RSA SECURID® ACCESS

Authentication Manager Implementation Guide

LumenVox Password Reset 7.0

Peter Waranowski, RSA Partner Engineering

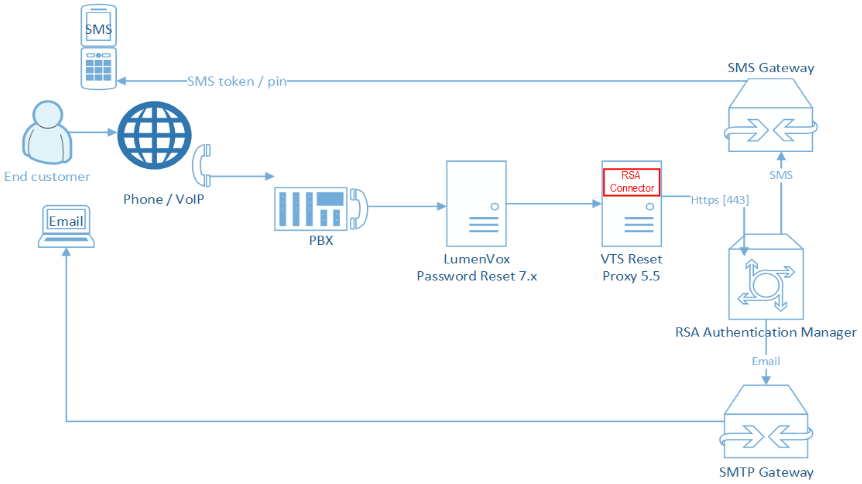
Last Modified: March 5th, 2019

RSA
READY

Solution Summary

LumenVox leverages the RSA Authentication Manager Administrative API as a means to integrate with the RSA Authentication Manager 8.4 to provide Administrative functionality. The LumenVox Password Reset Server provides users with the ability to enable, set new PIN and change PIN using voice automation. Further, it also provides users the ability to reset their On-Demand SMS Destination and On-Demand PIN.

Partner Integration Overview	
Manage Standard Card, Key Fob, PINPAD, and Software Tokens	No
Add RSA Authentication Manager users	No
Modify RSA Authentication Manager users	No
Delete RSA Authentication Manager users	No
Add RSA Authentication Manager groups	No
Modify RSA Authentication Manager groups	No
Delete RSA Authentication Manager groups	No
Assign/unassign RSA SecurID tokens	No
Enable/disable RSA SecurID tokens	Yes
Clear/Reset RSA SecurID token PINs	Yes
Enable Risk-Based Authentication (RBA).	No
Change users' authentication methods (PASSCODE, Fixed-Tokencode, On-Demand Token or RBA)	No
Perform initial import of RSA Authentication Manager resources	No
Reconcile RSA Authentication Manager identity source users and groups with the provisioning data store.	No
Reconcile RSA SecurID tokens with the provisioning data store.	No



Partner Product Configuration

Before You Begin

This section provides instructions for configuring LumenVox Password to provision RSA Authentication Manager resources. 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 Lumenvox Password Reset components must be installed and working prior to the integration. Perform the necessary tests to confirm that this is true before proceeding.

! Important: The configuration shown in this Implementation Guide is for example and testing purposes only. It is not intended to be the optimal setup for the device. It is recommended that customers make sure Lumenvox Password Reset is properly configured and secured before deploying to a production environment.

LumenVox Password Reset 7.0 - Product Requirements

CPU	Dual-Core Intel® Xeon® Processor, current generation
Memory	Min 16 GB
Storage	Min 20 GB disk space
Operating System	Windows Server 2012 R2, 2014 or 2016
.Net Framework	v 4.5 and v 4.6
LumenVox PasswordReset	v 7.x
VTS Reset Proxy (optional)	v 5.x
RSA Connector (RSA AM 8.4)	v 5.54.x

LumenVox Password Reset 7.0 – Configuration

In order to use automated RSA Pin and Password reset features, please follow the next steps:

1. Install and configure LumenVox Password Reset version 7.x (separate instructions manual)
2. Optional, install and configure VTS Reset Proxy version 5.54 (separate instructions manual)
3. Deploy RSA Connector on LumenVox Password Reset or VTS Reset Proxy machine.

   - Copy binaries to the VTS5 Reset Proxy binary path:

     - VTRSA84Reset.dll
     - VTRSA84.exe (configuration / test tool)
     - rsaws.dll

4. Install RSA AM server certificate on LumenVox Password Reset or on VTS Reset Proxy machine:

   - Start -> Run -> mmc
   - Go to File -> choose Add/Remove Snap-in
   - Select console root and press add
   - select Certificate -> add -> computer account -> next -> local computer -> finish -> close
   - double click on Certificate, then on ok
   - on the left window, go to Trusted Root Certification Authorities
   - go to Certificates
   - right click on certificates -> all Tasks -> import
   - next -> browse to your root certificate
   - place your certificate in the Trusted Root Certification Authorities store
   - complete the process until you are finished

5. Run the configuration / test tool (VTRSA84.exe) and configure the "VTResetInfo.xml". Configuration data will be saved and used later for all RSA related operations (PIN Clear, Reset)

   1. Set configuration to manual mode and specify the RSA AM host name:

```
**********************************************************************
*****************Starting RSA Reset Configuriation******************
**********************************************************************
You may enter the connect info manually or read it from a configured reset system.
Do you want to specify the values manually? (Y/N)y
**********************************************************************
If the url is in the form:
https://<HOST_NAME/IP>:7002/ims-ws/services/CommandServer you may specify just the
host name/ ip.
Please enter hostname or the entire url:VT-RSA84.dev-ref.de
You specified the following url:
https://VT-RSA84.dev-ref.de:7002/ims-ws/services/CommandServer
Is this correct? (Y/N)
```

   2. After confirming the URL you need to type in the Command API Client User ID and the Command API Client User Password (the Username used to authenticate against the Web Service):

```
**********************************************************************
In the following section you will be asked to provide administrative
credentials.
Please make sure that no unauthorized user is viewing this data.
**********************************************************************
**********************************************************************
NOTE:This user ID is in the form : CmdClient_<SOME STRING>
NOTE:If you do not have a userID that fits this description please read the
installation document
**********************************************************************
Please enter the Username used to authenticate against the
WebService:CmdClient_foecpphz
Please enter the Password for this user:*****************
```

3. Choose certificate validation mode for the tool: strong validation (if RSA server certificate is properly installed) or weak validation:

```
**********************************************************************
NOTE:In production  certificate validation should always be turned on.
**********************************************************************
Do you want weak server validation (Ace Server Certificate not validated)?(Y/N)
```

4. The tool is asking for the Technical User credentials (any RSA AM user with proper rights on Tokens and Passwords management):

```
Please Provide the User Name of the ACE Server Admin to use: Admin
Please Provide the Password for the User: **********
**********************Web Service Connect Summary**********************
Connecting to URL    :   https://VT-RSA84.dev-ref.de:7002/ims-
ws/services/CommandServer
Connecting with user:   CmdClient_foecpphz
Password            :   *********
Ace Tech. User      :   Admin
Ace Tech. Password  :   *********
*****************************End Summary******************************
```

5. Once the connection to the RSA Authentication Manager Server is established, you will be able to perform the RSA reset for a chosen User or Token:

```
**********************************************************************
****************************Authenticated*****************************
**********************************************************************
**********************************************************************
**********************Getting Reset Information***********************
**********************************************************************
-Are you specifying the (T)oken Serial or the (U)ser Login? U
Do you want to:
(C)lear a Pin.
(R)eset a Pin.
Reset a (P)assword (fixed tokencode).
Set Pin on (O)nDemand token.
Set (S)MS Destination on OnDemand token.
Set (E)mail Destination on OnDemand token.
Reset User (L)DAP Password (Self Service Password).
Change User (A)ttribute.(e.g on Demand with Custom Destination field)
Please select a mode:
```

6. After selecting one operation the tool will prompt for the desired User identifier and other additional data required to complete the operation. Once the operation is completed the tool will show the operation result and will offer the option to save configuration data:

```
Please select a mode:C
Please Enter the User Name:ama
Do you want to unlock the token in case it is locked(Y/N)?y
Do you want to force the user to to change the pin after login(Y/N)?n
Do you want to set token to next token mode(Y/N)?n
**********************************************************************
*******************Done Getting Reset Information.********************
**********************************************************************
Pin cleared on token:000512565932
**********************************************************************
***************************Saving Settings****************************
**********************************************************************
Do you want to create a reset system from that data?(Y/N)

Do you want to create a reset system from that data?(Y/N)y
You have the following tenant(s) available:
(1)VT6
(n)ew tenant.
Please press the appropiate index or e to exit:1
You selected: VT6
**********************************************************************
Please select the appropiate reset system.
Press 1 for     :RSA-8.4
Press 2 for     :RSA-8.1
Press 0 to:     Create a new System
Please select a number:1
**********************************************************************
*************************Done Saving Settings*************************
**********************************************************************
Do you want to perform another rsareset? (Y/N)
```

7. All collected configuration data is saved (encrypted) under VTResetInfo.xml:

```
<?xml version="1.0" encoding="utf-8"?>
<VT xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:xsd="http://www.w3.org/2001/XMLSchema">
  <TENANT NAME="VT6">
    <SYSTEMS>
      <SYSTEM NAME="RSA-8.4" TYPE="RSA8Reset">
        <FIELD NAME="reset.lib" VALUE="VTRSA84Reset.dll" ALIAS="Reset Library Name" />
        <FIELD NAME="reset.fnct" VALUE="DoRSAPinReset" ALIAS="Function Name" />
        <FIELD NAME="srv.descr" VALUE="CmdClient_foecpphz" ALIAS="Command User Name" />
        <FIELD NAME="srv.defpwd" VALUE="D0C2051E135B4C20F7F" ALIAS="Command User Password" />
        <FIELD NAME="srv.instance" VALUE="false" ALIAS="Weak Validation" />
        <FIELD NAME="srv.name" VALUE="https://VT-RSA84.dev-ref.de:7002/ims-ws/services/CommandServer"
ALIAS="Command Web Service URL" />
        <FIELD NAME="srv.admin.login" VALUE="admin" ALIAS="Technical User" />
        <FIELD NAME="srv.admin.pwd" VALUE="61732E931A3B094E" ALIAS="Technical User Password" />
        <FIELD NAME="srv.identity.src" VALUE="" ALIAS="Desired Identity Source" />
        <FIELD NAME="srv.client" VALUE="-c;-e;-l" ALIAS="Reset Flags" />
      </SYSTEM>
    </SYSTEMS>
  </TENANT>
</VT>
```

Configuration is complete. Configuration data will be reused later by the RSA Reset Connector.

Certification Checklist for RSA Authentication Manager

Date Tested: March 5th, 2019

Certification Environment		
Product Name	**Version Information**	**Operating System**
RSA Authentication Manager	8.4	Virtual Appliance
Lumenvox Password Reset	7.0	Windows 10
Lumenvox RSA Reset Connector	v 5.54.x	Windows 10

Test	Result
Authentication Management	
Assign a token	N/A
Un-assign a token	N/A
Enable a token (Unlock the User Whom the token belongs to)	✓
Disable a token	N/A
Clear/Reset a user PIN	✓
Change a user's authentication method	N/A
Enable RBA	N/A
Reset a user's LDAP (Self –Service Console) Password	✓
Reset a user's Fixed PassCode	✓
Reset a user's On Demand Pin	✓
Reset a user's On Demand SMS Destination	✓
Reset a user's On Demand SMTP Destination	✓
Reset a user's Custom Attribute	✓

✓ = Pass ✗ = Fail N/A = Non-Available Function

Known Issues

Unsupported User States

Using the API and the connector it is possible to achieve some states/functionality that might not be desirable and might become unsupported in future releases of the API. The state of a token being cleared and not put in NewPin Mode or the functionality of setting a Pin on a SecurID Token is some of these issues.

Appendix

PIN and Password Reset Parameters

PIN and Password Reset may take the following parameters in the server name field. (Flags are semicolon separated):

• **-l**: Use the "–l" if you are sending the user ID for the password reset (VT User Manager). The flag indicates that the vtt_usrsrv_lnk table holds the user login that the token belongs to. When reset is performed it will be done on the first token that the user possesses. (For users with multiple tokens it will reset the first token returned by the token lookup and not any others). If this flag is missing, the connector will assume that the value in VTUserManager is a numeric token Serial ID. This flag has no validity for password reset, since password reset may only be done on the user account and not a token. (Meaning that for password reset this flag is implicitly set).

• **-e**: The flag means that, if the user is unlocked, after reset, he will be unlocked.

• **-c:** This flag has validity only for pin reset and will be ignored for password reset. This flag indicates that there should be no pin on the token and that the user may sign in only with the part of the pass code that is displayed on the token. Once the flag "-c" is set, after a successful reset, the connector will receive the return code 2 (Pin Cleared) responsible to play the audio file "STR_PIN_CLEARED" (e.g.of the content:" your pin has been cleared. Please log on just using your token code". When missing, after a successful reset, LumenVox Password Reset will receive the return code 1 (Pin Set). And will play in this case the sequence "STR_PASSWORD_IS"+ <password>.

• **-n**: The flag means that for pin reset or pin clearance the user has to change the pin on the token when he or she signs in. For password reset the meaning is identical except that the user is forced to change the password after signing in (see limitation).