Security overview

Dell™ Email Management Services (EMS™)

Dell™ IT Management Software as a Service

Rev. 1.0, 20100824, JTOL

Commitment to Security

Protecting the integrity of the corporate network and the privacy of sensitive data is of utmost concern to any enterprise. Security is an essential component when providing Internet-based services to corporations. Dell IT Management Software as a Service (SaaS) applications are a portfolio of scalable cloud delivered services for systems management and business continuity that help reduce the risks and cost of managing IT. Dell is dedicated to providing a high level of security for its Dell IT Management SaaS customers and follows rigorous standards to insure the safety and privacy of the IT infrastructure that comprise the Dell IT Management SaaS portfolio of solutions. This document provides an overview of Dell's management of its internal security and privacy protection for the software and hardware that comprise the Dell Email Management Services, and ultimately protects customer information stored in the systems.

Dell Email Management Services

Dell is dedicated to providing a high level of security for Email Management Services (EMS) customers. Dell EMS is designed to provide email continuity, archiving, storage management, comprehensive search and virus/spam protection. Dell EMS is built to address key aspects of security including:

Integrity: Through Secure Socket Layer (SSL), Dell EMS provides industry standard encryption and message authentication to help ensure that customer data ("Customer Data") cannot be modified during transmission.

Confidentiality: Dell EMS is designed to allow only authorized users to access information within the Dell infrastructure. Encrypted transfer of Customer Data is used where it is available.

Availability: Dell EMS uses mission critical, highly robust, top-tier datacenters designed to enable service availability at all times.

Overview

Dell EMS uses the following controls designed to ensure that the integrity, confidentiality and availability of your information meet the highest standards.

Physical controls are countermeasures that effect the physical environment; for example, fire prevention systems, access controls, exit routes.

Technical controls (also called logical controls) are countermeasures that rely upon use of technology to mitigate risk; for example, firewalls, encryption and alternate systems.

Administrative controls are countermeasures that involve policy and procedures; for example, security policies, log audits and testing.

Physical Controls

Exceptional performance from state-of-the-art facilities for mission-critical operations
Dell EMS datacenters are designed to support and protect mission-critical operations. EMS datacenters provide multi-level physical security features and a rigidly controlled operating environment to help protect valuable customer assets and operations.

Access and Security controls

Access to EMS datacenters is highly controlled. All entrances are monitored and have alarms for protection. EMS datacenters are staffed with 24-hour security officers to augment physical security features, which provide protection for your mission-critical Internet operations.

CCTV Digital Recorders

CCTV security cameras monitor designated sensitive areas.

Fire Suppression

Industry standard fire suppression for multi-tenant datacenters are in use.

Environmental Controls

EMS datacenters provide critical power and cooling systems that are provisioned with appropriate redundant failover infrastructure. The critical power and cooling infrastructure is backed up by an emergency power generation system.

Technical Controls

Data Transmission

EMS is designed with security in mind. Customer Data and information collected over the Internet for the purposes of EMS use Secure Sockets Layer (SSL) with 128-bit encryption to protect against unauthorized access from third parties, loss and fraud. This protocol delivers authentication, data encryption and message integrity.

All connection to EMS is outbound from the customer to the Dell EMS datacenter and is made using an HTTPS connection. Archive mail transfer occurs via outbound SFTP connection using AES-128. Upon request, secure communications can be used to communicate to other message transfer agents (MTA) using Transport Layer Security, which encrypts all mail messages transferred between the EMS mail server and a customer MTA.

Authentication

Automated data transfer mechanisms authenticate with EMS using a unique username and password as well as industry standard Certificate Authorities.

User access to EMS occurs via a secure Web interface and Secure Socket Layer (SSL) connection encrypted with the same 128-bit SSL protocol. EMS requires a user to enter a username and password before accessing the system. If an incorrect username or password is entered, then access is not granted. Customers can define password strength and reuse rules, as well as account lockout policies.

Remote administration is performed over an encrypted VPN session that requires a username and password. Administrative passwords are generated and managed solely by Dell. Any attempts to access the system with an incorrect password are rejected and logged.

To access email and Customer Data, users must provide a username and password. The EMS system will only allow access to the specific information that is authorized by the provided credential. Additional authentication steps are required to pass this request from the Web interface to the email database. The EMS system will then retrieve the content based upon the username and password authentication. The authentication controls between the servers is managed by Dell. In addition to access controls, there is also a pass phrase is required when a request is made for Dell to activate the EMS Email Continuity system. This prevents unauthorized activation of the EMS system.

Authorization

All operational agents that manage or have access to Customer Data are subject to the standard Dell security background check. The security background check consists of a criminal check, drug screen, and verification of personally identifying information. As part of the system design, EMS will restrict unauthorized access to Customer Data. Although data center personnel will have physical access to the EMS equipment for emergency purposes, they have no access to the data contained within those systems.

Authorized access is granted to the customer and Dell support. Through multiple layers of access control, customers are only allowed to access their own information. The system is designed to prevent one customer from viewing data from another customer. Controls are put in place at the operating system level and the application level to limit data availability and prevent unauthorized access. Although Dell EMS administrators can view some Customer Data, there are policies in place that dictate this can occur only for troubleshooting purposes. Prior authorization is required from the customer before any access is attempted unless there are extenuating circumstances. This would include, but is not limited to legal requests for the information or an imminent threat to the integrity of the EMS system. In all cases the activity log is maintained and available for review upon request.

Data Storage

All email stored by Dell EMS Email Archive is stored in an encrypted format. Messages are only decrypted for authorized user access. Access to the data stores is authenticated by use of unique credentials and encrypted protocol, and all Archive Reviewer actions are logged.

Anti-Virus Software

The EMS system uses industry standard anti-virus software to scan incoming email for the presence of known viruses. If an infected email message is detected, it is automatically quarantined. A notification is sent to inform the sender that a virus has been detected. Anti-virus definitions are updated on a scheduled and frequent basis.

SyncManager

The SyncManager operates as an NT Service and is therefore restricted to the permissions assigned to the service account. The SyncManager does not require write or modify permissions – only read access. This is typically done by assigning the "View-Only Administrator" role in Microsoft® Exchange. After collecting data, the SyncManager compresses and encrypts the data, and sends it to the secure Dell datacenter by using outbound HTTPS (port 443).

Data Storage

All email stored by Dell EMS Email Archive is stored in an encrypted format. Messages are only decrypted for authorized user access. Access to the data stores is authenticated by use of unique credentials and encrypted protocol, and all Archive Reviewer actions are logged.

Administrative Controls

Data Center Access History

Physical access history to the data centers is recorded.

Personal Data

In performing EMS services, Dell only processes personal data in accordance with customers' instructions and does not disclose customer personal data to third parties, other than those engaged in the provision of the Services or as required by law.

About Dell IT Management Software as a Service solutions

Dell IT Management Software as a Service (SaaS) solutions simplify the management of your IT environment to get you up and running quickly, with lower deployment costs, fewer hassles, and less time spent on non-strategic tasks.

For more information about solutions for your business or organization, contact your Dell account representative or visit dell.com/services.

Availability varies by country. To learn more, customers and Dell Channel Partners should contact your sales representative for more information.

© 2010 Dell Inc. All rights reserved. Microsoft, and Microsoft Windows are registered trademarks of Microsoft Corporation in the United States and other countries. Trademarks and trade names may be used in this document to refer to either the entities claiming the marks and names or their products. Specifications are correct at date of publication but are subject to availability or change without notice at any time. Dell and its affiliates cannot be responsible for errors or omissions in typography or photography. Dell's Terms and Conditions of Sales and Service apply and are available on request. Dell service offerings do not affect consumer's statutory rights.