Faster, simpler employee device management with Dell Client Command Suite

Dell Client Command Suite enabled us to manage Dell desktops with less time and effort than Lenovo systems without the tool

For IT administrators, managing a fleet of employee devices can be as challenging as it is time consuming. Applying dozens of updates to dozens of devices typically means making individual changes to each device, one at a time—even with the robust features that come with the tricky-to-learn Intel® Active Management Technology (AMT), which is one of the Intel vPro™ technologies.

Fortunately, Dell™ Technologies has a solution. Their Dell Client Command Suite integrates with Intel AMT so admins can manage devices through an easy-to-use graphical user interface (GUI).

At Principled Technologies, we compared common device management tasks on two sets of desktops: Dell OptiPlex™ 7050 Micro Desktop devices with Intel AMT and Dell Client Command Suite and Lenovo ThinkCentre M910q desktops with only Intel AMT. We found that, because of Dell Client Command Suite, the Dell desktops were easier to manage than those from Lenovo. Faster, simpler device management can save your admins valuable time so they can get to other mission-critical work for your organization.

Simpler to use

The Dell GUI makes setting up Intel AMT easier than a manual approach

Faster device management

Up to 99.5% less admin time on several common tasks

More efficient management

Update any number of devices simultaneously

The technologies we used

Computers with Intel Core™ vPro™ processors come with Intel Active Management Technology (Intel AMT), a set of tools built into the system's motherboard that enhance management capabilities. Intel AMT, however, is a complex piece of software. Dell Client Command Suite is a host of integrations that simplify and build upon the strong foundation of Intel AMT to deliver a streamlined management experience.

In our tests, we compared management in three scenarios: Using Dell Client Command Suite to remotely manage Dell desktop devices; using only Intel AMT to remotely manage Lenovo desktops; and directly managing Lenovo desktops without Dell Client Command Suite or Intel AMT. In each of our tests, it was faster for an administrator to complete management tasks through Dell Client Command Suite rather than completing tasks with Intel AMT alone, or through direct, manual management. The diagram below shows our three test scenarios:

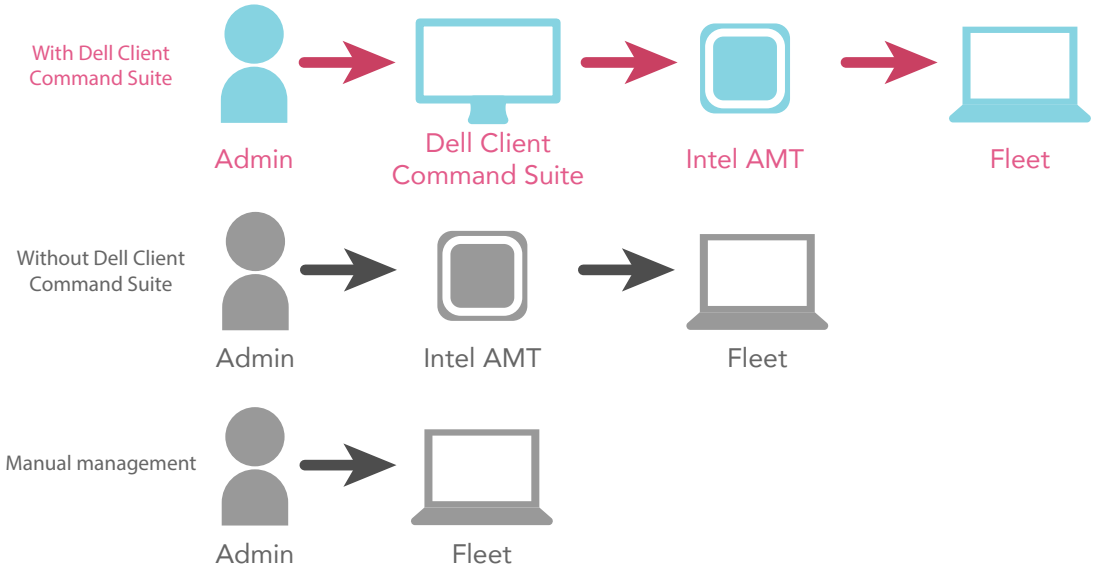


Figure 1: Logical diagram of our three test scenarios

Dell Client Command Suite tools make things easier for admins

Dell Client Command Suite has a ton of features admins can use to manage employee devices with less hassle:

- Task sequences to configure or disable AMT on the target client
- Reports with information on:
  - Out-of-band manageability (BIOS versions, firmware versions, and other information from AMT)
  - Provisioning information (date, time, certificate info)
  - Battery health for laptop devices
  - Hardware inventory reports: the model names of your entire fleet, as well as information on processors, RAM, storage, networks, and IP addresses
- Ability to monitor the state of any device in your fleet

An admin's story: Saving time with Dell Client Command Suite

It's been a sleepless week for Alyssa. Rapidly changing security protocols at her workplace mean she's had to update employee devices multiple times—a task that takes so much time out of her day that she's had to push other admin tasks to late at night.

Alyssa has been reading up on Dell Client Command Suite and thinks it would have been a huge help. Unfortunately, Alyssa's company uses only Lenovo devices, which aren't compatible with Dell Client Command Suite. Let's see what Alyssa's company is missing out on.

Before she could change even a single device's settings via Intel AMT, Alyssa had to spend weeks learning the ins and outs of the technology. In contrast, Dell Client Command Suite simplifies management by automating many tasks in the admin's stead. Configuring Intel AMT is also much easier with Command Suite: Just answer a few prompts and you're done!

Thanks to its one-to-many capabilities, an admin can use Dell Client Command Suite to push a change to as many devices as necessary, all from the same screen. Without Dell Client Command Suite, an admin would have to handle each device individually, wasting valuable time.

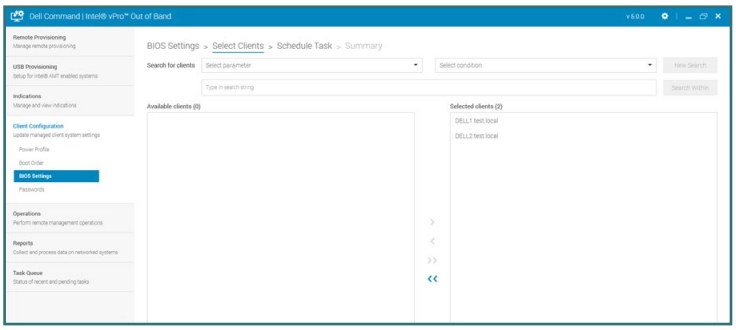


Figure 2: Editing BIOS settings in Dell Client Command Suite

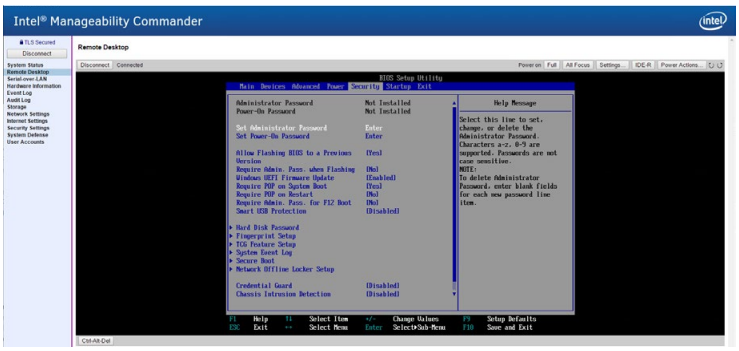


Figure 3: Editing BIOS settings via Intel AMT

Task (1 device)	Dell Client Command Suite	Lenovo (via Intel AMT)	Lenovo Manual
Provisioning Intel AMT	48s	N/A	51s
Changing 10 BIOS settings	1min 35s	1min 53s	2min 01s
Changing a security setting	28s	50s	42s

Table 1: Time to manage one system (tested)

Task (100 devices)	Dell Client Command Suite	Lenovo (via Intel AMT)	Lenovo Manual
Provisioning Intel AMT	48s	N/A	1h 25min 00s
Changing 10 BIOS settings	1min 35s	2h 23min 47s	3h 21min 40s
Changing a security setting	28s	1h 6min 37s	1h 05min 03s

Table 2: Time to manage 100 systems (estimated)

Table 1 is based on our test methodology. It compares how much time Alyssa would take to manage a single device through Dell Client Command Suite, through AMT on a Lenovo device, and without AMT at all. Dell Client Command Suite would save her the most time overall.

Extrapolating to 100 devices reveals a stark contrast: With Dell Client Command Suite, you can finish a management task for all your target devices in one sitting. With a Lenovo system that's incompatible with Dell Client Command Suite, you'd have to configure the devices one at a time. Table 2 shows our extrapolated figures.

Managing an employee fleet with Dell Client Command Suite is also much simpler than managing via Intel AMT alone. For example, changing 10 BIOS settings for 100 devices took just 16 steps with Dell Client Command Suite, but it would take 1,901 steps when using only Intel AMT.

For a detailed time and steps breakdown for the tasks we tested, see the results appendix on page 20.

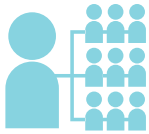
How Dell Client Command Suite saves valuable admin time

How does Dell Client Command Suite save so much time? We tested a variety of features that add up to make management with Dell Client Command Suite less time-intensive than managing through Intel AMT alone. Explore these key features to see how Alyssa's week could have been far less stressful:

Ease of setup

Dell Client Command Suite uses a clean GUI to walk you through Intel AMT configuration, using information you provide to set up the solution for you. Without Dell Client Command Suite, setting up Intel AMT can take many hours of research and trial and error if you aren't already an expert.

One-to-many administration



Traditionally, managing employee devices requires working with each device individually. This adds up to a lot of time wasted for management tasks that need to be applied en masse.

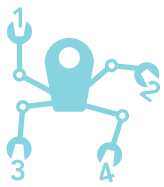
Dell Client Command Suite saves administrators time by only requiring single entry of a command before pushing that command out to any number of employee devices. Through the intuitive GUI, an admin simply specifies her desired changes and selects the target systems—that's the end of her involvement. Dell Client Command Suite then goes to work, sending the command to each targeted system and freeing the admin to take care of whatever's next for the day.

Thanks to this one-to-many capability, Alyssa would take the same amount of time no matter how many devices she configures. Whether it's five, ten, or 100 devices, Alyssa's time commitment would be the same—minimal and streamlined. But without Dell Client Command Suite, the amount of hands-on time grows proportionally with each additional device.

Out-of-band administration

A feature of Intel AMT, out-of-band management means administrators can push updates to employee devices regardless of whether they're turned off or disconnected from your office network. Combined with one-to-many administration, this means Alyssa would be able to push updates to hundreds of machines and not have to worry about whether someone's computer is offline or powered down.

Task sequences

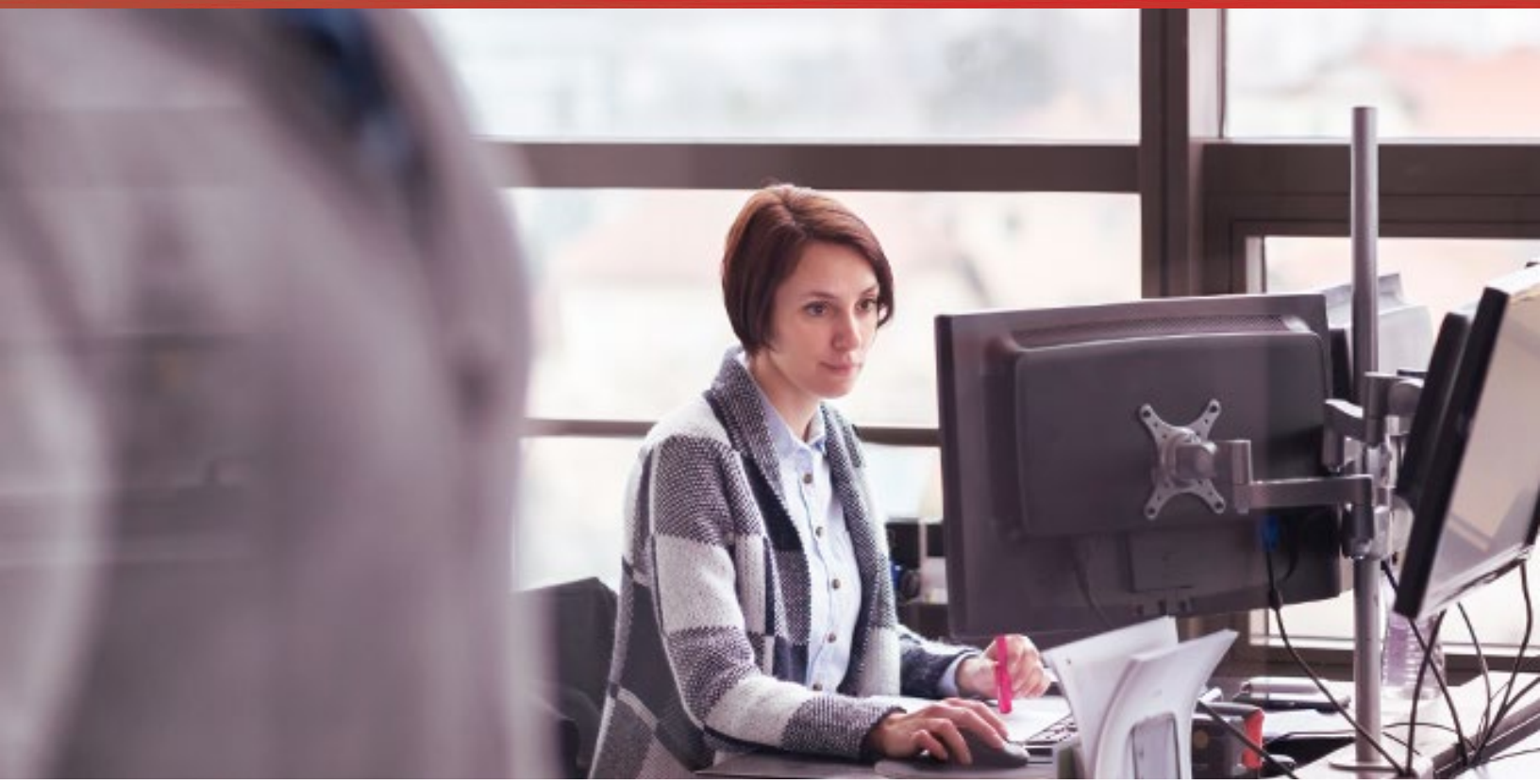


In Dell Client Command Suite, task sequences are automated scripts that run locally on the target client. Dell Client Command Suite comes with a task sequence that configures Intel AMT on target systems. Without task sequences, Alyssa had to manually configure each device, which took up hours of her time.

All these features add up to a more manageable management solution for admins. By the end of her stressful week, Alyssa will be sure to ask her company to invest in Dell Client Command Suite!

Manage devices from anywhere with Intel AMT

Management with Intel AMT can take place from any of your offices, no matter how remote. As long as the target device is connected to the corporate network, you can manage it just as you would your local fleet.



Conclusion

Managing a fleet of employee devices can be a challenging and time-consuming affair for your administrators to handle. But with the right tools, admins like Alyssa could finish their management tasks faster and dedicate their valuable time to other mission-critical work.

At Principled Technologies, we investigated how using Dell Client Command Suite could affect the device management process. We found that the tools afforded by Dell Client Command Suite allow for faster and simpler device management compared to completing tasks through Intel AMT alone on a Lenovo device. The ease of configuring Intel AMT through Dell Client Command Suite, combined with task sequences, out-of-band management capabilities, one-to-many administration, and other features, make Dell Client Command Suite an attractive management solution for fleets with Intel vPro technology.

On January 17, 2018, we finalized the hardware and software configurations we tested. Updates for current and recently released hardware and software appear often, so unavoidably these configurations may not represent the latest versions available when this report appears. For older systems, we chose configurations representative of typical purchases of those systems. We concluded hands-on testing on February 1, 2018.

Appendix A: System configuration information

System	Dell OptiPlex 7050 Micro Desktop	Lenovo ThinkCentre M910q
Processor		
Vendor	Intel®	Intel
Name	Core™ i5	Core i5
Model number	7500T	7500T
Core frequency (GHz)	2.7 – 3.3	2.7 – 3.3
Number of cores	4	4
Cache	6 MB L3	6 MB L3
Memory		
Amount (GB)	8 GB	8 GB
Type	DDR4	DDR4
Speed (MHz)	2,400	2,400
Graphics		
Vendor	Intel	Intel
Model number	HD Graphics 630	HD Graphics 630
Storage		
Amount	1 TB	500 GB
Type	7,200 RPM	7,200 RPM
Connectivity/expansion		
Wired internet	Intel I219-LM	Intel I219-LM
Wireless internet	N/A	N/A
Bluetooth	N/A	N/A
USB	1 x USB 3.1 Gen 1 Type-C Port 5 x USB 3.1 Gen 1 Port	6 x USB 3.0
Video	1 x DisplayPort 1.2 1 x HDMI	2 x DisplayPort 1.2
Display		
Size (in.)	22	22
Type	LED Backlit	LED Backlit
Resolution	1,920 x 1,080	1,920 x 1,080
Touchscreen	No	No

System	Dell OptiPlex 7050 Micro Desktop	Lenovo ThinkCentre M910q
Operating system		
Vendor	Microsoft	Microsoft
Name	Windows 10 Pro	Windows 10 Pro
Build number or version	Build 16299 (1709)	Build 16299 (1709)
BIOS		
BIOS name and version	Dell 1.6.5	Lenovo M1AKT2CA

Appendix B: How we tested

Setting up the tests

Setting up the Microsoft SCCM environment

Configuring Windows Server 2016

After installing Windows Server on our golden VM and installing all updates up to 01/19/2018, we configured Windows by making the following changes. We then cloned the VM to a template to use for all VMs.

Configuring Windows Update

1. In the left pane of the Server Manager window, click Local Server.
2. In the main frame, next to Windows Update, click Not configured.
3. In the Windows Update window, in the main pane, click Let me choose my settings.
4. Under Important updates, select Never check for updates (not recommended), and click OK.
5. In the left pane, click Check for updates, and install all available updates.
6. Close the Windows Update window.

Configuring Windows Firewall

1. In Server Manager, click Tools→Windows Firewall with Advanced Security.
2. In the Overview section, click Windows Firewall Properties.
3. In the Domain Profile tab, for Firewall state, click Off.
4. In the Private Profile tab, for Firewall state, click Off.
5. In the Public Profile tab, for Firewall state, click Off.
6. Click OK.
7. Close the Windows Firewall Properties window.

Setting up Remote Desktop

1. In the Local Server tab of the Server Manager window, next to Remote Desktop, click Disabled.
2. In the System Properties window that appears, in the Remote Desktop section, select the Allow remote connections to this computer radio button, and click OK when the warning message appears.
3. Uncheck Allow connections only from computers running Remote Desktop with Network Level Authentication (recommended) and click OK.

Disabling IE Enhanced Security Configuration

1. In the Local Server tab of the Server Manager window, next to IE Enhanced Security Configuration, click On.
2. In the Internet Explorer Enhanced Security Configuration window, select the Off radio buttons for both Administrators and Users, and click OK.

Installing and configuring the infrastructure server

We cloned our Windows Server 2016 DC VM to create an Active Directory VM, a Certificate Authority VM, and a System Center Configuration Manager VM.

Configuring AD/DNS/DHCP

1. Power on the Active Directory VM.
2. On the Active Directory server, open Windows PowerShell® as administrator.
3. Run the following command: `Install-WindowsFeature RSAT-ADDS`
4. When the installation is finished, close PowerShell.
5. Open Server Manager.
6. On the Welcome screen, click 2, and click Add roles and features.
7. At the initial Before you begin screen, click Next three times.
8. At the Server Roles screen, select Active Directory Domain Services.
9. On the pop-up window, click Add Features.
10. Click Next three times.
11. Verify the desired role is being installed, and click Install.

12. Once installation has finished, close the Add roles and features wizard.
13. In Server Manager, click the flag at the top, and select the Promote this server to a domain controller link.
14. Select Add a new forest, enter a root domain name of `test.local`, and click Next.
15. On the Domain Controller Options screen, enter a password, and click Next.
16. On the DNS Options screen, click Next.
17. On the Additional Options screen, click Next.
18. On the Paths screen, click Next.
19. On the Review Options screen, click Next.
20. On the Prerequisites screen, verify all prerequisites have passed, and click Install.
21. Once Active Directory Domain Services finishes installing, click Finish, and restart the system.

Adding DHCP

1. Open Server Manager.
2. On the Welcome screen, click 2, and click Add roles and features.
3. At the initial Before you begin screen, click Next three times.
4. At the Server Roles screen, select DHCP Server.
5. On the pop-up window, click Add Features.
6. Click Next three times.
7. Verify the desired role is being installed, and click Install.
8. Once installation has finished, close the Add roles and features wizard.
9. In Server Manager, click the flag at the top of the screen and select Complete DHCP configuration.
10. In the DHCP Post-Install configuration wizard window, click Next.
11. At the Authorization Screen, click Commit.
12. At the Summary screen, click Close.
13. In Administrative Tools, open the DHCP service.
14. Expand ad.test.local, then right click IPv4 and select New Scope
15. In the New Scope Wizard window, click Next.
16. At the scope name screen, name the scope Laptops, and click Next.
17. In the IP Address Range, enter the desired scope settings for your network.
18. Click Next four times.
19. At the Router screen, enter the gateway address to be used by the clients, and click Next.
20. Click Next three times.
21. At the Completing the New Scope Wizard screen, click Finish.

Creating Containers and Extending the AD Schema

1. On the Domain Controller, run ADSI Edit.
2. On the toolbar, select Action→Connect to…
3. Accept the defaults by clicking OK.
4. Under Default Naming Context→DC- test, DC=local, right-click CN = System, and select New→Object…
5. Select Container, and click Next.
6. Under Value, enter System Management. Click Next, and click Finish.
7. Run Active Directory Users and Computers.
8. On the toolbar, select View, and click Advanced Features.
9. Under test.local→System, right click System Management. Choose Delegate Control.
10. Click Next.
11. Click Add.
12. Click Object Types and select Computers, then click OK.
13. Enter CM, the computer account for the configuration server, as an object name and click OK.
14. Click Next.
15. Select Create a custom task to delegate, and click Next.
16. Choose This folder, existing objects… and click Next.
17. Click Full Control, and click Next.
18. Click Finish.
19. Attach the SCCM installation media to the VM.
20. From the installation media, navigate to \SMSSETUP\BIN\X64. Right-click extadsch, and run as administrator.
21. Review extadsch.log at the root of the system drive to confirm the operation was successful.

Creating Active Directory accounts for System Center Configuration Manager

1. On the Domain Controller, open Active Directory Administrative Center
2. Under test (local), in the Tasks panel, click New, and select Group from the drop-down menu.
3. In the Create Group window, use the following options:
   - **Group name:** Kerberos Admins
   - **Group type:** Security
   - **Group scope:** Global
4. Add Kerberos Admins as a member of the Domain Admins group.
5. Add the computer account of the SCCM server to the Kerberos Admins security group and click OK.
6. Create an Organizational Unit for AMT managed systems called AMT Managed.
7. Create a security group called AMT Control.

Configuring the environment

Configuring Post Active Directory Deployment

1. On the Certificate Authority and Configuration Manager servers, change the name of the server. For Certificate Authority, name it CA. For the Configuration Manager server, name it CM.
2. Set a static IP address for each server.
3. Join each server to the domain using the Join domain option.

Adding the configuration manager server as a trusted server

1. On the Certificate Authority and Configuration Manager servers, run `lusrmgr.msc`
2. Select Groups.
3. Right-click Administrators, and click Properties.
4. Click Add.
5. Select Object Types, check the box for Computers, and click OK.
6. Add the computer name for the management server.

Installing SQL 2016

1. Log into the Configuration Manager server as domain\administrator.
2. Attach the installation media for SQL 2016, and run the setup.exe file.
3. In the SQL Server Installation Window, select Installation from the menu on the left, and select New SQL Server stand-alone installation or add features to an existing installation.
4. In the SQL Server 2016 Setup Window, allow it to check prerequisites. When this is process is complete, click Next.
5. In the SQL Server 2016 Setup Window, at the Product Updates screen, click Next.
6. At the Install Setup Files screen, allow the wizard to install the files.
7. At the Setup Support rules screen, click Next.
8. At the Product Key screen, enter a valid product key, and click Next.
9. At the License Terms screen, accept the license terms, and click Next.
10. At the Setup Role screen, select SQL Server Feature Installation, and click Next.
11. At the Feature Selection screen, under Instances Features, select Database Engine Services with Full-Text and Semantic Extractions for Search and Data Quality Services, Reporting Services - Native, and SQL Client Connectivity SDK. Click Next.
12. Allow the Installation Rules check to run, and click Next.
13. At the Instance Configuration screen, select Default Instance and leave the default Instance ID.
14. At the Disk Space Requirements screen, click Next.
15. At the Server Configuration screen, set Startup Type for Server Agent, SQL Server Database Engine, and Server Browser as Automatic, and click Next.
16. At the Database Engine Configuration screen, select Mixed authentication mode, and add a password.
17. Click Add Current user.
18. Click Next three times.
19. Verify that the Summary is correct, and click Install.
20. Click finish when prompted.
21. Download Microsoft SQL Server Management Studio 17.4 from https://docs.microsoft.com/en-us/sql/ssms/download-sql-server-management-studio-ssms, and install using all defaults.
22. Open Microsoft SQL Server Management Studio.
23. Sign into your SQL database.

24. Right-click your SQL host, and select Properties.
25. Select the memory page.
26. Change the minimum server memory to 8192.
27. Change maximum server memory to `16384`. Click OK.
28. Click SQL Server Services in the tree.
29. Right-click SQL Server (Instance Name).
30. On the Log On tab, change the Account Name to test\administrator.
31. A popup will request to restart the service. Select Yes.

Installing the Certificate Authority

1. On the Certificate Authority Server, log in using the test.local\administrator account.
2. Launch Server Manager.
3. Click Add roles and features.
4. In the Add Roles and Features Wizard, click Next three times.
5. Select Active Directory Certificate Services. On the pop-up, click Add Features. Click Next.
6. Click Next until you reach the confirmation screen.
7. Click Install. When complete, click Close.
8. In Server Manager, click the flag, and select the Post-deployment Configuration task.
9. In the AD CS Configuration Window, click Next.
10. Check the box for Certification Authority, and click Next.
11. Select Enterprise for the setup type, and click Next.
12. Choose Root CA for the CA type, and click Next.
13. Select Create a New Private Key, and click Next.
14. Accept all remaining defaults, and click Next through the remaining screens.
15. When prompted to begin configuration, click Configure.
16. To exit the wizard, click Close. Restart the server before continuing to the next steps.

Creating certificate templates for out-of-band management

1. Sign into ca.test.local using the domain\administrator account.
2. Open the Certification Authority.
3. Right-click the test-CA-CA, and click Properties.
4. On the General tab, click View Certificate.
5. On the Details tab, scroll to and select Thumbprint. Copy the 40-character code displayed in the details. You will add this information to the AMT BIOS later.
6. Click Ok to close the Certificate Authority properties.

Create the AMT provisioning certificate

1. Expand the Certification Authority, and select Certificate Templates.
2. Right-click Certificate Templates, and select Manage.
3. Locate Web Server in the list of available certificate templates. Right-click the template, and select Duplicate Template.
4. Select Windows 2003.
5. In the General tab, change the template name to AMT Provisioning.
6. On the General tab, choose the option Publish Certificate in Active Directory.
7. On the Subject Name tab, select Build from this Active Directory Information. Select Common Name, and choose the option UPN.
8. On the Request Handling tab, check the box for Allow private key to be exported.
9. On the Security tab, add Kerberos Admins and domain computers. Add the Enroll permission for the security group. Ensure administrators and domain computers have Enroll permissions.
10. On the Extensions tab, select Application Policies, and click Edit.
11. Click Add. Click New. Type `AMT Provisioning` for the name, and `2.16.840.1.113741.1.2.3` as the Object Identifier. Click OK.
12. Ensure AMT Provisioning and Server Authentication are listed, and click OK.
13. Click OK to close the template properties.

Create the AMT Web Server Certificate

1. Right-click the web server template, and select Duplicate Template.
2. Select Windows 2003AMT.
3. On the General tab, change the template name to AMT Web Server Certificate.
4. On the General tab, choose the option Publish Certificate in Active Directory.

5. On the Subject Name tab, select Build from this Active Directory Information. Select Common Name, and choose the option UPN.
6. On the Security tab, ensure Domain Admins and Enterprise Admins have Enroll permissions.
7. Click OK to close the template properties.

Issue the certificate templates to Issue

1. In Certification Authority, expand test-CA-CA.
2. Right-click the Certificate Templates and select New→Certificate Template to Issue. If it is not available, restart the virtual machine.
3. Select the AMT Provisioning Template.
4. Click OK.
5. Repeat steps 2-4 for the AMT Web Server Certificate Template.

Request the certificates on the Configuration Manager server

1. Log into the Configuration Manager server as domain\administrator.
2. Click Start→Run. Type `mmc`, and press Enter.
3. In the mmc console, click File→Add/Remove Snap-in…
4. Select Certificates, and click Add. Select Computer account. Click Next.
5. Select Local computer, and click Finish.
6. Click OK.
7. Expand Certificates→Personal.
8. In the right panel, click More Actions→All Tasks→Request a new certificate…
9. Click Next.
10. Accept the defaults, and click Next.
11. Select the AMT Provisioning and AMT Web Server Certificate. Click Enroll.

Installing required Windows features and roles for System Center Configuration Manager

1. Sign into cm.test.local using the domain\administrator account.
2. Download the Windows Assessment and Deployment Kit for Windows 10 from the following Web site: https://go.microsoft.com/fwlink/p/?linkid=859206
3. Run adksetup.exe.
4. Select Install the Assessment and Deployment Kit to this computer, and choose an installation path. Click Next.
5. Select Deployment tools, Windows Pre-installation Environment features, and User State Migration Tool. Click Install.
6. When the install finishes, click Close.
7. Run the following commands in Windows PowerShell with administrator privileges:

```
Get-Module servermanager
Install-WindowsFeature Web-Windows-Auth
Install-WindowsFeature Web-ISAPI-Ext
Install-WindowsFeature Web-Metabase
Install-WindowsFeature Web-WMI
Install-WindowsFeature Web-DAV-Publishing
Install-WindowsFeature BITS
Install-WindowsFeature RDC
Install-WindowsFeature NET-Framework-Features -source \\yournetwork\yourshare\sxs
Install-WindowsFeature Web-Asp-Net
Install-WindowsFeature Web-Asp-Net45
Install-WindowsFeature NET-HTTP-Activation
Install-WindowsFeature NET-Non-HTTP-Activ
```

8. Run Windows Update, and install updates.
9. Restart the server.

Installing System Center Configuration Manager 1702

1. Sign into cm.domain using the domain\administrator account.
2. Attach the SCCM 1702 Installation media to the management server.
3. Open splash.hta.
4. Click Install.
5. Read the Before You Begin section, click Next.
6. Choose Install a primary site. Choose use typical options.
7. Enter the product key.
8. Check the box to accept the License Terms, and click Next.

9. Accept the license agreements, and click Next.
10. Enter a path for the prerequisite file downloads. We used C:\Downloads
11. Select a language, and click Next for both server and client.
12. Enter a site code for the primary site. We used PTT.
13. Enter a Site Name. We used PT Test.
14. Click Next twice.
15. On the Settings Summary Screen, click Next.
16. Ensure that the console will be installed, and click Next.
17. Install as a primary stand-alone site.
18. Enter the SQL server name, and click Next.
19. Leave the default Database information, and click Next.
20. Accept the default SMS provider, and click Next.
21. Select the option to Configure the communication method on each site system role.
22. Select Clients will use HTTPS when they have a valid PKI certificate and HTTPS-enabled site roles are available, and click Next.
23. Select HTTP for Management Point and Distribution point, and click Next.
24. Select I don't want to join the program at this time, and click Next.
25. Click Next.
26. Run the prerequisites check, and resolve any issues displayed.
27. Click Begin Install, and click Close when the installation is complete.
28. Download and install the installation for System Center R2 SP1 Configuration Manager from the following website: support.microsoft.com/kb/2922875/en-us
29. Download and install the cumulative update.

Configuring SCCM for Intel AMT testing

This is not required for testing DCCS and is completed only for the Intel AMT use cases.

1. In the SCCM console, under Administration→Site Configuration, click Server and Site System Roles.
2. Right-click cm.test.local, and select Add Site System Roles.
3. In the Add Site System Roles Wizard, click Next twice.
4. Select the Fallback status point, and click Next.
5. Click Summary.
6. Click Next.

Installing Intel Setup and Configuration Software (SCS) 11.1

1. Download IntelSCS_11.1.zip from https://downloadcenter.intel.com/download/26505.
2. Extract the contents to C:\IntelSCS_11.2.
3. Browse to C:\IntelSCS_11.2\IntelSCS\RCS.
4. Run IntelSCSInstaller.exe.
5. At the Welcome screen, click Next.
6. Select I accept the terms of the license agreement, and click Next.
7. Check the Boxes for Remote Configuration Service (RCS), Database Mode, and Console.
8. Enter the credentials of the Domain account that will run the service. We used `test.local\administrator`. Click Next.
9. Select cm.test.local as the location for the SCS database. This information may populate automatically. Select Windows Authentication, and click Next.
10. On the Create Intel SCS Database pop-up, click Create Database.
11. On the confirmation screen, click Close.
12. On the confirmation screen, leave the default Installation Folder, and click Install.
13. Once the installation is complete, click Next.
14. Click Finish.

Installing the provisioning certificate

1. Open MMC, and add the certificates snap-in, targeted at the local computer.
2. Navigate to Personal, Certificates.
3. Right-click the AMT Provisioning Certificate, and choose Open.
4. On the Details tab, click Copy to file.
5. On the Welcome screen, click Next.

6. On the Export Private Key screen, choose Yes, export the private key, and choose Next.
7. On the Export File Format screen, check the boxes for Include all certificates in the certification path if possible and Export all extended properties. Click Next.
8. On the Password screen, enter a password to protect the private key.
9. On the File to Export screen, enter C:\Install_Files\scs-prov-cert.pfx, and click Next.
10. On the Completed screen, click Close.
11. From an elevated command prompt, run the following commands:

```
\SCS_download_pacakge_11.2.0.35\utils\RCSutils.exe
/Certificate Add c:\Install_Files\scs-prov-cert.pfx Password1
net stop rcsserver
net start rcsserver
```

12. To verify, run the following command, and make sure the expected certificate is listed:
RCSUtils.exe /certificate view /RCSuser NetworkService /log file C:\rcsout.txt

Creating the AMT configuration profile

1. On the management server, launch the Intel Setup and Configuration Console.
2. Click Profiles.
3. To construct a profile for deployment, click New.
4. For Profile Name, enter a description of the target clients. We used wireless. Click OK.
5. On the Getting Started Screen, choose Configuration / Reconfiguration.
6. On the Optional Settings screen, choose the options Active Directory Integration, Access Control List (ACL), and Transport Layer Security (TLS), Network Configuration, Wired 802.1x and click Next.
7. On the AD Integration screen, browse for the OU created for the AMT managed devices. We used OU=AMT, DC=test, DC=local. Click Next.
8. On the Access Control List screen, click Add.
9. Select Active Directory User/Group. Click Browse.
10. Add Kerberos Admin, Domain Admins, or other administrative users groups. Click OK.
11. For Access Type, select Remote.
12. Choose the option for PT Administration. Click OK.
13. Click Next.
14. On the TLS screen, from the drop-down menu, select the Enterprise Certificate Authority, ca.test.local.
15. Select the Server Certificate Template to be used to generate certificates for the AMT devices. We selected AMTWebServerCertificate. Click Next.
16. On the Network Configuration Screen, select Allow Wired connection with the following WiFi setups.
17. Click Add…
18. On the 802.1x Setup screen, click Edit list.
19. Click Add, then use the test-CA certificate authority. Click OK.
20. Click OK.
21. On the System Settings screen, choose the options Web UI, Serial Over LAN, IDE Redirection, and KVM Redirection.
22. Select Use the following password for all systems. Enter the password for use after provisioning is complete. We used P@ssw0rd
23. Enter the RFB Password for KVM sessions. We used `P@ssw0rd`
24. Enter the MEBX password. We used P@ssw0rd
25. Click KVM Settings…, uncheck User Consent required before beginning KVM session, and click OK.
26. Check the boxes for the following options:
    a. Synchronize Intel AMT clock with operating system
    b. Enable Intel AMT to respond to ping requests
    c. Enable Fast Call for Help (within the enterprise network)
27. To Edit IP and FQDN settings, click Set.
28. In the Network Settings window, select Use the following as the FQDN, and choose Primary DNS FQDN from the drop-down menu.
29. Choose the option that indicates the device and the OS will have the same FQDN (Shared FQDN).
30. Select Get the IP from the DHCP server.
31. Select Update the DNS directly or via DHCP option 81. Click OK.
32. Click Next.
33. Click Finish.

Adding the configurator to a shared folder

1. Create a shared folder called `amtshare`
2. Copy the file at C:\IntelSCS_11.3\IntelSCS\Configurator to the shared C:\amtshare folder.

Installing certificates on target systems

Configuration for our laptop varied from this since we used a self-signed certificate. In order to configure the system, we first manually input our configuration information into the pre-boot MEBx menu. This work around will not be necessary for users who purchase their certificates.

1. On each target system, during boot, press Ctrl + P to enter the Intel Management Engine BIOS Extension.
2. Enter the Intel ME Password. The default is `admin`. We changed ours to `P@ssw0rd`
3. Navigate to Intel ME General SettingsRemote Setup and Configuration, TLS PKI, and select Manage Hashes.
4. Press the insert key to add a certificate hash.
5. Enter a name for the hash.
6. Enter the 40-character thumbprint recorded before.
7. Exit the MEBx menu.

Testing methodology

Before each test, ensure all target desktops are powered on and are signed out of the user account. Ensure that all systems are domain joined and that they have the configuration manager client installed prior to running the provisioning command. Ensure all systems are connected to a monitor.

Dell with DCCS

At the beginning of all tests, the administrator is logged into the management server at the desktop. Tests in this section require additional time for the commands to complete during which the administrator is not actively inputting commands. We refer to this as system time. We have recorded both admin time and system time in Appendix C.

Configuring AMT

Prior to this test, ensure all target clients have been added to the target collection.

1. On the Configuration Manager server, open the configuration manager console.
2. Open the Assets and Compliance panel.
3. Open Device Collections.
4. Right-click the collection that you wish to deploy to, and select Deploy→Task Sequence.
5. In the Deploy Software Wizard, next to Task Sequence, click Browse.
6. Select the vPro-AMT Configure Client task sequence, and click OK.
7. In the Deploy Software Wizard, click Next.
8. Next to Purpose, select Required, and click Next.
9. Select a time when the deployment will become available, and click Next.
10. On the user experience screen, click Next.
11. On the Alerts screen, click Next.
12. On the Distribution Points screen, click Next.
13. On the Summary screen, click Next.

For timing purposes, we used RDP to connect to the target system and ran a Machine Policy Retrieval & Evaluation Cycle using the Configuration Manager Properties menu in Control Panel to trigger the install.

For the two-system test, we completed steps 1 through 13 once, but added the additional client to the collection prior to running the test.

Changing one BIOS setting

1. Open the Dell Intel vPro Out of Band plugin.
2. Under Client Configuration, select BIOS Settings.
3. On Active Processor Cores, select All, and check the Apply checkbox. Click Next.
4. Add the target system, and click Next.
5. Add a description, and click Next. We typed test.
6. Click Finish.

For the two-system test, we completed steps 1 through 6 once, but selected all systems in step 4.

Changing 10 BIOS settings

1. Open the Dell Intel vPro Out of Band plugin.
2. Under Client Configuration, select BIOS Settings.
3. For Auto On, check the box, and select Every day.
4. For Active Processor Cores, check the box, and select All.
5. For Enable Audio, check the box, and select Enabled
6. For SATA-0, check the box, and select Enabled.
7. For Trusted Execution, check the box, and select Enabled.
8. For Intel TurboBoost, check the box, and select Enabled.
9. For Front USB Ports, check the box, and select Enabled.
10. For USB Rear Port 1, check the box, and select Enabled.
11. For VT for Direct IO, check the box, and select Enabled.
12. For Wake on LAN, check the box, and select LAN or WLAN. Click Next.
13. Select the clients to add.
14. Click Next.
15. Add a description.
16. Click Finish

For the two-system test, we completed steps 1 through 16 once, but selected all systems in step 13.

Changing the Boot Order

1. Open the Dell Intel vPro Out of Band plugin.
2. Under Client Configuration, select Boot Order.
3. Select only Internal HDD (IRRT) boot and click Next.
4. Add the target system and click Next.
5. Add a description and click Next. We typed `test`.
6. Click Finish.

For the two-system test, we completed steps 1 through 6 once, but selected all systems in step 4.

Setting a system password on the target system

1. Open the Dell Intel vPro Out of Band plugin.
2. Under Client Configuration, select Passwords.
3. Select Set, and select Administrator.
4. Enter and confirm a BIOS Password, and click Next. We used `Password1`.
5. Add the target system, and click Next.
6. Add a description, and click Next. We typed `test`.
7. Click Finish.

For the two-system test, we completed steps 1 through 7 once, but selected all systems in step 5.

Wiping the Client Data on the target system

1. Open the Dell Intel vPro Out of Band plugin.
2. Under Operations, select Wipe Client Disk.
3. Add the target system and click Next.
4. Add a description and click Next. We typed `test`.
5. Click Finish.

We do not include time or steps for this task, but did complete it to verify functionality.

Enabling Intel vPro without the Dell Command Integration Suite

We completed this test for the Dell desktops and recorded it as a manual task.

1. Log into the target system over RDP using test\administrator.
2. Navigate to the shared folder on the configuration server, and copy the Configurator folder onto the desktop.
3. Open the target folder.
4. Click File, navigate to Open command prompt, then click Open command prompt as Administrator.
5. Run the following command in the elevated command prompt:

```
ACUConfig.exe /Verbose /Output console ConfigViaRCSOnly cm.test.local test
```

After starting the previous command, stop the admin time timer, and start the system time timer. Stop the system time timer and once the command stops running and exits with code 0, indicating a successfully provisioned system.

For the two-system test, repeat steps 1-5 for the second system. Immediately start repeating the above steps on the second system and do not start the system time timer till you complete the steps for the second system.

Conducting the Intel vPro and manual tests

We used the steps in the sections below for both Intel vPro and Manual tests. Intel vPro tests use the KVM feature to complete the task. Manual tasks are completed at the target desktop's console.

For all Intel vPro tests, we use Intel Manageability KVM to complete the task.

1. Open the Intel Manageability Connector.
2. Connect to the target system.
3. Click Remote Desktop.

We added these steps to the total steps for all Intel vPro tasks. Additionally, all two-system tests repeat steps 2 through 3 for the second system.

Changing one BIOS setting

For tests involving Intel vPro, use Intel Manageability Commander to connect to the target system. For tests that did not involve Intel vPro, complete the actions when connected via the Intel Manageability Commander.

Dell OptiPlex 7050 Micro Desktop

1. Reboot the target client to System Setup.
2. Under Performance, select Multi Core Support.
3. For Multi Core Support, select All.
4. Click Exit and click Yes when prompted to save changes.
5. For the two-system test, repeat steps 1 through 4 on the second system.

Lenovo ThinkCentre M910q

1. Reboot the target client to System Setup.
2. In the Lenovo BIOS Setup Utility, under Advanced, select CPU setup.
3. For Core Multi-processing, select Enabled.
4. Press F10 to Save and Exit.
5. For the two system test, repeat steps 1-4 on the second system.

Changing 10 BIOS settings

For tests involving Intel vPro, use Intel Manageability Commander to connect to the target system. For tests that did not involve Intel vPro, complete the actions when connected via the Intel Manageability Commander.

Dell OptiPlex 7050 Micro Desktop

1. Reboot the target client to System Setup.
2. Under System Configuration, select Drives.
3. For SATA-0, check the box for SATA-0.
4. Under System Configuration, select USB Configuration.
5. Check the box for Enable Front USB Ports.
6. Under System Configuration, select Front USB Configuration.

7. Check the box for Front Port 1 w/ Power Share(Bottom)*.
8. Under Onboard Audio Controller, click Audio.
9. Check the box for the Enable Audio option.
10. Under Performance, select Multi Core Support.
11. For Multi Core Support, select All.
12. Select Intel TurboBoost.
13. Check the Box for Enable Intel Turboboost.
14. Under Virtualization Support, select Virtualization.
15. Check the box for Enable Intel Virtualization Technology.
16. For Direct I/O, Select VT.
17. For Direct I/O, Check the box for Enable VT.
18. Select Trusted Execution.
19. Check the box for Trusted Execution.
20. Under Power Management, select Wake on LAN/WLAN.
21. For Wake on LAN/WLAN, select LAN or WLAN.
22. Click Exit and click Yes when prompted to save changes.
23. For the two-system test, repeat steps 1-22 on the second system.

Lenovo ThinkCentre M910q

1. Reboot the target client to System Setup.
2. In the Lenovo BIOS Setup Utility, under Devices, select Audio Setup.
3. For Onboard Audio Controller, select Enabled.
4. Under Power, select Automatic Power on.
5. For Wake on LAN select Primary. Press ESC.
6. Under Advanced, select CPU setup.
7. For Core Multi-processing, select Enabled.
8. For Intel Virtualization Technology, select Enabled.
9. For VT-d, select Enabled.
10. For TxT, select Enabled.
11. For Turbo Mode, select Enabled. Press ESC.
12. Under Devices, select USB setup.
13. For Front USB ports, select Enabled.
14. For USB Port 1, select Enabled. Press ESC.
15. Select ATA Drive Setup.
16. For SATA Drive 1, select Enabled.
17. Press F10 to Save and Exit.
18. For the 2-system test, repeat steps 1-17 on the second system.

Changing the Boot order

For tests involving Intel vPro, use Intel Manageability Commander to connect to the target system. For tests that don't involve Intel vPro, complete the actions when connected via the Intel Manageability Commander.

Dell OptiPlex 7050 Micro Desktop

1. Reboot the target client to System Setup.
2. Under General, select Boot sequence.
3. Select the Onboard NIC and uncheck the box.
4. Click Exit and agree to save changes.
5. For the two-system test, repeat steps 1 through 4 on the second system.

Lenovo ThinkCentre M910q

1. Reboot the target client to System Setup.
2. Under Startup, select Primary Boot Sequence.
3. Select UEFI, IPv4 Intel Ethernet Connection and press X.
4. Press F10 to save and Exit.

Changing the system password

For Intel vPro tests, use Intel Manageability Commander to connect to the target system. For tests that don't involve Intel vPro, complete the following actions at the console.

Dell OptiPlex 7050 Micro Desktop

1. Reboot the target client to System Setup.
2. In the Dell OptiPlex 7050 setup menu, under security, select Admin Password.
3. Enter and confirm and the new Password. We used `Password1`.
4. Click Exit and click save when prompted.
5. For the two-system test, repeat steps 1 through 4 on the second system.

Lenovo ThinkCentre M910q

1. Reboot the target client to System Setup.
2. In the Lenovo BIOS Setup Utility, under security, select Set Administrator Password.
3. For Set Administrator Password, Enter and Confirm the New Password and press enter. We used Password1.
4. Press F10 to Save and Exit.
5. For the 2-system test, repeat steps 1-4 on the second system.

Appendix C: Our results

The tables below show the admin time required to manage one, two, and 100 systems. To estimate the time to perform tasks on 100 systems, we used the formula **W** + [**98** × **Δt**], where **W** is the time to perform a task on two systems, and **Δt** is the time difference between the one- and two-system tests.

Admin time to complete management tasks (mm:ss)	**Single-system tests**			**Two-system tests**		
Task	Dell	Lenovo with AMT	Lenovo Manual	Dell	Lenovo with AMT	Lenovo Manual
Provisioning AMT	0:48	N/A	0:51	0:48	N/A	1:42
Changing a BIOS setting	0:25	0:50	0:42	0:25	1:24	1:24
Changing 10 BIOS settings	1:35	1:53	2:01	1:35	3:19	4:02
Changing the boot order	0:21	0:47	0:45	0:21	1:27	1:30
Changing the system password	0:28	0:50	0:42	0:28	1:30	1:21

Admin time to complete management tasks - 100-system extrapolation (h:mm:ss)							
Task	Dell	Lenovo with AMT	Time saved	Percent savings	Lenovo Manual	Time saved	Percent savings
Provisioning AMT	0:00:48	N/A	N/A	N/A	1:25:00	1:23:38	99.1%
Changing a BIOS setting	0:00:25	0:56:56	0:56:31	99.3%	1:10:00	1:09:35	99.4%
Changing 10 BIOS settings	0:01:35	2:23:47	2:22:12	98.9%	3:21:40	3:20:05	99.2%
Changing the boot order	0:00:21	1:06:47	1:06:26	99.5%	1:15:00	1:14:39	99.5%
Changing the system password	0:00:28	1:06:50	1:06:22	99.3%	1:05:03	1:04:35	99.3%

The tables below show the admin steps required to manage one, two, and 100 systems.

Admin steps to complete management task	**Single-system tests**			**Two-system test**		
Task	Dell	Lenovo with AMT	Lenovo Manual	Dell	Lenovo with AMT	Lenovo Manual
Provisioning AMT	13	N/A	5	13	N/A	10
Changing a BIOS setting	6	7	4	6	13	8
Changing 10 BIOS settings	16	20	17	16	39	34
Changing the boot order	6	7	4	6	13	8
Changing the system password	7	7	4	7	13	8

Admin steps - 100-system extrapolation							
Task	DCCS	AMT only	Steps saved	Percent savings	Manual	Steps saved	Percent savings
Provisioning AMT	13	N/A	N/A	N/A	500	487	97.4%
Changing a BIOS setting	6	601	595	99.0%	400	394	98.5%
Changing 10 BIOS settings	16	1901	1,885	99.1%	1,700	1,684	99.0%
Changing the boot order	6	601	595	99.0%	400	394	98.5%
Changing the system password	7	601	594	98.8%	400	393	98.2%

This project was commissioned by Dell Technologies.

Facts matter.®