SMARTPASS

Product Overview

Juniper Networks SmartPass is a security management application that provides dynamic wireless LAN access control over any user or device.

With standards-based APIs, SmartPass integrates easily with third-party applications such as facility management, hospitality registration, and intrusion detection and prevention systems.

As part of Juniper Networks Wireless LAN Management portfolio, SmartPass works with the Juniper Networks WLM1200 Management Appliance to allow real-time access control and dynamic authorization based on a user's physical location. SmartPass also works with Juniper Networks RingMaster to provide custom reporting based on user identity, location, roaming, and activity history.

Product Description

Juniper Networks® SmartPass is part of the Juniper Networks Wireless LAN Management portfolio, along with Juniper Networks RingMaster and the Juniper Networks WLM1200 Wireless LAN Management Appliance. Together, these products unify infrastructure, security, and services management, enabling network administrators to plan, configure, deploy, monitor, and optimize wireless networks of any size and geography—all from one easy to use console.

SmartPass provides advanced location-aware access control with full dynamic authorization for all wireless users and devices. As a security management application, SmartPass helps network managers fine-tune network access and authorization to an extent never before possible, both for primary users and guests, allowing for greater security control and better wireless resource management.

With SmartPass, organizations with an ever-changing user base such as schools, universities, hospitals, and hotels can save time managing mobile users and their devices. For enterprises with visitors who would like temporary wireless access, SmartPass provides non-IT staff with an easy to use interface that allows them to safely provision thousands of guests on demand, without assistance from IT.

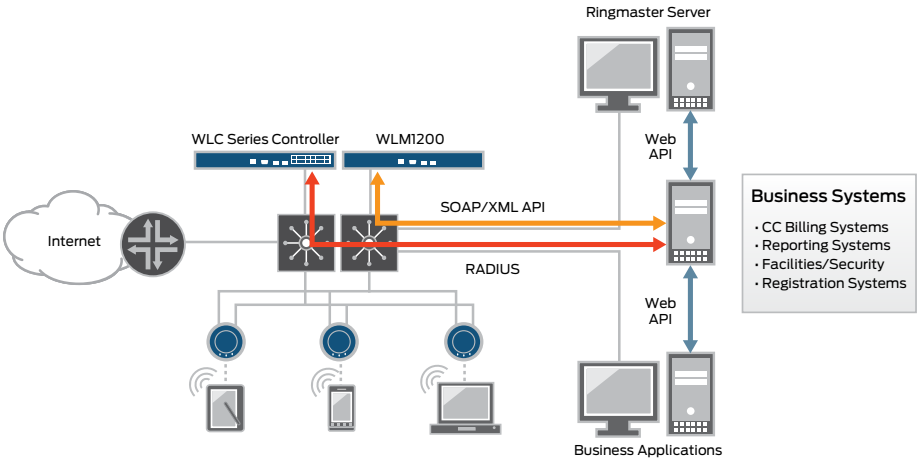

Figure 1. SmartPass integration architecture

Architecture and Key Components

SmartPass provides policy-based dynamic control over client access, and it enables easy provisioning of secure guest access by non-IT personnel.

Features and Benefits

Dynamic Authorization

By taking advantage of existing standards-based RADIUS infrastructures, SmartPass allows for privileges and authorization attributes to be adjusted dynamically, even during the middle of a networking session. Authorization adjustments can be based not only on a user's identity, but also on where users are, what they are doing, what time and day it is, and what others around them are doing as well.

Besides a user's physical location or change in location, SmartPass can dynamically adjust access privileges based on a user's service set identifier (SSID), VLAN, time of day, user's device and predetermined conditions from RADIUS accounting such as session life or amount of traffic passed.

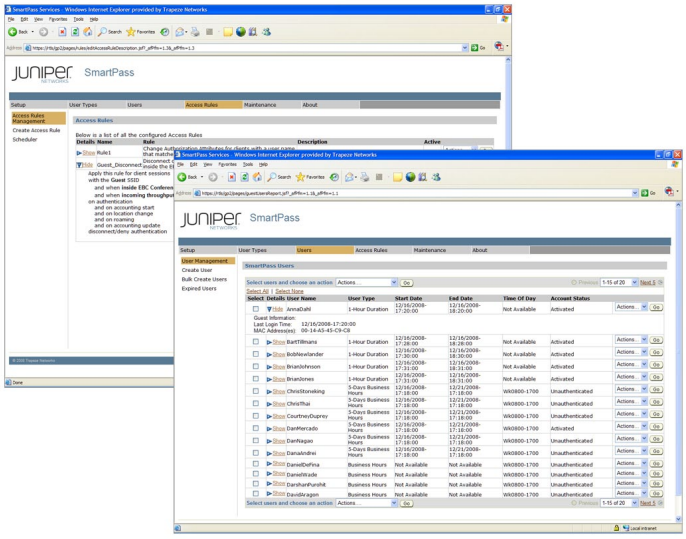

Figure 2. Access control rules and different access profiles

Access Control Rules

SmartPass uses sophisticated Access Control Rules (ACRs) or policies to enact dynamic authorization, allowing for extensive flexibility over the way access is controlled and changed for a user. With SmartPass, ACRs can be invoked on demand by triggering events such as change in location, via a Web API from another application, or by time or date via the SmartPass built-in scheduler.

Location Integration

SmartPass seamlessly integrates with the WLM1200 Management Appliance to obtain up-to-the-minute location positioning for any Wi-Fi device with accuracy to within three meters.

SmartPass combines this location information with a user's RADIUS accounting data, enabling network managers to invoke policies such as allow/deny, change of bandwidth, or change in allowed resources based on the physical location of the client.

Safe, Flexible Guest Provisioning

SmartPass provides guest access functionality with precise control by time of day, day of week, date range, and duration. Predefined guest profile templates are set up for different guest types, including passes for various hour and day designations. Custom guest profiles can be created as well. Additionally, administrators can extend password requirements that are on their corporate network to guests, including exclusion of certain characters, password length enforcement, change of password on first login and composition of the password. Enforcement of guest access policy by device type is also available. Thus, the administrator can have a guest environment with specific device types only.

Ease of Use for Non-IT Staff

With a highly intuitive, easy to use interface, SmartPass allows nontechnical staff such as receptionists and clerks to easily and quickly provision user or guest access accounts on demand, without any networking knowledge. For added convenience, networking managers can control which guest types individual provisioners can manage. SmartPass also provides the ability to create guest accounts in bulk, with intuitive or random user names.

SmartPass makes use of RADIUS credentials so that employees other than front desk staff can safely assign access privileges to their own guests as easily as booking a meeting room. IT can set up security limits and user privileges for different guest types. Administrators can even configure SmartPass to permit guests to self-provision temporary access, using a kiosk or via email and text (SMS).

Guest Credential Notification

SmartPass sends out SMS notifications when guest accounts are set up, and it also prints labels and company branded login instructions with guest credentials. This eliminates manual transcription, removes the risk of errors, and improves productivity before and during a guest's visit.

Scalable, Centralized Architecture

For each guest account, SmartPass uses a centralized guest account database, rather than storing data on a WLAN controller. This ensures that access security is independent of controllers and prevents unauthorized configuration changes from being made to the network by individuals with no domain expertise. In addition, SmartPass scales up to 10,000 users per SmartPass server, making it ideal for conventions, universities, hospitality, healthcare, and large enterprises.

Centralized Captive Portal

SmartPass' centralized architecture also allows for captive portals. This provides network managers an easy, device independent method for authenticating guests and other temporary users via a Web portal. SmartPass only keeps one instance of a captive portal which is served up to any user at any location, regardless of which Juniper Networks WLC Series Wireless LAN Controller is managing the user's authentication. This reduces the maintenance of replication on every controller when changes occur. The centralized architecture also reduces the cost of SSL Certificates. Instead of needing one per controller, only a single certificate is needed on the SmartPass server.

Session Persistence for Handhelds

SmartPass uses a cookie-based mechanism to maintain wireless session persistence for mobile devices. This overrides "sleep" modes and ensures session continuity, eliminating the need for users to log into the captive portal again to re-access applications after a session times out.

Open APIs for System Integration

SmartPass has open, standards-based APIs for easy integration with other systems such as credit card billing, guest registration, facility management, hospitality registration, intrusion detection and prevention, and custom reporting systems. This ensures that the ad hoc granting of secure wireless access can be automated safely and easily within other business processes.

RADIUS Accounting and Reporting

SmartPass uses standards-based RADIUS accounting to calculate and utilize per-user statistics, including lifetime session and total traffic passed for session counts. Reports can be generated in SmartPass, RingMaster, or from a third-party application.

Unified Services Management

SmartPass is tightly integrated with RingMaster, which enables user data, location information, and activity history to be correlated. This leverages collective network intelligence and allows for custom reporting and sophisticated visualization capabilities which dramatically simplify troubleshooting. SmartPass also provides a view into guest and employee session information on the wireless LAN to the extended network infrastructure (firewalls, wired IPD/IDS systems, etc.) using the TNC IF-MAP protocol. SmartPass acts as a MAP client publishing state information to a MAP server to enable applications such as unified policy enforcement (for guests and employees) and role management.

Key Applications

SmartPass granular and dynamic access control is illustrated in the following examples:

- **Controlling Internet and LAN access in classrooms.** A professor giving a test has the ability to change student wireless access, denying access to the Internet from the classroom while allowing access to relevant class materials on the LAN.
- **Restricting corporate guest access**. A large company may want to provide a consultant access to the Internet and certain LAN resources but only while working in an assigned area or building. If the consultant tries to access the network from another location, access will be denied—even with valid login credentials.
- **Limiting excessive bandwidth use**. If a user on the network is consuming an excessive amount of bandwidth, SmartPass throttles down bandwidth and priority for that user after a utilization threshold is crossed within an allotted time period.
- **Providing tiered access services.** SmartPass makes it possible for hotels to offer tiered services based on where someone is, or the accommodation package purchased. A hotel can offer free rate-limited access in public areas, while providing higher bandwidth services for a daily rate in rooms. At the same time, they can offer a special metered service for conference attendees.
- **Geo-fencing**. SmartPass can be used to create a perimeter radio frequency (RF) firewall for a building, preventing anyone outside the firewall from accessing the network, even if they have legitimate credentials.

Specifications

User Access Control

- Creation of custom policies and ACRs based on a combination of filters such as:
  - SSID/wireless network name
  - User name pattern (e.g., domain/username)
  - User type
  - Location
  - Accounting (lifetime or session)
  - Time of day
  - VLAN
  - Device type
- Dynamic disconnect or access attributes change using access control lists (ACLs), bandwidth restrictions, or quality-of-service (QoS) markings for any user session on the network

Guest Management

- Flexible and customizable guest profiles
- Customizable coupons
- Guest access reporting
- Bulk user creation
- Guest user notification via email or SMS
- Options for blocking unauthorized guest access such as multiple sign-in and excessive password retries
- Single click lock-out of guest user

Policy Management

- Separate roles for administrator, provisioner, and self sign-in user
- RADIUS authentication for all provisioner roles
- RADIUS proxy for authenticating against any RADIUS server
- Access reporting per user or media access control (MAC)
- Physical location information as a part of session reporting
- Customizable data traffic and client connection reporting via API

Third-Party Integration

- Fully open, easy to use Representational State Transfer (REST)-based API
- Complete set of functionality:
  - Access control
  - Geo-fencing
  - Custom reporting
  - Guest access integration
- Customizable centralized "captive portal"

Supported Operating Systems

- Windows XP (SP2 and higher)
- Windows 2003
- Windows 2008
- Windows Vista
- Windows 7
- SUSE Linux 10.2 and higher
- Red Hat Enterprise Linux 5.0 and higher
- Supported browsers:
- Internet Explorer 7.0 and higher
- Mozilla Firefox 4.3 and higher

Juniper Networks Services and Support

Juniper Networks is the leader in performance-enabling services that are designed to accelerate, extend, and optimize your high-performance network. Our services allow you to maximize operational efficiency while reducing costs and minimizing risk, achieving a faster time to value for your network. Juniper Networks ensures operational excellence by optimizing the network to maintain required levels of performance, reliability, and availability. For more details, please visit **www.juniper.net/us/en/products-services**.

Ordering Information

Model Number	Description
WLM-SP-GA-BASE	SmartPass Guest Access Base License (includes 50 guest accounts)
WLM-SP-GA-50	SmartPass Guest Access License for additional 50 guests
WLM-SP-GA-100	SmartPass Guest Access License for additional 100 guests
WLM-SP-GA-500	SmartPass Guest Access License for additional 500 guests
WLM-SP-GA-2500	SmartPass Guest Access License for additional 2,500 guests
WLM-SP-SM-50	SmartPass Subscriber Management License for additional 50 accounts. Converts existing WLM-SP-GA licenses to equivalent WLM-SP-SM licenses.
WLM-SP-SM-100	SmartPass Subscriber Management License for additional 100 accounts. Converts existing WLM-SP-GA licenses to equivalent WLM-SP-SM licenses.
WLM-SP-SM-500	SmartPass Subscriber Management License for additional 500 accounts. Converts existing WLM-SP-GA licenses to equivalent WLM-SP-SM licenses.
WLM-SP-SM-2500	SmartPass Subscriber Management License for additional 2,500 accounts. Converts existing WLM-SP-GA licenses to equivalent WLM-SP-SM licenses.
WLM-SP-SECURITY	SmartPass Advanced Security Feature License. Adds Dynamic Access Control with location awareness. Includes location (WLM1200-LA) integration.
WLM-SP-EVAL	SmartPass Evaluation 90-day evaluation license for up to 50 guest accounts.

About Juniper Networks

Juniper Networks is in the business of network innovation. From devices to data centers, from consumers to cloud providers, Juniper Networks delivers the software, silicon and systems that transform the experience and economics of networking. The company serves customers and partners worldwide. Additional information can be found at **www.juniper.net**.

Corporate and Sales Headquarters
Juniper Networks, Inc.
1194 North Mathilda Avenue
Sunnyvale, CA 94089 USA
Phone: 888.JUNIPER (888.586.4737)
or 408.745.2000
Fax: 408.745.2100
www.juniper.net

APAC Headquarters
Juniper Networks (Hong Kong)
26/F, Cityplaza One
1111 King's Road
Taikoo Shing, Hong Kong
Phone: 852.2332.3636
Fax: 852.2574.7803

EMEA Headquarters
Juniper Networks Ireland
Airside Business Park
Swords, County Dublin, Ireland
Phone: 35.31.8903.600
EMEA Sales: 00800.4586.4737
Fax: 35.31.8903.601

To purchase Juniper Networks solutions, please contact your Juniper Networks representative at 1-866-298-6428 or authorized reseller.

1000365-004-EN Oct 2012

Printed on recycled paper