

ARtem))))

The Wireless Connection.

User Manual

Wireless Communication

(((

)))

Onair Security Manager

Copyright © 2003 ARtem GmbH

ARtem GmbH
Olgastr. 152
D-89073 Ulm
Germany
<http://www.artem.de>

No part of this documentation may be reprinted without
the prior written permission of ARtem GmbH.

.....
Windows and Windows NT are registered trademarks of Microsoft Corporation.

*Other company, trademark, or product names not explicitly mentioned here are trademarks or registered
trademarks of their respective owners and are protected.*

.....
Imprint

This documentation was compiled by ARtem GmbH.

Status: April 2003

Table of Contents

Preface III
 Introduction III
 New Flexibility IV

Knowledge Prerequisites V

Further Documentation V

Manual Conventions V

Important Text Passages VI

ARtem Service VI

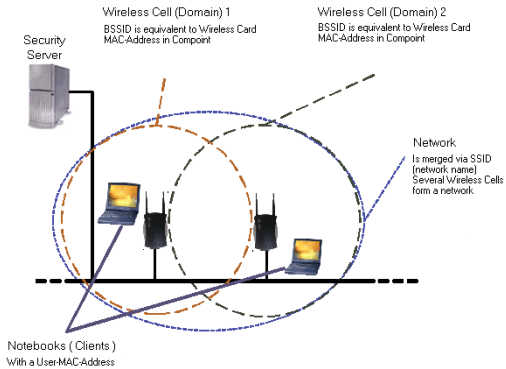
Installation and First Steps 1-1
 Introduction 1-1
 Installation 1-2
 Configuration of the ComPoints and Clients 1-10
 Description of the User Interface 1-14
 Filter 1-17
 Scenario 1-18
 Generating Reports 1-20

Description of the Application Dialog Boxes 2-1
 Network 2-1
 Client 2-5
 ComPoint 2-7
 Log 2-11
 System Parameter 2-13

Index A-1

Preface

The Onair Security Manager centrally administrates all subscribers located within a wireless infrastructure of the Onair product family. Here, it is possible to individually assign access rights which permit the precise control of the provenance of the clients.



Introduction

This mode of operation is very efficient. As soon as a wireless client (e.g. a PC, notebook, or telephone) attempts to log on at a ComPoint, the Onair Security Manager takes over the control of the access rights. For this purpose, the ComPoint forwards a request to the Security Server. In addition to a number of network parameters, this request also contains the MAC address of the wireless client. The Security Manager now checks in its database whether the client in question is authorized to access the ComPoint. Subsequently, it returns a message to the ComPoint which either grants or denies the access to the client.

For reasons of security, each attempt of an alien client to enter the network is logged, which makes it possible to take specific countermeasures.

New Flexibility

The Onair Security Manager offers multiple configuration options. In this context, the access to the wireless network is not limited, as in the case of most conventional access lists, to a single entry of the MAC addresses at the corresponding access points. It can very easily be registered and designed individually by the administrator, who performs this task centrally.

This planning can also comprise the access of specific clients on previously determined days and the logical or spatial subdivision of large-scale networks. A guest or temporary employee, for instance, would be able to access the wireless LAN in the section of the cafeteria on specific days, whereas it would be locked for him on other days or for other sections. This tool makes the management of the wireless LAN very simple.



Knowledge Prerequisites

It is assumed that the reader possesses or is in the process of acquiring the following knowledge:

- Basic knowledge of the setup of networks
- Knowledge of basic networking terms and concepts such as server, client, and IP address
- Basic understanding of Microsoft Windows operating systems

Further Documentation

You can find further information on the product Security Manager in the online help.

Manual Conventions

This manual uses the following text styles for the purpose of guiding you through the instructions:

- References to other manuals, chapters, or sections are represented in [blue](#) (in the online help screen and the PDF version of the manual) and are underlined.

Example:

See [Manual Conventions](#).

- Menus, folders, functions, hardware labels, switch settings, system messages, etc. are represented in *italic*.

Example:

Push the switch to the *off position*.

- Menus, functions, and subfunctions are separated from each other by the ">" character.

Example:

Select *File > Open...*

- Keys you need to press simultaneously are indicated by a "+" character preceding the second key.

Example:

Press Alt+A.

Important Text Passages

Important text passages are marked with symbols in the margin that indicate the following meanings:



Caution:

Contains instructions which have to be observed in order to avoid damaging the hardware or software.



Note:

Contains important general or additional information on a specific topic.



Prerequisite:

Advises you of any prerequisites which have to be fulfilled to perform the subsequent steps.

ARtem Service

Do you have any questions on our products or do you require specific information on ComPoint?

You can contact us as follows:

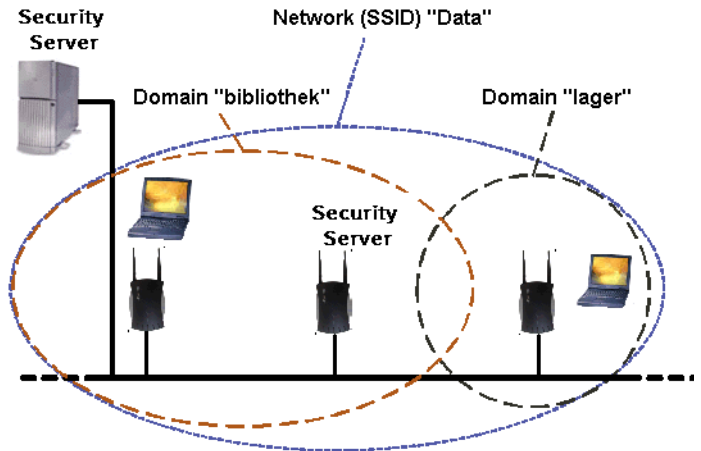
- Internet: <http://www.artem.de>
- E-mail (service): contact@artem.de
- E-mail (hotline): techsupp@artem.de

Installation and First Steps

Introduction

With the Security Manager, you can configure and monitor your network, as well as protect it against unauthorized access. By means of this configuration, you can define which clients are able to log on to a network or access it during which periods of time.

A network consists of one or several ComPoints or of one or several wireless cells with the identical, unambiguous network name. Each ComPoint contains one or two radio cards, which can be registered in one or several wireless networks.



Installation



For the installation of the Security Manager, you require administrator authorization.

To install the Security Manager, proceed as follows:

1. Double-click the *setup.exe* file which calls the installation wizard.
2. In the dialog box of the wizard, click the *Next* button. Please read the license agreement, then check the corresponding option and click *Next*. Select the preferred installation mode.
 - *Typical*
Only installs the most frequently used components to save hard disk memory. The server and client are installed in the following directory by default:
C:\Program Files\ARtem\Security Manager
3. If you wish to perform a user-specific installation, click the *Custom* button. In the following dialog box, you can select which components will be installed by clicking on the respective symbols in the drop-down list. If you click the *Disk Usage* button, you can control the required capacity of your hard disk memory. By clicking the *Reset* button, you can reset the initial state.

Use the *Browse* button to select an installation directory other than the directory used by default. If you have finished your adaptations, click the *Next* button.

4. Confirm your input by clicking the *Install* button. After the successful termination of the installation and a reboot, you can call the program from the start bar in the *ARtem\Security Manager* folder.

To execute the program, you require a valid license. A demo license for three wireless clients (secmgr.pem) comes with the Security Manager for free.

Components of the Security Manager

The program consists of a server and a client, which have to be booted separately. The server contains two components:

- the database server, which communicates with the database client via the port number 10000, and
- the server, which communicates with the ComPoint via the port number 1112.

You can either boot the server directly without additional parameters (the default parameters are 10000 or 1112), or boot it using the following values:

-p (x), --port=(x) Port number of the server

Example: **secmgr -p(port number)**

If the port number 10000 has already been assigned otherwise, this option serves to modify it from the command line. The port number which is used to perform the communication with the ComPoint (default 1112) is modified in the application. This is done upon booting the client in the *Administration > System Parameter* menu. Subsequently, you have to reboot both the client and the server. It is important that the port number entered at the ComPoint Manager (default 1112) is assigned this value.

-i,--install Install this application as service program.

-u, --uninstall Uninstall this application as service program.

-n, --noninteractive Boot without user interaction.

-U(u/p), Connect as user <u> with the password <p>.

-f(p), --logpath File for output at the server.

Example: **secmgr -f(path and name of the file)**

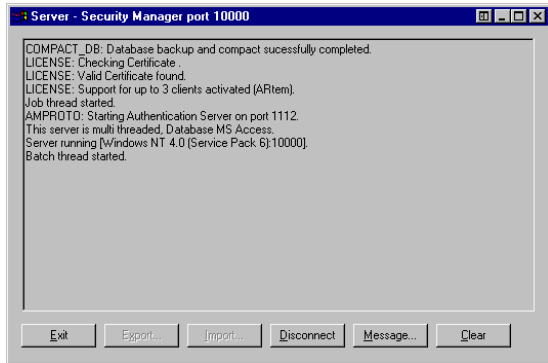
File where the output of the server window is logged. In this directory, the log file is created, as well, which contains all requests logged by the server.

-h,--help Help output.

Booting the Server

After booting the server successfully, the following dialog box is displayed:

Server - Security Manager port <port number of the server>.



The buttons have the following functions:

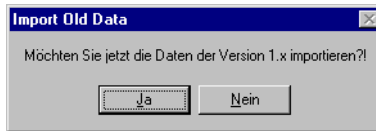
- **Exit**
The server is exited.
- **Disconnect**
This function serves to terminate the connection to all users who are logged on.
- **Message**
You can send a message to all or to specific users selected by you.
- **Clear**
The entries in the server window are deleted.

Data Import from Version 1.x

If you have installed the previous version (1.x) of the ACL Manager and wish to update it to the current version of Security Manager 2.1, you can import data from the old installation. You can import networks, ComPoints, clients, and access rules, but no logs!

After installing version 2.1, an empty database is created in the server directory. A data import can only be made as long as the database remains empty, i.e. as long as there are no clients or networks.

After booting the server, you will receive a message asking you whether you want to import old data.



You can now decide whether you want to import the old data immediately. If you want to use the existing database of version 1.x, you should do that now.

If your database does already contain entries, the import of old data cannot be carried out. In this case, delete the "SECMGR.mdb" and "secmgr_old.mdb" files in the server directory and copy the empty database supplied with version 2.1 (secmgr20.mdb) to secmgr.mdb (current database). You can now import data from an earlier version.

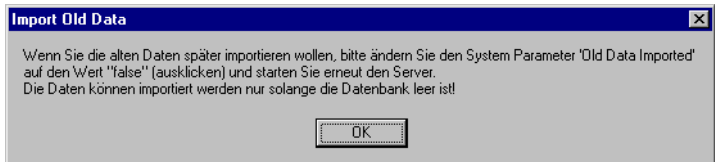


Please note that the data import of the clients will only work correctly if the "secmgr.pem" license file valid for the required number of clients is located in your server directory. If this is not the case, click *No*, exit the server, and copy the file to the server directory of the Security Manager.

After terminating the data import successfully, you will receive a message that the server has to be rebooted again.



If you want to carry out the data import later, answer with *No* and observe the following message.



To reactivate the request after the data import in the case of a server reboot at a later date, you have to set the attribute *Old Data Imported* to the value "false" (check the box) in the *Administration* > *System Parameter* client menu, and have to exit the client and server. After rebooting the server, you are asked again whether you wish to import the data.

Data Import from Version 2.x

To import data from version 2.x, select *Import* in the *Application* menu. Select the *aclmgr20.jex* bzw *secmgr2.x.jex* file.

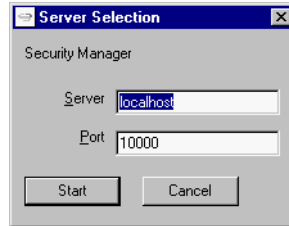
If your database does already contain entries, which are to be deleted, however, delete the "SECMGR.mdb" and "secmgr_old.mdb" files in the server directory and copy the empty database supplied with version 2.1 (secmgr20.mdb) to secmgr.mdb (current database).



Please note that the data import of the clients will only work correctly if the "secmgr.pem" license file valid for the required number of clients is located in your server directory. If this is not the case, click *No*, exit the server, and copy the file to the server directory of the Security Manager.

Booting the Client

When booting the client, the *Server Selection* dialog box is displayed.



The parameters of the dialog box are explained in the following:

- **Server**
IP address or name of the computer on which the Security Manager server is installed.
- **Port**
Port number over which the communication between the server and the client is performed (default 10000).

After entering all parameters, the administrator is booted as the first client. Initially, no entry is made under password. A further user is configured as "Guest" with the password "guest" via default. This user is only granted read authorization.

Configuration of the ComPoints and Clients

ComPoint Settings

1. Boot your ComPoint Manager and activate the *Search* function.

The ComPoint Manager automatically identifies the ComPoints installed in the network.

2. Select a device from the displayed list of ComPoints which you want to configure and start a Telnet connection.

```

Telnet - 192.168.12.47
Verbinden Bearbeiten Terminal ?
Onair ComPoint by ARtem )))
Test_CP

ComPoint BR2 - V3.08

Menu          Control Security Authenticate Submenu
-----
1 - w11_ap    [ -> ] | IP address [ 192.168.013.222 ]
2 - ACL local [ -> ] | Port number [ 1112 ]
3 - ACL remote [ -> ] | Comm. state [ connected ]
4 - ERP       [ -> ] | Def. access [ granted ]
5 - Auth. cache [ 0 ] | Sync period [ 1 ]

Configuration of the remote ACL service.

Enter a number or name, "=" main menu, [ESC] previous menu.
25:55:05[admin]>

```

After logging on as administrator, go to the *Control > Security > Authenticate > ACL remote* menu and make the following changes.

3. Enter the IP address of the Security Manager server.

The port number 1112 is preset. If this port number is used by another application, enter another free port number which you will also use to boot the Security Manager server.

The synchronization time (i.e. how often data from the cache is synchronized with data in the database) is given in minutes. The default value is 20 minutes. If you wish, you can modify this value.

4. In the *Control > Security > Authenticate* menu, activate the wireless port(s), according to the setup of the ComPoint, which are to be controlled via the Security Manager by setting the value from *disabled* to *enabled*.

Security Manager Settings

The first settings concern the *System Parameter* in the *Administration* menu. In the first step, these values have already been preset.

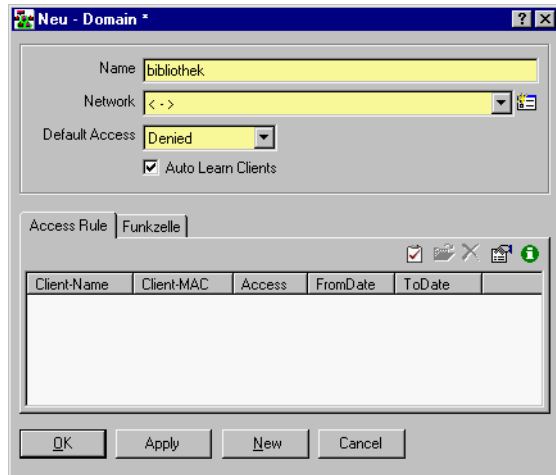
The Security Manager offers you the option to define a subnetwork within a network, which is designated as *Authentication Domain*. If a new wireless cell is learned, the *Auto Learn In Domain* attribute serves to decide in which subnetwork the information is stored. In this way, it is possible to define various subnetworks with diverging access rules within the same network. In an exemplary network "Data", for instance, the subnetworks "Library" and ""Meeting room" could be configured. All clients are authorized to access the "Library" subnetwork, while only specific clients are allowed to access the "Meeting room" subnetwork.

1. If you boot the client of the Security Manager now, the first entries will appear in the log table.

AccessCode = 2 shows that the network name (SSID) is unknown ("Unknown SSID").


2. You have to make this entry manually, the rest has to be "learned automatically". To do this, click the *New* symbol in the domain list.

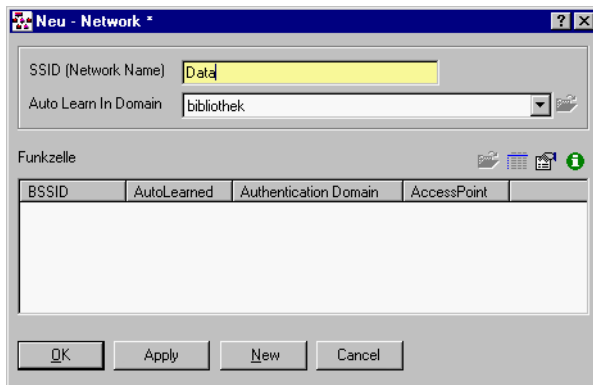
The *New – Domain** dialog box is displayed.



The parameters of the dialog box are explained in the following:

- **Name**
Name of the authentication domain.
- **Network**
Network name, as it is registered at the ComPoint.
- **Default Access**
Defines the access for recently learned clients.
- **Auto Learn Clients**
Permits or prevents the automatic learning of new clients.

3. You have to enter a name for the logical networks. Click the  icon to call the *New – Network** dialog box.

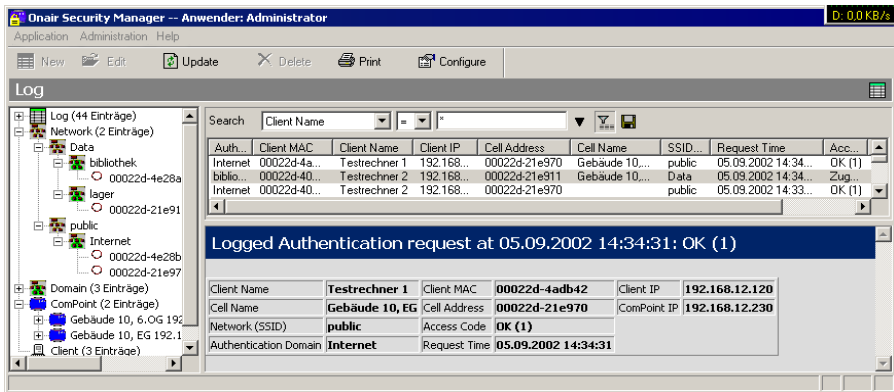


4. You can then enter a new SSID for a new network by opening the dialog box.
The relation *Auto Learn In Domain* shows in which logical network the information learned on a wireless cell is automatically stored. This value can be modified at a later point of time.

Description of the User Interface

The following sections describe the menus and the toolbar of the Security Manager software:

- [The Application Menu](#)
- [The Administration Menu](#)
- [Toolbar Buttons](#)



The Application Menu

- **Change user**
The application is exited and you can log on under a new name.
- **Change password**
You can change your password.
- **Import**
With the help of this function, you can import data from the database into a text file with the extension .jex.
- **Export**
With this function, you can export the data from the database into a text file with the name SECMGRx.x.jex (x.x is the version number), which is stored in the installation directory of the client. You can import this data again at a later point of time.

- **Deutsch/English**

Here, you can switch from German to English and back while the program is running.

The Administration Menu



The functions in this menu can only be activated by an administrator.

- **Configuration**

Under this menu item, you can define global settings of the application for the formatting for list printing.

- **User Management**

Under this menu item, all users are listed together with the corresponding data. The configuration of new users can only be performed by an administrator.

- **System Parameter**









contains the global settings of the application, such as port number of the application, log and security settings, as well as the option of notification via e-mail.

Toolbar Buttons

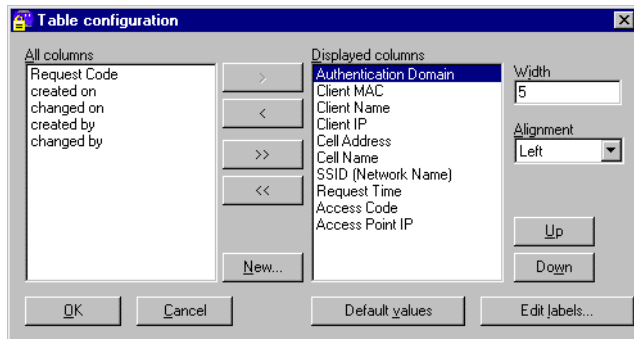
Both in the toolbar located below the main menu bar and in the head of each list view, there are buttons

- to create New <F2>,
- to Edit <F4>, and
- to Delete elements.


The effect of these actions always refers to the currently selected element type (with New) or the currently selected list element (with Edit and Delete).

-  Configures a new data set and directly creates a relation to it.
-  The selected data set from the list is edited. The same effect is obtained by double-clicking the respective data set.
-  Terminates the connection to the selected data set. The connected data set is deleted.
-  Terminates the connection to the selected data set. The connected data set is not deleted.
-  Selects a data set from the list.
-  The displayed list is updated.
-  The current list is printed.
-  The displayed attributes and the column sizes of the displayed list are adapted.

The *Table configuration* dialog box serves to adapt a list.



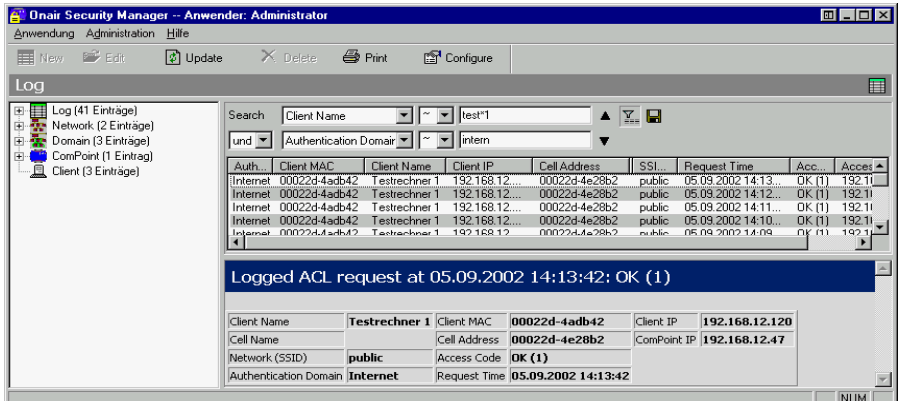
Filter

In the list view, you can define filter conditions. It is possible, for instance, to search for all requests in the log list which were initiated by a specific client. After entering the searched attribute, the relational expression, and the comparison value into the list view, click the  icon.

There are various relational expressions:

- ~ List value contains comparison value.
- = List value is equal to comparison value.
- != List value is unequal to comparison value.
- < List value is smaller than comparison value.
- <= List value is smaller than or equal to comparison value.
- > List value is larger than comparison value.
- >= List value is larger than or equal to comparison value.

In addition, wildcards (*) are permitted.



The screenshot shows the 'Onair Security Manager' interface. The 'Log' section is active, displaying a list of log entries. The search criteria are set to 'Client Name' with the value 'test*' and 'Authentication Domain' with the value 'intern'. Below the log list, a detailed view of a 'Logged ACL request' is shown for the entry at 05.09.2002 14:13:42.

Auth...	Client MAC	Client Name	Client IP	Cell Address	SSI...	Request Time	Acc...	Acces
Internet	00022d-4adb42	Testrechner 1	192.168.12...	00022d-4e28b2	public	05.09.2002 14:13...	OK (1)	192.11
Internet	00022d-4adb42	Testrechner 1	192.168.12...	00022d-4e28b2	public	05.09.2002 14:12...	OK (1)	192.11
Internet	00022d-4adb42	Testrechner 1	192.168.12...	00022d-4e28b2	public	05.09.2002 14:11...	OK (1)	192.11
Internet	00022d-4adb42	Testrechner 1	192.168.12...	00022d-4e28b2	public	05.09.2002 14:10...	OK (1)	192.11
Internet	00022d-4adb42	Testrechner 1	192.168.12...	00022d-4e28b2	public	05.09.2002 14:09...	OK (1)	192.11

Logged ACL request at 05.09.2002 14:13:42: OK (1)			
Client Name	Testrechner 1	Client MAC	00022d-4adb42
Cell Address	00022d-4e28b2	Client IP	192.168.12.120
Network (SSID)	public	ComPoint IP	192.168.12.47
Authentication Domain	Internet	Access Code	OK (1)
		Request Time	05.09.2002 14:13:42

Scenario

What happens if a client attempts to log on to a network?

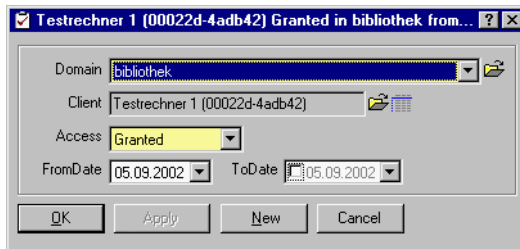
The precondition is that the network name (SSID) has correctly been entered at the client, at the ComPoint, and in the list of the Security Manager. If the ComPoint identifies a new client, it starts a request to the Security Manager server with the following parameters: (Client MAC, BSSID, SSID),

- **Client MAC**
the MAC address of the client is
- **Cell Name (BSSID)**
the MAC address of the wireless cell is
- **SSID**
the name of the physical network is

The Security Manager checks all database entries and receives an access code as answer. This access code describes whether the client will be granted access authorization or states the reason why this will not be the case.

On the side of the database, this client is "learned" if the system parameter is *Auto Learn Clients = true*. Furthermore, an access rule is created. For this objective, the parameter *allowed* is set to true/false (according to the value of the *Default Access* system parameter) and the start date (*FromDate*) is defined. By modifying these values, you can define whether and in which time intervals this client will be authorized to log on.

To make these modifications effective, you have to select the corresponding client in the client list and have to edit the access rule in the access rule list which you want to modify.



You can now modify the values of the *Access*, *FromDate*, and *ToDate* attributes.

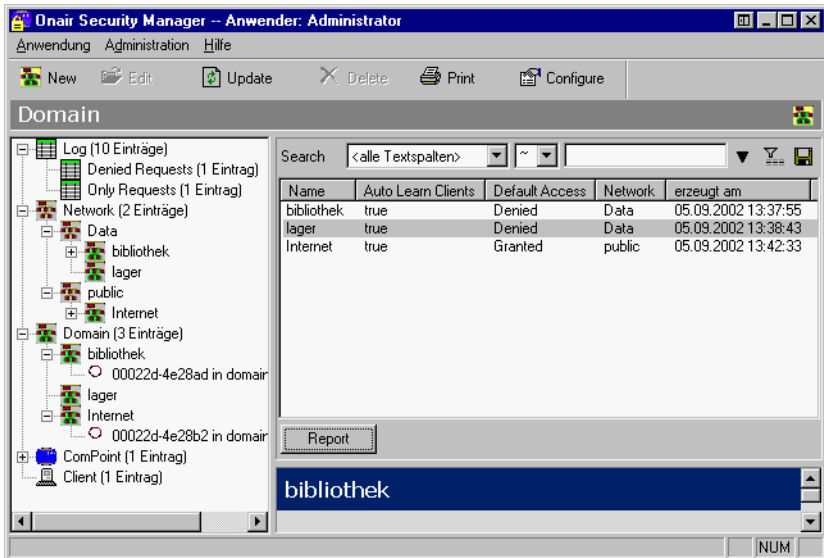
Generating Reports

To display the complete structure of the network, you can generate a report. As a result, all client access procedures on the ComPoints with the corresponding dates and access authorization can be logged.

The source file *secreport.rtf* is used, which is provided in the Rich Text Format (RTF). The report is then written into the target file *secreportout.rtf*, which is also provided in RTF.

Each generated report always has a reference object or a list of reference objects.

To display the structure of the network, you have to switch over to the *Domain* list view.

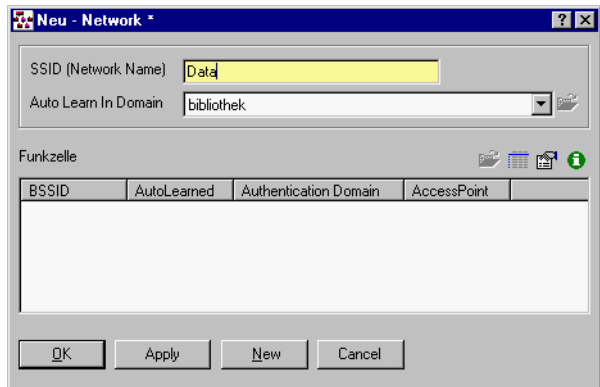


If you click the *Report* button, the *secreportout.rtf* file will be opened by Microsoft Word.

Description of the Application Dialog Boxes

Network

In contrast to LANs which have been set via Ethernet, a wireless LAN does not provide cabling to permit a permanent connection between server and clients. As a result, there is a parameter in each wireless network which identifies the network unambiguously. Only clients whose network configuration matches that of the ComPoint can communicate in this Wireless LAN (WLAN). The network is identified via the network name, the so-called SSID.



- **SSID (Network Name)**

The SSID is the network identification in a WLAN. Only clients who have entered this value in their network configurations are able to communicate with this WLAN.

- **Auto Learn In Domain**

This value contains the domain where information on the recently learned wireless cells is to be stored.

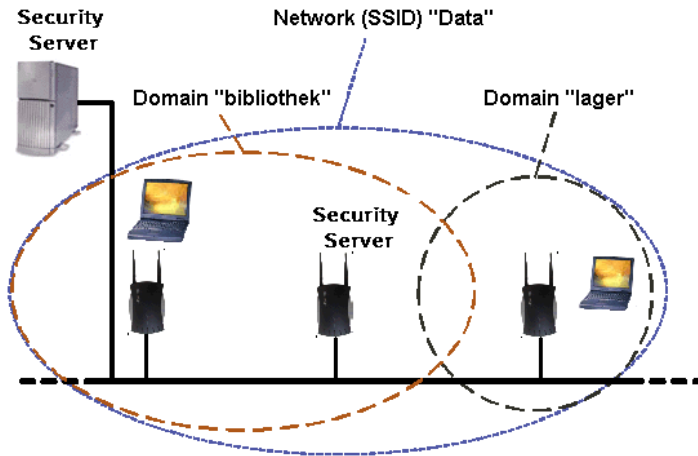
Wireless Cell

Each ComPoint contains one or two radio cards which form the wireless cell. These radio cards can be identified with the help of their unambiguous MAC addresses.

Configuring Domains in Networks

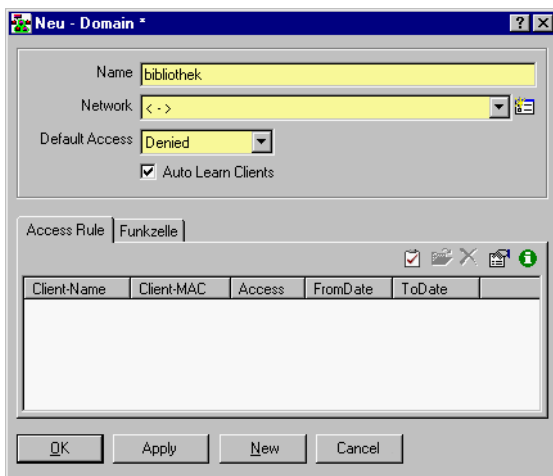
You can define an authentication domain for each network. A domain can be considered like a subnetwork. You can define several domains with the same network name in one network to map subnetworks with different access rules. In the following example, there is a wireless network "Data" with two domains: "Library" and "Meeting room".

All clients are granted access to "Library", for instance, while only specific clients are authorized to access "Meeting room".



For each network, there are two parameters which are assigned the values contained in the system parameters of the same name as default entries.

It is now also possible to define network-specific values which are only valid in one network.



The parameters of the dialog box are explained in the following:

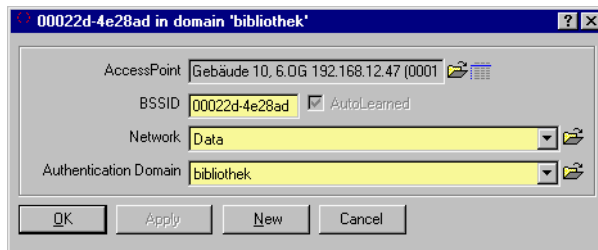
- **Name**
Name of the authentication domain.
- **Network**
Network name, as it is registered at the ComPoint.
- **Default Access**
Specifies how the network behaves when learning a new client. It may immediately contain a valid access authorization (Default Access = "Granted") or alternatively only be learned without being granted access (Default Access = "Denied").
The value "Granted" can be recommended if the Security Manager is set up anew. It is, thus, possible to monitor a network without disturbing the operation of the said network. If all clients have been learned, it can be switched over to "Denied". New clients then have to be manually granted access by the systems administrator.
- **Auto Learn Clients**
Specifies whether clients are learned automatically or manually.

The Access Rule Tab

This table shows the access authorization of the clients logged on to the network. The table can be sorted by clicking the column headings. Individual columns can be enlarged or reduced in size by shifting the separator lines with the mouse.

The Wireless Cell Tab

Each ComPoint contains one or two radio cards which form the wireless cell. These radio cards can be identified with the help of their unambiguous MAC addresses.



The parameters of the dialog box are explained in the following:

- **ComPoint**
Name (if specified), IP address, and MAC address of the corresponding ComPoint.
- **BSSID**
MAC address of the wireless cell, which is also designated as Basis Service Set Identification in Standard IEEE802.11.
- **Network**
Contains the assignment of ComPoints to networks. The assignment is generated automatically, but it can also be modified manually.
- **Authentication Domain**
Specifies in which domain the wireless cell is located. By modifying this value you can determine in which logical network (authentication domain) this ComPoint or wireless cell will log on.

Client

This dialog box serves to define parameters for the client to make it easier, for instance, to find the client in your WLAN.

Testrechner 2 (00022d-404ffe)

Name: Testrechner 2

MAC: 00022d-404ffe

IP: 192.168.12.121

AutoLearned

Last Notified: 05.09.2002 14:00:37

Access Rule

Domain-Name	Access	FromDate	ToDate
bibliothek	Denied	05.09.2002	
Internet	Granted	05.09.2002	

Buttons: OK, Apply, New, Cancel

The parameters of the dialog box are explained in the following:

- **Name**
To be able to identify the clients more easily, you can assign names to them.
- **MAC**
Contains the unambiguous MAC address of the client.
- **IP**
This is the IP address of the client. It is not automatically learned and can be entered freely, like the name.
- **AutoLearned**
According to the value of the *Auto Learn Clients* system parameter, the clients can be learned automatically (Auto Learn Clients = box is checked) or manually (Auto Learn Clients = box is not checked).

- **Last Notified**

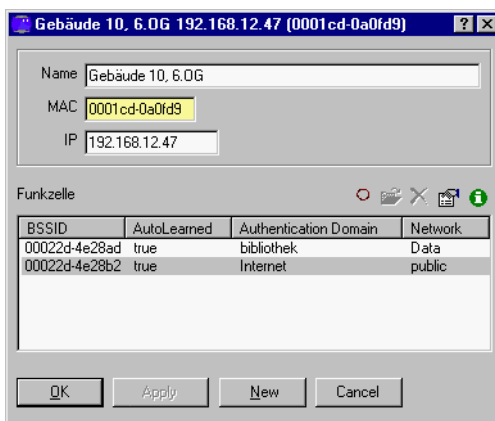
Specifies when the last e-mail was sent for this client to the administrator.

Access Rule

This table serves to display the combined elements of the access rule. This table can also remain empty. The table can be sorted by clicking the column headings. Individual columns can be enlarged or reduced in size by shifting the separator lines.

ComPoint

This dialog box serves to define parameters for the ComPoint.



The parameters of the dialog box are explained in the following:

- **Name**
Name of the ComPoint, as it is registered at the ComPoint Manager.
- **MAC**
The MAC address of the ComPoint. It is automatically learned.
- **IP**
The IP address of the ComPoint. It is automatically learned.

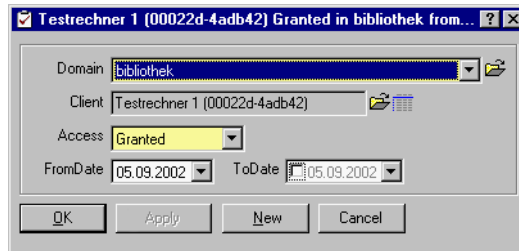
Wireless Cell

This table serves to display the combined elements of the wireless cell. This table can also remain empty.

The table can be sorted by clicking the column headings. Individual columns can be enlarged or reduced in size by shifting the separator lines.

Access Rule

In this table, all access rights are entered in the form of a logical value for the client/network.



The parameters of the dialog box are explained in the following:

- **Domain**
Select an element of network from the list which is to be combined with this access rule element. You have to select precisely one element.
- **Client**
This input field serves to set up a connection to the client. You can also select an element from the list. You have to select precisely one element.
- **Access**
This logical value describes a network access authorization for the network/client. It has an unambiguous value.
- **FromDate**
Specifies from which time on the client is allowed to log on to the network.
- **ToDate**
Specifies up to which time on the client is allowed to log on to the network.

Access Code

If a client attempts to log on to a network via a ComPoint, the ComPoint initiates a request to the database server.

This request contains the following information: MAC address of the client, MAC address of the wireless cell, and the SSID (network name). The AccessCode table contains a list with possible replies, which the administrator may receive from the server if a client attempts to log on to the network.

The following table provides a detailed explanation of the values:

Value	Meaning
0	An internal (communications) error has occurred.
1	Everything is OK, i.e. the client is allowed to log on to this network.
2	Network name (SSID) unknown (this entry does not exist in the database). To enable a client to log, the network name has to be entered by the administrator.
3	The wireless cell contains an invalid MAC address (this address has to be unambiguous).
4	The client cell contains an invalid MAC address (this address has to be unambiguous).
5	The wireless cells can be learned automatically during the first request if the administrator has checked the box for the <i>Auto Learn Cells</i> system parameter. If the box of the <i>Auto Learn Cells</i> system parameter has not been checked, this error message (AccessCode) is sent.
6	For this client, an access rule via this wireless cell has been defined in a network (but with the value "false").
7	For this client, an access rule via this wireless cell has been defined in a network, but the date does not correspond to the permitted time range, i.e. the access is only allowed at a later date.

Value	Meaning
8	If the <i>Auto Learn Clients</i> system parameter has been set by the administrator by checking the box, the clients can be learned automatically during the first request. If the box of the <i>Auto Learn Clients</i> system parameter has not been checked, this error message (AccessCode) is sent.
9	For this client, an access rule via this wireless cell has been defined in a network, but the date does not correspond to the permitted time range, i.e. the access time has run out.
10	The ComPoint contains an invalid MAC address (this address has to be unambiguous).
11	Your software license is invalid.
12	System error 12.
13	System error 13.
14	System error 14.
15	The local MAC addresses of the client cannot be learned automatically.

The parameters of the dialog box are explained in the following:

- **Code**
The code is the reply of the database. It describes whether a client was able to log on or – if not – why this was the case.
- **Description**
This is a short description of the access code.

Log

This table contains all requests initiated by the ComPoint during a specific period of time, as well as the replies with the corresponding access codes of the database server. These requests contain the client MAC address, wireless cell MAC address (BSSID), and network name (SSID). The data in this table can be written into a file at a specific log time – LogTime – if the *SaveLog* system parameter has been activated by checking the box. If it has not been activated (box of the *SaveLog* system parameter not checked), only the data of the last x days are displayed. x is defined via the *LogWindow* system parameter.

All three system parameters can only be edited by the administrator.

Logged Authentication request at 05.09.2002 14:34:31: OK (1) - Log

SSID (Network Name) public Authentication Domain Internet

Client MAC 00022d-4adb42 Client Name Testrechner 1

Cell Address 00022d-21e970 Cell Name Gebäude 10. EG

Access Code OK (1)

Request Code 1 Request Time 05.09.2002 14:34:31

Client IP 192.168.12.120

Access Point IP 192.168.12.230

Cancel < >

The parameters of the dialog box are explained in the following:

- **SSID (Network Name)**
Corresponds to the name of the wireless network (the SSID).
- **Authentication Domain**
Specifies the domain where the client has logged on via the ComPoint.
- **Client MAC**
The MAC address of the client.

- **Client Name**
The client name assigned by the systems administrator.
- **Cell Address**
The MAC address of the wireless cell (BSSID).
- **Cell Name**
The cell name corresponds to the name of the respective ComPoint.
- **Access Code**
The access codes provide information on the status of the request.
- **Request Code**
The request code indicates which type of request is made. Was it a synchronization request (RequestCode = 2) or a first log-on request (RequestCode = 1)? If this value is used in a filter condition, only the first requests will be visible.
- **Request Time**
Start time of the request.
- **Client IP**
The IP address of the client.
- **ComPoint IP**
The IP address of the ComPoint.

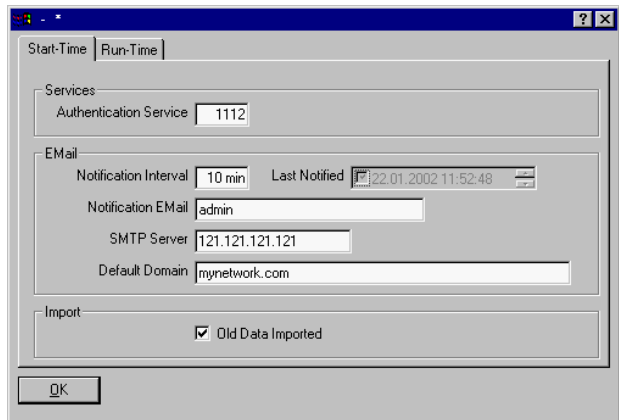
Settings of the Log Table:

- **Log Window**
By setting this attribute, the number of days is defined for which the requests are displayed in the log table.
- **Log Time**
This value serves to define at which time the log table will be written into a file. This file is stored in the current (server) directory under the name: SECMGR-yyyy-mm-dd.log
- **Save Log**
The value of this attribute serves to define whether a log file will be created.

System Parameter

With the help of the following parameters, you can influence the behavior of the system (of the network). These parameters are distributed onto two tabs, in dependence on the date when your modifications will become effective.

The values in the *Start-Time* tab will only be updated upon a reboot of the server.



The parameters of the dialog box are explained in the following:

Services

- **Authentication Service**

Specifies the port number over which the communication with the ComPoint is performed.

E-Mail Notification Settings

For each request which does not reply with OK, an e-mail is sent to the systems administrator.

- **Notification Interval**

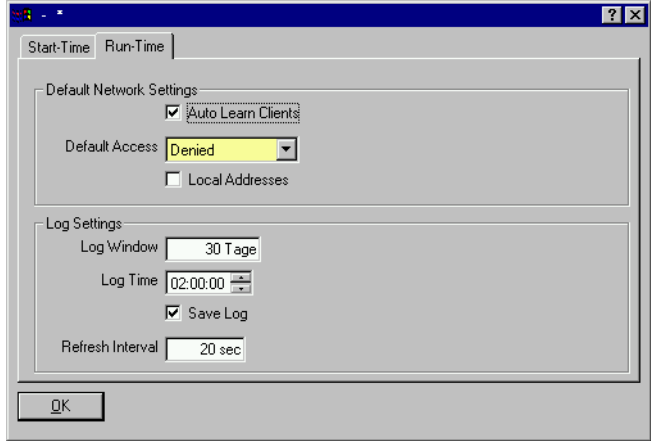
To avoid that too many e-mails are sent to the administrator, you can configure the minimum time between two notifications sent to the same client.

- **Last Notified**
Indicates when the last notification of an unknown client was sent.
- **Notification E-Mail**
If you wish the systems administrator to be notified in the case of failed log-on attempts, you have to enter the corresponding mail parameters here.
- **SMTP Server**
The IP address of the SMTP server.
- **Default Domain**
Name of the domain which is used for the e-mail address.

Import

- **Old Data Imported**
Indicates whether a database has already been imported from an ACL version 1.x. Uncheck the box if you wish to import a database. See [Data Import from Version 1.x](#).

The values in the *Run-Time* tab will be without rebooting the server.



The parameters of the dialog box are explained in the following:

Default Network Settings

- **Auto Learn Clients**

This system parameter specifies the behavior of the network in the case of a new request and can only be modified by the administrator. If the clients are to be learned automatically, the box has to be checked. If they are to be entered manually, the box should not be checked.

- **Default Access**

If a new client logs on, he is taken over into the database without gaining access authorization in the process if the value is "Denied". If the value is "Granted", an access rule with the value "Granted" is created.

- **Local Address**

The Security Manager distinguishes between locally administrated MAC addresses and the client MAC address assigned by the manufacturer. If local addresses are not to be supported (the box next to *Local Address* is not checked), these clients are not automatically learned and entered into the database. If the box next to *Local Address* is checked, this client is treated according to the standard procedure.

Log Table Settings

- **Save Log**

Specifies whether a log file is desired ("true" or "false").

- **Log Window**

Specifies in days in which time window requests will be displayed.

- **Log Time**

Specifies at which time the log file will be written.

- **Refresh Interval**

How often should the log window be updated automatically? If this attribute has the value "= sec", the log window is not automatically updated. In this case, the user has to push the <F5> button or has to click the *Update* button to update the window.

Index

A

Access [1-19](#), [2-8](#)
Access authorization [1-20](#)
Access code [2-9](#), [2-12](#)
Access rights [2-8](#)
Access rule [2-4](#), [2-6](#), [2-8](#)
ACL remote [1-10](#)
Administration menu [1-15](#)
Administrator authorization [1-2](#)
Application dialog boxes [2-1](#)
Application menu [1-14](#)
ARtem Service [1-VI](#)
Authentication domain [2-2](#), [2-4](#), [2-11](#)
Authentication service [2-13](#)
Auto Learn Clients [1-12](#), [2-3](#), [2-15](#)
AutoLearned [2-5](#)

B

Booting the client [1-9](#)
Booting the server [1-5](#)
BSSID [1-18](#), [2-4](#)

C

Cell address [2-12](#)
Cell name [1-18](#)
Change password [1-14](#)
Change user [1-14](#)
Clear [1-5](#)
Client [2-5](#), [2-8](#)
Client IP [2-12](#)
Client MAC [1-18](#), [2-11](#)
Client name [2-12](#)
ComPoint [2-4](#), [2-7](#)
ComPoint IP [2-12](#)
ComPoint Manager [1-10](#)
ComPoint settings [1-10](#)
Components of the Security Manager [1-4](#)
Configuration [1-15](#)
Configuration of the clients [1-10](#)
Configuration of the ComPoints [1-10](#)
Configuring domains [2-2](#)
Custom [1-2](#)

D

Data import from version 1.x [1-6](#)
Data import from version 2.x [1-7](#)
Database client [1-4](#)
Database server [1-4](#)
Default access [1-12](#), [2-3](#), [2-15](#)
Default domain [2-14](#)
Default network settings [2-15](#)
Del button [1-15](#)
Delete [1-15](#)
Demo license [1-3](#)
Deutsch/English [1-15](#)
Disconnect [1-5](#)
Disk usage [1-2](#)
Documentation [V](#)
Domain [2-8](#)

E

Edit [1-15](#)
E-mail [1-VI](#)
E-mail notification settings [2-13](#)
Exit [1-5](#)
Export [1-14](#)

F

Filter [1-17](#)
Filter conditions [1-17](#)
FromDate [1-19](#), [2-8](#)
F2 button [1-15](#)
F4 button [1-15](#)

G

Generating reports [1-20](#)

I

Import [1-14](#)
Installation [1-2](#)
Installation mode [1-2](#)
 Typical [1-2](#)
Internet [1-VI](#)
IP [2-5](#), [2-7](#)
IP address of the ComPoint [2-7](#)
IP address of the Security Server [1-10](#)

K

Knowledge prerequisites [1-V](#)

L

Last notified [2-6](#), [2-14](#)

License agreement [1-2](#)

Local address [2-16](#)

Log [2-11](#)

Log table settings [2-16](#)

Log time [2-16](#)

Log window [2-16](#)

M

MAC [2-5](#), [2-7](#)

MAC address of the ComPoint [2-7](#)

Manual conventions [1-V](#)

Message [1-5](#)

N

Name [2-5](#)

Name of the ComPoint [2-7](#)

Name of the security domain [2-3](#)

Name of the Security Manager domain [1-12](#)

Network [1-12](#), [2-1](#), [2-3](#), [2-4](#)

Network name (SSID) [2-4](#)

New [1-15](#)

Notification e-mail [2-14](#)

Notification interval [2-13](#)

O

Onair Security Manager [III](#)

Online help [V](#)

P

Port [1-9](#)

Port number [1-4](#)

R

Radio card [2-1](#), [2-4](#)

Reboot of the server [2-13](#)

Refresh interval [2-16](#)

Report [1-20](#)

Request code [2-12](#)

Request time [2-12](#)

Run-Time [2-15](#)

S

Save log [2-16](#)
Scenario [1-18](#)
secmgr.pem [1-6](#), [1-8](#)
secreportout.rtf [1-20](#)
secreport.rtf [1-20](#)
Security Manager settings [1-11](#)
Server [1-4](#), [1-9](#)
Server parameters [1-4](#)
Services [2-13](#)
setup.exe [1-2](#)
SMTP server [2-14](#)
Source file [1-20](#)
SSID [1-18](#), [2-11](#)
Start-Time [2-13](#)
Subnetwork [2-2](#)
Symbols [1-VI](#)
Synchronization time [1-11](#)
System parameter [1-11](#), [1-15](#), [2-11](#), [2-13](#)

T

Table configuration [1-16](#)
Target file [1-20](#)
Text passages [1-VI](#)
ToDate [1-19](#), [2-8](#)
Toolbar buttons [1-15](#)

U

User interface [1-14](#)
User management [1-15](#)

W

Wireless cell [2-4](#), [2-7](#)
Wireless LAN [2-1](#)

Numerics

10000 [1-4](#)
1112 [1-4](#)