SmartPass 7.5
API User Guide

Juniper Network, Inc.
1194 N. Mathilda Avenue
Sunnyvale, CA 94089 USA
408-745-2000
www.juniper.net

Part Number: 730-9502-0282 Rev. B

Trademarks

Juniper Networks, the Juniper Networks logo, NetScreen, NetScreen Technologies, the NetScreen logo, NetScreen-Global Pro, ScreenOS, and GigaScreen are registered trademarks of Juniper Networks, Inc. in the United States and other countries.

The following are trademarks of Juniper Networks, Inc.: ERX, ESP, E-series, Instant Virtual Extranet, Internet Processor, J2300, J4300, J6300, J-Protect, J-series, J-Web, JUNOS, JUNOScope, JUNOScript, JUNOSe, M5, M7i, M10, M10i, M20, M40, M40e, M160, M320, M-series, MMD, NetScreen-5GT, NetScreen-5XP, NetScreen-5XT, NetScreen-25, NetScreen-50, NetScreen-204, NetScreen-208, NetScreen-500, NetScreen-5200, NetScreen-5400, NetScreen-IDP 10, NetScreen-IDP 100, NetScreen-IDP 500, NetScreen-Remote Security Client, NetScreen-Remote VPN Client, NetScreen-SA 1000 Series, NetScreen-SA 3000 Series, NetScreen-SA 5000 Series, NetScreen-SA Central Manager, NetScreen Secure Access, NetScreen-SM 3000, NetScreen-Security Manager, NMC-RX, SDX, Stateful Signature, T320, T640, T-series, and TX Matrix. All other trademarks, service marks, registered trademarks, or registered service marks are the property of their respective owners. All specifications are subject to change without notice. Juniper Networks assumes no responsibility for any inaccuracies in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.

Disclaimer

All statements, specifications, recommendations, and technical information are current or planned as of the date of the publication of this document. They are reliable as of the time of this writing and are presented without warranty of any kind, expressed or implied. In an effort to continuously improve the product and add features, Juniper Networks reserves the right to change any specifications contained in this document without prior notice of any kind.

Copyright © 2011, Juniper Networks, Inc. All rights reserved.

Juniper Networks, the Juniper Networks logo, NetScreen, NetScreen Technologies, the NetScreen logo, NetScreen-Global Pro, ScreenOS, and GigaScreen are registered trademarks of Juniper Networks, Inc. in the United States and other countries.

The following are trademarks of Juniper Networks, Inc.: ERX, ESP, E-series, Instant Virtual Extranet, Internet Processor, J2300, J4300, J6300, J-Protect, J-series, J-Web, JUNOS, JUNOScope, JUNOScript, JUNOSe, M5, M7i, M10, M10i, M20, M40, M40e, M160, M320, M-series, MMD, NetScreen-5GT, NetScreen-5XP, NetScreen-5XT, NetScreen-25, NetScreen-50, NetScreen-204, NetScreen-208, NetScreen-500, NetScreen-5200, NetScreen-5400, NetScreen-IDP 10, NetScreen-IDP 100, NetScreen-IDP 500, NetScreen-Remote Security Client, NetScreen-Remote VPN Client, NetScreen-SA 1000 Series, NetScreen-SA 3000 Series, NetScreen-SA 5000 Series, NetScreen-SA Central Manager, NetScreen Secure Access, NetScreen-SM 3000, NetScreen-Security Manager, NMC-RX, SDX, Stateful Signature, T320, T640, T-series, and TX Matrix. All other trademarks, service marks, registered trademarks, or registered service marks are the property of their respective owners. All specifications are subject to change without notice. Juniper Networks assumes no responsibility for any inaccuracies in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.

Table of Contents

About This Guide

SmartPass 7.5 User's Guide

This guide is intended for network administrators or persons responsible for installing and managing SmartPass 7.5 software.

7.5 API User Guide

SmartPass provides a fully functional REST-based web API that can be used to integrate the data stored in SmartPass with any third party system. The API is described in the SmartPass API Reference Guide.

Internally, RingMaster manages the reporting for the accounting data stored in the SmartPass accounting tables. The actual reporting is performed within RingMaster and the data is provided by SmartPassvia an API.

RingMaster Publication Suite

SmartPass 7.5 is used with RingMaster (versions 6.2 and higher)and allows you to configure SmartPass as an accounting as well as a DAC server and also generate client session reports based on accounting information collected by the **SmartPass** server.

Publications that make up the Ringmaster Publication Suite are:

- *RingMaster 7.1 Quick Start Guide* — This guide provides a description of prerequisites and procedures required to install and begin using RingMaster 7.1 software. Information is provided about system requirements for optimum performance, as well as how to install RingMaster Client and RingMaster Services software.
- *RingMaster Planning Guide* — This guide provides instructions for planning a WLAN with the RingMaster tool suite.It describes RingMaster 7.1 planning tools. It is intended for network administrators or persons responsible for planning a WLAN using RingMaster 7.1 software.
- *RingMaster Configuration Guide* — This guide provides detailed procedures for configuring a Wireless Local Area Network (WLAN) using RingMaster 7.1 software.
- *RingMaster Management Guide* — This guide provides instructions for managing a WLAN with the RingMaster tool suite. It describes RingMaster 7.1 WLAN management and monitoring tools. It is intended for administrators of WLANs using RingMaster 7.1 software.

Mobility System Configuration and Management

SmartPass 7.5 is used with Trapeze Mobility System hardware and software, as described in the following publications:

- *Trapeze Mobility System Software Configuration Guide* — This guide provides instructions for configuring and managing a system using the Trapeze Mobility System Software (MSS) Command Line Interface (CLI).
- *Trapeze Mobility System Software Command Reference* — This publication provides functional and alphabetic reference to all MSS commands supported on MXs and MPs
- *Trapeze Mobility Exchange Hardware Installation Guide* — Instructions and specifications for installing an MX.
- *Trapeze Mobility System Software Quick Start Guide* — Instructions for performing setup of secure (802.1X) and guest (WebAAA™) access, and configuring a Mobility Domain for roaming
- *Trapeze Mobility Point MP-422 Installation Guide* — Instructions and specifications for installing an MP access point and connecting it to an MX.
- *Trapeze Mobility Point MP-620 Installation Guide* — Instructions and specifications for installing the MP-620 access point and connecting it to an MX.

- *Trapeze Regulatory Information* — Important safety instructions and compliance information that you must read before installing Trapeze Networks products

Trapeze Documentation Conventions

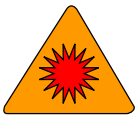
Safety and Advisory Notices

The following types of safety and advisory notices appear in this guide.

This is an Electrostatic Discharge warning.

This is a frame ground message.

This is a Laser warning.



This is a protectrive ground message.

This situation or condition can lead to data loss or damage to the product or other property.

This is a process or procedural tip or other useful suggestion.

This information you should note relevant to the current topic.

This alerts you to a possible risk of personal injury or major equipment problems.

Hypertext Links

Hypertext links appear in Blue.

As an example, this is a link to **Contacting the Technical Assistance Center**.

Text and Syntax Conventions

Trapeze guides use the following text and syntax conventions:

Convention	Use
Monospace text	Sets off command syntax or sample commands and system responses.
Bold text	Highlights commands that you enter or items you select.
Italic text	Designates command variables that you replace with appropriate values or highlights publication titles or words requiring special emphasis.
Bold italic text font	Bold italic text font in narrative, capitalized or not, indicates a program name, function name, or string.
Menu Name > **Command**	Indicates a menu item. For example, **File** > **Exit** indicates that you select **Exit** from the **File** menu.
[ ] (square brackets)	Enclose optional parameters in command syntax.
{ } (curly brackets)	Enclose mandatory parameters in command syntax.
| (vertical bar)	Separates mutually exclusive options in command syntax.

For information about Trapeze support services, visit http://www.trapezenetworks.com/supportportal/, or call 1-866-877-9822 (in the US or Canada) or +1 925-474-2400 and select option 5.

Trapeze Networks sells and services its products primarily through its authorized resellers and distributors. If you purchased your product from an authorized Trapeze reseller or distributor and do not have a service contract with Trapeze Networks, you must contact your local reseller or distributor for technical assistance.

Contacting the Technical Assistance Center

Contact the Trapeze Networks Technical Assistance Center (TAC) by telephone, email, or via web support portal.

- Within the US and Canada, call 1-866-TRPZTAC (1-866-877-9822).
- Within Europe, call +31 35 64 78 193.
- From locations outside the US and Canada, call +1 925-474-2400.
- In non-emergencies, send email to support@trapezenetworks.com
- If you have a service contract or are a Trapeze Authorized Partner, log in to http://www.trapezenetworks.com/supportportal/ to create a ticket online.

TAC Response Time

TAC responds to service requests as follows:

Contact method	Priority	Response time
Telephone	Emergency	One hour
	Non-emergency	Next business day
Email	Non-emergency	Next business day

Information Required When Requesting Service

To expedite your service request, please have the following information available when you call or write to TAC for technical assistance:

- Your company name and address
- Your name, phone number, cell phone or pager number, and email address
- Name, model, and serial number of the product(s) requiring service
- Software version(s) and release number(s)
- Output of the show tech-support command
- Wireless client information
- Description of any problems and status of any troubleshooting effort

Warranty and Software Licenses

Current Trapeze Networks warranty and software licenses are available at http://www.trapezenetworks.com/support/warranty.

Limited Warranty for Hardware and Software

TERMS AND CONDITIONS OF SALE

1. Software

Any software provided is licensed pursuant to the terms and conditions of Trapeze Networks' Software License Agreement, an electronic copy of which is provided with the software ("Software License Agreement") and a printed copy of which is available upon request. The Software License Agreement is incorporated by this reference into these Terms and Conditions of Sale (collectively referred to as "Terms and Conditions of Sale"). In the event of any conflict between the Software License Agreement and these Terms and Conditions of Sale, the Software License Agreement shall control, except for the terms of the limited hardware and software warranty set forth below ("Limited Warranty").

2. Limited Hardware Warranty

Trapeze Networks, Inc. ("Trapeze Networks" or "Trapeze") warrants solely to Customer, subject to the limitation and disclaimer below, that all Trapeze hardware will be free from defects in material and workmanship under normal use as follows: (a) if the hardware was purchased directly from Trapeze Networks, for a period of one (1)

year after original shipment by Trapeze Networks to Customer, (b) if the hardware was purchased from a Trapeze Networks Authorized Distributor or Reseller, for a period of one (1) year from the date of delivery to Customer, but in no event more than fifteen (15) months after the original shipment date by Trapeze, or (c) for certain indoor Mobility Point® access points that are specifically identified on Trapeze's price list for the lifetime of the hardware (each of the foregoing, the "Limited Hardware Warranty"). The date of original shipment from Trapeze Networks will be determined by shipping evidence on file at Trapeze Networks. This Limited Hardware Warranty shall not apply to any third party products provided under this Agreement which shall be subject exclusively to the manufacturers warranty for such products and extends only to the Customer who was the original purchaser of the hardware and may not be transferred to any subsequent repurchasing entity. During the Limited Hardware Warranty period upon proper notice to Trapeze Networks by Customer, Trapeze Networks will, at its sole option, either:

- Repair and return of the defective hardware;
- Replace the defective hardware with a new or refurbished component;
- Replace the defective hardware with a different but similar component that contains compatible features and functions; or
- Refund the original purchase price paid upon presentation of proof of purchase to Trapeze Networks.

3. Restrictions on the Limited Hardware Warranty.

This Limited Hardware Warranty does not apply if the hardware (a) is altered from its original specifications, (b) is installed, configured, implemented or operated in any way that is contrary to its documentation, (c) has damage resulting from negligence, accident, or environmental stress, (d) was subject to unauthorized repair or modification, or (e) is provided to Customer for pre-production, evaluation or charitable purposes.

4. Limited Software Warranty

Trapeze Networks warrants solely to Customer, subject to the limitation and disclaimer below, that the software will substantially conform to its published specifications as follows: (a) if the software was purchased directly from Trapeze Networks, for a period of ninety (90) days after original shipment by Trapeze Networks to Customer, or (b) if the software was purchased from a Trapeze Networks Authorized Distributor or Reseller, for a period of ninety (90) days from the date of delivery to Customer commencing not more than ninety (90) days after original shipment date by Trapeze), ("Limited Software Warranty"). The date of original shipment from Trapeze Networks will be determined by shipping evidence on file at Trapeze Networks. This Limited Software Warranty shall not apply to any third party products provided under this Agreement which shall be subject exclusively to the manufacturers warranty for such products and extends only to the Customer of original purchaser of the software and may not be transferred to any subsequent repurchasing entity.

During the Limited Software Warranty period upon proper notice to Trapeze Networks byCustomer, Trapeze Networks will, at its option, either:

- Use reasonable commercial efforts to attempt to correct or provide workarounds for errors;
- Replace the software with functionally equivalent software; or
- Refund to Customer the license fees paid by Customer for the software.

Trapeze Networks does not warrant or represent that the software is error free or that the software will operate without problems or disruptions. Additionally, and due to the steady and ever-improving development of various attack and intrusion technologies, Trapeze Networks does not warrant or represent that any networks, systems or software provided by Trapeze Networks will be free of all possible methods of access, attack or intrusion.

5. Restrictions on the Limited Software Warranty

This Limited Software Warranty does not apply if the software (a) is altered in any way from its specifications, (b) is installed, configured, implemented or operated in any way that is contrary to its documentation, (c) has damage resulting from negligence, accident, or environmental stress, (d) was subject to unauthorized repair or modification, or (e) is provided to Customer for pre-production, evaluation or charitable purposes

6. General Warranty Disclaimer

EXCEPT AS SPECIFIED IN THIS LIMITED WARRANTY, ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS, AND WARRANTIES INCLUDING, WITHOUT LIMITATION, ANY IMPLIED WARRANTY OR CONDITION OF MERCHANTABILITY, FITNESS FOR A PARTICULAR APPLICATION OR PURPOSE, NONINFRINGEMENT, SATISFACTORY QUALITY OR ARISING FROM A COURSE OF DEALING, LAW, USAGE, OR TRADE PRACTICE, ARE HEREBY EXCLUDED TO THE EXTENT ALLOWED BY APPLICABLE LAW. TO THE EXTENT AN IMPLIED WARRANTY CANNOT BE EXCLUDED, SUCH WARRANTY IS LIMITED IN DURATION TO THE AFOREMENTIONED WARRANTY PERIOD. BECAUSE SOME STATES, COUNTRIES OR JURISDICTIONS DO NOT ALLOW LIMITATIONS ON HOW LONG AN IMPLIED WARRANTY LASTS, THE ABOVE LIMITATION MAY NOT APPLY. THIS LIMITED WARRANTY GIVES YOU SPECIFIC LEGAL RIGHTS, AND YOU MAY ALSO HAVE OTHER RIGHTS, WHICH VARY FROM JURISDICTION TO JURISDICTION. THE LIMITED WARRANTY ABOVE IS THE SOLE REMEDY FOR ANY BREACH OF ANY WARRANTY WITH RESPECT TO THE HARDWARE AND SOFTWARE AND IS IN LIEU OF ANY AND ALL OTHER REMEDIES.

7. Limitation of Liabilities

IN NO EVENT SHALL TRAPEZE NETWORKS, ITS SUPPLIERS, OR ITS AUTHORIZED DISTRIBUTORS OR RESELLERS BE LIABLE TO CUSTOMER OR ANY THRID PARTY FOR ANY LOST REVENUE, PROFIT, OR DATA, OR FOR SPECIAL, INDIRECT, CONSEQUENTIAL, INCIDENTAL, OR PUNITIVE DAMAGES REGARDLESS OF HOW THOSE DAMAGES WERE CAUSED. NOR WILL TRAPEZE NETWORKS, ITS SUPPLIERS, OR ITS AUTHORIZED RESELLERS BE LIABLE FOR ANY MONETARY OR PUNITIVE DAMAGES ARISING OUT OF THE USE OF, OR INABILITY TO USE TRAPEZE NETWORKS HARDWARE OR SOFTWARE. TRAPEZE NETWORKS' LIABILITY SHALL NOT EXCEED THE PRICE PAID BY THE CUSTOMER FOR ANY HARDWARE OR SOFTWARE COVERED UNDER THE TERMS AND CONDITIONS OF THIS WARRANTY. THIS LIMITATION OF LIABILITY AND RESTRICTION ON DAMAGES APPLIES WHETHER IN CONTRACT, TORT, NEGLIGENCE, OR OTHERWISE, AND SHALL APPLY EVEN IF THE LIMITED WARRANTY FAILS OF ITS ESSENTIAL PURPOSE. WARRANTY LAWS VARY FROM JURISDICTION TO JURISDICTION, AND THE ABOVE LIMITATIONS AND EXCLUSION OF CONSEQUENTIAL AND INCIDENTAL DAMAGES MAY NOT APPLY TO YOU, DEPENDING UPON YOUR STATE, COUNTRY OR JURISDICTION.

8. Procedures for Return of Hardware or Software under the Limited Warranty

Where repair or replacement is required under the Limited Warranty, Customer will contact Trapeze Networks and obtain a Return Materials Authorization number ("RMA Number") prior to returning any hardware and/or software, and will include the Trapeze Networks RMA Number on all packaging. Trapeze Networks will ship repaired or replacement components within a commercially reasonable time after receipt of any hardware and/or software returned for the Limited Warranty purposes to the address provided by Customer. Customer will pay freight and handling charges for defective return to the address specified by Trapeze Networks and Trapeze Networks will pay freight and handling charges for return of the repair or replacement materials to Customer.

9. Miscellaneous

These Terms and Conditions of Sale and Limited Warranty shall be governed by and construed in accordance with the laws of the State of California without reference to that State's conflict of laws rules and as if the contract was wholly formed within the State of California. Customer agrees that jurisdiction and venue shall be in Santa Clara County, California. Under no circumstances shall the United Nations Convention on the International Sale of Goods be considered for redress of grievances or adjudication of any warranty or other disputes that include Trapeze Networks hardware or software. If any provision of these Terms and Conditions of Sale are held invalid, then the remainder of these Terms and Conditions of Sale will continue in full force and effect. Where a Customer has entered into a signed contractual agreement with Trapeze Networks for supply of hardware, software or services, the terms of that agreement shall supersede any terms contained within this Terms and Conditions of Sale and Limited Warranty. Customer understands and acknowledges that the terms of this Terms and Conditions of Sale and Limited Warranty, as well as material information regarding the form, function, operation and limitations of Trapeze Networks hardware and software will change from time to time, and that the most current revisions will be publicly available at the Trapeze Networks corporate web site (www.trapezenetworks.com).

Limited Warranty for Hardware and Software

Introduction

SmartPass provides a REST based web API to query and add data to the SmartPass database. The queries can be categorized as authentication, accounting or usage and access control. This document provides an in-depth look at the various available queries with SmartPass, the expected response structure and options that can be added to the query that would provide more specific detail.

Software Licensing for SmartPass

The new licensing scheme used by SmartPass 7.5 includes new SKUs that are more functional and solution based.

SmartPass 7.5 SKUs:

- Guest Access
- Subscriber Management
- Security
- SmartPass Evaluation licenses (SP-EVAL)

  SP-EVAL licenses have all SmartPass 7.5 functionalities available for 50 users and are valid for 90 days from activation.

Guest Access Licensing

The Guest Access License allows the Administrator, Provisioner and Self-Signed User roles to provision guest access, create custom user types, upload bulk users and access the API calls that are specific to that function.

SKU	Version 7.1 or earlier equivalent SKU (transition)	Comments / Description
SP-GA-Base SP	SP	SmartPass Guest Access Base License; Includes 50 guest accounts
SP-GA-50		SmartPass Guest Access License for additional 50 guests; requires current / previous purchase of SP-GA-BASE or SP (SmartPass 7.1 and earlier)
SP- GA-100		SmartPass Guest Access License for additional 100 guests; requires current / previous purchase of SP-GA-BASE or SP (SmartPass 7.1 and earlier)
SP-GA-500		SmartPass Guest Access License for additional 500 guests; requires current / previous purchase of SP-GA-BASE or SP (SmartPass 7.1 and earlier)
SP-GA-2500		SmartPass Guest Access License for additional 2500 guests; requires current / previous purchase of SP-GA-BASE or SP (SmartPass 7.1 and earlier)

User license counts are performed during upgrades to ensure that the number of SmartPass users does not exceed the set number of users in a specific license. Error messages alert you if the maximum numbers of users is exceeded when adding new users.

Subscriber Management Licensing

Subscriber Management licenses allow you to have functionality in the guest access bundle and in the new external Web Portal Authentication capabilities. The RADIUS proxy feature and accounting features are also available as part of this license, including the WEP API operations that are required by RingMaster for Accounting reports.

SKU	Version 7.1 or earlier equivalent SKU (transition)	Comments / Description
SP-SM-UPGR		SmartPass Subscriber Management Base License; Used to upgrade from SP-GA-xx to SP-SM-xx with same user count
SP-SM-50		SmartPass Subscriber Management License for additional 50 accounts; requires current / previous purchase of SP-GA-BASE, or SP (SmartPass 7.1 and earlier)
SP- SM-100		SmartPass Subscriber Management License for additional 100 accounts; requires current / previous purchase of SP-GA-BASE or SP (SmartPass 7.1 and earlier)
SP-SM-500		SmartPass Subscriber Management License for additional 500 accounts; requires current / previous purchase of SP-GA-BASE or SP (SmartPass 7.1 and earlier)
SP-SM-2500	SP-ENT	SmartPass Subscriber Management License for additional 2500 accounts; requires current / previous purchase of SP-GA-BASE or SP (SmartPass 7.1 and earlier)

Security Licensing

The SmartPass Security license allows you to have extended user access control and provides accounting RADIUS proxy capabilities so you can track user activity details. The base license is the SP (a license available in releases prior to 7.5) or the SP-GA-BASE. The maximum number of users that can be in the database is 10,000.

SKU	Version 7.1 or earlier equivalent SKU (transition)	Comments / Description
SP-SEC-ADV	SP-ACC	SmartPass Advanced Security Feature License; Includes location (LA-200/ LA-200E) integration; Dynamic Access Control based on Network Usage, User Identity and Location; requires the current / previous purchase of SP-GA-BASE, SP (SmartPass 7.1 and earlier)

SP-SEC-ADV

The advanced security license is a SmartPass security feature that allows integration with the Location Appliance-200 (LA-200) platform. This is the only difference between the Advanced and Basic security license types. The SP-SEC-ADV license and the SP 7.1 SP-ACC license both allow you to set access rules on the Location Appliance platform.

Upgrading the SP 7.5 License

Upgrading the License Feature Set and User Count

It is important that you use the SP-SM-UPGR license to upgrade a SP-GA-XX license to a SP-SM-XX license. The features offered in the Subscriber Management license are activated only after installation of the SP-SM-XX license.

Upgrading Only the Feature Set

If you are upgrading from SP-GA-XX to SP-SM-XX, you need to install SP-SM-UPGR to go from Guest Access to Subscriber Management functionality. The user count on the upgraded SP-SM-xx license can be increased by adding new user counts to the existing SP-GA-xx license.

If you are a new customer and want only Subscriber Management functions, then you can install the SP-SM-UPGR license to activate the features without increasing the user count.

Downgrading the License Set

Once SP-SM-XX licenses are installed the SmartPass server no longer accepts SP-GA-XX licenses.

Upgrading from a Previous Version of SmartPass

License upgrades from SmartPass 7.0 or 7.1 versions to SP 7.5 licenses are as follows:

- SP is interpreted as SP-GA-BASE
- SP-ENT is interpreted as SP-SM-2500
- SP-ACC is interpreted as SP-SEC-ADV

If you have SP-ACC installed then you receive SP-GA-BASE, SP-SM-2500 and SP-SEC-ADV because the SP-ACC requires SP and SP-ENT licenses.

SmartPass license upgrades do not take place when upgrading SmartPass to 7.5. If you upgrade the SP application without an upgraded license the license file retains SP 7.0 or 7.1 licenses.

Downgrading to an Earlier Version of SmartPass
Downgrading from SmartPass 7.5 to 7.1 or 7.0 requires manual TAC intervention.

Obtaining a SmartPass License

SmartPass is shipped with a Base License and upgrades may be obtained by contacting your authorized Trapeze Networks reseller or partner.

Your Trapeze SmartPass software serial number may be found on the original shipping box and on the CD case.

When you upgrade your license, you receive an Upgrade Coupon that contains a new serial number.

To Upgrade and Activate your new license online:

1. Open a browser window and go to http://www.trapezenetworks.com/support/product_licenses.
2. Click on **Generate a SmartPass license key**.
3. Complete the online form.
4. Click **OK**. Your SmartPass License Key is sent to the e-mail address provided in the online form on the License site.

Scripting / Application Environment

The API calls into SmartPass can be made using standard web or network scripting languages. If there is a general structure or best practice we want to suggest, please provide. The https authentication needed to perform set up operations and access control operations may require administrative credentials. Some operations such as the ability to create users etc can use provisioning or self-sign credentials.

As a general rule SmartPass queries contain options which help filter the responses. While some of the parameters in a query are required others are optional. These optional parameters help with categorizing or filtering results of the query.

SmartPass Authentication API

Get a list of User Types

This API call is used to get the list of all user-types available on the SmartPass server.

Query:

```
https://<SmartPassServerIP>:<PortNumber>/webservice/provision/v1/user-types
```

Response:

```
<USER-TYPES>
         <USER-TYPE name="" duration="" activate_immediately="" start_date=""
         end_date="" time_of_day="" use-lock="" retries="" time_interval=""
         restricted_same_mac="" lock-on-disconnect="" />
         <RESTRICTED-MAC-ADDRESS pattern=" mac_address_pattern1" />
         <RESTRICTED-MAC-ADDRESS pattern="mac_address_pattern2" />
</USER-TYPES>
```

Sample and Query response:

```
https://172.21.64.36/webservice/provision/v1/user-types
```

Sample response:

```
  <?xml version="1.0" encoding="UTF-8" ?>
<USER-TYPES>
         <USER-TYPE name="Business Hours" duration="" activate_immediately="false"
         start_date="" end_date="" time_of_day="Wk0800-1700" use-lock="false"
         retries="3" time_interval="60" restricted_same_mac="false" lock-on-discon-
         nect="true" />
         <USER-TYPE name="5-Days Business Hours" duration="7200"
         activate_immediately="false" start_date="" end_date=""
         time_of_day="Wk0800-1700" use-lock="false" retries="3" time_interval="60"
         restricted_same_mac="false" lock-on-disconnect="true" />
-                  <USER-TYPE name="12-Hours Duration" duration="720"
         activate_immediately="false" start_date="" end_date="" time_of_day=""
         use-lock="false" retries="3" time_interval="60"
         restricted_same_mac="false" lock-on-disconnect="true">
           <RESTRICTED-MAC-ADDRESS pattern="00-0B-0E-*" />
           <RESTRICTED-MAC-ADDRESS pattern="00-0E-11-*" />
           <RESTRICTED-MAC-ADDRESS pattern="00-C4-ED-*" />
           </USER-TYPE>
         <USER-TYPE name="5-Days" duration="7200" activate_immediately="false"
         start_date="" end_date="" time_of_day="" use-lock="false" retries="3"
         time_interval="60" restricted_same_mac="false" lock-on-disconnect="true" /
         >
         <USER-TYPE name="24-Hours Duration" duration="1440"
         activate_immediately="false" start_date="" end_date="" time_of_day=""
         use-lock="false" retries="3" time_interval="60"
         restricted_same_mac="false" lock-on-disconnect="true" />
         <USER-TYPE name="1-Hour Duration" duration="60"
         activate_immediately="false" start_date="" end_date="" time_of_day=""
         use-lock="false" retries="3" time_interval="60"
         restricted_same_mac="false" lock-on-disconnect="true" />
  </USER-TYPES>
```

Get a list of Users

This API call is used to get the list of all users available on the SmartPass server.

Parameter	Value	Description
Username	String (required)	Username for the account created
Password	String (optional)	Default value is “passw” if none specified
user-type	String (optional)	

With some minor changes, the basic request to add, delete, modify or activate a guest account remains the same. Some additional parameters may need to be passed based on the specific use. If no options are passed the response is a list of all users on the SmartPass server.

Query:

```
https://<ServerIPAddress>:<PortNumber>/webservice/provision/v1/users
```

Response:

```
<USERS>
<USER name="janedoe" type="5-Days" password="passw" user-info="next building"
         start-date="03/22/2010-17:05" end-date="03/27/2010-17:05"
         last-login-time="" mac-auth-method="Standard Authentication"
         mac-based-auth-address="" is-bonded-auth="false" email-address="jane-
         doe@itcnetworks.ro" phone-number="40721870190" person-name="jane doe" com-
         pany-name="Trapeze Networks" state="Activated" />

<USER name="test1" type="WebbPortalUser" password="passw" user-info="" start-date=""
         end-date="" last-login-time="" mac-auth-method="Standard Authentication"
         mac-based-auth-address="" is-bonded-auth="false" email-address="jane-
         doe@trpz.com" phone-number="40721870190" person-name="Jim Joy" com-
         pany-name="" state="Activated" />
              </USERS>
```

Add a User

In SmartPass there are various types of authentication - standard user authentication, MAC authentication and MAC-bonded authentication. All three types of users can be created using the API and the calls for them differ slightly

This API call is used to get the list of all users available on the SmartPass server.

Parameter	Value	Description
Op	add|delete|modify|activate| bulk (required)	Action to add / delete / modify or activate a user requires "op" parameter to have the correct value. Activate is used to immediately activate a particular account to override the user-type setting for the activate_immediately parameter. The bulk parameter is used with bulk user creation
Username	String (required)	
Password	String (optional)	Default value is "passw" if none specified
user-type	String (required)	
mac-auth-method	Numeric (optional)	Value of "1" implies MAC authentication in which the username is optional but the "auth-mac addr" parameter is required Value of "2" implies Bonded MAC authentication in which username and MAC address is required.
is-bonded-auth	Boolean (optional)	This parameter indicates whether the user created will be using the bonded authentication mechanism for machine and user auth as defined by Microsoft

auth-mac-addr	String (optional)	This is a parameter used for MAC address authentication
person-name	String (optional)	Person Name
email-address	String (optional)	E-mail Address
phone-number	String (optional)	Mobile Phone Number
company name	String (optional)	Company Name

With some minor changes, the basic request to add, delete, modify or activate a guest account remains the same. Some additional parameters may need to be passed based on the specific use. If no options are passed the response is a list of all users on the SmartPass server.

Standard User Creation

This API call is used to create a standard user with a username and password. If no password parameter is passed in the request, SmartPass will provide a default "passw" as the password. The username and user-type are required parameters that need to be passed.

Sample Query:

```
https://127.0.0.1/webservice/provision/v1/users?op=add&username=jane-
        doe&user-type=5-Days&user-info=next%20building&phone-number=40721870190&ema
        il-address=janedoe@trpz.com&person-name=jane%20doe&company-name=Tra-
        peze%20Networks
```

Sample Response:

```
<USERS>
<USER name="janedoe" type="5-Days" password="passw" user-info="next building"
        start-date="03/22/2010-17:05" end-date="03/27/2010-17:05"
        last-login-time="" mac-auth-method="Standard Authentication"
        mac-based-auth-address="" is-bonded-auth="false" email-address="jane-
        doe@trpz.com" phone-number="40721870190" person-name="jane doe" com-
        pany-name="Trapeze Networks" state="Activated" />
  </USERS>
```

Bulk User Creation

This call provides the ability to create bulk users in a SmartPass server. The usernames and passwords will be automatically generated.

Request URL:

```
https://<SmartPassServer IP>/webservice/provision/v1/users?<requestParameters>
```

Request Parameters:

Parameter	Value	Description
Op	String (required)	To create a number of bulk users, this attribute should have the value of "bulk"
Number	String (required)	The number of created bulk users
user-type	String (required)	The user type of the created bulk users

Request and Response Example:

Sample Query:

```
https://172.21.64.36/webservice/provision/v1/users?op=bulk&num-
        ber=3&user-type=1-Hour%20Duration
```

Expected Response

```
  <?xml version="1.0" encoding="UTF-8" ?>
<USERS>
```

```
        <USER name="kb8aBV" type="1-Hour Duration" password="RXKS9q" start-date=""
        end-date="" last-login-time="" state="Unauthenticated" />
        <USER name="ligD4U" type="1-Hour Duration" password="TbGgaJ" start-date=""
        <USER name="QkFeZX" type="1-Hour Duration" password="b5kvXb" start-date=""
        end-date="" last-login-time="" state="Unauthenticated" />
</USERS>
```

Creating a MAC Address User using the WEB API

The Web API does not allow adding a MAC Address User with a MAC Address that is already associated to another MAC User. If the user tries to add a duplicate MAC Address in this context, SmartPass returns a specific error message stating that the MAC Address is already associated to an existing MAC address user. The username parameter is passed along with the RADIUS-Accept message to the NAS to display instead of the MAC address.

Sample query and response:

```
Query:
https://172.21.64.36/webservice/provision/v1/users?op=add&username=MAC_1&pass-
        word=test&user-type=1-Hour%20Duration&mac-auth-method=1&auth-mac-addr=00:0
        b:0e:00:1a:c5
```

Response

```
<?xml version="1.0" encoding="UTF-8" ?>
<USERS>
        <USER name="MAC_1" type="1-Hour Duration" password="test" start-date=""
        end-date="" last-login-time="" mac-auth-method="MAC Authentication"
        mac-based-auth-address="00-0B-0E-00-1A-C5" is-bonded-auth="false"
        state="Unauthenticated" />
</USERS>
```

Error Response for duplicate MAC address / MAC address already associated:

<?xml version="1.0" encoding="UTF-8" ?>

```
<ERROR>
  <MESSAGE>Error: The MAC Address is already associated to an existing MAC address
        user.</MESSAGE>
</ERROR>
```

Creating a Bonded MAC Address User using the WEB API

A bonded MAC user is an account that needs both the username and the MAC address authenticated before letting the user onto the network. If either the MAC authentication or the username / password authentication fail the authentication fails.

Sample query and response:

Query:

```
https://172.21.64.36/webservice/provision/v1/users?op=add&user-
        name=MAC_Bonded_User1&pass-
        word=test&user-type=1-Hour%20Duration&mac-auth-method=2&auth-mac-addr=00:0
        b:0e:f7:c4:ed
```

Response:

```
<?xml version="1.0" encoding="UTF-8" ?>
<USERS>
        <USER name="MAC_Bonded_User1" type="1-Hour Duration" password="test"
        start-date="" end-date="" last-login-time="" mac-auth-method="Bonded MAC
        Authentication" mac-based-auth-address="00-0B-0E-F7-C4-ED"
        is-bonded-auth="false" state="Unauthenticated" />
</USERS>
```

Creating a Standard User using the WEB API that is also a Bonded Authentication™ user

Sample Query:

```
https://127.0.0.1/webservice/provision/v1/users?op=modify&username=jane-
        doe&user-type=5-Days&user-info=next%20building&phone-number=40721870190&ema
        il-address=janedoe@itcnetworks.ro&person-name=jane%20doe&company-name=Tra-
        peze%20Networks
```

Sample Response:

```
<USERS>
<USER name="janedoe" type="5-Days" password="passw" user-info="next building"
        start-date="03/22/2010-17:05" end-date="03/27/2010-17:05"
        last-login-time="" mac-auth-method="Standard Authentication"
        mac-based-auth-address="" is-bonded-auth="false" email-address="jane-
        doe@itcnetworks.ro" phone-number="40721870190" person-name="jane doe" com-
        pany-name="Trapeze Networks" state="Activated" />
  </USERS>
```

Creating Users with Specific Start and End Dates

Pre-SmartPass 7.5, the time restrictions were defined only based on the user-type definition. If time restrictions are defined on a per-user basis, they take precedence over restrictions defined at user-type level. The table below summarizes all the possible scenarios and shows which time restrictions are used in each case.

The basic rules are:

- API Start Date and End Date take precedence over any User-Type Start Date or End-Date restriction.
- API Start Date and End Date take precedence over User-Type Duration restriction.

Add User API Associate User-Type	No Time Restrictions	Start Date	End Date	Start Date and End Date
No Time Restrictions	**SD**: None **ED**: None	**SD**: API Start-Date **ED**: None	**SD**: None **ED**: API End-Date	**SD**: API Start-Date **ED**: API End-Date
Start Date	**SD**: User-Type Start Date, *after activation* **ED**: None	**SD**: API Start-Date **ED**: None	**SD**: User-Type Start Date, *after activation* **ED**: API End-Date	**SD**: API Start-Date **ED**: API End-Date
End Date	**SD**: None **ED**: User-Type End Date, *after activation*	**SD**: API Start-Date **ED**: User-Type End Date, *after activation*	**SD**: None **ED**: API End-Date	**SD**: API Start-Date **ED**: API End-Date
Start Date and End Date	**SD**: User-Type Start Date, *after activation* **ED**: User-Type Start Date, *after activation*	**SD**: API Start-Date **ED**: User-Type End Date, *after activation*	**SD**: User-Type Start Date, *after activation* **ED**: API End-Date	**SD**: API Start-Date **ED**: API End-Date
Duration	**SD**: Authentication Date ED: Start Date +Duration	**SD**: API Start-Date **ED:** Start Date + Duration	**SD**: Authentication Date **ED:** API-End Date	**SD**: API Start-Date **ED**: API End-Date
Duration and Activate Immediately	**SD:** Creation Date **ED:** Start Date + Duration	**SD**: API Start-Date **ED:** Start Date + Duration	**SD:** Creation Date **ED:** API-End Date	**SD**: API Start-Date **ED:** API-End Date
Start Date and Duration	**SD:** User-Type Start Date, *after activation* **ED:** Start Date + Duration	**SD**: API Start-Date **ED:** Start Date + Duration	**SD:** User-Type Start Date, *after activation* **ED:** API-End Date	**SD**: API Start-Date **ED:** API-End Date
Start Date and Duration and Activate Immediately	**SD:** Creation Date **ED:** Start Date + Duration	**SD**: API Start-Date **ED:** Start Date + Duration	**SD:** Creation Date **ED:** API-End Date	**SD**: API Start-Date **ED:** API-End Date

End Date and Duration	**SD:** None **ED:** User-Type End Date, *after activation*	**SD**: API Start-Date **ED:** Min (Start Date + Duration, User-Type End Date), *after activation*	**SD:** None **ED:** API-End Date	**SD**: API Start-Date **ED:** API-End Date
End Date and Duration and Activate Immediately	**SD:** Creation Date **ED:** Start Date + Duration	**SD**: API Start-Date **ED:** Min (Start Date + Duration, User-Type End Date)	**SD:** Creation Date **ED:** API-End Date	**SD**: API Start-Date **ED:** API-End Date
Start Date and End Date and Duration	**SD:** User-Type Start Date, *after activation* **ED:** Min (Start Date + Duration, User-Type End Date) *after activation*	**SD**: API Start-Date **ED:** Min (Start Date + Duration, User-Type End Date) *after activation*	**SD:** User-Type Start Date, *after activation* **ED:** API-End Date	**SD**: API Start-Date **ED:** API-End Date
Start Date and End Date and Duration and Activate Immediately	**SD:** Creation Date **ED:** Min (Start Date + Duration, User-Type End Date)	**SD**: Min (Start-Date + Duration, User-Type End Date)	**ED:** API-End Date	**ED:** API-End Date

Sample Query:

```
https://localhost/webservice/provision/v1/users?op=add&username=test&pass-
        word=123&user-type=restr&start-date=05/12/2010-17:11&end-date=05/20/
        2010-17:11
```

Sample Response:

```
<USERS>
<USER name="test" type="restr" password="123" user-info="" start-date="05/12/
        2010-17:11" end-date="05/20/2010-17:11" last-login-time=""
        mac-auth-method="Standard Authentication" mac-based-auth-address=""
        is-bonded-auth="false" email-address="" phone-number="" person-name="" com-
        pany-name="" state="Activated"/>
</USERS>
```

Modify a user account

Modifying a Standard User using the WEB API

Sample query and response

Query:

```
https://<SmartPassServerIP>:<PortNumber>/webservice/provision/v1/users?op=mod-
        ify&username=tom&password=foo

<USERS>
        <USER name="tom" type="24-hrs" password="foo" start-date="" end-date=""
        last-login-time="0"  state="Inactive"/>
</USERS>
```

Modifying a Standard User by turning it into a MAC Address User

Query:

```
https://SERVER-IP:SERVER-PORT/webservice/provision/v1/users?op=modify&user-
        name=USER-NAME&password=PASS-
        WORD&user-type=USER-TYPE-NAME&mac-auth-method=1&auth-mac-addr="MAC-ADDRESS"
```

Response:

```
<USERS>
        <USER name="USER-NAME" type="USER-TYPE-NAME" password="PASSWORD"
        start-date="" end-date="" last-login-time="" mac-auth-method="MAC Authenti-
        cation" mac-based-auth-address="MAC-ADDRESS" is-bonded-auth="false" state=
        "Unauthenticated" />
</USERS>
```

The Web API should not allow editing a MAC Address User with a MAC Address that is already associated to another MAC User. If the user tries to add a duplicate MAC Address in this context, SmartPass should return a specific error message stating that the MAC Address is already associated to an existing MAC address user.

Delete a user account

To delete a user, the only parameter required to pass is the username (for all types of authentication - standard, MAC or bonded auth users).

Query:

```
https://172.21.64.36/webservice/provision/v1/users?op=delete&username=test1
```

Response:

```
<?xml version="1.0" encoding="UTF-8" ?>
<INFO>
        <MESSAGE>User test1 has been deleted</MESSAGE>
</INFO>
```

Error Message:

```
Username not found
<?xml version="1.0" encoding="UTF-8" ?>
        <ERROR>
<MESSAGE>The user cannot be found</MESSAGE>
        </ERROR>
Wrong parameter passed (MAC address)
<?xml version="1.0" encoding="UTF-8" ?>
        <ERROR>
<MESSAGE>Invalid UserName</MESSAGE>
        </ERROR>
```

Text Coupon

The Text Coupon action is available through API using the following operation name: text-coupon. The only required parameter is username, any other parameter is ignored. This API is available only if the user has a Subscriber Management SmartPass license.

Sample Query:

```
https://172.21.64.36.444/webservice/provision/v1/users?op=text-coupon&user-
        name=janedoe
```

Sample Response

```
<INFO>
<MESSAGE>The coupon was successfully texted to user 'janedoe'.
</MESSAGE>
  </INFO>
```

Error Message:

The Text Coupon action depends on the SMS configuration and SMTP configuration (for Email-to-SMS profiles). If these are not valid, the Web API response shows the same error messages as the user interface, but specifies the configuration problems. Sample error messages are shown below.

```
<ERROR>
<MESSAGE>The coupon cannot be e-mailed to user 'janedoe' because of the following
        configuration problems: The associated user-type is configured to use the
        Default SMTP Profile, which is not yet defined.</MESSAGE>
</ERROR>
```

SmartPass Accounting / Usage API

Usage Summary API

This API provides data for the usage summary report. It will return all of the session statistics given a certain time interval. Several optional parameters can be used to further filter the available accounting data.

Typically the query would look as follows:

```
https://<SmartPassServerIP>/webservice/reporting/v1/account-
        ing?op=usage_summary&<requestParameters>
```

Summary reports for daily, weekly or monthly reports can be run to find out the number of sessions and connects to the network by each MX or SSID.

Parameter	Value	Description
start-date	String (required)	The request will return all of the accounting sessions that have an event time stamp equal to or greater than this parameter. The format is: MM/DD/YY-HH:MM:SS
end-date	String (required)	The request will return all of the accounting sessions that have an event time stamp equal to or less than this parameter. The format is: MM/DD/YY-HH:MM:SS
acct-ssid	String (optional)	The SSID that the user connected to. Only one SSID can be specified as the request parameter and must match an entry in the database.
nas-ip	String (optional)	The IP address(es) of the NAS(es) that have been sending the accounting information to the SmartPass server. The delimiter for the different NAS IP addresses is represented by a blank space: " " (without the quotation marks).

Sample query and response:

Query:

```
https://172.21.64.36/webservice/provision/v1/account-
        ing?op=usage_summary&start-date=03/01/09-00:00:01&end-date=03/31/
        09-23:59:59
```

Response: (this response has been truncated to conserve space)

```
<?xml version="1.0" encoding="UTF-8" ?>
<ACCOUNTING-SUMMARY>
<SSID-TOTALS>
<SSID ssid-name="alpha-aes" total-ssid-connects="1146" distinct-ssid-users="66" />
<SSID ssid-name="alpha-tkip" total-ssid-connects="66" distinct-ssid-users="5" />
</SSID-TOTALS>
<CLIENTS>
<CLIENT client-mac="00-21-E9-38-1F-A9" name="trapeze\cpechard" cli-
        ent-ip="172.21.50.120" ssid="alpha-tkip" sessions="34"
        usage-time="00:25:33" bytes-sent="105825" bytes-received="377623" />
<CLIENT client-mac="00-19-D2-AF-91-A0" name="TRAPEZE\jpegueros" cli-
        ent-ip="172.21.50.79" ssid="alpha-aes" sessions="7" usage-time="70:41:07"
        bytes-sent="26321152" bytes-received="12168092" />
        .
        .
        .
        .
            <CLIENT client-mac="00-16-CF-A9-DF-51" name="trapeze\tash" cli-
        ent-ip="169.254.184.163" ssid="alpha-aes" sessions="1"
        usage-time="09:49:22" bytes-sent="23098344" bytes-received="39613801" />
</CLIENTS>
```

```
</ACCOUNTING-SUMMARY>
```

Usage Details API

This API provides data for all session details based on accounting records received during the specified time interval. Several optional parameters can be used to further filter the available accounting data.

Typically a request URL to post would be something as below:

```
https://<SmartPassServerIP>/webservice/reporting/v1/account-
        ing?op=usage_details&<OptionalRequestParameters>
```

This query is useful to run usage details for by session for each user, usage at each MX or on each SSID.

Request Parameters:

Parameter	Value	Description
start-date	String (required)	The request will return all of the accounting session details that have an event time stamp equal to or greater than this parameter's value. The format is: MM/DD/YY-HH:MM:SS
end-date	String (required)	The request will return all of the accounting session details that have an event time stamp equal to or less than this parameter's value. The format is: MM/DD/YY-HH:MM:SS
username	String (optional)	The user-name attribute used in the AAA processes. This user-name is uniquely assigned at user creation time. This parameter does not uniquely identify a session.
acct-ssid	String (optional)	The SSID that the user connected to. Only one SSID can be specified as the request parameter and it must match an entry in the database.
client-ip	String (optional)	The IP address contained within the accounting packets corresponding to an accounting session: contents of the Framed-IP-Address attribute. Start packets don't usually have a client IP address in the Framed-IP-Address attribute.
nas-ip	String (optional)	The IP address(es) of the NAS(es) that have been sending the accounting information to the SmartPass server. The delimiter for the different NAS IP addresses is represented by a blank space: " " (without the quotation marks).

Sample query and response:

Query:

```
https://172.21.64.36/webservice/provision/v1/account-
        ing?op=usage_details&start-date=04/23/09-00:00:01&end-date=04/23/
        09-23:59:59&nas-ip=192.168.254.82
```

Response:

```
<?xml version="1.0" encoding="UTF-8" ?>
<ACCOUNTING-DETAILS>
        <CLIENTS>
         <CLIENT
               client-mac="00-21-E9-38-1F-A9"
               client-ip="172.21.50.120"
               username="trapeze\cpechard"
               nas-ip="192.168.254.82"
               ssid="alpha-tkip"
               login-date="2009 Thu Apr 23 10:33:52 PDT"
               session-duration="00:00:36"
               bytes-sent="1325"
               bytes-received="6453"
               locale="Unknown"
               session-status="completed" />

        <CLIENT
              client-mac="00-21-E9-38-1F-A9"
              client-ip="172.21.50.120"
```

```
                username="trapeze\cpechard"
                nas-ip="192.168.254.82"
                ssid="alpha-tkip"
                login-date="2009 Thu Apr 23 10:36:38 PDT"
                session-duration="00:00:36"
                bytes-sent="1375"
                bytes-received="8091"
                locale="Unknown"
                session-status="completed" />

                .
                .
                .
        <CLIENT
                client-mac="00-14-A5-4C-8D-48"
                client-ip="172.21.50.160"
                username="TRAPEZE\yun"
                nas-ip="192.168.254.82"
                ssid="alpha-aes"
                login-date="2009 Thu Apr 23 17:01:35 PDT"
                session-duration="00:00:00"
                bytes-sent="1042"
                bytes-received="8943"
                locale="Unknown"
                session-status="active" />
            </CLIENTS>
          <SESSIONS-TOTALS>
                <TOTAL
                 total-connects="135"
                 total-sessions-duration="74:57:33"
                 total-bytes-sent="189381911"
                 total-bytes-received="1090381247" />
         </SESSIONS-TOTALS>
</ACCOUNTING-DETAILS>
```

Accounting History Details API

This API retrieves data for a given session ID. It returns all of the session accounting packets and their contents as stored in the database entries.

Typically a request URL to post would be something as below:

```
https://<SmartPassServerIP>/webservice/reporting/v1/account-
        ing?op=active_acct_history&acct-session-id=<session-id-value>
```

Request Parameters:

Parameter	Value	Description
acct-session-id	String (required)	The accounting session id that uniquely identifies the session in the database. Example: SESS-462-330a3a-70842-4922a7

Sample query and response:

Query:

```
https://172.21.64.36/webservice/provision/v1/account-
        ing?op=active_acct_history&acct-session-id=SESS-6767-30ea43-507544-0dc6
```

Response:

```
<?xml version="1.0" encoding="UTF-8" ?>
<ACCOUNTING-DETAILS>
<CLIENTS>
       <CLIENT
             client-mac="00-19-7D-52-C4-ED"
```

```
                client-ip="172.21.54.159"
                username="TRAPEZE\spradhan"
                nas-ip="192.168.254.82"
                ssid="alpha-aes"
                login-date="2009-04-23 10:43:16.0"
                session-duration="00:17:26"
                bytes-sent="2651854"
                bytes-received="497811"
                locale="Unknown"
                vlan-name="pm-alpha"
                nas-port-id="AP22/1" />
        <CLIENT
              client-mac="00-19-7D-52-C4-ED"
              client-ip="172.21.54.159"
              username="TRAPEZE\spradhan"
              nas-ip="192.168.254.82"
              ssid="alpha-aes"
              login-date="2009-04-23 10:43:16.0"
              session-duration="00:17:26"
              bytes-sent="2651854"
              bytes-received="497811"
              locale="Unknown"
              vlan-name="pm-alpha"
              nas-port-id="AP22/1" />
        <CLIENT
               client-mac="00-19-7D-52-C4-ED"
               client-ip="172.21.54.159"
               username="TRAPEZE\spradhan"
               nas-ip="192.168.254.82"
               ssid="alpha-aes"
               login-date="2009-04-23 10:43:27.0"
               session-duration="00:17:37"
               bytes-sent="2661956"
               bytes-received="499610"
               locale="Unknown"
               vlan-name="pm-alpha"
               nas-port-id="AP22/2" />
        <CLIENT
               client-mac="00-19-7D-52-C4-ED"
               client-ip="172.21.54.159"
               username="TRAPEZE\spradhan"
               nas-ip="192.168.254.82"
               ssid="alpha-aes"
               login-date="2009-04-23 11:02:09.0"
               session-duration="00:36:19"
               bytes-sent="2662830"
               bytes-received="499610"
               locale="Unknown"
               vlan-name="pm-alpha"
               nas-port-id="AP22/2" />
        </CLIENTS>
</ACCOUNTING-DETAILS>
```

Expected error responses

Bad start date or end date in the request indicates at least one of the required date parameters is missing.

```
<ERROR>
   <CODE>1</CODE>
   <MESSAGE>Invalid start date or end date</MESSAGE>
</ERROR>
```

Mistaken URL

```
<ERROR>
```

```
    <CODE>2</CODE>
    <MESSAGE>Unknown request</MESSAGE>
</ERROR>
```

API not allowed by the SmartPass license

```
<ERROR>
    <CODE>3</CODE>
    <MESSAGE>The web API is not accessible for this license</MESSAGE>
<ERROR>
```

API not allowed by the SmartPass license

SmartPass Call Detail Record (CDR) API

SIP CDR Retrieval

The API method named GET-CDRS allow the retrieval of all or part of the current CDR data stored in the SmartPass database. This feature requires MSS 7.1 GA or higher to be running on the MXs.

A typical structure of the request URL to post would be something as below:

```
https://<SmartPassServerIP>:<PortNumber>/webservice/reporting/v1/
        sip?op=get_cdrs&<requestParameters>
```

Request Parameters:

Parameter	Value	Description
start-date	String (optional)	If specified, this attribute will restrict returned results to CDRs received on or after the specified start-date. If this parameter is missing, no additional restriction will be applied to the returned CDRs.
end-date	String (optional)	If specified, this attribute will restrict returned results to CDRs received on or before the specified end-date. If this parameter is missing, no additional restriction will be applied to the returned CDRs.
user-name	String (optional)	If specified, this attribute will restrict returned results to accounting packets containing a user name matching the specified user-name pattern. The pattern may contain wildcards, e.g. "TRAPEZE*". If this parameter is missing, no additional restriction will be applied to the returned CDRs.
mac-address	String (optional)	If specified, this attribute will restrict returned results to CDRs corresponding to a MAC Address, which matches the given mac-address pattern. The pattern can contain one wildcard at the end of the pattern, e.g. "00:11:2*" If this parameter is missing, no additional restriction will be applied to the returned CDRs.
nas-ip-address	String (optional)	If specified, this attribute will restrict returned results to CDRs received from a NAS whose IP matches the specified nas-ip-address. If this parameter is missing, no additional restriction will be applied to the returned CDRs.

Sample query and response:

Query:

```
https://172.21.16.153:444/webservice/reporting/v1/sip?op=get_cdrs&start-date=03/20/
        09-00:00:01&end-date=03/20/09-23:59:59
Response:
<?xml version="1.0" encoding="UTF-8" ?>
   <CDRS>
    <CDR
        event-timestamp="2009-03-20 15:55:40.0"
        accounting-packet-type="Start"
        user-name="ext. 6007"
        nas-ip="172.21.16.215"
        accounting-session-id="SESS-28-31470a-589561-b0abe8"
        ap-number="AP2/1"
        nas-port-number="28"
        client-mac="00:17:9A:AA:6F:11"
        ap-radio-mac-address="00:0B:0E:45:7A:00"
        sip-call-status="VC_CS_UP_OUT"
        sip-server-address="null"
        calling-station-ip-address="172.21.16.164:51000"
        calling-station-phone-number="6007@172.21.16.191" c
        alling-station-sip-server-ip-address="null"
        called-station-ip-address="172.21.16.191:17784"
        called-station-phone-number="8000@172.21.16.191"
        called-station-sip-server-ip-address="null"
        call-duration="0"
        codec="null"
        data-rate="54 Mb/s"
        rssi="-38"
        call-quality="VC_CQ_EXCELLENT"
        ssid="sip"
        sip-call-id="a9d5b3759be359d7e06c8ad2485044f9@172.21.16.164"
        vlan-name="default"
        sip-call-medium-time="null" />
        .
        .
    <CDR
        event-timestamp="2009-03-20 15:59:57.0"
        accounting-packet-type="Stop"
        user-name="ext 6009"
        nas-ip="172.21.16.215"
        accounting-session-id="SESS-27-31470a-589561-a7e9cb"
        ap-number="AP2/1"
        nas-port-number="27"
        client-mac="00:17:9A:AA:67:9E"
        ap-radio-mac-address="00:0B:0E:45:7A:00"
        sip-call-status="VC_CS_DOWN_OUT"
        sip-server-address="null"
        calling-station-ip-address="172.21.16.165:51000"
        calling-station-phone-number="6009@172.21.16.191"
        calling-station-sip-server-ip-address="null"
        called-station-ip-address="172.21.16.191:14956"
        called-station-phone-number="8000@172.21.16.191"
        called-station-sip-server-ip-address="null"
        call-duration="105"
        codec="null"
        data-rate="54 Mb/s"
        rssi="-37"
        call-quality="VC_CQ_GOOD"
        ssid="sip"
        sip-call-id="6e7218df135dd0cb24af1f4cd9155f62@172.21.16.165"
        vlan-name="default"
        sip-call-medium-time="null" />
</CDRS>
```

SmartPass Access Control API

Disconnect a User / Session

This API call will allow the ability to disconnect a users or sessions. Optional parameters allow the ability to disconnect multiple sessions at a time.

A typical structure of the request URL to post would be something as below:

```
https://<SmartPassServer IP>/webservice/provision/v1/users?op=disconnect&<request-
        Parameters>
```

Request Parameters:

Parameter	Value	Description
username	String (required)	The username of the session to disconnect
user-mac	String (optional)	When used for users that are not created with SmartPass, this attribute is required to be sure that the session is uniquely identified and, more than that, to be able to forward disconnect requests when a user roams on a different MX that the one provided in the request For users created with SmartPass, this attribute is not required.
nas-ip	String (optional)	The IP address of the switch on witch the user wants to send the disconnect message. For users created with SmartPass, this attribute is not required. For others, it is.
secret	String (optional)	Used only in association with nas-ip attribute. If the secret is not provided, we assume that we already have an entry for this IP in the NAS table. If the IP is not found, we return an error message.

Sample query and response:

Query:

```
https://172.21.16.153:444/webservice/provision/v1/users?op=disconnect&user-
        name=test1
```

Response:

```
<?xml version="1.0" encoding="UTF-8" ?>
<INFO>
    <MESSAGE>Operation succeeded</MESSAGE>
</INFO>
```

Change of Authorization for a User / Session

SmartPass allows the change of authorization for a particular active user session by sending RFC 3576 CoA messages to the switch. Various standard and Trapeze specific session attributes can be changed, these are listed in the table below.

A typical structure of the request URL to post would be something as below:

```
https://<SmartPassServer IP>/webservice/provision/v1/users?op=coa&<requestParame-
        ters>
```

Request Parameters:

Parameter	Value	Description
username	String (required)	The username of the session that the change of authorization attributes will be applied to
user-mac	String (optional)	When used for users that are not created with SmartPass, this attribute is required to be sure that the session is uniquely identified and, more than that, to be able to forward coa requests when a user roams on a different MX that the one provided in the request For users created with SmartPass, this attribute is not required.
nas-ip	String (required)	The IP address of the switch on which the user wants to send the disconnect message
secret	String (optional)	If the secret is not provided, we assume that we already have an entry for this IP in the NAS table. If the IP is not found, we return an error message
time-of-day	String (optional)	
end-date	String (optional)	
mobility-profile	String (optional)	
vlan	String (optional)	
acct-interim-interval	String (optional)	
class	String (optional)	
session-timeout	String (optional)	
filter-id	String (optional)	
tunnel-group-id	String (optional)	
replace-username	String (optional)	

Sample query and response:

Query:

```
https://172.21.16.153:444/webservice/provision/v1/users?op=coa&user-
        name=test1&nas-ip=172.21.16.215&filter-id=deny-all
```

Response:

```
<?xml version="1.0" encoding="UTF-8" ?>
   <INFO>
<MESSAGE>Operation succeeded</MESSAGE>
   </INFO>
```

Expected Error Responses

The error responses for both the disconnect user and change of authorization for a session are the same. These error responses along with sample requests are below.

General Error Messages

```
https://127.0.0.1/webservice/provision/v1/users?op=disconnect&username=test
< ERROR >
         <CODE>8</CODE>
         <MESSAGE> Database problems have occurred. Incomplete operation</MESSAGE>
</ ERROR >
```

Invalid or Missing Username in request

```
https://127.0.0.1/webservice/provision/v1/users?op=disconnect&nas-ip=172.31.217.58
< ERROR >
       <CODE>4</CODE>
       <MESSAGE>Invalid UserName</MESSAGE>
</ ERROR >
```

Username not matching any entry in database

https://127.0.0.1/webservice/provision/v1/users?op=disconnect&username=user_not_created

```
< ERROR >
       <CODE>5</CODE>
       <MESSAGE>The user cannot be found</MESSAGE>
</ ERROR >
```

Missing Shared Secret for NAS entry in request

```
https://127.0.0.1/webservice/provision/v1/users?op=disconnect&user-
         name=userdot1x&nas-ip=127.31.217.58&user-mac=00-1A-C1-35-83-7C
< ERROR >
       <CODE>6</CODE>
       <MESSAGE>Could not found an entry for the given NAS IP. Please provide a
         shared secret key also.</MESSAGE>
< ERROR >
```

NACK response from MX

This may be caused due to mis-configuration of the MX-SmartPass dynamic authorization setup or due to a bad shared secret etc. Other cases in which this will occur are passing all required parameters including correct shared secret and NAS IP but wrong MAC address for client or when there is a user in SmartPass with the username mentioned but there is no session record on the MX.

```
<ERROR>
       <CODE>9</CODE>
       <MESSAGE>Received NACK response</MESSAGE>
</ERROR>
```

Bad start date or end date in the request

```
<ERROR>
<CODE>1</CODE>
<MESSAGE>Invalid start date or end date</MESSAGE>
</ERROR>
```

Mistaken URL:

```
<ERROR>
<CODE>2</CODE>
<MESSAGE>Unknown request</MESSAGE>
</ERROR>
```

API not allowed by the SmartPass license

```
<ERROR>
<CODE>3</CODE>
<MESSAGE>The web API is not accessible for this license</MESSAGE>
</ERROR>
```

Error Handling

Unless otherwise specified in the call SmartPass web API will return standard HTTP errors. The following errors have been identified:

- Code 400: Bad request
- Code 403: Forbidden
- Code 503: Service Unavailable

When an error is returned, the following XML fragment will be passed in the HTML body:

```
<ERROR>
<MESSAGE>The error message</MESSAGE>
</ERROR>
```