

SecureAware®

SecureAware Quick Guide

- for Superusers and System Administrators

Applies to SecureAware version 3

Document date: April 2009

About this document

This document is a brief description of how to get started using SecureAware. The guide gives a short introduction aimed at system administrators who need to perform a basic install of the program. Super users are introduced to the modules Awareness, Risk, Compliance and Policy.

For more detailed information, please refer to the system administrator manual or the manuals concerning the various modules.

Table of content

Basic Install	3
First Time Installation of SecureAware	3
System Administrator Access:	3
New license key installation	4
Super User Access.....	4
How to create and manage user accounts.....	4
Create New Policy	6
Create New Awareness quiz	7
Start an Awareness Screen Saver Program	7
Create new compliance check	8
How to perform a risk assessment	9
Start an assessment	9
Contact Information	10

Basic Install



The typical responsibilities of a SecureAware System Administrator include:

- Installation of the SecureAware software on a server
- Uploading license keys

First Time Installation of SecureAware

If you have a previous version of SecureAware installed, please skip this section and proceed to the *'SecureAware System Administrator Guide'* for further information about how to upgrade SecureAware.



Follow these steps to install and initialize SecureAware on your server:

- Run setup.exe on your server to install the SecureAware server software (you must have administrative rights to the machine)
- After installation, run the SecureAware Manager (you will find a shortcut in Start > All Programs > SecureAware > Management > SecureAware Manager)
- Wait for the SecureAware “Stop” button is marked. Then type the “Start” button.
- Start SecureAware up in the (you will find a shortcut in Start > All Programs > SecureAware > Management > SecureAware Manager). If you are using SecureAware on a server, you can Point your browser to <http://<NameOfYourServer>:8080/>
- You should see a screen displaying “Welcome to SecureAware. The application is currently in management mode....”
- Click on the link:  ‘Continue the installation or the upgrade’
- Database initialization will begin . Wait for the message: “The Database was successfully upgraded.”. Type on the link ‘Return to SecureAware’ (this will log you in as System Administrator)
- Read the End User License Agreement (EULA), select portal “SecureAware”, acknowledge your EULA consent, select your license file and press the ‘Upload’ button
- Log out, SecureAware is now ready for use

System Administrator Access:


After initial installation and set-up, you may need system administrator access to perform tasks such as uploading new license keys, managing portal settings, security modes, LDAP or Active Directory settings, and date formats. To do so, follow these steps:

- Point your browser to <http://<NameOfYourServer>:8080/>

- Log in with username 'sa' and password 'snRt!32w'
- Using the icons in upper right corner, you can manage license keys  and portal settings 

New license key installation






To install a new license key:

- Point your browser to `http://<NameOfYourServer>:8080/`
- Log in using 'sa' as username and 'snRt!32w' as password
- Select the 'License Management' icon  at the top of the screen
- Read the End User License Agreement
- Select the portal for which you want to install the license key
- Select your license file and press the 'Upload' button

The typical responsibilities of a SecureAware Super User include:

- Managing policies, awareness programs, risk assessments, and compliance assessments
- Assignment of roles to users (both internal SecureAware users and users defined in an external Active Directory or other LDAP-based user directory)


Super User Access

- Point your browser to `http://<NameOfYourServer>:8080/`
- Log in with username 'su' and password 'snRt!32w'
- Using the icons in upper right corner, you can work with policies , awareness programs , risk management , compliance management  and user management .


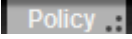

How to create and manage user accounts

- SecureAware user creation and management depend on the security mode of your SecureAware portal. Your System Administrator has the task of selecting a Portal Security Mode. The most important modes are:
- Users defined in your Active Directory can log into SecureAware with their standard usernames and passwords. Other LDAP-based user directories can be used similarly. Users are created in SecureAware when they log into SecureAware first time, or when a super user imports the users from AD. SecureAware does not store the passwords of AD users.
- Users defined internally in SecureAware can log in using the IDs and passwords defined by a super user.
- If your system administrator has allowed "identity based" access, users are created in SecureAware as they log in the first time. If they supply a password, that password must be used from the 2nd login.







Super user(s) manage the roles and groups of the users. For internal users, the super user can also reset passwords.

- To access the user manager, log in as super user and select the User Manager icon . Here you will have the options: Create new user account, Manage user accounts or Import external users.
- You also have the opportunity for assignment deference roles for the users, read more about it in the 'SecureAware Super User guide'.



Create New Policy

- As a super user, select the Policy Manager icon 
- Select 'Create new policy'
- Type the name and a description for your policy
- Select a template (for example, 'High Security') and press the 'Create' button
- Click on the new policy and click the 'Activate Policy' button to activate the policy for end users
- Your new policy is now available for users at <http://<NameOfYourServer>:8080/> if they click 
- To edit the content of your policy, click  then select your policy and click Policy, Rules or Procedures in the pyramid to the right




Create New Awareness quiz

- As a super user, Select the Awareness Manager icon 
- Click 'New awareness program' 
- Type a name, a description, select a category (for example, "Passwords"), click 'Add', then select a target group (e.g. "Management"), click 'Add' then click the 'Create' button
- To change the elements included in your awareness program, select 'Edit awareness program settings' (Note: This can only be done before the program starts)
- To start, your awareness program, select 'Run the awareness Program against target group' . Select a target group.
- The  select target groups will be in the right top corner and you can start the programs by click the green start icon
- When the test's are finish, you have to select the stop icon 
- You can see the finale result by selecting the 'View result' icon 

Start an Awareness Screen Saver Program

- As a super user, select the Awareness Manager icon , and select the awareness program to which you are adding a screen saver activity
- Click 'Activate Screen Saver Program' and add one or more content categories, then click 'Create'
- By selecting the 'Start' button , the screen saver program will begin.
- Workstations on which the SecureAware screen saver has been installed can then display content matching the categories and target group set in the awareness program







Create new compliance check

- As a super user, select the Compliance Manager icon 
- Click 'Create new Compliance Evaluation', specify a name and a description and click 'Create'
- Click Start and confirm to start Compliance Evaluation immediately, then click 'Update'
- You can assign different users to different chapters of ISO27001 / DS484 by selecting the link: 'Manage who will be responsible for checking for compliance of each standard section' (by default, the current user, meaning you as a super user, is assigned to all sections)
- Users who have been assigned to the compliance evaluation task for one or more standard sections will be presented with a questionnaire when they click "Compliance" on the end user menu: 
- As a super user, you have access to draft compliance reports from Super User's menu .
- If you want to create your own questionnaire for a compliance check, click 'Compliance Question Management' from the front page.


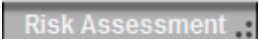

How to perform a risk assessment

Minimum Preparation

You must create systems and users in SecureAware and assign user assessment roles for your systems

- ✔ First, create the users who are to have an assessment role (user creation is described in the User Management section).
- ✔ Then assign the role “System Owner” to each of the users who shall participate in one or more risk assessments. Choose User Manager , then select ‘Manage user accounts’, and follow the instructions on screen.
- ✔ As a super user, select the Risk Manager icon .
- ✔ Click ‘Systems’ in the left side menu. Review the system list to make sure that the priority systems or applications that you want to assess are included in the list. You can add systems using the ‘Create new system’ icon . Optionally, you can delete any of the default systems that you are unlikely to use.
- ✔ For each of your priority systems, you must assign one person to perform a business impact assessment and one person to perform a vulnerability assessment. Do this: Select the Risk Manager icon , select a system, go to the “Assessment Role” tab and specify the users. Be sure you click the Update button before you navigate away from the system section.
- ✔ Optionally, you can link your systems with your business processes or vice versa.
- ✔ Optionally, you can link your systems with your physical assets, e.g. servers or other equipment.
- ✔ Optionally, review the questions that SecureAware uses for the vulnerability assessment questionnaire: Click the Risk Manager icon , then choose the  Question menu. You can add, delete or modify questions. Questions can address threats and security controls for confidentiality, integrity and availability. Questions can have individual weight in relation to other questions. Each answer option for a question has a weight between 0 and 100 for confidentiality, integrity and availability respectively.
- ✔ Optionally, review the severity scale values. Default is 1 – 5 assessment scale. You can change the scale and the meaning of the words that relate to the values 1, 2, 3, 4 or 5 respectively.

Start an assessment

- ✔ Click the Risk Manager icon , then choose ‘Create a new assessment’. specify a name and a description and click ‘Create’
- ✔ Click ‘Start’ and confirm to start the assessment immediately, then click ‘Update’
- ✔ Users who have been assigned to the task of assessing vulnerability or business impact will be presented with a questionnaire when they click on the Risk Assessment end user menu:

- ✔ As a super user, you have access to draft assessment reports from Super User’s Risk Manager menu 
- ✔ When you end an Assessment, from the Assessment menu, users can no longer respond to the questions or change their existing answers. As a super user, you can still edit the text in the assessment reports.

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.