ARtem

The Wireless Connection.

# User Manual

## Wireless Communication

Onair Security Manager

ARtem GmbH
Olgastr. 152
D-89073 Ulm

http://www.artem.de

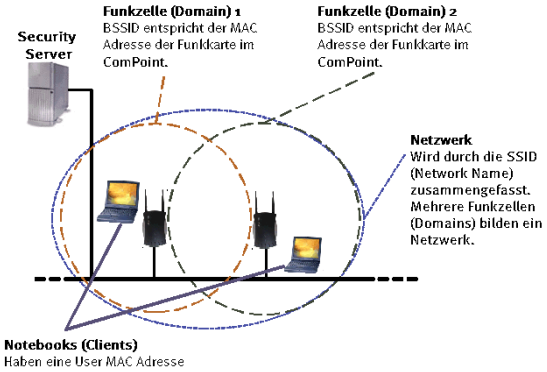


***Stand September 2002***

# *Inhaltsverzeichnis*

## Vorwort

Der Onair Security Manager verwaltet alle Teilnehmer zentral, die sich innerhalb einer Funkinfrastruktur aus der Onair-Familie aufhalten. Hier können Zugriffsrechte individuell vergeben werden, die genaue Kontrollen über die Herkunft der Clients erlauben.




### Vorbetrachtungen

Die Funktionsweise ist dabei sehr effektiv, denn sobald ein Wireless Client (z.B. ein PC, Notebook oder Telefon) versucht, sich an einem ComPoint anzumelden, übernimmt der Onair Security Manager die Regelung der Zugriffsrechte. Dazu startet der ComPoint eine Anfrage beim Security Server. Diese Anfrage enthält außer einigen Netzwerkparametern des ComPoints auch die MAC Adresse des Wireless Clients. Der Security Manager prüft nun in seiner Datenbank, ob dieser Client zugriffsberechtigt ist. Anschließend schickt er eine Meldung an den ComPoint zurück, die entweder den Zugriff des Clients erlaubt oder untersagt.

Zur Sicherheit wird jeder Versuch eines fremden Clients in das Netz einzudringen protokolliert, wodurch sich gezielte Gegenmaßnahmen ergreifen lassen.

***Neue Flexibilität***

Der Onair Security Manager bietet vielfältige Konfigurationsmöglichkeiten. Der Zugriff auf das Funknetz ist dabei nicht wie bei den meisten üblichen Zugangslisten auf den einmaligen Eintrag der MAC Adressen in den jeweiligen Access Points beschränkt, sondern lässt sich vom Administrator sehr einfach zentral registrieren und individuell gestalten.

In diese Planung kann auch der Zugriff bestimmter Clients an zuvor festgelegten Tagen einbezogen und logische oder räumliche Untergliederungen von umfangreichen Netzen ausgestaltet werden. So steht z.B. einem Gast oder temporärem Mitarbeiter im Bereich der Cafeteria das Wireless LAN für einzelne Tage offen, für andere Bereiche und Tage wäre es gesperrt. Mit diesem Tool wird das Management des Wireless LANs sehr einfach.






## Vorkenntnisse

Die Inhalte dieses Handbuches setzen die folgenden Basiskenntnisse voraus:

- Basiskenntnisse im Netzwerkaufbau
- Kenntnisse über die grundlegende Netzwerkterminologie, wie beispielsweise Server, Client und IP-Adresse
- Grundkenntnisse bei der Bedienung von Microsoft Windows Betriebssystemen

## Weitere Dokumentation

Weitere Informationen über das Produkt Security Manager finden Sie in der Online-Hilfe.

## Schreibkonventionen

Folgende Schreibkonventionen werden verwendet:

- Verweise auf andere Handbücher, Kapitel und Abschnitte sind blau (am Bildschirm in der Online-Hilfe bzw. im PDF) und unterstrichen.

  Beispiel: Siehe Schreibkonventionen.

- Menüs, Ordner, Funktionen, Hardwarebeschriftungen, Schalterstellungen, Systemmeldungen etc. werden *kursiv* dargestellt.

  Beispiel: Stellen Sie den Schalter auf *off*.

- Menüs, Funktionen und Unterfunktionen werden durch „›“ voneinander getrennt.

  Beispiel: Wählen Sie *Datei › Öffnen...*

- Tasten, die Sie gleichzeitig gedrückt halten sollen, werden durch ein Plus-Zeichen verbunden.

  Beispiel: Drücken Sie ‹Alt›+‹A›.

## *Wichtige Textstellen*

Wichtige Textstellen sind am Rand mit Symbolen versehen, die folgende Bedeutung haben:


Vorsicht:

Enthält Informationen, die beachtet werden müssen, um Schaden an Hardware oder Software zu verhindern.

Hinweis:

Enthält wichtige allgemeine oder zusätzliche Informationen zu einem bestimmten Thema.

Voraussetzung:

Benennt Voraussetzungen, die erfüllt sein müssen, damit die nachfolgenden Handlungsschritte durchgeführt werden können.

## ARtem Service

Haben Sie Fragen zu unseren Produkten oder benötigen Sie konkrete Informationen zum Security Manager?

Dann können Sie uns wie folgt kontaktieren:

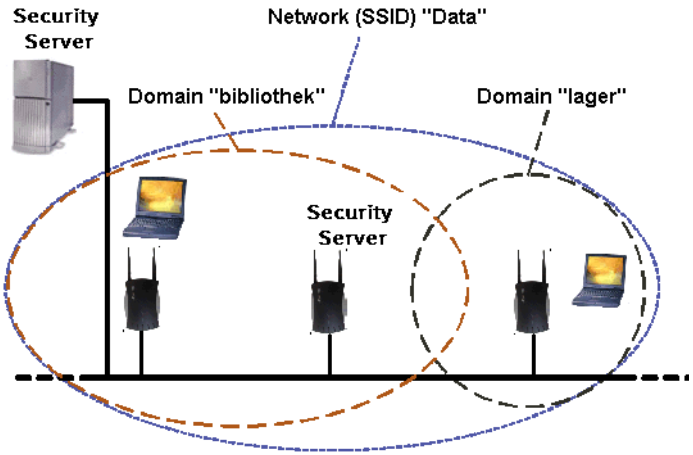
- Internet: http://www.artem.de
- E-Mail (Service): contact@artem.de
- E-Mail (Hotline): techsupp@artem.de

# Installation und erste Schritte

## Einführung

Der Security Manager bietet Ihnen die Möglichkeit, Ihr Netzwerk zu konfigurieren, zu überwachen und gegen unerlaubten Zugriff abzusichern. Diese Konfiguration bedeutet, dass Sie einstellen können, welche Clients sich in welchem Zeitraum und in welchem Netz anmelden können, bzw. Zugang bekommen.

Ein Netzwerk besteht aus einem oder mehreren ComPoints bzw. aus einer oder mehreren Funkzellen, die den gleichen eindeutigen Netzwerknamen haben. Jeder ComPoint enthält eine oder zwei Funkkarten, die in einem oder verschiedenen Funknetzen eingetragen sein können.



## *Installation*

Zur Installation benötigt man Administratorrechte.

Gehen Sie wie folgt vor, um den Security Manager zu installieren:

1. Doppelklicken Sie die Datei *Setup.exe*, die den Installationsassistenten aufruft.
2. Betätigen Sie im Dialogfenster des Assistenten die Schaltfläche *Weiter*. Lesen Sie bitte den Lizenzvertrag, aktivieren Sie anschließend das entsprechende Optionsfeld, und klicken Sie auf *Weiter*.
   Wählen Sie nun die gewünschte Installationsart.
   - *Typisch*
     Installiert nur die am häufigsten verwendeten Komponenten, um Festplattenplatz zu sparen.
   - *Vollständig*
     Installiert sämtliche Features des Security Managers und benötigt dadurch den meisten Speicherplatz. Bei beiden Optionen werden Server und Client defaultmäßig in das folgende Verzeichnis installiert:

     *C:\Programme\ARtem\Security Manager*
3. Wünschen Sie eine benutzerspezifische Installation, betätigen Sie die Schaltfläche *Angepasster Installationsmodus*.
   Im folgenden Dialogfenster können Sie auswählen, welche Komponenten installiert werden sollen, indem Sie auf die dazugehörigen Symbole im Auswahlfenster klicken. Per Klick auf die Schaltfläche *Speicherplatz* kontrollieren Sie die dazu auf Ihrer Festplatte benötigte Kapazität. Über die Schaltfläche *Zurücksetzen* können Sie den Ausgangszustand wieder herstellen.

   Möchten Sie ein anderes als das defaultmäßig verwendete Installationsverzeichnis angeben, nutzen Sie die Schaltfläche *Durchsuchen*. Klicken Sie nach dem Beenden Ihrer Anpassungen die Schaltfläche *Weiter*.

4. Betätigen Sie abschließend die Schaltfläche *Installieren*. Nach erfolgreichem Abschluss der Installation und einem Neustart können Sie das Programm von der Startleiste im Ordner *ARtem\Security Manager* aufrufen.

Zum Ausführen des Programms benötigen Sie eine gültige Lizenz. Die Demolizenz für drei wireless Clients ist mitgeliefert (secmgr.pem).

### *Komponenten des Security Manager*

Das Programm besteht aus einem Server und einen Client, die separat gestartet werden müssen. Der Server beinhaltet zwei Komponenten:

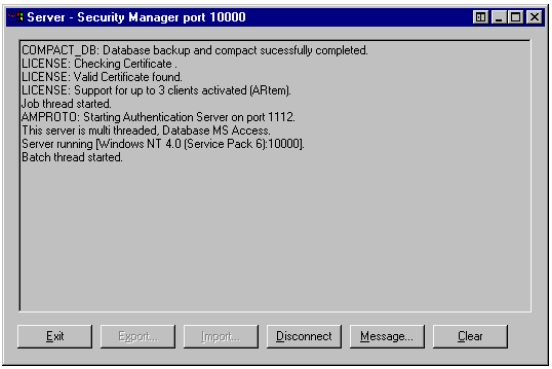
- den Datenbankserver, der über die Portnummer 10000 mit dem Datenbankclient kommuniziert, und
- den Server, der mit dem ComPoint über die Portnummer 1112 kommuniziert.

  Den Server kann man direkt ohne zusätzliche Parameter starten (die Default Portnummern sind 10000 bzw. 1112), oder mit folgenden Werten:

| | |
|---|---|
| -p (x), --port=(x) | Portnummer des Servers<br><br>Beispiel: **secmgr -p(portnummer)**<br>Falls die Portnummer 10000 besetzt ist, können Sie sie mit dieser Option von der Kommandozeile ändern. Die Portnummer, über welche die Kommunikation mit dem ComPoint erfolgt (Default 1112) wird in der Anwendung geändert. Dies erfolgt beim Start des Clients im Menü *Administration › Systemparameter.* Anschließend müssen Sie sowohl den Client als auch den Server neu starten. Wichtig ist, dass die im ComPoint Manager eingetragene Portnummer (Default 1112), auch diesen Wert erhält. |
| -i,--install | Diese Applikation als Serviceprogramm installieren. |
| -u, --uninstall | Diese Applikation als Serviceprogramm deinstallieren. |
| -n, --noninteractive | Ohne Userinteraktion starten |
| -U(u/p), | Als User ‹u› mit Passwort ‹p› verbinden |
| -f(p), --logpath | Datei zur Serverausgabe<br><br>Beispiel: **secmgr -f(Pfad und Name der Datei)**<br>Datei, in der die Ausgaben des Serverfensters protokolliert werden. In diesem Verzeichnis wird auch die Log-Datei erzeugt, die alle vom Server protokollierten Anfragen enthält. |
| -h,--help | Ausgabe der Hilfe |

### *Server starten*

Nach dem Starten des Servers erscheint der Dialog *Server - Security Manager port‹Portnummer des Servers›*.




Die Schaltflächen haben folgende Funktionalität:

- **Exit**
  Der Server wird beendet.
- **Disconnect**
  Mit dieser Funktion können Sie die Verbindung zu allen angemeldeten Usern trennen.
- **Message**
  Sie können allen oder auch nur den ausgewählten Usern eine Nachricht schicken.
- **Clear**
  Die Einträge aus dem Server-Fenster werden gelöscht.

### *Datenimport aus Version 1.x*

Falls Sie die vorherige Version (1.x) des ACL Managers installiert hatten und auf die aktuelle Version Security Manager 2.1 updaten möchten, können Sie Daten aus ihrer älteren Installation importieren. Importiert werden Netzwerke, ComPoints, Clients und Access Rules, keine Logs!

Nach dem Installieren der Version 2.1 befindet sich im Server Verzeichnis eine leere Datenbank. Die Datenübernahme kann nur durchgeführt werden solange die Datenbank leer ist, d.h. solange noch keine Clients oder Netzwerke vorhanden sind.

Sobald Sie den Server gestartet haben bekommen Sie die Meldung, ob Sie alte Daten importieren möchten.

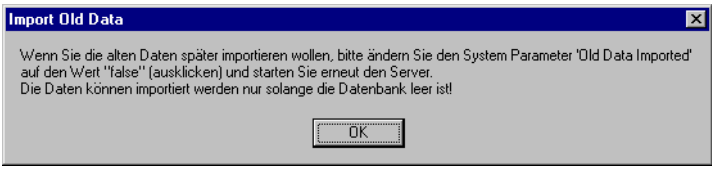

Jetzt können Sie entscheiden, ob Sie gleich die alten Daten importieren. Wenn Sie eine bestehende Datenbank der Version 1.x weiterverwenden möchten, sollten Sie das jetzt tun.

Falls Ihre Datenbank schon Einträge enthält, kann der Import der alten Daten nicht durchgeführt werden. In diesem Fall löschen Sie bitte die Datei "SECMGR.mdb" und "secmgr_ old.mdb" im Server Verzeichnis, und kopieren Sie die mitgelieferte leere Datenbank (secmgr20.mdb) nach secmgr.mdb (aktuelle Datenbank). Jetzt können Sie die Daten aus einer früheren Version importieren.

Bitte beachten Sie, dass der Datenimport der Clients nur dann korrekt funktioniert, wenn sich die für die benötigte Anzahl gültige Lizenzdatei "secmgr.pem" in ihrem Serververzeichnis befindet. Sollte dies nicht der Fall sein, antworten Sie mit *Nein*, beenden Sie den Server und kopieren Sie die Datei in das Security Manager Serververzeichnis.

Nachdem der Datenimport erfolgreich abgeschlossen wurde bekommen Sie die Meldung, dass der Server erneut gestartet werden muss.


Wenn Sie den Datenimport später durchführen wollen, beantworten Sie die Frage mit *Nein*, und beachten Sie die folgende Meldung.




Um bei einem späteren Neustart des Servers die Abfrage nach dem Datenimport wieder zu aktivieren, müssen Sie in das Client Menü *Administration › System Parameter* das Attribut *Old Data Imported* auf den Wert "false" setzen (Haken in der Checkbox deaktivieren), Client und Server beenden. Beim nächsten Neustart des Servers werden Sie erneut gefragt, ob Sie die Daten importieren möchten.

### *Datenimport aus Version 2.x*

Um Daten aus einer Version 2.x zu importieren wählen Sie im Menü *Anwendung › Importieren*. Wählen Sie hier die gewünschte Datei aclmgr20.jex bzw secmgr2.x.jex aus.

Sollte Ihre Datenbank zwar bereits Einträge enthalten, die jedoch gelöscht werden sollen, löschen Sie bitte die Datei "SECMGR.mdb" und "secmgr_old.mdb" im Server Verzeichnis, und kopieren Sie die mitgelieferte leere Datenbank (secmgr20.mdb) nach secmgr.mdb (aktuelle Datenbank).

Bitte beachten Sie, dass der Datenimport der Clients nur dann korrekt funktioniert, wenn sich die für die benötigte Anzahl gültige Lizenzdatei "secmgr.pem" in ihrem Serververzeichnis befindet. Sollte dies nicht der Fall sein, antworten Sie mit *Nein*, beenden Sie den Server und kopieren Sie die Datei in das Security Manager Serververzeichnis.

### *Client starten*

Beim Starten des Clients erscheint der Dialog *Server Selection*.


Die Parameter des Dialoges werden im folgenden erläutert:

- **Server**
  IP-Adresse oder der Name des Rechners, auf dem der Security Manager Server läuft.
- **Port**
  Portnummer, über die die Kommunikation zwischen dem Server und dem Client erfolgt (Default 10000).

Nach der Angabe aller Parameter startet als erster Client der Administrator. Das Passwort ist anfangs leer. Ein weiterer Benutzer "Gast" mit dem Passwort "gast" ist defaultmäßig angelegt. Dieser Benutzer besitzt nur Leserechte.

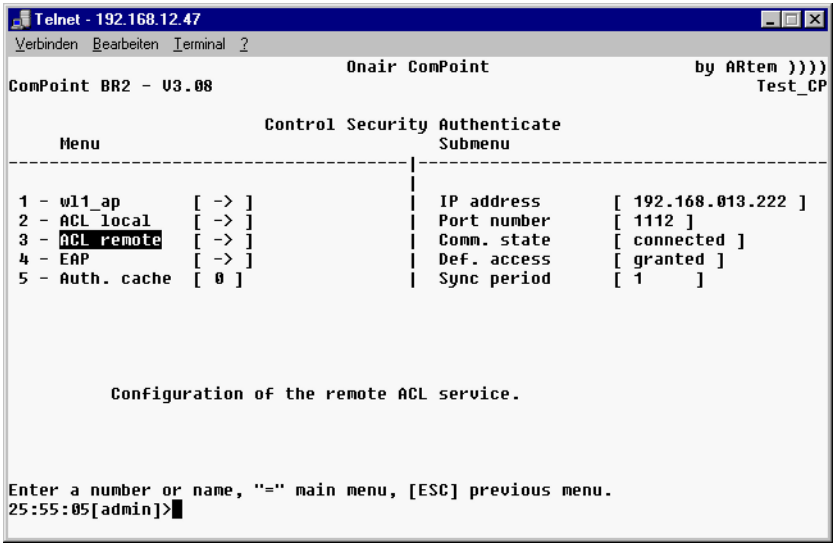
# *Konfiguration der ComPoints und Clients*

## *ComPoint Einstellungen*

1. Starten Sie Ihren ComPoint Manager, und rufen Sie die Funktion *Suchen* auf.

   Der ComPoint Manager erkennt automatisch die im Netz installierten ComPoints.

2. Wählen Sie aus der angezeigten Liste der ComPoints das Gerät aus, das Sie konfigurieren möchten, und starten Sie eine Telnet Verbindung.




   Nachdem Sie sich als Admin angemeldet haben, gehen Sie in das Menü *Control › Security › Authenticate › Acl remote* und führen Sie folgende Änderungen aus.

3. Tragen Sie die IP-Adresse des Security Manager Servers ein.

Die Portnummer 1112 ist voreingestellt. Falls diese Portnummer von einer anderen Anwendung benutzt wird, tragen Sie eine andere freie Portnummer ein, mit der Sie auch den Security Manager Server starten.

Die Synchronisationszeit (wie oft Daten aus dem Cache mit denen aus der Datenbank synchronisiert werden) wird in Minuten angegeben. Der Ausgangswert entspricht 20 Minuten; falls gewünscht, können Sie diesen Wert ändern.

4. Aktivieren Sie im Menü *Control › Security › Authenticate* den oder die Wireless Ports, je nach Ausstattung des Com-Points, die über den Security Manager kontrolliert werden sollen, indem Sie den Wert von *disabled* auf *enabled* ändern.

### *Security Manager Einstellungen*

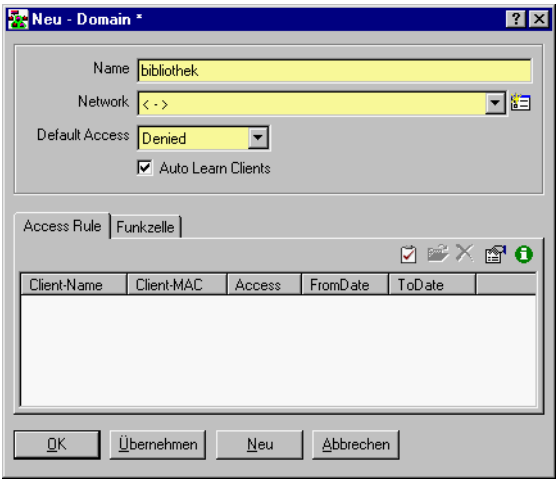
Die ersten Einstellungen sind die *System Parameter* im Menü *Administration*. Die Werte sind im ersten Schritt schon vorbelegt.

Der Security Manager bietet Ihnen die Möglichkeit, innerhalb eines Netzes ein Subnetz zu definieren, welches als *Authentification Domain* bezeichnet wird. Wenn eine neue Funkzelle gelernt wird, kann man mit Hilfe des Attributes *AutoLearn In Domain* entscheiden, in welchem Subnetz diese Informationen gespeichert werden sollen. Auf diese Weise ist es möglich, im selben Netz mehrere Subnetze mit verschiedenen Zugriffsregeln zu definieren. In einem Beispielnetz "Data" könnte es die Subnetze "Bibliothek" und "Besprechungsraum" geben. Auf das Subnetz "Bibliothek" dürfen alle Clients Zugriff bekommen, während auf das Subnetz "Besprechungsraum" nur bestimmte Clients Zugriff haben.

1. Wenn Sie jetzt den Client des Security Managers starten, erscheinen in der Log-Tabelle die ersten Eintragungen.

   Der AccessCode = 2 zeigt, dass der Netzwerkname (SSID) unbekannt ist ("unbekannte SSID").

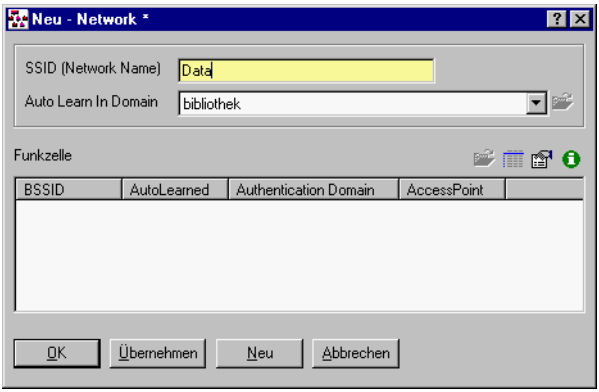
2. Diesen Eintrag müssen Sie manuell durchführen, der Rest wird "automatisch gelernt". Klicken Sie hierfür in der Domain Liste das Symbol *Neu* an.
   Es erscheint der Dialog *Neu - Domain**.




Die Parameter des Dialoges werden im folgenden erläutert:

- **Name**
  Name der Authentification Domain.
- **Network**
  Netzwerkname, so wie er im ComPoint eingetragen ist.
- **Default Access**
  Definiert den Zugriff für neu gelernte Clients.
- **Auto Learn Clients**
  Erlaubt oder verhindert das automatische Lernen neuer Clients.

3. Sie müssen einen Namen für die logischen Netze eingeben. Klicken Sie auf das Icon , um den Dialog *Neu - Network ** aufzurufen.

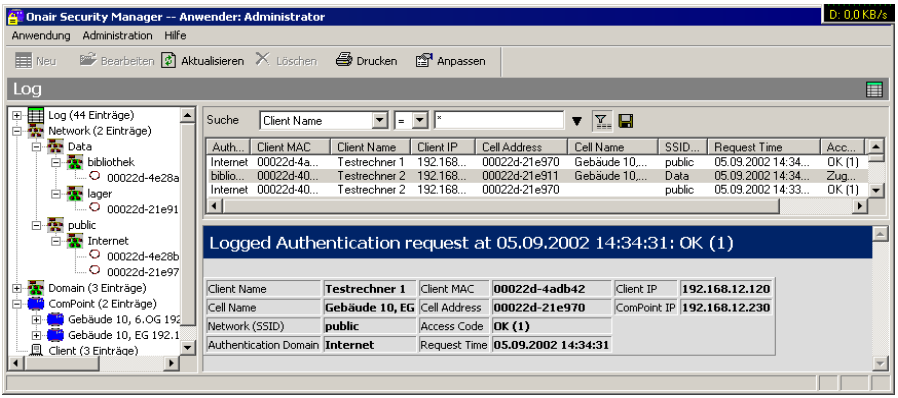



4. Anschließend können Sie durch das Öffnen des Dialoges für ein neues Netz eine neue SSID eintragen.
   Die Beziehung *Auto Learn In Domain* zeigt an, in welchem logischen Netz die gelernten Informationen über eine Funkzelle automatisch gespeichert werden. Diesen Wert kann man zu einem späteren Zeitpunkt ändern.

# *Beschreibung der Benutzeroberfläche*

Im den folgenden Abschnitten werden die Menüs und die Toolbar der Security-Manager-Software beschrieben:






## *Menü Anwendung*

- **Neu Anmelden**
  Die Anwendung wird beendet, und Sie können sich unter einem anderen Namen anmelden.
- **Passwort ändern**
  Sie können Ihr Passwort ändern.
- **Importieren**
  Mit Hilfe dieser Funktion können Sie die Daten aus der Datenbank in eine Textdatei mit der Erweiterung .jex importieren.
- **Exportieren**
  Mit Hilfe dieser Funktion können Sie die Daten aus der Datenbank in eine Textdatei mit dem Namen SECMGRx.x.jex (x.x ist die Versionsnummer) exportieren, die im Installationsverzeichnis des Clients gespeichert wird. Diese Daten können Sie zu einem späteren Zeitpunkt wieder importieren.

- **deutsch/englisch**
  Hier kann zur Laufzeit des Programms zwischen englisch und deutsch umgeschaltet werden.

### *Menü Administration*

Die Funktionen, die unter diesem Menü stehen, können nur vom Administrator aufgerufen werden.

- **Einstellungen**
  Hier können Sie globale Einstellungen der Anwendung zur Formatierung beim Listendruck festlegen.
- **Benutzerverwaltung**
  Hier sind alle Benutzer und die dazugehörigen Daten aufgelistet. Das Anlegen neuer Benutzer kann nur vom Administrator durchgeführt werden.
- **System Parameter**
  sind die globalen Einstellungen der Anwendung wie Portnummer der Anwendung, Log- und Sicherheitseinstellungen sowie die Option zur Benachrichtigung per E-Mail.

### *Toolbar Buttons*

Sowohl in der unterhalb der Hauptmenüleiste angeordneten Symbolleiste als auch am Kopf jeder Listendarstellung existieren die Schaltflächen

- zur Neuanlage ‹F2›,
- zum Bearbeiten ‹F4› und
- zum Löschen ‹Entf› von Elementen.

Die Wirkung dieser Aktionen bezieht sich immer auf den aktuell ausgewählten Elementtyp (bei Neu) bzw. auf das aktuell ausgewählte Listenelement (bei Bearbeiten und Löschen).

Einen neuen Datensatz anlegen und direkt eine Beziehung zu ihm herstellen.

Der ausgewählte Datensatz aus der Liste wird zur Bearbeitung editiert. Den gleichen Effekt erzielt man, wenn man auf dem gewünschten Datensatz doppelklickt.

Die Verbindung zum selektierten Datensatz aufheben. Der verbundene Datensatz wird gelöscht.

Die Verbindung zum selektierten Datensatz aufheben. Der verbundene Datensatz wird nicht gelöscht.

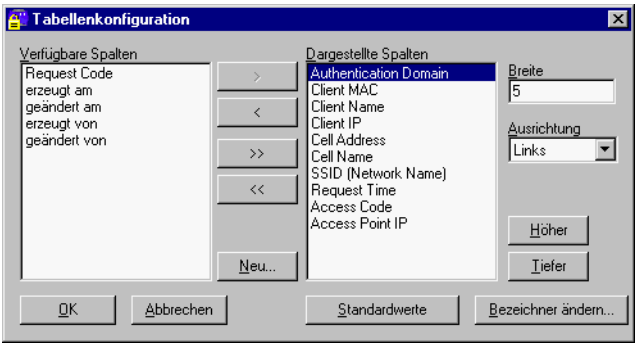
Einen Datensatz aus einer Liste auswählen.

Die angezeigte Liste wird aktualisiert.

Die aktuelle Liste wird ausgedruckt.

Die dargestellten Attribute und die Größe der Spalten der angezeigten Liste werden angepasst.

Der Dialog *Tabellenkonfiguration* dient dem Anpassen einer Liste.



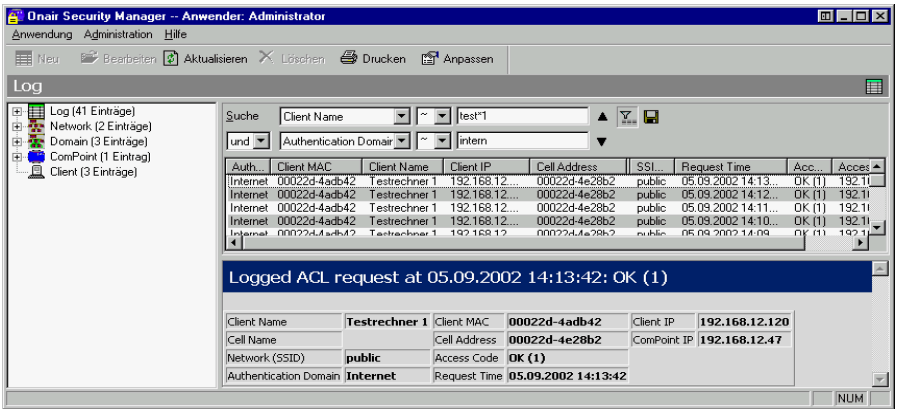
## *Filtern*

In der Listenansicht können Sie Filterbedingungen definieren. Es ist beispielsweise möglich, in der Log Liste nach allen Anfragen zu suchen, die von einem bestimmten Client gestartet wurden. Nachdem Sie in der Listenansicht das zu suchende Attribut, den Vergleichsausdruck und den Vergleichswert eingetragen haben, klicken Sie auf das Icon .

Es gibt verschiedene Vergleichsausdrücke:

| | |
|---|---|
| ~ | Listenwert enthält Vergleichswert |
| = | Listenwert ist gleich Vergleichswert |
| != | Listenwert ist ungleich Vergleichswert |
| ‹ | Listenwert ist kleiner Vergleichswert |
| ‹= | Listenwert ist kleiner oder gleich Vergleichswert |
| › | Listenwert ist größer Vergleichswert |
| ›= | Listenwert ist größer oder gleich Vergleichswert |

Weiterhin sind Wildcards (*) erlaubt.



## *Szenario*

Was passiert, wenn ein Client versucht, sich in einem Netz anzumelden?

Voraussetzung ist, dass der Netzwerkname (SSID) sowohl beim Client, im ComPoint, als auch in der Liste des Security Managers korrekt eingetragen wurde. Wenn der ComPoint einen neuen Client erkennt/identifiziert, startet er eine Anfrage an den Security Manager Server mit folgenden Parametern: (ClientMAC, BSSID, SSID),

- **Client MAC**
  die MAC-Adresse des Clients ist
- **Cell Name (BSSID)**
  die MAC-Adresse der Funkzelle ist
- **SSID**
  der Name des physikalischen Netzes ist

Der Security Manager Server überprüft die Datenbankeinträge und bekommt als Antwort einen Access Code. Dieser Access Code beschreibt, ob der Client eine Zugangsberechtigung erhält bzw. nennt auch den Grund, falls dies nicht der Fall sein sollte.

Auf der Datenbankseite wird dieser Client "gelernt", falls der Systemparameter *AutoLearn Clients = true* ist, und es wird eine Access Rule erzeugt. Dafür wird der Parameter *allowed* auf true/false gesetzt (je nach Wert des Systemparameters *Default Access)* und es wird ein Anfangsdatum (*From Date*) definiert. Durch Änderungen dieser Werte können Sie entscheiden, ob und in welchem Zeitraum sich dieser Client weiterhin anmelden darf.

Um diese Änderungen durchzuführen, müssen Sie in der Client Liste den entsprechenden Client auswählen und in der AccessRule Liste diejenige Zugriffsregel editieren, die Sie ändern möchten.

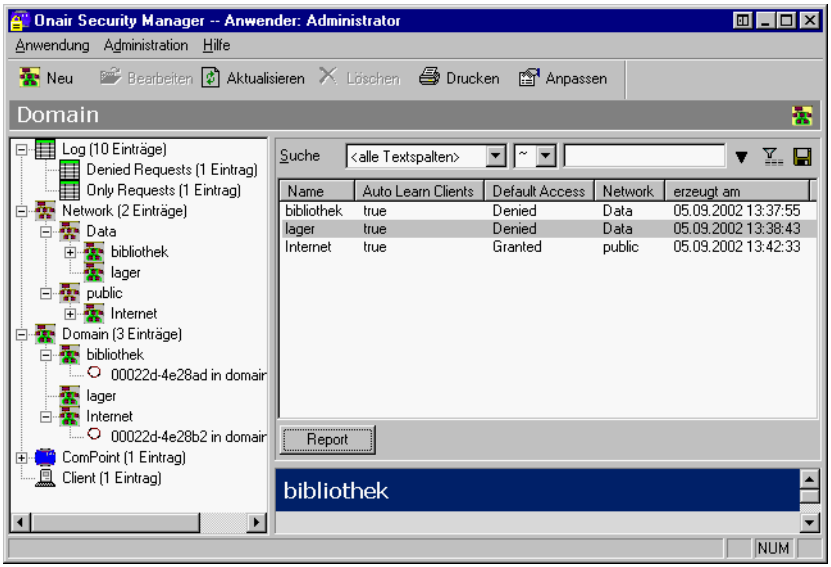

Jetzt können Sie die Werte der Attribute *Access*, *FromDate* und *ToDate* ändern.

## *Reports generieren*

Um die gesamte Struktur Ihres Netzes darzustellen, können Sie einen Report generieren. Dadurch lassen sich sämtliche Clientzugriffe auf ComPoints mit den dazu gehörigen Zeitpunkten und Zugangsberechtigungen protokollieren.

Benutzt wird die Quelldatei *secreport.rtf*, die im Rich Text Format vorliegt. Der Report wird anschließend in die Zieldatei *secreportout.rtf* geschrieben, die ebenfalls im Rich Text Format vorliegt.

Jeder generierte Report besitzt immer ein Bezugsobjekt oder eine Liste von Bezugsobjekten.
Um die Struktur des gesamten Netzes darzustellen, müssen Sie in die Listenansicht von *Domain* umschalten:

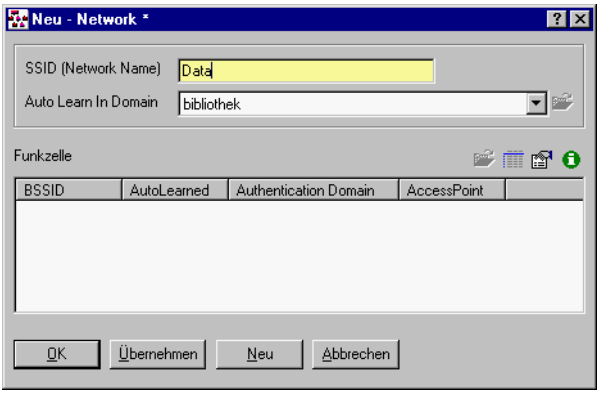



Wenn Sie die Schaltfläche *Report* betätigen, wird die Datei *secreportout.rtf* vom Microsoft Word geöffnet.

# Beschreibung der Anwendungsdialoge

## Network

Im Gegensatz zu einem über Ethernet eingerichteten LAN verfügt ein Wireless LAN nicht über Kabelstränge, mit denen eine feste Verbindung zwischen Server und Clients hergestellt wird. Daher gibt es in jedem Funknetz einen Parameter, der das Netz eindeutig kennzeichnet. Nur Clients, deren Netzwerk-Konfiguration mit der des ComPoints übereinstimmt, können in diesem Wireless LAN (WLAN) kommunizieren. Das Netzwerk wird durch einen Netzwerkname (Network Name), die sogenannte SSID identifiziert.




- **SSID (Network Name)**
  Die SSID ist die Netzwerk-Identifizierung in einem WLAN. Nur Clients, die in ihrer Netzwerk-Konfiguration diesen Wert eingetragen haben, können in diesem WLAN kommunizieren.
- **AutoLearn In Domain**
  Dieser Wert beinhaltet die Domain, in der die Information über neu gelernte Funkzellen gespeichert werden soll.

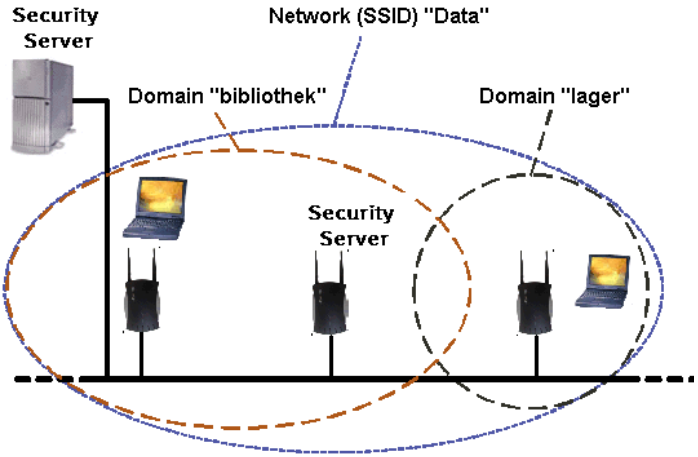
**Funkzelle**

In jedem ComPoint befinden sich eine oder zwei Funkkarten, die Funkzelle bilden. Diese Funkkarten sind durch ihre eindeutige MAC-Adresse identifizierbar.

### *Einrichten von Domains in Netzwerken*

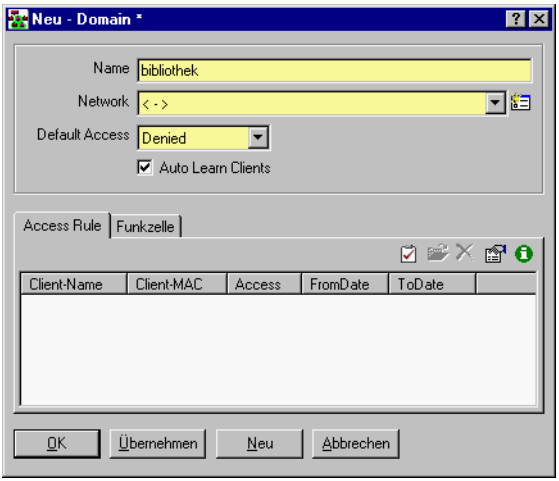
Für jedes Netz kann eine Security Domain definiert werden. Eine Domain kann wie ein Subnetz betrachtet werden. Man kann in einem Netz mehrere Domains mit gleichem Netzwerknamen definieren, um Subnetze mit unterschiedlichen Zugriffsregeln abzubilden. Im folgenden Beispiel gibt es ein Funknetz "Data", mit zwei Domains: "Bibliothek" und "Besprechungsraum".

In der "Bibliothek" dürfen z.B. alle Clients Zugang bekommen, während im "Besprechungsraum" nur ausgewählte Clients Zugang haben.




Für jedes Netz gibt es zwei Parameter, die als Default Einträge die Werte bekommen, die in den gleichnamigen Systemparametern enthalten sind.

Es ist auch möglich netzspezifische Werte zu definieren, die nur in diesem Netz gültig sind.




Die Parameter des Dialoges werden im folgenden erläutert:

- **Name**
  Name der Security Domain.
- **Network**
  Netzwerkname, so wie er im ComPoint eingetragen ist.
- **Default Access**
  Gibt an, wie sich das Netz verhält, wenn ein neuer Client gelernt wird. Er kann gleich eine gültige Zugangsberechtigung erhalten (Default Access = "Granted") oder alternativ nur gelernt werden, ohne Zugang zu erhalten (Default Access = "Denied").

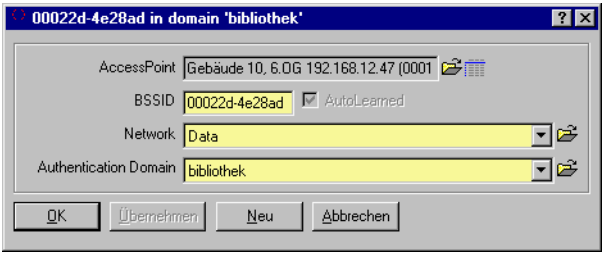
  Der Wert "Granted" bietet sich an, wenn der Security Manager neu eingerichtet wurde. Damit ist eine Überwachung des Netzes möglich, ohne den Betrieb zu stören. Wenn alle Clients gelernt wurden, kann auf "Denied" umgestellt werden. Neue Clients müssen dann vom Systemadministrator manuell freigegeben werden.
- **Auto Learn Clients**
  Gibt an, ob die Clients automatisch oder manuell gelernt werden.

### Register Access Rule

Diese Tabelle zeigt die Zugangsberechtigungen der im Netz angemeldeten Clients an. Durch Anklicken der Spaltenüberschriften kann die Tabelle sortiert werden. Einzelne Spalten lassen sich durch Verschieben der Trennstriche mit der Maus vergrößern und verkleinern.

### Register Funkzelle

In jedem ComPoint befinden sich eine oder zwei Funkkarten, die die Funkzelle bilden. Diese Funkkarten sind durch ihre eindeutige MAC-Adresse identifizierbar.

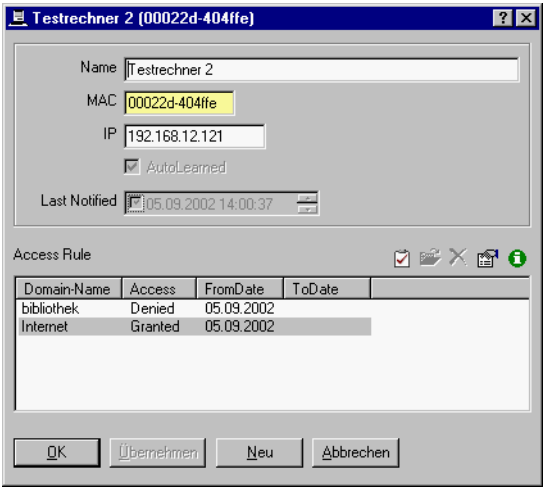



Die Parameter des Dialoges werden im folgenden erläutert:

- **ComPoint**
  Name (sofern angegeben) IP-Adresse und MAC-Adresse des entsprechenden ComPoints.
- **BSSID**
  MAC-Adresse der Funkzelle, in dem Standard IEEE802.11 auch als Basis Service Set Identification bezeichnet.
- **Network**
  Enthält die Zuordnung von ComPoints zu Netzwerken. Diese wird automatisch generiert, kann aber auch manuell geändert werden.
- **Security Domain**
  Gibt an, in welcher Domain sich diese Funkzelle befindet. Durch Änderung dieses Wertes können Sie entscheiden, in welchem logischen Netz (Security Domain) sich dieser ComPoint bzw. diese Funkzelle anmelden soll.

## *Client*

Über diesen Dialog können Sie Parameter für den Client definieren, um den Client zum Beispiel einfacher in Ihrem WLAN zu identifizieren.




Die Parameter des Dialoges werden im folgenden erläutert:

- **Name**
  Um die Clients besser zu identifizieren, können Sie ihnen einen Namen zuordnen.
- **MAC**
  Enthält die eindeutige MAC-Adresse des Clients.
- **IP**
  Ist die IP-Adresse dieses Clients. Diese wird nicht automatisch gelernt und kann wie der Name frei eingetragen werden.
- **AutoLearned**
  Die Clients können je nach dem Wert des Systemparameters *AutoLearnClients* automatisch (AutoLearnClients = Checkbox mit Haken) oder manuell (AutoLearnClients = Checkbox ohne Haken) gelernt werden.

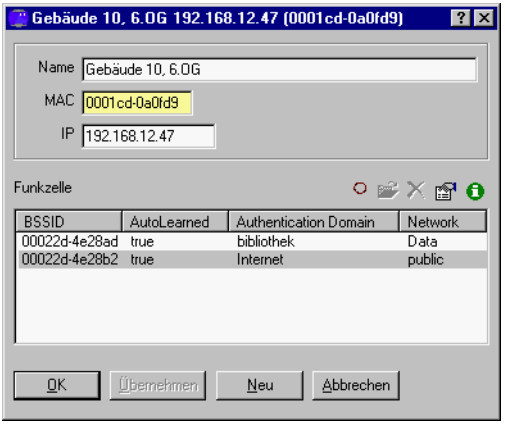
- **Last Notified**
  Gibt an, wann die letzte E-Mail Notification für diesem Client an den Admin gesendet wurde.

### Access Rule

Diese Tabelle dient zur Darstellung der verbundenen Elemente der Access Rule. Die Tabelle darf auch leer bleiben. Durch Anklicken der Spaltenüberschriften kann die Tabelle sortiert werden. Einzelne Spalten lassen sich durch Bewegen der Trennstriche vergrößern und verkleinern.

## *ComPoint*

Über diesen Dialog können Sie Parameter für den ComPoint definieren.




Die Parameter des Dialoges werden im folgenden erläutert:

- **Name**
  Name des ComPoint, so wie er im ComPoint Manager eingetragen ist.
- **MAC**
  Die MAC-Adresse des ComPoints. Sie wird automatisch gelernt.
- **IP**
  Die IP-Adresse des ComPoints. Sie wird automatisch gelernt.

### Funkzelle

Diese Tabelle dient zur Darstellung der verbundenen Elemente der Funkzelle. Die Tabelle darf auch leer bleiben.

Durch Anklicken der Spaltenüberschriften kann die Tabelle sortiert werden. Einzelne Spalten lassen sich durch Bewegen der Trennstriche vergrößern und verkleinern.

### *Access Rule*

In dieser Tabelle sind alle Zugangsrechte in Form eines logischen Wertes für Client/Netzwerk eingetragen.


Die Parameter des Dialoges werden im folgenden erläutert:

- **Domain**
  Wählen Sie aus der Liste ein Element von Network aus, das mit diesem Access Rule Element verbunden sein soll. Es muss genau ein Element ausgewählt werden.
- **Client**
  Dieses Eingabefeld dient dem Herstellen einer Verbindung zum Client. Sie können auch ein Element aus der Liste wählen. Es muss genau ein Element ausgewählt werden.
- **Access**
  Dieser logische Wert beschreibt die Netzzugangserlaubnis für Netzwerk/Client. Er hat einen eindeutigen Wert.
- **FromDate**
  Gibt an, ab wann sich ein Client im Netz anmelden darf.
- **ToDate**
  Gibt an, bis wann sich ein Client in diesem Netz anmelden darf.

### *Access Code*

Wenn ein Client versucht, sich über einen ComPoint in einem Netz anzumelden, startet dieser ComPoint eine Anfrage an den Datenbankserver.

Diese Anfrage enthält folgende Informationen: MAC-Adresse des Clients, MAC-Adresse der Funkzelle und die SSID (Name des Netzes). Die AccessCode Tabelle enthält die Liste der möglichen Antworten, die der Administrator vom Server erhalten kann, wenn ein Client versucht, sich in einem Netz anzumelden.

In der folgenden Tabelle werden Ihnen die Werte näher erklärt:

| Wert | Bedeutung |
|---|---|
| 0 | Ein interner (Kommunikations-) Fehler ist aufgetreten. |
| 1 | Alles OK, d.h. dass der Client sich in diesem Netz anmelden darf. |
| 2 | Netzname (SSID) ist nicht bekannt (dieser Eintrag existiert nicht in der Datenbank). Damit sich ein Client anmelden kann, muss der Netzname vom Administrator eingetragen sein. |
| 3 | Die Funkzelle enthält eine ungültige MAC-Adresse (diese muss eindeutig sein). |
| 4 | Der Client enthält eine ungültige MAC-Adresse (diese muss eindeutig sein). |
| 5 | Die Funkzellen können bei der ersten Anfrage automatisch gelernt werden, wenn vom Administrator der Systemparameter *AutoLearnCells* durch einen Haken in der Checkbox gesetzt ist. Falls die Checkbox des Systemparameters *AutoLearnCells* ohne Haken ist, wird diese Fehlermeldung (AccessCode) ausgegeben. |
| 6 | Für diesen Client ist eine Zugriffsregel über diese Funkzelle in einem Netz definiert (aber mit dem Wert "false"). |

| Wert | Bedeutung |
|---|---|
| 7 | Für diesen Client ist eine Zugriffsregel über diese Funkzelle in einem Netz definiert, aber das Datum liegt nicht in dem erlaubten Bereich, d.h. der Zugriff ist ab einem späteren Zeitpunkt erlaubt. |
| 8 | Wenn der Systemparameter *AutoLearnClients* vom Administrator durch einen Haken in der Checkbox gesetzt ist, können die Clients bei der ersten Anfrage automatisch gelernt werden. Falls die Checkbox des Systemparameters *AutoLearnClients* ohne Haken ist, wird diese Fehlermeldung (AccessCode) ausgegeben. |
| 9 | Für diesen Client ist eine Zugriffsregel über diese Funkzelle in einem Netz definiert, aber das Datum liegt nicht mehr in dem erlaubten Bereich, d.h. die Zugriffszeit ist abgelaufen. |
| 10 | Der ComPoint enthält eine ungültige MAC-Adresse (diese muss eindeutig sein). |
| 11 | Ihre Softwarelizenz ist ungültig. |
| 12 | System error 12. |
| 13 | System error 13. |
| 14 | System error 14. |
| 15 | Die lokalen MAC-Adressen des Clients können nicht automatisch gelernt werden. |

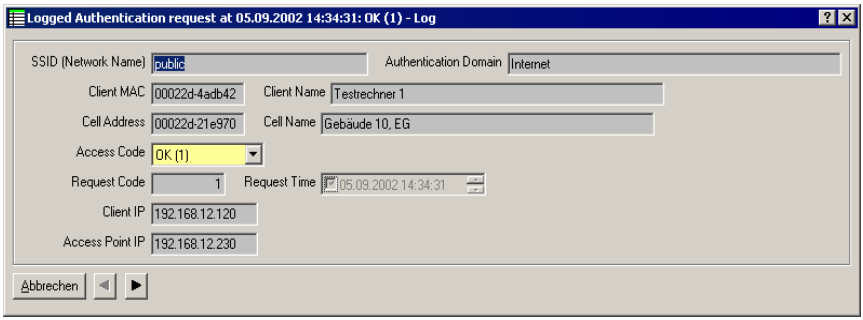
Die Parameter des Dialoges werden im folgenden erläutert:

- **Code**
  Der Code ist die Antwort der Datenbank. Er beschreibt, ob sich ein Client anmelden konnte, oder falls nicht, aus welchem Grund.
- **Beschreibung**
  Das ist eine kurze Beschreibung des AccessCodes.

## *Log*

Diese Tabelle enthält alle Anfragen, die in einem bestimmten Zeitraum vom ComPoint gestartet wurden sind, und deren Antworten mit dem entsprechendem AccessCode vom Datenbankserver. Die Anfragen sind enthalten Client MAC-Adresse, Funkzellen MAC-Adresse (BSSID) und Netzname (SSID). Die Daten in dieser Tabelle können zu einer bestimmten Uhrzeit - LogTime - in eine Datei geschrieben werden, wenn der Systemparameter *SaveLog* durch einen Haken in der Checkbox aktiviert wurde. Falls er nicht aktiviert wurde (Checkbox des Systemparameter *SaveLog ohne Haken)*, werden nur die Daten der letzten x Tage angezeigt, wobei x durch den Systemparameter *LogWindow* festgelegt ist.

Alle drei Systemparameter sind nur vom Administrator editierbar.




Die Parameter des Dialoges werden im folgenden erläutert:

- **SSID (Network Name)**
  Entspricht dem Name des Funknetzes, der SSID.
- **Security Domain**
  Gibt die Domain an, in der sich der Client über den ComPoint angemeldet hat.
- **Client MAC**
  Die MAC-Adresse des Clients.

- **Client Name**
  Der vom Systemadministrator vergebene Client Name.
- **Cell Address**
  Die MAC-Adresse der Funkzelle (BSSID).
- **Cell Name**
  Der Cell Name entspricht dem Namen des entsprechenden ComPoints.
- **Access Code**
  Die Access Codes geben Aufschluss über den Status der Anfrage.
- **Request Code**
  Der Request Code signalisiert, um was für eine Anfrage es sich handelt. War es eine Synchronisationsanfrage (RequestCode=2) oder eine Erstanmeldungsanfrage (RequestCode=1)? Wird dieser Wert in einer Filter-Bedingung benutzt, kann man nur die Erstanfragen sehen.
- **Request Time**
  Startzeitpunkt der Anfrage.
- **Client IP**
  Die IP-Adresse des Client.
- **ComPoint IP**
  Die IP-Adresse des ComPoint.

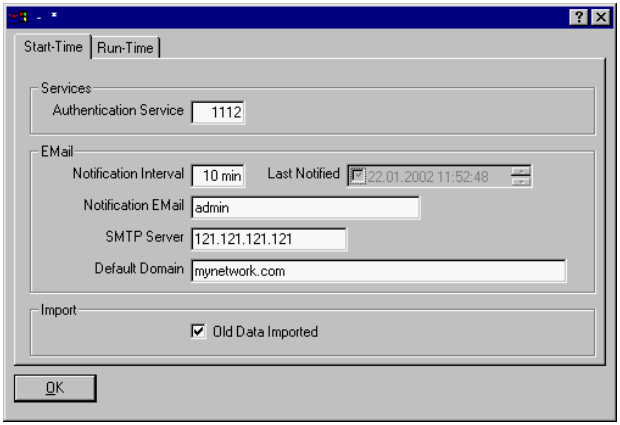
**Einstellungen der Log Tabelle:**

- **Log Window**
  Durch die Einstellung dieses Attributes wird die Anzahl der Tage festgelegt, deren Anfragen in der Log Tabelle dargestellt werden.
- **Log Time**
  Mit dem Wert können Sie einstellen, zu welcher Uhrzeit die Log Tabelle in eine Datei geschrieben werden soll. Diese Datei wird im aktuellen (Server) Verzeichnis gespeichert unter dem Namen: SECMGR-jjjj-mm-tt.log
- **Save Log**
  Durch den Wert dieses Attributes können Sie auswählen, ob eine Log Datei erstellt werden soll.

## *System Parameter*

Mit Hilfe folgender Parameter können Sie das Verhalten des Systems (des Netzes) beeinflussen. Diese Parameter sind auf zwei Registern verteilt, abhängig davon, wann Ihre vorgenommenen Änderungen wirksam werden.

Die Werte im Register *Start-Time* werden erst nach einem Neustart des Servers aktualisiert.




Die Parameter des Dialoges werden im folgenden erläutert:

### Services

- **Authentication Service**
  Gibt die Portnummer an, über die die Kommunikation mit dem ComPoint abläuft.

### Mail Notification Settings

Bei jeder Anfrage, die kein OK zurückliefert, wird eine E-Mail an dem Systemadministrator geschickt.

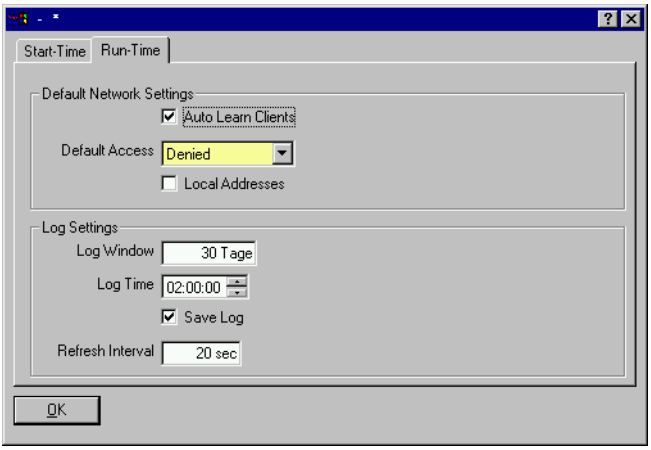
- **Notification Interval**
  Um zu vermeiden, dass zu viele E-Mails an den Administrator geschickt werden, können Sie die Mindestzeit zwischen zwei Notifications des selben Clients einstellen.

- **Last Notified**
  Gibt an, wann die letzte Notification eines unbekannten Clients gesendet wurde.
- **Notification E-Mail**
  Wenn der Systemadministrator über fehlgeschlagene Anmeldungen benachrichtigt werden soll, müssen hier die entsprechenden Mail-Parameter eingetragen werden.
- **SMTP Server**
  Die IP-Adresse des SMTP Servers.
- **Default Domain**
  Name der Domain, der für die E-Mail Adresse verwendet wird.

### Import

- **Old Data Imported**
  Gibt an, ob schon eine Datenbank aus einer ACL Version 1.x importiert wurde. Deaktivieren Sie das Häkchen in der Checkbox, wenn Sie eine Datenbank importieren möchten. Siehe auch Datenimport aus Version 1.x.

Die Werte im Register *Run-Time* werden ohne Neustart des Servers aktualisiert.




Die Parameter des Dialoges werden im folgenden erläutert:

### Default Network Settings

- **Auto Learn Clients**
  Dieser Systemparameter gibt das Verhalten des Netzes bei einer neuen Anfrage an und ist nur vom Administrator änderbar. Sollen die Clients automatisch gelernt werden, dann muss die Checkbox mit einem Haken markiert sein. Sollen sie manuell eingetragen werden, dann ist die Checkbox ohne Haken.
- **Default Access**
  Wenn ein neuer Client sich anmeldet, wird er in die Datenbank aufgenommen, ohne dass er gleich eine Zugangsberechtigung in diesem Netz hat, falls dieser Wert "Denied" ist. Falls dieser Wert "Granted" ist, wird eine Access Rule mit dem Wert "Granted" erstellt.

- **Local Addresses**
  Der Security Manager unterscheidet zwischen einer lokal verwalteten MAC-Adresse und der vom Hersteller vergebenen MAC-Adresse des Clients. Wenn die lokalen Adressen nicht unterstützt werden sollen (die Checkbox vor *Local Addresses* ist ohne Haken), dann werden diese Clients auch nicht automatisch gelernt und in die Datenbank eingetragen. Ist die Checkbox vor *Local Addresses* durch einen Haken markiert, wird dieser Client normal behandelt.

### Log Table Settings

- **Save Log**
  Gibt an, ob eine Log Datei erwünscht ist ("true" oder "false").
- **Log Window**
  Gibt in Tagen an, in welchem Zeitfenster Anfragen angezeigt werden sollen.
- **Log Time**
  Gibt an, zu welcher Uhrzeit die Log Datei ausgeschrieben werden soll.
- **Refresh Interval**
  Wie oft muss das Log-Fenster automatisch aktualisiert werden? Falls dieses Attribut den Wert "o sec" hat, wird das Log-Fenster nicht automatisch aktualisiert, sondern muss vom Benutzer durch Drücken der ‹F5› Taste oder durch Klicken auf die Schaltfläche *Aktualisieren* durchgeführt werden.

# Index

## E



## F



## I



## K



## L



## M

## N



## O



## P



## Q



## R



## S

## T



## V



## W



## Z



## Numerics