RSA Professional Services

AM INTEGRATION SERVICES PLATFORM

API Document for AMIS 1.7

RSA Professional Services

Contact Information

Go to the RSA corporate web site for regional Customer Support telephone and fax numbers: www.rsa.com.

Trademarks

RSA, the RSA Logo and EMC are either registered trademarks or trademarks of EMC Corporation (“EMC”) in the United States and/or other countries. All other trademarks used herein are the property of their respective owners. For a list of RSA trademarks, go to www.rsa.com/legal/trademarks_list.pdf.

License Agreement

The guide and any part thereof is proprietary and confidential to EMC and is provided only for internal use by licensee. Licensee may make copies only in accordance with such use and with the inclusion of the copyright notice below. The guide and any copies thereof may not be provided or otherwise made available to any other person.

No title to or ownership of the guide or any intellectual property rights thereto is hereby transferred. Any unauthorized use or reproduction of the guide may be subject to civil and/or criminal liability.

The guide is subject to update without notice and should not be construed as a commitment by EMC.

Note on Encryption Technologies

The referenced product may contain encryption technology. Many countries prohibit or restrict the use, import, or export of encryption technologies, and current use, import, and export regulations should be followed when using, importing or exporting the referenced product.

Distribution

Use, copying, and distribution of any EMC software described in this publication requires an applicable software license.

Disclaimer

EMC does not make any commitment with respect to the software outside of the applicable license agreement.

EMC believes the information in this publication is accurate as of its publication date. EMC disclaims any obligation to update after the date hereof. The information is subject to update without notice.

THE INFORMATION IN THIS PUBLICATION IS PROVIDED TO SUGGEST BEST PRACTICES, IS PROVIDED "AS IS," AND SHALL NOT BE CONSIDERED PRODUCT DOCUMENTATION OR SPECIFICATIONS UNDER THE TERMS OF ANY LICENSE OR SIMILAR AGREEMENT. EMC CORPORATION MAKES NO REPRESENTATIONS OR WARRANTIES OF ANY KIND WITH RESPECT TO THE INFORMATION IN THIS PUBLICATION, AND SPECIFICALLY DISCLAIMS IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

All references to “EMC” shall mean EMC and its direct and indirect wholly-owned subsidiaries, including RSA Security LLC.

April 2012

Table of Contents

DOCUMENT INFORMATION

Prepared By:	**Sean P. Doyle**
E-mail:	spdoyle@rsasecurity.com
Reviewed/Approved By:	
Create Date:	**November 19, 2010**
Version:	**1.5**
Updated:	**December 7, 2012**

Version History			
Version	**Author**	**Date**	**Revision Notes**
0.1	Sean P. Doyle	11/19/2010	Initial DRAFT created for mock
0.2	Sean P. Doyle	11/19/2010	Updated information with test scripts and new test features
.9	Sean P. Doyle	3/9/2011	Includes full TDS
1.0	Sean P. Doyle	3/11/2011	Finale edits
1.1	Sean P. Doyle	2/2/2012	TDS 1.6 Edits and New Content
1.2	Margaret Mulligan	4/20/2012	Minor Consistency Edits and Formatting
1.3	Sean P. Doyle	5/17/2012	Updates and changes
1.4	Sean P. Doyle	7/2/2012	Updates
1.5	Sean P. Doyle	12/7/2012	Updates

AM 7.1 AMIS User Methods

amXX - "XX" refers to either 61 or 71, depending on the versions of the Authentication Manger in the underlying system.

Enable User

UserSearchString is a wildcard searchable value on the userID.

SearchType determines the search scope, including the following valid options:

- Equals
- Begins With
- Ends With
- Contains

amXX User ID - Enable	
GET	http://10.100.89.138:8080/amXX/user/enable/<**UserID**>?searchType=<**equals**>
Request HEADER	

`GET /amXX/user/enable/protester?searchType=equals HTTP/1.1`
`Host: 10.100.89.138:8080`
`Connection: Keep-Alive`	

Request BODY	
`n/a`	
Response HEADERS	

`HTTP/1.1 200 OK`
`Server: Apache-Coyote/1.1`
`Content-Type: application/xml`
`Transfer-Encoding: chunked`
`Date: Wed, 07 Mar 2012 00:49:11 GMT`	

Response BODY	
`<?xml version="1.0" encoding="UTF-8" standalone="no"?>` `<serviceResult result="true"/>`	

Disable User(s) - /amXX/user/disable

UserSearchString is a wildcard searchable value on the userID.

SearchType determines the search scope, including these valid options:

- equals
- beginsWith
- endsWith
- contains

amXX – Disable	
GET	http://10.100.89.138:8080/amXX/user/disable/<***UserSearchString***>?searchType=<***equals***>
Request HEADER	
`GET /amXX/user/disable/protester?searchType=equals HTTP/1.1` `Host: 10.100.89.138:8080`	
Request BODY	
`n/a`	
Response HEADERS	

`HTTP/1.1 200 OK`
`Server: Apache-Coyote/1.1`
`Content-Type: application/xml`
`Transfer-Encoding: chunked`
`Date: Wed, 07 Mar 2012 00:54:42 GMT`	

Response BODY	
`<?xml version="1.0" encoding="UTF-8" standalone="no"?>` `<serviceResult result="true"/>`	

Search User(s) - /amXX/user/search

UserSearchString is a wildcard searchable value on the userID.

SearchType determines the search scope, including these valid options:

- equals
- beginsWith
- endsWith
- contains

amXX – Search	
GET	http://10.100.89.138:8080/amXX/user/search/ <***UserSearchString***>?searchType=<***beginsWith***>

Request HEADER

```
GET /amXX/user/search/protester?searchType=equals HTTP/1.1
Host: 10.100.89.138:8080
Connection: Keep-Alive
```

Request BODY

```
n/a
```

Response HEADERS

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: application/xml
Transfer-Encoding: chunked
Date: Wed, 07 Mar 2012 00:56:52 GMT
```

Response BODY

```
<?xml version="1.0" encoding="utf-8" standalone="no"?>
<serviceResult result="true">
  <UserSearchResults Count="1">
    <Item isRegistered="true">
      <CustomAttributes />
      <firstName>Pro</firstName>
      <isEnabled>false</isEnabled>
      <isLocked>false</isLocked>
      <lastName>Tester</lastName>
      <userID>protester</userID>
    </Item>
  </UserSearchResults>
</serviceResult>
```

Assign Next Token to User - /amXX/user/assignNext

tokenType can be software or hardware.

Grabs next available token of chosen type and assigns to provided userID.

Note: Software tokens must be distributed either via CT-KIP or STDID. See the token update functions for these details.

amXX Token Assignment – Assign Next Software Token	
GET	http://10.100.89.138:8080/amXX/user/assignNext/<***UserID***>/software
Request HEADER	

`GET /amXX/user/assignNext/protester/software HTTP/1.1`
`Host: 10.100.89.138:8080`
`Connection: Keep-Alive`	

Request BODY	
`n/a`	
Response HEADERS	

`HTTP/1.1 200 OK`
`Server: Apache-Coyote/1.1`
`Content-Type: application/xml`
`Transfer-Encoding: chunked`
`Date: Wed, 07 Mar 2012 01:01:22 GMT`	

Response BODY	

`<?xml version="1.0" encoding="utf-8" standalone="no"?>`
`<serviceResult result="true">`
`  <TokenSerialNumber>000115876402</TokenSerialNumber>`
`</serviceResult>`	

amXX Token Assignment – Assign Next Hardware Token	
GET	http://10.100.89.138:8080/amXX/user/assignNext/<***UserID***>/hardware
Request HEADER	

`GET /amXX/user/assignNext/protester/hardware HTTP/1.1`
`Host: 10.100.89.138:8080`
`Connection: Keep-Alive`	

Request BODY	
`n/a`	
Response HEADERS	

`HTTP/1.1 200 OK`
`Server: Apache-Coyote/1.1`
`Content-Type: application/xml`
`Transfer-Encoding: chunked`
`Date: Wed, 07 Mar 2012 01:04:28 GMT`	

Response BODY	

`<?xml version="1.0" encoding="utf-8" standalone="no"?>`
`<serviceResult result="true">`
`  <TokenSerialNumber>000119751886</TokenSerialNumber>`
`</serviceResult>`	

Assign Token to User - /amXX/user/assign

Assigns token specified by serial number to provided userID.

Note: The user must exist and the token specified must not be assigned to another user. If a software token is assigned, it must be distributed via the token update function.

amXX Assign Token	
GET	http://10.100.89.138:8080/amXX/user/assign/<UserID>/<serialNumber>
Request HEADER	
GET /amXX/user/assign/protester/000120881431 HTTP/1.1 Host: 10.100.89.138:8080	
Request BODY	
n/a	
Response HEADERS	
HTTP/1.1 200 OK Server: Apache-Coyote/1.1 Content-Type: application/xml Transfer-Encoding: chunked Date: Wed, 07 Mar 2012 01:09:05 GMT	
Response BODY	
<?xml version="1.0" encoding="utf-8" standalone="no"?> <serviceResult result="true"> <TokenSerialNumber>000120881431</TokenSerialNumber> </serviceResult>	

Attribute Search Fields

Fetch the list of available attributes for searching, only applicable to AM 7.1 systems:

am71 Attribute Search	
GET	http://10.100.89.139:8080/am71/user/searchFields/

Request HEADER

```
GET /amXX/user/searchFields HTTP/1.1
Host: 10.100.89.139:8080
```

Request BODY

```
n/a
```

Response HEADERS

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: application/xml
Transfer-Encoding: chunked
Date: Wed, 07 Mar 2012 01:26:07 GMT
```

Response BODY

```
<?xml version="1.0" encoding="utf-8" standalone="no"?>
<serviceResult result="true">
    <UserSearchFields Count="9">
        <Value name="First Name">FIRST_NAME</Value>
        <Value name="Last Name">LAST_NAME</Value>
        <Value name="Email Address">EMAIL</Value>
        <Value name="User ID">LOGINUID</Value>
        <Value name="ActivationCode">ActivationCode</Value>
        <Value name="AlternateEmail">AlternateEmail</Value>
        <Value name="phone">phone</Value>
        <Value name="SMSEmailProvider">SMSEmailProvider</Value>
        <Value name="VPNCertification">VPNCertification</Value>
    </UserSearchFields>
</serviceResult>
```

Attribute Search

The Attribute Search method is only currently available on AM 7.1 systems. The Attribute Search provides the following search parameters:

- Equals
- Begins With
- Ends With
- Contains

am71 Attribute Search	
GET	http://10.100.89.138:8080/am71/user/search/ <attribute>/<value>?searchType=<beginsWith>

Request HEADER

```
GET /am71/user/search/phone/206?searchType=beginsWith HTTP/1.1
Host: 10.100.89.138:8080
```

Request BODY

```
n/a
```

Response HEADERS

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: application/xml
Transfer-Encoding: chunked
Date: Wed, 07 Mar 2012 01:26:07 GMT
```

Response BODY

```
<?xml version="1.0" encoding="utf-8" standalone="no"?>
<serviceResult result="true">
  <UserSearchResults Count="2">
    <Item isRegistered="true">
      <CustomAttributes>
        <attribute name="phone">
          <values>
            <value>2065551212</value>
          </values>
        </attribute>
        <attribute name="SMSEmailProvider">
          <values>
            <value>twistester3@proservices-2.com</value>
          </values>
        </attribute>
      </CustomAttributes>
      <emailAddress>twistester3@proservices-2.com</emailAddress>
      <firstName>ondemand</firstName>
      <isEnabled>true</isEnabled>
      <isLocked>false</isLocked>
      <lastName>tester2</lastName>
      <userID>ondemandtester2</userID>
    </Item>
    <Item isRegistered="true">
      <CustomAttributes>
```

am71 Attribute Search
<attribute name="phone"> <values> <value>206-931-1523</value> </values> </attribute> </CustomAttributes> <emailAddress>sdoyle@proservices-2.com</emailAddress> <firstName>Sean</firstName> <isEnabled>true</isEnabled> <isLocked>false</isLocked> <lastName>Doyle</lastName> <userID>sdoyle</userID> </Item> </UserSearchResults> </serviceResult>

User Actions – Register User

This service is only applicable to AM 7.1 systems. User accounts in external identity sources must be registered with Authentication Manager to make token requests via User Credential Manager or to assign tokens and/or ondemand authenticators. This function will permit the registration of a user without assigning an authenticator.

am71 User Actions Register User	
GET	http://10.100.89.138:8080/am71/user/register/<***UserID***>
Request HEADER	
GET /am71/user/register/protester HTTP/1.1 Host: 10.100.89.138:8080 Connection: Keep-Alive	
Request BODY	
n/a	
Response HEADERS	
HTTP/1.1 200 OK Server: Apache-Coyote/1.1 Content-Type: application/xml Transfer-Encoding: chunked Date: Wed, 07 Mar 2012 01:39:43 GMT	
Response BODY	
<?xml version="1.0" encoding="UTF-8" standalone="no"?> <serviceResult result="true"/>	

User Actions – Get Admin Roles

Returns the list of admin roles assigned to a user. Only applicable on AM 7.1 systems.

am71 User Actions – Get Admin Roles	
GET	http://10.100.89.138:8080/am71/user/adminRoles/<***UserID***>

Request HEADER

```
GET /am71/user/adminRoles/admin HTTP/1.1
Host: 10.100.89.138:8080
```

Request BODY

```
n/a
```

Response HEADERS

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: application/xml
Transfer-Encoding: chunked
Date: Wed, 07 Mar 2012 14:24:30 GMT
```

Response BODY

```
<?xml version="1.0" encoding="utf-8" standalone="no"?>
<serviceResult result="true">
  <AdminRoles userName="admin">
    <AdminRole description="Administrative Role used by the SYSTEM for
Trusted Realm Command Execution"
    guid="ims.00000000000000000000001000e0031001"
    isSuperAdminRole="false" name="TrustedRealmAdminRole" />
    <AdminRole description="Admin Role for Super Admin"
    guid="ims.00000000000000000000001000e0031000"
    isSuperAdminRole="true" name="SuperAdminRole" />
  </AdminRoles>
</serviceResult>
```

User Actions – Delete User

UserID is the login UserID of the user account to be deleted. Any assigned tokens will be unassigned automatically.

Note: This method uses the HTTP DELETE verb not GET.

amXX User Actions – Delete User	
DELETE	http://10.100.89.138:8080/amXX/user/delete/<***UserID***>
Request HEADER	

`DELETE /amXX/user/delete/protester2 HTTP/1.1`
`Host: 10.100.89.138:8080`
`Connection: Keep-Alive`	

Request BODY	
`n/a`	
Response HEADERS	

`HTTP/1.1 200 OK`
`Server: Apache-Coyote/1.1`
`Content-Type: application/xml`
`Transfer-Encoding: chunked`
`Date: Wed, 07 Mar 2012 14:46:04 GMT`	

Response BODY	
`<?xml version="1.0" encoding="UTF-8" standalone="no"?>` `<serviceResult result="true"/>`	

User Actions – Get Authentication Activity

Allows for the retrieval of the authentication log details for a user for the last number of configurable minutes on AM 7.1 systems only. Similar to the raw details presented by the real-time authentication activity lodge except it can retrieve historical details.

am71 User Actions – Get Activity	
GET	http://10.100.89.138:8080/am71/user/activity/<UserID>/<minutes>
Request HEADER	
GET /am71/user/activity/protester/60 HTTP/1.1 RSA_AUTHENTICATION_TOKEN: amXXsdkbind Host: 10.100.89.138:8080 Connection: Keep-Alive	
Request BODY	
n/a	
Response HEADERS	
HTTP/1.1 200 OK Server: Apache-Coyote/1.1 Content-Type: application/xml Transfer-Encoding: chunked Date: Wed, 07 Mar 2012 14:56:31 GMT	
Response BODY	

am71 User Actions – Get Activity

```
<?xml version="1.0" encoding="utf-8" standalone="no"?>
<serviceResult result="true">
  <UserActivity Count="3" userID="protester">
    <activities Count="29" id="eda76a248d59640a023baea7ebce8404">
      <Value name="Activity Key">PIN change attempted</Value>
      <Value name="Activity Result Key">Success</Value>
      <Value name="Description">User protester in security domain
      SystemDomain from identity source Internal Database attempted
      to change pin for token serial number 000120881431</Value>
      <Value name="User First Name">Pro</Value>
      <Value name="Actor GUID">
      1d47cdd78d59640a01591c7b76979606</Value>
      <Value name="User ID">protester</Value>
      <Value name="User Identity Source">Internal Database</Value>
      <Value name="User Last Name">Tester</Value>
      <Value name="User Security Domain">SystemDomain</Value>
      <Value name="Agent GUID">
      08003d518d59640a02db2eb9b7c29cd0</Value>
      <Value name="Agent IP">10.100.89.139</Value>
      <Value name="Agent Name">ps-esg-139.ps-esg.com</Value>
      <Value name="Agent Security Domain">SystemDomain</Value>
      <Value name="Agent Type">7</Value>
      <Value name="Argument 2">5</Value>
      <Value name="Argument 3">2</Value>
      <Value name="Argument 8">
      d75aa4c38d59640a0203b154f9bbb2bb</Value>
      <Value name="Argument 9">000120881431</Value>
      <Value name="Authentication Method">SecurID_Native</Value>
      <Value name="Client IP">10.100.89.139</Value>
      <Value name="INSTANCE_ID">
      eb2049468d59640a0035414XX9e388a6</Value>
      <Value name="LOCAL_LOG_TIME">2012-03-07 09:54:26.34</Value>
      <Value name="Log Level">INFO</Value>
      <Value name="RESULT_KEY">AM_PIN_VALID</Value>
      <Value name="Result">PIN change accepted</Value>
      <Value name="Server Node IP">10.100.89.141</Value>
      <Value name="Session ID">
      eda731338d59640a023453d8577cfc99-uHpRmBv/h/iw</Value>
      <Value name="User ID">protester</Value>
      <Value name="UTC_LOG_TIME">2012-03-07 14:54:26.34</Value>
    </activities>
    <activities Count="30" id="eda76a348d59640a023cc51f3755d962">
      <Value name="Activity Key">Principal authentication</Value>
      <Value name="Activity Result Key">Success</Value>
      <Value name="Description">User protester attempted to
      authenticate using authenticator SecurID_Native. The user
      belongs to security domain SystemDomain</Value>
      <Value name="User First Name">Pro</Value>
      <Value name="Actor GUID">
      1d47cdd78d59640a01591c7b76979606</Value>
      <Value name="User ID">protester</Value>
      <Value name="User Identity Source">Internal Database</Value>
      <Value name="User Last Name">Tester</Value>
      <Value name="User Security Domain">SystemDomain</Value>
      <Value name="Agent GUID">
      08003d518d59640a02db2eb9b7c29cd0</Value>
      <Value name="Agent Name">ps-esg-139.ps-esg.com</Value>
      <Value name="Agent Security Domain">SystemDomain</Value>
      <Value name="Agent Type">7</Value>
      <Value name="Argument 1">AUTHN_LOGIN_EVENT</Value>
```

am71 User Actions – Get Activity

```
      <Value name="Agent IP">10.100.89.139</Value>
      <Value name="Agent Name">ps-esg-139.ps-esg.com</Value>
      <Value name="Agent Security Domain">SystemDomain</Value>
      <Value name="Agent Type">7</Value>
      <Value name="Argument 1">AUTHN_LOGIN_EVENT</Value>
      <Value name="Argument 2">5</Value>
      <Value name="Argument 3">2</Value>
      <Value name="Argument 8">
      d75aa4c38d59640a0203b154f9bbb2bb</Value>
      <Value name="Argument 9">000120881431</Value>
      <Value name="Authentication Method">SecurID_Native</Value>
      <Value name="Client IP">10.100.89.139</Value>
      <Value name="INSTANCE_ID">
      eb2049468d59640a0035414XX9e388a6</Value>
      <Value name="LOCAL_LOG_TIME">2012-03-07 09:55:09.09</Value>
      <Value name="Log Level">INFO</Value>
      <Value name="RESULT_KEY">AUTHN_METHOD_SUCCESS</Value>
      <Value name="Result">Authentication method success</Value>
      <Value name="Server Node IP">10.100.89.141</Value>
      <Value name="Session ID">
      eda811028d59640a0256139746c51615-gUA6lVrm/6vq</Value>
      <Value name="User ID">protester</Value>
      <Value name="UTC_LOG_TIME">2012-03-07 14:55:09.09</Value>
    </activities>
  </UserActivity>
</serviceResult>
```

AM 7.1 TDS Token Methods

Token Methods - Enable Token

amXX – Enable Token	
GET	Error! Hyperlink reference not valid.http://10.100.89.138:8080/amXX/token/enable/< ***serialNumber*** >
Request HEADER	
GET /amXX/token/enable/000115876402 HTTP/1.1 Host: 10.100.89.138:8080 Connection: Keep-Alive	
Request BODY	
n/a	
Response HEADERS	
HTTP/1.1 200 OK **Server: Apache-Coyote/1.1** **Content-Type: application/xml** **Transfer-Encoding: chunked** **Date: Tue, 06 Mar 2012 19:47:54 GMT**	
Response BODY	
<?xml version="1.0" encoding="utf-8" standalone="no"?> <serviceResult result="true" />	

Token Methods - DisableToken

amXX Disable Token	
GET	http://10.100.89.138/amXX/token/disable/< ***serialNumber*** >
Request HEADER	
GET /amXX/token/disable/000115876402 HTTP/1.1 Host: 10.100.89.138:8080 Connection: Keep-Alive	
Request BODY	
n/a	
Response HEADERS	
HTTP/1.1 200 OK Server: Apache-Coyote/1.1 Content-Type: application/xml Transfer-Encoding: chunked Date: Tue, 06 Mar 2012 19:54:30 GMT	
Response BODY	
<?xml version="1.0" encoding="utf-8" standalone="no"?> <serviceResult result="true" />	

Token Methods – New Pin Mode

Sets a token into new PIN mode forcing a user to enter a new PIN upon authentication.

amXX Token New Pin	
GET	http://10.100.89.138:8080/amXX/token/newpin/<***serialNumber***>
Request HEADER	
GET /amXX/token/newpin/000115876402 HTTP/1.1 Host: 10.100.89.138:8080 Connection: Keep-Alive	
Request BODY	
n/a	
Response HEADERS	
HTTP/1.1 200 OK Server: Apache-Coyote/1.1 Content-Type: application/xml Transfer-Encoding: chunked Date: Tue, 06 Mar 2012 20:00:10 GMT	
Response BODY	
<?xml version="1.0" encoding="UTF-8" standalone="no"?> <serviceResult result="true"/>	

Token Methods – Un-assign Token

amXX Unassign Token	
GET	http:// 10.100.89.138:8080/amXX/token/unassign/ < ***serialNumber*** >
Request HEADER	
`GET /amXX/token/unassign/000115876402 HTTP/1.1` `Host: 10.100.89.138:8080`	
Request BODY	
n/a	
Response HEADERS	

`HTTP/1.1 200 OK`
`Server: Apache-Coyote/1.1`
`Content-Type: application/xml`
`Transfer-Encoding: chunked`
`Date: Tue, 06 Mar 2012 20:06:22 GMT`	

Response BODY	
`<?xml version="1.0" encoding="UTF-8" standalone="no"?>` `<serviceResult result="true"/>`	

Token Methods – Clear PIN

amXX Clear PIN	
GET	http://10.100.89.138:8080/amXX/token/clearpin/<***serialNumber***>
Request HEADER	

`GET /amXX/token/clearpin/000115876402 HTTP/1.1`
`Host: 10.100.89.138:8080`
`Connection: Keep-Alive`	

Request BODY	
n/a	
Response HEADERS	

`HTTP/1.1 200 OK`
`Server: Apache-Coyote/1.1`
`Content-Type: application/xml`
`Transfer-Encoding: chunked`
`Date: Tue, 06 Mar 2012 20:09:07 GMT`	

Response BODY	
`<?xml version="1.0" encoding="UTF-8" standalone="no"?>` `<serviceResult result="true"/>`	

Token Methods – Token Set Pin

amXX Token Set Pin	
GET	http://10.100.89.138:8080/amXX/token/setpin/<*serialNumber*>?value=<*PIN*>

Request HEADER

```
GET /amXX/token/setpin/000115876402?value=1234 HTTP/1.1
Host: 10.100.89.138:8080
```

Request BODY

```
n/a
```

Response HEADERS

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: application/xml
Transfer-Encoding: chunked
Date: Tue, 06 Mar 2012 20:15:22 GMT
```

Response BODY

```
<?xml version="1.0" encoding="UTF-8" standalone="no"?>
<serviceResult result="true"/>
```

Token Search – User ID

Search Mode determines the search scope, with the following valid options:

- equals
- beginsWith (AM 7.1 only)
- endsWith (AM 7.1 only)
- contains (AM 7.1 only)

Can return one or more users and all their tokens based on the search criteria. Token details are high-level. Equals is the only search mode supported on AM 6.1 systems.

amXX Token Search – UserID - Equals	
GET	http://10.100.89.138:8080/amXX/token/search/UserID/<userID>?searchMode=equals

Request HEADER

```
GET /amXX/token/search/UserID/PROTESTER?searchType=equals HTTP/1.1
Host: 10.100.89.138:8080
Connection: Keep-Alive
```

Request BODY

```
n/a
```

Response HEADERS

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: application/xml
Transfer-Encoding: chunked
Date: Tue, 06 Mar 2012 20:21:07 GMT
```

Response BODY

```
<?xml version="1.0" encoding="utf-8" standalone="no"?>
<serviceResult result="true">
  <TokenSearchResults Count="2">
    <Item>
      <algorithm>AES-TIME</algorithm>
      <assignedUser>protester</assignedUser>
      <expirationDate>2013-01-31T00:00:00-05:00</expirationDate>
      <isCTKIPCapable>true</isCTKIPCapable>
      <isEnabled>true</isEnabled>
      <isPinSet>true</isPinSet>
      <newPinMode>true</newPinMode>
      <pinType>passcode</pinType>
      <tokenSN>000115876402</tokenSN>
      <tokenType>4</tokenType>
    </Item>
    <Item>
      <algorithm>AES-TIME</algorithm>
      <assignedUser>protester</assignedUser>
      <expirationDate>2012-07-31T00:00:00-04:00</expirationDate>
      <isCTKIPCapable>false</isCTKIPCapable>
```

amXX Token Search – UserID - Equals

```
      <isEnabled>true</isEnabled>
      <isPinSet>true</isPinSet>
      <lastLoginDate>2012-03-06T10:32:23.419-05:00</lastLoginDate>
      <newPinMode>false</newPinMode>
      <pinType>passcode</pinType>
      <tokenSN>000120881431</tokenSN>
      <tokenType>9</tokenType>
    </Item>
  </TokenSearchResults>
</serviceResult>
```

Am71 Token Search – UserID – Begins With

GET	http://10.100.89.138:8080/am71/token/search/UserID/<**userIDfragment**>?searchType=**beginsWith**

Request HEADER

```
GET /am71/token/search/UserID/PROT?searchType=beginsWith HTTP/1.1
Host: 10.100.89.138:8080
Connection: Keep-Alive
```

Request BODY

```
n/a
```

Response HEADERS

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: application/xml
Transfer-Encoding: chunked
Date: Tue, 06 Mar 2012 20:24:57 GMT
```

Response BODY

```
<?xml version="1.0" encoding="utf-8" standalone="no"?>
<serviceResult result="true">
  <TokenSearchResults Count="3">
    <Item>
      <algorithm>AES-TIME</algorithm>
      <assignedUser>Protester1</assignedUser>
      <expirationDate>2013-01-31T00:00:00-05:00</expirationDate>
      <isCTKIPCapable>true</isCTKIPCapable>
      <isEnabled>false</isEnabled>
      <isPinSet>true</isPinSet>
      <lastLoginDate>2012-01-11T02:11:39.775-05:00</lastLoginDate>
      <newPinMode>false</newPinMode>
      <pinType>passcode</pinType>
      <tokenSN>000115877321</tokenSN>
      <tokenType>4</tokenType>
    </Item>
    <Item>
      <algorithm>AES-TIME</algorithm>
      <assignedUser>protester</assignedUser>
      <expirationDate>2013-01-31T00:00:00-05:00</expirationDate>
```

Am71 Token Search – UserID – Begins With

```
      <isCTKIPCapable>true</isCTKIPCapable>
      <isEnabled>true</isEnabled>
      <isPinSet>true</isPinSet>
      <newPinMode>true</newPinMode>
      <pinType>passcode</pinType>
      <tokenSN>000115876402</tokenSN>
      <tokenType>4</tokenType>
    </Item>
    <Item>
      <algorithm>AES-TIME</algorithm>
      <assignedUser>protester</assignedUser>
      <expirationDate>2012-07-31T00:00:00-04:00</expirationDate>
      <isCTKIPCapable>false</isCTKIPCapable>
      <isEnabled>true</isEnabled>
      <isPinSet>true</isPinSet>
      <lastLoginDate>2012-03-06T10:32:23.419-05:00</lastLoginDate>
      <newPinMode>false</newPinMode>
      <pinType>passcode</pinType>
      <tokenSN>000120881431</tokenSN>
      <tokenType>9</tokenType>
    </Item>
  </TokenSearchResults>
</serviceResult>
```

am71 Token Search – UserID – Ends With

GET	http://10.100.89.138:8080/am71/token/search/UserID/<**userIDfragment**>?searchType=**endsWith**

Request HEADER

```
GET /am71/token/search/UserID/tester?searchType=endsWith HTTP/1.1
Host: 10.100.89.138:8080
Connection: Keep-Alive
```

Request BODY

```
n/a
```

Response HEADERS

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: application/xml
Transfer-Encoding: chunked
Date: Tue, 06 Mar 2012 20:38:42 GMT
```

Response BODY

```
<?xml version="1.0" encoding="utf-8" standalone="no"?>
<serviceResult result="true">
  <TokenSearchResults Count="2">
    <Item>
      <algorithm>AES-TIME</algorithm>
      <assignedUser>protester</assignedUser>
      <expirationDate>2013-01-31T00:00:00-05:00</expirationDate>
      <isCTKIPCapable>true</isCTKIPCapable>
      <isEnabled>true</isEnabled>
```

am71 Token Search – UserID – Ends With

```
      <isPinSet>true</isPinSet>
      <newPinMode>true</newPinMode>
      <pinType>passcode</pinType>
      <tokenSN>000115876402</tokenSN>
      <tokenType>4</tokenType>
    </Item>
    <Item>
      <algorithm>AES-TIME</algorithm>
      <assignedUser>protester</assignedUser>
      <expirationDate>2012-07-31T00:00:00-04:00</expirationDate>
      <isCTKIPCapable>false</isCTKIPCapable>
      <isEnabled>true</isEnabled>
      <isPinSet>true</isPinSet>
      <lastLoginDate>2012-03-06T10:32:23.419-05:00</lastLoginDate>
      <newPinMode>false</newPinMode>
      <pinType>passcode</pinType>
      <tokenSN>000120881431</tokenSN>
      <tokenType>9</tokenType>
    </Item>
  </TokenSearchResults>
</serviceResult>
```

am71 Token Search – UserID – Contains

GET	http://10.100.89.138:8080/am71/token/search/UserID/<**userIDfragment**>?searchType=**contains**

Request HEADER

```
GET /am71/token/search/UserID/rotest?searchType=contains HTTP/1.1
Host: 10.100.89.138:8080
Connection: Keep-Alive
```

Request BODY

```
n/a
```

Response HEADERS

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: application/xml
Transfer-Encoding: chunked
Date: Tue, 06 Mar 2012 20:43:06 GMT
```

Response BODY

```
<?xml version="1.0" encoding="utf-8" standalone="no"?>
<serviceResult result="true">
  <TokenSearchResults Count="3">
    <Item>
      <algorithm>AES-TIME</algorithm>
      <assignedUser>Protester1</assignedUser>
      <expirationDate>2013-01-31T00:00:00-05:00</expirationDate>
      <isCTKIPCapable>true</isCTKIPCapable>
      <isEnabled>false</isEnabled>
      <isPinSet>true</isPinSet>
      <lastLoginDate>2012-01-11T02:11:39.775-05:00</lastLoginDate>
```

am71 Token Search – UserID – Contains

```
      <newPinMode>false</newPinMode>
      <pinType>passcode</pinType>
      <tokenSN>000115877321</tokenSN>
      <tokenType>4</tokenType>
    </Item>
    <Item>
      <algorithm>AES-TIME</algorithm>
      <assignedUser>protester</assignedUser>
      <expirationDate>2013-01-31T00:00:00-05:00</expirationDate>
      <isCTKIPCapable>true</isCTKIPCapable>
      <isEnabled>true</isEnabled>
      <isPinSet>true</isPinSet>
      <newPinMode>true</newPinMode>
      <pinType>passcode</pinType>
      <tokenSN>000115876402</tokenSN>
      <tokenType>4</tokenType>
    </Item>
    <Item>
      <algorithm>AES-TIME</algorithm>
      <assignedUser>protester</assignedUser>
      <expirationDate>2012-07-31T00:00:00-04:00</expirationDate>
      <isCTKIPCapable>false</isCTKIPCapable>
      <isEnabled>true</isEnabled>
      <isPinSet>true</isPinSet>
      <lastLoginDate>2012-03-06T10:32:23.419-05:00</lastLoginDate>
      <newPinMode>false</newPinMode>
      <pinType>passcode</pinType>
      <tokenSN>000120881431</tokenSN>
      <tokenType>9</tokenType>
    </Item>
  </TokenSearchResults>
</serviceResult>
```

Token Search –Token Serial Number

Search Mode determines the search scope, with the following valid options:

- equals
- beginsWith - (AM 7.1 only)
- endsWith - (AM 7.1 only)
- contains - (AM 7.1 only)

am71 Token Search – Token Serial – Begins With	
GET	http://10.100.89.138:8080/am71/token/search/SerialNumber/<TokenSerial>?searchType=beginsWith

Request HEADER

```
GET /am71/token/search/SerialNumber/00011587640?searchType=beginsWith
HTTP/1.1
Host: 10.100.89.138:8080
Connection: Keep-Alive
```

Request BODY

```
n/a
```

Response HEADERS

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: application/xml
Transfer-Encoding: chunked
Date: Tue, 06 Mar 2012 20:50:42 GMT
```

Response BODY

```
<?xml version="1.0" encoding="utf-8" standalone="no"?>
<serviceResult result="true">
  <TokenSearchResults Count="5">
    <Item>
      <algorithm>AES-TIME</algorithm>
      <assignedUser>tdstester8</assignedUser>
      <expirationDate>2013-01-31T00:00:00-05:00</expirationDate>
      <isCTKIPCapable>true</isCTKIPCapable>
      <isEnabled>true</isEnabled>
      <isPinSet>true</isPinSet>
      <lastLoginDate>2012-03-05T19:07:36.078-05:00</lastLoginDate>
      <newPinMode>false</newPinMode>
      <pinType>passcode</pinType>
      <tokenSN>000115876401</tokenSN>
      <tokenType>4</tokenType>
    </Item>
    <Item>
      <algorithm>AES-TIME</algorithm>
      <assignedUser>protester</assignedUser>
      <expirationDate>2013-01-31T00:00:00-05:00</expirationDate>
      <isCTKIPCapable>true</isCTKIPCapable>
      <isEnabled>true</isEnabled>
      <isPinSet>true</isPinSet>
```

am71 Token Search – Token Serial – Begins With

```
      <newPinMode>true</newPinMode>
      <pinType>passcode</pinType>
      <tokenSN>000115876402</tokenSN>
      <tokenType>4</tokenType>
    </Item>
    <Item>
      <algorithm>AES-TIME</algorithm>
      <assignedUser>stwstoken2</assignedUser>
      <expirationDate>2013-01-31T00:00:00-05:00</expirationDate>
      <isCTKIPCapable>true</isCTKIPCapable>
      <isEnabled>true</isEnabled>
      <isPinSet>false</isPinSet>
      <newPinMode>true</newPinMode>
      <pinType>passcode</pinType>
      <tokenSN>000115876403</tokenSN>
      <tokenType>4</tokenType>
    </Item>
    <Item>
      <algorithm>AES-TIME</algorithm>
      <assignedUser>stwstoken3</assignedUser>
      <expirationDate>2013-01-31T00:00:00-05:00</expirationDate>
      <isCTKIPCapable>true</isCTKIPCapable>
      <isEnabled>true</isEnabled>
      <isPinSet>false</isPinSet>
      <newPinMode>true</newPinMode>
      <pinType>passcode</pinType>
      <tokenSN>000115876404</tokenSN>
      <tokenType>4</tokenType>
    </Item>
    <Item>
      <algorithm>AES-TIME</algorithm>
      <assignedUser>stwstoken4</assignedUser>
      <expirationDate>2013-01-31T00:00:00-05:00</expirationDate>
      <isCTKIPCapable>true</isCTKIPCapable>
      <isEnabled>true</isEnabled>
      <isPinSet>false</isPinSet>
      <newPinMode>true</newPinMode>
      <pinType>passcode</pinType>
      <tokenSN>000115876405</tokenSN>
      <tokenType>4</tokenType>
    </Item>
  </TokenSearchResults>
</serviceResult>
```

am71 Token Search – Token Serial – Ends With	
GET	http://10.100.89.138:8080/am71/token/search/SerialNumber/ <***tokenSerialfragment***>?searchType=***endsWith***

Request HEADER

```
GET /am71/token/search/SerialNumber/115876402?searchType=endsWith
HTTP/1.1
Host: 10.100.89.138:8080
Connection: Keep-Alive
```

Request BODY

```
n/a
```

Response HEADERS

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: application/xml
Transfer-Encoding: chunked
Date: Tue, 06 Mar 2012 20:54:06 GMT
```

Response BODY

```
<?xml version="1.0" encoding="utf-8" standalone="no"?>
<serviceResult result="true">
  <TokenSearchResults Count="1">
    <Item>
      <algorithm>AES-TIME</algorithm>
      <assignedUser>protester</assignedUser>
      <expirationDate>2013-01-31T00:00:00-05:00</expirationDate>
      <isCTKIPCapable>true</isCTKIPCapable>
      <isEnabled>true</isEnabled>
      <isPinSet>true</isPinSet>
      <newPinMode>true</newPinMode>
      <pinType>passcode</pinType>
      <tokenSN>000115876402</tokenSN>
      <tokenType>4</tokenType>
    </Item>
  </TokenSearchResults>
</serviceResult>
```

am71 Token Search – Token Serial – Contains	
GET	http://10.100.89.138:8080/am71/token/search/SerialNumber/ <***tokenSerialfragment***>?searchType=***contains***

Request HEADER

```
GET /am71/token/search/SerialNumber/115876402?searchType=contains
HTTP/1.1
Host: 10.100.89.138:8080
```

Request BODY

```
n/a
```

Response HEADERS

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: application/xml
Transfer-Encoding: chunked
Date: Tue, 06 Mar 2012 20:57:15 GMT
```

Response BODY

```
<?xml version="1.0" encoding="utf-8" standalone="no"?>
<serviceResult result="true">
  <TokenSearchResults Count="1">
    <Item>
      <algorithm>AES-TIME</algorithm>
      <assignedUser>protester</assignedUser>
      <expirationDate>2013-01-31T00:00:00-05:00</expirationDate>
      <isCTKIPCapable>true</isCTKIPCapable>
      <isEnabled>true</isEnabled>
      <isPinSet>true</isPinSet>
      <newPinMode>true</newPinMode>
      <pinType>passcode</pinType>
      <tokenSN>000115876402</tokenSN>
      <tokenType>4</tokenType>
    </Item>
  </TokenSearchResults>
</serviceResult>
```

Token Information Details by User ID

The /token/info functions return full token details based on the search criteria. More details are provided than when using the token search functions. Now includes replacement pairing and token lost status detailsf

amXX Token Information by User ID	
GET	http://10.100.89.138:8080/amXX/token/info/UserID/<*UserID*>

Request HEADER

```
GET /amXX/token/info/UserID/pstester1 HTTP/1.1
Host: 10.100.89.138:8080
```

Request BODY

```
n/a
```

Response HEADERS

```
HTTP/1.1 200 OK
Content-Type: application/xml
Date: Tue, 06 Mar 2012 21:01:34 GMT
```

Response BODY

```
<?xml version="1.0" encoding="utf-8" standalone="no"?>
<serviceResult result="true">
  <TokenInfoResults Count="4">
    <Item replaceTokenPair="000115876439"
    replacementStatus="Original" serialNumber="000115876420"
    temporaryTokenCodeUsed="true" tokenLost="true">
      <algorithm>time</algorithm>
      <assignedTo>pstester1</assignedTo>
      <dateAssigned>2012-10-25T01:49:02.087-04:00</dateAssigned>
      <deviceGuid>ims.00000000000000000000002001f0050014</deviceGuid>
      <deviceName>Generic AES 128 0</deviceName>
      <distribution />
      <expirationDate>2013-01-30T19:00:00-05:00</expirationDate>
      <formFactor>Key FOB</formFactor>
      <formFactor>Software</formFactor>
      <formFactor>SoftID on PC</formFactor>
      <formFactor>SoftID storing seeds on a smart card</formFactor>
      <formFactor>SoftID running on a PDA</formFactor>
      <formFactor>SoftID running (native) on a cell
      phone</formFactor>
      <formFactor>SoftID running (native) on a Java
      card</formFactor>
      <formFactor>SoftID running (native) on a pager</formFactor>
      <formFactor>USB Cosmo token</formFactor>
      <hasBeenUsed>true</hasBeenUsed>
      <interval>60</interval>
      <isEnabled>true</isEnabled>
      <isNewPinMode>true</isNewPinMode>
      <isPinSet>true</isPinSet>
      <lastPinModifiedDate>
      2012-11-05T13:35:41.071-05:00</lastPinModifiedDate>
      <length>8</length>
```

amXX Token Information by User ID

```
      <nextTokenMode>false</nextTokenMode>
      <pinType>passcode</pinType>
      <properties clearValues="false" />
      <startDate>2011-01-05T19:00:00-05:00</startDate>
      <tokenType>4</tokenType>
      <version>0</version>
    </Item>
    <Item replacementStatus="NotPartOfReplacementPair"
    serialNumber="000115876438" temporaryTokenCodeUsed="false"
    tokenLost="false">
      <algorithm>time</algorithm>
      <assignedTo>pstester1</assignedTo>
      <dateAssigned>2012-12-07T17:00:35.400-05:00</dateAssigned>
      <deviceGuid>ims.4df8ae1d655a640a156bdc6dc34e6870</deviceGuid>
      <deviceName>iPhone 1.3</deviceName>
      <distribution>
        <CTKIP activationCode="001069960092"
        serviceAddress="https://psoqa101.proservices-
2.com:7004/ctkip/services/CtkipService"
        triggerURL="https://psoqa101.proservices-
2.com:7004/ctkip/trigger.jsp?authcode=001069960092&amp;url=https://psoqa
101.proservices-2.com:7004/ctkip/services/CtkipService" />
      </distribution>
      <expirationDate>2013-01-30T19:00:00-05:00</expirationDate>
      <formFactor>Key FOB</formFactor>
      <formFactor>Software</formFactor>
      <formFactor>SoftID on PC</formFactor>
      <formFactor>SoftID storing seeds on a smart card</formFactor>
      <formFactor>SoftID running on a PDA</formFactor>
      <formFactor>SoftID running (native) on a cell
      phone</formFactor>
      <formFactor>SoftID running (native) on a Java
      card</formFactor>
      <formFactor>SoftID running (native) on a pager</formFactor>
      <formFactor>USB Cosmo token</formFactor>
      <hasBeenUsed>true</hasBeenUsed>
      <interval>60</interval>
      <isEnabled>true</isEnabled>
      <isNewPinMode>true</isNewPinMode>
      <isPinSet>false</isPinSet>
      <length>8</length>
      <nextTokenMode>false</nextTokenMode>
      <pinType>passcode</pinType>
      <properties clearValues="false">
        <property name="DeviceSerialNumber"
        value="556f1985-33dd-442c-9155-3a0e994f21b1" />
        <property name="Nickname" />
      </properties>
      <startDate>2011-01-05T19:00:00-05:00</startDate>
      <tokenType>4</tokenType>
      <version>0</version>
    </Item>
```

amXX Token Information by User ID

```
    <Item replaceTokenPair="000115876420"
    replacementStatus="Replacement" serialNumber="000115876439"
    temporaryTokenCodeUsed="false" tokenLost="false">
      <algorithm>time</algorithm>
      <assignedTo>pstester1</assignedTo>
      <dateAssigned>2012-12-07T17:03:11.181-05:00</dateAssigned>
      <deviceGuid>ims.17ad9acd655a640a148da84f3d2d3a7c</deviceGuid>
      <deviceName>Android 1.x</deviceName>
      <distribution />
      <expirationDate>2013-01-30T19:00:00-05:00</expirationDate>
      <formFactor>Key FOB</formFactor>
      <formFactor>Software</formFactor>
      <formFactor>SoftID on PC</formFactor>
      <formFactor>SoftID storing seeds on a smart card</formFactor>
      <formFactor>SoftID running on a PDA</formFactor>
      <formFactor>SoftID running (native) on a cell
      phone</formFactor>
      <formFactor>SoftID running (native) on a Java
      card</formFactor>
      <formFactor>SoftID running (native) on a pager</formFactor>
      <formFactor>USB Cosmo token</formFactor>
      <hasBeenUsed>true</hasBeenUsed>
      <interval>60</interval>
      <isEnabled>true</isEnabled>
      <isNewPinMode>false</isNewPinMode>
      <isPinSet>true</isPinSet>
      <lastPinModifiedDate>
      2012-11-05T13:35:41.071-05:00</lastPinModifiedDate>
      <length>8</length>
      <nextTokenMode>false</nextTokenMode>
      <pinType>passcode</pinType>
      <properties clearValues="false">
        <property name="DeviceSerialNumber"
        value="a01c4380-fc01-4df0-b113-7fb98ec74694" />
        <property name="Nickname" />
      </properties>
      <startDate>2011-01-05T19:00:00-05:00</startDate>
      <tokenType>4</tokenType>
      <version>0</version>
    </Item>
    <Item replacementStatus="NotPartOfReplacementPair"
    serialNumber="000110615294" temporaryTokenCodeUsed="false"
    tokenLost="false">
      <algorithm>time</algorithm>
      <assignedTo>pstester1</assignedTo>
      <dateAssigned>2012-12-07T17:01:55.495-05:00</dateAssigned>
      <expirationDate>2014-05-30T16:00:00-04:00</expirationDate>
      <formFactor>Hardware</formFactor>
      <formFactor>Key FOB</formFactor>
      <formFactor>Standard Card</formFactor>
      <formFactor>PINPad Card</formFactor>
      <formFactor>Proteus</formFactor>
```

amXX Token Information by User ID

```
      <formFactor>SoftID on PC</formFactor>
      <formFactor>USB Cosmo token</formFactor>
      <hasBeenUsed>false</hasBeenUsed>
      <interval>60</interval>
      <isEnabled>true</isEnabled>
      <isNewPinMode>true</isNewPinMode>
      <isPinSet>false</isPinSet>
      <lastLogin>1985-12-31T19:00:00-05:00</lastLogin>
      <lastPinModifiedDate>
      2010-12-09T23:47:52-05:00</lastPinModifiedDate>
      <length>6</length>
      <nextTokenMode>false</nextTokenMode>
      <notes>Migrated from AM 6.1.x on Jun 7, 2012</notes>
      <pinType>tokencode</pinType>
      <properties clearValues="false" />
      <startDate>2010-02-16T14:00:00-05:00</startDate>
      <tokenType>2</tokenType>
      <version>0</version>
    </Item>
  </TokenInfoResults>
</serviceResult>
```

Token Information Details by Serial Number

The /token/info functions return full token details based on the search criteria. More details are provided than when using the token search functions.

amXX Token Information By Serial Number	
GET	http:// 10.100.89.138:8080/amXX/token/info/SerialNumber/<*serialNumber*>

Request HEADER

```
GET /amXX/token/info/SerialNumber/000115876402 HTTP/1.1
Host: 10.100.89.138:8080
Connection: Keep-Alive
```

Request BODY

```
n/a
```

Response HEADERS

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: application/xml
Transfer-Encoding: chunked
Date: Tue, 06 Mar 2012 21:24:33 GMT
```

Response BODY

```
<?xml version="1.0" encoding="utf-8" standalone="no"?>
<serviceResult result="true">
  <TokenInfoResults Count="1">
    <Item replaceTokenPair="000115876420"
    replacementStatus="Replacement" serialNumber="000115876439"
    temporaryTokenCodeUsed="false" tokenLost="false">
      <algorithm>time</algorithm>
      <assignedTo>pstester1</assignedTo>
      <dateAssigned>2012-12-07T17:03:11.181-05:00</dateAssigned>
      <deviceGuid>ims.17ad9acd655a640a148da84f3d2d3a7c</deviceGuid>
      <deviceName>Android 1.x</deviceName>
      <distribution />
      <expirationDate>2013-01-30T19:00:00-05:00</expirationDate>
      <formFactor>Key FOB</formFactor>
      <formFactor>Software</formFactor>
      <formFactor>SoftID on PC</formFactor>
      <formFactor>SoftID storing seeds on a smart card</formFactor>
      <formFactor>SoftID running on a PDA</formFactor>
      <formFactor>SoftID running (native) on a cell
      phone</formFactor>
      <formFactor>SoftID running (native) on a Java
      card</formFactor>
      <formFactor>SoftID running (native) on a pager</formFactor>
      <formFactor>USB Cosmo token</formFactor>
      <hasBeenUsed>true</hasBeenUsed>
      <interval>60</interval>
      <isEnabled>true</isEnabled>
      <isNewPinMode>false</isNewPinMode>
      <isPinSet>true</isPinSet>
      <lastPinModifiedDate>
```

amXX Token Information By Serial Number

```
      2012-11-05T13:35:41.071-05:00</lastPinModifiedDate>
      <length>8</length>
      <nextTokenMode>false</nextTokenMode>
      <pinType>passcode</pinType>
      <properties clearValues="false">
        <property name="Nickname" />
        <property name="DeviceSerialNumber"
        value="a01c4380-fc01-4df0-b113-7fb98ec74694" />
      </properties>
      <startDate>2011-01-05T19:00:00-05:00</startDate>
      <tokenType>4</tokenType>
      <version>0</version>
    </Item>
  </TokenInfoResults>
</serviceResult>
```

Replace Token – Keep Existing PIN

Set up a replacement token for an existing token preserving the PIN if possible. Replacing a token with an alphanumeric PIN with a software token in PinPad mode will result in the new token being set in New PIN mode regardless of the newPinMode flag.

amXX Replace Token	
GET	http://10.100.89.138:8080/amXX/token/replace/<***serialNumber***>/ <***replTokSerial***>?newPinMode=False
Request HEADER	

`GET /amXX/token/replace/000115876402/000115877394?newPinMode=False HTTP/1.1`
`Host: 10.100.89.138:8080`
`Connection: Keep-Alive`	

Request BODY	
`n/a`	
Response HEADERS	

`HTTP/1.1 200 OK`
`Server: Apache-Coyote/1.1`
`Content-Type: application/xml`
`Transfer-Encoding: chunked`
`Date: Tue, 06 Mar 2012 21:39:11 GMT`	

Response BODY	
`<?xml version="1.0" encoding="utf-8" standalone="no"?>` `<serviceResult result="true" />`	

The user will need to authenticate with their new token and existing PIN to complete the replacement process.

Replace Token – New Pin Mode

Replaces the current token and places the replacement token in New Pin Mode. When attempting to replace a token set to use an alphanumeric PIN with a software token in PinPad/Passcode mode the replacement token will automatically placed in new PIN mode.

amXX amXX Replace Token – New Pin Mode	
GET	http://10.100.89.138:8080/amXX/token/replace/<***serialNumber***>/ <***replTokSerial***>?newPinMode=True
Request HEADER	

`GET /amXX/token/replace/000115877394/000115876402?newPinMode=True HTTP/1.1`
`Host: 10.100.89.138:8080`
`Connection: Keep-Alive`	

Request BODY	
`n/a`	
Response HEADERS	

`HTTP/1.1 200 OK`
`Server: Apache-Coyote/1.1`
`Content-Type: application/xml`
`Transfer-Encoding: chunked`
`Date: Tue, 06 Mar 2012 21:45:44 GMT`	

Response BODY	
`<?xml version="1.0" encoding="UTF-8" standalone="no"?>` `<serviceResult result="true"/>`	

When authenticating with their new token, they will be required to use their existing PIN to complete the replacement process.

Emergency Access - Lost

Sets a user's token into lost mode and sets a temporary tokencode.

amXX Emergency Access – Lost	
GET	http://10.100.89.138:8080/amXX/token/lost/<***serialNumber***>
Request HEADER	
`GET /amXX/token/lost/000119751886 HTTP/1.1` `Host: 10.100.89.139:8080`	
Request BODY	
`n/a`	
Response HEADERS	

`HTTP/1.1 200 OK`
`Server: Apache-Coyote/1.1`
`Content-Type: application/xml`
`Transfer-Encoding: chunked`
`Date: Fri, 18 May 2012 12:23:10 GMT`	

Response BODY	

`<?xml version="1.0" encoding="utf-8" standalone="no"?>`
`<serviceResult result="true">`
`  <EmergencyAccess temporaryTokenCode="9XX05828"`
`tokenSerialNumber="000119751886" />`
`</serviceResult>`	

Emergency Access - Found

Takes a token out of emergency access mode.

amXX Emergency Access – Found	
GET	http://10.100.89.138:8080/amXX/token/found/<***serialNumber***>
Request HEADER	
`GET /amXX/token/found/000119751886 HTTP/1.1` `Host: 10.100.89.139:8080`	
Request BODY	
`n/a`	
Response HEADERS	

`HTTP/1.1 200 OK`
`Server: Apache-Coyote/1.1`
`Content-Type: application/xml`
`Transfer-Encoding: chunked`
`Date: Fri, 18 May 2012 12:23:20 GMT`	

Response BODY	
`<?xml version="1.0" encoding="UTF-8" standalone="no"?>` `<serviceResult result="true"/>`	

Emergency Access – Temporary Token Code

Parameters are duration in minutes and

- Never allow token Auth
- Allow Token Auth At any time
- Never Allow Token Auth after expiration

The user is "Enabled for Online Emergency Access."

amXX Emergency Access –Temporary Token Code – Never allow token auth	
GET	http://10.100.89.138:8080/amXX/token/emergencyAccess/<***serialNumber***>?lostMode=denytokenauth
Request HEADER	
`GET /amXX/token/emergencyAccess/000119751886/7200?lostMode=denytokenauth HTTP/1.1` `Host: 10.100.89.138:8080`	
Request BODY	
`n/a`	
Response HEADERS	

`HTTP/1.1 200 OK`
`Server: Apache-Coyote/1.1`
`Content-Type: application/xml`
`Transfer-Encoding: chunked`
`Date: Tue, 06 Mar 2012 21:54:10 GMT`	

Response BODY	

`<?xml version="1.0" encoding="utf-8" standalone="no"?>`
`<serviceResult result="true">`
`  <EmergencyAccess temporaryTokenCode="14019867"`
`  tokenSerialNumber="000115877394">`
`  <ExpriationDate>2012-03-06T22:54:10.819-05:00</ExpriationDate>`
`  </EmergencyAccess>`
`</serviceResult>`	

amXX Emergency Access –Temporary Token Code – Allow Token Anytime	
GET	http://10.100.89.138:8080/amXX/token/emergencyAccess/<***serialNumber***>?lostMode=tokenauthdisablesea
Request HEADER	
`GET /amXX/token/emergencyAccess/000115877394/360?lostMode=tokenauthdisablesea HTTP/1.1` `Host: 10.100.89.138:8080`	
Request BODY	
`n/a`	
Response HEADERS	

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: application/xml
Transfer-Encoding: chunked
Date: Tue, 06 Mar 2012 21:54:10 GMT
```

Response BODY

```
<?xml version="1.0" encoding="utf-8" standalone="no"?>
<serviceResult result="true">
    <EmergencyAccess temporaryTokenCode="82372528"
tokenSerialNumber="000119751886">
        <ExpriationDate>2012-05-23T08:24:09.644-04:00</ExpriationDate>
    </EmergencyAccess>
</serviceResult>
```

amXX Emergency Access –Temporary Token Code –Token Auth Onyl After Expiration

GET	http://10.100.89.138:8080/amXX/token/emergencyAccess/<***serialNumber***>?lostMode=tokenonlyafterexpire

Request HEADER

```
GET
/amXX/token/emergencyAccess/000115877394/360?lostMode=tokenonlyafterexpi
re HTTP/1.1
Host: 10.100.89.138:8080
```

Request BODY

```
n/a
```

Response HEADERS

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: application/xml
Transfer-Encoding: chunked
Date: Tue, 06 Mar 2012 21:54:10 GMT
```

Response BODY

```
<?xml version="1.0" encoding="utf-8" standalone="no"?>
<serviceResult result="true">
  <EmergencyAccess temporaryTokenCode="14019867"
  tokenSerialNumber="000115877394">
    <ExpriationDate>2012-03-06T22:54:10.819-05:00</ExpriationDate>
  </EmergencyAccess>
</serviceResult>
```

Token Update/Software Token Distribution

Used to update token details such as device type, number of digits, etc. and distribute the token by generating CT-KIP credentials. If STDID files are to be used, the file will be returned in the response as base64 encoded XML.

In the first example below, a token is updated for WebSDK and PIN-less CT-KIP distribution. The distribution result contains the CT-KIP activation code. Samples applicable to 7.1 are listed as am71 while those applicable to both are amXX

Token Update

am71 - Token – Update

PUT http://192.168.177.42:8080/am71/token/update/<***SerialNumber***>

Request HEADER

```
PUT /am71/token/update/000115876440 HTTP/1.1
Host: 192.168.177.42:8080
```

Request BODY

```
<tokenEntry>
   <enabled>true</enabled>
   <distribution>
      <CTKIP />
   </distribution>
   <deviceType>ims.ee1ecf9c8d59640a03c1eb5498b525bd</deviceType>
   <algorithm>time</algorithm>
   <tokenCodeLength>8</tokenCodeLength>
   <interval>60</interval>
   <properties clearValues="true">
      <property name="TOOLBAR_SITEURL1" value="http://*" />
      <property name="TOOLBAR_SITEURL2" value="https://*" />
      <property name="TOOLBAR_SITEURL3" value="file://*" />
   </properties>
   <pin requirePintAtNextLogin="false" action="nothing"
pinType="tokencode" />
</tokenEntry>
```

Response HEADERS

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: application/xml
Transfer-Encoding: chunked
Date: Wed, 19 Jan 2011 11:40:49 GMT
```

Response BODY

```
<?xml version="1.0" encoding="UTF-8" standalone="no"?>
<serviceResult result="true">
    <distributionResult>0010695631</distributionResult>
</serviceResult>
```

In the example below, the token 000115876439 is updated for CT-KIP deployment, as a Desktop 4.0 soft token. AM 7.1 only.

am71 - Token – Update – Desktop CT-KIP

PUT	http://192.168.177.42:8080/am71/token/update/<***SerialNumber***>

Request HEADER

```
PUT /am71/token/update/000115876439 HTTP/1.1
Host: 192.168.177.42:8080
```

Request BODY

```
<tokenEntry>
   <enabled>true</enabled>
   <distribution>
      <CTKIP />
   </distribution>
   <deviceType>ims.00000000000000000002001f0050000</deviceType>
   <algorithm>time</algorithm>
   <tokenCodeLength>8</tokenCodeLength>
   <interval>60</interval>
   <properties clearValues="true" />
   <pin requirePintAtNextLogin="false" action="nothing"
pinType="tokencode" />
</tokenEntry>
```

Response HEADERS

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: application/xml
Transfer-Encoding: chunked
Date: Wed, 19 Jan 2011 11:40:49 GMT
```

Response BODY

```
<?xml version="1.0" encoding="UTF-8" standalone="no"?>
<serviceResult result="true">
    <distributionResult>001946170812</distributionResult>
</serviceResult>
```

In the example below, the token 000121573740 will be deployed via CT-KIP using a custom activation code, “customactivationcode”, a token nickname, a PIN and bound to the device with ID “72f41af2438caa4bc233a2e6” (see image above).

am71 - Token – Update – iPhone 1.3 With CT-KIP	
PUT	http://192.168.177.42:8080/am71/token/update/<***SerialNumber***>

Request HEADER

```
PUT /am71/token/update/000121573740 HTTP/1.1
Host: 192.168.177.42:8080
```

Request BODY

```
<tokenEntry>
   <enabled>true</enabled>
   <distribution>
      <CTKIP activationCode="customactivationcode" />
   </distribution>
   <deviceType>ims.18e7b5da8d59640a022a08fb2b1a6ca4</deviceType>
   <algorithm>time</algorithm>
   <tokenCodeLength>8</tokenCodeLength>
   <interval>60</interval>
   <properties clearValues="false">
    <property name="DeviceSerialNumber" value="72f41af2438caa4bc233a2e6" />
    <property name="Nickname" value="iphone sample with devicebind" />
   </properties>
   <pin requirePintAtNextLogin="true" action="setPinValue"
pinType="passcode" value="12341234" />
</tokenEntry>
```

Response HEADERS

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: application/xml
Transfer-Encoding: chunked
Date: Wed, 19 Jan 2011 11:40:49 GMT
```

Response BODY

```
<?xml version="1.0" encoding="UTF-8" standalone="no"?>
<serviceResult result="true">
    <distributionResult>customactivationcode</distributionResult>
</serviceResult>
```

The following example is a generic software token format output in SDTID mode compatible with AM 6.1 and 7.1 instances of AMIS.

amXX - Token – Update – AES Generic SDTID File	
PUT	http://192.168.177.42:8080/amXX/token/update/<*SerialNumber*>

Request HEADER

```
PUT /amXX/token/update/000121573740 HTTP/1.1
Host: 192.168.177.42:8080
```

Request BODY

```
<tokenEntry>
   <enabled>true</enabled>
   <distribution>
      <STDID copyProtected="true" regenerateTokenCode="true"
passwordProtect="Password" password="filepassword" />
   </distribution>
   <deviceType>ims.00000000000000000000002001f0050014</deviceType>
   <algorithm>time</algorithm>
   <tokenCodeLength>8</tokenCodeLength>
   <interval>60</interval>
   <properties clearValues="false" />
   <pin requirePintAtNextLogin="true" action="clearPin" pinType="tokencode"
/>
</tokenEntry>
```

Response HEADERS

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: application/xml
Transfer-Encoding: chunked
Date: Wed, 19 Jan 2011 11:40:49 GMT
```

Response BODY

```
<?xml version="1.0" encoding="UTF-8" standalone="no"?>
<serviceResult result="true">
<distributionResult>PD94bWwgdmVyc2lvbj0nMS4wJyBlbmNvZGluZz0iVVRGLTgiPz4NCjx
US05CYXRjaD4NCiAgICA8VEtOSGVhZGVyPg0KICAgIj4wPC
                                    …truncated…
bzQyaEVucE94OWoycnFjc09Xb3N2TnlmbTlud2txSmZodUpDbEx3T3p3NVE9PTwvQmF0Y2hDZXJ
 0aWZpY2F0ZT4NCjwvVEtOVHJhaWxlcj4NCjwvVEtOQmF0Y2g+DQo=</distributionResult>
</serviceResult>
```

The details between the <distributionResult> tags is a base64 encoded SDTID file. The actual valu is truncated above.

List Token Device Types

AM 7.1 only: When using the token update function, the proper IMS token GUID must be used, not the friendly, human readable name. For instance, in the example below the Android token GUID is ims.a0e281bc8d59640a03866f698f53f4cf. The IMS guid value is to use the value just after the family key name. See the highlighted section below.

WARNING: The IMS Guid for Android, iPhone and other tokens will vary on each AM environment as they are generated at runtime during the device type

AM71 Token Device Types

GET http://10.100.89.139:8080/am71/token/devicetypes

Request HEADER

```
GET /am71/token/devicetypes HTTP/1.1
Content-Type: application/xml
Host: 10.100.89.139:8080
Connection: Keep-Alive
```

Request BODY

n/a

Response HEADERS

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: application/xml
Transfer-Encoding: chunked
Date: Sat, 12 Mar 2011 18:16:00 GMT
```

Response BODY

```
<?xml version="1.0" encoding="UTF-8" standalone="no"?>
<serviceResult result="true">
<DeviceTypes Count="18">
<Device>
<attributes>
<Attribute>
<category>TOKEN_SOFT_ANDROID_1.x</category>
<defaultValue>a01c4380-fc01-4df0-b113-7fb98ec74694</defaultValue>
<guid>ims.a0e2816e8d59640a03846fa7dc9c7c18</guid>
<isRequired>false</isRequired>
<name>DeviceSerialNumber</name>
<notes>Android device type or device IMEI or MEID</notes>
<type>STRING</type>
</Attribute>
<Attribute>
<category>TOKEN_SOFT_ANDROID_1.x</category>
<guid>ims.a0e2816e8d59640a038460d8a74001bb</guid>
<isRequired>false</isRequired>
<name>Nickname</name>
<notes>Software Token Nickname</notes>
<type>STRING</type>
</Attribute>
</attributes>
<CTKipCapable>true</CTKipCapable>
<description>RSA SecurID(R) Software Token 1.x for Android(TM)</description>
<familyKey>Android</familyKey>
<guid>ims.a0e281bc8d59640a03866f698f53f4cf</guid>
<labelKey>RSA SecurID(R) Software Token 1.x for Android(TM)</labelKey>
```

AM71 Token Device Types

```
<modifySettings>true</modifySettings>
<pinpad>true|false</pinpad>
<TSFCapable>false</TSFCapable>
<tokenCodeInterval>60|30</tokenCodeInterval>
<tokenCodeLength>8|6</tokenCodeLength>
<tokenCodeType>time</tokenCodeType>
<version>1.x</version>
<XMLCapable>true</XMLCapable>
</Device>
<Device>
<attributes>
<Attribute>
<category>TOKEN_SOFT_PC_4.0</category>
<defaultValue>8f94b026-d362-4554-ac52-3b01fa333b6f</defaultValue>
<guid>ims.00000000000000000000002001f0030013</guid>
<isRequired>false</isRequired>
<name>DeviceSerialNumber</name>
<notes>Software Token Device Serial Number or Device Type</notes>
<type>STRING</type>
</Attribute>
<Attribute>
<category>TOKEN_SOFT_PC_4.0</category>
<guid>ims.00000000000000000000002001f0030012</guid>
<isRequired>false</isRequired>
<name>Nickname</name>
<notes>Software Token Nickname</notes>
<type>STRING</type>
</Attribute>
</attributes>
<CTKipCapable>true</CTKipCapable>
<description>RSA SecurID(R) Token 4.0 for Windows(R) Desktops</description>
<familyKey>Desktop PC</familyKey>
<guid>ims.00000000000000000000002001f0050000</guid>
<labelKey>SWT_DESKTOP</labelKey>
<modifySettings>true</modifySettings>
<pinpad>true|false</pinpad>
<TSFCapable>false</TSFCapable>
<tokenCodeInterval>60|30</tokenCodeInterval>
<tokenCodeLength>8|6</tokenCodeLength>
<tokenCodeType>time</tokenCodeType>
<version>4.0</version>
<XMLCapable>true</XMLCapable>
</Device>
<Device>
<attributes>
<Attribute>
<category>TOKEN_SOFT_PC_128BIT_3.0.x</category>
<guid>ims.00000000000000000000002001f0030014</guid>
<isRequired>false</isRequired>
<name>Nickname</name>
<notes>Software Token Nickname</notes>
<type>STRING</type>
</Attribute>
</attributes>
<CTKipCapable>false</CTKipCapable>
<description>(Passcode) RSA SecurID(R) Token 3.0.x for Windows(R) Desktops(AES 128-
bit)</description>

......
```

Create / Update User

List Identity Source

This method is available on AM 7.1 systems only.

am71 – List Identity Source	
GET	http://10.100.89.138:8080/am71/info/identitySources

Request HEADER

```
GET /am71/info/identitySources HTTP/1.1
Host: 10.100.89.138:8080
```

Request BODY

```
n/a
```

Response HEADERS

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: application/xml
Transfer-Encoding: chunked
Date: Wed, 07 Mar 2012 18:10:27 GMT
```

Response BODY

```
<?xml version="1.0" encoding="utf-8" standalone="no"?>
<serviceResult result="true">
  <IdentitySources Count="2">
    <IdentitySource displayName="System Identity Source Oracle"
    id="ims.00000000000000000000001000d0011000"
    name="Internal Database" />
    <IdentitySource id="ims.76c6be338d59640a03939631c937cd1a"
    name="proservices2" />
  </IdentitySources>
</serviceResult>
```

Create User

The **Create User** function can create the user as enabled or disabled and loaded with optional Custom Atributes (AM 7.1 only):

- Activation Code - (AM 7.1 only)
- Alternate Email - (AM 7.1 only)
- Phone - (AM 7.1 only)
- SMS Email Provider – (AM 7.1 only)
- VPN Certification - (AM 7.1 only)

The Email Address and Password fields are optional.

The first example uses standard attributes available in 6.1 and 7.1 systems.

AmXX – Create User	
PUT	http://10.100.89.138:8080/amXX/user/create/<***userID***>
Request HEADER	
PUT /amXX/user/create/jimtester5 HTTP/1.1 Content-Type: application/xml Host: 10.100.89.138:8080 Content-Length: 218 Expect: 100-continue	
Request BODY	
<userEntry> <firstName>Jim</firstName> <lastName>Tester5</lastName> <enabled>true</enabled> </userEntry>	
Response HEADERS	
HTTP/1.1 200 OK Server: Apache-Coyote/1.1 Content-Type: application/xml Transfer-Encoding: chunked Date: Wed, 07 Mar 2012 18:26:35 GMT	
Response BODY	
<?xml version="1.0" encoding="UTF-8" standalone="no"?> <serviceResult result="true"/>	

Example for AM 7.1 system with custom attributes.

am71 – Create User

PUT http://10.100.89.138:8080/am71/user/create/<***userID***>

Request HEADER

```
PUT /am71/user/create/jimtester7 HTTP/1.1
Content-Type: application/xml
Host: 10.100.89.138:8080
Content-Length: 218
Expect: 100-continue
```

Request BODY

```
<userEntry>
      <emailAddress>jimtester7@rsa.com</emailAddress>
      <firstName>Jim</firstName>
      <lastName>Tester7</lastName>
      <enabled>true</enabled>
      <CustomAttributes>
            <attribute name="COUNTRY">
                  <values>
                        <value>USA</value>
                  </values>
            </attribute>
      </CustomAttributes>
</userEntry>
```

Response HEADERS

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: application/xml
Transfer-Encoding: chunked
Date: Wed, 07 Mar 2012 18:26:35 GMT
```

Response BODY

```
<?xml version="1.0" encoding="UTF-8" standalone="no"?>
<serviceResult result="true"/>
```

Update User

The **Update User** function can enable or disable the specified user account and update with the following attributes:

- Email Address
- Password
- Activation Code
- Alternate Email
- Phone
- SMS Email Provider
- VPN Certification

AmXX – Update User
PUT http://10.100.89.138:8080/amXX/user/update/<***userID***>
Request HEADER

`PUT /amXX/user/update/jimtester5 HTTP/1.1`
`Content-Type: application/xml`
`Host: 10.100.89.138:8080`
`Content-Length: 308`
`Expect: 100-continue`

Request BODY

`<userEntry>`
`  <firstName>Jim5</firstName>`
`  <lastName>Tester5</lastName>`
`  <enabled>true</enabled>`
`</userEntry>`

Response HEADERS

`HTTP/1.1 200 OK`
`Server: Apache-Coyote/1.1`
`Content-Type: application/xml`
`Transfer-Encoding: chunked`
`Date: Wed, 07 Mar 2012 18:50:54 GMT`

Response BODY
`<?xml version="1.0" encoding="UTF-8" standalone="no"?>` `<serviceResult result="true"/>`

Load Custom Attributes

AM 7.1 only.

am71 – Load Custom Attributes	
GET	http://10.100.89.138:8080/am71/user/attributeDefinitions

Request HEADER

```
GET /am71/user/attributeDefinitions HTTP/1.1
Host: 10.100.89.138:8080
Connection: Keep-Alive
```

Request BODY

```
n/a
```

Response HEADERS

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: application/xml
Transfer-Encoding: chunked
Date: Wed, 07 Mar 2012 18:52:56 GMT
```

Response BODY

```
<?xml version="1.0" encoding="utf-8" standalone="no"?>
<serviceResult result="true">
  <UserCustomAttributeDefinitions>
    <AttributeDefinition category="Attributes" dataType="String"
    isMultiValued="false" isReadOnly="false" isRequired="false"
    name="ActivationCode" />
    <AttributeDefinition category="Attributes" dataType="String"
    isMultiValued="false" isReadOnly="false" isRequired="false"
    name="AlternateEmail" />
    <AttributeDefinition category="Attributes" dataType="String"
    isMultiValued="false" isReadOnly="false" isRequired="false"
    name="phone" />
    <AttributeDefinition category="Attributes" dataType="String"
    isMultiValued="false" isReadOnly="false" isRequired="false"
    name="SMSEmailProvider" />
    <AttributeDefinition category="Attributes" dataType="String"
    isMultiValued="false" isReadOnly="false" isRequired="false"
    name="VPNCertification" />
  </UserCustomAttributeDefinitions>
</serviceResult>
```

Update Token (XML Builder)

Token Update- Update Token

NOTE: CT-KIP distribution is only applicable for AM 7.1 systems.

Used to update token details such as device type, number of digits, etc. and distribute the token by generating CT-KIP credentials. If STDID files are to be used, the file will be returned in the response as XML.

Token Update is used to set the PIN Properties; Require PIN at next login, Clear PIN, and Set PIN. The specified token can also be enabled.

In the first example below, a token is updated for WebSDK and PIN-less CT-KIP distribution. The distribution result contains the CT-KIP activation code.

amXX - Token – Update Token Distribution

PUT http://192.168.177.42:8080/amXX/token/update/<***SerialNumber***>

Request HEADER

```
PUT /amXX/token/update/000115876440 HTTP/1.1
Host: 192.168.177.42:8080
```

Request BODY

```
<tokenEntry>
   <enabled>true</enabled>
   <distribution>
      <CTKIP />
   </distribution>
   <deviceType>ims.ee1ecf9c8d59640a03c1eb5498b525bd</deviceType>
   <algorithm>time</algorithm>
   <tokenCodeLength>8</tokenCodeLength>
   <interval>60</interval>
   <properties clearValues="true">
      <property name="TOOLBAR_SITEURL1" value="http://*" />
   </properties>
   <pin requirePintAtNextLogin="false" action="nothing"
pinType="tokencode" />
</tokenEntry>
```

Response HEADERS

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: application/xml
Transfer-Encoding: chunked
Date: Wed, 19 Jan 2011 11:40:49 GMT
```

Response BODY

```
<?xml version="1.0" encoding="UTF-8" standalone="no"?>
<serviceResult result="true">
    <distributionResult>0010695631</distributionResult>
</serviceResult>
```

In the example below, the token 000115876439 is updated for CT-KIP deployment, as a Desktop 4.0 soft token.

Request HEADER

```
PUT /amXX/token/update/000115876439 HTTP/1.1
Host: 192.168.177.42:8080
```

Request BODY

```
<tokenEntry>
   <enabled>true</enabled>
   <distribution>
      <CTKIP />
   </distribution>
   <deviceType>ims.00000000000000000002001f0050000</deviceType>
   <algorithm>time</algorithm>
   <tokenCodeLength>8</tokenCodeLength>
   <interval>60</interval>
   <properties clearValues="true" />
   <pin requirePintAtNextLogin="false" action="nothing"
pinType="tokencode" />
</tokenEntry>
```

Response HEADERS

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: application/xml
Transfer-Encoding: chunked
Date: Wed, 19 Jan 2011 11:40:49 GMT
```

Response BODY

```
<?xml version="1.0" encoding="UTF-8" standalone="no"?>
<serviceResult result="true">
    <distributionResult>001946170812</distributionResult>
</serviceResult>
```

Token Update – PIN Properties

Update Pin Properties offers the following options:

- Require PIN at next login
- Clear PIN
- Set PIN

In the second example below, a token is updated for Desktop PC 4.0 and CT-KIP distribution. The distribution result contains the CT-KIP activation code.
The PIN is set to a value{1234}.

amXX - Token – Update Token PIN Properties

PUT http://10.100.89.138:8080/amXX/token/update/<***serialNumber***>

Request HEADER

```
PUT /amXX/token/update/000115877394 HTTP/1.1
Content-Type: application/xml
Host: 10.100.89.138:8080
Content-Length: 572
Expect: 100-continue
Connection: Keep-Alive
```

Request BODY

```
<tokenEntry>
      <enabled>false</enabled>
      <distribution>
            <CTKIP />
      </distribution>
      <deviceType>ims.00000000000000000002001f0050000</deviceType>
      <algorithm>time</algorithm>
      <tokenCodeLength>6</tokenCodeLength>
      <interval>60</interval>
      <properties clearValues="false">
            <property name="DeviceSerialNumber" value="8f94b026-d362-
4554-ac52-3b01fa333b6f" />
      </properties>
      <pin requirePintAtNextLogin="false" action="setPinValue"
pinType="passcode" value="1234" />
</tokenEntry>
```

Response HEADERS

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: application/xml
Transfer-Encoding: chunked
Date: Thu, 08 Mar 2012 18:33:00 GMT
```

Response BODY

```
<?xml version="1.0" encoding="utf-8" standalone="no"?>
<serviceResult result="true">
  <distributionResult>001279011835</distributionResult>
</serviceResult
```

Token Update – Enable Token

amXX - Token – Update Token Disable Token	
PUT	http://10.100.89.138:8080/amXX/token/update/<*serialNumber*>

Request HEADER

```
PUT /amXX/token/update/000120881431 HTTP/1.1
Content-Type: application/xml
Host: 10.100.89.138:8080
Content-Length: 427
Expect: 100-continue
```

Request BODY

```
<tokenEntry>
      <enabled>true</enabled>
      <deviceType>ims.00000000000000000000002001f0050000</deviceType>
      <algorithm>time</algorithm>
      <tokenCodeLength>6</tokenCodeLength>
      <interval>60</interval>
      <properties clearValues="false">
            <property name="DeviceSerialNumber" value="8f94b026-d362-
4554-ac52-3b01fa333b6f" />
      </properties>
      <pin requirePintAtNextLogin="false" action="nothing"
pinType="passcode" />
```

Response HEADERS

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: application/xml
Transfer-Encoding: chunked
Date: Thu, 08 Mar 2012 18:47:19 GMT
```

Response BODY

```
<?xml version="1.0" encoding="UTF-8" standalone="no"?>
<serviceResult result="true"/>
```

TDS Session Statistics - /amXX/info/statistics

Session Statistics

TDS Session Statistics

GET http://10.100.89.139:8080/amXX/info/statistics

Request HEADER

```
GET /amXX/info/statistics HTTP/1.1
Content-Type: application/xml
Host: 10.100.89.139:8080
Connection: Keep-Alive
```

Request BODY

n/a

Response HEADERS

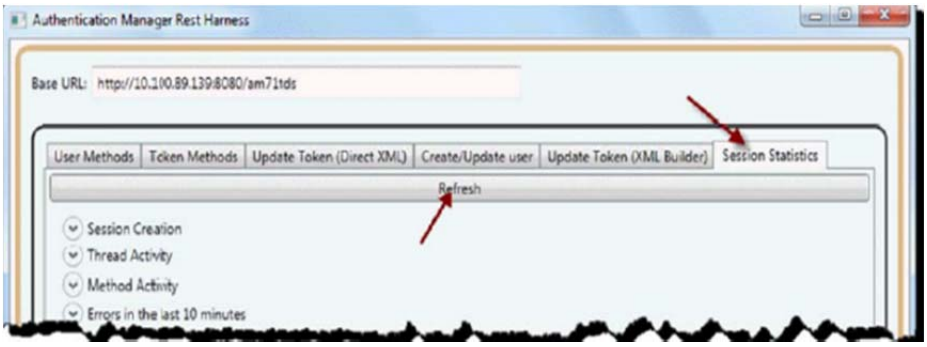
```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: application/xml
Transfer-Encoding: chunked
Date: Sat, 12 Mar 2011 18:16:00 GMT
```

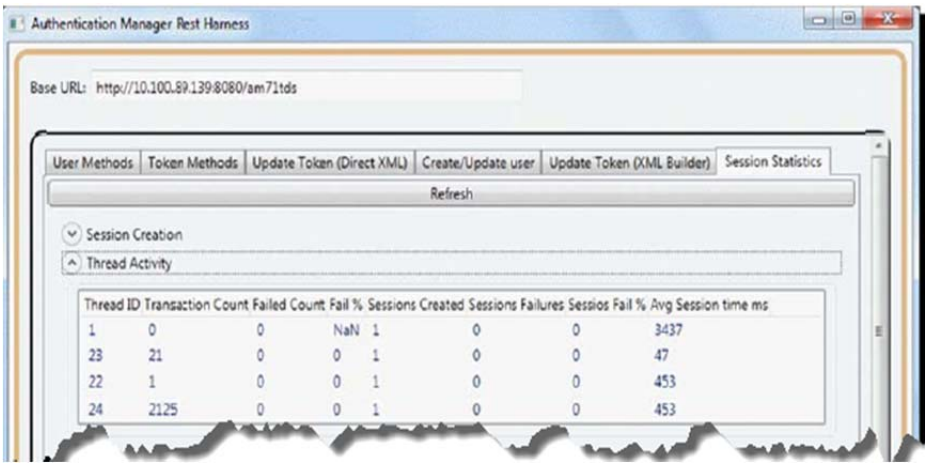
Response BODY

```
<?xml version="1.0" encoding="UTF-8" standalone="no"?>
<serviceResult result="true">
<ResultLog totalSessionCreateTime="4390" totalSessionCreatonFailures="0"
totalSessionsCreated="4">
<threadActivity threadID="1" totalFailedTransactions="0"
totalSessionCreateTime="3437"
totalSessionCreatonFailures="0" totalSessionsCreated="1" totalTransactions="0"/>
<threadActivity threadID="23" totalFailedTransactions="0"
totalSessionCreateTime="47"
totalSessionCreatonFailures="0" totalSessionsCreated="1" totalTransactions="21"/>
<threadActivity threadID="22" totalFailedTransactions="0"
totalSessionCreateTime="453"
totalSessionCreatonFailures="0" totalSessionsCreated="1" totalTransactions="1"/>
<threadActivity threadID="24" totalFailedTransactions="0"
totalSessionCreateTime="453"
totalSessionCreatonFailures="0" totalSessionsCreated="1"
totalTransactions="2125"/>
<transactionDetails count="3" failure="0" method="userAssignToken"
totalTime="345"/>
<transactionDetails count="2" failure="0" method="tokenClearPin" totalTime="125"/>
<transactionDetails count="1" failure="0" method="userCreate" totalTime="219"/>
<transactionDetails count="1" failure="0" method="tokenSetPin" totalTime="78"/>
<transactionDetails count="3" failure="0" method="tokenSearch" totalTime="2764"/>
<transactionDetails count="4" failure="0" method="userSearch" totalTime="4438"/>
<transactionDetails count="2123" failure="0" method="tokenInfo"
totalTime="66598"/>
<transactionDetails count="1" failure="0" method="tokenUpdate" totalTime="578"/>
<transactionDetails count="1" failure="0" method="userDelete" totalTime="500"/>
<transactionDetails count="2" failure="0" method="tokenUnassign" totalTime="172"/>
<transactionDetails count="2" failure="0" method="setUserEnabledState"
totalTime="125"/>
<transactionDetails count="2" failure="0" method="setTokenEnabledState"
```

TDS Session Statistics

```
totalTime="109"/>
<transactionDetails count="2" failure="0" method="listDeviceTypes"
totalTime="343"/>
</ResultLog>
</serviceResult>
```





Authenticate

Authentication

auth – authenticate	
GET	http://<servername:port>/auth/authenticate/<*userID*>/<*passcode*>

Request HEADER

```
GET /auth/authenticate/tdstester8/31020507 HTTP/1.1
Host: 10.100.89.138:8080
Connection: Keep-Alive
```

Request BODY

```
n/a
```

Response HEADERS

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: application/xml
Transfer-Encoding: chunked
Date: Fri, 09 Mar 2012 23:28:38 GMT
```

Response BODY

```
<?xml version="1.0" encoding="utf-8" standalone="no"?>
<authenticationResult>
  <authenticated>true</authenticated>
  <authenticationToken>17363893</authenticationToken>
  <code>0</code>
  <message>ACCESS_OK</message>
</authenticationResult>
```

Authorization

auth – authorization	
GET	http(s)://<servername:port>/auth/<*sessionToken*>/<*AppID*>
Request HEADER	
GET /auth/authorization/App1 HTTP/1.1 RSA_AUTHENTICATION_TOKEN: 17363893 Host: 10.100.89.138:8080 Connection: Keep-Alive	
Request BODY	
n/a	
Response HEADERS	
HTTP/1.1 200 OK Server: Apache-Coyote/1.1 Content-Type: application/xml Transfer-Encoding: chunked Date: Fri, 09 Mar 2012 23:32:33 GMT	
Response BODY	
<?xml version="1.0" encoding="UTF-8" standalone="no"?> <serviceResult result="true"/>	

Validation

auth –Validate	
GET	http(s)://<servername:port>/auth/validate/<*sessionToken*>
Request HEADER	
GET /auth/validate/70823173 HTTP/1.1 Host: 10.100.89.138:8080	
Request BODY	
url: http://10.100.89.138:8080/auth/validate/70823173 <?xml version="1.0" encoding="UTF-8" standalone="no"?> <tokenValidationResult> <isValid>true</isValid> <token>70823173</token> <userID>tdstester8</userID> </tokenValidationResult>	
Response HEADERS	
HTTP/1.1 200 OK Server: Apache-Coyote/1.1 Content-Type: application/xml Transfer-Encoding: chunked Date: Fri, 09 Mar 2012 23:16:51 GMT	
Response BODY	

```
<?xml version="1.0" encoding="UTF-8" standalone="no"?>
<tokenValidationResult>
<isValid>true</isValid>
<token>70823173</token>
<userID>tdstester8</userID>
</tokenValidationResult>
```

New Pin Mode

Authentication – Result New PIN Required

auth – authenticate – New PIN required	
GET	http(s://<servername:port>/auth/authenticate/<*userID*>/<*passcode*>

Request HEADER

```
GET /auth/authenticate/tdstester8/31020507 HTTP/1.1
Host: 10.100.89.138:8080
Connection: Keep-Alive
```

Request BODY

```
n/a
```

Response HEADERS

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: application/xml
Transfer-Encoding: chunked
Date: Fri, 09 Mar 2012 23:28:38 GMT
```

Response BODY

```
<?xml version="1.0" encoding="utf-8" standalone="no"?>
<authenticationResult>
    <PinConfiguration isAlphanumeric="false" maxPinLength="8"
minPinLength="4" userSelectable="MustChoosePin" />
    <authenticated>false</authenticated>
    <authenticationToken>36287693</authenticationToken>
    <code>5</code>
    <failed>false</failed>
    <message>NEW_PIN_REQUIRED</message>
</authenticationResult>
```

Set PIN in Response to New PIN

Get System Generated PIN	
PUT	http(s)://<servername:port>/auth/pin/<*sessionToken*>

Request HEADER

```
PUT /auth/pin HTTP/1.1
Content-Type: application/xml
Host: 10.100.89.139:8080
Content-Length: 39
Expect: 100-continue
```

Request BODY

```
<Pin pin="11223344" token="36287693" />
```

Response HEADERS

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: application/xml
Transfer-Encoding: chunked
Date: Tue, 15 May 2012 18:42:48 GMT
```

Response BODY

```
<?xml version="1.0" encoding="utf-8" standalone="no"?>
<authenticationResult>
    <authenticated>false</authenticated>
    <code>6</code>
    <failed>false</failed>
    <message>PIN_ACCEPTED</message>
</authenticationResult>
```

Next Tokencode Required

Authentication – Result Next Tokencode Required

Authenticate – Response is Next Token Code
GET http://10.100.89.138:8080/auth/authenticate/<**userID**>/<**passcode**>
Request HEADER
GET /auth/authenticate/tdstester8/31020507 HTTP/1.1 Host: 10.100.89.138:8080 Connection: Keep-Alive
Request BODY
n/a
Response HEADERS
HTTP/1.1 200 OK Server: Apache-Coyote/1.1 Content-Type: application/xml Transfer-Encoding: chunked Date: Tue, 15 May 2012 18:42:48 GMT
Response BODY
<?xml version="1.0" encoding="utf-8" standalone="no"?> <authenticationResult> <authenticated>false</authenticated> <authenticationToken>**43682633**</authenticationToken> <code>2</code> <failed>false</failed> <message>NEXT_CODE_REQUIRED</message> </authenticationResult>

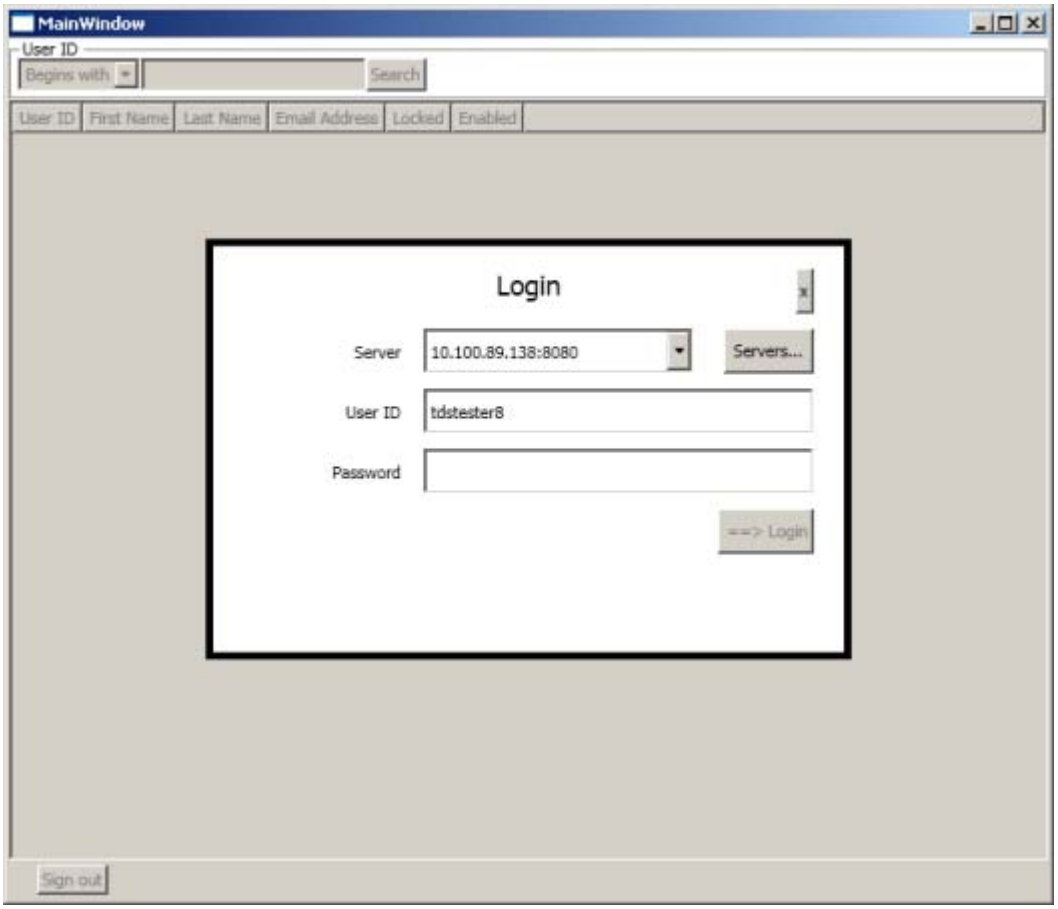
Next Tokencode

Next Token Code	
GET	http://10.100.89.138:8080/auth/next/<**authtoken**>/<**tokencode**>
Request HEADER	
GET /auth/next/**43682633**/59985209 HTTP/1.1 Host: 10.100.89.138:8080 Connection: Keep-Alive	
Request BODY	
n/a	
Response HEADERS	
HTTP/1.1 200 OK Server: Apache-Coyote/1.1 Content-Type: application/xml Transfer-Encoding: chunked Date: Fri, 18 May 2012 16:06:15 GMT	
Response BODY	
<?xml version="1.0" encoding="UTF-8" standalone="no"?> <authenticationResult> <authenticated>true</authenticated> <authenticationToken>**38289113**</authenticationToken> <code>0</code> <failed>false</failed> <message>ACCESS_OK</message> </authenticationResult>	

Note that in the successful response to a next tokencode event is a new AMIS authentication token replacing the one generated in the initial authentication. Use this new value for any addition authentication if using AMIS security.

HelpDesk.exe - Endpoint

Login



Endpoints	
GET	http(s)://<servername:port/rsa-endpoints/endpoints

Request HEADER

```
GET /rsa-endpoints/endpoints HTTP/1.1
Host: 10.100.89.138:8080
Connection: Keep-Alive
```

Request BODY

```
n/a
```

Response HEADERS

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: application/xml
Transfer-Encoding: chunked
Date: Mon, 12 Mar 2012 17:54:19 GMT
```

Endpoints

Response BODY

```
<?xml version="1.0" encoding="utf-8" standalone="no"?>
<serviceResult result="true">
  <Endpoints>
    <Endpoint endpointType="Authentication">
    http://10.100.89.138:8080/auth</Endpoint>
    <Endpoint endpointType="TDS">
    http://10.100.89.138:8080/amXX</Endpoint>
  </Endpoints>
</serviceResult>
```

Login

GET `http(s)://<servername:port>/auth/authenticate/<userID>/<tokenCode>`

Request HEADER

```
GET /auth/authenticate/tdstester8/84492887 HTTP/1.1
Host: 10.100.89.138:8080
```

Request BODY

```
n/a
```

Response HEADERS

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: application/xml
Transfer-Encoding: chunked
Date: Mon, 12 Mar 2012 15:22:58 GMT
```

Response BODY

```
<?xml version="1.0" encoding="utf-8" standalone="no"?>
<authenticationResult>
  <authenticated>true</authenticated>
  <authenticationToken>79XX5233</authenticationToken>
  <code>0</code>
  <message>ACCESS_OK</message>
</authenticationResult>
```

Search UserID

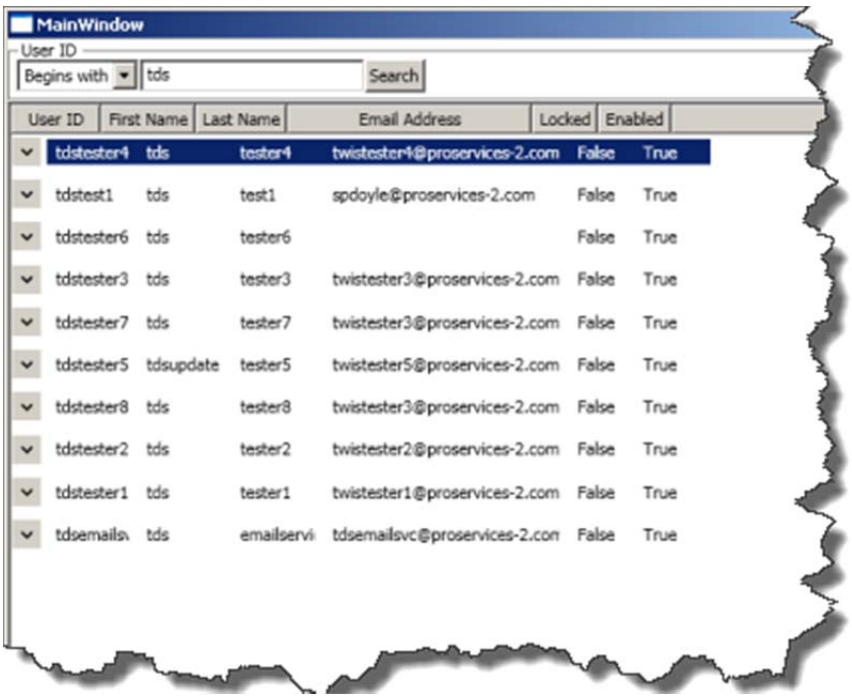
UserSearchString is a wildcard searchable value on the userID.

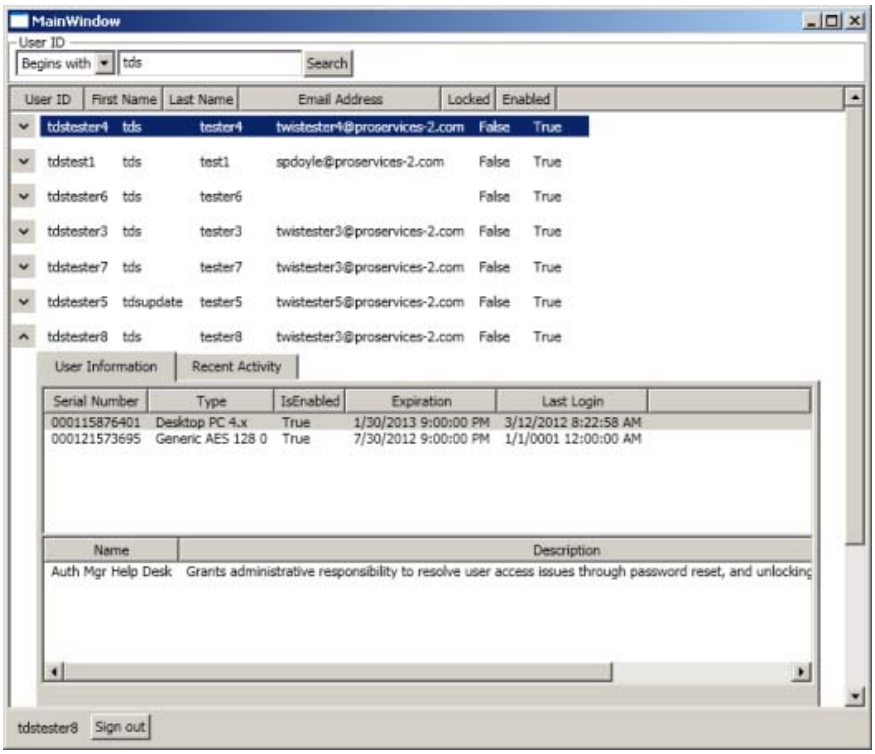
SearchType determines the search scope, valid options include

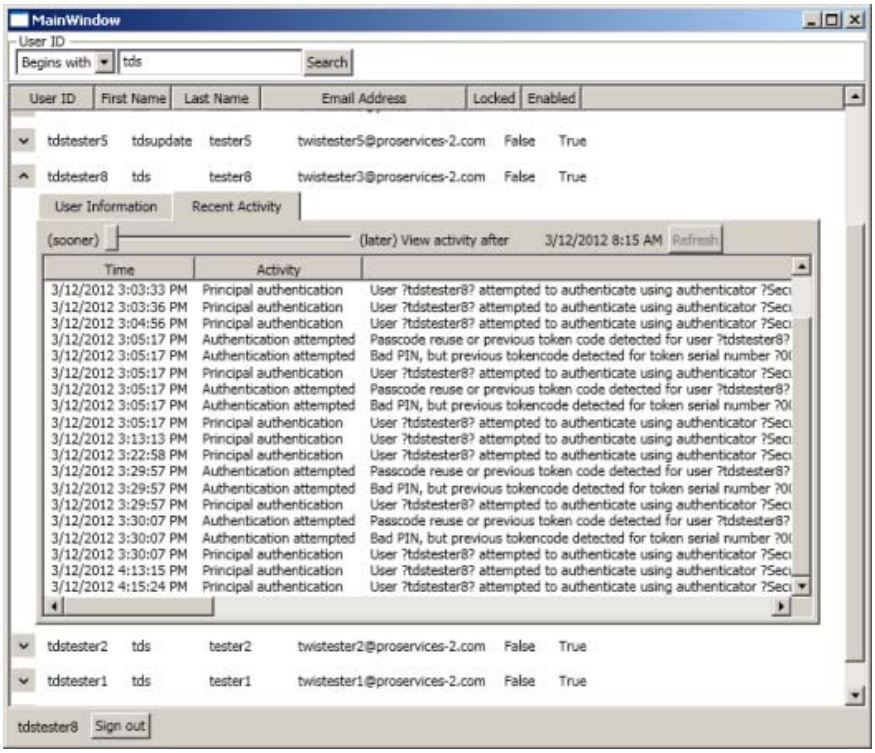
- equals
- beginsWith
- endsWith
- contains

Search User ID	
GET	http(s)://<servername:port/amXX/user/search/<*UserSearchString*>?searchType=<*SearchType*>
Request HEADER	
GET /amXX/user/search/tester8?searchType=endsWith HTTP/1.1 RSA_AUTHENTICATION_TOKEN: 79XX5233 Host: 10.100.89.138:8080 Connection: Keep-Alive	
Request BODY	
n/a	
Response HEADERS	
HTTP/1.1 200 OK Server: Apache-Coyote/1.1 Content-Type: application/xml Transfer-Encoding: chunked Date: Mon, 12 Mar 2012 15:34:37 GMT	
Response BODY	

```
<?xml version="1.0" encoding="utf-8" standalone="no"?>
<serviceResult result="true">
  <UserSearchResults Count="1">
    <Item isRegistered="true">
      <CustomAttributes>
        <attribute name="ActivationCode">
          <values>
            <value>activationcode--timestamp</value>
          </values>
        </attribute>
        <attribute name="VPNCertification">
          <values>
            <value>newtimestamp</value>
          </values>
        </attribute>
      </CustomAttributes>
      <emailAddress>twistester3@proservices-2.com</emailAddress>
      <firstName>tds</firstName>
      <isEnabled>true</isEnabled>
      <isLocked>false</isLocked>
      <lastName>tester8</lastName>
      <userID>tdstester8</userID>
    </Item>
  </UserSearchResults>
</serviceResult>
```




MainWindow
User ID
Begins with
tds
Search
User ID
First Name
Last Name
Email Address
Locked
Enabled
tdstester4 tds tester4 twistester4@proservices-2.com False True
tdstest1 tds test1 spdoyle@proservices-2.com False True
tdstester6 tds tester6 False True
tdstester3 tds tester3 twistester3@proservices-2.com False True
tdstester7 tds tester7 twistester3@proservices-2.com False True
tdstester5 tdsupdate tester5 twistester5@proservices-2.com False True
tdstester8 tds tester8 twistester3@proservices-2.com False True
User Information
Recent Activity
Serial Number
Type
IsEnabled
Expiration
Last Login
000115876401 Desktop PC 4.x True 1/30/2013 9:00:00 PM 3/12/2012 8:22:58 AM
000121573695 Generic AES 128 0 True 7/30/2012 9:00:00 PM 1/1/0001 12:00:00 AM
Name
Description
Auth Mgr Help Desk Grants administrative responsibility to resolve user access issues through password reset, and unlocking
tdstester8
Sign out


MainWindow
User ID
Begins with
tds
Search
User ID
First Name
Last Name
Email Address
Locked
Enabled
tdstester5 tdsupdate tester5 twistester5@proservices-2.com False True
tdstester8 tds tester8 twistester3@proservices-2.com False True
User Information
Recent Activity
(sooner)
(later) View activity after
3/12/2012 8:15 AM
Refresh
Time
Activity
3/12/2012 3:03:33 PM Principal authentication User ?tdstester8? attempted to authenticate using authenticator ?Secu
3/12/2012 3:03:36 PM Principal authentication User ?tdstester8? attempted to authenticate using authenticator ?Secu
3/12/2012 3:04:56 PM Principal authentication User ?tdstester8? attempted to authenticate using authenticator ?Secu
3/12/2012 3:05:17 PM Authentication attempted Passcode reuse or previous token code detected for user ?tdstester8?
3/12/2012 3:05:17 PM Authentication attempted Bad PIN, but previous tokencode detected for token serial number ?0(
3/12/2012 3:05:17 PM Principal authentication User ?tdstester8? attempted to authenticate using authenticator ?Secu
3/12/2012 3:05:17 PM Authentication attempted Passcode reuse or previous token code detected for user ?tdstester8?
3/12/2012 3:05:17 PM Authentication attempted Bad PIN, but previous tokencode detected for token serial number ?0(
3/12/2012 3:05:17 PM Principal authentication User ?tdstester8? attempted to authenticate using authenticator ?Secu
3/12/2012 3:13:13 PM Principal authentication User ?tdstester8? attempted to authenticate using authenticator ?Secu
3/12/2012 3:22:58 PM Principal authentication User ?tdstester8? attempted to authenticate using authenticator ?Secu
3/12/2012 3:29:57 PM Authentication attempted Passcode reuse or previous token code detected for user ?tdstester8?
3/12/2012 3:29:57 PM Authentication attempted Bad PIN, but previous tokencode detected for token serial number ?0(
3/12/2012 3:29:57 PM Principal authentication User ?tdstester8? attempted to authenticate using authenticator ?Secu
3/12/2012 3:30:07 PM Authentication attempted Passcode reuse or previous token code detected for user ?tdstester8?
3/12/2012 3:30:07 PM Authentication attempted Bad PIN, but previous tokencode detected for token serial number ?0(
3/12/2012 3:30:07 PM Principal authentication User ?tdstester8? attempted to authenticate using authenticator ?Secu
3/12/2012 4:13:15 PM Principal authentication User ?tdstester8? attempted to authenticate using authenticator ?Secu
3/12/2012 4:15:24 PM Principal authentication User ?tdstester8? attempted to authenticate using authenticator ?Secu
tdstester2 tds tester2 twistester2@proservices-2.com False True
tdstester1 tds tester1 twistester1@proservices-2.com False True
tdstester8
Sign out

Get User Info / Admin Roles

Only applicable to AM 7.1 servers.

am71 - Admin Roles	
GET	http://10.100.89.139:8080/am71-16/user/adminRoles/<UserID>

Request HEADER

```
GET /am71/user/adminRoles/lapadmin1 HTTP/1.1
RSA_AUTHENTICATION_TOKEN: 21949613
Host: 10.100.89.138:8080
```

Request BODY

```
n/a
```

Response HEADERS

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: application/xml
Transfer-Encoding: chunked
Date: Mon, 12 Mar 2012 18:03:13 GMT
```

Response BODY

```
<?xml version="1.0" encoding="utf-8" standalone="no"?>
<serviceResult result="true">
  <AdminRoles userName="lapadmin1">
    <AdminRole guid="ims.9657d749655a640a149996c4471ba578"
    isSuperAdminRole="false" name="Admin-1" />
  </AdminRoles>
</serviceResult>
```

Get User Activity

AM 7.1 only.

Get User Activity

GET http(s)://<servername:port>/am71/user/activity/tdstester8/60

Request HEADER

```
GET /amXX/user/activity/tdstester8/60 HTTP/1.1
RSA_AUTHENTICATION_TOKEN: 69809393
Host: 10.100.89.138:8080
```

Request BODY

```
n/a
```

Response HEADERS

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: application/xml
Transfer-Encoding: chunked
Date: Mon, 12 Mar 2012 16:15:59 GMT
```

Response BODY

```
<?xml version="1.0" encoding="utf-8" standalone="no"?>
<serviceResult result="true">
  <UserActivity Count="22" userID="tdstester8">
    <activities Count="28" id="075ee3758d59640a02e3968dea15aed6">
      <Value name="Activity Key">Principal authentication</Value>
      <Value name="Activity Result Key">Failure</Value>
      <Value name="Description">User tdstester8 attempted to
      authenticate using authenticator SecurID_Native. The user
      belongs to security domain SystemDomain</Value>
      <Value name="User First Name">tds</Value>
      <Value name="Actor GUID">
      549e03158d59640a028560f66ebe1e9e</Value>
      <Value name="User ID">tdstester8</Value>
      <Value name="User Identity Source">Internal Database</Value>
      <Value name="User Last Name">tester8</Value>
      <Value name="User Security Domain">SystemDomain</Value>
      <Value name="Agent GUID">
      181ccaf08d59640a02XX8d0fb2ff4cb2</Value>
      <Value name="Agent IP">10.100.89.138</Value>
      <Value name="Agent Name">ps-esg-138.ps-esg.com</Value>
      <Value name="Agent Security Domain">SystemDomain</Value>
      <Value name="Agent Type">7</Value>
      <Value name="Argument 1">AUTHN_LOGIN_EVENT</Value>
      <Value name="Argument 2">5</Value>
      <Value name="Argument 3">2</Value>
      <Value name="Authentication Method">SecurID_Native</Value>
      <Value name="Client IP">10.100.89.138</Value>
      <Value name="INSTANCE_ID">
      eb2049468d59640a0035414XX9e388a6</Value>
      <Value name="LOCAL_LOG_TIME">2012-03-12 10:45:20.885</Value>
      <Value name="Log Level">ERROR</Value>
      <Value name="RESULT_KEY">AUTHN_METHOD_FAILED</Value>
```

Get User Activity

```
      <Value name="Result">Authentication method failed</Value>
      <Value name="Server Node IP">10.100.89.141</Value>
      <Value name="Session ID">
      075ee1b08d59640a025e926c6653f13b-nDpO6HC8t0TK</Value>
      <Value name="User ID">tdstester8</Value>
      <Value name="UTC_LOG_TIME">2012-03-12 14:45:20.885</Value>
    </activities>
    <activities Count="30" id="076134c58d59640a03464bc58b0d3bf3">
      <Value name="Activity Key">Principal authentication</Value>
      <Value name="Activity Result Key">Success</Value>
      <Value name="Description">User tdstester8 attempted to
      authenticate using authenticator SecurID_Native. The user
      belongs to security domain SystemDomain</Value>
      <Value name="User First Name">tds</Value>
      <Value name="Actor GUID">
      549e03158d59640a028560f66ebe1e9e</Value>
      <Value name="User ID">tdstester8</Value>
      <Value name="User Identity Source">Internal Database</Value>
      <Value name="User Security Domain">SystemDomain</Value>
      <Value name="Agent GUID">
      181ccaf08d59640a02XX8d0fb2ff4cb2</Value>
      <Value name="Agent IP">10.100.89.138</Value>
      <Value name="Agent Name">ps-esg-138.ps-esg.com</Value>
      <Value name="Agent Security Domain">SystemDomain</Value>
      <Value name="Agent Type">7</Value>
      <Value name="Argument 1">AUTHN_LOGIN_EVENT</Value>
      <Value name="Argument 2">5</Value>
      <Value name="Argument 3">2</Value>
      <Value name="Argument 8">
      edd5b4748d59640a02b613317d12d748</Value>
      <Value name="Argument 9">000115876401</Value>
      <Value name="Authentication Method">SecurID_Native</Value>
      <Value name="Client IP">10.100.89.138</Value>
      <Value name="INSTANCE_ID">
      eb2049468d59640a0035414XX9e388a6</Value>
      <Value name="LOCAL_LOG_TIME">2012-03-12 10:47:52.773</Value>
      <Value name="Log Level">INFO</Value>
      <Value name="RESULT_KEY">AUTHN_METHOD_SUCCESS</Value>
      <Value name="Result">Authentication method success</Value>
      <Value name="Server Node IP">10.100.89.141</Value>
      <Value name="Session ID">
      076134578d59640a034dfd077085dc44-XnULXr7a7Ix6</Value>
      <Value name="User ID">tdstester8</Value>
      <Value name="UTC_LOG_TIME">2012-03-12 14:47:52.773</Value>
    </activities>
    <activities Count="28" id="076f50848d59640a01c470490a48a0f7">
      <Value name="Activity Key">Principal authentication</Value>
      <Value name="Activity Result Key">Failure</Value>
      <Value name="Description">User tdstester8 attempted to
      authenticate using authenticator SecurID_Native. The user
      belongs to security domain SystemDomain</Value>
      <Value name="User First Name">tds</Value>
```

Get User Activity

```
      <Value name="Actor GUID">
      549e03158d59640a028560f66ebe1e9e</Value>
      <Value name="User ID">tdstester8</Value>
      <Value name="User Identity Source">Internal Database</Value>
      <Value name="User Last Name">tester8</Value>
      <Value name="User Security Domain">SystemDomain</Value>
      <Value name="Agent GUID">
      181ccaf08d59640a02XX8d0fb2ff4cb2</Value>
      <Value name="Agent IP">10.100.89.138</Value>
      <Value name="Agent Name">ps-esg-138.ps-esg.com</Value>
      <Value name="Agent Security Domain">SystemDomain</Value>
      <Value name="Agent Type">7</Value>
      <Value name="Argument 1">AUTHN_LOGIN_EVENT</Value>
      <Value name="Argument 2">5</Value>
      <Value name="Argument 3">2</Value>
```

```
   <Value name="User Last Name">tester8</Value>
      <Value name="User Security Domain">SystemDomain</Value>
      <Value name="Agent GUID">
      181ccaf08d59640a02XX8d0fb2ff4cb2</Value>
      <Value name="Agent IP">10.100.89.138</Value>
      <Value name="Agent Name">ps-esg-138.ps-esg.com</Value>
      <Value name="Agent Security Domain">SystemDomain</Value>
      <Value name="Agent Type">7</Value>
      <Value name="Argument 1">AUTHN_LOGIN_EVENT</Value>
      <Value name="Argument 2">5</Value>
      <Value name="Argument 3">2</Value>
      <Value name="Argument 8">
      edd5b4748d59640a02b613317d12d748</Value>
      <Value name="Argument 9">000115876401</Value>
      <Value name="Authentication Method">SecurID_Native</Value>
      <Value name="Client IP">10.100.89.138</Value>
      <Value name="INSTANCE_ID">
      eb2049468d59640a0035414XX9e388a6</Value>
      <Value name="LOCAL_LOG_TIME">2012-03-12 10:47:52.773</Value>
      <Value name="Log Level">INFO</Value>
      <Value name="RESULT_KEY">AUTHN_METHOD_SUCCESS</Value>
      <Value name="Result">Authentication method success</Value>
      <Value name="Server Node IP">10.100.89.141</Value>
      <Value name="Session ID">
      076134578d59640a034dfd077085dc44-XnULXr7a7Ix6</Value>
      <Value name="User ID">tdstester8</Value>
      <Value name="UTC_LOG_TIME">2012-03-12 14:47:52.773</Value>
    </activities>
    <activities Count="28" id="076f50848d59640a01c470490a48a0f7">
      <Value name="Activity Key">Principal authentication</Value>
      <Value name="Activity Result Key">Failure</Value>
      <Value name="Description">User tdstester8 attempted to
      authenticate using authenticator SecurID_Native. The user
      belongs to security domain SystemDomain</Value>
      <Value name="User First Name">tds</Value>
      <Value name="Actor GUID">
```

Get User Activity

```
      549e03158d59640a028560f66ebe1e9e</Value>
      <Value name="User ID">tdstester8</Value>
      <Value name="User Identity Source">Internal Database</Value>
      <Value name="User Last Name">tester8</Value>
      <Value name="User Security Domain">SystemDomain</Value>
      <Value name="Agent GUID">
      181ccaf08d59640a02XX8d0fb2ff4cb2</Value>
      <Value name="Agent IP">10.100.89.138</Value>
      <Value name="Agent Name">ps-esg-138.ps-esg.com</Value>
      <Value name="Agent Security Domain">SystemDomain</Value>
      <Value name="Agent Type">7</Value>
      <Value name="Argument 1">AUTHN_LOGIN_EVENT</Value>
      <Value name="Argument 2">5</Value>
      <Value name="Argument 3">2</Value>
```

```
      <Value name="Authentication Method">SecurID_Native</Value>
      <Value name="Client IP">10.100.89.138</Value>
      <Value name="INSTANCE_ID">
      eb2049468d59640a0035414XX9e388a6</Value>
      <Value name="LOCAL_LOG_TIME">2012-03-12 11:03:17.38</Value>
      <Value name="Log Level">ERROR</Value>
      <Value name="RESULT_KEY">AUTHN_METHOD_FAILED</Value>
      <Value name="Result">Authentication method failed</Value>
      <Value name="Server Node IP">10.100.89.141</Value>
      <Value name="Session ID">
      076f50078d59640a01ce386ab675f47e-vovGgOG+tbb9</Value>
      <Value name="User ID">tdstester8</Value>
      <Value name="UTC_LOG_TIME">2012-03-12 15:03:17.38</Value>
    </activities>
    <activities Count="28" id="076f8fXX8d59640a01f24c593177053d">
      <Value name="Activity Key">Principal authentication</Value>
      <Value name="Activity Result Key">Failure</Value>
      <Value name="Description">User tdstester8 attempted to
      authenticate using authenticator SecurID_Native. The user
      belongs to security domain SystemDomain</Value>
      <Value name="User First Name">tds</Value>
      <Value name="Actor GUID">
      549e03158d59640a028560f66ebe1e9e</Value>
      <Value name="User ID">tdstester8</Value>
      <Value name="User Identity Source">Internal Database</Value>
      <Value name="User Last Name">tester8</Value>
      <Value name="User Security Domain">SystemDomain</Value>
      <Value name="Agent GUID">
      181ccaf08d59640a02XX8d0fb2ff4cb2</Value>
      <Value name="Agent IP">10.100.89.138</Value>
      <Value name="Agent Name">ps-esg-138.ps-esg.com</Value>
      <Value name="Agent Security Domain">SystemDomain</Value>
      <Value name="Agent Type">7</Value>
      <Value name="Argument 1">AUTHN_LOGIN_EVENT</Value>
      <Value name="Argument 2">5</Value>
      <Value name="Argument 3">2</Value>
      <Value name="Authentication Method">SecurID_Native</Value>
```

Get User Activity

```
      <Value name="Client IP">10.100.89.138</Value>
      <Value name="INSTANCE_ID">
      eb2049468d59640a0035414XX9e388a6</Value>
      <Value name="LOCAL_LOG_TIME">2012-03-12 11:03:33.489</Value>
      <Value name="Log Level">ERROR</Value>
      <Value name="RESULT_KEY">AUTHN_METHOD_FAILED</Value>
      <Value name="Result">Authentication method failed</Value>
      <Value name="Server Node IP">10.100.89.141</Value>
      <Value name="Session ID">
      076f8f528d59640a01dfae4a4eaa58d3-sETqSTI0qNVC</Value>
      <Value name="User ID">tdstester8</Value>
      <Value name="UTC_LOG_TIME">2012-03-12 15:03:33.489</Value>
    </activities>
```

```
    <activities Count="28" id="076f9bb58d59640a01f7ddb6d9e68efc">
      <Value name="Activity Key">Principal authentication</Value>
      <Value name="Activity Result Key">Failure</Value>
      <Value name="Description">User tdstester8 attempted to
      authenticate using authenticator SecurID_Native. The user
      belongs to security domain SystemDomain</Value>
      <Value name="User First Name">tds</Value>
      <Value name="Actor GUID">
      549e03158d59640a028560f66ebe1e9e</Value>
      <Value name="User ID">tdstester8</Value>
      <Value name="User Identity Source">Internal Database</Value>
      <Value name="User Last Name">tester8</Value>
      <Value name="User Security Domain">SystemDomain</Value>
      <Value name="Agent GUID">
      181ccaf08d59640a02XX8d0fb2ff4cb2</Value>
      <Value name="Agent IP">10.100.89.138</Value>
      <Value name="Agent Name">ps-esg-138.ps-esg.com</Value>
      <Value name="Agent Security Domain">SystemDomain</Value>
      <Value name="Agent Type">7</Value>
      <Value name="Argument 1">AUTHN_LOGIN_EVENT</Value>
      <Value name="Argument 2">5</Value>
      <Value name="Argument 3">2</Value>
      <Value name="Authentication Method">SecurID_Native</Value>
      <Value name="Client IP">10.100.89.138</Value>
      <Value name="INSTANCE_ID">
      eb2049468d59640a0035414XX9e388a6</Value>
      <Value name="LOCAL_LOG_TIME">2012-03-12 11:03:36.629</Value>
      <Value name="Log Level">ERROR</Value>
      <Value name="RESULT_KEY">AUTHN_METHOD_FAILED</Value>
      <Value name="Result">Authentication method failed</Value>
      <Value name="Server Node IP">10.100.89.141</Value>
      <Value name="Session ID">
      076f9ba68d59640a01efc6edfa742bf5-sUfTbfhLghGK</Value>
      <Value name="User ID">tdstester8</Value>
      <Value name="UTC_LOG_TIME">2012-03-12 15:03:36.629</Value>
    </activities>
    <activities Count="30" id="0770d4538d59640a02246115e9b772f0">
      <Value name="Activity Key">Principal authentication</Value>
```

Get User Activity

```
      <Value name="Activity Result Key">Success</Value>
      <Value name="Description">User tdstester8 attempted to
      authenticate using authenticator SecurID_Native. The user
      belongs to security domain SystemDomain</Value>
      <Value name="User First Name">tds</Value>
      <Value name="Actor GUID">
      549e03158d59640a028560f66ebe1e9e</Value>
      <Value name="User ID">tdstester8</Value>
      <Value name="User Identity Source">Internal Database</Value>
      <Value name="User Last Name">tester8</Value>
      <Value name="User Security Domain">SystemDomain</Value>
      <Value name="Agent GUID">
      181ccaf08d59640a02XX8d0fb2ff4cb2</Value>
      <Value name="Agent IP">10.100.89.138</Value>
      <Value name="Agent Name">ps-esg-138.ps-esg.com</Value>
      <Value name="Agent Security Domain">SystemDomain</Value>
      <Value name="Agent Type">7</Value>
      <Value name="Argument 1">AUTHN_LOGIN_EVENT</Value>
      <Value name="Argument 2">5</Value>
      <Value name="Argument 3">2</Value>
      <Value name="Argument 8">
      edd5b4748d59640a02b613317d12d748</Value>
      <Value name="Argument 9">000115876401</Value>
      <Value name="Authentication Method">SecurID_Native</Value>
      <Value name="Client IP">10.100.89.138</Value>
      <Value name="INSTANCE_ID">
      eb2049468d59640a0035414XX9e388a6</Value>
      <Value name="LOCAL_LOG_TIME">2012-03-12 11:04:56.659</Value>
      <Value name="Log Level">INFO</Value>
      <Value name="RESULT_KEY">AUTHN_METHOD_SUCCESS</Value>
      <Value name="Result">Authentication method success</Value>
      <Value name="Server Node IP">10.100.89.141</Value>
      <Value name="Session ID">
      0770d4448d59640a021b5c2479294623-aEvyUV/LTCVF</Value>
      <Value name="User ID">tdstester8</Value>
      <Value name="UTC_LOG_TIME">2012-03-12 15:04:56.659</Value>
    </activities>
    <activities Count="29" id="07XX24288d59640a022ed6d74a508808">
      <Value name="Activity Key">Authentication attempted</Value>
      <Value name="Activity Result Key">Failure</Value>
      <Value name="Description">Passcode reuse or previous token
      code detected for user tdstester8 in security domain
      SystemDomain from Internal Database identity source. Request
      originated from agent ps-esg-138.ps-esg.com with IP address
      10.100.89.138 in security domain SystemDomain with protocol
      version Internal Database. Authentication method:
      SecurID_Native, Authentication policy exp: , Activation
      Group: , Token serial number: 000115876401, Alias:</Value>
      <Value name="User First Name">tds</Value>
      <Value name="Actor GUID">
      549e03158d59640a028560f66ebe1e9e</Value>
```

Get User Activity

```
      <Value name="User ID">tdstester8</Value>
      <Value name="User Identity Source">Internal Database</Value>
      <Value name="User Last Name">tester8</Value>
      <Value name="User Security Domain">SystemDomain</Value>
      <Value name="Agent GUID">
      181ccaf08d59640a02XX8d0fb2ff4cb2</Value>
      <Value name="Agent IP">10.100.89.138</Value>
      <Value name="Agent Name">ps-esg-138.ps-esg.com</Value>
      <Value name="Agent Security Domain">SystemDomain</Value>
      <Value name="Agent Type">7</Value>
      <Value name="Argument 2">5</Value>
      <Value name="Argument 3">2</Value>
      <Value name="Argument 8">
      edd5b4748d59640a02b613317d12d748</Value>
      <Value name="Argument 9">000115876401</Value>
      <Value name="Authentication Method">SecurID_Native</Value>
      <Value name="Client IP">10.100.89.138</Value>
      <Value name="INSTANCE_ID">
      eb2049468d59640a0035414XX9e388a6</Value>
      <Value name="LOCAL_LOG_TIME">2012-03-12 11:05:17.096</Value>
      <Value name="Log Level">ERROR</Value>
      <Value name="RESULT_KEY">AUTHN_METHOD_FAILED</Value>
      <Value name="Result">Authentication method failed</Value>
      <Value name="Server Node IP">10.100.89.141</Value>
      <Value name="Session ID">
      07XX24288d59640a022818c82ce43425-RD/2dLhn9V7c</Value>
      <Value name="User ID">tdstester8</Value>
      <Value name="UTC_LOG_TIME">2012-03-12 15:05:17.096</Value>
    </activities>
    <activities Count="29" id="07XX24388d59640a022e4a915d7c2a55">
      <Value name="Activity Key">Authentication attempted</Value>
      <Value name="Activity Result Key">Failure</Value>
      <Value name="Description">Bad PIN, but previous tokencode
      detected for token serial number 000115876401 assigned to
      user tdstester8 in security domain SystemDomain from Internal
      Database identity source</Value>
      <Value name="User First Name">tds</Value>
      <Value name="Actor GUID">
      549e03158d59640a028560f66ebe1e9e</Value>
      <Value name="User ID">tdstester8</Value>
      <Value name="User Identity Source">Internal Database</Value>
      <Value name="User Last Name">tester8</Value>
      <Value name="User Security Domain">SystemDomain</Value>
      <Value name="Agent GUID">
      181ccaf08d59640a02XX8d0fb2ff4cb2</Value>
      <Value name="Agent IP">10.100.89.138</Value>
      <Value name="Agent Name">ps-esg-138.ps-esg.com</Value>
      <Value name="Agent Security Domain">SystemDomain</Value>
      <Value name="Agent Type">7</Value>
      <Value name="Argument 2">5</Value>
      <Value name="Argument 3">2</Value>
```

Get User Activity

```
      <Value name="Argument 8">
      edd5b4748d59640a02b613317d12d748</Value>
      <Value name="Argument 9">000115876401</Value>
      <Value name="Authentication Method">SecurID_Native</Value>
      <Value name="Client IP">10.100.89.138</Value>
      <Value name="INSTANCE_ID">
      eb2049468d59640a0035414XX9e388a6</Value>
      <Value name="LOCAL_LOG_TIME">2012-03-12 11:05:17.112</Value>
      <Value name="Log Level">ERROR</Value>
      <Value name="RESULT_KEY">AUTHN_METHOD_FAILED</Value>
      <Value name="Result">Authentication method failed</Value>
      <Value name="Server Node IP">10.100.89.141</Value>
      <Value name="Session ID">
      07XX24288d59640a022818c82ce43425-RD/2dLhn9V7c</Value>
      <Value name="User ID">tdstester8</Value>
      <Value name="UTC_LOG_TIME">2012-03-12 15:05:17.112</Value>
    </activities>
    <activities Count="30" id="07XX24388d59640a022f2374c7dd70f4">
      <Value name="Activity Key">Principal authentication</Value>
      <Value name="Activity Result Key">Failure</Value>
      <Value name="Description">User tdstester8 attempted to
      authenticate using authenticator SecurID_Native. The user
      belongs to security domain SystemDomain</Value>
      <Value name="User First Name">tds</Value>
      <Value name="Actor GUID">
      549e03158d59640a028560f66ebe1e9e</Value>
      <Value name="User ID">tdstester8</Value>
      <Value name="User Identity Source">Internal Database</Value>
      <Value name="User Last Name">tester8</Value>
      <Value name="User Security Domain">SystemDomain</Value>
      <Value name="Agent GUID">
      181ccaf08d59640a02XX8d0fb2ff4cb2</Value>
      <Value name="Agent IP">10.100.89.138</Value>
      <Value name="Agent Name">ps-esg-138.ps-esg.com</Value>
      <Value name="Agent Security Domain">SystemDomain</Value>
      <Value name="Agent Type">7</Value>
      <Value name="Argument 1">AUTHN_LOGIN_EVENT</Value>
      <Value name="Argument 2">5</Value>
      <Value name="Argument 3">2</Value>
      <Value name="Argument 8">
      edd5b4748d59640a02b613317d12d748</Value>
      <Value name="Argument 9">000115876401</Value>
      <Value name="Authentication Method">SecurID_Native</Value>
      <Value name="Client IP">10.100.89.138</Value>
      <Value name="INSTANCE_ID">
      eb2049468d59640a0035414XX9e388a6</Value>
      <Value name="LOCAL_LOG_TIME">2012-03-12 11:05:17.112</Value>
      <Value name="Log Level">ERROR</Value>
      <Value name="RESULT_KEY">AUTHN_METHOD_FAILED</Value>
      <Value name="Result">Authentication method failed</Value>
      <Value name="Server Node IP">10.100.89.141</Value>
```

Get User Activity

```
      <Value name="Session ID">
      07XX24288d59640a022818c82ce43425-RD/2dLhn9V7c</Value>
      <Value name="User ID">tdstester8</Value>
      <Value name="UTC_LOG_TIME">2012-03-12 15:05:17.112</Value>
    </activities>
    <activities Count="29" id="07XX24d48d59640a023c6d87702732eb">
      <Value name="Activity Key">Authentication attempted</Value>
      <Value name="Activity Result Key">Failure</Value>
      <Value name="Description">Passcode reuse or previous token
      code detected for user tdstester8 in security domain
      SystemDomain from Internal Database identity source. Request
      originated from agent ps-esg-138.ps-esg.com with IP address
      10.100.89.138 in security domain SystemDomain with protocol
      version Internal Database. Authentication method:
      SecurID_Native, Authentication policy exp: , Activation
      Group: , Token serial number: 000115876401, Alias:</Value>
      <Value name="User First Name">tds</Value>
      <Value name="Actor GUID">
      549e03158d59640a028560f66ebe1e9e</Value>
      <Value name="User ID">tdstester8</Value>
      <Value name="User Identity Source">Internal Database</Value>
      <Value name="User Last Name">tester8</Value>
      <Value name="User Security Domain">SystemDomain</Value>
      <Value name="Agent GUID">
      181ccaf08d59640a02XX8d0fb2ff4cb2</Value>
      <Value name="Agent IP">10.100.89.138</Value>
      <Value name="Agent Name">ps-esg-138.ps-esg.com</Value>
      <Value name="Agent Security Domain">SystemDomain</Value>
      <Value name="Agent Type">7</Value>
      <Value name="Argument 2">5</Value>
      <Value name="Argument 3">2</Value>
      <Value name="Argument 8">
      edd5b4748d59640a02b613317d12d748</Value>
      <Value name="Argument 9">000115876401</Value>
      <Value name="Authentication Method">SecurID_Native</Value>
      <Value name="Client IP">10.100.89.138</Value>
      <Value name="INSTANCE_ID">
      eb2049468d59640a0035414XX9e388a6</Value>
      <Value name="LOCAL_LOG_TIME">2012-03-12 11:05:17.268</Value>
      <Value name="Log Level">ERROR</Value>
      <Value name="RESULT_KEY">AUTHN_METHOD_FAILED</Value>
      <Value name="Result">Authentication method failed</Value>
      <Value name="Server Node IP">10.100.89.141</Value>
      <Value name="Session ID">
      07XX24d48d59640a022b26858d5d5e11-N76XYnv6+a4I</Value>
      <Value name="User ID">tdstester8</Value>
      <Value name="UTC_LOG_TIME">2012-03-12 15:05:17.268</Value>
    </activities>
    <activities Count="29" id="07XX24e48d59640a02389d2f4ab47674">
      <Value name="Activity Key">Authentication attempted</Value>
      <Value name="Activity Result Key">Failure</Value>
```

Get User Activity

```
      <Value name="Description">Bad PIN, but previous tokencode
      detected for token serial number 000115876401 assigned to
      user tdstester8 in security domain SystemDomain from Internal
      Database identity source</Value>
      <Value name="User First Name">tds</Value>
      <Value name="Actor GUID">
      549e03158d59640a028560f66ebe1e9e</Value>
      <Value name="User ID">tdstester8</Value>
      <Value name="User Identity Source">Internal Database</Value>
      <Value name="User Last Name">tester8</Value>
      <Value name="User Security Domain">SystemDomain</Value>
      <Value name="Agent GUID">
      181ccaf08d59640a02XX8d0fb2ff4cb2</Value>
      <Value name="Agent IP">10.100.89.138</Value>
      <Value name="Agent Name">ps-esg-138.ps-esg.com</Value>
      <Value name="Agent Security Domain">SystemDomain</Value>
      <Value name="Agent Type">7</Value>
      <Value name="Argument 2">5</Value>
      <Value name="Argument 3">2</Value>
      <Value name="Argument 8">
      edd5b4748d59640a02b613317d12d748</Value>
      <Value name="Argument 9">000115876401</Value>
      <Value name="Authentication Method">SecurID_Native</Value>
      <Value name="Client IP">10.100.89.138</Value>
      <Value name="INSTANCE_ID">
      eb2049468d59640a0035414XX9e388a6</Value>
      <Value name="LOCAL_LOG_TIME">2012-03-12 11:05:17.284</Value>
      <Value name="Log Level">ERROR</Value>
      <Value name="RESULT_KEY">AUTHN_METHOD_FAILED</Value>
      <Value name="Result">Authentication method failed</Value>
      <Value name="Server Node IP">10.100.89.141</Value>
      <Value name="Session ID">
      07XX24d48d59640a022b26858d5d5e11-N76XYnv6+a4I</Value>
      <Value name="User ID">tdstester8</Value>
      <Value name="UTC_LOG_TIME">2012-03-12 15:05:17.284</Value>
    </activities>
    <activities Count="30" id="07XX24f38d59640a02395e1ff93dff1b">
      <Value name="Activity Key">Principal authentication</Value>
      <Value name="Activity Result Key">Failure</Value>
      <Value name="Description">User tdstester8 attempted to
      authenticate using authenticator SecurID_Native. The user
      belongs to security domain SystemDomain</Value>
      <Value name="User First Name">tds</Value>
      <Value name="Actor GUID">
      549e03158d59640a028560f66ebe1e9e</Value>
      <Value name="User ID">tdstester8</Value>
      <Value name="User Identity Source">Internal Database</Value>
      <Value name="User Last Name">tester8</Value>
      <Value name="User Security Domain">SystemDomain</Value>
      <Value name="Agent GUID">
      181ccaf08d59640a02XX8d0fb2ff4cb2</Value>
```

Get User Activity

```
      <Value name="Agent IP">10.100.89.138</Value>
      <Value name="Agent Name">ps-esg-138.ps-esg.com</Value>
      <Value name="Agent Security Domain">SystemDomain</Value>
      <Value name="Agent Type">7</Value>
      <Value name="Argument 1">AUTHN_LOGIN_EVENT</Value>
      <Value name="Argument 2">5</Value>
      <Value name="Argument 3">2</Value>
```

```
      <Value name="Argument 8">
      edd5b4748d59640a02b613317d12d748</Value>
      <Value name="Argument 9">000115876401</Value>
      <Value name="Authentication Method">SecurID_Native</Value>
      <Value name="Client IP">10.100.89.138</Value>
      <Value name="INSTANCE_ID">
      eb2049468d59640a0035414XX9e388a6</Value>
      <Value name="LOCAL_LOG_TIME">2012-03-12 11:05:17.299</Value>
      <Value name="Log Level">ERROR</Value>
      <Value name="RESULT_KEY">AUTHN_METHOD_FAILED</Value>
      <Value name="Result">Authentication method failed</Value>
      <Value name="Server Node IP">10.100.89.141</Value>
      <Value name="Session ID">
      07XX24d48d59640a022b26858d5d5e11-N76XYnv6+a4I</Value>
      <Value name="User ID">tdstester8</Value>
      <Value name="UTC_LOG_TIME">2012-03-12 15:05:17.299</Value>
    </activities>
    <activities Count="30" id="077867fc8d59640a020129b6bc63d8d1">
      <Value name="Activity Key">Principal authentication</Value>
      <Value name="Activity Result Key">Success</Value>
      <Value name="Description">User tdstester8 attempted to
      authenticate using authenticator SecurID_Native. The user
      belongs to security domain SystemDomain</Value>
      <Value name="User First Name">tds</Value>
      <Value name="Actor GUID">
      549e03158d59640a028560f66ebe1e9e</Value>
      <Value name="User ID">tdstester8</Value>
      <Value name="User Identity Source">Internal Database</Value>
      <Value name="User Last Name">tester8</Value>
      <Value name="User Security Domain">SystemDomain</Value>
      <Value name="Agent GUID">
      181ccaf08d59640a02XX8d0fb2ff4cb2</Value>
      <Value name="Agent IP">10.100.89.138</Value>
      <Value name="Agent Name">ps-esg-138.ps-esg.com</Value>
      <Value name="Agent Security Domain">SystemDomain</Value>
      <Value name="Agent Type">7</Value>
      <Value name="Argument 1">AUTHN_LOGIN_EVENT</Value>
      <Value name="Argument 2">5</Value>
      <Value name="Argument 3">2</Value>
      <Value name="Argument 8">
      edd5b4748d59640a02b613317d12d748</Value>
      <Value name="Argument 9">000115876401</Value>
      <Value name="Authentication Method">SecurID_Native</Value>
      <Value name="Client IP">10.100.89.138</Value>
```

Get User Activity

```
      <Value name="INSTANCE_ID">
      eb2049468d59640a0035414XX9e388a6</Value>
      <Value name="LOCAL_LOG_TIME">2012-03-12 11:13:13.212</Value>
      <Value name="Log Level">INFO</Value>
      <Value name="RESULT_KEY">AUTHN_METHOD_SUCCESS</Value>
      <Value name="Result">Authentication method success</Value>
      <Value name="Server Node IP">10.100.89.141</Value>
      <Value name="Session ID">
      077867ed8d59640a0199c6880f0ab9ce-+wpq/mQdeKEh</Value>
      <Value name="User ID">tdstester8</Value>
      <Value name="UTC_LOG_TIME">2012-03-12 15:13:13.212</Value>
    </activities>
    <activities Count="30" id="078155298d59640a030aa2ea2673440a">
      <Value name="Activity Key">Principal authentication</Value>
      <Value name="Activity Result Key">Success</Value>
      <Value name="Description">User tdstester8 attempted to
      authenticate using authenticator SecurID_Native. The user
      belongs to security domain SystemDomain</Value>
      <Value name="User First Name">tds</Value>
      <Value name="Actor GUID">
      549e03158d59640a028560f66ebe1e9e</Value>
      <Value name="User ID">tdstester8</Value>
      <Value name="User Identity Source">Internal Database</Value>
      <Value name="User Last Name">tester8</Value>
      <Value name="User Security Domain">SystemDomain</Value>
      <Value name="Agent GUID">
      181ccaf08d59640a02XX8d0fb2ff4cb2</Value>
      <Value name="Agent IP">10.100.89.138</Value>
      <Value name="Agent Name">ps-esg-138.ps-esg.com</Value>
      <Value name="Agent Security Domain">SystemDomain</Value>
      <Value name="Agent Type">7</Value>
      <Value name="Argument 1">AUTHN_LOGIN_EVENT</Value>
      <Value name="Argument 2">5</Value>
      <Value name="Argument 3">2</Value>
      <Value name="Argument 8">
      edd5b4748d59640a02b613317d12d748</Value>
      <Value name="Argument 9">000115876401</Value>
      <Value name="Authentication Method">SecurID_Native</Value>
      <Value name="Client IP">10.100.89.138</Value>
      <Value name="INSTANCE_ID">
      eb2049468d59640a0035414XX9e388a6</Value>
      <Value name="LOCAL_LOG_TIME">2012-03-12 11:22:58.217</Value>
      <Value name="Log Level">INFO</Value>
      <Value name="RESULT_KEY">AUTHN_METHOD_SUCCESS</Value>
      <Value name="Result">Authentication method success</Value>
      <Value name="Server Node IP">10.100.89.141</Value>
      <Value name="Session ID">
      078154cb8d59640a02cfe7f450740578-9DUWVdMZtNSW</Value>
      <Value name="User ID">tdstester8</Value>
      <Value name="UTC_LOG_TIME">2012-03-12 15:22:58.217</Value>
    </activities>
```

Get User Activity

```
    <activities Count="29" id="0787ba658d59640a01a13e0a4ecaa702">
      <Value name="Activity Key">Authentication attempted</Value>
      <Value name="Activity Result Key">Failure</Value>
      <Value name="Description">Passcode reuse or previous token
      code detected for user tdstester8 in security domain
      SystemDomain from Internal Database identity source. Request
      originated from agent ps-esg-138.ps-esg.com with IP address
      10.100.89.138 in security domain SystemDomain with protocol
      version Internal Database. Authentication method:
      SecurID_Native, Authentication policy exp: , Activation
      Group: , Token serial number: 000115876401, Alias:</Value>
      <Value name="User First Name">tds</Value>
      <Value name="Actor GUID">
      549e03158d59640a028560f66ebe1e9e</Value>
      <Value name="User ID">tdstester8</Value>
      <Value name="User Identity Source">Internal Database</Value>
      <Value name="User Last Name">tester8</Value>
      <Value name="User Security Domain">SystemDomain</Value>
      <Value name="Agent GUID">
      181ccaf08d59640a02XX8d0fb2ff4cb2</Value>
      <Value name="Agent IP">10.100.89.138</Value>
      <Value name="Agent Name">ps-esg-138.ps-esg.com</Value>
      <Value name="Agent Security Domain">SystemDomain</Value>
      <Value name="Agent Type">7</Value>
      <Value name="Argument 2">5</Value>
      <Value name="Argument 3">2</Value>
      <Value name="Argument 8">
      edd5b4748d59640a02b613317d12d748</Value>
      <Value name="Argument 9">000115876401</Value>
      <Value name="Authentication Method">SecurID_Native</Value>
      <Value name="Client IP">10.100.89.138</Value>
      <Value name="INSTANCE_ID">
      eb2049468d59640a0035414XX9e388a6</Value>
      <Value name="LOCAL_LOG_TIME">2012-03-12 11:29:57.349</Value>
      <Value name="Log Level">ERROR</Value>
      <Value name="RESULT_KEY">AUTHN_METHOD_FAILED</Value>
      <Value name="Result">Authentication method failed</Value>
      <Value name="Server Node IP">10.100.89.141</Value>
      <Value name="Session ID">
      0787ba658d59640a018dc6c7e3552883-qRI1+mjPUG/U</Value>
      <Value name="User ID">tdstester8</Value>
      <Value name="UTC_LOG_TIME">2012-03-12 15:29:57.349</Value>
    </activities>
    <activities Count="29" id="0787ba948d59640a01a7c3c8b3f51ed3">
      <Value name="Activity Key">Authentication attempted</Value>
      <Value name="Activity Result Key">Failure</Value>
      <Value name="Description">Bad PIN, but previous tokencode
      detected for token serial number 000115876401 assigned to
      user tdstester8 in security domain SystemDomain from Internal
      Database identity source</Value>
      <Value name="User First Name">tds</Value>
```

Get User Activity

```
      <Value name="Actor GUID">
      549e03158d59640a028560f66ebe1e9e</Value>
      <Value name="User ID">tdstester8</Value>
      <Value name="User Identity Source">Internal Database</Value>
      <Value name="User Last Name">tester8</Value>
      <Value name="User Security Domain">SystemDomain</Value>
      <Value name="Agent GUID">
      181ccaf08d59640a02XX8d0fb2ff4cb2</Value>
      <Value name="Agent IP">10.100.89.138</Value>
      <Value name="Agent Name">ps-esg-138.ps-esg.com</Value>
      <Value name="Agent Security Domain">SystemDomain</Value>
      <Value name="Agent Type">7</Value>
      <Value name="Argument 2">5</Value>
      <Value name="Argument 3">2</Value>
      <Value name="Argument 8">
      edd5b4748d59640a02b613317d12d748</Value>
      <Value name="Argument 9">000115876401</Value>
      <Value name="Authentication Method">SecurID_Native</Value>
      <Value name="Client IP">10.100.89.138</Value>
      <Value name="INSTANCE_ID">
      eb2049468d59640a0035414XX9e388a6</Value>
      <Value name="LOCAL_LOG_TIME">2012-03-12 11:29:57.396</Value>
      <Value name="Log Level">ERROR</Value>
      <Value name="RESULT_KEY">AUTHN_METHOD_FAILED</Value>
      <Value name="Result">Authentication method failed</Value>
      <Value name="Server Node IP">10.100.89.141</Value>
      <Value name="Session ID">
      0787ba658d59640a018dc6c7e3552883-qRI1+mjPUG/U</Value>
      <Value name="User ID">tdstester8</Value>
      <Value name="UTC_LOG_TIME">2012-03-12 15:29:57.396</Value>
    </activities>
    <activities Count="30" id="0787ba948d59640a01a62bd68d2f787b">
      <Value name="Activity Key">Principal authentication</Value>
      <Value name="Activity Result Key">Failure</Value>
      <Value name="Description">User tdstester8 attempted to
      authenticate using authenticator SecurID_Native. The user
      belongs to security domain SystemDomain</Value>
      <Value name="User First Name">tds</Value>
      <Value name="Actor GUID">
      549e03158d59640a028560f66ebe1e9e</Value>
      <Value name="User ID">tdstester8</Value>
      <Value name="User Identity Source">Internal Database</Value>
      <Value name="User Last Name">tester8</Value>
      <Value name="User Security Domain">SystemDomain</Value>
      <Value name="Agent GUID">
      181ccaf08d59640a02XX8d0fb2ff4cb2</Value>
      <Value name="Agent IP">10.100.89.138</Value>
      <Value name="Agent Name">ps-esg-138.ps-esg.com</Value>
      <Value name="Agent Security Domain">SystemDomain</Value>
      <Value name="Agent Type">7</Value>
      <Value name="Argument 1">AUTHN_LOGIN_EVENT</Value>
```

Get User Activity

```
      <Value name="Argument 2">5</Value>
      <Value name="Argument 3">2</Value>
      <Value name="Argument 8">
     edd5b4748d59640a02b613317d12d748</Value>
      <Value name="Argument 9">000115876401</Value>
      <Value name="Authentication Method">SecurID_Native</Value>
      <Value name="Client IP">10.100.89.138</Value>
      <Value name="INSTANCE_ID">
      eb2049468d59640a0035414XX9e388a6</Value>
      <Value name="LOCAL_LOG_TIME">2012-03-12 11:29:57.396</Value>
      <Value name="Log Level">ERROR</Value>
      <Value name="RESULT_KEY">AUTHN_METHOD_FAILED</Value>
      <Value name="Result">Authentication method failed</Value>
      <Value name="Server Node IP">10.100.89.141</Value>
      <Value name="Session ID">
      0787ba658d59640a018dc6c7e3552883-qRI1+mjPUG/U</Value>
      <Value name="User ID">tdstester8</Value>
      <Value name="UTC_LOG_TIME">2012-03-12 15:29:57.396</Value>
    </activities>
    <activities Count="29" id="0787e3698d59640a018fcd92677281d1">
      <Value name="Activity Key">Authentication attempted</Value>
      <Value name="Activity Result Key">Failure</Value>
      <Value name="Description">Passcode reuse or previous token
      code detected for user tdstester8 in security domain
      SystemDomain from Internal Database identity source. Request
      originated from agent ps-esg-138.ps-esg.com with IP address
      10.100.89.138 in security domain SystemDomain with protocol
      version Internal Database. Authentication method:
      SecurID_Native, Authentication policy exp: , Activation
      Group: , Token serial number: 000115876401, Alias:</Value>
      <Value name="User First Name">tds</Value>
      <Value name="Actor GUID">
      549e03158d59640a028560f66ebe1e9e</Value>
      <Value name="User ID">tdstester8</Value>
      <Value name="User Identity Source">Internal Database</Value>
      <Value name="User Last Name">tester8</Value>
      <Value name="User Security Domain">SystemDomain</Value>
      <Value name="Agent GUID">
      181ccaf08d59640a02XX8d0fb2ff4cb2</Value>
      <Value name="Agent IP">10.100.89.138</Value>
      <Value name="Agent Name">ps-esg-138.ps-esg.com</Value>
      <Value name="Agent Security Domain">SystemDomain</Value>
      <Value name="Agent Type">7</Value>
      <Value name="Argument 2">5</Value>
      <Value name="Argument 3">2</Value>
      <Value name="Argument 8">
      edd5b4748d59640a02b613317d12d748</Value>
      <Value name="Argument 9">000115876401</Value>
      <Value name="Authentication Method">SecurID_Native</Value>
      <Value name="Client IP">10.100.89.138</Value>
      <Value name="INSTANCE_ID">
```

Get User Activity

```
      eb2049468d59640a0035414XX9e388a6</Value>
      <Value name="LOCAL_LOG_TIME">2012-03-12 11:30:07.849</Value>
      <Value name="Log Level">ERROR</Value>
      <Value name="RESULT_KEY">AUTHN_METHOD_FAILED</Value>
      <Value name="Result">Authentication method failed</Value>
      <Value name="Server Node IP">10.100.89.141</Value>
      <Value name="Session ID">
      0787e3698d59640a01ae4647bf599153-d1yAuy0hxQkL</Value>
      <Value name="User ID">tdstester8</Value>
      <Value name="UTC_LOG_TIME">2012-03-12 15:30:07.849</Value>
    </activities>
    <activities Count="29" id="0787e3698d59640a01b5ba4f4e342a0a">
      <Value name="Activity Key">Authentication attempted</Value>
      <Value name="Activity Result Key">Failure</Value>
      <Value name="Description">Bad PIN, but previous tokencode
      detected for token serial number 000115876401 assigned to
      user tdstester8 in security domain SystemDomain from Internal
      Database identity source</Value>
      <Value name="User First Name">tds</Value>
      <Value name="Actor GUID">
      549e03158d59640a028560f66ebe1e9e</Value>
      <Value name="User ID">tdstester8</Value>
      <Value name="User Identity Source">Internal Database</Value>
      <Value name="User Last Name">tester8</Value>
      <Value name="User Security Domain">SystemDomain</Value>
      <Value name="Agent GUID">
      181ccaf08d59640a02XX8d0fb2ff4cb2</Value>
      <Value name="Agent IP">10.100.89.138</Value>
      <Value name="Agent Name">ps-esg-138.ps-esg.com</Value>
      <Value name="Agent Security Domain">SystemDomain</Value>
      <Value name="Agent Type">7</Value>
      <Value name="Argument 2">5</Value>
      <Value name="Argument 3">2</Value>
      <Value name="Argument 8">
      edd5b4748d59640a02b613317d12d748</Value>
      <Value name="Argument 9">000115876401</Value>
      <Value name="Authentication Method">SecurID_Native</Value>
      <Value name="Client IP">10.100.89.138</Value>
      <Value name="INSTANCE_ID">
      eb2049468d59640a0035414XX9e388a6</Value>
      <Value name="LOCAL_LOG_TIME">2012-03-12 11:30:07.849</Value>
      <Value name="Log Level">ERROR</Value>
      <Value name="RESULT_KEY">AUTHN_METHOD_FAILED</Value>
      <Value name="Result">Authentication method failed</Value>
      <Value name="Server Node IP">10.100.89.141</Value>
      <Value name="Session ID">
      0787e3698d59640a01ae4647bf599153-d1yAuy0hxQkL</Value>
      <Value name="User ID">tdstester8</Value>
      <Value name="UTC_LOG_TIME">2012-03-12 15:30:07.849</Value>
    </activities>
    <activities Count="30" id="0787e3798d59640a01b6fd219c01a287">
```

Get User Activity

```
      <Value name="Activity Key">Principal authentication</Value>
      <Value name="Activity Result Key">Failure</Value>
      <Value name="Description">User tdstester8 attempted to
      authenticate using authenticator SecurID_Native. The user
      belongs to security domain SystemDomain</Value>
      <Value name="User First Name">tds</Value>
      <Value name="Actor GUID">
      549e03158d59640a028560f66ebe1e9e</Value>
      <Value name="User ID">tdstester8</Value>
      <Value name="User Identity Source">Internal Database</Value>
      <Value name="User Last Name">tester8</Value>
      <Value name="User Security Domain">SystemDomain</Value>
      <Value name="Agent GUID">
      181ccaf08d59640a02XX8d0fb2ff4cb2</Value>
      <Value name="Agent IP">10.100.89.138</Value>
      <Value name="Agent Name">ps-esg-138.ps-esg.com</Value>
      <Value name="Agent Security Domain">SystemDomain</Value>
      <Value name="Agent Type">7</Value>
      <Value name="Argument 1">AUTHN_LOGIN_EVENT</Value>
      <Value name="Argument 2">5</Value>
      <Value name="Argument 3">2</Value>
      <Value name="Argument 8">
      edd5b4748d59640a02b613317d12d748</Value>
      <Value name="Argument 9">000115876401</Value>
      <Value name="Authentication Method">SecurID_Native</Value>
      <Value name="Client IP">10.100.89.138</Value>
      <Value name="INSTANCE_ID">
      eb2049468d59640a0035414XX9e388a6</Value>
      <Value name="LOCAL_LOG_TIME">2012-03-12 11:30:07.865</Value>
      <Value name="Log Level">ERROR</Value>
      <Value name="RESULT_KEY">AUTHN_METHOD_FAILED</Value>
      <Value name="Result">Authentication method failed</Value>
      <Value name="Server Node IP">10.100.89.141</Value>
      <Value name="Session ID">
      0787e3698d59640a01ae4647bf599153-d1yAuy0hxQkL</Value>
      <Value name="User ID">tdstester8</Value>
      <Value name="UTC_LOG_TIME">2012-03-12 15:30:07.865</Value>
    </activities>
    <activities Count="30" id="07af5e948d59640a0208ce8f869a7eec">
      <Value name="Activity Key">Principal authentication</Value>
      <Value name="Activity Result Key">Success</Value>
      <Value name="Description">User tdstester8 attempted to
      authenticate using authenticator SecurID_Native. The user
      belongs to security domain SystemDomain</Value>
      <Value name="User First Name">tds</Value>
      <Value name="Actor GUID">
      549e03158d59640a028560f66ebe1e9e</Value>
      <Value name="User ID">tdstester8</Value>
      <Value name="User Identity Source">Internal Database</Value>
      <Value name="User Last Name">tester8</Value>
      <Value name="User Security Domain">SystemDomain</Value>
```

Get User Activity

```
      <Value name="Agent GUID">
       181ccaf08d59640a02XX8d0fb2ff4cb2</Value>
       <Value name="Agent IP">10.100.89.138</Value>
       <Value name="Agent Name">ps-esg-138.ps-esg.com</Value>
       <Value name="Agent Security Domain">SystemDomain</Value>
       <Value name="Agent Type">7</Value>
       <Value name="Argument 1">AUTHN_LOGIN_EVENT</Value>
       <Value name="Argument 2">5</Value>
       <Value name="Argument 3">2</Value>
       <Value name="Argument 8">
       edd5b4748d59640a02b613317d12d748</Value>
       <Value name="Argument 9">000115876401</Value>
       <Value name="Authentication Method">SecurID_Native</Value>
       <Value name="Client IP">10.100.89.138</Value>
       <Value name="INSTANCE_ID">
       eb2049468d59640a0035414XX9e388a6</Value>
       <Value name="LOCAL_LOG_TIME">2012-03-12 12:13:15.284</Value>
       <Value name="Log Level">INFO</Value>
       <Value name="RESULT_KEY">AUTHN_METHOD_SUCCESS</Value>
       <Value name="Result">Authentication method success</Value>
       <Value name="Server Node IP">10.100.89.141</Value>
       <Value name="Session ID">
       07af5e368d59640a01ee94cc0c053bfb-38fG2r6IOMXB</Value>
       <Value name="User ID">tdstester8</Value>
       <Value name="UTC_LOG_TIME">2012-03-12 16:13:15.284</Value>
     </activities>
     <activities Count="30" id="07b155dd8d59640a01da0c6b6b92dc16">
       <Value name="Activity Key">Principal authentication</Value>
       <Value name="Activity Result Key">Success</Value>
       <Value name="Description">User tdstester8 attempted to
       authenticate using authenticator SecurID_Native. The user
       belongs to security domain SystemDomain</Value>
       <Value name="User First Name">tds</Value>
       <Value name="Actor GUID">
       549e03158d59640a028560f66ebe1e9e</Value>
       <Value name="User ID">tdstester8</Value>
       <Value name="User Identity Source">Internal Database</Value>
       <Value name="User Last Name">tester8</Value>
       <Value name="User Security Domain">SystemDomain</Value>
       <Value name="Agent GUID">
       181ccaf08d59640a02XX8d0fb2ff4cb2</Value>
       <Value name="Agent IP">10.100.89.138</Value>
       <Value name="Agent Name">ps-esg-138.ps-esg.com</Value>
       <Value name="Agent Security Domain">SystemDomain</Value>
       <Value name="Agent Type">7</Value>
       <Value name="Argument 1">AUTHN_LOGIN_EVENT</Value>
       <Value name="Argument 2">5</Value>
       <Value name="Argument 3">2</Value>
       <Value name="Argument 8">
       edd5b4748d59640a02b613317d12d748</Value>
      <Value name="Argument 9">000115876401</Value>
```

Get User Activity

```
      <Value name="Authentication Method">SecurID_Native</Value>
      <Value name="Client IP">10.100.89.138</Value>
      <Value name="INSTANCE_ID">
      eb2049468d59640a0035414XX9e388a6</Value>
      <Value name="LOCAL_LOG_TIME">2012-03-12 12:15:24.125</Value>
      <Value name="Log Level">INFO</Value>
      <Value name="RESULT_KEY">AUTHN_METHOD_SUCCESS</Value>
      <Value name="Result">Authentication method success</Value>
      <Value name="Server Node IP">10.100.89.141</Value>
      <Value name="Session ID">
      07b155cd8d59640a01c91378f9fd4e36-SAZY9U7O0OwI</Value>
      <Value name="User ID">tdstester8</Value>
      <Value name="UTC_LOG_TIME">2012-03-12 16:15:24.125</Value>
    </activities>
  </UserActivity>
</serviceResult>
```