



# WebEx System Management Security Whitepaper

A thick, solid green horizontal bar with a wavy, undulating top edge, spanning the width of the page below the title.

**WebEx Communications Inc.**

3979 Freedom Circle, Santa Clara, CA 95054, U.S.A.

**Corp.:** +1.408.435.7000 **Sales:** 1.877.509.3239

[www.webex.com](http://www.webex.com)

## Introduction

WebEx System Management, part of the WebEx Support Center solution, is a secure, on-demand application that automates tasks associated with desktop management—such as asset management, software updates, patch management, virus protection, and backup management.

System Management provides a responsive, adaptive, and secure hosted infrastructure that ensures the availability, control, and integrity of personal computing devices on every client's network. State-of-the-art security ensures that your network, computers and data are never compromised. Significant resources are devoted to continually develop our world-class security infrastructure with our attention focused on stringent security policies and procedures.

System Management is based on a comprehensive patented computer management services that allow you to easily manage, secure, and support your end-users' computers by reducing the risk, vulnerability, and cost of IT while increasing the security and protection of your network.

The purpose of this document is to provide information on the data security features and functions of System Management in its technology and infrastructure.



# System Management Technology

*The System Management agent uses SSL encryption via ports 80 and 443 to report information about the PC—such as hardware and software inventory, patch status, virus information, and back-up status.*

## The System Management Agent

The core of the System Management service is the System Management Agent (SMA). SMA is a software agent that gets installed and runs on every one of your managed PCs. It receives all of its instructions securely from the System Management Console (SMC), which maintains centralized management for your company.

The SMA is a proprietary software agent that enables remote management of the client PC. Once installed on a PC, its minimal footprint consumes less than 4MB of RAM, ensuring zero impact on the performance of the PC. Communication from the agent to the fully-redundant System Management data centers occurs every fifteen minutes, for round-the-clock device management via the data centers' library of software services. This outbound communication uses 128-bit SSL encryption via ports 80 and 443 to report information about the PC—such as hardware and software inventory, patch status, virus information, and back-up status. Because the agent communication is always outbound and initiated from the client, it provides top level security, managing systems located both inside and outside of the corporate network. This patent pending architecture works in any environment without requiring customers to create holes in their firewalls, or would otherwise introduce vulnerabilities.

Major security features in the SMA:

- Transmits all communications securely over SSL
- Downloads all packages through an authorized source and verifies signatures before execution.
- Encrypts all agent instructions to prevent unauthorized users from gaining elevated privileges.



*The System Management Console undergoes regular penetration testing by internal employees as well as third-party penetration testing companies. The penetration testing is done in accordance with the Web Application Security Consortium guidelines and includes testing on a long list of threat classifications.*

## The System Management Console

IT Administrators are able to use the web-based System Management Console (SMC) to perform all PC management functions to the clients with the System Management agent installed. For example, the Information Security department can distribute software applications and security patches from the SMC enabling the SMA to retrieve the updates by using an outbound communication to pull the software directly from the data centers.

This is made possible because all PC Management (PCM) functions are permissions-based, enabling multiple departments throughout the organization to concurrently use the SMC depending on the specific job function. Additionally, since the SMC is Web-based and proprietary, new features can be easily rolled out to all users ensuring that the latest PCM capabilities are available to all SMC users.

The SMC acts as the portal for managing your computing devices on your network. Because this easy-to-use Web interface is very powerful and affects your entire infrastructure, System Management implements the following security measures:

- Strictly controls and logs every action performed on your assets.
- Uses SSL for enhanced security with every logon.
- Times out user sessions after a specified period of inactivity.
- Logs off users if an IP address changes during an active session.
- Maintains sessions using a unique, encrypted, tamper-proof session ID.
- Requires regular update of user passwords, which must meet complexity criteria.
- Employs granular permissions within the SMC controls to adjust security policies to the types of activities users perform on your assets.

The System Management Console undergoes regular penetration testing by internal employees as well as third-party penetration testing companies. The penetration testing is done in accordance with the Web Application Security Consortium guidelines and includes testing on a long list of threat classifications (Brute Force, Insufficient Authentication, Weak Password Recovery Validation, Credential / Session Prediction, Insufficient Authorization, Insufficient Session Expiration, Session Fixation, Content Spoofing, Cross-site Scripting, Buffer Overflow, Format String Attack, LDAP Injection, OS, Commanding, SQL Injection, SSI Injection, XPath Injection, Directory Indexing, Information Leakage, Path Traversal, Predictable Resource Location, Abuse of Functionality, Denial of Service, Insufficient Anti-automation, Insufficient Process Validation).



*System Management storage service meets and exceeds the CISSP (Certified Information Systems Security Professional) and ISC2 (International Information Systems Security Certification Consortium) security tenets of InfoSec, specifically Confidentiality, Integrity and Availability.*

## System Management Services

Each System Management application service has unique security measures to completely address the intrinsic risks of centralized management of remote PCs. Depending on the services selected these security measures are directly applicable:

- **Online Backup** protects your data using 128-bit AES encryption and key-based authentication (PKI) prior to being transmitted offsite, and can only be retrieved with proper authentication. System Management storage service meets and exceeds the CISSP (Certified Information Systems Security Professional) and ISC2 (International Information Systems Security Certification Consortium) security tenets of InfoSec, specifically with respect to Confidentiality, Integrity and Availability.
- **Remote Access** employs SSL encryption with multiple levels of security and granular access controls to ensure that only authorized personnel accesses the permitted PCs. Remote Access sessions can be logged and recorded for compliance and security purposes. (Please refer to the WebEx Remote Access Security Whitepaper for detail.)
- **Anti-virus Compliance** provides centralized security management. In today's networked environment, security technology alone is not sufficient to protect businesses from the lost productivity, equipment damage and diversion of IT resources that result from continuing vulnerabilities and threats. Even though enterprisewide virus protection is now a core business requirement, many organizations try to protect against viruses by installing numerous security products, resulting in costly and processes that are difficult to manage.
- **Proactive Monitoring and Security Assessment** monitors and evaluates new Microsoft security bulletins and virus reports. New patches are reviewed and classified based on criticality. Patches and virus threats are then immediately communicated to your IT staff along with a recommended course of action.



# System Management Infrastructure

System Management houses its mission critical servers in an outsourced, highly-managed hosted secure environment. This secure environment manages server hardware, networks, power, data, biometrics and staffing.

The data centers' redundant systems include clustered three-node data base servers, multiple front end communication servers, load-balancing, redundant DNS servers, primary and secondary telephone switches with "in-the-cloud" 800-number failover services, network, connectivity and monitoring. A secondary data center is maintained in a California location in the event of a catastrophic event impacting the primary data center located in the Dallas, Texas area.

## Security Technologies

Sophisticated system and network security technologies provide security for the System Management infrastructure, its products and services. These technologies are described below.

**Secure Sockets Layer (SSL)** is an encryption protocol that encodes data sent over the Internet, rendering it unreadable to anyone intercepting the transmission. Used by most e-commerce servers, this high-level security protocol protects the confidentiality and security of data transmitted through the Internet. Based on RSA Data Security's public-key cryptography, SSL is an open protocol that has been submitted to several industry groups as the industry security standard. URLs that begin with "https" indicate that an SSL connection is in place to secure the connection. SSL provides 3 important elements of security: Privacy, Authentication, and Message Integrity.

**Intrusion Detection System (IDS)** is a type of security management system for computers and networks. An IDS gathers and analyzes information from various areas within a computer or a network to identify possible security breaches, which may include both intrusions, or attacks from outside the organization, and misuse, or attacks from within the organization. An IDS system uses vulnerability assessment technology, also known as "scanning," to assess the security of a computer system or network.

**Firewall** is a system of hardware and software components that prevent unauthorized access to or from a private network. Firewalls are frequently used to prevent unauthorized Internet users from accessing private networks connected to the Internet, especially intranets. All messages entering or leaving the intranet pass through the firewall, which examines each message and blocks those that do not meet the specified security criteria.

*The data centers' redundant systems include clustered three-node data base servers, multiple front end communication servers, load-balancing, redundant DNS servers, primary and secondary telephone switches with "in-the-cloud" 800-number failover services, network, connectivity and monitoring.*



*The System Management storage service meets and exceeds the CISSP (Certified Information Systems Security Professional) and ISC2 (International Information Systems Security Certification Consortium) security tenets of InfoSec, specifically with respect to Confidentiality, Integrity and Availability.*

## **Data Security**

Keeping your data secure is critical.

The first level of security addressed within System Management is physical. The primary data center requires both badge access and a palm scan for entry. All servers are installed in secure metal cabinets and are accessible only by authorized data center employees for maintenance or other necessary actions.

System Management backup tapes are stored in secure, offsite vaults by an insured third-party company to protect against fire, flood, and other natural disasters. Iron Mountain Inc., the same company that provides storage solutions for backup tapes and media for most corporations in America, owns and manages the System Management storage service. The System Management storage service meets and exceeds the CISSP (Certified Information Systems Security Professional) and ISC2 (International Information Systems Security Certification Consortium) security tenets of InfoSec, specifically with respect to Confidentiality, Integrity and Availability.

Customers that require data for use on their internal systems may use web service APIs to download this information securely.



## Accreditation

TRUSTe - System Management Console has received the TRUSTe Privacy Seal of Approval. TRUSTe is an independent, nonprofit organization dedicated to enabling individuals and organizations to establish trusting relationships based on respect for personal identity and information in the evolving networked world.

Through extensive consumer and website research, and the support and guidance of many established companies and industry experts, TRUSTe has earned a reputation as the leader in promoting privacy policy disclosure, informed user consent, and consumer education.

### **Data Center Certifications**

The primary data center is provided by Data Return, a managed service provider located in the Dallas, Texas area, manages the primary data center. Data Return has earned the following certifications:

### **Microsoft Gold Certified Partner, Hosting & App Services.**

The Microsoft Gold Certified Partner Program provides recognition to companies that offer hosting and application services that demonstrate, through the program's certification process, a consistent, high quality delivery of solutions built on Microsoft technology and the .NET Framework. The program awards certification status only for those specific hosted or application services that meet eligibility qualifications, proven service quality, and operational readiness benchmarks. Data Return has met these standards since the inception of the Gold Certified program.

### **Hewlett-Packard Service Provider Signature Certified, Hosting Services.**

HP's SP Signature Certification program provides confirmation and recognition that a Service Provider (SP) can consistently deliver reliable services to a defined standard based on industry best practices. The criteria employed during the assessment phase represent a very high standard of service infrastructure and have been drawn from a combination of HP's extensive experience in the design and support of enterprise-level business-critical solutions, and industry best practices such as OGC IT Infrastructure Library (ITIL).

Two levels of certification are offered: SP Certified, based on an assessment of the IT infrastructure used to deliver a named service; and SP Signature Certified, based on an end-to-end assessment of all relevant IT infrastructure and service management practices



involved in the delivery of the named service. Data Return has held Signature Certified status since the inception of the HP SP certification program.

## **SAS 70 Type II.**

Data Return has achieved a SAS-70 Type II certification with an unqualified opinion. This certification represents that Data Return has had its control objectives and control activities examined by an independent accounting and auditing firm and demonstrated that it has adequate controls and safeguards in place for information technology and related processes used to host and process data belonging to customers. This Type II certification not only includes Data Return's description of controls, but also includes detailed testing of the organization's controls over a specified period of time.

The Statement on Auditing Standards (SAS) No. 70, Service Organizations, is an internationally recognized auditing standard developed by the American Institute of Certified Public Accountants (AICPA). A SAS 70 audit or examination is widely recognized, because it represents that a service organization has been through an in-depth audit of their control activities. These activities generally include controls over information technology and related processes. In today's global economy, service organizations or service providers must demonstrate that they have adequate controls and safeguards when they host or process data belonging to their customers.

User organizations that obtain a Service Auditor's Report receive valuable information regarding the service organization's controls and the effectiveness of those controls. The user organization receives a detailed description of the service organization's controls and an independent assessment of whether the controls were placed in operation, suitably designed, and operating effectively (in the case of a Type II report).



## Conclusion

Businesses around the world use WebEx System Management applications. WebEx devotes extensive resources toward implementing and maintaining secure product and infrastructure to ensure that the data entrusted to WebEx by its customers is secure and meets or exceeds the International Information Systems Security Certifications Consortium (IS2) standards of Confidentiality, Integrity and Availability.

©2006 WebEx Communications, Inc. WebEx, WebEx MediaTone, and the WebEx logo are registered trademarks of WebEx Communications, Inc. All rights reserved. All other trademarks are the property of their respective owners.

### Worldwide Sales Offices:

Americas & Canada

Tel: +1.877.509.3239

[AmericasInfo@webex.com](mailto:AmericasInfo@webex.com)

China (HK)

Tel: + 852.8201.0228

[AsiaPacInfo@webex.com](mailto:AsiaPacInfo@webex.com)

Europe, Middle East & Africa

Tel: + 31 (0)20.4108.700

[europe@webex.com](mailto:europe@webex.com)

India

Tel: 080.2228.6377/17030 9330

[sales@cyberbazaarindia.com](mailto:sales@cyberbazaarindia.com)

United Kingdom

Tel: 0800.389.9772

[europe@webex.com](mailto:europe@webex.com)

Japan

Tel: + 81 3 5501 3272

[JapanInfo@webex.com](mailto:JapanInfo@webex.com)

Australia & New Zealand

Tel: + 61 (0)3.9653.9581

[AsiaPacInfo@webex.com](mailto:AsiaPacInfo@webex.com)

