SecurID Ready Implementation Guide

Last Modified 12/20/99

1. Partner Information

Partner Name	Lantronix
Web Site	www.lantronix.com
Product Name	LRS1, LRS2, LRS16, LRS32F
Version & Platform	
Product Description	Lantronix's LRS line of Remote Access Servers provide secure access for Dial-in, Dial-out, LAN-to-LAN, Console Server and ISP connections. An ideal choice for secure connectivity, all LRS models support PPP (PAP/CHAP), SLIP/CSLIP, SecurID, Radius, Kerberos, Unix, NetWare and local users database for authentication on both inbound and outbound connections. All LRS products support dial-back, Network Address Translation (NAT), routing of TCP/IP, IPX, and AppleTalk protocols is supported using RIP and static routes.
Product Category	Remote access server

2. Contact Information

	Pre-Sales	Post-Sales
Name	Sales	Technical Support
E-mail	sales@lantronix.com	support@lantronix.com
Phone	1-800-422-7055	1-800-422-7044
Web	www.lantronix.com	www.lantronix.com

3. Solution Summary

Feature	Details
Authentication methods supported	Login, Privileged Passwords PAP/CHAP (PPP) Dial Back Kerberos Authentication Support SecurID Authentication Support Radius Authentication Support Routing Firewall Local Users Database
New PIN support	All
Next tokencode support	Yes
Secondary server support	Slave ACE/Server
Location of node secret on client	None stored
ACE/Server client definition type	Communication Server
SecurID user specification	Designated users
SecurID protection of administrators	Yes

4. Product Specifications

ROUTING PROTOCOLS	TCP/IP (RIP and Static Routing) IPX (RIP/SAP and Static Route)
SERIAL INTERFACES	LRS1 - 1 RS232 DB25 (DTE) male connector 115 Kbps LRS2 - 2 RS232 DB25 (DTE) male connectors & 1 RS423 (RS232C compatible) RJ45 interface 115Kbps LRS16 - 16 RJ45 (RS232C / RS423) serial ports support up to 115Kbps LRS32F - 32 RJ45 (RS232C / RS423) serial ports support up to 230Kbps All supporting full modem control, V.90, ISDN modems and asynchronous CSU/DSUs.
ETHERNET INTERFACES	LRS1 - RJ45 (10BASE-T) LRS2, LRS16 - AUI, RJ45 (10BASE-T), BNC (10BASE2) LRS32F - 10/100 (BASE-T), AUI, BNC (10BASE2)
MODEM SHARING	IP hosts IPX hosts Free Lantronix Comm Port Redirector Software Supporting: Windows 95/98, Windows NT, Windows 3.11, DOS. Supports 16- and 32-bit applications
REMOTE ROUTING FUNCTIONALITY	Dial-on-Demand Routing Link Management Features IPX Protocol Spoofing Link Timeout Function Packet Filtering
REMOTE NODE FUNCTIONALITY	Support for all PPP-based Client Software including Windows 95/98 & Windows NT DUN
PRINT & TERMINAL SERVER FUNCTIONALITY	IPX (Novell NetWare) TCP/IP (Unix)

5. Product's ACE/Agent configuration

The LRS supports the ACE/Server security system manufactured by RSA Security Inc. ACE/Server is a system of client-server software and accompanying token cards.

> Note: Refer to your RSA Security documentation for ACE/Server installation instructions.

The SecurID card generates single-use, unpredictable numerical codes. These "tokencodes," together with the user's PIN, form the basis of the SecurID authentication. The PIN and generated tokencode are referred to collectively as SecurID **PASSCODES**. To gain access to a network protected by SecurID, both elements of the PASSCODE must be entered correctly.

The RSA Security SecurID system requires certain communication between the ACE/Server and the end-user. For example, the user must enter a new PIN when a SecurID card is first used, and a second PASSCODE when locked out.

PAP does not allow for these types of messages or additional user input. Therefore, it is strongly recommended that SecurID be run from character mode only. It is possible to use SecurID with PAP, provided that situations like those mentioned above are either prevented or handled in text mode on the next call.

To log into the LRS, the user must enter a username at the username prompt, and the PASSCODE at the password prompt.

To specify the SecurID ACE/Server for authentication of username/ PASSCODE, use the Set/Define Authentication SecurID command:

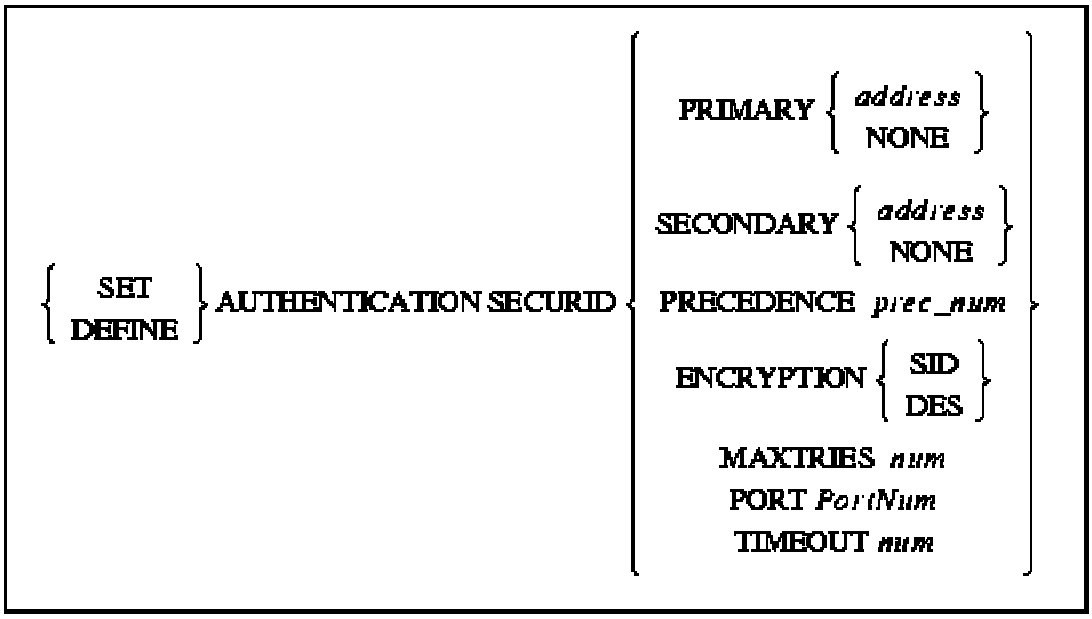
Figure: Configuring the LRS to Use SecurID

```
Local>> DEFINE AUTHENTICATION SECURID PRECEDENCE 1
Local>> DEFINE AUTHENTICATION SECURID PRIMARY 192.0.1.50
Local>> DEFINE AUTHENTICATION SECURID SECONDARY 192.0.1.51
```

After SecurID is configured on the LRS, the LRS will receive further configuration information from the ACE/Server. However, this only happens the first time that the LRS and ACE/Server communicate. If you purge the authentication information on the LRS or change the precedence of SecurID, this learned information will be lost. You will need to have your ACE/Server administrator reinitialize the LRS with ACE/Server for SecurID to function properly again.

If SecurID receives repeated authentication requests for an invalid username/password pair, it assumes that a login attack is taking place. SecurID will react by continually slowing its responses to the LRS. This problem can be avoided by ensuring that SecurID has the highest precedence number. For example, if you're using SecurID, Kerberos, and a UNIX password file, set SecurID's precedence to 3.

Set/Define Authentication SecurID



Specifies that a Security Dynamics ACE/SecurID server will be used for authentication.

Restrictions

You must be the privileged user to use this command.

Parameters

Primary
Specifies the first database or server to be checked. A specific address may be set with the address parameter, or the None parameter may be used to indicate that the database or file will not be used.

Secondary
If the LRS fails to authenticate the user using the primary database or server (due to network failure, server failure, missing or incorrect username/password), the secondary database or server will be checked. A specific address may be set with the address parameter, or the None parameter may be used to indicate that the server will not be used.
If the user cannot be authenticated using the secondary database or server, the database or server with the next precedence level will be checked. If all precedence levels fail to authenticate the user, the user is prevented from logging in.

address
A text host name (if a DNS is available for name resolution) or an IP address in standard numeric format (for example, 193.23.71.49).

None
Clears the current server address.

Precedence
Set the precedence in which this database or server is checked. The precedence number must be specified using the *prec_num* parameter.

prec_num
A precedence number between 1 and 6.

Encryption
SecurID (SID) or DES encryption will be used for authentication.

SID
Enables use of SecurID encryption.

DES
Enables use of DES encryption.

Maxtries
Specifies the maximum number of times the LRS will attempt to contact the SecurID server. Must be used in conjunction with the *tries* parameter.

tries
An integer between 1 and 255, inclusive.

Port
Specifies the UDP/IP Port number used to communicate with the primary and secondary SecurID servers. Must be used in conjunction with the *PortNum* parameter.

PortNum
An integer between 1 and 65535.

Timeout
Specifies the timeout period for a response from the SecurID server.Must be used in conjunction with the *seconds* parameter.

seconds
An integer between 1 and 255, inclusive.

Defaults
Encryption: DES.
MaxTries: 5.
UDP/IP port: 755
Timeout: 3 seconds.

Examples
Local>> DEFINE AUTHENTICATION SECURID PRIMARY 192.0.1.55
Local>> DEFINE AUTHENTICATION SECURID TIMEOUT 10 MAXTRIES 4
Local>> DEFINE AUTHENTICATION SECURID ACCOUNTING ENABLED

6. Certification Checklist

Indicate here the tests that were run to ensure the product is SecurID Ready::

Test	Pass	Fail
1st time auth. (node secret creation)	X	
New PIN mode:		
System-generated		
Non-PINPAD token	X	
PINPAD token	X	
User-defined (4-8 alphanumeric)		
Non-PINPAD token	X	
Password	X	
User-defined (5-7 numeric)		
Non-PINPAD token	X	
PINPAD token	X	
SoftID token	X	
Deny Alphanumeric	X	
User-selectable		
Non-PINPAD token	X	
PINPAD token	X	
Next Tokencode mode		
Non-PINPAD token	X	
PINPAD token	X	
Slave ACE/Server	X	
No ACE/Server	X	

X=Pass

7. Known Problems

None