



R3000

8E6 AUTHENTICATOR

INSTALLATION NOTES

FOR VERSIONS 1.9.00 AND HIGHER

OCTOBER 30, 2006



Copyright © 2006 8e6 Technologies

8e6 Technologies
828 W. Taft Avenue
Orange, CA 92865
Phone: (714) 282-6111

This document contains confidential and proprietary information. All rights reserved. No part of this document may be reproduced or disclosed in any form without the written permission of 8e6 Technologies.

8e6 Technologies makes no warranties, expressed or implied, with respect to this documentation. The information contained herein is subject to change without notice. Revisions may be issued to advise of such changes.

Product names have been used only for identification, and may be trademarks of their respective companies.

INSTALLING THE 8E6 AUTHENTICATOR

About the 8e6 Authenticator

The 8e6 Authenticator ensures the end user is authenticated on his/her workstation, via an executable file that launches during the login process. To use this feature, the 8e6 Authenticator client (authenticat.exe) must be installed on the domain controller.

NOTE: The 8e6 Authenticator is available for use with R3000 software version 1.9.00 or later. The latest version of 8e6 Authenticator client (authenticat.exe) can be downloaded from http://www.8e6.com/products/R3000/patches/r3000_patches.htm.

OS Requirements

The 8e6 Authenticator client works with the following operating systems:

- Windows XP Pro SP1 and 2
- Windows 2000 Pro SP4
- Windows XP and Windows 2000 with Novell client v4.91

NOTE: Any non-domain supported Windows operating system, such as ME or XP Home Edition, will not work with the 8e6 Authenticator unless the Novell eDirectory client is installed for login and deployment of the 8e6 Authenticator client using a Novell server.

Work flow in a Windows environment

- 1 The administrator stores the 8e6 Authenticator client (authenticat.exe) in a network-shared location that a login script can access.
- 2 An end user logs on the domain from a Windows machine.
- 3 The end user's login script evokes authenticat.exe.
- 4 The 8e6 Authenticator client determines the authentication environment by examining the Windows registry, then retrieves the username and domain name using either Windows or Novell APIs, and sends this information (LOGON event) to the R3000.
- 5 The R3000 looks up the groups to which the end user belongs (Windows AD, PDC, or eDirectory through LDAP or NTLM/Samba), and determines the profile assignment.
- 6 The R3000 sets the profile for the end user with username (including the group name, if it is available) and IP.
- 7 The 8e6 Authenticator client continually sends a "heartbeat" to the R3000—with a specified interval of seconds between each "heartbeat"—until the end user logs off.

- 8 The end user logs off, and the 8e6 Authenticator client sends a LOGOFF event to the R3000. The R3000 removes the user's profile.

8e6 Authenticator configuration priority

The source and order in which parameters are received and override one another are described below.

NOTE: Any parameter set at the end of the list will override any parameter that was previously set.

- 1 **Compiled Defaults:** Given no parameters at all, the client will try to execute using the default compilation.
- 2 **Configuration File** (optional): The default location of the configuration file is the same path/name as the authenticat.exe client, but with a “.cfg” extension instead of “.exe”. The full path/name can be specified on the command line with the CF[] parameter. Review the ++ comment following Table 1 for more information.
- 3 **Command Line** (optional): Options on the command line will override compiled defaults and the configuration file. The command line can be left blank.
- 4 **R3000 Configuration Packet** (optional): The R3000 may send a configuration packet that will override all other settings, including the command line. If the R3000 changes the IP address or port used by authenticat.exe, then when authenticat.exe reconnects, authenticat.exe will use the new IP address and port.

NOTE: The R3000 can force authenticat.exe to reconnect with a re-logout event packet.

8e6 Authenticator configuration syntax

All configuration parameters, regardless of their source, will use the following format/syntax:

```
wAA[B]w{C}w  
{Parameter 'AA' with Data 'B', and Comment 'C' ignored.}
```

```
w;DD[E]w{C}w  
{The semicolon causes 'DD[E]' to be ignored, 'C' is also ignored.}
```

Whereas **'AA'** is a two-letter, case-insensitive parameter name, **'B'** is the value for this parameter wrapped in brackets ([]), and **'w'** is zero or more white spaces (space, tab, carriage return, line feed). **'C'** is completely ignored, and anything wrapped in braces ({ }) is considered a comment. A **';**' immediately preceding a parameter will cause that parameter and its data to be ignored, which is convenient for temporarily reverting a parameter to default values during testing.

Sample command line parameters

```
authenticat.exe LF[c:\] ra[192.168.0.43]Rr[40000]
```

Sample configuration file

```
RA[100.10.101.30] { R3000 Virtual IP address }  
RP[139] { R3000 Port }  
RH[30000] { Heartbeat timer (30 seconds) }  
RR[30000] { Reconnect time (before connecting again) }  
RC[10000] { Connect Timeout (how long to wait for a connection  
response) }  
LE[0]  
LF[\\100.10.101.117\publogs\] { Where to put logs }
```

Sample R3000 configuration update packet 'PCFG'

After decryption, with protocol headers removed:

```
RH[30000]RC[1000]LE[1]
```

You only need to change the options you do not wish to remain as default. Often the IP address of the R3000 (RA) and the log file (LF) are the most desired options to change. Note that full network paths are allowed.

Table of parameters

The following table contains the different parameters, their meanings, and possible values.

Param ID	Parameter Meaning	Values	Dbg Default	Release Default
UT +	User's Logon Environment	1-256 (0 = Win32, 1 = Novell)	255 (auto)	255 (auto)
RA # *	R3000 Virtual IP Address	255.255.255.255:PORT; ...	0.0.0.0	0.0.0.0
RV #	R3000 VPN Support Table	(IP-IP;IP:PORT;...),...		
RP	R3000 Port	1-65535	139	139
RH	R3000 Heartbeat Timer MS	1-4 billion (milliseconds)	30000	30000 (30 sec)
RR	R3000 Reconnect Time MS	1-4 billion (milliseconds)	30000	30000 (30 sec)
RC	R3000 Connect Timeout MS	1-4 billion (milliseconds)	10000	10000 (10 sec)
LE	Log using Event Viewer	1 or 0 (event view or log file)	0 (log file)	1 (event view)
LD	Logging Detail	1, 2, 3, or 4	1 (light)	0 (errors only)
LF *	Path-ONLY to output log file	1-1000 alphanum	C:\	C:\
CF ++	Full path/name of Config File	1-1000 alphanum	-	-

+ If UT[0] is set, then the Novell environment will be ignored, if present, and only the Windows environment information will be retrieved and sent to the R3000. If UT[1] is set and the Novell environment is invalid or the user is not authenticated with its Novell server, then the results sent to the R3000 are invalid (probably empty values). The default UT[255] auto detects Novell vs. Win32 and will automatically favor Novell authentication over Windows, if possible.

* Special Interest. Values most likely to change during testing, configuration, and production implementation.

++ Alternate configuration file is only valid when specified on the command line. It will be ignored in any other context. If the configuration file cannot be loaded from the alternate location, an error will be logged and an attempt will be made to load the default configuration file. If the alternate configuration file is specified and is blank (CF[]), the 8e6 Authenticator will *not* attempt to load any configuration file; this can minimally speed up execution time. The compiled default value of CF[-] causes the default configuration file loading to be attempted, which has the same full path and filename of the current, loaded 8e6 Authenticator executable, but with an extension of ".cfg" instead of ".exe". That is, if the 8e6 Authenticator client is "\\example\authenticat.exe", the search for the default configuration file

would be “\\example\authenticat.cfg”. It is *not* an error if the default configuration file does not exist. It *is* an error if the default configuration file exists but cannot be read or parsed correctly. Unknown parameters are ignored. Format/syntax errors will abort the reading and report an error, but the 8e6 Authenticator will attempt to continue running.

- For each IP address where “:PORT” is omitted from the address, the RP[] port value is used. For example, if RA[1.1.1.1:5555] is set, the RP[] parameter is ignored. RP[] affects port-less addresses specified in the RV[] command as well.
- For RA[], each IP address is separated by a semi-colon ‘;’ and the first IP address will be tried for each new connection attempt. When the main IP address fails to respond, the next IP address in the list will be tried, and so on, if it fails. After the last IP address is tried, the logic will continue from the first IP address again. A retry attempt on the main IP address is subject to the RR[] Reconnect time. After any disconnection, the logic will always begin with the main IP address as its first attempt.
- For RV[], sets of R3000 addresses are specified based on an IP range that matches the client’s IP address; multiple destination R3000 addresses may be used in each set and will have the same functionality as multiple destinations specified in the RA[] parameter. Each set is surrounded by parentheses ‘()’s, and sets are separated by commas ‘,’. Any local client IP address that does not match any set will use the RA[] address. Sample format:

```
RV[(102.108.1.0-102.108.1.255;1.1.1.1;2.2.2.2),(102.108.2.0-102.108.2.255;3.3.3.3:222)]
```

In this example, a client with an IP address of 102.108.1.5 would try to connect to 1.1.1.1 using the RP[] port (2.2.2.2 as the backup). A client with 192.168.2.15 would try to connect to 3.3.3.3 port 222, which has no backup.

- Any local address that would end up connecting to 0.0.0.0 will not be observed by the 8e6 Authenticator. This allows RV[] to allow only specified ranges of IP addresses to be observed by the 8e6 Authenticator.