Service Overview

Distributed Device Management Services helps you track dispersed assets, distribute software and manage patches – no matter where your PC clients are located on the Internet.

- Manage local and remote PCs via the Internet
- Reduce costs with policy-based management
- Minimize network and end-user impact
- Lower infrastructure costs with a SaaS-enabled solution
- Intuitive, easy to configure and use dynamic interface

Protect your PCs and help ensure end-point security with Dell Anti-Malware & Virus Management. Centrally deploy and enforce Symantec™ and McAfee™ anti-virus software and updates for distributed PCs – whether or not they are on the corporate network.

- Automate virus & malware policy compliance – Set policies to ensure the latest software and virus definition files are automatically distributed.

- Infection & vulnerability monitoring – Centrally monitor virus and malware infections, track update compliance and identify known vulnerabilities.

- Scan enforcement – Control outbreaks by centrally activating administrative scans on devices to enable virus identification and quarantine.

Optional Services (additional fees apply)

Custom Services

The following optional custom deployment services may be available for purchase separately (may be defined in a separate statement of work or other signed agreement between the parties):

- Dell Custom Factory Integration services for installing Service-Enabling Software on a new system.
- Distribution of Service-Enabling Software packages to Customer’s Systems and End Users.
- Additional “getting started” assistance, beyond the training included in the standard offer.
- Dell Anti Malware & Virus Administration services for remote management, reporting and updating of Customer Anti-Malware & Virus applications.

Support Procedures

Activation of Services

Customer and Dell will collaborate to complete the following:
- Review minimum technical requirements.
- Assess environment/infrastructure.
- Review network topology.
- Identify office or site locations.
- Identify the preferred Service-Enabling Software distribution method.

Upon completion of this review, a Service-Enabling Software (SES) installer will be provisioned by Dell and Customer will be sent an email activation notice to the technical contact email address along with a Service-Enabling Software deployment guide on how to activate the service and contact Dell for implementation support.

**Installation of Service-Enabling Software**

Support (phone and electronic) is provided to Customer for assistance deploying the Service-Enabling Software as follows:

- Dell shall define and enable the Customer in the Administrator Console.
- Dell shall deliver a configured installer and corresponding installation instructions to Customer IT contact.
- Dell shall provide initial remote online training to Customer’s IT administrators.

**Customer Responsibilities**

- Ensuring that the Service-Enabling Software is installed on all devices to be monitored.
- Customer shall ensure any devices to be managed using active software firewalls (e.g., Zone Alarm) are configured to avoid blocking transmissions to/from the Service-Enabling Software.
- Ensuring applications to be inventoried launch from a standard executable file as defined by the System’s operating system and are not launched from a server or run from within a Web browser.
- Registering all Service-Enabling Software on Dell Software website (provided in email activation notice). Dell will provide Services only for Devices with Registered Service-Enabling Software. Customer may disable or re-assign a Registered Service-Enabling Software at any time, but in no case will previously paid fees be refunded.
- Providing a single point of contact that will serve as the primary Customer counterpart for coordinating services with end-users or groups within the Customer’s IT environment.
- Service-Enabling Software makes extensive use of the System Management BIOS ("SMBIOS") Specification as promulgated by the Distributed Management Task Force (DMTF) and the associated Windows Management Instruction ("WMI") (where applicable) to properly recognize and identify hardware characteristics. Devices that do not support SMBIOS or WMI or that have implemented SMBIOS or WMI improperly, or are not current may display incomplete or erroneous hardware information. Dell makes no claim that the Service-Enabling Software can or will provide support for all hardware, applications or device types.
- Troubleshooting and remediation of virus infections and related issues or errors on End User machines.
- Service-Enabling Software is able to automatically uninstall common pre-existing anti-virus software, but removal of such software is not warranted or guaranteed as part of this Service, and Customer is ultimately responsible for such removal. At Customer’s request, Dell may provide such removal services as an additional or optional managed service offering pursuant to a separate SOW.
- When Service-Enabling Software is uninstalled from any applicable System upon the expiration or earlier termination of the Agreement (or Schedule), any anti-virus and anti-malware software that was resident on any Systems prior to the install of SES will not be reinstalled or restored by Dell. Customer is solely responsible for restoring such software, or obtaining an alternative anti-virus solution or anti-malware solution, at Customer’s own cost.
- Working with Dell to ensure pre-existing Anti-Virus software is removed from systems prior to deploying this Service.
- Deployment and installation on Systems of the selected Anti-Malware & Virus Management Services if provided by Customer.
• Deployment and installation on Systems of the selected Anti-Malware & Virus Management Services if provided by Customer.

Technical Responsibilities and Requirements

• Customer shall ensure, for deployment options and services that require a domain, that a domain(s) exists and all computers to be managed are members of the domain(s).
• Customer shall ensure that the network protocol UDP is allowed to transverse the scanned network.
• Customer shall ensure any devices to be managed using active software firewalls (e.g., Zone Alarm) are configured to avoid blocking transmissions to/from the Service-Enabling Software.
• Customer is responsible for installing or, when applicable, facilitating remote distribution of Service-Enabling Software to its End User Systems.
• Custom reports or reports that differ from standard Dell reporting deliverables.
• Customer is responsible for uninstalling the Service-Enabling Software in order to disable the collection of system configuration data upon termination or expiration of the Term of Subscription Service.
• Customer is responsible for ensuring that FIPS is not enabled on any devices to be managed.

For more information about any of our service offerings, please contact your Dell 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. 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.

Distributed Device Management – Anti-Malware & Virus Management: Offer Specifications; 5/14/2010