



The power to do more



Dell ProSupportTM Proactive Systems Management

Frequently Asked Questions

Proactive Systems Management (PSM) is a Web-based application that enables transparent visibility to your server and storage infrastructure, helps to proactively identify hardware failures and monitors warranty status through a secure portal view of your IT environment.

Available when you purchase a Dell ProSupportTM service contract, Dell Proactive Systems Management provides you with a more efficient and personalized support experience on your covered Dell servers and storage. With Proactive Systems Management, you'll also get access to new ProSupport remote support features at no additional charge.

General Questions

How much does it cost?

The new remote support features are available at no additional charge, based on the level of your Dell ProSupport service contract. If you choose to install PSM yourself, you can receive expert assistance from Dell technical support at no extra charge. However, if you would like Dell to install the software and do an initial discovery of your systems, a fee-based remote installation is available.

How do I get support for Proactive Systems Management?

You can get installation or post installation technical support for PSM by calling the appropriate regional number listed in the table at the following link, [Global Technical Support](#), and following the Special Instructions.

What is the language support for PSM-E 1.4?

As a stand-alone solution PSM-E 1.4 will support all of the languages that are supported today. These include: German, French, Spanish, Italian, and Portuguese.

Supported Systems

Which systems are supported?

All sixth-generation or newer Dell PowerEdge™ servers are supported, including Dell PowerVault MD3000, MD3000i and NX300.

A list of compatible Dell servers and storage can be found [here](#).

Why doesn't Proactive Systems Management currently support EMC and EqualLogic?

Currently both EMC and EqualLogic already have a self-contained phone-home solution that is easy to set up and requires few deployment resources.

Which non-Dell systems are compatible with inventory tracking?

Proactive Systems Management supports the discovery and inventory of a wide variety of servers, including those running AIX, HP-UX, Linux, Novell NetWare, Solaris and Windows.

System Requirements

What are the installation requirements for the Proactive Systems Management proxy?

The proxy software must be installed on a system running one of the following Windows operating systems, using Administrator privileges.

- Windows Server 2008 R2
- Windows 7 Enterprise or Professional, 32-bit or 64-bit
- Windows Vista Business, Enterprise, or Ultimate 32-bit or 64-bit (Service Pack 1 or higher recommended), with User Access Control (UAC) disabled
- Windows XP Professional 32-bit or 64-bit with Service Pack 1 or higher (Service Pack 2 or higher recommended, with the Microsoft firewall's Startup Type set to Manual)
- Windows 2003 Server 32-bit or 64-bit
- Windows 2000 Professional or Server with any Service Pack (Service Pack 4 recommended)

What are the system requirements for monitored servers?

Proactive Systems Management can monitor Dell PowerEdge™ servers with Dell OpenManage™ Server Administrator (OMSA) 4.5 or later installed.

Requirements for Windows® systems:

Monitored Windows assets must meet the following requirements:

- Windows Server 2000, 2003, or 2008
- Dell PowerEdge 6th generation server or higher (e.g., 2650, 6600, 4600)
- OpenManage Server Administrator (OMSA) 4.5 or newer installed on the server to be monitored
- Server, RPC, Remote Registry and TCP/IP NetBIOS Helper services running
- NetBIOS over TCP enabled, in order to allow hostname resolution. Otherwise, the asset's IP address will be used as its hostname.



Requirements for VMware/Linux systems:

Monitored VMware/Linux assets must meet the following requirements:

- Red Hat Enterprise Linux 3, 4, 5, or 6
- SUSE Linux Enterprise Server 10 or 11 (64-bit only)
- VMware ESX (vSphere) 4.1 and 4.5
- VMware ESXi (vSphere) 4.1 and 4.5
- SSH access to Linux/VMware systems
- Dell PowerEdge 6th generation server or higher (e.g., 2650, 6600, 4600)
- OpenManage Server Administrator (OMSA) 4.5 or newer installed on the server to be monitored
- SNMP installed
- UDP ports 161 and 514, and TCP port 161, open between the monitored system and the SilverStreak host

What are the memory and bandwidth requirements for the proxy?

The proxy requires a server with 2 GB to 4 GB of memory (see the [Deployment Guide](#) for specific memory requirements for your environment) and at least 200 MB of available disk space. The proxy bandwidth (both local and external) is usually less than or equal to 20 Kbps. For networks with T1 or greater capacity, bandwidth usage should have a negligible impact on overall traffic.

Features

Which hardware faults are monitored?

On Dell PowerEdge servers, the Proactive Systems Management proxy can monitor roughly 100 hardware fault events. These faults include memory, disk, power supply, controller and other component failures. On Dell PowerVault storage devices, the proxy can monitor such faults as disks, controllers, power supplies, cache batteries and other component failures.

What happens when an Auto-Support Case is created?

When a fault occurs on a system configured with the Auto-Support Case policy, Proactive Systems Management opens a new case with Dell technical support. You receive an email notification containing the case number, and then a support technician contacts you to resolve the issue. If you receive IT Advisory Services (formerly Enterprise-Wide Contract) and Mission Critical support from Dell, you can also configure the Auto-Support Case policy to have a support technician contact you by email or phone.

How does Proactive Systems Management save me time during the troubleshooting process?

When you call Dell for technical support, you are often asked to run a diagnostic utility, such as the Dell System E-Support Tool (DSET), and to send the data to Dell for analysis. Proactive



Systems Management can streamline this process by installing and running the diagnostic tool when an alert occurs, and sending the results to Dell. If you choose to disable the automatic diagnostics, you can still use Proactive Systems Management to run the diagnostics on demand and to automatically send the data to Dell.

Will Dell notify me when my service contracts expire?

Dell notifies you before your service contracts expire to ensure that you do not have a disruption in coverage. When you configure the settings within the PSM portal, you may choose to receive warranty expiration notifications each month, alerting you of any monitored systems service contracts due to expire within a defined time period (such as 30, 60 or 90 days).

What happens to the Proactive Systems Management features when ProSupport coverage on my monitored systems expires?

Proactive Systems Management can help you avoid unintended lapses in coverage by sending monthly service contract expiration email notifications. However, if you allow your Dell ProSupport service contract to expire, the Auto-Support Case monitoring or email alert monitoring on that system will be disabled. You will not receive email notifications of hardware faults, and Dell will not receive new support cases for that system. After you extend your ProSupport contract, you may use the customer portal to re-enable monitoring.

Who receives the warranty expirations notifications?

By default, email notices are sent to primary and secondary contacts for each domain, at notification times that you may specify. Through the Preference Feature, you may also set up other contacts to receive these expiration notifications.

How do I renew my service contracts?

The expiration notification email includes a renewal link. You may request a warranty renewal quote and your Dell representative will contact you to complete the renewal process.

Why doesn't Auto Diagnostics work with ESXi?

Unlike ESX, ESXi does not allow another device to use SSH to access it. This is among the ways that a DSET collection is run on a system that generates an alert. Dell is working to update the DSET version to support ESXi and plan to release this as part of a 1.4.1 maintenance release.

Security and Data Protection

Which types of data does the Proactive Systems Management proxy collect?

The Proactive Systems Management proxy collects system attributes and basic performance



data. System attributes include the make, model, service tag, OS and last reboot time. The proxy does not collect any data stored on the system, any passwords or any information about application usage. Moreover, the only files ever transmitted to Dell are the automated diagnostics files, which are collected when an alert occurs.

How is my data protected?

Dell hosts Proactive Systems Maintenance data — including the application, systems, network and security components — in a US-based data center designed to maintain high levels of availability and security. Dell protects your data by using a wide variety of measures, including:

- **Physical security** — Features include, but are not limited to:
 - On-premises security guards
 - Rigorous exterior building security, including cameras, false entrances, vehicle blockades, specialized parking lot design, bulletproof glass and walls, and the use of an unmarked building
 - Interior pan/tilt/zoom security cameras with digital recorders
- **Network security** — All monitoring components are located behind a firewall and are managed by a Dell network security team. We tightly control all network traffic, requiring all inbound traffic to be transmitted via specific ports and sent and only to appropriate destination network addresses.
- **Server and database security** — Servers and OS components reside on standard images that have undergone security review. We regularly review security updates used by the application, including those published by Microsoft and vendors of other software. When critical security updates are issued, we test them first on nonproduction images and generally apply them to live servers within 48 hours.
- **Procedural security** — Dell groups who have access to Dell Remote Monitoring components (such as the database administration group and the operational support team) are assigned separate duties and access rights. All updates to the production environment go through a well-defined change control process that incorporates checks and balances.
- **Auditing** — Dell retains proprietary monitoring hosting device logs, accessible only by Dell. These logs record all attempts to log into or access the OS or Management Console, as well as every write or escalation operation that is performed by an authenticated user on the Management Console.

