DELL CLIENT
SYSTEMS MANAGEMENT

TAKE CONTROL OF YOUR ENVIRONMENT

Powered by Intel® Core™2 processor with vPro™ technology
Dell simplifies systems management. Dell’s approach delivers systems management solutions that integrate and interoperate to help ease deployment, speed problem resolution, and enable you to manage smarter.

When you invest in Dell™ OptiPlex™ client systems, you gain flexibility of choice to design and deploy the right systems management solution for your environment. You can choose from a suite of optimized, industry standard-based management solutions to integrate into your existing framework, or you can choose Dell Managed Services to manage your clients for you. In addition, you can also create your own custom solution by mixing and matching technologies to run your business your way.
DELL™ SYSTEMS MANAGEMENT OFFERINGS

ONE-TO-ONE MAINTENANCE
Stand-alone Tools:
- Dell Update Package (Software updates)
- Dell ControlPoint (Security options)
- Dell Client Configuration Utility (sets BIOS configuration)
Asset Management Tools:
- OpenManage™ Client Instrumentation agent

DELL REMOTE MANAGEMENT
- Dell Client Manager
- Free Basic Hardware Management
- Upgrade Options
  - Dell Client Manager Plus
  - Dell Client Management Suite

DELL PARTNERSHIP MANAGEMENT
- Microsoft®
  - SCCM Integration (Software/BIOS updates)
  - SCOM Management Packs (Health status monitoring)
- Partner Certification Program (LanDesk)

DELL SERVICES
- Service offerings available to manage part or all client systems
  - Custom solutions

USE DELL SYSTEMS MANAGEMENT TOOLS

Understanding Dell Client Manager (DCM) 3.0
Dell Client Manager™ provides three levels of capability. Each level — Dell Client Manager Standard, Dell Client Manager Plus, and Dell Client Management Suite — builds upon the previous one and leverages the same familiar interface, database, and management agent.

<table>
<thead>
<tr>
<th>FEATURES</th>
<th>STANDARD</th>
<th>PLUS</th>
<th>SUITE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Identify, inventory, and add computers to the pool of managed resources</td>
<td>•</td>
<td>•</td>
<td>•</td>
</tr>
<tr>
<td>Configure or update the BIOS of multiple computers simultaneously</td>
<td>•</td>
<td>•</td>
<td>•</td>
</tr>
<tr>
<td>Monitor the health of key computers</td>
<td>•</td>
<td>•</td>
<td>•</td>
</tr>
<tr>
<td>Enable out-of-band management functionality</td>
<td>•</td>
<td>•</td>
<td>•</td>
</tr>
<tr>
<td>Migrate users to a new computer or OS</td>
<td>•</td>
<td>•</td>
<td>•</td>
</tr>
<tr>
<td>Image new computers or re-image existing computers</td>
<td>•</td>
<td>•</td>
<td>•</td>
</tr>
<tr>
<td>Create, distribute, and install software packages</td>
<td>•</td>
<td>•</td>
<td>•</td>
</tr>
<tr>
<td>Scan computers for detailed OS and application information</td>
<td>•</td>
<td>•</td>
<td>•</td>
</tr>
<tr>
<td>Facilitate compliance with published security patches</td>
<td>•</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Track the distribution and usage of software licenses</td>
<td>•</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Establish and enforce system configuration and software licenses</td>
<td>•</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Take control of a remote computer on a LAN</td>
<td>•</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Centrally manage backup and recovery</td>
<td>•</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Standards Based Management Agent
When installed on each OptiPlex system, OpenManage™ Client Instrumentation (OMCI) is a Standards-based agent allowing administrators to extend their console to perform Dell client hardware management. Available for free download at www.support.dell.com.
REMOTE MANAGEMENT ADVANCES

“Out-of-Band” Management using Intel® vPro™ or Intel®
Standard Manageability
Remote client systems management has traditionally relied on
the client hardware being powered on and the operating system
being up and functional. This type of management has been
known as “in-band” management. In-band management cannot
manage a client device that is either powered off or has an
operating system that is not functioning. The limitations of
in-band management have led to the development of out-of-band
(OOB) capabilities to enable management of a client even
if the system is powered down or the operating system is
non-functional. By performing management communications
directly from the management console to the hardware, OOB
management allows you to manage your client systems
regardless of the power state or OS condition. Implemented
through Intel® Core™2 processors with vPro™ technology or Intel®
Standard Manageability offerings, client systems can now be
managed with no intervention on the client side.

Freedom from Deskside Operations
Out-of-band management is a key component of the Intel®
Core™ 2 processors with vPro™ technology offering, available on
select OptiPlex™ systems. OptiPlex systems with vPro™ technology
can be equipped with Intel® Core™2 Duo or Quad processors
(E8000 and Q9000 series processors), Intel® Q45 chipset, Intel's®
on-board gigabit NIC, and other components working together to
enable superb remote management capabilities.

PROCESSOR
- Intel® Core™2 Duo processor
- Intel® Core™2 Quad processor
- Intel® Virtualization Technology
- Intel® Trusted Execution Technology

CHIPSET
- Security and Manageability
  - Manageability Engine
  - Non-Volatile Memory
  - Intel® Active Management Technology
  - Intel® Virtualization Technology

NETWORK
- Independent Network Access
  - Intel® Active Management Technology

UTILIZE YOUR EXISTING SYSTEMS MANAGEMENT TOOLS

Effective Client Management
with Microsoft
Microsoft® System Center Configuration
Manager (SCCM) provides configuration
management to assess, deploy, and
update client systems effectively.
You gain robust system security and
comprehensive asset management.

Dell Client Update Catalog (DCUC) integrates with Microsoft® SCCM to
automate the process of downloading and synchronizing the latest BIOS,
Firmware, and Driver updates to Dell
Client PCs from the SCCM console.
Through our partnership, DCUC
seamlessly integrates with Microsoft
SCCM products and includes a connection
to Dell’s support site to download the
drivers supported by Microsoft’s SCCM/
SCE formats. IT departments can now
streamline tasks by reducing manual
steps to update new drivers and BIOS to
help improve efficiency.

Discovery and Health Monitoring
with Microsoft
Dell Management Packs for Microsoft
System Center Operations Manager
(SCOM) and Microsoft System Center
Essentials (SCE) enable discovery and
health status monitoring of Dell hardware
by providing alerts on hardware events
and reports on hardware versions,
configuration, and event logs. Dell
Management Packs for SCOM and SCE
are available as no-charge downloads

- Extend problem reporting
  and operations monitoring to
client systems
- Support vPro and Intel Standard
  Manageability functionality using
  Intel Management Pack
- Discover client systems with OMCI
  installed to receive alerts, allow
  shutdown, and reboot
**WHAT'S NEW FOR ADVANCED REMOTE MANAGEMENT IN 2009?**

**Dell Advanced Remote Management**

Dell’s hardware-enabled advanced management features are designed to help simplify operations and reduce costs through advanced remote management capabilities. With select Dell™ OptiPlex™ systems, IT administrators, from a single point-of-control console, have the ability to inventory, remotely diagnose, and protect computers throughout the organization, even if the operating system is unresponsive or the PC is powered off.

- Intel® Core™2 with vPro™ available on the OptiPlex 960 and OptiPlex 755
- Intel® Standard Manageability offering available only on the OptiPlex 760
- Multiple hardware-enabled management system choices with support for out-of-band management capabilities

Dell OptiPlex 755, 760, and 960 desktops feature robust systems management capabilities enabled in the hardware for OS-absent manageability and down-the-wire security, even when the PC is off or the OS is unresponsive. Below is a detailed overview of the features available across our OptiPlex 755 and into our OptiPlex 760 and 960 desktops.

<table>
<thead>
<tr>
<th>FEATURES</th>
<th>755 Intel® Core™2 Duo with vPro™ (Q35 with ICH9DD)</th>
<th>760 Intel® Standard Manageability (Q43 and ICH10DD)</th>
<th>960 Intel® Core™2 Duo or Quad with vPro™ (Q45 and ICH10DD)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Securely power up and power down systems to schedule maintenance tasks (e.g., patches)</td>
<td>•</td>
<td>•</td>
<td>•</td>
</tr>
<tr>
<td>Secure communication within management console via authenticated and encrypted commands (Transport Layer Security)</td>
<td>•</td>
<td>•</td>
<td>•</td>
</tr>
<tr>
<td>Remotely discover and inventory assets such as hardware configuration, OS, BIOS settings, etc. (even when powered down or OS is hung)</td>
<td>•</td>
<td>•</td>
<td>•</td>
</tr>
<tr>
<td>Utilize on-board Non-Volatile Memory (NVM) to store software and hardware asset information</td>
<td>•</td>
<td>•</td>
<td>•</td>
</tr>
<tr>
<td>Access system remotely to diagnose and repair without desk-side visit by rebooting to another location out-of-band</td>
<td>•</td>
<td>•</td>
<td>•</td>
</tr>
<tr>
<td>Check for agent to ensure agent management functioning</td>
<td>•</td>
<td>•</td>
<td>•</td>
</tr>
<tr>
<td>Quarantine infected systems from network for repair to prevent threat from spreading</td>
<td>•</td>
<td>•</td>
<td>•</td>
</tr>
<tr>
<td>Manage OS-absent clients in Cisco NAC-secured networks</td>
<td>•</td>
<td>•</td>
<td>•</td>
</tr>
<tr>
<td>Create Virtual Trusted Desktops (VTD) where security-sensitive applications and data can be isolated to ease the hardware processing load</td>
<td>•</td>
<td>•</td>
<td>•</td>
</tr>
<tr>
<td>Maintain software integrity with Trusted Execution Technology (TXT), which helps ensure applications haven’t been compromised</td>
<td>•</td>
<td>•</td>
<td>•</td>
</tr>
<tr>
<td>Maintain hardware integrity with Intel® AMT Secure Measure to determine whether ME firmware has been compromised</td>
<td>•</td>
<td>•</td>
<td>•</td>
</tr>
<tr>
<td>Audit all admin tasks with Access Monitor with visibility to all logs</td>
<td>•</td>
<td>•</td>
<td>•</td>
</tr>
<tr>
<td>Maintain OS-absent clients in Microsoft® NAP-secured networks</td>
<td>•</td>
<td>•</td>
<td>•</td>
</tr>
<tr>
<td>Enable management of client inside or outside the firewall to initiate a “call for help” via a BIOS screen or alert-triggered connection</td>
<td>•</td>
<td>•</td>
<td>•</td>
</tr>
<tr>
<td>Enable a client device to initiate a remote scheduled maintenance request outside the firewall as programmed by the IT staff</td>
<td>•</td>
<td>•</td>
<td>•</td>
</tr>
</tbody>
</table>
SIMPLY PUT:

DELL SERVICES

Dell can assist you with your provisioning process with the following Custom Factory Integration (CFI) service options:

Factory Provisioning of Intel® Management Engine Private Keys
The Dell factory can pre-provision your system by burning in private keys into the management engine. By pre-provisioning hardware, systems can be directly shipped to the end user’s desk and authenticate to the setup and configuration server without a touch to the client system.

Customization of Intel Management Engine Passwords
Similar to the BIOS password, pre-population of the management engine password helps improve transit security and prevent end user tampering.

Powered by Intel® Core™2 processor with vPro™ technology

SIMPLIFY DESKTOP COMPUTING AT DELL.COM/OptiPlex

1 Intel® Active Management Technology (Intel® AMT) requires the computer system to have an Intel® AMT-enabled chipset, network hardware and software, as well as connection with a power source and a corporate network connection. Setup requires configuration by the purchaser and may require scripting with the management console or further integration into existing security frameworks to enable certain functionality. It may also require modifications of implementation of new business processes. With regard to notebooks, Intel AMT may not be available or certain capabilities may be limited over a host OS-based VPN or when connecting wirelessly, on battery power, sleeping, hibernating or powered off. For more information, see www.intel.com/technology/platform-technology/intel-amt/.

2 No computer system can provide absolute security under all conditions. Intel® Trusted Execution Technology requires a computer system with Intel® Virtualization Technology, an Intel TXT-enabled processor, chipset, BIOS, Authenticated Code Modules and an Intel TXT-compatible measured launched environment (MLE). The MLE could consist of a virtual machine monitor, an OS or an application. In addition, Intel TXT requires the system to contain a TPM v1.2, as defined by the Trusted Computing Group, and specific software for some uses. For more information, see www.intel.com/technology/security.

3 Intel® vPro™ processor technology in 2007 DASH implementation is based on draft DASH 1.0 specifications.

Intel, the Intel logo, Intel Core, Intel vPro, Core Inside and vPro Inside are trademarks of Intel Corporation in the U.S. and other countries.