LiteScape Technologies
Secure Profile Management (SPM)

RSA SecurID Ready Implementation Guide

Last Modified: February 1, 2011

Partner Information

Product Information	
Partner Name	LiteScape Technologies, Inc
Web Site	www.litescape.com
Product Name	SPM (Secure Profile Management)
Version & Platform	SPM 4.4 R3 for Microsoft Windows server (2003, 2008)
Product Description	LiteScape SPM is an identity management solution for VOIP systems that enables secure 3-factor log in from VOIP enabled end points (Cisco, Avaya, Polycom, etc). SPM enables extension mobility and end-user application personalization for the users while increasing the security of the VOIP end-point device data traffic.

Solution Summary

LiteScape SPM is an identity management solution for VOIP systems that enables secure 3-factor log in (Magnetic card, RFID, biometrics, bar-code and password based login are supported) from VOIP enabled end points (Cisco, Avaya, Polycom, etc).

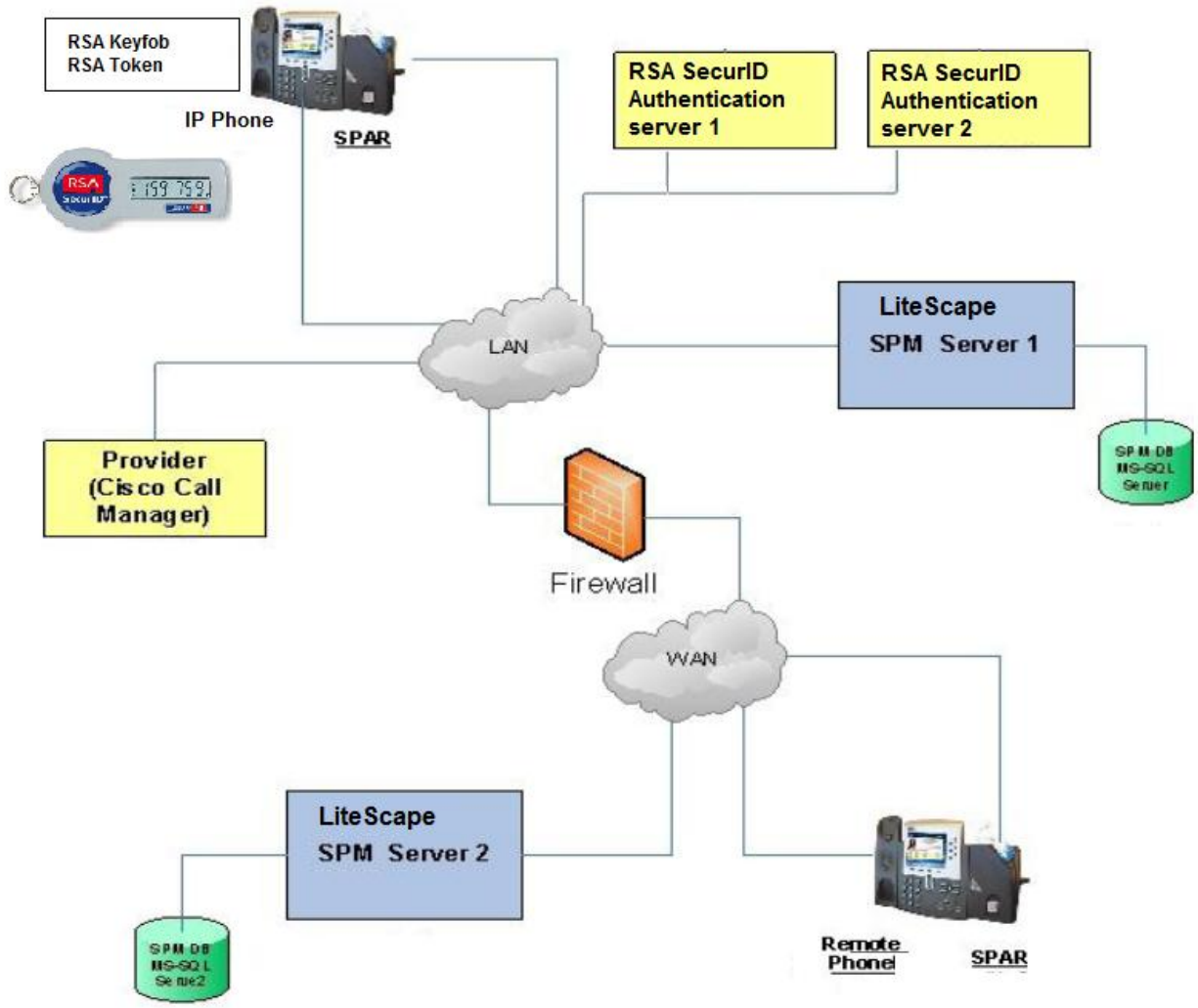
Once logged-in, the extension of the IP device along with the accessible/enabled applications is changed automatically to reflect the organizational policies for each user.

In addition, the SPM presence component provides an interface for other applications who can now firmly assert the location and identity of a specific user within the organization.

SPM enables the use of RSA SecurID Tokens to securely log-in to IP phones.

RSA key fob and RSA On-demand tokens can also be used in combination with the other verification methods supported by SPM to provide 2 of the factors of user verification (passcode and token) from the IP phones.

RSA SecurID supported features	
LiteScape Secure Profile Management (SPM) 4.4	
RSA SecurID Authentication via Native RSA SecurID Protocol	Yes
RSA SecurID Authentication via RADIUS Protocol	No
On-Demand Authentication via Native SecurID Protocol	Yes
On-Demand Authentication via RADIUS Protocol	No
On-Demand Authentication via API	Yes
RSA Authentication Manager Replica Support	Yes
Secondary RADIUS Server Support	No
RSA SecurID Software Token Automation	Yes
RSA SecurID SD800 Token Automation	No
RSA SecurID Protection of Administrative Interface	Yes


RSA Keyfob
RSA Token
IP Phone
SPAR
RSA SecurID Authentication server 1
RSA SecurID Authentication server 2
LAN
LiteScape SPM Server 1
Provider (Cisco Call Manager)
Firewall
WAN
LiteScape SPM Server 2
Remote Phone
SPAR


SPM User swipes card or accesses SPM login services from IP phone Services
RSA SecurID
RSA Authentication Client (SPM Server)
RSA Authentication Manager

Authentication Agent Configuration

Authentication Agents are records in the RSA Authentication Manager database that contain information about the systems for which RSA SecurID authentication is provided. All RSA SecurID-enabled systems require corresponding Authentication Agents. Authentication Agents are managed using the RSA Security Console.

The following information is required to create an Authentication Agent:

- Hostname
- IP Addresses for network interfaces

Set the Agent Type to “Standard Agent” when adding the Authentication Agent. This setting is used by the RSA Authentication Manager to determine how communication with LiteScape SPM will occur.

Note: Hostnames within the RSA Authentication Manager / RSA SecurID Appliance must resolve to valid IP addresses on the local network.

Partner Product Configuration

Before You Begin

This section provides instructions for configuring the LiteScape SPM with RSA SecurID Authentication. This document is not intended to suggest optimum installations or configurations.

It is assumed that the reader has both working knowledge of all products involved, and the ability to perform the tasks outlined in this section. Administrators should have access to the product documentation for all products in order to install the required components.

All LiteScape SPM components must be installed and working prior to the integration. Perform the necessary tests to confirm that this is true before proceeding.

Configuring SPM for RSA SecurID

To use RSA SecurID authentication, you will need to install an RSA Authentication Manager server, import the certificate to client server (SPM), and make configuration adjustments on the SPM server.

Creation and Export of the RSA Authentication Manager Certificate

When you install RSA Authentication Manager, the system creates a self-signed root certificate and stores it in RSA_AM_HOME/server/security/server_name.jks. You must export this certificate from the server, and import it into the keystore for remote API clients such as SPM. Use the Java keytool, as described below, to export the certificate and follow the instructions for importing the certificate into SPM.

To export the server root certificate:

1. Open a command prompt
2. Determine the RSA_AM_HOME environment variable by typing the following command: set RSA_AM_HOME. Copy the value assigned to this environment variable for the next steps.
3. Change the directory to RSA_AM_HOME/appserver/.Type the following command: jdkjdk/jre/bin/keytool -export -keystore RSA_AM_HOME/server/security/server_name.jks -file am_root.cer -alias rsa_am_ca
4. At the prompt for the keystore_password, press **Enter** without typing a password.

> **Note: You will see a warning screen, but the server root certificate will still be exported.**
>
> **The Java keytool outputs the certificate file am_root.cer to the RSA_AM_HOME/appserverdirectory.**

Importing the Server Root Certificate

1. Locate the server root certificate file that you exported from Authentication Manager, and copy it to the SPM Server.
2. On SPM server, open the **am_root.cer** file (exported from RSA AM server) to start the wizard.
3. Click through the wizard.
4. Select Automatically -> Select the certificate store based on the type of certificate.

Setting the Command Client User Name and Password

When you install Authentication Manager, the system creates a ‚command client' user name and password for secure connections to the RSA Command server. These user name and passwords are randomly generated upon creation, and are unique to each deployment.

You need to set the command client and user name values for each connection being made to the RSA command server. Use the RSA Manage Secrets' utility to obtain these values from RSA Authentication Manager.

To obtain the RSA Command client user name and password from Authentication Manager:

1. Open a new command prompt on your RSA Authentication Manager host and change the directory to RSA_AM_HOME/utils.
2. Type the following command: rsautil manage-secrets --action list
3. When prompted, type your master RSA password. The system displays the list of your internal system passwords.
4. Locate the values for your Command client user name and password. For example:
    a. Command Client User Name .....: CmdClient_vKr9aLK9
    b. Command Client User Password .....: e9SHbK0W4i

Adding a User to RSA Authentication Manager

Launch RSA Security Console**:**

1. To add a user, go to Identity > Users > Add New.
2. When you are done adding a user, go to **Authentication**>**SecurID Tokens**>**Manage Existing**. Under the **Unassigned** tab select a serial number >Select **Assign to User** to assign the user to the token created earlier.
3. Click checkbox of the user and select the **Select Require SecurID pin**>click GO.
4. Launch RSA Self-Service Console.
5. Login as the user you just created.
6. Answer all the user information related questions and click next.
7. Click Create PIN and create a new PIN, (for example ‚1234').

Configure the RSA SecurID Password Provider for SPM

1. Encrypt the Password and AdminPassword values
   RSA connectivity Password and AdminPassword values are encrypted using http://SPM-SERVER-ADDRESS/LSSparSPMWeb/FormPwdEncrypt.aspx
2. Go to C:\Documents and Settings\All Users\Application Data\Litescape\OnCast\ and open OnCast.SPM.Configuration.xml to modify the RSA connectivity settings and add the following to the OnCastConfiguration/SPM (if it doesn't already exist)

<RsaAuthManager>

<CmdServer>

<Url> https://RSA_AM_Server_IP/ims-ws/services/CommandServer </Url>

<UserName>CmdClient_hcmrc67u</UserName>

<Password>21Rt8HajQ7wEX59XM4XibQ==</Password>

</CmdServer>

<AdminUserName>administrator</AdminUserName>

<AdminPassword>YNNMzbptaAQIFEHgcqcf5Q==</AdminPassword>

</RsaAuthManager>

Url: change RSA_AM_Server_IP to reflect the RSA server's IP address

UserName – RSA Command client user name

Password – Encrypted RSA Command client user password

AdminPassword – RSA user with administrative rights

AdminPassword – Encrypted password

To configure for RSA Server redundancy, add RSA server URL's in the URL tag separate by commas:

<Url> https://RSA_AM_Server1_IP/ims-ws/services/CommandServer,https://RSA_AM_Server2_IP/ims-ws/services/CommandServer,https://RSA_AM_Server3_IP/ims-ws/services/CommandServer </Url>

3. Change OnCastConfiguration/CiscoInputFlag/CiscoInputFlag_User to L (User name is case sensitive use U for upper and L for lower)
4. Once configuration is completed, login to SPM Web Admin to set login type. You can either configure the system for PIN only or multi-factor Authentication-. Using RSA SecurID, users can either securely login to SPM via IP Phone services and without the presence of a SPAR device or login to SPM through a SPAR and leverage RSA SecurID.
5. You will need to configure each user for RSA SecurID authentication access. Refer to the SPM Enrollment Admin Guide for further detail.

Phone Service URL

Using the provided IP-PBX administrative interface (3rd party), add a phone service with the following URL:

http://SPM Server IP/LSSparSPMWeb/LSSparUrlService.aspx

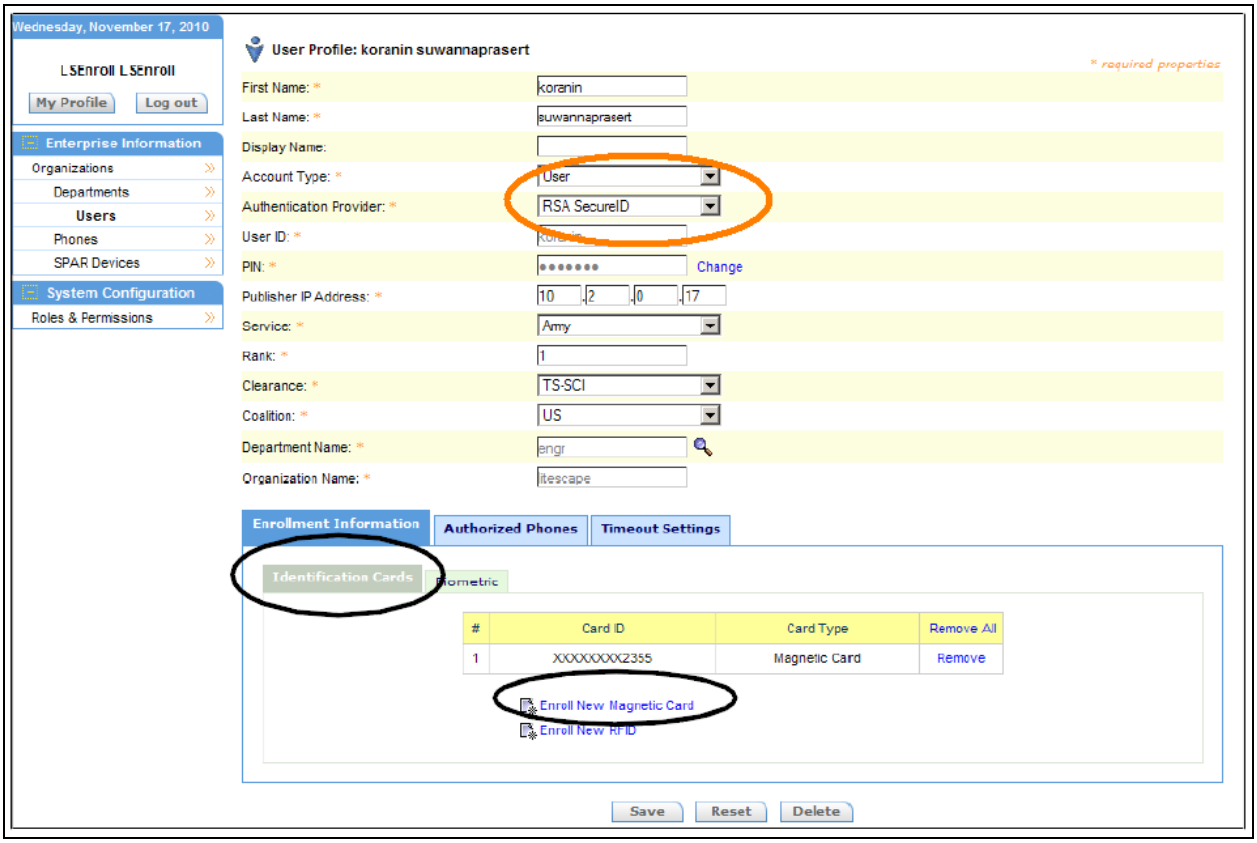
Subscribe this service to the IP Phones that will allow users to login via RSA SecurID.

Enrollment: Enabling RSA SecurID for Users

Authentication Provider

If you are required to use RSA SecurID for authentication, with or without a SPAR device, select RSA SecurID or RSA SecurID On-Demand.

If a user does not have Token device, Enrollment administrator must change user's Authentication Provider to RSA SecurID On-Demand.



End-user: Using RSA SecurID

With RSA SecurID authentication, login to the SPM application does not require SPAR device.

RSA SecurID can be configured to be used with or without a SPAR.

Create a PIN

When RSA SecurID is used with SPM to allow users to login to the phone, the PIN used for login purposes is the RSA SecurID User PIN (Not the PIN configured in SPM web admin). Each user is required to create a PIN upon their first login:

1. Select IP Phone Services to select the RSA SecurID service subscribed to the phone or use the SPAR and swipe your ID card.
2. To login for the first time, you are required to provide UserID and Token in the Password field. Subsequent times will require the RSA SecurID Passcode in the Password field which is the combination of the Token and PIN.

3. Once logged in, you will see your UserID at the top of the page. Enter a new PIN as requested and verify. PIN length is based on your organization's policy. Please check with the SecurID administrator.
4. If you are required to provide ID card or biometrics, you will be requested to provide further verification/identification at this time.

RSA SecurID without a SPAR

To use the RSA SecurID authentication without a SPAR, user's phone must be subscribed to the RSA SecurID service. User can access this service from any phone that is subscribed to it. When RSA SecurID is used without a SPAR, users do not need to have authorized phones to login. To login to the phone:

1. Select IP Phone Services button from the phone.
2. Select the RSA SecurID service subscribed to the phone.
   Enter username and password. User password is a combination of the PIN followed by the
3. RSA SecurID code.
4. Submit your credentials.

> **Note: RSA SecurID authentication can coexist with SPAR authentications. In this case, either the user can first swipe magnetic card and then provide other types of authentication or the user can invoke the phone service and subsequently will be asked to provide ID and swipe finger for biometric authentication.**

RSA SecurID On-Demand

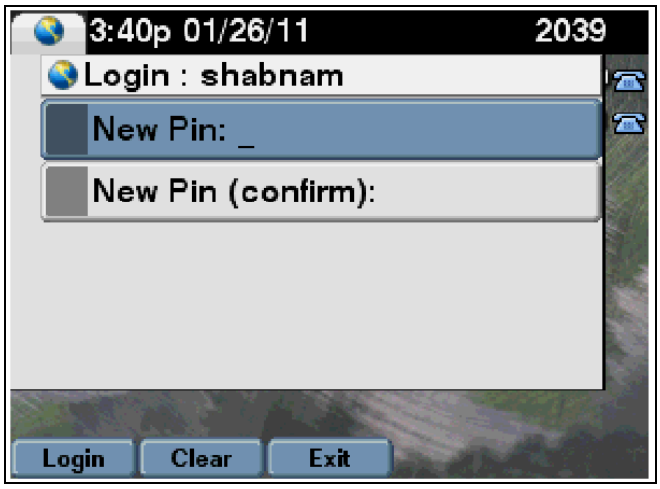
There are a few steps a user is required to take in order to use RSA On-Demand with SPM application. First, user needs to communicate with SPM administrator to change their profile's Authentication Provider to **RSA SecurID On-Demand**. Next, user needs to retrieve their On-Demand passcode from the RSA administrator. User will be required to create a new PIN upon their login to the phone and subsequently will be provided with a token via email.

1. From the phone, select IP Phone Services button.
2. Select the RSA SecurID service subscribed to the phone.
   Enter username in the **UserID** field and the On-Demand passcode provided by the RSA administrator in the **Password** field.
3. User will be prompted to create a new PIN. The password policy (numeric or alphanumeric) depends on the set policies in the RSA server.
4. Once the new PIN is created, the system will automatically email a Token to the user and the next screen will be prompted. Use the newly created PIN followed by the Token as the Passcode to login to the phone.

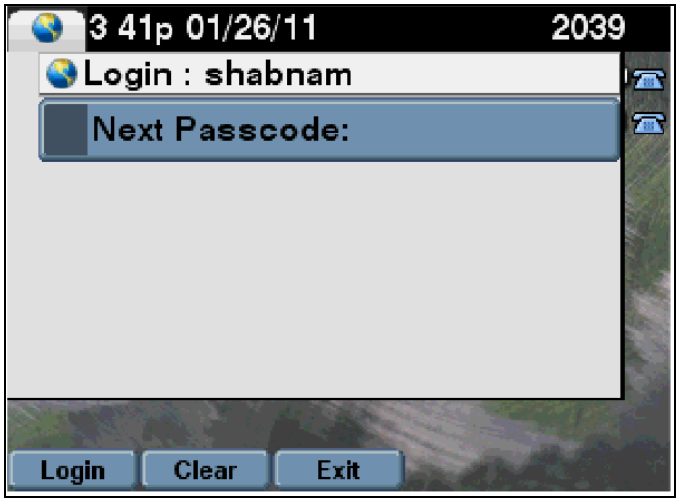
Screens

Login screen:

User-generated New PIN:



System-generated New PIN:



Certification Checklist for RSA Authentication Manager

Date Tested: **February 1, 2011**

Certification Environment		
Product Name	**Version Information**	**Operating System**
RSA Authentication Manager	7.1.2 (am-7.1.2-build20091007190003)	Windows 2003 Server R2
LiteScape SPM	4.4 R3	Windows 2003, 2008

Mandatory Functionality			
RSA Native Protocol		**RADIUS Protocol**	
New PIN Mode			
Force Authentication After New PIN	✓	Force Authentication After New PIN	NA
System Generated PIN	✓	System Generated PIN	NA
User Defined (4-8 Alphanumeric)	✓	User Defined (4-8 Alphanumeric)	NA
User Defined (5-7 Numeric)	✓	User Defined (5-7 Numeric)	NA
Deny 4 and 8 Digit PIN	✓	Deny 4 and 8 Digit PIN	NA
Deny Alphanumeric PIN	✓	Deny Alphanumeric PIN	NA
Deny Numeric PIN	✓	Deny Numeric PIN	NA
Deny PIN Reuse	✓	Deny PIN Reuse	NA
Passcode			
16 Digit Passcode	✓	16 Digit Passcode	NA
4 Digit Fixed Passcode	✓	4 Digit Fixed Passcode	NA
Next Tokencode Mode			
Next Tokencode Mode	✓	Next Tokencode Mode	NA
On-Demand Authentication			
On-Demand Authentication	✓	On-Demand Authentication	NA
On-Demand New PIN	✓	On-Demand New PIN	NA
Load Balancing / Reliability Testing			
Failover (3-10 Replicas)	✓	Failover	NA
No RSA Authentication Manager	✓	No RSA Authentication Manager	NA

GLS / PAR

✓ = Pass ✗ = Fail N/A = Not Applicable to Integration

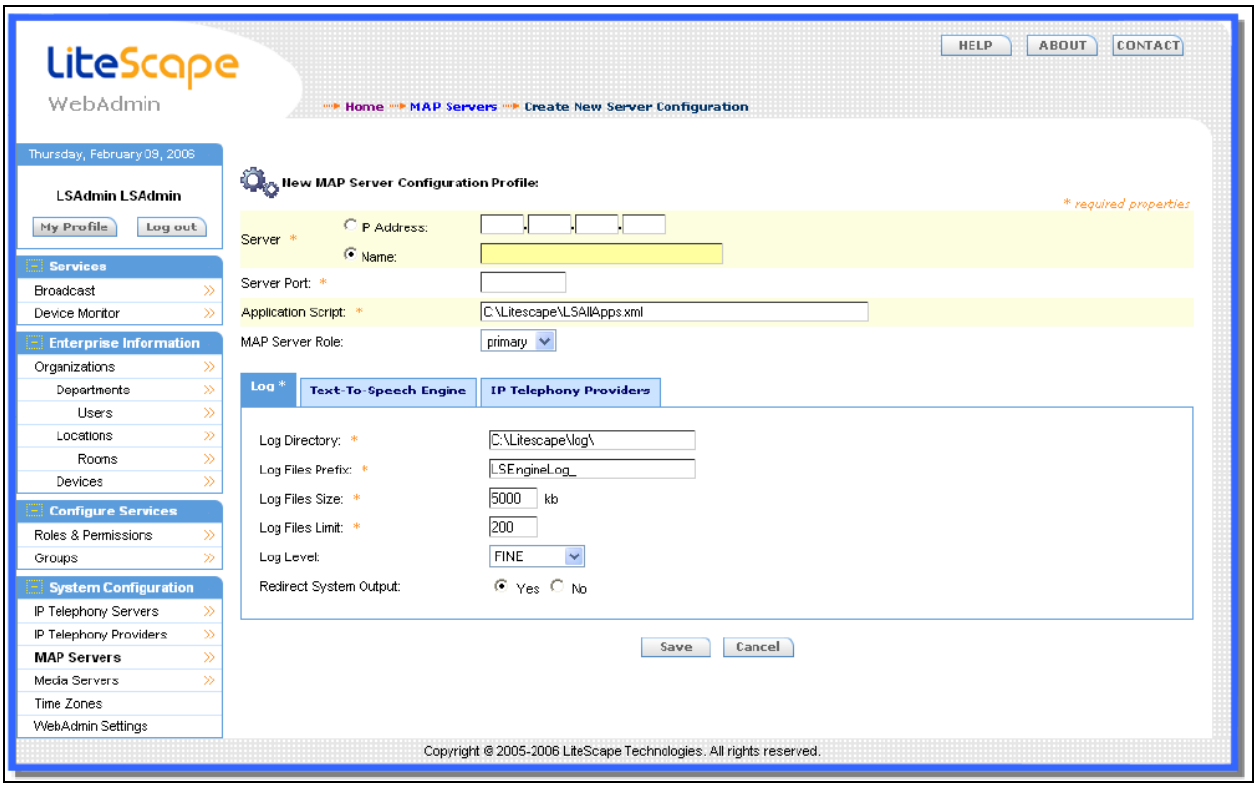
Agent Tracing:

Setting server log output

To configure MAP servers, you must setup the server output log.
To set the server log parameters:

1. Click MAP Servers to display the MAP Servers window.
2. Click the IP address or host name of the server whose properties you want to view or modify to display the MAP Server Configuration window.
3. Expand the Log section.
4. Specify the server log properties according to their descriptions:

Log Directory	The path to the directory where the server log files will be stored.
Log File Prefix	The prefix to be added to the log file name when a new log file is created.
Log File Size	The maximum size of the log file, in kilobytes. A new log file will be created after this maximum size is reached.
Log Files Limit	The maximum number of log files to be stored before they are overwritten by new log files.
Log Level	The output level of the server log.
Redirect System Output	When set to Yes, the system redirects error messages and exceptions - System.out and System.err - to a separate log file. The file name will consist of the same prefix as a server log file and a corresponding suffix.



Appendix

Partner Integration Details	
RSA SecurID API	Version or Custom Build; API details below
RSA Authentication Agent Type	Standard Agent
RSA SecurID User Specification	Designated Users, All Users, Default Method
Display RSA Server Info	Yes or No
Perform Test Authentication	Yes
Agent Tracing	Yes