licenses. The private keys are located in a special license generator and will not be available outside of Neupart.

License file

In a SecureAware installation the license is uploaded to a portal using the special built-in system administrator account, and a single server installation can operate multiple portals (each with its own license or the same license if multiple portals are granted within the license). The company information within the license is used in the portal and reports generated by the application.

The license files are named with a combination of the client company name, the product modules and limitations in the license, expiration date and a “.lic” files extension.

Note that the license validation code and signature will be broken if any information within the file is changed, so special care should be used when handling the license file. E-Mail servers are known to change attached documents, so when transporting the license with emails, we may wrap the file in a container – such as a zip compressed archive.

Note that zip wrapped license files must to be unpacked before they are uploaded to SecureAware.

Secure Communication

In a SecureAware installation there are a number of independent systems that need to communicate, and in a standard installation these communication channels are not encrypted. Since the application typically operates in a protected environment (such as an internal company network), the standard configuration will be appropriate for most installations.

Client server communication

All clients use a standard web browser to communicate with the SecureAware application, and the standard protocol is http. This communication can be changed to the SSL encrypted https protocol supported by most browsers, and this is typically implemented using a proxy web server like Apache or Internet Information Server. The proxy then handles all client communications and all proxy requests to the servlet engine running the SecureAware application.

For stronger encryption the http or https communication can be wrapped in an encrypted tunnel provided by services like VPN or SSH.

Using a front-end web server also enables external user authentication, where the users are verified by the front-end server and the user credentials are passed along with the request to log into SecureAware. This enables SecureAware to be part of a single sign on system. A full description of this setup is included in this document.

Application to database communication

The SecureAware application is able to use different back-end database storage engines. The standard installation works with a java based engine that operates within the same virtual environment so all database communication is protected within the engine.

In installations where external database providers are used, the application uses standard JDBC connections, normally based on a TCP/IP communication. The exact communication is vendor specific, but most likely the communication can be protected with certificates and encryption, or by tunneling all communication through a secure channel, like VPN.

Protecting this communication will impact the performance of the application, and because the communication is most likely inside a single server or within a secure net segment in the server area, this protection is most likely not needed.

LDAP user authentication

The SecureAware application can operate in a secure mode where an external user directory is used with the LDAP protocol. In a standard installation unencrypted LDAP protocol communication is used, but the SecureAware implementation supports the SSL encrypted version of the LDAP protocol, and like the other communication this can be tunneled for extended security.

Protecting this communication will not have significant impact on the SecureAware performance as the user authentication is only performed once for each user session.

Web service communication

As with the client communication, the web service clients use the http protocol but can be protected with the SSL encrypted https protocol.

The Screen Saver application uses http to retrieve information, and as this information is intended for public display the communication is not encrypted.

Portal Security modes

The SecureAware system supports different security modes, so system administrators can select the appropriate one for their environment. Basically the modes configure access for anonymous, internal and external defined users. Users are able to authenticate using different systems including form based prompts, cookies, URL parameters, and external authentication.

Protected Mode

Anonymous and SecureAware internal users.

In protected mode, some parts of the portal are available to anonymous users with no authentication, and some parts of the application are available to users defined in the SecureAware application. A user is able to switch between the anonymous and authenticated state with the login and logout buttons on the portal. This mode is the default for a new installation.

Public Mode

Anonymous, non-validated, and SecureAware internal users.

This mode is equal to the protected mode, except that it also allows users to identify themselves to the system without real authentication. In this setup users are able to gain access to some parts of the application by providing some unique information, like a user ID or an email address. This mode is equal to SecureAware version 2.0 and older releases. Users that provide unknown user ID's will be created on the fly and gain access to the application.

Private Mode

SecureAware internal users only.

This mode is more restrictive, and unauthenticated users are prompted for user authentication before they can access any information within the portal. Only users defined in the internal user database will be granted access.

Mixed Protected

Anonymous, external, and SecureAware internal users.

This mode extends the protected mode with users defined in an external directory, and the directory must support the standard LDAP protocol. When a user is authenticated from the external provider for the first time, they will be created in SecureAware with an access profile matching the roles they have in the external directory. The external users will not be created as internal users, but with a setting so they can, in the future, be authenticated using the external provider, which precludes the need for password synchronization.

In Mixed Protected Mode the authentication can also be moved to a front-end web server, which enables a single sign on environment.

Mixed Private

External and SecureAware internal users.

This extends the restrictive private access mode with users from an external directory provider. This mode, or the Mixed Protected mode, will probably be the preferred mode for most companies, as this requires the least administration of users.

In Mixed Private Mode the authentication can also be moved to a front-end web server, which enables a single sign on environment.

User Authentication

The application has a built-in user access control system, where users are granted access to parts of the application based on a role system. The authentication is performed against an internal user database or an external access provider like Microsoft Active Directory.

SecureAware functionality can be publicly available or protected by the authentication system. Users are able to authenticate using different systems, but normally an authentication form is used where the user is able to supply a user id and password.

Anonymous access

When a SecureAware portal is in a security mode that allows anonymous access to parts of the application, new users will not be presented with a login form. Users are able to browse all public information, but all functionality that requires user identification will be disabled or hidden.

Anonymous users are able to change status using the login button, which will show the standard authentication form.

Standard Authentication Form

The standard authentication form can be shown in two modes, either with a clear background or with the menus that provide access to the public parts of the application. The standard form enables the user to provide information (user id and password) for internal or external authorization. The information provided is used to create a calculated hash, as the SecureAware application does not store user passwords.

Public Authentication Form

The public authentication form does not require a password, so the application might not be able to authenticate the user but only provide a unique handle for identification. SecureAware can be configured to allow these identified unauthenticated users to gain access to functionality that normally requires authentication, such as feedback and quizzes.

Parameter based authentication

Authentication or identification can also be performed using parameters provided in an URL for “get” requests, and http parameters in “post” requests. This can be used to integrate the SecureAware user system with other applications, or with agent and automation systems.

A user id is required and, if a password is provided, the application will try to authenticate the user. If an email address is provided, the user will be identified.

Special care should be taken with this authentication scheme, especially if the authentication includes a password as this information can be stored in cache, recently used links etc.

Front-end authentication

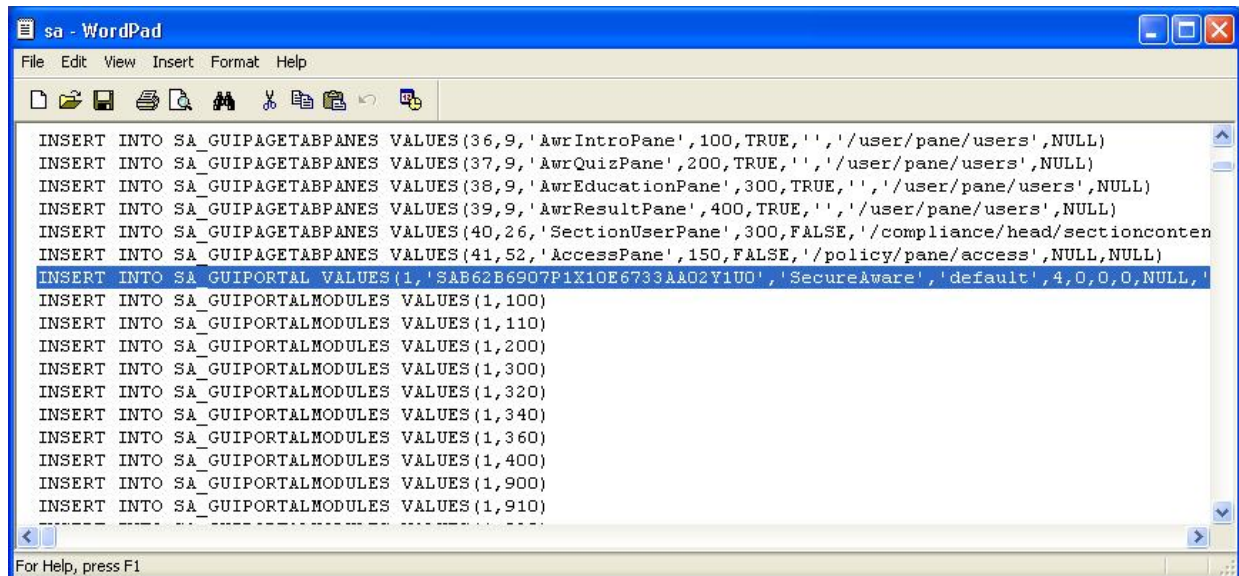
In the 2 mixed mode settings, you are able to use a front-end web server to make the authentication and then pass the credentials to SecureAware. Detailed information about this setup is found in the IIS Guide.

Resetting system administrator passwords

Users that are defined using an external authentication provider are fully managed in the external system. Internal SecureAware users are only defined within SecureAware and are managed with the SecureAware User Manager. If a password for a System Administrator is lost, a special manual password reset procedure is needed.

1. Stop the SecureAware Service, which ensures that we have exclusive access to the data in the database. SecureAware is able to use multiple database providers so the exact access to the database content can be different, but the basics in this procedure are the same.
2. When the Service is stopped, you need to locate the SecureAware Database. In a standard SecureAware installation the database is located within the C:\windows\database folder and the data file is named sa.script. If another database is used, you are able to see the database connection specification in the catalina.properties file in the SecureAware configuration folder at C:\Program Files\Neupart\SecureAware3\conf.
3. Open sa.script with in a text editor. Other database vendors provide tools to access the data within the database. Depending on the size of the database the open process can take some time.

- In a standard SecureAware you start a search in the editor (normally selecting a menu or pressing CTRL-F) and search for the text “INSERT INTO SA_GUIPORTAL”. One or more lines will be found, one for each portal defined in the SecureAware application.

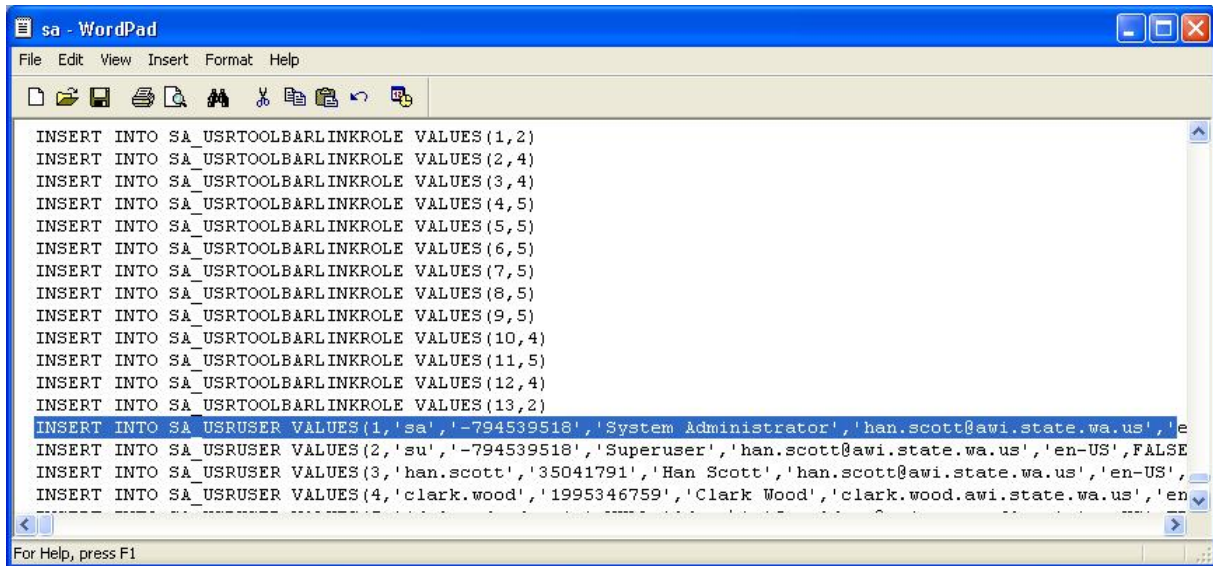


```

sa - WordPad
File Edit View Insert Format Help
[Icons]
INSERT INTO SA_GUIPAGETABPANES VALUES (36,9,'AwrIntroPane',100,TRUE,'','/user/pane/users',NULL)
INSERT INTO SA_GUIPAGETABPANES VALUES (37,9,'AwrQuizPane',200,TRUE,'','/user/pane/users',NULL)
INSERT INTO SA_GUIPAGETABPANES VALUES (38,9,'AwrEducationPane',300,TRUE,'','/user/pane/users',NULL)
INSERT INTO SA_GUIPAGETABPANES VALUES (39,9,'AwrResultPane',400,TRUE,'','/user/pane/users',NULL)
INSERT INTO SA_GUIPAGETABPANES VALUES (40,26,'SectionUserPane',300,FALSE,'/compliance/head/sectionconten
INSERT INTO SA_GUIPAGETABPANES VALUES (41,52,'AccessPane',150,FALSE,'/policy/pane/access',NULL,NULL)
INSERT INTO SA_GUIPORTAL VALUES (1,'SAB62B6907P1X10E6733AA02Y1U0','SecureAware','default',4,0,0,0,NULL,'
INSERT INTO SA_GUIPORTALMODULES VALUES (1,100)
INSERT INTO SA_GUIPORTALMODULES VALUES (1,110)
INSERT INTO SA_GUIPORTALMODULES VALUES (1,200)
INSERT INTO SA_GUIPORTALMODULES VALUES (1,300)
INSERT INTO SA_GUIPORTALMODULES VALUES (1,320)
INSERT INTO SA_GUIPORTALMODULES VALUES (1,340)
INSERT INTO SA_GUIPORTALMODULES VALUES (1,360)
INSERT INTO SA_GUIPORTALMODULES VALUES (1,400)
INSERT INTO SA_GUIPORTALMODULES VALUES (1,900)
INSERT INTO SA_GUIPORTALMODULES VALUES (1,910)
-----
For Help, press F1

```

- The 3rd parameter is the name of the portal, and you now need to locate the portal for which you want to reset the user. The 1st parameter is the system ID of the portal which we need when finding the correct user. If the SA account needs to be reset you should use the default first portal (normally ID 1).
- Now you need to search for the user, use the search string “INSERT INTO SA_USRUSER” to find the user records. The 2nd parameter is the user login name, so you need to locate the user with the name you want to reset. PLEASE NOTE that there can be more than one user with the same name!



```
sa - WordPad
File Edit View Insert Format Help
INSERT INTO SA_USRTOOLBARLINKROLE VALUES (1,2)
INSERT INTO SA_USRTOOLBARLINKROLE VALUES (2,4)
INSERT INTO SA_USRTOOLBARLINKROLE VALUES (3,4)
INSERT INTO SA_USRTOOLBARLINKROLE VALUES (4,5)
INSERT INTO SA_USRTOOLBARLINKROLE VALUES (5,5)
INSERT INTO SA_USRTOOLBARLINKROLE VALUES (6,5)
INSERT INTO SA_USRTOOLBARLINKROLE VALUES (7,5)
INSERT INTO SA_USRTOOLBARLINKROLE VALUES (8,5)
INSERT INTO SA_USRTOOLBARLINKROLE VALUES (9,5)
INSERT INTO SA_USRTOOLBARLINKROLE VALUES (10,4)
INSERT INTO SA_USRTOOLBARLINKROLE VALUES (11,5)
INSERT INTO SA_USRTOOLBARLINKROLE VALUES (12,4)
INSERT INTO SA_USRTOOLBARLINKROLE VALUES (13,2)
INSERT INTO SA_USRUSER VALUES (1,'sa','-794539518','System Administrator','han.scott@awi.state.wa.us','e
INSERT INTO SA_USRUSER VALUES (2,'su','-794539518','Superuser','han.scott@awi.state.wa.us','en-US',FALSE
INSERT INTO SA_USRUSER VALUES (3,'han.scott','35041791','Han Scott','han.scott@awi.state.wa.us','en-US',
INSERT INTO SA_USRUSER VALUES (4,'clark.wood','1995346759','Clark Wood','clark.wood.awi.state.wa.us','en
For Help, press F1
```

7. When the correct user record is found, you need to overwrite the password hash, which is the 3rd parameter. The hash needs to be set to '-794539518' which is the default SecureAware password. Note that this is a text value so it must be enclosed in apostrophes.
8. Save the changes and restart the service, you should now be able to log into SecureAware with the standard SecureAware password: snRt!32w .

Backup – Restore

It's recommended to make a daily backup of your SecureAware database, in case data becomes corrupted or is erased by accident.

If you are using a non-standard SecureAware configuration, it's recommended also to have a backup copy of the configurations file.

This article describes how to make a daily backup, and how you restore your database again.

Backup and restore of a Standard SecureAware installation

Backup

To ensure database consistency, the SecureAware service must be stopped before backup. In Windows, this is done either using the Windows Service Manager or the SecureAware Manager. Make a copy of the files in the Database folder. In version 3.x.x it should be 8 files.

Database location

In a standard SecureAware installation the database is placed in

`C:\Windows\Database\`

Note: That the Windows map are named “Winnt” in some version of Microsoft Windows.

Important: Save the database in a secure place.

Restore

Stop the SecureAware services. Overwrite your database with the backup database.

Start the SecureAware Service again.

Bat file for automatic backup of your SecureAware database

Following is a description of how you can make an automatic routine, to help you with making your daily backup. It's very helpful if you are using a server installation.

You can make a bat file, that stops the SecureAware service, makes a backup of the database and then starts the SecureAware service again.

Note: If your SecureAware installation or your database is not installed in the standard location, you have to modify the paths in the bat file accordingly.

Open a text editor, for example Windows Notepad.

Copy the text below, into the document.

Save the file as <Name>.bat

```
@echo off
Rem Variable declaration
:: variables
Rem Destination directory
set drive=C:\Backup\
set backupcmd=xcopy /s /c /d /e /h /i /r /k /y

Rem SecureAware installation directory source
set folder="C:\Program Files\Neupart\SecureAware3"
Rem Database folder source
set backupfolder="C:\windows"

echo ### Backing up your SecureAware %folder% database directory...
call %folder%\bin\stopsa.bat
%backupcmd% "%backupfolder%\database" "%drive%"

Rem start SecureAware again
call %folder%\bin\startsa.bat
```

With Microsoft Schedule Task manager you can set a job to start after work time, so you are not disturbing any SecureAware users.

Backup and Restore of a Non-standard SecureAware installation

In a non-standard SecureAware installation, we suggest that you read the manufacturer recommendations for backing up and restoring data on your specific type of database system. It's a very good idea to make a single backup of your configuration files, if you are using a non-standard configuration, or if you have changed the default configuration. For example, if you are

using a differing database location than `C:\windows\database` which is the standard, or if you are using an other database, for example a SQL database.

The configuration files are placed in `..\|Neupart\SecureAware3\conf` folder.

Portals

SecureAware 3 allows one or more independent portals running within the same installation. These can be useful for very large organizations with many departments/locations requiring separate policies. SecureAware can centrally manage the entire organization with one database.

By default there is a single portal called “SecureAware”. This portal cannot be deleted, and it is shown as long there are no other matching aliases.

Creating a new portal

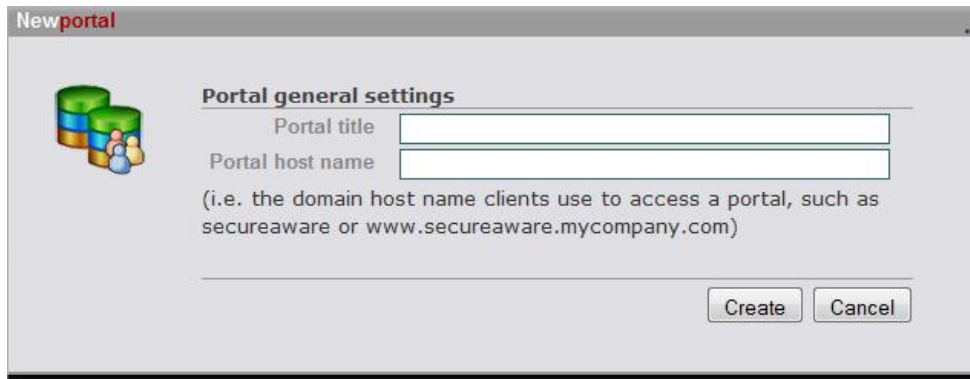
You must be logged in as user SA (system administrator) to manage portals. Click on the portal management icon.



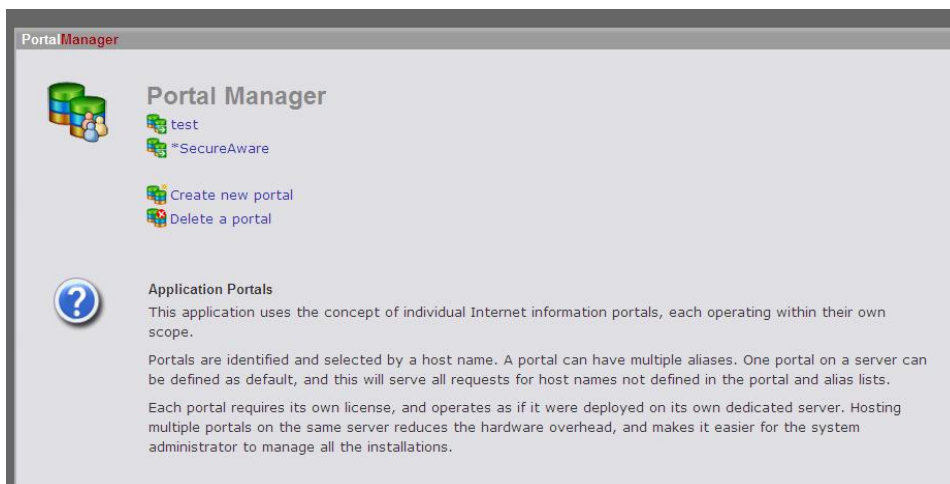
To create a portal, click “Create new portal”.

Type a name in the Portal title field. The Portal title is shown in the browser title bar. In this example, the name is “Test”.

Type a Portal host name. The name can be a host name or DNS name. In this example we are using the name “secureaware.test”

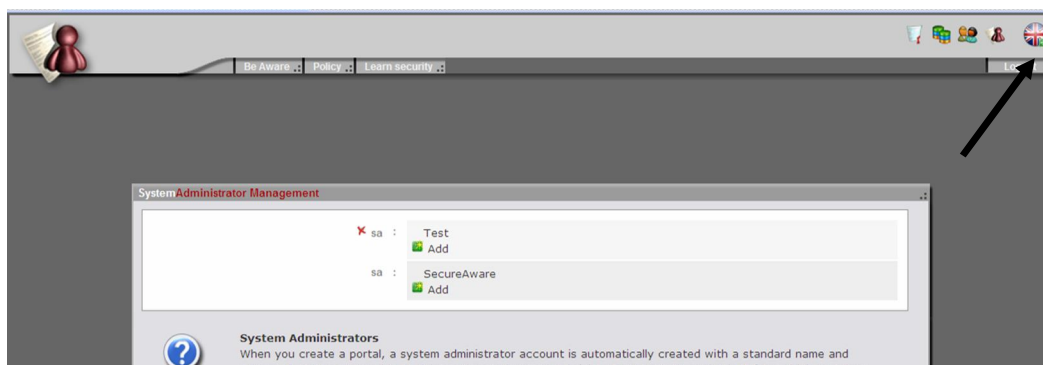


It can take a couple of minutes before the portal is created. Click “Back” when the portal is created.
created.



Installing the license

Select the License manager icon.



The License Management menu will show.



Read the Neupart end user license agreement (EULA).

Select the portal. In this example, are we using the portal "Test".



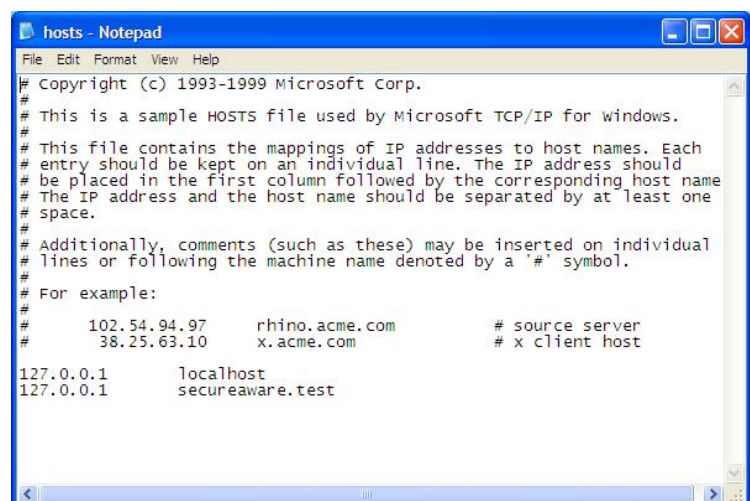
Check the box indicating that you have read the EULA (Important: This must be checked before the license key can be installed). With the Browse button, find your SecureAware license file and click the upload button.

Log in to the new portal

To use your new portal, you must make the portal "visible" to the browser. This can either be done by configuring your alias name in a DNS server, or by configuring your local host file.

Important: The local host file is normally only used for test purposes, such as running the application on your local computer.

Important: The IP address should point to the server where SecureAware is



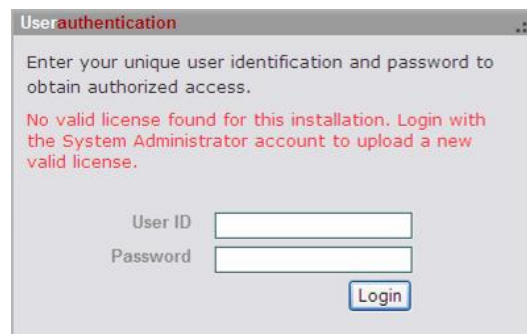
installed.

In this example, it is a local installation.

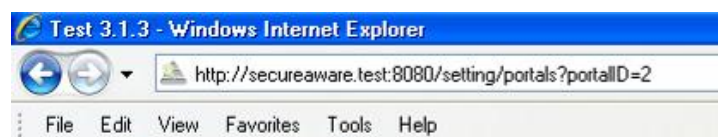
In the browser, type `http://Aliasname:8080` where alias name is the name of the portal. In this example, it is “secureaware.test”.

Port 8080 is the default port in SecureAware. If another port is desired, see the SecureAware Technical Whitepaper.

A logon screen will now open. Type “SA” for user ID and default password ‘snRt!32w’.



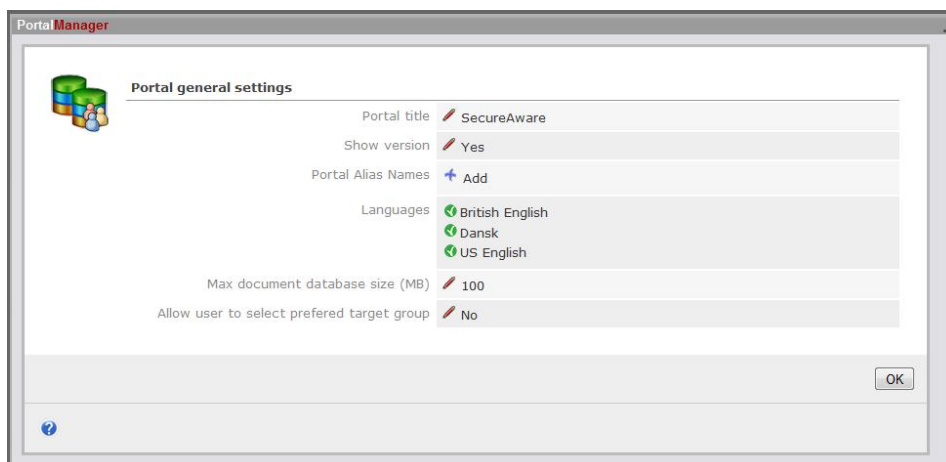
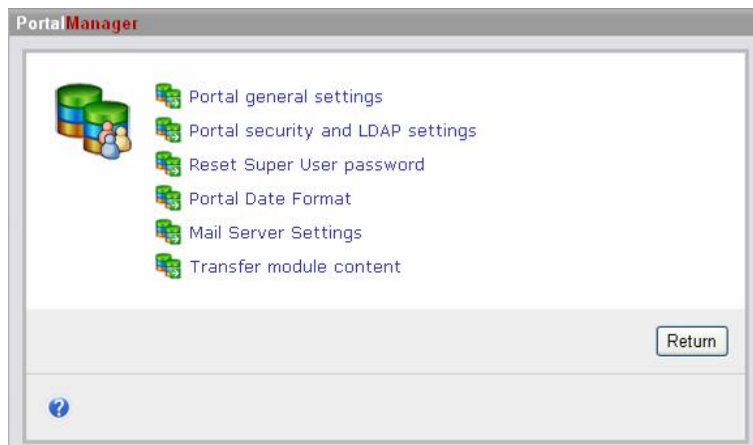
In the browser title bar, you can see if you are in the right Portal. The portal alias name should appear in the browser title bar. In this example, “Test” appears in the title bar.



The new portal is now ready for use.

General settings

General settings are managed by clicking the portal name, and then “Portal general settings”



Portal title

The name of the portal as it is shown in the browser’s title bar.

Show version

This determines whether or not the version number should be shown in the browser. It can be turned off for security reasons by selecting “NO”.

Portal Alias Names

This is related to the Host (Server name), the name for the portal shown in the browser. A portal can have one or more aliases, but each alias can only refer to one portal.

Languages

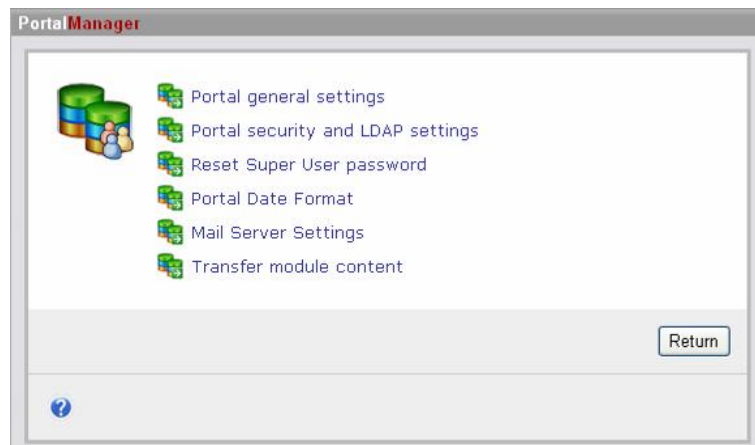
Enable/disable the text languages included in your license file.

Max document database size (MB): It is possible to alter the amount of space you wish to allocate to the document database.

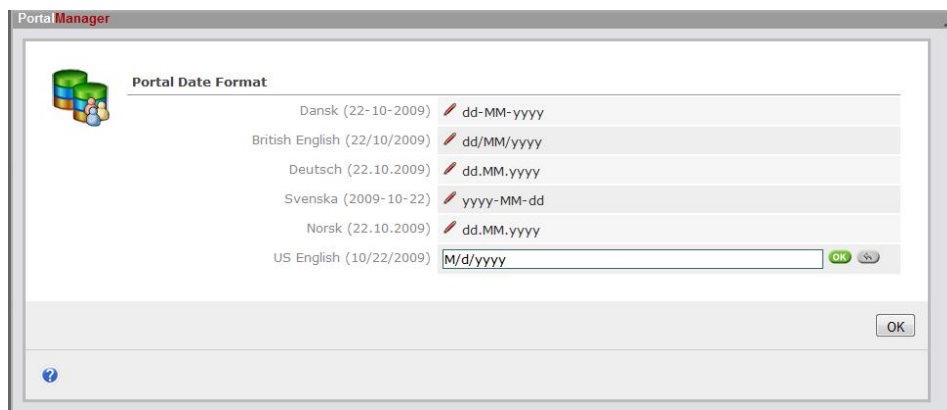
Allow user to select preferred target group: As standard, a user is able to change his or her preferred target group. Users can be denied this option by selecting 'No' by the Allow user to select preferred target group option. Note that this in itself is not a access-limiting procedure.

Date formats

How dates are displayed in SecureAware can be managed by clicking the portal name, and then “Portal Date Format”



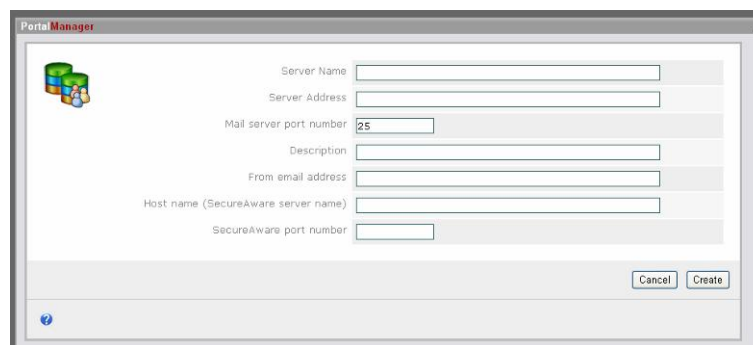
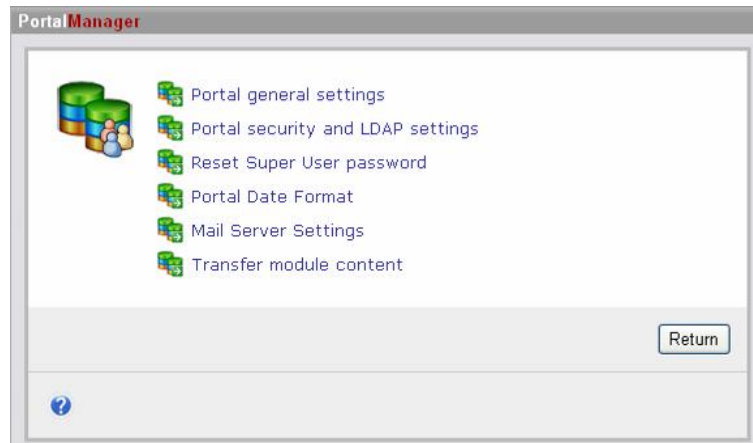
Configuration of the date format can be changed by clicking the pencil icon next to the language name.



Save your configuration by clicking the OK button.

Mail server settings

Mail server settings can be managed by clicking the portal name, and then “Mail server settings”



The Mail Server Settings screen in the Portal Manager lets you configure which settings you wish apply when emails are sent from SecureAware to users. The two fields at the top allow you to enter the mail server’s name and address. As a default setting, the mail server port number has been set at 25. This can be changed if you wish to use a different port. Should you choose this option, you can also enter a short description of this new mail server.

If no sender address is entered in the ‘From email address’ field the sender address (as seen by the recipients of the email) will be that of the system administrator. If no system administrator email address has been given, the sender address seen by recipients will be secureaware@neupart.com.

Emails sent from external addresses on internal systems can cause problems and therefore this practice should be discouraged.

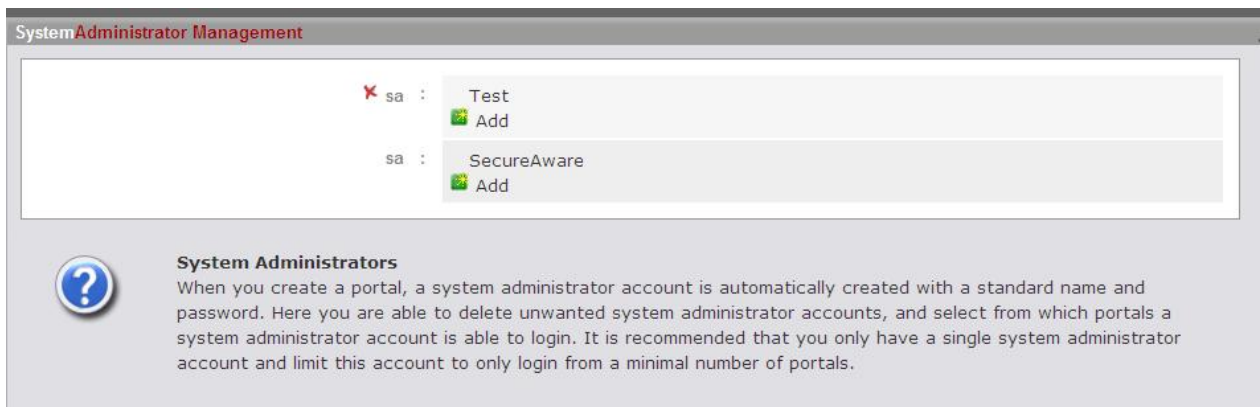
As a default setting, SecureAware is set to run on port 8080.

System Administrators

For each Portal, there will be one or more System Administrators (SA). System administrators are managed by clicking the System Administrator icon as shown below.



You can delete all System Administrators except for the default one, or assign System Administrators to one or more portals.



To assign more Portals to a System Administrator (SA), select “Add” and choose one of the portals in the role menu.

You can deselect a portal or SA, by clicking the red X.

LDAP (AD connection)

The SecureAware application can operate in a secure mode with an external user directory using the LDAP protocol. In a standard installation, unencrypted LDAP protocol communication is used, but SecureAware also supports the SSL encrypted version of the LDAP protocol, and like other communication this can be tunneled for extended security.

SecureAware uses LDAP for handling users with Microsoft Active Directory (AD).

When a user is authorized by the server for the first time, they will be included in SecureAware with an access profile similar to what they have from the AD server.

Users can then log into SecureAware without being included as users within SecureAware, as long as they are validated by the LDAP provider each time.

Setting up LDAP

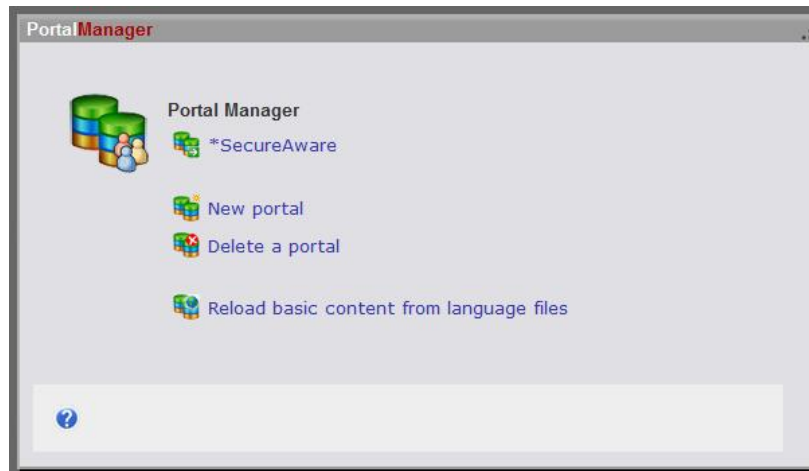
You must be logged on as SA (system administrator) to manage LDAP settings.

Click on the portal management icon.

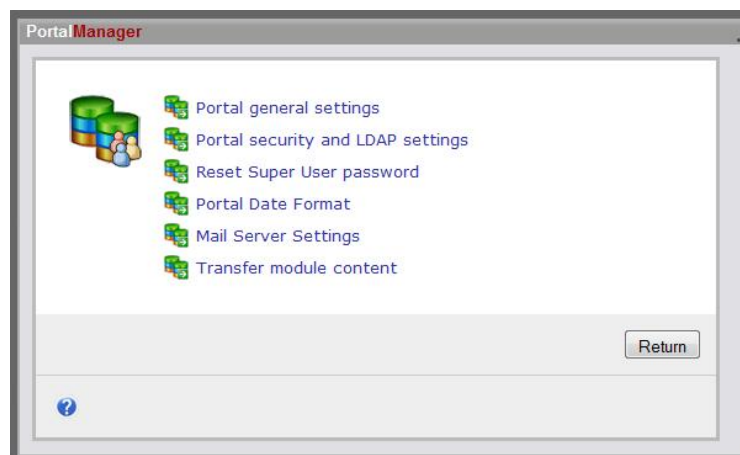


The Portal manager menu will be displayed.

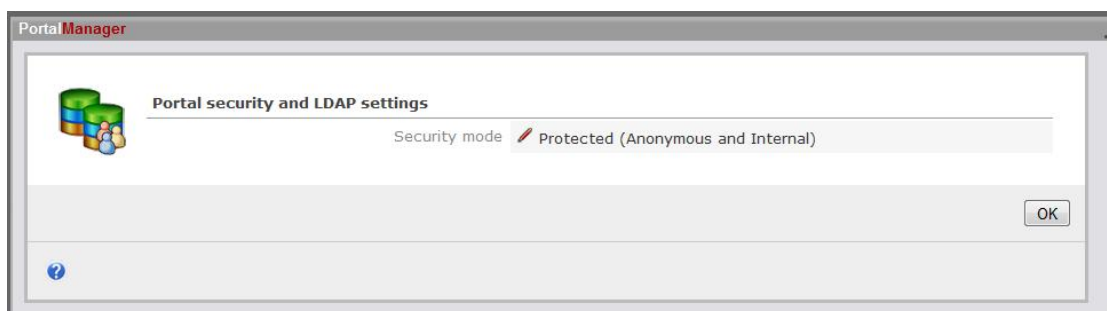
Select the portal that you wish to use LDAP on.



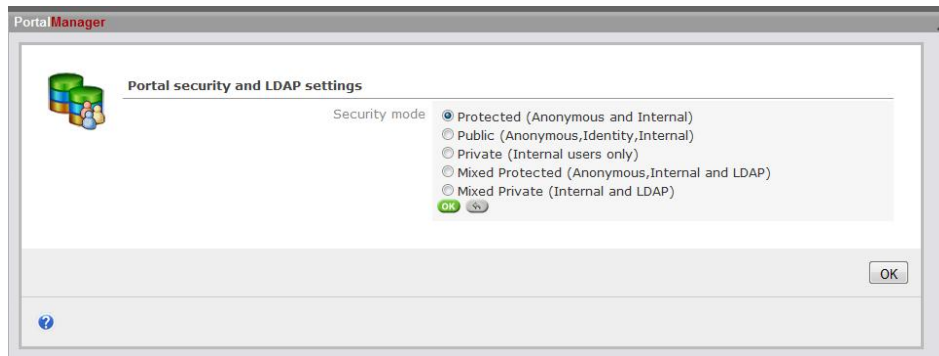
If you only have one, it will be called SecureAware as default.



Click Portal security and LDAP settings, and click the “Security mode” pencil.



You will now see your choices for which kind of users you will allow in SecureAware. You have to select either of the two last options:



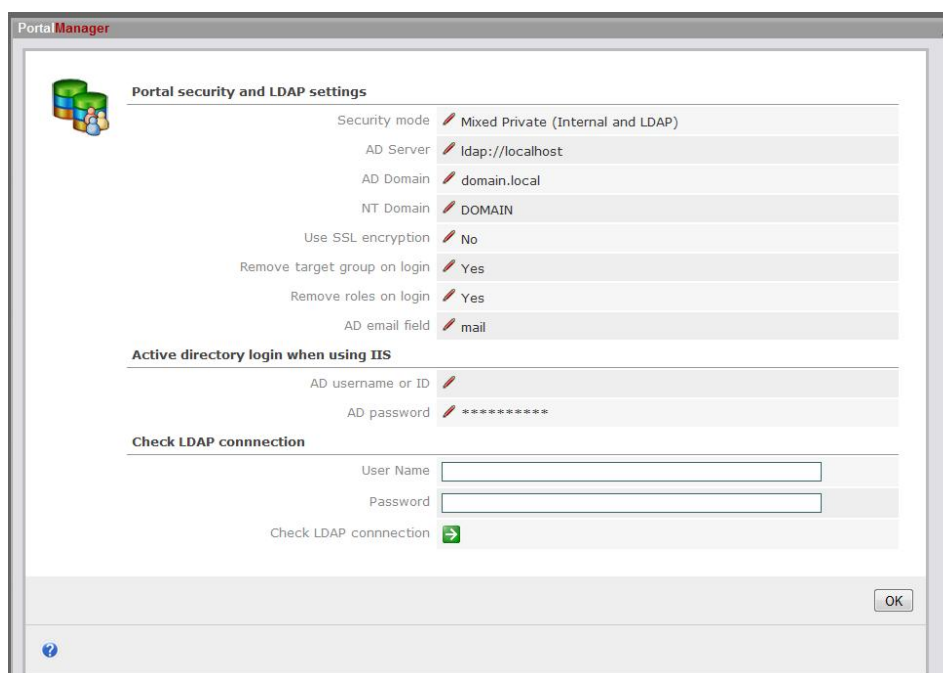
Unknown: Users who are not logged on to SecureAware. As a default setting, these users will only have access to the system's Education material.

Internal: Users who have been set up directly within SecureAware.

Identified: Users can log on to SecureAware using a user name and password of their choice which will be registered and logged by SecureAware together with the user's preferences.

LDAP: Users can be imported from an AD and be assigned user roles which match the profile defined.

Click OK and fill out the rest of the fields:



The following should be set for communication to the server:

*AD Server	The servers URL. ldap://[ad-servernavn]
*AD Domæne	The name of the domain server [ad-domænenavn]
*NT Domæne	The name of the domain (NT/Windows 2000(3) domain [nt-domænenavn] You will have to use the NT domain name if users are not registered with their names, but with their IDs.
Use SSL Encryption	To use SSL encryption, select “Yes”. When using SecureAware over the Internet, or other unsecured communication, SSL encryption is recommended
Remove target groups and roles at login	To make sure that a users access roles and target groups are fully controlled by his AD groups it is recommended to select “Yes” here. This will ensure that a user cannot be granted roles and target groups that the AD group does not allow.
AD email field	SecureAware needs to be able to find the users’ e-mail addresses. So you will have to make sure that the field where the e-mail addresses are registered in in AD is called the same as in this field (usually “mail”).
*Active Directory login when using IIS	Username / ID and password for an AD user. This should be an administration user who does not change password. SecureAware will use this to make AD lookups if you use IIS.
Check the LDAP connection	Check if the LDAP connection has been set up correctly by typing a domain name/user name (first the domain name, (then semicolon); then user name) and a password for a user in AD. Then click on Check the LDAP connection.

***Please note:** If you have more than one AD domain, you will have to type the information of all of these in the fields AD server, AD domain and NT domain separated by ; (semicolon). You have to type the information in the same order in all three fields. Furthermore, the user in “Active Directory login when using IIS” has to be the same in all domains.

Internet Information Server

Installing the redirector

The redirector is an IIS filter API application, that proxy all requests from the IIS web server to the Tomcat web server.

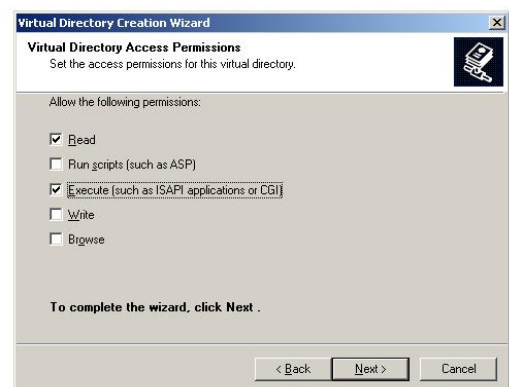
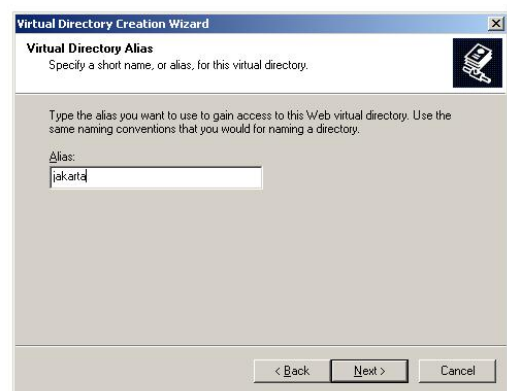
Setting up the redirector in IIS

Now we need to configure IIS to host the web site and the redirector filter.

Start the Microsoft IIS manager application and create or select the web site which will be the SecureAware web site.

In the web site you must create a new virtual directory called “jakarta” that points to the folder
C:\Program Files\Neupart\SecureAware\iis

A virtual directory can be created as a new task in the action menu or by right clicking the mouse on the web site.

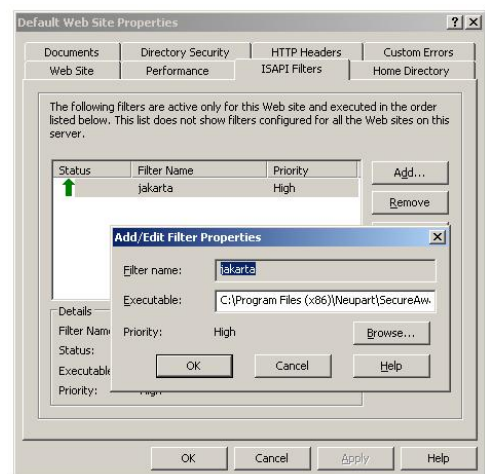


When setting the Virtual directory Access permissions, please be sure that you allow execution if ISAPI applications (the redirector is an ISAPI application)

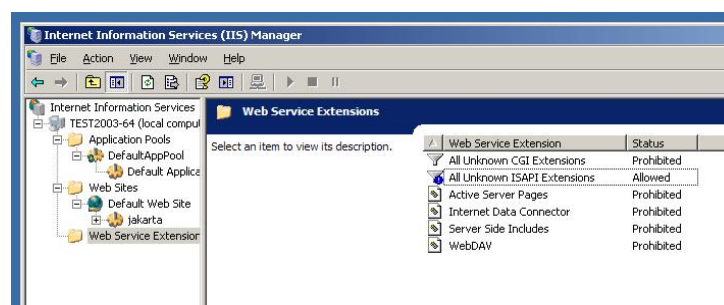
In the web sites properties you now need to add the redirector as an IIS API filter.

Locate the filter tab and add the new filter with the name “jakarta” and the path to the redirector DLL file: C:\Program Files\Neupart\SecureAware\iis\isapi_redirect.dll

Note that the status and the Priority will be updated when the IIS web site have been restarted and you used the web site for the first time.



On an IIS version 6 you must also enable the Web Service extension “All unknown ISAPI Extensions”



This is a global setting in the IIS manager application, under “Web service Extensions”.

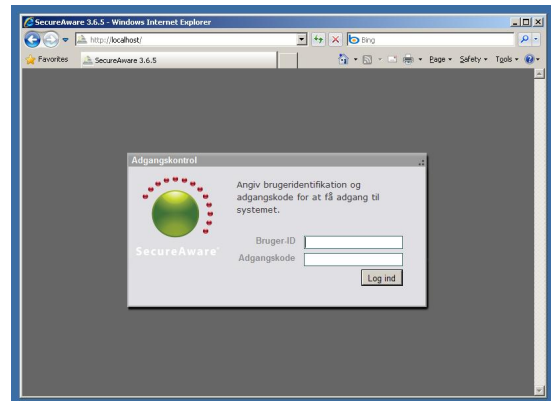
Restarting IIS web site

To enable your changes you must restart the web site that you configured for SecureAware. This can be done in the IIS manager by selecting the website and then use the Stop and Start buttons.

Test the redirection

Now you are able to point a web browser to the web site you created in IIS and it should show the content redirected from the Tomcat web server.

If the site is not working, you might need to restart the IIS web service or the server for IIS to enable your changes. Remember that redirections only works if the Tomcat web server (the SecureAware Service) is started before the IIS web site hosting the SecureAware application.



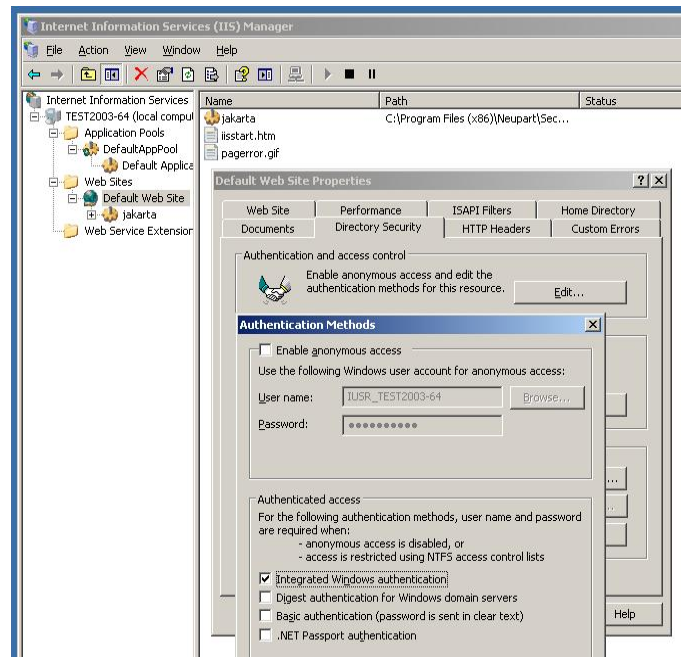
If you get an access denied message, you need to ensure that the service configured in your IIS web server is allowed read and execute access to the SecureAware IIS folder you created.

Please ensure that the redirection works before continuing with setting up single sign on.

Single sign on

Before setting up single sign on, please setup SecureAware to use Active Directory for user validation, and configure the IIS user in the SecureAware portal management.

If you want the IIS web site to operate in a Single Sign On solution, you now need to remove Anonymous access to the web site. This is done in the web site properties, under the Directory Security tab. Select Edit the Anonymous access and authentication control, and disable anonymous access.



Only the option “Integrated Windows authentication” should be selected. Remember to restart the web site to enable the changes.

Microsoft SQL Server 7, 2000 or 2005

The SecureAware standard installation contains all files that are required to operate the application on the Microsoft database, even the JDBC driver.

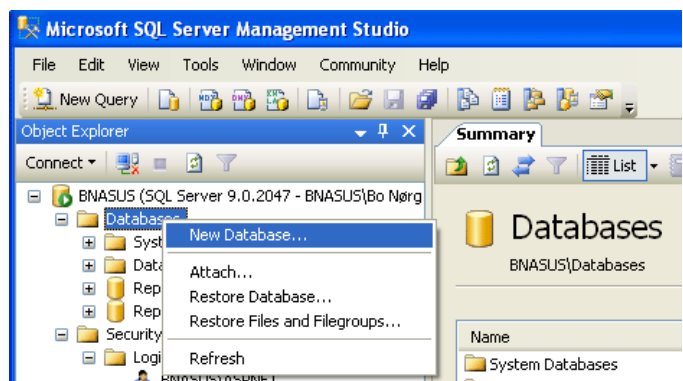
Database installation

Ensure that the database is installed and working, and if the SecureAware server and the SQL Server are not located on the same server, do ensure that the connection port (default 1433) is not blocked by firewalls.

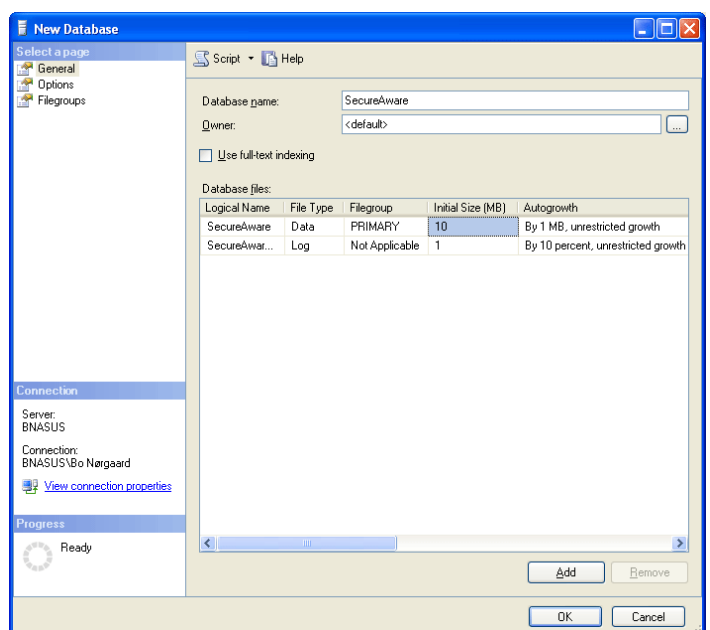
Create a database

Create a new database called “SecureAware” in your SQL server. Tables and content will be created by SecureAware on installation and upgrades.

On Microsoft SQL server 2005 you start the SQL server management studio application, right click the databases item in the object explorer tree view, then select the option “New Database...”



In the new database dialog, enter “SecureAware” as the database name, and change the Initial size of the data file to 10MB which will fit the initial installation. .

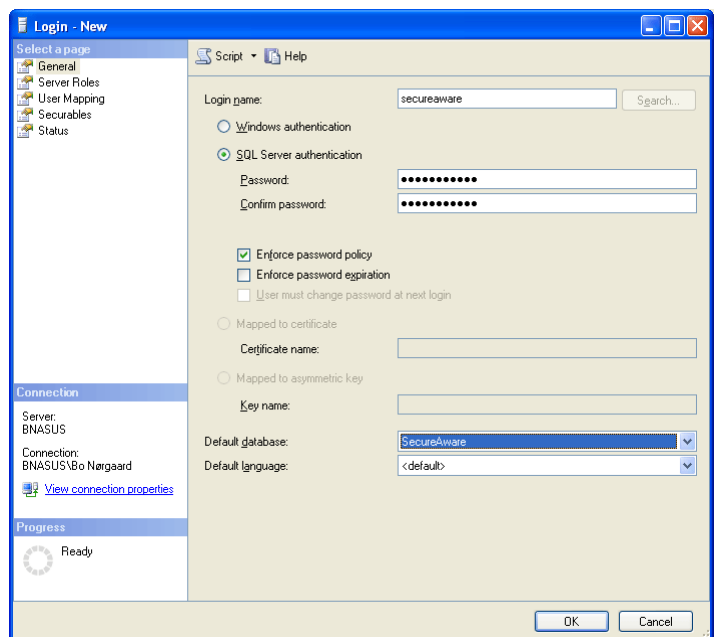


Create a user for SecureAware

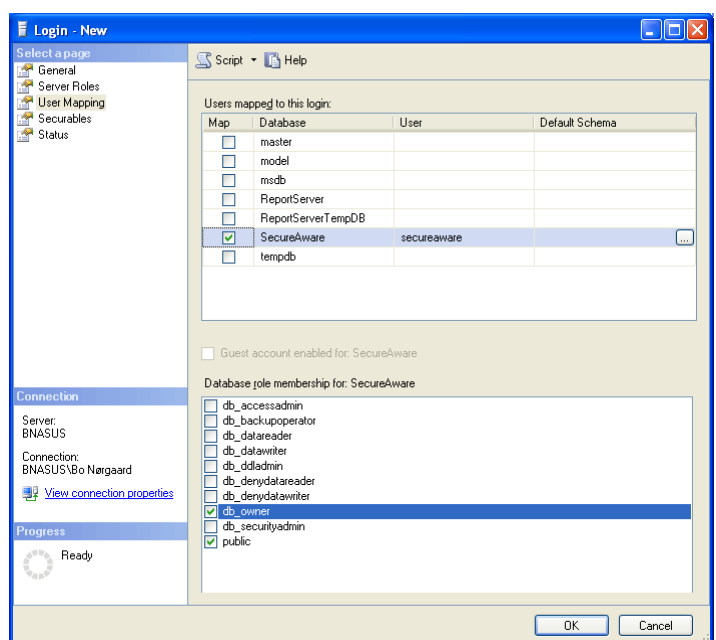
For the SecureAware database connection we need a database user account. In this sample we use a user called “secureaware” with the password “secureaware” (which is not recommended for production systems). The database user should have database owner rights during installations and upgrades, but only needs select, update and delete rights during normal operation.

In MS SQL 2005 the user is also created in the management studio application. In the security folder you right click the login item and select to create a new login.

In the new login dialog you enter “secureaware” as the login name. The new user should then be configured to use SQL server authentication, which lets you enter “secureaware” as password. You need to disable the password expiration feature or this will require regular configuration changes. You can set the default database to be the SecureAware database.



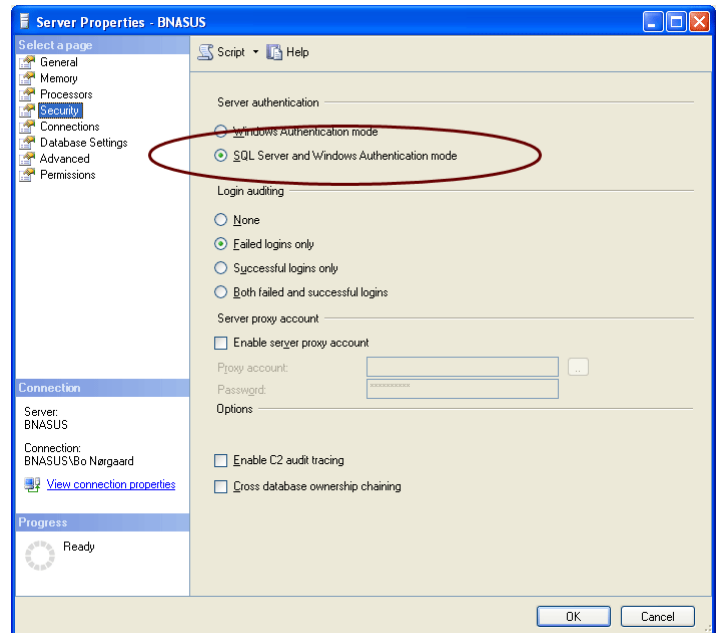
Then you map the user to the SecureAware database, and when mapped you add the role db_owner which ensures that the login user is able to create and maintain the data model (create and alter table rights).



As we set the login to use the SQL server authentication, we need to ensure that the database was installed to allow this authentication method.

Be aware that a default installed Microsoft SQL server only enables Windows integrated security, so you have to manually select to enable the SQL authentication mode during installation.

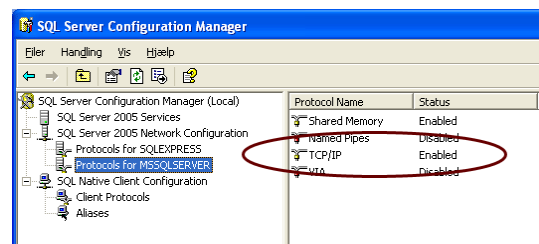
In SQL server 2005 you can change this from within the management studio application, by selecting server properties on the database.



In the Security area you can select to enable both SQL server and Windows authentication mode.

As the SecureAware application uses a JDBC driver that is based on creating a database connection using TCP, we need to ensure that the SQL server enables this. In SQL 2005 the connection settings are controlled in the SQL server configuration manager application, which can be found in the start menu.

A standard installed SQL server 2005 does not enable TCP connections, only the shared memory connection method. And when you enable the TCP connection you can also configure which port is used (default 1433).



Remember that after making changes with the SQL server configuration manager, you need to restart the SQL server service to activate your changes.

SecureAware configuration changes

Stop the SecureAware service before making any changes to the configuration files.

To change the database used you must edit the “cateline.properties” file in the conf folder with a standard text editor like notepad. The first section is the configuration of the in memory database HSQLDB, and should be disabled by placing a # character in front of all the lines.

Section two is the MS SQL server settings and should all be enabled by removing the # character that is in front of all the lines.

Correct the user name in “hibernate.connection.username” and the password in “hibernate.connection.password” to the one created on the SQL server. The connection URL should be changed to match your settings,

```
hibernate.connection.url jdbc:jtds:sqlserver://localhost:1433/secureaware;tds=8.0;lastupdatecount=true
```

The “localhost” is the name of the server running MS SQL, 1433 is the port, and SecureAware is the catalog (database) name. The last parameters are needed by the driver to optimize the communication.

In SecureAware versions above 3.0.4 the configuration was extended to include two database connections (see separate document for upgrade instructions), one for the normal SecureAware data, and one for the document database. You can make both points to the same database if you don’t need to store the large binary document objects in a separate place.

If you make two separate databases, you could optimize the SecureAware database for the random access and update of small texts using joins and advanced content filtering. The Document database could be optimized for storing simple tables containing large binary objects.

Here is the configuration that would work with the setup we described here, on a SQL server installed on the same machine as SecureAware and both connections pointing at the same database.

```
## MS SQL Server
```

```
hibernate.dialect org.hibernate.dialect.SQLServerDialect
```

```
hibernate.connection.driver_class net.sourceforge.jtds.jdbc.Driver
```

```
hibernate.connection.username secureaware
```

```
hibernate.connection.password secureaware
```

```
hibernate.default_schema dbo
```

```
hibernate.default_catalog secureaware
```

```
hibernate.connection.url jdbc:jtds:sqlserver://localhost:1433/secureaware;tds=8.0;lastupdatecount=true
```

```
document.dialect org.hibernate.dialect.SQLServerDialect
```

```
document.connection.driver_class net.sourceforge.jtds.jdbc.Driver
```

```
document.connection.username secureaware
```

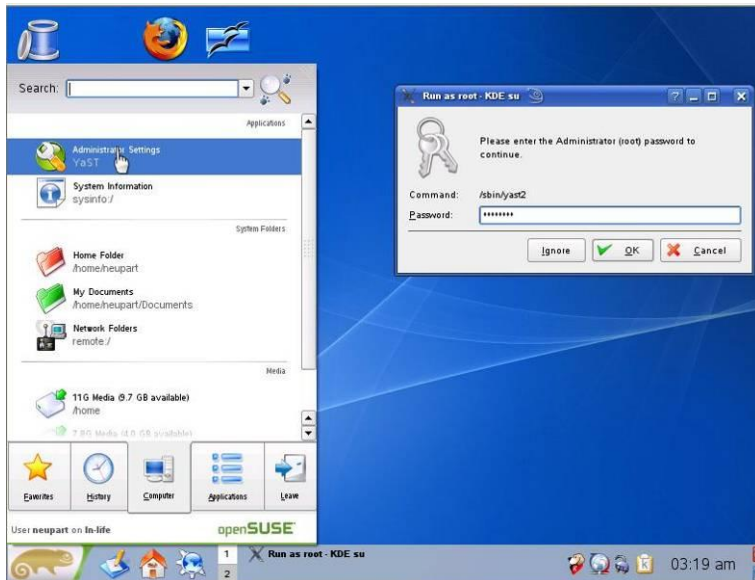
```
document.connection.password secureaware
```

```
document.default_schema dbo
```

```
document.default_catalog secureaware
```

```
document.connection.url jdbc:jtds:sqlserver://localhost:1433/secureaware;tds
```

Installation and upgrade on a Linux server



administrator password and click **OK**.

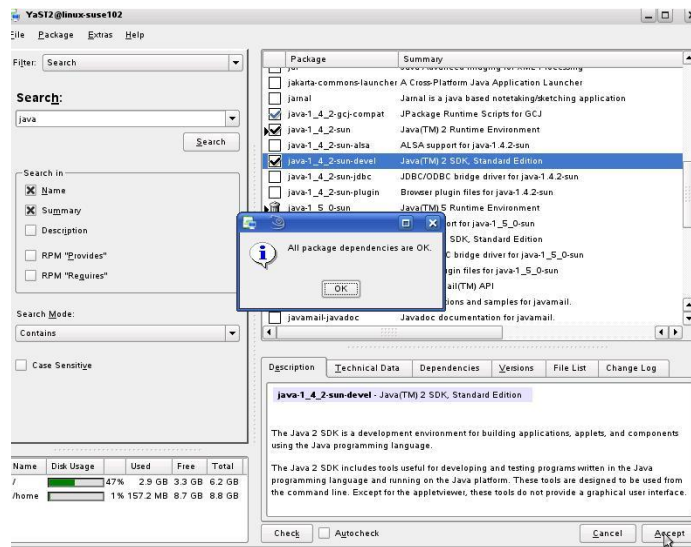
In order to be able to run SecureAware, Java SDK should be installed. The following tutorial shows information about installation procedure of java 1.6.0 SDK in OpenSUSE (32 bit).

Click on the chameleon (like start in windows) from the computer tab icon choose the administrator configuration YaST. Type the

After login as administrator, click on software management which is one of the Software tab options. Use the search function to find the package you want by writing “java” and clicking the search button. In the list to your right “java-1.6.0-sun-devel” will appear. If it is unchecked then click on it then click on the check button below. If the pop-up screen reads: “All package dependencies are OK” you can click **OK**. After that click accept to install the java-1.6.0 package. You may need the installation CD/DVD to do this.

When this is done you can start installing SecureAware. On other Linux distributions you need to find the correct package or download it from java.sun.com

If you already have a version of java, please uninstall it before installing the new one.



Installing SecureAware

First you need to download the SecureAware Linux version to your computer. Please note that the installation package is RMP file type which has the extension .rpm. RPM is a Red Hat package manager to manage software but could easily use by other Linux distributed system too.

After downloading there are two ways to install SecureAware on the system. The first one is through Terminal by using the RPM tool as following:

```

neupart@ln-life: ~ - Shell - Konsole
Session Edit View Bookmarks Settings Help

neupart@ln-life:~> sudo -s
root's password:
ln-life:/home/neupart # cd Desktop
ln-life:/home/neupart/Desktop # rpm -i secureaware-3.2.3-1.i586.rpm

```

Open the terminal and go to the directory where you put your installation file. In this case we have the installation package on the Desktop. In order to be able to install software on the system you should have administrator ability. Therefore you should write this in the terminal: `sudo -s`. after writing the administrator password the symbol is going to change to # next to your host name. If this is the first time you install the SecureAware you have to write: **`rpm -i full name of SecureAware`**. If you already have an older version of SecureAware installed and you want to update to the newest version you write: **`rpm -u full name of SecureAware`**. In case you have an old version you want to remove from the system or just uninstall you should write this in the terminal: **`rpm -e full name of SecureAware`**.

The SecureAware RPM unpack the files to: `/opt/secureaware` and return when the files are unpacked.



The other way to install the SecureAware is through the graphical client. You can right click on the SecureAware package you downloaded and select to install it with the “install software”. The files are going to be unpacked the same way as with the RPM tool and return when it is finished.

Before the SecureAware is able to start, the `JAVA_HOME` environment variable must point to the SDK version of Java 1.6.0 or higher. This can either be done globally or by editing the `setenv.sh` file which is located in the SecureAware bin folder.

On a OpenSUSE Linux distributed system you can edit the file `/opt/secureaware/bin/setenv.sh` and set the environment variable to: `JAVA_HOME=/usr/lib/jvm/java-1.6.0`

The editing process can be made through the terminal or an editor. If you use an editor you should remember to open the editor as system administrator by writing: `sudo editor-name` then opens the `setenv.sh` from the opened editor. In case you are using the terminal you should first go to the specific directory which is `/opt/secureaware/bin/` and write: **`nano setenv.sh`** or **`vi setenv.sh`** then edit the file there and save the changes.

If you try to start SecureAware and the environment variable does not exist or it points to JRE version of java, the application will put an error message on the screen explaining that the environment variable needs to point to an SDK version of Java.

Starting SecureAware

The folder `/opt/secureaware/bin` contains the following scripts:

`Startup.sh` which starts the SecureAware daemon and returns.

`Shutdown.sh` which stops the SecureAware demon and returns.

These files can be included in the Linux boot and shutdown sequence so that the SecureAware application will start and stop automatically with the Linux Distributed system. But if you want to start and stop the SecureAware manually, open the terminal and change to administrator by writing **sudo -s** and go to the `/opt/secureaware/bin` path then write `./startup` to run the daemon and `./shutdown` to stop the daemon.

Locating the Database

In a SecureAware Linux installation the database files are located at:

`/opt/secureaware/database`

When you want to create a backup of the database you need to stop the SecureAware service first. It is a good idea to include the backup in a script which is called regularly.

SecureAware Support

This guide explains how to send the SecureAware database to the Neupart support team. If the problem is solved with direct database changes, then this guide can also be used to restore the database to your system, simply by copying the files from the mail to the database folder.

Note: Remember always to make a backup of your old database, before you overwrite it.

Stopping SecureAware

To ensure that all data is flushed to the database, the SecureAware service must be stopped while the database files are copied. In Windows this is done either with the Windows Service Manager, or preferably with the SecureAware Manager. Read more about how to stop/start SecureAware Services in the paragraph '*Change location of SecureAware database*'

On Windows XP the SecureAware manager can be found in the Windows Start menu:

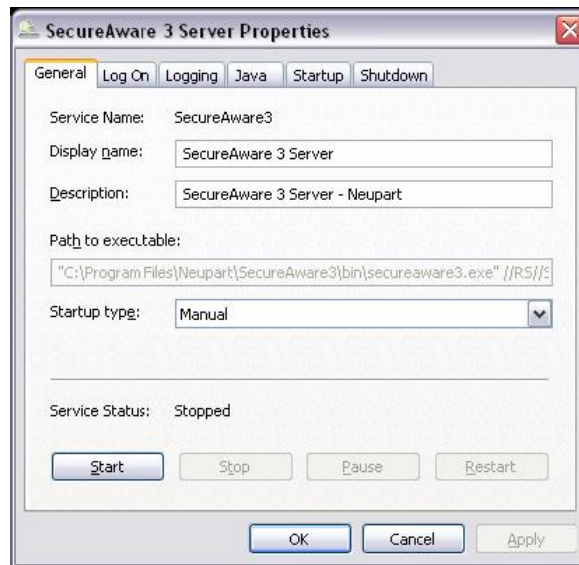
1. Open the "Start" Menu
2. Open "All programs"
3. Select the "SecureAware" folder
4. Select the "Management" folder
5. Select the "SecureAware Manager"

If there are no SecureAware links in the start menu, the manager can be located at:

C:\Program Files\Neupart\SecureAware3\bin\SecureAware3w.exe

Note: The folder "Program Files" could be named differently in localized versions of Windows.

In the SecureAware manager you should then the Service Status in the main tab "General". The status of the service must be "Stopped". If the service status is "Started" you can stop the service with the button called "Stop".



After copying the database you can use the manager to restart the SecureAware service. If you use the Windows Service Manager you should locate the SecureAware service called “SecureAware3” and ensure that the service is stopped.

Locating the Database

In a standard SecureAware installation the database files to send are located at:
C:\Windows\Database\

Note: The Windows folder is called “Winnt” in some versions of Microsoft Windows.

In Windows XP you can pack the files before sending these to the support team, to pack the files, select all the files and use the mouse to right-click on one of the selected files. In the popup menu select the “Send to” and “Compressed (Zipped) folder”. A new packed file containing all the selected files will be created.

Send the zipped or individual files to Neupart support team support@neupart.com, along with a description of your problem.

Automatic log off

SecureAware will, as default log a user out if he has not been active for 30 minutes. You can change this by stopping the SecureAware service and locating the file web.xml and changing the session timeout duration. You will find the file in C:\Program Files\Neupart\SecureAware\conf (take a backup of the file just in case). Search for the string:

```
<session-timeout>30</session-timeout>
```

Now change the "30" to the number of minutes you want to pass before a user is logged out. Save, close and start the service again.

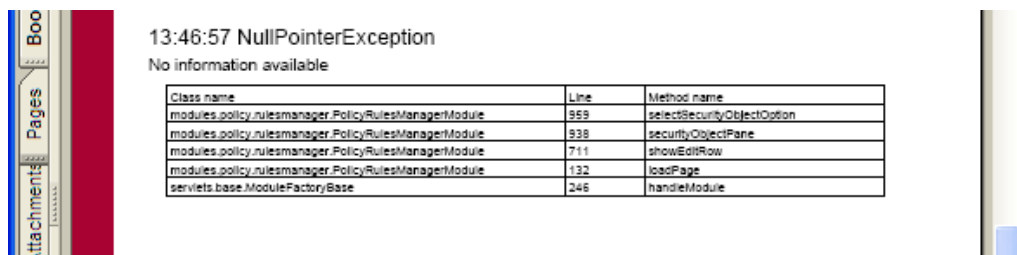
SecureAware logging capabilities

SecureAware’s various logging capabilities allow you to easily track and document any editing carried out within the Policy module. These programme’s logging functions also let you document any errors that occur anywhere across the entire system. To enable this, logging capabilities have been fully integrated into the Policy module (refer to the the Policy manual) and are linked with all of the System Administrator’s administrative functions.

In addition, several of SecureAware’s modules record information linking data to specific users, though here, tracking and documentation of the general system data is not recorded in a specific log.

Error log


This report contains technical information covering all errors registered from across the system.



13:46:57 NullPointerException
No information available

Class name	Line	Method name
modules.policy.rulesmanager.PolicyRulesManagerModule	959	selectSecurityObjectOption
modules.policy.rulesmanager.PolicyRulesManagerModule	938	securityObjectPage
modules.policy.rulesmanager.PolicyRulesManagerModule	711	showEditRow
modules.policy.rulesmanager.PolicyRulesManagerModule	132	loadPage
serviets.base.ModuleFactoryBase	246	handleModule

SecureAware Error log.

To access these logs you must be logged in as a System Administrator (SA). To view, click on the Log Files  icon at the top right of the screen. These logs can be particularly useful in a wide range of support situations.

Logging in general

If you use Microsoft Internet Information Server with your SecureAware installation, you can use this to track how users use the system.

SecureAware has not been designed to deal with the specific logging of personal information of which authorities may be legally obliged to provide a record. As a result, the systems logging capabilities do not necessarily comply with applicable legislative standards.

If a public authority using SecureAware is, however, legally required to record and log personal user information Neupart recommends that such information be registered in an ESDH system, or similar. Such a system should have the requisite logging capabilities and can make use of SecureAware's ability to link to external documentation.

Contact Information

- Further information is available by contacting Neupart

Europe

Neupart A/S
Hollandsvej 12
2800 Lyngby
Denmark
Tel +45 7025 8030
Fax +45 7025 8031

North America

United States
Neupart Inc.
2553 Crescent St
Ferndale, WA 98248
Tel. 360-820-2545
Fax 360-392-6078

Neupart GmbH

Kaiserwerther Strasse 115
40880 Ratingen/Düsseldorf
Germany:
Tel. +49 (0) 2102/4209-26
Fax +49 (0) 2102/42062

Copyright © 2006 Neupart A/S. All rights reserved.

The author of this documentation is Neupart A/S. All information herein including text and graphics belongs to Neupart A/S unless stated otherwise and is protected by copyright laws in Denmark and international agreements.

Permission to quote this documentation in its entire form or partly is given under the premises that no changes are made and that information about this copyright is clearly stated on all copies. No material may be copied or distributed without explicit approval of Neupart A/S. Neupart A/S preserves the right to - at any time and without warning - make changes and/or improvements in the products mentioned.

Names of other companies and their products are or can be registered trademarks or trademarks that belong to their owners. Neupart and SecureAware logo and the name "SecureAware" are trademarks belonging to Neupart A/S. The documentation is provided "as is", without warranty of any kind, express or implied, including but not limited to the warranties of merchantability, fitness for a particular purpose and non-infringement. In no event shall the authors or copyright holders be liable for any claim, damages or other liability, whether in an action of contract, tort or otherwise, arising from, out of or in connection with the documentation or the use or other dealings in the documentation. The documentation including graphics could contain inaccuracies or typographic errors. Furthermore there are no guarantees regarding results achieved by using this information.

All rights not explicitly mentioned herein are preserved.