TAF

August 2000

TAF

REFERENCE

1 Token Authentication Firewall (TAF)

In this chapter we will cover the configuration of TAF (Token Authentication Firewall).

We place emphasis on the configuration of the BinTec router as ACE/Agent using the Setup Tool, describing the TAF client, PC configuration and all related steps in setting up TAF.

1.1 Overview

Token Authentication Firewall (TAF) is an advanced feature for controlling access to central site computing resources that goes beyond the theoretical limitations of existing security mechanisms. TAF is a user-oriented security system, which affords human interaction and by that grants that an authorized user is sitting in front of the remote host, which is connected to the central site. TAF can only be used to control IP traffic.

TAF login user verification is based on the established and well-respected Token-Card-ACE/Server solution provided by Security Dynamics.

You will need a special TAF license to use TAF on your BinTec router. Along with this license you will get 10 TAF Login licenses for PCs you wish to use as TAF clients.

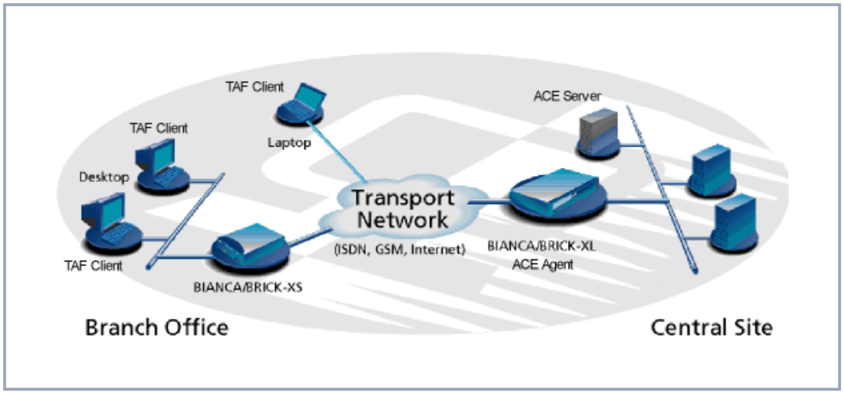


Figure A-1: TAF Clients, ACE Agent and ACE Server

A security solution using TAF is made up of four components:

- an ACE/Agent by BinTec (BRICK-XL2, BRICK-XM with 2 MB flash or BRICK-XMP) in the central site
- an ACE/Server by Security Dynamics in the central site
- a Token Card by Security Dynamics for the user of the TAF client PC
- an application for the TAF client PC by BinTec (Windows 3.x, Windows 95/ 98 and Windows NT)

In this TAF security solution the BinTec router as an ACE/Agent answers login attempts from a TAF client with a request for authentication. It then sends the user's response to the ACE/Server for verification. On the other hand, the BinTec router verifies the authenticity of the ACE/Server so that no other server can masquerade as an ACE/Server with the intention to acquire security data. Above that the BinTec router encrypts and decrypts messages between the TAF client and the ACE/Server.

You must bear in mind that TAF can only authenticate IP connections.

1.1.1 Requirements

As a requirement for the TAF authentication procedure, the four components (as mentioned above) must be established. Based on an existing WAN partner connection (Remote Client – LAN, LAN – LAN), the following conditions must be provided:

- In the central site LAN an ACE Server must be set up and the central site's BinTec router must be configured as an ACE/Agent to serve as remote access server to the central site's LAN.
- The client side PC must have installed and configured the TAF login program and its user must be in possession of the Token Card, which generates one part of the password for the TAF login.

Figure A-2: Token Card

1.1.2 Authentication

User authentication by the ACE/Server uses a "two factor" user authentication, i.e. the password consists of a static PIN, which is secret and memorized by the user and of a second part, which is generated by the user's token card.

1.1.3 Encryption

Additionally two different encryption methods are used:

- For the communication between ACE/Server and ACE/Agent (the BinTec router of the central site) Node Secret, a string of pseudorandom data known only to the client (ACE/Agent) and the ACE/Server, is combined with other data to encrypt client/server communications.
- For the communication between TAF client and ACE/Agent the BinTec router generates a pair of keys (private key and public key), where the private key stays on the BinTec router (ACE/Agent) and the public key is sent to the TAF client. By the help of these keys the transmission of authentication data is encrypted and the TAF client also uses them to check the identity of the central site.

1.2 Configuration of TAF

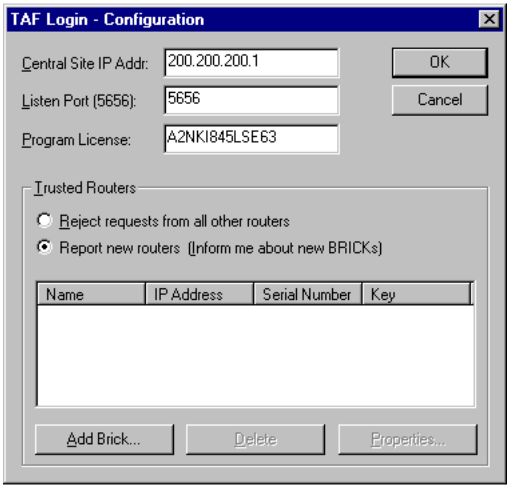
1.2.1 Configuring the ACE/Server

The following steps require that you have already installed an ACE/Server in your network. For instructions on how to install and configure the ACE/Server, please refer to its manuals.

Please note that the ACE/Server configuration described in this document refers to ACE/Server Version 3.01.

On the ACE/Server you first have to configure the BinTec router to act as a gateway for the TAF-protected network, and then you have to configure each user who will be authenticated.

➤ Go to the **Client** menu of your Server administration tool and select **Add Client.**



Central Site IP Addr: 200.200.200.1

Listen Port (5656): 5656

Program License: A2NKI845LSE63

Trusted Routers

○ Reject requests from all other routers

● Report new routers (Inform me about new BRICKs)

Name	IP Address	Serial Number	Key

Figure A-3: ACE/Server (Windows NT): Add Client

Now enter the name and network (IP) address of the BinTec router, select Communication Server as the client type, and select the encryption type based on the client device configuration.

Please note that the same encryption type must also be configured on the BinTec router.

If you want to modify ACE/Server system settings under Unix – e.g. the port to use for communication with the BinTec router (default: 5500) – you can use the `sdsetup -config` command. In most cases no changes are necessary.

When the server receives the first authentication request from the BinTec router, it will send a Node Secret, which is subsequently used to encode the messages exchanged between the ACE/Server and the BinTec router.

The Sent Node Secret checkbox should not be selected. Once the Node Secret has been sent the corresponding checkbox in the dialog shown earlier will appear selected (for detailed information see “Node Secret” in table A-3, page 17).

You can find a detailed description of this dialog box and related configuration steps in the ACE/Server Administration Manual.

- If you have not already done so, you now have to import the Token Card information into your ACE/Server (see ACE/Server Administration Manual).
- You should then enable the Token Cards, and synchronize them with the server.
- You can now start adding users (TAF clients). For each user you have to enter his first and last name, login name, whether he will be allowed or required to create his own PIN and some other items.
  The final step is to assign a Token Card to the user.

  After you have entered all users the server configuration is complete (for TAF purposes).

As already mentioned earlier, we recommend referring to the ACE/Server’s manuals for detailed information on the configuration of the ACE/Server.

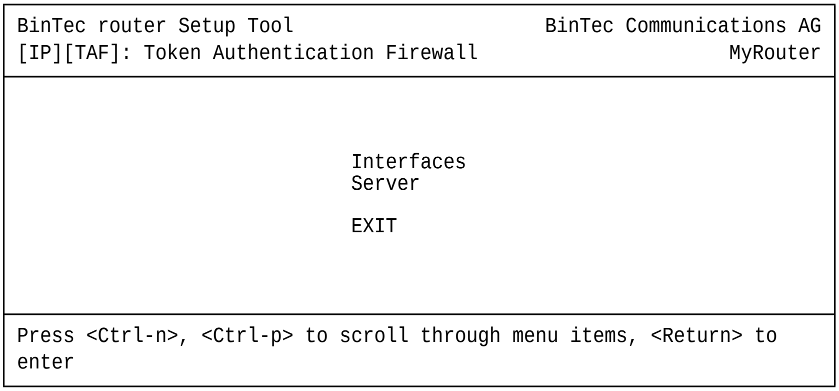
1.2.2 Configuring the BinTec router (ACE/Agent)

In the following the TAF configuration of the BinTec router is described in detail.

The first part introduces the Setup Tool menus dealing with TAF and in a second part the necessary configuration steps are listed.

Setup Tool Menus

- Go to ***IP*** ➧ ***TOKEN AUTHENTICATION FIREWALL***
  This menu consists of two submenus where Token Authentication Firewall relevant settings are configured.



```
BinTec router Setup Tool                      BinTec Communications AG
[IP][TAF]: Token Authentication Firewall                      MyRouter



                             Interfaces
                             Server

                             EXIT



Press <Ctrl-n>, <Ctrl-p> to scroll through menu items, <Return> to
enter
```

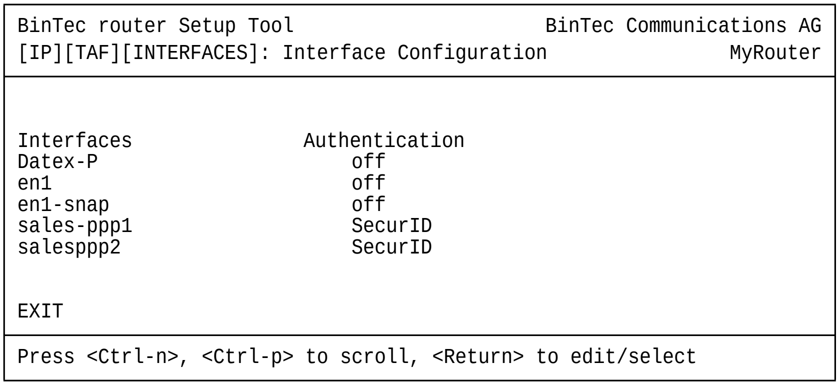
Field	Meaning
Interfaces	used to enable/disable SecurID support separately for each BinTec router interface.
Server	used for configuring SecurID Server relevant settings on the BinTec router. These settings must correspond to the parameters configured on the ACE/Server.

TABLE A-1: TOKEN AUTHENTICATION FIREWALL

Configuring Interfaces

➤ Go to ***INTERFACES***.
This menu lists the BinTec router interfaces that may be configured for Token Authentication Firewall support. TAF can only be used on interfaces which have been explicitly enabled for use with SecurID.

Typically, the SecurID Server (ACE/Server) is accessible via the BinTec router's LAN interface. Authentication for this interface should be set to *off*. Dial-Up interfaces used for accepting secure connections from TAF clients must be set to *SecurID*.



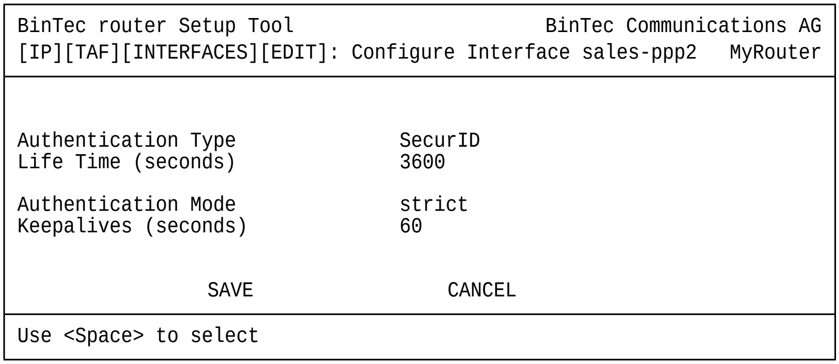
```
BinTec router Setup Tool                             BinTec Communications AG
[IP][TAF][INTERFACES]: Interface Configuration                       MyRouter


Interfaces                  Authentication
Datex-P                         off
en1                             off
en1-snap                        off
sales-ppp1                      SecurID
salesppp2                       SecurID


EXIT

Press <Ctrl-n>, <Ctrl-p> to scroll, <Return> to edit/select
```

By default, Authentication is disabled (set to *off*) for existing BinTec router interfaces.

- ➤ To enable TAF support for an interface, select the interface and press the **Enter** key. In the resulting menu ensure that Authentication is set to *SecurID* and select **SAVE.**

Configuring Interface-Specific Settings

- ➤ ***EDIT***
  To configure interface-specific settings for Token Authentication Firewall.



```
BinTec router Setup Tool                             BinTec Communications AG
[IP][TAF][INTERFACES][EDIT]: Configure Interface sales-ppp2   MyRouter


Authentication Type                 SecurID
Life Time (seconds)                 3600

Authentication Mode                 strict
Keepalives (seconds)                60


                 SAVE                    CANCEL

Use <Space> to select
```

Field	Meaning
Authentication Type	This field is used to enable/disable TAF for the respective interface. By default Authentication Type is disabled (*off*). Setting to *SecurID* enables TAF for the interface.
Life Time (seconds)	The time in seconds allows data traffic on this connection. 180 seconds before the Life Time expires a new passcode is requested. Possible Values: 180 - 3600 Default Value: 3600
Authentication Mode	The authentication policy used by the ACE/ Server. If set to *strict* each source IP address must be authenticated separately. If set to *loose* all source IP addresses are allowed if at least one IP address was successfully authenticated on this interface. Default value: *strict*
Keepalives (seconds)	The interval in seconds after which a new keep-alive request is sent to the BinTec router by the ACE/Server. Keepalive packets will never cause a new connection to be set up, nor will they affect the shorthold mechanism.

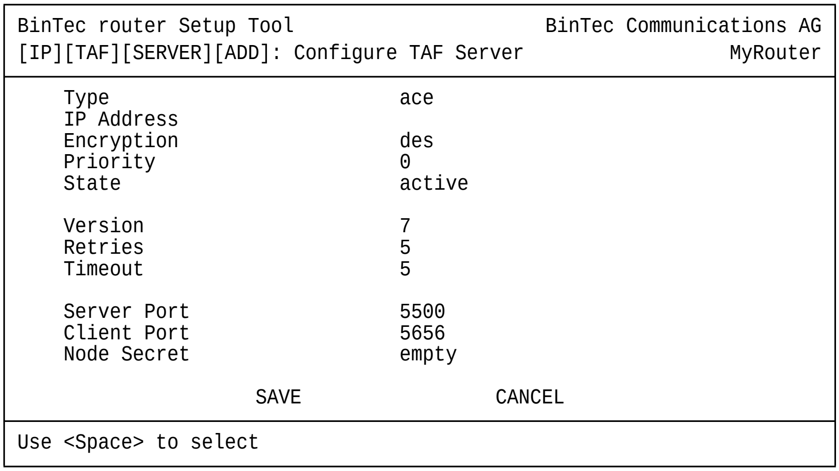
Table A-2: ***CONFIGURE INTERFACE***

Configuring TAF Servers

- Go to ***SERVER***
  This menu contains a list of the TAF servers currently configured. At the moment up to two active ACE/Servers (Master and Slave server) are supported.

By choosing **ADD** or **EDIT** you will get to the following menu, which contains the BinTec router settings relevant to the configuration of the SecurID server (ACE/ Server). The settings here must correspond to the values used by the ACE/ Server.

Under Unix the parameters to use here can easily be retrieved from the ACE/Server with the included sdinfo program. Refer to your ACE/Server documentation for information.



```
BinTec router Setup Tool                          BinTec Communications AG
[IP][TAF][SERVER][ADD]: Configure TAF Server                      MyRouter

    Type                             ace
    IP Address
    Encryption                       des
    Priority                         0
    State                            active

    Version                          7
    Retries                          5
    Timeout                          5

    Server Port                      5500
    Client Port                      5656
    Node Secret                      empty

                     SAVE                     CANCEL

Use <Space> to select
```

Field	Meaning
Type	The type of authentication server. Currently *ace* (ACE/Server) is the only type supported.
IP Address	The IP address of the authentication server.
Encryption	Specifies the type of encryption to use when communicating with the authentication server. For ACE/Servers this can currently be either *des* (Data Encryption Standard) or *sdi* (Security Dynamics proprietary) encryption. Default value is *des*.
Priority	The authentication server with the lowest priority value is the first used for requests. Use the value *0* for the master server and the value *1* for the slave server.
State	Either *active* or *disabled.*
Version	The file version number used by the authentication server. Default value is 7.
Retries	This is the number of times the BinTec router will attempt to connect to the authentication server before reporting a connection failure. Valid range is 1 through 6.
Timeout	The time in seconds to wait for a reply from the authentication server before retrying. Valid range is 1 through 20. Default value is *5.*
Server Port	The port number to use for communication between the BinTec router and the authentication server. By default port *5500* is used.

Field	Meaning
Client Port	The port number to use for communication with TAF Clients. Default port is *5656*.
Node Secret	Indicates whether the Node Secret has already been received by the BinTec router (*received*) or not (*empty*). The node secret is automatically generated by the ACE/Server and then transmitted to the BinTec router. It is a password used to encode messages between the BinTec router (ACE/Agent) and the ACE/Server. Usually the node secret is initially sent by the ACE/Server and after that the **Sent Node Secret** checkbox on the ACE/Server is automatically selected. See "Configuring the ACE/Server" in section A, chapter 1.2.1, page 9. You can use RESET NODE SECRET to momentarily clear the Node Secret on the BRICK. When the **Sent Node Secret** checkbox on the ACE/Server is cleared, the ACE/Server will transmit a new Node Secret at the next communication. Whenever the BRICK receives a new Node Secret form the ACE/Server, the **tafServerTable**, where the Node Secret is stored, is saved to the flash ROM.

Table A-3: ***CONFIGURE TAF SERVER***

TAF Commands on the BinTec router

Command	Meaning/Tab
`makekey [-g]`	The makekey command can be used to show the current public key (stored on the **biboAdmPublicKey** variable), or – when invoked with the `-g` option – to generate a new pair of keys (public and private). You will only need to use `makekey -g` once before configuring TAF for a WAN partner for the first time.
`shtaf`	The `shtaf` command can be used to test the TAF authentication procedure. The BinTec router will prompt you for an ACE/Server user name and a passcode (the Token currently displayed on this user's Token Card). If the authentication was successful, it will give you a normal BinTec router login prompt. After logging in to the BinTec router you can terminate `shtaf` by typing `exit`.

Table A-4: TAF commands

Configuration of the BinTec router (ACE/Agent) via Setup Tool

We will assume that your BinTec router is up and running, and that a TAF license is available.

➤ Login to your BinTec router as the admin user and start the Setup Tool (`setup`).

➤ Go to the ***IP*** ➧ ***TAF*** ➧ ***SERVER*** menu and **ADD** a new Server.
First you have to add a main ACE/Server.
Enter the ACE/Server's name or IP address and select the same encryption as configured on the Server. Make sure to use the correct (Config File) Version, Retries, and Timeout settings (you can obtain a list of the important

Server settings under Unix by issuing the `sdinfo` command on your ACE/Server).
For normal applications it is advisable to use the default port setting (*5500*).
The Node Secret field is filled in automatically (table A-3, page 17).

➤ You can then, if necessary, add one slave server, which must be configured identically to the main server, only its Priority value must be set to *1* or higher (i.e. it gets a lower priority than the main server).
Exit the Setup Tool and execute the command `makekey -g` (table A-4, page 18). This will generate a pair of keys (public and private) which will be used to encode the authentication messages exchanged between the BinTec router and the user's PC.

These steps only have to be taken once.

At this point you should test your configuration by executing the `shtaf` (table A-4, page 18) command on your BinTec router. The BinTec router will then contact the main ACE/Server and request you to enter a user name and passcode for authentication.

When the respective TAF client is part of a LAN, the remote BinTec router, the gateway to the TAF client's LAN, must be configured as a WAN Partner. When you have TAF clients, which are single remote PCs (via modem or ISDN), then you have to create a WAN Partner entry for every PC that will be used to authenticate users.

For this WAN Partner only the IP protocol should be configured, because TAF can only authenticate IP packets. If you activate IPX or Bridging simultaneously, this traffic will not be verified by TAF.

- ➤ After you made sure the connection works, go to the ***IP*** ➧ ***TAF*** ➧ ***INTERFACES*** menu and select the interface you just created (interface name = WAN partner name).
  Switch **Authentication Type** to *SecurID*. Adjust the other three parameters if necessary for your application (for an explanation of the parameters please refer to table A-2, page 14).
- ➤ Repeat this procedure until all partners are configured.

System Logging Messages

Syslog messages are created during various events. TAF Syslog messages are reported on the BinTec router under the INET subsystem. The following messages may be seen in connection with Token Authentication Firewall and SecurID.

Message	Meaning	Level
TAF: new session for <IP addr> ifc <ifindex>		Debug
TAF: delete session for <IP addr>		Debug
TAF: set Authlifetime to <seconds> for <IP addr> ifc <ifindex>		Debug
TAF: allow auth packet from if <ifindex> prot <protocol> <IP addr> :<port>-><IP addr> :<port>		Debug
TAF: early request for ‹IP addr.> ifc <ifindex>		Info
TAF: life timer expired for <IP addr.> ifc <ifindex>		Info
Taf: mibio: ACE server <IP addr.> ignored - wrong Configuration	The named server was deactivated, because its configuration was different to the configuration of the Master Server.	Err

Message	Meaning	Level
`Taf: mibio: ACE server <IP addr.> ignored - too many masters`	Two Master Servers have the same priority; one of them was deactivated.	Err
`Taf: mibio: ACE server <IP addr.> ignored - too many slaves`	Two Slave Servers have the same priority; one of them was deactivated.	Err
`Taf: mibio: Saving tafServerTable to the flash ROM`	The **tafServerTable** was automatically saved to flash ROM after the Node Secret had been transmitted. All changes, made to this table are still existent after the next reboot.	Notice
`Taf: clienudp: Unable to create/bind ACE/Server socket - errno = …`		Err
`Taf: clienudp: Unable to locate ACE/Server host - errno = …`	There are no servers configured in the **tafServerTable**.	Err
`Taf: clienudp: Unable to send to the ACE/Server - errno = …`	Cannot send message to the ACE/Server; internal error.	Err
`Tafd: PC Message corrupted`	The message from the client was wrongly coded	Notice
`Tafd: decryption error 0x<type>`	The message from the client was wrongly coded	Err
`Tafd: encryption error 0x<type>`	The message from the client was wrongly coded	Err
`Tafd: no key for encryption`	You have to call `makekey -g` to generate a new key	Err
`Tafd: Request for token authentication ignored - no key available`	You have to call `makekey -g` to generate a new key.	Err
`Tafd: TAF server unreachable`	The ACE/Server is unreachable/does not answer/ is not working	Err
`Tafd: No TAF License`		Err

Message	Meaning	Level
`Tafd: Authentication result for <IP addr> ifc <ifindex>: <result>`		Info
`Tafd: Tafd: received <message type> Message from <IP addr> ifc <ifindex>`		Debug
`Tafd: Tafd: sent <message type> Message to <IP addr> ifc <ifindex>`		Debug

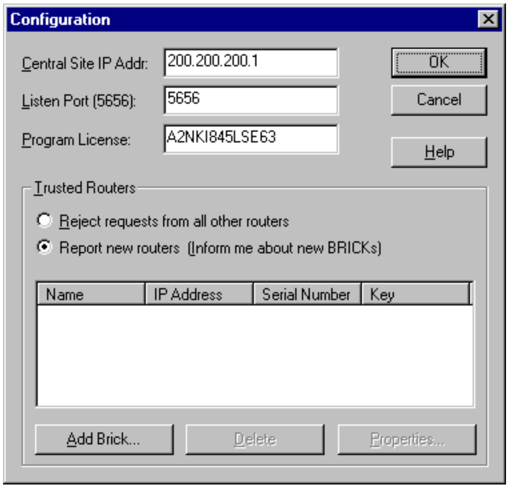
Table A-5: **biboAdmSyslogMessage**

1.2.3 Configuring the TAF Client PC

The TAF client application is a component of BinTec's BRICKware, which can be found on the BinTec ISDN Companion CD or can be downloaded from BinTec's Web Server at http://www.bintec.de (Section: Download). To reach the section Download, click Solutions & Products. You can install it together with BRICKware on the TAF client PC.

- If you want to use TAF Login from a PC, you must select **TAF Login** in the Components list during the installation of BRICKware for Windows. In case you already have installed other components of BRICKware and want to add TAF Login, we recommend reinstalling all components of BRICKware (including TAF).
- The TAF Login program will automatically be installed in your **Startup** menu (you may have to select this during installation). When the TAF Login is not automatically started after the installation is complete, you must select TAF Login from the BRICKware group in the **Start** menu.
- In the Login dialog box, you must select Configuration to configure the Login program. In this dialog, you enter the BinTec router's (ACE/Agent of the central site LAN) IP address and can modify the Listen Port if necessary (the listen port setting on the PC must be identical to the setting on the BinTec router). Above that you must initially enter the program's license key

for the TAF client, which is provided together with your BinTec router’s TAF license.



Configuration

Central Site IP Addr: 200.200.200.1

Listen Port (5656): 5656

Program License: A2NKI845LSE63

Trusted Routers

○ Reject requests from all other routers

● Report new routers (Inform me about new BRICKs)

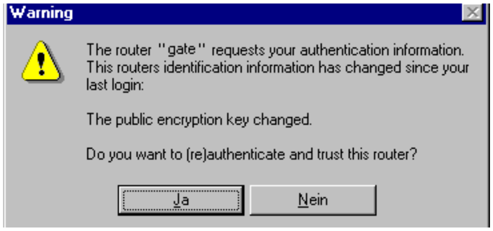
Name	IP Address	Serial Number	Key

Figure A-4: TAF Configuration

- Repeat this procedure on each PC you want to use for TAF authentication purposes. Each PC needs its own TAF client license.
- In the **Trusted Routers** group, you can select whether only to accept logins from trusted routers or also be notified when a router not contained in the trusted routers list below sends a login request. In the notification (shown below), you can then decide whether to trust the new router. Trusted routers are displayed in the list at the bottom of the Trusted Routers group.

Using TAF Login

The TAF Login program is added to the Autostart menu and will remain in the background until it receives an authentication request from the remote LAN.



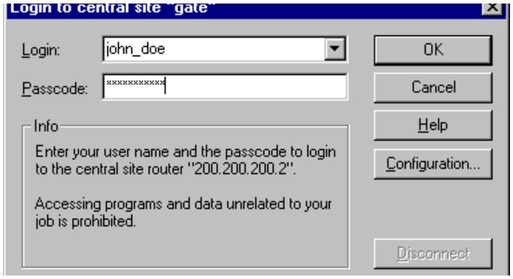
The router "gate" requests your authentication information. This routers identification information has changed since your last login:

The public encryption key changed.

Do you want to (re)authenticate and trust this router?

Figure A-5: Notification about the login request of a not-trusted router

- You can also activate the program by double-clicking on the TAF icon in the task bar or by starting it from the BRICKware program group to start the authentication procedure from your TAF client PC.



Login: john_doe

Passcode: ***********

Enter your user name and the passcode to login to the central site router "200.200.200.2".

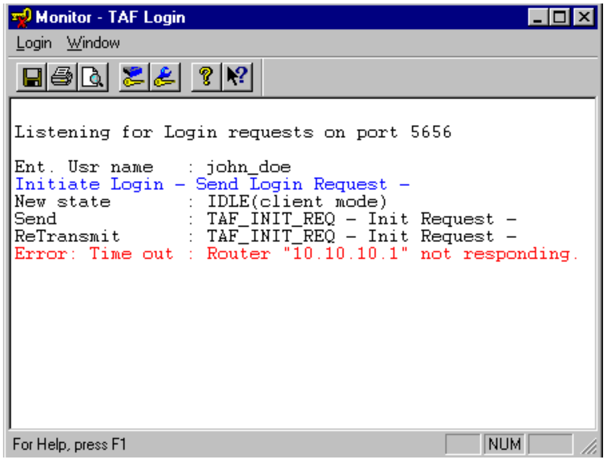
Accessing programs and data unrelated to your job is prohibited.

Figure A-6: TAF Login

- Enter your login name for the ACE/Server and the passcode displayed on your Token Card. Click **OK**.

  If the authentication was successful the TAF Login dialog will be closed and the TAF icon in the task bar will change to ✓ , if the authentication failed an error message is displayed, and the icon will remain ✗ .

- TAF Login also includes a monitoring function. If you right-click on the TAF icon, you will get a menu from which you can select **Show Monitor Window**.



```
Listening for Login requests on port 5656

Ent. Usr name     : john_doe
Initiate Login - Send Login Request -
New state         : IDLE(client mode)
Send              : TAF_INIT_REQ - Init Request -
ReTransmit        : TAF_INIT_REQ - Init Request -
Error: Time out : Router "10.10.10.1" not responding.
```

Figure A-7: TAF Monitor

All important activities concerning TAF are logged in this window. You can also initiate a login or configure the program from this window.