SupportAssist for Business PCs

Administrator Guide

March 2026
Rev. A40

DELL Technologies

Notes, cautions, and warnings

NOTE: A NOTE indicates important information that helps you make better use of your product.

CAUTION: A CAUTION indicates either potential damage to hardware or loss of data and tells you how to avoid the problem.

WARNING: A WARNING indicates a potential for property damage, personal injury, or death.

Contents

Chapter 1: Introduction **6**
Version 6
New and enhanced features 6
Audience 6
Document purpose 6
Connect and manage capabilities and Dell service plans 7
Connect and manage roles in TechDirect 9
Supported systems 11
Dispatchable parts 11

Chapter 2: Overview **13**
Customize the Overview page 14

Chapter 3: Search **15**
Search by rules or criteria 15
Search by identifiers 16

Chapter 4: Managing your PC fleet and groups **17**
PC fleet inventory 17
Create a service request 20
Create dispatch request 20
Remove disconnected PCs 21
Groups overview 21
Create a group 22
Move assets between existing groups 22
Update site name 23
Update group name 23
Delete group 23
Create a custom or dynamic group 24

Chapter 5: Managing a single PC **25**
PC overview 25
Recommendations for a specific PC 27
Restoring PC files and settings 27
Health of a specific PC 28
Application experience for a specific PC 29
Security for a specific PC 29
Component verification for a specific PC 30

Chapter 6: Recommendations for your PC fleet **32**
Review and schedule PC updates 33
Scan hardware 34
Boost performance 34
Optimize network 35

Remove viruses & malware... 35

Chapter 7: Custom catalogs for your PC fleet... 36
Managing catalogs for PCs connected to Dell... 36
Create a new catalog... 37
Managing catalogs... 38
Catalog states... 38
Modifying update catalogs... 39
Download updates to the network location... 41
Deploy a catalog remotely... 41
Catalog deployments... 42
Managing catalogs for PCs not connected to Dell... 43
Create a new catalog... 43
Deploying a catalog manually... 44

Chapter 8: Managing SupportAssist alerts... 46
Alerts overview... 46
Details of a specific alert... 47
Alert actions... 48

Chapter 9: Remediation rules for your PC fleet... 49
Create a remediation rule using predefined Dell library scripts... 50
Creating remediation rules using Custom Workflow scripts... 55
Details of a specific rule... 56
Update a remediation rule... 58
Delete a remediation rule... 58
Manage PowerShell scripts... 58

Chapter 10: Application experience for your PC fleet... 60

Chapter 11: Security for your PC fleet... 62
Security health... 62
Component verification... 63

Chapter 12: Configuring settings... 65
Set inventory identifiers... 65
Enable or disable remote support... 65
Set alert rules... 66
Set PC update source... 67
Roles and permissions... 68
User details and permissions... 68
Features, roles, and user permissions... 68
Connecting SupportAssist alerts with external solutions... 69
Connect to an external solution... 69
Edit an external solution connection... 70
Delete an external solution connection... 70

Chapter 13: Data exports... 71

Chapter 14: Performance indicators....72

Chapter 15: Audit trail....74

Chapter 16: Email notifications from SupportAssist....76

Chapter 17: Retrieve SupportAssist data using WMI....77

Chapter 18: Retrieve SupportAssist data using APIs....80

Appendix A: Remote actions....81

Appendix B: Features and enhancements in previous versions....82

Appendix C: Resources....85

Appendix D: Contact Dell....87

1

Introduction

SupportAssist is a proactive and predictive technology that offers automated technical support for Dell PCs. It proactively monitors both hardware and software, addressing performance issues, preventing security threats, and automating engagement with Dell Technical Support.

Depending on your service plan, SupportAssist can also create support requests for detected issues. Additionally, it optimizes PC performance by removing unwanted files, optimizing network settings, boosting system performance, removing viruses and malware, and identifying available updates.

SupportAssist collects and sends the required PC information securely to Dell Technical Support. The collected information enables Dell to provide you an enhanced, efficient, and accelerated support experience.

SupportAssist also collects telemetry, application experience, health, and security data proactively from your PCs and provides various performance insights about your PCs, based on your service plan.

After you have deployed SupportAssist on your PCs, you can manage the PC fleet using Connect and manage in TechDirect.

Topics:

- Version
- New and enhanced features
- Audience
- Document purpose
- Connect and manage capabilities and Dell service plans
- Connect and manage roles in TechDirect
- Supported systems
- Dispatchable parts

Version

v5.0.1.2516

New and enhanced features

- Simplified Deployment Process for PCs preinstalled with SupportAssist 5.0.
- Enhanced “Deployment Package Manager” to create SupportAssist Deployment Package.
- Improved retry mechanism for PC update installations.
- Support for Windows 11 25H2.
- Performance improvements, Security and Bug fixes.

Audience

The information in this administrator guide is intended for administrators, technicians, and partners who manage SupportAssist on PCs running the Windows operating system.

Document purpose

This document provides information about:

- Managing your PC fleet and groups.
- Viewing and managing recommendations, health, security, and application experience for a single PC.

- Viewing and managing recommendations, health, and application experience for your PC fleet.
- Updating catalogs for your PC fleet.
- Managing remediation rules to identify and remediate issues with your PC fleet.
- Assessing the number of PCs at risk and acting on the potential security threats.
- Managing SupportAssist alerts in TechDirect or ServiceNow.
- Managing roles and permissions.
- Viewing key performance indicators that help determine the fleet behavior.
- Viewing the record of changes and activities performed for the Connect and manage service in TechDirect.
- Remotely updating BIOS/Drivers/Firmware/Application updates for your PC fleet.

For more information about SupportAssist, see the documentation resources and other useful links in Resources.

Connect and manage capabilities and Dell service plans

The following table summarizes the Connect and manage capabilities available in TechDirect for different service plans:

Table 1. SupportAssist capabilities available in TechDirect for Dell service plans

Capability	Description	Contract Expired	Basic	ProSupport and Premium Support	ProSupport Plus, Premium Support Plus, and ProSupport Flex for Client *
Manage PCs and groups	View the PC fleet inventory.	Full support	Full support	Full support	Full support
	Create groups and organize PCs.	Full support	Full support	Full support	Full support
PC health and fleet performance	View fleet performance and utilization.	No support	No support	Full support	Full support
	View health data for a single PC and for your PC fleet.	No support	Limited support	Full support	Full support
Dell Recommendations	View recommendations for a single PC and for your PC fleet.	Full support	Full support	Full support	Full support
	Remotely optimize the PCs based on the recommendations —scan hardware, boost performance, optimize network, and remove viruses & malware.	No support	No support	No support	Full support
	Remotely perform PC updates— BIOS, driver, firmware, and Dell application software updates.	Full support	Full support	Full support	Full support
	Restore the files and settings to its previous state in a single PC.	No support	No support	No support	Full support

Table 1. SupportAssist capabilities available in TechDirect for Dell service plans (continued)

Capability	Description	Contract Expired	Basic	ProSupport and Premium Support	ProSupport Plus, Premium Support Plus, and ProSupport Flex for Client *
Custom catalogs for PCs connected to Dell	Manage product series or fleet catalogs.	No support	No support	No support	Full support
	Manage model catalogs.	No support	Full support	Full support	Full support
	Remotely deploy custom catalogs.	No support	No support	No support	Full support
Custom catalogs for PCs without SupportAssist and not connected to Dell	Manage model catalogs.	No support	Full support	Full support	Full support
	Manually deploy custom catalogs.	No support	Full support	Full support	Full support
Remediation rules	Manage remediation rules to identify and remediate issues with your PC fleet.	No support	No support	No support	Full support
Application experience	View application experience data for a single PC and for your PC fleet.	No support	Limited support	Full support	Full support
Security	Track and manage the security of a single PC and your PC fleet.	No support	Limited support	Full support	Full support
Alerts	Manage proactive alerts. Proactive issue detection and resolution help in automated hardware failure detection, case creation, and support.	No support	No support	Full support	Full support
	Manage predictive alerts. Predictive issue detection and resolution help reduce disruptions before the occurrence of hardware failures.	No support	No support	Full support	Full support
Schedule scans and optimizations	Perform scheduled scans to detect PC updates and the required system optimizations.	Full support	Full support	Full support	Full support
	Perform scheduled scans to detect hardware issues.	No support	Full support	Full support	Full support

Table 1. SupportAssist capabilities available in TechDirect for Dell service plans (continued)

Capability	Description	Contract Expired	Basic	ProSupport and Premium Support	ProSupport Plus, Premium Support Plus, and ProSupport Flex for Client *
Automatic PC optimization	Perform automatic PC optimizations such as boosting performance, optimizing the network, and removing viruses and malware.	No support	No support	No support	Full support

* ProSupport Plus, Premium Support, and ProSupport Flex for Client service plans are available only in certain regions.

[1] SupportAssist automatically detects and proactively alerts on failures of hard drives, batteries, memory, internal cables, thermal solutions and fans, heat sinks, solid state drives and video cards.

[2] SupportAssist predictive analysis failure detection includes hard drives, solid state drives, and batteries.

NOTE: If autoforward is turned off in TechDirect for technical support or parts dispatch, you can review the alerts in the **Alerts** page and determine if the alert should be forwarded to Dell or to a configured external solution. See Set alert rules.

Connect and manage roles in TechDirect

TechDirect enables organizations to designate administrators and add technicians under that administrator account.

To add a company administrator, go to **Utilities** > **Administrator Control Panel**, **Company administrators**, and click **ADD COMPANY ADMINISTRATOR**. Select the user from the list, click **NEXT**, review the selections, and click **SUBMIT**. A message is displayed after the company administrator is successfully added.

To add a technician, go to **Utilities** > **Administrator Control Panel** > **Technicians**, and click **ADD TECHNICIAN**. Enter the technician information, review the entries, and click **SUBMIT**. A message is displayed after the technician is successfully added.

The following table summarizes the SupportAssist capabilities available for different Connect and manage roles in TechDirect:

Table 2. SupportAssist capabilities and roles in TechDirect

Capability	Description	TechDirect navigation	Connect and manage administrator	Connect and manage technician
Overview	View a summary of various details about your PC fleet.	**Connect and manage** > **Manage PC fleet** > **Connect and manage PCs** > **Overview**	Supported	Supported
Set up and connect	Configure and download SupportAssist to centrally manage and monitor your Dell PCs.	**Connect and manage** > **Manage PC fleet** > **Connect and manage PCs** > **Set up and connect**	Supported	Requires permissions from the Connect and manage administrator.
PCs and groups	View the PC fleet inventory, fleet performance, and utilization.	**Connect and manage** > **Manage PC fleet** > **Connect and manage PCs** > **Manage** > **Groups**	Supported	Supported
			Supported	Requires permissions from the Connect and manage administrator.
Recommendations	**Multiple PCs**—view recommendations for your PC fleet and remotely optimize them.	**Connect and manage** > **Manage PC fleet** > **Connect and manage PCs**	Supported	Requires permissions from the Connect and manage administrator.

Table 2. SupportAssist capabilities and roles in TechDirect (continued)

Capability	Description	TechDirect navigation	Connect and manage administrator	Connect and manage technician
		> **Manage** > **Recommendations**		
	Single PC—view recommendations for a single PC and remotely optimize the PC.	**Connect and manage** > **Manage PC fleet** > **Connect and manage PCs** > **Manage** > **Recommendations**	Supported	Requires permissions from the Connect and manage administrator.
	System restore—remotely initiate a system restore to rollback driver updates on a single PC.	**Connect and manage** > **Manage PC fleet** > **Connect and manage PCs** > **Manage** > **Recommendations**	Supported	Requires permissions from the Connect and manage administrator.
Update catalogs	Create, edit, and deploy custom catalogs to update your fleet of PCs	**Connect and manage** > **Manage PC fleet** > **Connect and manage PCs** > **Manage** > **Update catalogs**	Supported	Requires permissions from the Connect and manage administrator.
Alerts	Manage SupportAssist alerts.	**Connect and manage** > **Manage PC fleet** > **Connect and manage PCs** > **Manage** > **Alerts**	Supported	Requires permissions from the Connect and manage administrator.
Remediation rules	Manage remediation rules to identify and remediate issues with your PC fleet.	**Connect and manage** > **Manage PC fleet** > **Connect and manage PCs** > **Manage** > **Remediation rules**	Supported	Requires permissions from the Connect and manage administrator.
Application experience	View application experience data for a single PC and for your PC fleet.	**Connect and manage** > **Manage PC fleet** > **Connect and manage PCs** > **Manage** > **Applications**	Supported	Requires permissions from the Connect and manage administrator.
Health	View health data for a single PC and for your PC fleet.	**Connect and manage** > **Manage PC fleet** > **Connect and manage PCs** > **Manage** > **Inventory**	Supported	Requires permissions from the Connect and manage administrator.
Security	**Security health**—track and manage the security of a single PC and your PC fleet.	**Connect and manage** > **Manage PC fleet** > **Connect and manage PCs** > **Manage** > **Security**	Supported	Requires permissions from the Connect and manage administrator.
	Component verification—view information about the components inside your PC against the factory configuration.	**Connect and manage** > **Manage PC fleet** > **Connect and manage PCs** > **Manage** > **Security**	Supported	Requires permissions from the Connect and manage administrator.

Table 2. SupportAssist capabilities and roles in TechDirect (continued)

Capability	Description	TechDirect navigation	Connect and manage administrator	Connect and manage technician
Settings	• Set an inventory identifier to identify PCs associated with your PC fleet. • Enable remote support. • Set alert rules. • Set PC update source. • Integrate alerts with ServiceNow. • View and modify Connect and manage technician roles and permissions.	**Connect and manage** > **Manage PC fleet** > **Connect and manage PCs** > **Manage** > **Settings**	Supported	Not supported
Summary	**Performance indicators (KPIs)**—view an overview of KPIs to help determine the PC fleet behavior.	**Connect and manage** > **Manage PC fleet** > **Connect and manage PCs** > **Summary** > **Performance indicators (KPIs)**	Supported	Requires permissions from the Connect and manage administrator.
	Audit trail—view a record of activities performed by the Connect and manage administrator and Connect and manage technician.	**Connect and manage** > **Manage PC fleet** > **Connect and manage PCs** > **Summary** > **Audit trail**	Supported	Requires permissions from the Connect and manage administrator.

Supported systems

SupportAssist is supported on the following Dell devices:

- **Laptops and desktops**
  - Latitude
  - Precision
  - OptiPlex
  - Inspiron
  - XPS
  - Alienware
  - Vostro
  - Dell
  - Dell Pro
  - Dell Pro Max
  - Video conferencing room solution- Logitech and OptiPlex devices
- **Docking Stations**—For the list of supported docking stations, see Dell Commercial Docking Compatibility.

NOTE: SupportAssist is not supported on virtual machines.

Dispatchable parts

When SupportAssist detects an issue on your PC, a replacement part may be automatically dispatched to you depending on your PC service plan.

The following parts may be dispatched automatically:

- Hard drive

- Memory module
- Keyboard
- Mouse
- Battery
- Video card

2

Overview

The **Overview** page provides a summary of various details about your PC fleet.

To view the **Overview** page, from the TechDirect dashboard, go to **Connect and manage** > **Manage PC fleet** > **Connect and manage PCs** > **Overview**.

- **Health**—displays the overall health score, the number of unhealthy PCs, the number of PCs that need attention, the number of healthy PCs, and the status for each category. Click the specific status to view information about the PCs on the **Inventory** page.
- **Application experience**—displays the application experience score, the number of applications with issues, the number of most used applications, and the status for each category. Click the specific status to view information about the applications on the **Applications** page.
- **Security**—displays the security score, the number of PCs at risk, the number of PCs that need attention, the number of PCs that are secure, and the status for each category. Click the specific status to view information about the PCs on the **Security** page.
- **Trend**
  - **Health**—displays a trend chart of PCs that are healthy, needs attention, and unhealthy for the last 26 weeks (Weekly view) or 30 days (Daily view).
    - You can switch between **View by PCs** and **View by score** to view the data.
    - Click a specific date or week to view more information about the PCs for the selected time period.
    - In the **View by PCs** view, click a specific color-coded section in the trend chart to view detailed information about the PCs on the **Inventory** page.
  - **Application experience**—displays a trend chart for applications with issues and most used applications for the last 26 weeks (Weekly view) or 30 days (Daily view).
    - You can switch between **View by applications** and **View by score** to view the data.
    - Click a specific date or week to view more information about the applications for the selected time period.
    - In the **View by applications** view, click a specific color-coded section in the trend chart to view detailed information about the applications on the **Applications** page.
  - **Security**—displays a trend chart for the security assessment performed on the PC, for the last 26 weeks (Weekly view) or 30 days (Daily view).
    - You can switch between **View by PCs** and **View by score** to view the data.
    - Click a specific date or week to view more information about the PCs for the selected time period.
    - In the **View by PCs** view, click a specific color-coded section in the trend chart to view detailed information about the PCs on the **Security** page.
- **Service plans**—displays the number of PCs and the associated service plan of the PC. Click a specific color-coded section to view detailed information about the PCs on the **Inventory** page. By default, the **Service plans** widget is not displayed. You can view this widget by customizing the **Overview** page. See Customize the Overview page.
- **Versions**—displays the number of PCs and the associated SupportAssist version that is installed on the PCs. Click a specific color-coded section to view detailed information about the PCs in the category, on the **Inventory** page. By default, the **Versions** widget is not displayed. You can view this widget by customizing the **Overview** page. See Customize the Overview page.
- **Alerts**—displays the number of dispatches and cases. Click a specific color-coded section to view detailed information about the alerts on the **Alerts** page.
- **PC recommendations**—displays a list of recommendations that help improve the PCs efficiency. Click the corresponding link to view and act on each recommendation.
- **PC utilizations**—displays insights about the overall performance of the PC fleet. Click the corresponding link to view more information about the fleet performance and utilization on the **Inventory** page.
- **Central Resource Manager**—displays the list of registered Central Resource Manager instances, their versions, and statuses. The data is displayed only if your systems are running Central Resource Manager version 4.5.
- **PCs connected to Dell**—displays the number of PCs that are connected to Dell and the number of PCs that have not connected to Dell from 30 days.
- **Pinned PCs**—displays the PCs that you pinned on the **Inventory** page.

Topics:

- Customize the Overview page

Customize the Overview page

About this task

You can show or hide the widgets, and move the placement of the widgets on the **Overview** page. You can only customize the following widgets:

- **Alerts**
- **PC utilizations**
- **PC recommendations**
- **Service plans**
- **Versions**
- **PCs connected to Dell**
- **Operating system versions**

NOTE: The **Health**, **Application experience**, and **Security** widgets, and the **Trend** charts are not customizable.

Steps

1. From the TechDirect dashboard, go to **Connect and manage** > **Manage PC fleet** > **Connect and manage PCs** > **Overview**.
2. Click **Customize**.
3. Customize the widgets as per your preference and click **Done**.

3

Search

The **Search** page enables you to search for specific information about your PCs.

To perform a search, from the TechDirect dashboard, go to **Connect and manage** > **Manage PC fleet** > **Connect and manage PCs** > **Search**.

You can perform the search either by using the rules or criteria or by using the PC identifiers.

Saved searches

After you have performed a search, you can save the search criteria for later use. The search criteria that you saved are displayed in the **Saved searches** section. This section displays the following information:

- **Name**—the name that you provided while saving the search criteria.
- **Description**—the description defined for the search criteria.
- **Searched by**—the search method that was used to perform the search—**Rules** or **Identifiers**.
- **Last updated**—date on which the search was last updated.

You can also perform certain actions on the saved searches. Click ⋮ and perform the following actions based on your preference:

- **Run search**—to run the search criteria and view the results.
- **Edit**—to view and modify the search criteria.
- **Duplicate**—to copy and modify the search criteria.
- **Delete**—to delete the saved search criteria.

Topics:

- Search by rules or criteria
- Search by identifiers

Search by rules or criteria

About this task

You can perform an advanced search using a combination of parameter, operator, and value.

Steps

1. From the TechDirect dashboard, go to **Connect and manage** > **Manage PC fleet** > **Connect and manage PCs** > **Search**. The **Search** page is displayed.
2. Click **Using rules or criteria**. The **Search by Rules** page is displayed.
3. From the **Select** lists, select the search criteria and the operator.
4. Apply and **AND** or **OR** condition to refine your search results.
5. Add additional conditions to the search based on your preference.
6. In the **Exclusion criteria** section, enter the Service Tag, asset tag, or hostname of the PCs that you want to exclude in the search.
7. Click one of the following:
   - **Search** to view and export the results.
   - **Save search criteria** to save the search criteria. You can view and use the saved criteria from the **Saved searches** section.

Search by identifiers

About this task

You can perform a search using PC identifiers for specific information about your PCs. For information about how to set the PC identifiers, see Set inventory identifiers.

Steps

1. From the TechDirect dashboard, go to **Connect and manage** > **Manage PC fleet** > **Connect and manage PCs** > **Search**.
   The **Search** page is displayed.
2. Click **Using PC identifiers**.
   The **Search by Identifiers** page is displayed.
3. Enter the Service Tag, asset tag, or hostname of the PCs that you want to include in the search.
4. Click one of the following:
   - **Search** to view and export the results.
   - **Save search criteria** to save the search criteria. You can view and use the saved criteria from the **Saved searches** section.

4

Managing your PC fleet and groups

After you deploy SupportAssist, the PCs are automatically displayed on the **Inventory** page in TechDirect within 30 minutes after they connect to the Internet. You can update the contact and shipping details, and SupportAssist preferences in the SupportAssist configuration anytime. The updated configuration is automatically applied to the PCs immediately after they connect to Dell. For information about configuring and deploying SupportAssist, see the *SupportAssist for Business PCs Deployment Guide* available on the SupportAssist for Business PCs documentation page.

The **Inventory** page enables you to:

- View all the PCs in your fleet, and its health, performance, and utilization details.
- View recommendations, insights about PC health, and application experience for each PC.
- Create groups and organize PCs. See Groups overview.

To manage your PCs, from the TechDirect dashboard, go to **Connect and manage** > **Manage PC fleet** > **Connect and manage PCs** > **Manage**.

Topics:

- PC fleet inventory
- Groups overview
- Create a custom or dynamic group

PC fleet inventory

The **Inventory** page displays information about your PCs.

The **All PCs** list displays information about all the PCs in your fleet. The **Connected PCs** list displays information about the PCs that are connected to Dell. The **Disconnected PCs** list displays information about PCs that have not connected to Dell in last 30 days. For information about removing the disconnected PCs, see Remove disconnected PCs.

The following table describes information about PCs that is displayed on the **Inventory** page:

NOTE: The performance and utilization data are not available for PCs with Expired service plan. You can view limited data on PCs with the Basic service plan. You can view all the data on PCs with ProSupport, ProSupport Plus, or ProSupport Flex for Client service plan.

Table 3. Inventory

Column	Description
Site	Name of the site to which the asset is assigned.
Group	Group to which the asset is assigned.
Service tag	A unique five-to-seven digit-alphanumeric code which is found on a white bar-coded label affixed on your Dell PC or peripheral. **NOTE:** To view the asset details, PC health details, and to optimize the PC, click the Service Tag. See Managing a single PC.
Asset tag	Asset tag of the PC that helps to easily track and inventory the PC. **NOTE:** This column is displayed if you have selected **Asset tag** as an asset identifier. See Set inventory identifiers.

Table 3. Inventory (continued)

Column	Description
	NOTE: To view the asset details, PC health details, and to optimize the PC, click the Asset tag. See Managing a single PC.
Region	Region where the asset is present, for example, Americas.
Product type	Type of Dell device, for example, Latitude.
Service plan	Service plan of the asset, for example, ProSupport Plus. **NOTE:** A graphical representation of the numbers of PCs and the associated service plans is displayed on the **Overview** page.
Model	Model of the PC, for example, Latitude 5400.
Expiration date	Date on which the service plan expires.
Software version	Version of SupportAssist installed on the PC, for example, 3.0.0.4.
System BIOS version	Version of BIOS installed on the PC, for example, 1.31.0.
Last contact to Dell	Date on which the asset last connected to Dell Technologies.
OS	Edition of Windows operating system installed on the PC, for example, Microsoft Windows 10 Enterprise.
OS version	Version of the Windows operating system installed on the PC, for example, 1909.
PC Utilization*	The extent to which a critical hardware component of the PC is used. This is used to gauge the overall performance of the PC. The utilization is categorized as follows based on the criteria defined by Dell: • **Normal**—average load on the PC is normal. • **Elevated**—average load on the PC is increased. • **High**—average load on the PC is at the highest level and may affect the device performance.
CPU utilization*	The average load on the processor of the PC over a selected time period. The utilization is categorized as follows based on the criteria defined by Dell: • **Normal**—average load on the CPU is normal. • **Elevated**—average load on the CPU is increased. • **High**—average load on the CPU is at the highest level and may affect the device performance.
GPU utilization*	The average amount of video memory (VRAM) used over a selected time. The utilization is categorized as follows based on the criteria defined by Dell: • Normal—average GPU utilization is within the normal level. • Elevated—average GPU utilization is increased. • High—average GPU utilization is at the highest level which may affect the device performance and can lead to the video card to wear out sooner than expected.
Memory utilization*	The amount of memory (RAM) installed on the PC and the average amount of memory used over a selected time period. Low memory or consistently high memory reduces the device performance.
Installed memory*	Size of RAM installed on the PC, for example, 32 GB.

Table 3. Inventory (continued)

Column	Description
Battery health*	Average percentage of charge that the battery holds against its designed capacity, when it is fully charged.
Battery runtime*	Average number of hours the PC ran when it was not connected to an electrical outlet.
Free storage remaining*	Average storage remaining out of the installed memory.
PC age*	Number of years/months/days since Dell shipped the PC, for example, 3 yr, 6 mo, 7 d
OS crashes*	Number of operating system failures that occurred on the PC.
App failures*	Number of application failures that occurred on the PC.
Battery event*	Number of errors or failures encountered by the PC battery.
Storage event*	Number of errors or failures encountered by the PC storage.
Thermal event*	Number of components that exceeded sustainable temperature.
OS events*	Number of errors or failures encountered by the operating system.
Utilization events*	Number of errors or failures encountered by a critical hardware component of the PC.
System events*	Number of errors or failures encountered by a key component of the PC.
Health status*	The overall health status of the PC fleet for the selected week or day. The status is categorized as follows: • **Healthy**—the health score is within 51-100, therefore the PC is healthy. • **Needs attention**—the health score is within 10-49, therefore the PC needs attention. • **Unhealthy**—the health score is within 0-9, therefore the PC is not running optimally and affects the fleet performance. • **Data unavailable**—the health data was not received from the PC. **NOTE: Health status** is displayed for PCs with an active warranty.
Current health status*	The current or last updated health status of the PC fleet for the selected week or day. The status is categorized as follows: • **Healthy**—the health score is within 51-100, therefore the PC is healthy. • **Needs attention**—the health score is within 10-49, therefore the PC needs attention. • **Unhealthy**—the health score is within 0-9, therefore the PC is not running optimally and affects the fleet performance. • **Data unavailable**—the health data was not received from the PC. **NOTE: Current health status** is displayed for PCs with an active warranty.

* This data is collected only when the user has logged in and is actively using the PC.

NOTE: The health status and score of the PC are calculated based on various utilization parameters and not based on the hardware failure alerts.

You can use the **Filter** option to filter and view specific information about the PCs, and use the **Advanced Search** option to specify additional requirements for a search. The **Inventory** page also enables you to view the PC details weekly or daily based on your preference.

To download the PC inventory data as a CSV file, from the **Export** list, select **PC inventory**.

You can enter the BIOS passwords that are required for BIOS updates in a spreadsheet. To download the spreadsheet, from the **Export** list, select **Central Resource Manager List**. Enter the BIOS administrator passwords and import the spreadsheet in Central Resource Manager. For information about how to install Central Resource Manager, see the *SupportAssist for Business PCs Deployment Guide* available on the SupportAssist for Business PCs documentation page.

Create a service request

Prerequisites

You must be signed in to TechDirect as a Connect and manage administrator or Connect and manage technician.

About this task

You can create a service request for connected PCs and submit it to Dell Technologies.

NOTE: You cannot create service requests for disconnected PCs.

Steps

1. From the TechDirect dashboard, go to **Connect and manage** > **Manage PC fleet** > **Connect and manage PCs** > **Manage** > **Inventory**.
   The **Inventory** page is displayed.
2. Locate the PC for which you want to create a service request, click ⋮, and then click **Create service request**.
   The **Create Service Request** page is displayed.
3. Verify the Service Tag, select a group, and click **NEXT**.
4. Enter the incident and contact information.
5. Review the information that you entered and click **NEXT**.
6. Click **SUBMIT**.

Results

The service request is submitted to Dell Technologies.

Create dispatch request

Prerequisites

You must be signed in to TechDirect as a Connect and manage administrator or Connect and manage technician.

NOTE: To manage dispatch requests, you must enroll for the self-dispatch service in TechDirect.

About this task

You can create dispatch requests for parts if there is a hardware failure.

NOTE: You cannot create dispatch requests for disconnected PCs.

Steps

1. From the TechDirect dashboard, go to **Connect and manage** > **Manage PC fleet** > **Connect and manage PCs** > **Manage** > **Inventory**.
   The **Inventory** page is displayed.

2. Locate the PC for which you want to create a dispatch request, click ⋮, and then click **Create dispatch request**.
   The **Create Dispatch Request** page is displayed.
3. Verify the Service Tag, select a group, and click **NEXT**.
4. Enter the incident and contact information.
5. Review the information that you entered and click **NEXT**.
6. Click **SUBMIT**.

Results

The dispatch request is submitted to Dell Technologies.

Remove disconnected PCs

About this task

You can remove PCs that are no longer managed or used in your organization.

CAUTION: Ensure that you review the disconnected PCs before you remove them from the inventory.

Steps

1. From the TechDirect dashboard, go to **Connect and manage** > **Manage PC fleet** > **Connect and manage PCs** > **Manage** > **Inventory**.
   The **Inventory** page is displayed.
2. Select **Disconnected PCs** from the list.
3. Select the PCs that you want to remove and click **Remove PCs**.

Results

The selected PCs are removed from the fleet inventory, and the status is displayed on the **Audit Trail** page.

NOTE: If SupportAssist is installed on the PCs, removing the disconnected PCs from the inventory will not uninstall SupportAssist on the PCs.

NOTE: If a disconnected PC was unintentionally removed, you must reinstall SupportAssist. After the reinstallation, you can manage the PC in TechDirect.

Groups overview

Site

When you configure and download SupportAssist from TechDirect using the Connect and manage administrator account, a site is automatically created for that administrator.

When you deploy SupportAssist on PCs, all the PCs on which SupportAssist is deployed is displayed in TechDirect for that site. By default, every site contains a **Default** group.

Groups

A group is a logical entity of PCs within a site. You can create groups to organize the PCs during deployment or in TechDirect. You can create one or more groups and organize your PCs within a site, but you cannot move PCs across groups in different sites.

The **Groups** tab on the **Inventory** page enables you to create a group and organize your PCs.

NOTE: You require Connect and manage administrator rights to organize groups in TechDirect. Connect and manage technicians can organize groups if permitted by the administrator. See Roles and permissions.

For more information about sites and groups, see the *SupportAssist for Business PCs Frequently Asked Questions* available on the SupportAssist for Business PCs documentation page.

Create a group

Prerequisites

You must be signed in to TechDirect as a Connect and manage administrator or Connect and manage technician.

Steps

1. From the TechDirect dashboard, go to **Connect and manage** > **Manage PC fleet** > **Connect and manage PCs** > **Manage** > **Groups** > **Site groups**.
   The **Groups** page is displayed.
2. Click **Create group**.
   The **Create a new group** window is displayed.
3. Select a site and enter a group name.
4. Click **Create**.

Results

The group is created, and the default group configuration of the site is copied to the newly created group.

NOTE: If the primary and secondary contacts are different, ensure that you create separate groups and assign unique primary and secondary contacts for managing these devices.

NOTE: To configure the new preferences, refer to the **Managing SupportAssist preferences** section in Deployment Guide.

Move assets between existing groups

Prerequisites

- You must be signed in to TechDirect as a Connect and manage administrator or Connect and manage technician.
- To move PCs from one group to another, the source and target groups must be within the same site.

Steps

1. From the TechDirect dashboard, go to **Connect and manage** > **Manage PC fleet** > **Connect and manage PCs** > **Manage** > **Groups** > **Site groups**.
   The **Groups** page is displayed.
2. Click **Organize PCs**.
   The **Organize PCs** window is displayed.
3. Select one of the following options:
   - **By using online forms**—to organize PCs by moving them from one group to another group in TechDirect.

     You can move upto 5000 PCs by using online forms.
   - **By downloading and uploading a spreadsheet**—to organize PCs by moving them from one group to another using a spreadsheet.

     You can move unlimited number of PCs by using a spreadsheet.
4. If you selected **By using online forms**, perform the following steps:
   a. From the **Site** list, select the site.
   b. From the **From group** list, select the group from which you want to move the assets.
   c. From the **To group** list, select the asset group to which you want to move the assets.
   d. Select the PCs that you want to move and click **Move**.
5. If you selected **By downloading and uploading a spreadsheet**, perform the following steps:
   a. From the **Site** list, select the site.
   b. From the **Select group** list, select the groups.

c. Download and update the inventory file, and then click **Next**.

   In the spreadsheet, enter the group names in the **To Group** column. If you do not want to move the PC to another group, leave the **To Group** cell blank.

d. Upload the inventory file and click **OK**.
   The group names that are provided in **To Group** column are automatically created, if they do not exist.

Results

The PCs are moved to the new group.

Update site name

Prerequisites

- You must be signed in to TechDirect as a Connect and manage administrator or Connect and manage technician.
- To edit the site name, ensure that you have created one or more asset groups within a site.

Steps

1. From the TechDirect dashboard, go to **Connect and manage** > **Manage PC fleet** > **Connect and manage PCs** > **Manage** > **Groups** > **Site groups**.
   The **Groups** page is displayed.
2. Locate the row where the details of the asset site that you want to update is listed, click ⋮, and click **Edit**.
3. Edit the site name, and click **Save**.

Update group name

Prerequisites

You must be signed in to TechDirect as a Connect and manage administrator or Connect and manage technician.

Steps

1. From the TechDirect dashboard, go to **Connect and manage** > **Manage PC fleet** > **Connect and manage PCs** > **Manage** > **Groups** > **Site groups**.
   The **Groups** page is displayed.
2. Locate the site that contains the group that you want to update and expand the site list.
3. Locate the row where the details of the group that you want to update is listed, click ⋮, and click **Edit**.
4. Edit the group name, and click **Save**.

Delete group

Prerequisites

- Ensure that the group that you want to delete does not contain any assets. To delete a group that has assets in it, move the assets to another group. See Move assets between existing groups.
- You must be signed in to TechDirect as a Connect and manage administrator or Connect and manage technician.

Steps

1. From the TechDirect dashboard, go to **Connect and manage** > **Manage PC fleet** > **Connect and manage PCs** > **Manage** > **Groups** > **Site groups**.
   The **Groups** page is displayed.
2. Locate the site that contains the group that you want to delete and expand the site list.
3. Locate the row where the details of the group that you want to delete is listed, click ⋮, and click **Delete**.

   NOTE: You cannot delete the **Default** group.

Create a custom or dynamic group

Prerequisites

You must be signed in to TechDirect as a Connect and manage administrator or Connect and manage technician.

Steps

1. From the TechDirect dashboard, go to **Connect and manage** > **Manage PC fleet** > **Connect and manage PCs** > **Manage** > **Custom groups**.
   The **Custom groups** page is displayed.
2. Click **Create custom group**.
   The **Search** page is displayed.
3. Click search **Using rules or criteria**
   The **Search by rule** page is displayed.
4. Select the product and, click **Search**.
   The **Search results** page is displayed.
5. Click **Create custom group**, and enter a group name and description.
6. If you want to switch from a static group to a dynamic group, enable the **Switch to a dynamic group** option in the **Create custom group** window.

   NOTE: If you search the groups by criteria, then only **Switch to a dynamic group** option is available.

7. Click **Create group**.
   The custom group is created, and the default configuration settings of the site are applied to the newly created group.

5

Managing a single PC

SupportAssist enables you to view recommendations and perform remote optimizations on a PC. SupportAssist also provides insights about PC health, application experience, and security data, that help manage your PC better.

To manage the PC, go to the **Inventory** page and click the Service Tag of the PC.

Topics:

- PC overview

PC overview

Device details

When you click a Service Tag on the **Inventory** page, the following details are displayed on the **PC Overview** page:

- **Device overview**
  - **Model type**—model of the PC, for example, Latitude 5400.
  - **Service tag**—unique five-to-seven digit alphanumeric code.
  - **Asset tag**—asset tag of the PC.
  - **Express service code**—unique numeric code that Dell uses to identify the PC.
  - **Hostname**—unique hostname of the PC.
  - **Operating system**—edition of Windows operating system installed on the PC, for example, Microsoft Windows 10 Enterprise.
  - **OS version**—version of the Windows operating system installed on the PC, for example, 1909.
  - **System BIOS version**—version of BIOS installed on the PC.
  - **PC age**—number of years/months/days since Dell shipped the PC, for example, 3 yr, 6 mo, 7 d.
- **Service information**
  - **Service plan**—the active service plan of the PC, for example, ProSupport Plus. Click the service plan to view the service plan and warranty details of the PC.
  - **Warranty expiration**—date on which the service plan expires.
  - **Software version**—version of SupportAssist installed on the PC, for example, 3.0.0.35.
  - **Last contact to Dell**—date on which the asset last connected to Dell Technologies.
  - **Recent case details**—case or dispatch request details and its status.
- **Hardware configuration**
  - **Commodity name**—components provided by Dell for the PC, for example, Touchpad.
  - **Dell part #**—unique identifier of the component.
  - **Part description**—unique description of the component.
  - **PPID (Piece Part Identification)**—unique number affixed to the components that can be used to identify and track the component.
  - **Age**—the age of the component in month and year.
  - **Manufacturing date**—the month, date, and year in which the component was manufactured, for example, Jan 1, 2021.
  - **Original configuration (as shipped)**—indicates if the PC contains the components that was originally shipped from Dell Technologies.
- **Driver inventory**
  - **Category**—category of the driver.
  - **Name**—name of the driver.
  - **Current version**—version of the driver.
  - **Last release date**—date on which the driver was released.
- **External devices**
  - **Device type**—type of Dell device, for example, monitor.

- **Service tag**—unique five-to-seven digit alphanumeric code.
- **PPID/Serial number**—unique number affixed to the components that can be used to identify and track the component.
- **Model**—model of the Dell device.
- **Firmware**—firmware details of the device.

NOTE: The **External devices** details are displayed if your PC is connected to the Dell monitor and Dell docking station.

Actions

In the **Actions** section, you can:

- Review the recommendations for the PC and take action on them to keep your PC running at the best. See Recommendations for a specific PC.
- Restore the files and settings of the PC to the previous restore point. See Restoring PC files and settings.

Scores and trends

The **Scores and trends** section enables you to view the scores and trends for the following:

- PC Health
- Application experience
- Security

You can also view a summary of the PC health, application experience, and security in the respective widgets.

NOTE: To view the PC health, application experience, and security data, your PC must have an active ProSupport, ProSupport Plus, or ProSupport Flex for Client service plan.

Table 4. Scores and trends

Widget	Assessment factors	Scoring
Health—displays the health score of the PC and the overall result of the health assessment.	• Battery events • Hardware utilization • OS events • Thermal events • Storage events • System events	The status and scoring is categorized as follows: • **51-100**—PC is healthy. • **10-49**—PC needs attention. • **0-9**—PC is unhealthy and not running optimally. This affects the fleet performance. • **Data unavailable**—health data was not received from the PC.
Application experience—displays the application experience score, number of applications with issues, and the number of most used applications.	• Most used applications • Application context • Application crashes • PCs impacted by the application crash	The application experience is considered good when the score is greater than 10, and is poor when the score is less than 10.
Security—displays the security score and the overall result of the security assessment.	• Anti-virus • BIOS administrator password • BIOS Verification • Disk encryption • Firewall • Indicators of attack • Trusted Platform Module • Intel Management Engine	The status and scoring is categorized as follows: • **70-100**—PC is secure and the risk is minimal. • **50-69**—PC needs attention. • **0-49**—PC is at risk. • **Data unavailable**—data was not received from the PC.

Recommendations for a specific PC

To perform updates and optimizations on the PC, go to the **Inventory** page and click the Service Tag of the PC. You can view or perform optimizations based on the roles and permissions configured by the administrator. See Roles and permissions.

NOTE: You can view recommendations for all PCs that are under warranty. However, remote optimizations are exclusively available for PCs with an active ProSupport Plus or ProSupport Flex for Client service plan. Additionally, regardless of the PC service plan or warranty status, you can remotely update BIOS, drivers, firmware, and Dell applications for all PCs.

You can initiate the following optimizations on PCs for maintenance purposes at regular intervals:

- Scan and install PC updates.
- Scan the PC for hardware issues.
- Boost PC performance by freeing up hard drive space, removing clutter, and improving performance with file optimization.
- Optimize network connectivity by updating the PC settings to ensure that your network is efficient and reliable.
- Isolate, remove, and restore files that are corrupted by viruses and malware to keep PCs secure.

NOTE: For PCs running SupportAssist version 3.6 or earlier, the **Clean files** and **Tune performance** optimizations are displayed instead of **Boost performance**.

NOTE: You cannot install PC updates when using a Remote Desktop Protocol (RDP) connection.

NOTE: When initiating a remote PC update, the process pauses if an audio/video call is in progress using Skype, Teams, Zoom, or Avaya conferencing applications, and resumes automatically when the call ends.

To initiate the optimizations, select the required optimization tasks and click **Run tasks**. When the PC is online and connected to Dell, it checks for pending tasks. Depending on the SupportAssist configuration, the PC user is notified about the optimization tasks or the tasks are performed in the background without user intervention. If the user is notified, the notification is displayed for 90 seconds on the PC. The user can opt to defer the task twice, after which the task is performed automatically. If the PC is unable to run the task, you can initiate the task again.

NOTE: The scan notifications are not displayed on the user PC if:

- The **Display notifications** option is disabled in the SupportAssist configuration.
- The PC is in presentation mode.
- The notifications in the Windows action center are disabled.
- There was no activity on the PC for 15 minutes.
- The PC is locked or signed out.

After the optimization tasks are complete on the PC, a confirmation message is displayed on each tile.

NOTE: You cannot initiate another remote optimization when a task is queued or in progress.

NOTE: After the PC updates are completed, a message is displayed if a PC reboot is required. You cannot perform other optimizations until you reboot the PC.

Restoring PC files and settings

SupportAssist scans the PC and proactively suggests the required driver updates. Before installing an update on the PC, SupportAssist automatically creates a restore point, where applicable. When required, you can use the restore point to uninstall the update from the PC and restore the PC to its previous state remotely. The restore points are available for 30 days.

NOTE: You can only restore the files and settings to the selected restore point. Restoring the BIOS and firmware is not supported.

NOTE: To restore the PC files and settings, the following criteria must be met:

- SupportAssist version 3.5 or later must be installed on the PC.
- PCs must have an active ProSupport Plus or ProSupport Flex for Client service plan.
- You require Connect and manage administrator rights to restore the PC. Connect and manage technicians can restore the PC if permitted by the administrator. See Roles and permissions.
- The **Run all remote scans and updates without end user interaction** option must be disabled in the **Set up and connect** > **Configure preferences** > **Remote actions** section.

NOTE: The restore points are removed when you update SupportAssist to the latest version.

To restore the PC files and settings to its previous state, go to the **Inventory** page and click the Service Tag of the PC. Click the **System restore** tab, select a restore point, and then click **Restore**.

When you initiate the restore process, the PC user is notified and is prompted to confirm the request. When the PC user confirms to request, the operating system reverts to the selected restore point and you can monitor the progress in TechDirect. After the restore is complete, the PC user is prompted to restart the PC, and you can view the PC restore status on the **Summary** > **Audit trail** page. See Audit trail.

Health of a specific PC

Related video: How to view health of your PC fleet using SupportAssist for Business PCs

The **Health** section of the **PC overview** page provides PC health data that helps you assess the overall performance of your PC.

To view the health data, go to the **Inventory** page and click the Service Tag of the PC.

NOTE: The health data is collected only if:

- The user has logged in and is actively using the PC.
- Your PC has an active ProSupport, ProSupport Plus, or ProSupport Flex for Client service plan.

The **Health** section also displays a trend chart of PCs that are healthy, needs attention, and unhealthy, for the last 26 weeks (Weekly view) or 30 days (Daily view). The trend chart is derived based on the overall result of the following health assessments that are performed on the PC:

- Battery events
- Hardware utilization
- OS events
- Thermal events
- Storage events
- System events

The status is categorized as follows:

- **Healthy**—the health score is within 50-100, therefore the PC is healthy.
- **Needs attention**—the health score is within 10-49, therefore the PC needs attention.
- **Unhealthy**—the health score is within 0-9, therefore the PC is not running optimally and affects the fleet performance.
- **Data unavailable**—the health data was not received from the PC.

You can click a specific color-coded section, or date or week, to view information about the performance of the PC.

NOTE: The health status and score of the PC are calculated based on various utilization parameters and not based on the hardware failure alerts.

PC usage

The **PC usage** section provides an overview of system utilization and performance.

This section displays the following:

- **PC utilization**—the extent to which a critical hardware component of the PC is used. This is used to gauge the overall performance of the PC.
- **Memory utilization**—the amount of memory (RAM) installed on the PC and the average amount of memory that is used over a selected time period.
- **CPU utilization**—the average load on the processor of the PC over a selected time period.
- **GPU utilization**—the average amount of video memory (VRAM) used over a selected time.
- **Disk**—the amount of hard drive still available for file storage and the average hard drive activity over a selected time period.
- **Battery health**—average percentage of charge that the battery holds against its designed capacity, when it is fully charged.

PC events

The **PC events** section provides an overview of events that contribute to your PC health score. PC events are system logs that specify an event type, when it occurred, and the impact on your PC.

To view the event type, event description, and date and time on which the event occurred, select an event. The types of events are as follows:

- **Battery**—number of errors or failures encountered by the PC battery.
- **Storage**—number of errors or failures encountered by the PC storage.
- **Thermal**—number of components that exceeded sustainable temperature.
- **Utilization**—number of errors or failures encountered by a critical hardware component of the PC.
- **System Errors**—number of errors or failures encountered by a key component of the PC.
- **OS**—number of errors or failures encountered by the operating system.

Application experience for a specific PC

Related video: How to view application experience for your PC fleet using SupportAssist for Business PCs

The **Application experience** section of the **PC overview** page provides insights on application usage and crashes that help understand the PC performance. This data is collected only when the user has logged in and is actively using the PC.

To view the application experience data, go to the **Inventory** page and click the Service Tag of the PC.

The **Application experience** section also displays a trend chart for application crashes for 26 weeks (Weekly view) or 30 days (Daily view). You can click a specific color-coded section, or date or week, to view information about application crashes and most used applications.

Application crashes and most used applications

The **Application experience** also displays the type of application crash, reason for the crash, and when the crash occurred.

Additionally, this section also displays details about most used applications such as application name, version, crashes per application, time spent on each application, average CPU usage, average memory usage, and average disk usage by the application.

Security for a specific PC

Related video: How to view security of your PC fleet using SupportAssist for Business PCs

The **Security** section of the **PC overview** page provides information about PC security that helps assess the risk to ensure that the PC is free from vulnerabilities and threats.

To view the security data, go to the **Inventory** page and click the Service Tag of the PC.

NOTE: The security data is collected only if:

- You have deployed Dell Trusted Device on your PC fleet. For more information about Dell Trusted Device, see the Dell Trusted Device manuals available on the Dell Trusted Device documentation page.
- Your PC has an active ProSupport, ProSupport Plus, or ProSupport Flex for Client service plan.

The **Security** section displays a trend chart derived based on the overall result of security assessments that are performed on the PC for 90 days.

The following table describes the assessments that are performed on the PC and the associated results:

Table 5. Risk measurements

Risk assessment factor	Possible assessment results
Anti-virus	• **Pass**—anti-virus solution is installed and enabled. • **Fail**—anti-virus solution is not installed and not enabled. • **Data unavailable**—data could not be retrieved from the Dell Trusted Device.

Table 5. Risk measurements (continued)

Risk assessment factor	Possible assessment results
BIOS administrator password	• **Pass**—BIOS administrator password is set. • **Fail**—BIOS administrator password is not set. • **Data unavailable**—data could not be retrieved from the Dell Trusted Device.
BIOS Verification	• **Pass**—BIOS verification test is pass. • **Warning**—other failures detected during the verification. • **Fail**—BIOS verification test is fail. • **Data unavailable**—data could not be retrieved from the Dell Trusted Device.
Disk encryption	• **Pass**—disk encryption is detected. • **Fail**—disk encryption is not detected. • **Data unavailable**—data could not be retrieved from the Dell Trusted Device.
Firewall	• **Pass**—firewall solution is installed and enabled. • **Fail**—firewall solution is not installed and not enabled. • **Data unavailable**—data could not be retrieved from the Dell Trusted Device.
Indicators of Attack	• **Pass**—no indicators of attacks detected. • **Warning**—partial indicators of attacks detected. • **Fail**—complete indicators of attacks detected. • **Data unavailable**—data could not be retrieved from the Dell Trusted Device.
Trusted Platform Module	• **Pass**—Trusted Platform Module is enabled. • **Fail**—Trusted Platform Module is not enabled. • **Data unavailable**—data could not be retrieved from the Dell Trusted Device.
Intel Management Engine	• **Pass**—Intel Management Engine verification test is pass. • **Warning**—other failures detected during the verification • **Fail**—Intel Management Engine verification test is fail. • **Data unavailable**—data could not be retrieved from the Dell Trusted Device

Component verification for a specific PC

The **Component verification** section of the **PC overview** page provides information about the components inside your PC against the factory configuration.

To view the component verification data, go to the **Inventory** page or **Security** > **Component verification** page, click the **Service Tag** of the PC, and select the **Component verification** option.

NOTE: The component verification data is collected only if:

- You have deployed Trusted Device on your PC fleet. For more information about Trusted Device, see the Trusted Device manuals available on the Dell Trusted Device documentation page.
- The PCs have an active entitlement for Secure Component Verification (Cloud).

The **Component verification** section displays tiles for each component inside your PC. Each component tile displays the component model number, revision, serial number, and verification status.

NOTE: PCs with multiple memory modules and fixed storage devices display each component on a single tile.

The following table describes the component verifications that are performed on the PC and the associated results:

Table 6. Component verification

Component	Verification results
CPU	• **Verified**—the CPU inside your PCs match the factory configuration. • **Verification Error**—the CPU inside your PC do not match the factory configuration. • **Data unavailable**—data was not received from the PC.
Onboard Networking	• **Verified**—the components inside your PCs match the factory configuration. • **Verification Error**—the components inside your PC do not match the factory configuration. • **Data unavailable**—data was not received from the PC.
Memory	• **Verified**—the memory inside your PCs match the factory configuration. • **Verification Error**—the memory inside your PC do not match the factory configuration. • **Data unavailable**—data was not received from the PC.
Motherboard	• **Verified**—the motherboard inside your PCs match the factory configuration. • **Verification Error**—the motherboard inside your PC do not match the factory configuration. • **Data unavailable**—data was not received from the PC.
Fixed Storage	• **Verified**—the fixed storage inside your PCs match the factory configuration. • **Verification Error**—the hard drive inside your PC do not match the factory configuration. • **Data unavailable**—data was not received from the PC.
System	• **Verified**—the system information of the PC match the factory configuration. • **Verification Error**—the components inside your PC do not match the factory configuration. • **Data unavailable**—data was not received from the PC.
Trusted Platform Module	• **Verified**—the trusted platform module inside your PCs match the factory configuration. • **Verification Error**—the trusted platform module inside your PC do not match the factory configuration. • **Data unavailable**—data was not received from the PC.

6

Recommendations for your PC fleet

SupportAssist enables you to review the recommendations for the PCs and act on them to keep your PCs running at their best. These recommendations are displayed based on scheduled scans or the latest telemetry data that is collected from the PCs. You can view or perform optimizations based on the roles and permissions configured by the administrator. See Roles and permissions.

To optimize the PCs, from the TechDirect dashboard, go to **Connect and manage** > **Manage PC fleet** > **Connect and manage PCs** > **Manage** > **Recommendations** and select the site and groups from the **Sites & groups** list.

You can initiate the following recommended optimizations on PCs for maintenance purposes at regular intervals:

- Review and schedule PC updates—scan and install PC updates.
- Scan hardware—scan the PC for hardware issues.
- Boost performance—boost PC performance by freeing up hard drive space, removing clutter, and improving performance with file optimization.
- Optimize network—optimize network connectivity by updating the PC settings to ensure that your network is efficient and reliable.
- Remove viruses & malware—isolate, remove, and restore files that are corrupted by viruses and malware to keep PCs secure.

NOTE: You can view recommendations for all PCs that are under warranty. However, remote optimizations are exclusively available for PCs with an active ProSupport Plus or ProSupport Flex for Client service plan. Additionally, regardless of the PC service plan or warranty status, you can remotely update BIOS, drivers, firmware, and Dell applications for all PCs.

NOTE: When initiating a remote PC update, the process pauses if an audio/video call is in progress using Skype, Teams, Zoom, or Avaya conferencing applications, and resumes automatically when the call ends.

NOTE: If you have enabled automatic PC optimization for PCs in SupportAssist preferences, recommendations are not displayed for PCs with an active ProSupport Plus or ProSupport Flex for Client service plan. Instead, optimizations for such PCs are automatically performed during scheduled scans.

If there are any actionable recommendations available for your fleet of PCs, a quick view of PC recommendations is displayed on the **Overview** page. Click the corresponding link to remotely optimize the PC fleet. When the PCs are online and connected to Dell, they automatically check for pending tasks. Based on the group configuration, these tasks are executed on the PCs. If PC updates are not completed within five days, and other tasks within 30 days, they time out. You can then reinitiate the tasks.

NOTE: The scan notifications are not displayed on the user PC if:

- The **Display notifications** option is disabled in the SupportAssist configuration.
- The PC is in presentation mode.
- The notifications in the Windows action center are disabled.
- There was no activity on the PC for 15 minutes.
- The PC is locked or signed out.

NOTE: For larger fleets with numerous recommendations, it is advisable to perform up to 50,000 updates at once.

Topics:

- Review and schedule PC updates
- Scan hardware
- Boost performance
- Optimize network
- Remove viruses & malware

Review and schedule PC updates

About this task

SupportAssist enables you to monitor and update the recommended BIOS, drivers, firmware, and Dell applications for all PCs in your fleet. If your fleet includes more than 100 PCs, you can schedule the PC updates to occur in stages to selected PCs at your preferred date and time.

The **Check for updates** tile on the **Recommendations** page displays the number of updates available for your PC fleet, which you can filter by categories such as critical, recommended, and optional.

- **Critical**—updates that are necessary to ensure that the PCs are healthy.
- **Recommended**—updates that improve the performance of your PCs.
- **Optional**—updates that you can choose to install on your PCs.

NOTE: You may have to restart the PC to complete the installation of certain drivers.

NOTE: You cannot install updates on PCs when using a Remote Desktop Protocol (RDP) connection.

Steps

1. From the TechDirect dashboard, go to **Connect and manage** > **Manage PC fleet** > **Connect and manage PCs** > **Manage** > **Recommendations**.
   The **Recommendations** page is displayed.
2. In the **Check for updates** tile, click **View updates** or **View PCs**.
   The **Check for updates** page is displayed.
3. Select the updates to run on your PCs and click **Next**.
   The **Schedule software updates** page is displayed.
4. In the **Name** section, enter a unique name for the update request and click **Next**.
5. In the **Schedule** section, choose the date and time to begin updating your PCs and click **Next**.
   You can schedule the start date up to three days in advance.
6. In the **Select PCs** section, perform the following steps:

   NOTE: This section is enabled only when your fleet includes more than 100 PCs.

   a. PC updates can be deployed in two stages. For the first stage, you can either use the slider to set the percentage of PCs or enter the number of PCs manually.
      Any PCs not in the first stage is automatically assigned to the second stage.
   b. Optionally, enable the threshold toggle and select a success threshold value for first-stage PCs.
      The second-stage PCs receive updates only if the first-stage PCs meet the set threshold. If this threshold is not met, the second-stage PCs do not receive any updates.
7. Click **Schedule**, and then click **Confirm**.

Results

The PC updates are scheduled. If the PC updates are not executed within five days, they time out and you can initiate the tasks again. You can monitor the progress in the **Track scheduled tasks** section on the **Recommendations** page. If the end user is in an active audio or video call, or a Windows update is in progress, then PC updates automatically pause and resume once the call ends or the update completes.

NOTE: The PC updates are scheduled according to the Connect and Manage administrator PC time zone, instead of the end-user PC time zone.

The following actions can be performed on the scheduled tasks in the **Track scheduled tasks** section:

- To edit the scheduled task, locate the task, click ⋮, and click **Edit**.
- To view the task details, locate the task, click ⋮, and click **View update details**.
- To cancel a queued task, locate the task, click ⋮, and click **Cancel**. You cannot cancel tasks that are in progress.

Scan hardware

About this task

SupportAssist enables you to remotely scan the hardware of your PC fleet to identify any hardware issues.

The **Scan hardware** tile on the **Recommendations** page displays the number of PCs that have not been scanned in **x** number of days, where **x** denotes 30 days, 60 days, or 90 days.

Steps

1. From the TechDirect dashboard, go to **Connect and manage** > **Manage PC fleet** > **Connect and manage PCs** > **Manage** > **Recommendations**.
   The **Recommendations** page is displayed.
2. In the **Scan hardware** tile, click **View PCs**.
   The **Scan hardware** page is displayed.
3. Select the PCs to scan and click **Run**.

Results

The task is queued to run when the PCs are online and connected to Dell. You can monitor the progress in the **Track other tasks** section on the **Recommendations** page.

NOTE: To cancel the task, select **Queued** from the **Status** list, select the updates that you want to cancel, and then click **Cancel**. You cannot cancel tasks that are in progress.

Boost performance

About this task

SupportAssist enables you to remotely boost the PC performance by freeing up hard drive space, removing clutter, and improving performance with file optimization.

The **Boost performance** tile on the **Recommendations** page the amount of cleanable disk space across PCs and the count of PCs that have not been tuned for performance. This information is available for 30, 60, or 90 days.

NOTE: For PCs running SupportAssist version 3.6 or earlier, the **Clean files** and **Tune performance** optimizations are displayed instead of **Boost performance**.

Steps

1. From the TechDirect dashboard, go to **Connect and manage** > **Manage PC fleet** > **Connect and manage PCs** > **Manage** > **Recommendations**.
   The **Recommendations** page is displayed.
2. In the **Boost performance** tile, click **View PCs**.
   The **Boost performance** page is displayed.
3. Select the PCs to boost the performance and click **Run**.

Results

The task is queued to run when the PCs are online and connected to Dell. You can monitor the progress in the **Track other tasks** section on the **Recommendations** page.

NOTE: To cancel the task, select **Queued** from the **Status** list, select the updates that you want to cancel, and then click **Cancel**. You cannot cancel tasks that are in progress.

Optimize network

About this task

SupportAssist enables you to remotely optimize network connectivity by updating the PC settings to ensure that your network is efficient and reliable.

The **Optimize network** tile on the **Recommendations** page displays the number of PCs that have not been optimized for network settings in **x** number of days, where **x** denotes 30 days, 60 days, or 90 days.

Steps

1. From the TechDirect dashboard, go to **Connect and manage** > **Manage PC fleet** > **Connect and manage PCs** > **Manage** > **Recommendations**.
   The **Recommendations** page is displayed.
2. In the **Optimize network** tile, click **View PCs**.
   The **Optimize network** page is displayed.
3. Select the PCs to optimize network and click **Run**.

Results

The task is queued to run when the PCs are online and connected to Dell. You can monitor the progress in the **Track other tasks** section on the **Recommendations** page.

NOTE: To cancel the task, select **Queued** from the **Status** list, select the updates that you want to cancel, and then click **Cancel**. You cannot cancel tasks that are in progress.

Remove viruses & malware

About this task

SupportAssist enables you to remotely isolate, remove, and restore files that are corrupted by viruses and malware to keep PCs secure.

The **Remove viruses & malware** tile on the **Recommendations** page displays the number of unwanted programs available on PCs. You can also filter and view the count of viruses, malware, and Potentially Unwanted Programs (PUPs).

Steps

1. From the TechDirect dashboard, go to **Connect and manage** > **Manage PC fleet** > **Connect and manage PCs** > **Manage** > **Recommendations**.
   The **Recommendations** page is displayed.
2. In the **Remove viruses & malware** tile, click **View PCs**.
   The **Remove viruses & malware** page is displayed.
3. Select the PCs from which you want to remove the unwanted programs and click **Remove**.

Results

The task is queued to run when the PCs are online and connected to Dell. You can monitor the progress in the **Track other tasks** section on the **Recommendations** page.

NOTE: To cancel the task, select **Queued** from the **Status** list, select the updates that you want to cancel, and then click **Cancel**. You cannot cancel tasks that are in progress.

7

Custom catalogs for your PC fleet

In Connect and manage, you can create, manage, edit, and deploy customized catalogs of the latest BIOS, driver, firmware, and Dell application software updates. These custom catalogs help streamline the process of finding and determining PC updates that are essential to keep the PCs secure and updated.

- If your PC fleet is connected to Dell, SupportAssist is installed on your PC fleet, and the PCs have an active ProSupport Plus or ProSupport Flex for Client service plan, you can deploy the custom catalogs in Connect and manage. See Managing catalogs for PCs connected to Dell.
- If your PC fleet is not connected to Dell, SupportAssist is not installed on your PC fleet, or the PCs have an active Basic or ProSupport service plan, you can only deploy the catalogs manually. See Managing catalogs for PCs not connected to Dell.

To manage custom catalogs for your PC fleet, from the TechDirect dashboard, go to **Connect and manage** > **Manage PC fleet** > **Connect and manage PCs** > **Manage** > **Update catalogs**.

NOTE: You require Connect and manage administrator rights to manage custom catalogs. Connect and manage technicians can manage the catalogs only if permitted by the administrator. See Roles and permissions.

The following table summarizes the custom catalog capabilities available for different service plans:

Table 7. Custom catalogs capabilities and Dell service plans

Update catalogs management mode	Service plans	Catalog types	Capabilities		
			Create, manage, and download catalogs	Deploy catalogs manually	Deploy catalogs remotely
PCs connected to Dell and SupportAssist is installed on the PC fleet	• ProSupport Plus • ProSupport Flex for Client	Product Series	Full support	Full support	Full support
		Fleet	Full support	Full support	Full support
		Model	Full support	Full support	Full support
	• Basic • ProSupport	Product Series	No support	No support	No support
		Fleet	No support	No support	No support
		Model	Full support	Full support	No support
PCs not connected to Dell and SupportAssist is not installed on the PC fleet	• Basic • ProSupport • ProSupport Plus • ProSupport Flex for Client	Product Series	No support	No support	No support
		Fleet	No support	No support	No support
		Model	Full support	Full support	No support

NOTE: Arm64-based processors is not supported for Custom catalogs.

Topics:

- Managing catalogs for PCs connected to Dell
- Managing catalogs for PCs not connected to Dell

Managing catalogs for PCs connected to Dell

Related video: How to create and manage catalogs for your PC fleet using SupportAssist for Business PCs

If your PCs are connected to Dell, SupportAssist is installed on the PC fleet, and the PCs have an active ProSupport Plus or ProSupport Flex for Client service plan, you can create, edit, manage, and remotely deploy the catalogs in Connect and manage.

The PC updates can be managed using custom catalogs or by using Dell recommendations. See Set PC update source.

NOTE: Driver scans are supported, and PC users can perform driver scans on their PCs only if:

- You have allowed the PC users to open and run SupportAssist on their PCs.
- You have deployed the catalog remotely through TechDirect. See Deploy a catalog remotely.
- The PCs have an active ProSupport Plus or ProSupport Flex for Client service plan.

Create a new catalog

Prerequisites

You must be signed in to TechDirect as a Connect and manage administrator or Connect and manage technician.

About this task

If your PCs connect to Dell and if the PCs have an active ProSupport Plus or ProSupport Flex for Client service plan, you can create a **Product series**, **Fleet**, or **Model** catalog.

- **Product series**—includes devices in your environment for a particular Dell business PC family.
- **Fleet**—includes all business PCs in your environment.
- **Model**—allows you to select up to 80 individual business PC device models.

NOTE: The Dell business PC models include Latitude, Precision, Optiplex, XPS, Dell Pro and Dell Pro Max.

Steps

1. From the TechDirect dashboard, go to **Connect and manage** > **Manage PC fleet** > **Connect and manage PCs** > **Manage** > **Update catalogs**.
   The **Update catalogs** page is displayed.
2. Click **Create catalog**.
   The **Create new catalog** page is displayed.
3. In the **Catalog type** section, perform the following steps:
   a. From the **Select catalog type** list, select **Product series**, **Fleet**, or **Model**.
   b. If you selected **Product series**, from the **Select family** list, select the PC family.
   c. Enter a catalog name and description.
   d. Click **Next**.
4. If you selected **Model**, perform the following steps:
   a. In the **PC model selection** section, select the PC family and the PC models that you want to include in the catalog, and then click **Next**.
   b. In the **OS selection** section, select the operating systems for the PC models, and click **Next**.
      NOTE: You can select up to 80 individual business PC models. For more than 80 device models, create additional catalogs.
5. In the **Update type** section, perform the following steps:
   a. From the **Select update type** list, select the updates that you want to include in the catalog.
      The PC updates include drivers, BIOS, firmware, and Dell applications.
   b. Click **Next**.
6. In the **Criticality type** section, perform the following steps:
   a. From the **Select criticality type** list, select the type of updates that you want to include in the catalog.
      Depending on the severity, PC updates are classified as follows:
      - **Critical**—updates that are necessary to ensure that the PCs are healthy.
      - **Recommended**—updates that improve the performance of your PCs.
      - **Optional**—updates that you can choose to install on the PCs.
   b. Click **Next**.
7. Click **Create**.

Results

The catalog is created with the latest components preselected and is displayed in the **Catalog list** section of the **Update catalogs** page.

Managing catalogs

After you create a catalog, you can manage the catalogs in the **Catalog list** section of the **Update catalogs** page.

Each catalog definition displays the catalog description, and the models and operating systems in the catalog. To view the catalog description, list of models, and list of operating systems in the catalog, hover over the catalog name.

The following table describes the information that is displayed in the **Catalog list** section:

Table 8. Catalog list

Column	Description
Name	Name that is assigned to the catalog.
Status	The status of the catalog.
Type	The type of catalog deployment, for example, Automatic.
Version	The version of the catalog.
Last modified date	The date and time on which the catalog was last modified.
Last modified by	Name of the administrator or technician who last modified the catalog.

You can also perform various actions on a catalog. To perform the following actions, click ⋮, and click the corresponding action.

- **View Archive**—download or view the catalogs that you archived in the **Production** state.
- **Create Draft**—create another draft catalog. This replaces the existing draft with a new draft.
- **Delete**—delete the catalog definition and the associated catalogs in various states such as **Draft**, **Test**, and **Production**.
- **Edit Definition**—edit the catalog definition.

When a new version of the software component is available or the existing version is discontinued, a ⚠ icon is displayed. To view the list of new or discontinued software components, expand the catalog definition and click the corresponding ⚠ icon.

To update the version that displays the ⚠ icon, perform one of the following steps:

- For catalogs in the **Test** and **Production** states, click ⋮, click **Create Draft**, and then edit the draft. See Modifying update catalogs.
- For catalogs in the **Draft** state, delete the draft and create a new draft.

Catalog states

When you create a catalog, every catalog within the definition is assigned a state. You can assign each catalog to three states—**Draft**, **Test**, and **Production**.

When you create a new catalog, the catalog is automatically assigned the **Draft** state. After approval, you can assign the catalog to the **Test** state where you can test the PC updates. After testing is complete, you can assign the catalog to the **Production** state.

Every catalog also displays the models included for that catalog and the operating systems. To view the list of models and operating systems, hover over the catalog name. To view the catalog state, definition, and its status expand the catalog row.

The following table describes the different states available for a catalog and the associated actions available for each state. To perform the associated actions, expand the catalog definition, click ⋮, and then select the corresponding action that you want to perform on the catalog.

Table 9. Catalog states

State	Catalog definition	Available actions
Draft	Draft Ready—a draft catalog is ready to be tested.	• **Delete**—allows you to delete the catalog in the **Draft** state.

Table 9. Catalog states (continued)

State	Catalog definition	Available actions
		• **Change to Test**—changes the catalog to the **Test** state where you can test the PC updates. • **Edit Draft**—allows you to update the type of PC updates that you want to include or exclude in the catalog. See Modifying update catalogs.
Test	Download Ready—the catalog is ready to be downloaded and tested on the PCs.	• **Create Download**—prepares the catalog for download. • **Download**—allows you to download the catalog to a local environment for testing. To download the catalog, the catalog must contain at least one selected update type. • **Delete**—allows you to delete the catalog in the **Test** state. • **Create Draft**—replaces the existing draft with a new draft as you continue testing. • **Change to Production**—changes the catalog to the **Production** state that you can use to deploy on the PC fleet. • **Edit Test**—allows you to update the type of PC updates that you want to include or exclude in the catalog. See Modifying update catalogs.
Production	Download Ready—the catalog is tested and is ready to be downloaded and deployed on the PC fleet.	• **Download**—allows you to download the catalog for deployment. • **Create Draft**—replaces the existing draft with a new draft as you continue testing. • **Move to Archive**—allows you to archive the catalog if you do not plan to use it anymore. • **Edit Production**—allows you to update the type of PC updates that you want to include or exclude in the catalog. See Modifying update catalogs. When you select **Edit Production**, the current catalog version is archived and a new incremental version is created.

Modifying update catalogs

Before you deploy the customized catalog, you can modify the type of PC updates that you want to include or exclude in the catalog.

To modify the type of PC updates, expand the catalog definition, select ⋮, and then select one of the following options depending on the catalog states:

- **Draft** > **Edit Draft**
- **Test** > **Edit Test**
- **Production** > **Edit Production**

NOTE: When you select **Edit Production**, the current catalog version is archived, and a new incremental version is created.

The PC updates that are displayed are based on your selections while creating the catalog. You can modify the components, updates, and criticality. The latest updates are preselected by default. A roll-up count is also displayed for each filter option.

The following table describes the options that you can modify to include or exclude in the catalog:

Table 10. Filter options

Category	Filter options	Description
Component Display	Selected	Components that you have selected.

Table 10. Filter options (continued)

Category	Filter options	Description
	Unselected	Components that you have not selected.
Version	Latest	Latest version of the components.
	Recent	Latest version and the previous two versions of the components. The current version of the component is selected by default.
	Older	Components older than the n-2 versions, where n is the latest version.
What's New	New Availability	New components that are available when you create a draft or test version of the catalog from an existing production catalog. The latest components are starred.
	Discontinued	Components that are no longer available. Expand the list to review the alternate components and select the appropriate ones. The latest components are starred.
Model Names	-	Enables you to search for model names, and view and edit the components for those models. **NOTE:** If you want to modify or delete components for a model, ensure that it does not affect any other model.
Release ID	-	Enables you to search for release IDs. If the release IDs do not have associated software components, a ⚠ icon is displayed.
Driver Pack ID	-	Enables you to search for a driver pack. The **Name** column displays the software components that are associated with the release IDs in the driver pack.
Update Type	Application	List of Dell application software updates.
	BIOS	List of BIOS updates.
	Driver	List of driver updates.
	Firmware	List of firmware updates.
Importance	Critical	Updates that are necessary to ensure that the PCs are healthy.
	Recommended	Updates that improve the performance of your PCs.
	Optional	Updates that you can choose to install on your PCs.

NOTE: The settings are not autosaved. You must click **Save** after you modify the settings.

The following table describes the information about the components and update packages:

Table 11. Components and update packages

Column	Description
Name	Name of the update package.
Type	Type of the PC update, for example, Firmware.
Release ID	Unique identifier of the update package.
Version	Version of the update package.
Criticality	Severity of the update package, for example, Recommended.
Release Date	Date on which the update package was released.
Size	Size of the update package.

Download updates to the network location

About this task

If you have chosen to store the updates in a network location, you must manually download the updates to that network location before you remotely deploy the catalog using Connect and manage.

Steps

1. Download a catalog.
2. Optionally, Verify the catalog.
3. Extract the downloaded catalog file to a folder.
   The following files are extracted:
   - `<catalog-name>.xml`—the catalog definition file.
   - `UpdateCatalogs.Maker.exe`—the executable file that reads the <catalog name>.xml file and downloads the update packages.
   - `README.txt`—a deployment instructions file.
4. Search for **Command Prompt** and click **Run as administrator**.
5. Type `UpdateCatalogs.Maker.exe -c <catalog_definition_file> -t <specified network location>` and press Enter.

Results

The updates are downloaded to the specified network location.

Deploy a catalog remotely

Prerequisites

- You must be signed in to TechDirect as a Connect and manage administrator or Connect and manage technician.
- The catalogs that you want to deploy must be in the **Test** or **Production** states.
- The PCs that you want to update must be connected to Dell.

About this task

After you create a custom catalog, you can deploy the catalog remotely. The catalog deployment is valid for 30 days.

NOTE: By default, the latest catalogs are downloaded from `https://downloads.dell.com`. If you have specified to save the updates to a local file server or to a different network location in Set PC update source, ensure that you manually download the updates to the specified server, or network location and then deploy the catalog remotely. See Download updates to the network location.

Steps

1. From the TechDirect dashboard, go to **Connect and manage** > **Manage PC fleet** > **Connect and manage PCs** > **Manage** > **Update catalogs**.
   The **Update catalogs** page is displayed.
2. Click **Deploy catalog**.
   The **Deploy catalog** window is displayed.
3. Select the catalog that you want to deploy.
4. From the **Select site & group** list, select the site and group to deploy the selected catalog.
5. Click **Deploy catalog**.

Results

The selected catalog is queued for deployment and may take several minutes to appear on the **Catalog deployments** page depending on the size of the catalog.

The catalog is deployed, and the selected updates are automatically installed on connected PCs with ProSupport Plus or ProSupport Flex for Client service plan. However, for connected PCs with the Basic, ProSupport, or Expired service plan, the catalog is available for you to scan for selected updates and install them manually using the SupportAssist user interface. The updates are also automatically applied to the PCs moved to the site and group to which catalog was deployed.

Catalog deployments

The following table describes information about the deployed catalogs that is displayed on the **Catalog deployments** page:

Table 12. Catalog deployments

Column	Description
Name	Name of the catalog that is selected for deployment. Click the catalog name to view details of the catalog deployment.
Version	The version of the catalog state that is selected for deployment.
Deploy initiated on	The date and time on which the catalog deployment was initiated.
Queued	The number of PCs that are pending catalog deployment. When you deploy a catalog, the PC updates are queued to run when the PC is online and connected to Dell. You can cancel the catalog deployment only when the deployment in the **Queued** status. To cancel the catalog deployment, locate the catalog deployment that you want to cancel, click ⋮, click **Cancel queued catalog** and cancel the deployment.
In progress	The number of PCs on which the catalog deployment is in progress. When the PC is online and connected to Dell, the catalog is deployed on the PC fleet.
Success	The number of PCs on which the catalog is successfully deployed.
Failed	The number of PCs on which the catalog deployment expired or failed. The catalog deployment expires if the catalog is not deployed to the PCs in 30 days. You can try redeploying the catalog.

Affected PCs

When you click a catalog name on the **Catalog deployments** page, the following details about the catalog are displayed on the **Affected PCs** page:

Table 13. Affected PCs

Column	Description
Service tag	A unique five-to-seven digit-alphanumeric code which is found on a white bar-coded label affixed on your Dell PC or peripheral.
Asset tag	Asset tag of the PC that helps to easily track and inventory the PC.
Hostname	Unique hostname of the asset.
Site	Name of the site selected for deployment.
Group	Name of the group within a site selected for deployment.
Reboot required	Displays if a PC restart is required after the PC updates.
Status	The status of the catalog deployment. The status is categorized as follows: • **Queued**—when you deploy a catalog, the PC updates are queued to run when the PC is online and connected to Dell. • **In progress**—when the PC is online and connected to Dell, the catalog is deployed on the PC fleet and the **In progress** status is displayed. • **Success**—the catalog is successfully deployed to the PC. • **Failed**—the catalog deployment expired or failed. The catalog deployment expires if the catalog is not deployed to the PCs in 30 days. You can try redeploying the catalog. After the catalogs are deployed, the status of deployment is also displayed on the **Audit trail** page. See Audit trail.
Reason	Information about the catalog deployment.

Managing catalogs for PCs not connected to Dell

If your PC fleet is not connected to Dell, SupportAssist is not installed on your PC fleet, and the PCs have an active Basic or ProSupport service plan, you can manually select the PC models to create, edit, and download the catalogs in Connect and manage, and then deploy the catalogs manually to your PC fleet.

Create a new catalog

About this task

If your PCs do not connect to Dell, you can only create a **Model** catalog in Connect and manage. This catalog allows you to select up to 80 individual business PC models such as Latitude, Precision, OptiPlex, and XPS. For more than 80 device models, create an additional catalog.

Steps

1. From the TechDirect dashboard, go to **Connect and manage** > **Manage PC fleet** > **Connect and manage PCs** > **Manage** > **Update catalogs**.
2. Click **Create catalog**.
   The **Create new catalog** page is displayed.
3. In the **Catalog type** section, enter a catalog name and description, and click **Next**.
4. In the **PC model selection** section, select the PC line of business and PC models that you want to include in the catalog, and then click **Next**.
5. In the **OS selection** section, select the operating systems for the PC models, and click **Next**.
6. In the **Update type** section, perform the following steps:
   a. From the **Select update type** list, select the updates that you want to include in the catalog.

The PC updates include drivers, BIOS, firmware, and Dell applications.

b. Click **Next**.

7. In the **Criticality type** section, perform the following steps:
   a. From the **Select criticality type** list, select the type of updates that you want to include in the catalog.
      Depending on the severity, PC updates are classified as follows:
      - **Critical**—updates that are necessary to ensure that the PCs are healthy.
      - **Recommended**—updates that improve the performance of your PCs.
      - **Optional**—updates that you can choose to install on the PCs.

   b. Click **Next**.
8. Click **Create**.

Results

The catalog is created with the latest components preselected and is displayed in the **Catalog list** section of the **Update catalogs** page.

Next steps

1. Manage the catalogs.
2. Assign the catalogs to Draft, Test, and Production states.
3. Include or exclude the updates in the catalog.
4. Download and deploy the catalogs manually.

Deploying a catalog manually

To deploy a catalog manually, perform the following steps:

1. Download a catalog.
2. Optionally, Verify the catalog.
3. Download update packages.
4. Deploy the catalog.

Download a catalog

Prerequisites

- You must be signed in to TechDirect as a Connect and manage administrator or Connect and manage technician.
- The catalogs that you want to download must be in the **Test** or **Production** states.

Steps

1. From the TechDirect dashboard, go to **Connect and manage** > **Manage PC fleet** > **Connect and manage PCs** > **Manage** > **Update catalogs**.
   The **Update catalogs** page is displayed.
2. Expand the catalog that you want to download, click ⋮, and then select **Create Download**.
   To download a catalog, the catalog must be in the **Download Ready** status.
   The status of the catalog changes from **Creating Download** to **Download Ready**.
3. Click ⋮ and select **Download**.
   The **Download catalog** window is displayed.
4. Note the checksum value and click **Download catalog**.

Results

The selected catalog is downloaded on your PC.

Verify the catalog

About this task

After you download a catalog, to ensure the integrity of your download, you can verify the checksum value of the catalog.

Steps

1. Open **Windows PowerShell**.
2. Change directory to the folder where you have downloaded the catalog.
3. Type `Get-FileHash .\<name_of_the_downloaded_catalog_file>.zip` and press Enter.
   The SHA-256 Hash value is displayed.
4. Compare the checksum value displayed in the PowerShell window with the value displayed in the **Download Catalog** window.

Results

If the checksum values match, the downloaded catalog file is authentic and not corrupted.

Download update packages

Steps

1. Extract the downloaded catalog file to a folder.
   The following files are extracted:
   - `<catalog-name>.xml`—the catalog definition file.
   - `<catalog-name>.cab`—supports signed CAB files when the *Cab Creation in Zip* feature is enabled.
   - `UpdateCatalogs.Maker.exe`—the executable file that reads the <catalog name>.xml file and downloads the update packages.
   - `README.txt`—a deployment instructions file.
2. Search for **Command Prompt** and click **Run as administrator**.
3. Run the following commands along with `UpdateCatalogs.Maker.exe`:
   - To view the help information, type `-?, -h, or --help` and press Enter.
   - To specify the .xml file, type `-c or --catalog <catalog_definition_file>` and press Enter.

     NOTE: If no catalog file is specified, <catalog name>.xml is searched in the current folder.

   - To specify a target folder for the update packages, type `-t or --target <path>` and press Enter.

     NOTE: If a target folder is not specified, the location of the `UpdateCatalogs.Maker.exe` is chosen by default.

   - The default baseLocation is `https://downloads.dell.com`. To define a new baseLocation, type `-b or --baseLocation <path>` and press Enter.
   - To perform a force-download if a software component installer exists and the download was ignored, type `-f` and press Enter.
   - To combine the .xml files from two or more downloaded catalogs, type `-o or --combine <combineXml.xml>` and press Enter.

Deploy the catalog

After you have downloaded and extracted the update catalog, you can either host that catalog locally or use a deployment tool of your choice to distribute it. Each endpoint must then be configured to point to the location of your update catalog.

The specified catalog is read, and the update packages are downloaded from `https://downloads.dell.com` or from the specified baseLocation.

8

Managing SupportAssist alerts

Hardware failure alerts generated by SupportAssist from connected PCs can be managed in Connect and manage or through an external connected solution. You can manage the alerts for an individual site and group or for all the sites and groups.

If you have configured SupportAssist to manage the alerts in Connect and manage, all alerts are processed as per the configured alert rules.

To manage the alerts in Connect and manage, from the TechDirect dashboard, go to **Connect and manage** > **Manage PC fleet** > **Connect and manage PCs** > **Manage** > **Alerts**.

You can also configure the alerts to be managed through an external solution such as ServiceNow. See Connecting SupportAssist alerts with external solutions.

Topics:

- Alerts overview
- Alert actions

Alerts overview

You can manage alerts generated by SupportAssist manually, or you can forward the alerts to Dell or to a configured external solution. To view the alert details and manage them manually, go to the **Alerts** page in TechDirect.

If you are a Connect and manage administrator or if you are a Connect and manage technician who is permitted by the administrator, you can take various actions on the alert. See, Alert actions.

By default, all alerts generated by SupportAssist are displayed in the **Active alerts** section of the **Alerts** page. If the alerts are not closed or forwarded to Dell or ServiceNow within 60 days of alert creation, the alerts are automatically archived. You can view and close these alerts from the **Archived alerts** section of the **Alerts** page.

The following table describes the information that is displayed on the **Alerts** page:

Table 14. Alerts

Alerts details	Description
Site	Name of the site to which the PC is associated.
Group	Group to which the PC is assigned.
Alert number	The unique number that is assigned to the alert. **NOTE:** To view the alert details and take action on the alert, click the alert number. See Details of a specific alert.
Service tag	A unique five-to-seven digit alphanumeric code which is found on a white bar-coded label affixed on your Dell PC or peripheral.
Asset tag	Asset tag of the PC that helps to easily track and inventory the PC. **NOTE:** This column is displayed if you have selected **Asset tag** as an asset identifier. See Set inventory identifiers.
Hostname	Unique hostname of the asset. **NOTE:** This column is displayed if you have selected **Hostname** as an asset identifier. See Set inventory identifiers.

Table 14. Alerts (continued)

Alerts details	Description
Alert type	The type of alert—**Technical Support** or **Dispatch**. Technical support alerts are the alerts that are created for issues that may need further troubleshooting on the user PCs. If required, the Dell technical support agent connects with the primary and secondary contacts that are mentioned in the group configuration to resolve the PC issues. Dispatch alerts are the alerts that are created when issues are detected in a failing component of the user PCs. These issues may require shipment of a replacement part depending on the Dell business policies.
Commodity	The hardware component on which the alert was generated.
Alert count	The number of alerts generated on the components. The alert count is incremented when an alert is generated or recurred on the PC. However, the alert count is not incremented if the same alert recurs within 24 hours. For technical support alerts, the alert count includes the: ● Alert that first occurred on the PC for one or more components. ● Number of alerts that have recurred for a component. ● Number of alerts appended from a different component in the same PC. For dispatch alerts, the alert count includes the: ● Alert that first occurred on the PC for one or more components. ● Number of alerts that have recurred for a component. To view the alert details, click the alert number. See Details of a specific alert.
Last activity	Date and time of the last activity on the alert. An **Overdue** status is displayed when the alerts have exceeded the inactivity period entered by the administrator when the alert rules are configured. See Set alert rules.
Owner	The owner of the alert. The following is displayed depending on the ownership: ● If the alerts are not assigned, the **Unassigned** status is displayed. ● If the alert is assigned to a technician, the name of the TechDirect administrator or technician is displayed.
Alert created on	Date and time when the alert was created on the PC.
Model	Type of Dell device, for example, Latitude.
Region	Region where the asset is present, for example, Americas.
Service plan	Service plan of the asset, for example, ProSupport Plus.
Logged in user	Details about the logged in user.

Details of a specific alert

When you click an alert number on the **Alerts** page, the following details are displayed:

- **Service tag**—unique five-to-seven digit alphanumeric code.
- **Asset tag**—asset tag of the PC.

- **Hostname**—unique hostname of the PC.
- **Alert type**—the type of alert—**Technical Support** or **Dispatch**.
- **Last activity**—date and time of the last activity on the alert.
- **Due date**—date by which the alert must be resolved.
- **Owner**—the owner of the alert.

If you are a Connect and manage administrator or if you are a Connect and manage technician who is permitted by the administrator, you can take various actions on the alert. See Alert actions.

The **Overview** section displays the following details about all the alerts created on the PC:

- **Details**—the alert description, details about the logged in user, and when the alert was created.
- **Activity history**—provides the record of activities on the alert.

Alert actions

When you select or click an alert number on the **Alerts** page, a list of actions that you can take on the alert are displayed.

The following table describes the actions available for every alert that is created in TechDirect:

Table 15. Alert actions

Available actions	Description
Change ownership	Allows you to do one of the following actions: • **Take ownership**—to assign the alert to yourself. • **Assign ownership**—to assign an administrator, technician, or user as the owner of the alert. • **Unassign ownership**—to unassign the ownership of the alert.
Add notes	Allows you to add details about the alert, for example, issue that was detected or error information for investigation. The notes must not exceed 1000 characters.
Close alert	Allows you to close the alert when the necessary action is taken to resolve the issue. After the alert is closed, the administrator, technician, or Dell Technologies cannot take any further actions on the alert.
Forward To Dell	Allows you to add or update the contact and shipping information and forward the support request to technical support. The contact and shipping information is used by technical support to create support requests and ship any necessary replacement parts. **NOTE:** To avail the onsite services for entitled PCs, you can add notes to request the service before forwarding the alert to Dell. You can continue to monitor the progress of the support request from the **Technical Support** page or **Dispatch Summary** page in TechDirect. To view the **Technical Support** page, from TechDirect, go to **Services** > **Get Support and Replace Parts** > **Technical Support**. To view the **Dispatch** page, from TechDirect, go to **Services** > **Get Support and Replace Parts** > **Self-Dispatch**.
Forward to ServiceNow	Allows you to forward an alert to a configured external solution. **NOTE:** If you are using the ServiceNow instance to manage alerts, and if a technical support alert or incident is already open in ServiceNow for a PC, the forwarded alert is appended to an existing incident in ServiceNow.

9

Remediation rules for your PC fleet

Related video: How to create remediation rules for your PC fleet using SupportAssist for Business PCs

In Connect and manage, you can create remediation rules that help proactively identify and resolve issues or threats that occur on the PCs.

To proactively remediate issues on your fleet, you can configure a mechanism to automatically run remediation rules using Dell SupportAssist scripts or your own PowerShell scripts.

You can create custom workflows with PowerShell scripts or pre-defined skills to remediate issues when using Dell SupportAssist version 4.5.2 or later.

- Dell library scripts are easy-to-use predefined readily available scripts that can be applied to diagnose and remediate issues.
- You can upload your own PowerShell scripts, which are automatically signed, to diagnose and remediate issues on your PCs.

The **Remediation rules** page enables you to create a remediation rule and view information about the rules that are created for your PC fleet. You can define the rule to run for a specific site and group and at a specific frequency.

The Remediation rules are designed to assist administrators in handling issues within their PC fleet. It leverages PC data and fleet insights to allow the creation, customization, and monitoring of rules that aim to resolve common problems and enhancing the end-user experience.

NOTE: You can only remediate PCs that have an active ProSupport Plus or ProSupport Flex for Client service plan.

NOTE: You require Connect and manage administrator rights to create and manage remediation rules. Connect and manage technicians can create and manage remediation rules only if permitted by the administrator. See Roles and permissions.

To create and manage remediation rules for your PC fleet, from the TechDirect dashboard, go to **Connect and manage** > **Manage PC fleet** > **Connect and manage PCs** > **Manage** > **Remediation rules**.

The following table describes the information that is displayed on the **Remediation rules** page:

Table 16. Remediation rules

Column	Description
Rule name	An unique name that is assigned to a rule.
Status	The status of the rule displays whether it is active, inactive, or in draft mode. You can use the toggle to activate or deactivate the rule.
Rule type	Indicates the type of rule, such as Scheduled, Telemetry or Run Once Now.
Category	The workflow category that the rule belongs to, for instance, Dell Workflow or Custom Workflow.
Created by	Name of the administrator or technician who created the rule.
Created on	Date and time when the rule was created.
Last modified by	Name of the administrator or technician who last modified the rule.
Modified on	The date and time of the last modification.

NOTE: Administrators can customize the visibility of columns to display only the most relevant information, simplifying the management of multiple rules.

The interface includes search and filter options, enabling users to quickly locate specific rules based on various criteria such as rule name, category, status, so on.

A **Guide me** option provides additional assistance and instructions on how to use the remediation rules interface, helping users navigate the features more efficiently.

The **Learn More** option is designed to provide users with detailed information about creating and managing remediation rules, along with best practices and advanced usage scenarios. This feature ensures that users have access to all necessary information to optimize their use of remediation rules to enhance their device fleet management.

Topics:

- Create a remediation rule using predefined Dell library scripts
- Creating remediation rules using Custom Workflow scripts
- Details of a specific rule
- Update a remediation rule
- Delete a remediation rule
- Manage PowerShell scripts

Create a remediation rule using predefined Dell library scripts

Prerequisites

- You must be signed in to TechDirect as a Connect and manage administrator or Connect and manage technician.
- The PCs must run SupportAssist version 3.5 or later.

  NOTE: Newer Dell library remediation scripts and enhanced remediation capabilities are available only if you upgrade to SupportAssist for Business PC 4.5.2 or higher version.

- ASP.NET Core Runtime version 8.0.x to install Dell Trusted Device. See Microsoft .NET 8.0.
- The PCs must have an active ProSupport Plus or ProSupport Flex for Client service plan.

About this task

Remediation rules help identify and remediate issues within your PC fleet proactively. You can remediate the PCs by selecting the script from the Dell library and apply it to eligible PCs in your site and group. The following are the scripts available in the Dell library to remediate the PCs:

Table 17. Dell Library Remediation Scripts

Prod Script Name	Description
Slow Boot Time Detection	Monitors boot time over 30 days to find slowdowns, identifying the top three problematic applications. For accurate detection, set the script to run daily and ensure it operates for at least 30 device restarts.
High Network Latency Detection	Detects high network latency on a device by monitoring performance over a minimum period of three weeks, requiring a total execution time of 3–5 weeks, during which it reports any remediation failures.
Windows 11 Readiness	Check if a PC is ready to be upgraded to Windows 11 and checks if the PC meets the minimum requirements for the upgrade.
BIOS Password Compliance	Check if the BIOS on the PC is password-protected.
BitLocker Compliance	Check if BitLocker is enabled on the PC.
Firewall Enabled Compliance	Check if a firewall is activated on the PC.
SafeBIOS Check	Installs the Dell Trusted Device agent and checks if the BIOS signature on the PC matches the known Dell BIOS signature to detect any signs of tampering.
Anti-virus Software Compliance	Check if the PC has either Next-Gen or classic anti-virus installed.
Classic anti-virus Software Compliance	Check whether the PC has a classic antivirus that is installed, which mainly uses signature-based detection to identify malicious software.
NexGen anti-virus Software Compliance	Check if the PC has Next-Gen anti-virus, which uses signature-based detection and AI to identify malicious software.

Table 17. Dell Library Remediation Scripts (continued)

Prod Script Name	Description
Create System Restore Point	Creates a system restore point that can be accessed from the restore page.
Detect AHCI mode	Check if the Advanced Host Controller Interface (AHCI) storage mode is enabled in the BIOS.
Check Local Admin Rights	Detects if the logged-in user has local admin rights on the PC. The script does not verify administrative rights that are granted through Domain Admin Groups (Active Directory, Azure Active Directory, or other directory services).
Detect Chassis Intrusion Compliance	• Determines the current setting of the **Chassis Intrusion** option in the BIOS—**Detection Only** or **Set Chassis Intrusion to On-Silent**. • **Detection Only**—determines if the **Chassis Intrusion** option is set to **Enabled** or **On-Silent**.
Set Chassis Intrusion to On-Silent	Configures the **Chassis Intrusion** option to **On-Silent**. This script works only if the PC BIOS password is not set.
Chassis Intrusion Alert Status	Check if the chassis intrusion switch on the device is tripped.
Clear Chassis Intrusion Warning	Check for any occurrences of chassis intrusion alerts. If an intrusion alert is detected, the script proceeds to clear the warning.
Disable Sleep Mode on AC Power	Set the computer sleep time to **Never** overriding the default of 5 minutes (or any other setting) to prevent the device from entering sleep mode. This ensures that data is not lost due to failed sleep state recovery and helps speed up boot times by eliminating sleep state transitions.
Uninstall DCU when SA-Business PCs are installed	Detects whether both Dell Command Update and SupportAssist for Business PCs are installed, and it uninstalls Dell Command Update. This action prevents conflicts between the two products since SupportAssist for Business PCs already updates drivers and firmware.
Disable RDP	Detects the state of RDP and checks whether it is enabled or disabled. If RDP is enabled, the script disables it and also disables any associated firewall rules.
Rename Computer- Model name and service tag	Update the computer name to the format ModelnameServicetag.
Rename Computer- OS and Service tag.	Update the computer name to the format OSSservicetag.
Rename Computer- Dell and Service tag	Update the computer name to the format DellServicetag.
Audio Optimization with Dell Optimizer	Installs Dell Optimizer to reduce background noise and improves audio quality to optimize the end user's audio experience.
System Reboot - Detection Only	Check whether a reboot has occurred on the device in the past 7 days. Scheduled reboots are essential for maintaining system health, resolving software-related issues, and resetting various operating system services.
System Reboot - Notify User and Reboot	Checks the device's reboot status. If the device has not rebooted in the past 7 days, it issues a toast message to the end user and, upon their consent, reboots the device.
Clear Microsoft Outlook Cache for Improved Performance	Proactively clears the Microsoft Teams cache to enhance performance across the PC fleet. Clearing the cache can resolve corruption sues and significantly improve the overall user experience with Microsoft Teams.
Windows Hello Compliance - Detection Only	Checks the status of Windows Hello capability. **Detection only**—checks if Windows Hello is enabled and if a camera or fingerprint scanner is set up.
Windows Hello Compliance - Show Windows Notification	Notifies the end user to set up Windows Hello Biometrics if Windows Hello is enabled but not yet configured.
Detect and Remediate GPO Policy Refresh	Check whether Group Policy Objects (GPO) have been refreshed in the last 24 hours. If they have, no action is taken. If it has been longer, the script attempts to force an update of the GPO policy.

Table 17. Dell Library Remediation Scripts (continued)

Prod Script Name	Description
Memory Leak Detection	Continuously monitors and logs memory consumption on a device, capturing allocation values daily. After a minimum of seven consecutive daily runs, it analyzes the data for a 10% increase in memory consumption and identifies the top memory-consuming app over the period.
File System Maintenance	Verify the integrity of the file system on the hard drive and fix the file system to prevent operating system issues with the hard disk.
Detect IoA events using Dell Trusted Device	Check for Dell Trusted Device IoA (Indicators of Attack) events and notifies you if any events occur. It helps you proactively manage your device's security at the BIOS level.
Clear DNS Cache	Clears and verifies the DNS cache, which is useful after network changes or when connectivity issues arise.
Update Docking station firmware	Identifies devices with outdated docking firmware and updates them to the latest version to prevent functional issues. It also installs any available drivers that accompany these firmware updates.
Clean Files	Clears temporary, redundant, and other unwanted files from your PC fleet.
Delete Orphan Profiles	Detects and deletes temporary files from your PC fleet.
Detect CVEs and DSAs using Dell Trusted Device	Checks for Dell Trusted Device Common Vulnerabilities and Exposures (CVE) and Dell Security Advisories (DSA) events and provides information about any relevant issues. It helps you proactively manage device security. If events are found, it notifies you of the applicable DSA or CVE, which can be addressed through firmware, BIOS, or operating systemS updates.
Microsoft Store Taskbar Management	Manage the Microsoft Store icon on your taskbar.
Update Storage Firmware for HDDs and SSDs	Proactively identifies devices with outdated SSD/HDD firmware and updates them to the latest version. This helps prevent data corruption, data loss, and system crashes for end users.
Optimize Browser Performance	Optimizes browser performance by clearing cookies and temporary files, updating the browser, resetting host files, updating drivers, and disabling hardware rendering or acceleration in the browser.
Disable Power Management on Network Devices	Disables the default power-saving mode for networkdevices that are enabled by firmware, preventing them from entering sleep mode when inactive. This ensures continuous network connectivity and prevents potential issues that are related to devices not waking up properly.
Disable Power Management on Bluetooth Devices	Disables the default behavior that allows Bluetooth devices to enter power-saving mode when not in use.
BSOD	updates drivers, firmware, and BIOS if it detects one or more BSOD in a week.
Thermal Optimization	Updates drivers, firmware, and BIOS if the CPU temperature is high. The thermal setting is also updated to cool, if required.
Delete Old Profiles	Detects and deletes profiles that have not been logged in on the PC in more than 60 days. **NOTE:** In certain PCs, the **Delete Old Profile** remediation script may not delete user profiles even if the profiles have not been logged in on the PC for 60 days.
Intel RST driver compliance for RAID mode	Detects systems with RAID storage mode that is enabled in the BIOS and, if detected, updates the Intel RST driver along with all recommended BKC drivers. It displays the results in the TechDirect user interface.
BIOS Update for Intel 13th and 14th Gen Processors	Scans to determine if the device is running an affected processor and checks if a BIOS update has not been performed. If no update is found, it initiates a driver update on the device.
USB Headset Issue Detection and Remediation	Updates drivers/firmware/BIOS and sets audio/Realtek services to automatic to address USB headset issues.

Table 17. Dell Library Remediation Scripts (continued)

Prod Script Name	Description
HDD Performance Dectection and Remediation	Monitors hard disk drive performance, identifies potential issues affecting speed and efficiency, and implements necessary remediations to enhance overall drive functionality and reliability.
Battery Charge Policy Update	Updates the battery charge policy to **Primarily AC**, which extends battery life by lowering the charge threshold to prevent the battery from charging to 100 percent capacity.
13_SR_Remediate MS Teams Cache Clearing_SPL-43161.ps1	Proactively clears the Teams cache to enhance performance across the PC fleet. Clearing the cache helps resolve corruption issues and improves overall Teams functionality.
Detect and Enable Microsoft Defender anti-virus services	Detects if Defender A/V services are enabled.
Restart Microsoft Defender anti-virus Services	Detects if Defender A/V services are running.
Detect and Enable Trend Micro anti-virus Services	Detects if Trend A/V services are enabled.
Restart Trend Micro anti-virus Services	Detects if Trend A/V services are running.
Detect and Enable Carbon Black anti-virus Services	Detects if Carbon Black A/V services are enabled.
Restart Carbon Black anti-virus Service	Detects if Carbon Black A/V services are running.
Detect and Enable CrowdStrike anti-virus Service	Detects if Crowdstrike A/V services are enabled.
Restart CrowdStrike Anti-Virus service	Detects if Crowdstrike A/V services are running.
Detect and Enable Symantec Anti-Virus Service	Detects if Symantec A/V services are enabled.
Restart Symantec Anti-Virus service	Detects if Symantec A/V services are running.
Detect and Enable McAfee/Trellix Anti-Virus Service	Detects if Symantec A/V services are running.
Restart McAfee/Trellix Anti-Virus service	Detects if McAfee/Trellix A/V services are running.
Apps Affecting Battery Usage	Identifies the top battery-consuming applications if battery usage is beyond acceptable range.
Disable O365 telemetry sharing	Detects whether the Microsoft Office 365 telemetry feature is enabled. If telemetry is enabled, the script disables it by modifying the registry.
Detect and Remediate Microsoft OneDrive Sync	Detects if Microsoft OneDrive has not synced in 8 hours. If Microsoft OneDrive has not synced, then it restarts Microsoft OneDrive services and checks to ensure if syncing is restored.
Detection ONLY of gaming platforms/applications	Detects the gaming applications: Battle.net, Steam, Epic Game Launcher, Ubisoft Connect, GOG Galaxy, EA, BlueStacks, NOX Player, LDPlayer, MEmu, GameLoop, Ubisoft Nano.
Detection and removal of gaming platforms/applications	Detects the gaming applications: Battle.net, Steam, Epic Game Launcher, Ubisoft Connect, GOG Galaxy, EA, BlueStacks, NOX Player, LDPlayer, MEmu, GameLoop, Ubisoft Nano. If found, this script will run a registry change that blocks Windows execution of the applications so that they cannot be run, started or used.

Table 17. Dell Library Remediation Scripts (continued)

Prod Script Name	Description
Microsoft Teams Network Assessment.	• Executes the Microsoft Teams Network Assessment Tool on a Dell PC three times daily - at 9:00AM, 12:00PM, and 3:00PM (local system time). If a Teams or Zoom call is in progress, the assessment will automatically wait until the call ends before proceeding. • The script runs for seven consecutive days, capturing network performance data. After the collection period, the results are averaged and analyzed to determine whether the device meets the threshold requirements for a high-quality Teams audio/video experience.

NOTE: After the remediation scripts run, they are classified as either remediation or detection scripts.

Remediation scripts display four key data points:

- PCs targeted by this rule
- PCs detected with the issue
- PCs successfully remediated
- PCs that failed remediation

Detection scripts display two key data points:

- PCs targeted by this rule
- PCs detected with the issue

Steps

1. From the TechDirect dashboard, go to **Connect and manage** > **Manage PC fleet** > **Connect and manage PCs** > **Manage** > **Remediation rules**.
   The **Remediation rules** page is displayed.
2. Click **Create a rule**.
   The **Create a rule** page is displayed.
3. In the **Build workflow** section, enter a name for your rule in the **Name your rule** field.
4. In the **Select workflow type** section, choose **Dell Workflow** and, click **Next**.
5. Select a Script From the list of available scripts, select the most appropriate one by clicking the radio button next to the script name.
6. Click **Next** to proceed after selecting the script or **Cancel** if you need to cancel the process.
7. In the **Rule type and schedule** section, choose the occurrence and frequency at which a rule should be executed:
   - ○ **Scheduled**—runs at specific intervals. You must specify the frequency and time (AM or PM).
   - ○ **Telemetry**—based on telemetry data.
   - ○ **Run Once Now**—runs immediately.
8. If you choose **Scheduled**, a drop-down menu appears to select the frequency daily or weekly, and then you select the specific time (AM or PM) suitable for execution.
9. Click **Next** .
10. In the **Assign** section, perform one of the following methods to assign the rule:
    - Assign PCs by site and groups
    - Assign PCs manually

    a. If you choose **Assign PCs by site and groups**, select the site and group to which you want to assign the rule. Click **View PCs** to generate the list of targeted PCs.

    NOTE: The **Sites & groups** list displays only PCs that have an active ProSupport Plus or ProSupport Flex for Client service plan.

    b. Select the rule and, click **Create rule** to finalize, or you can choose to **Save draft** if you need to make further modifications later.

    c. If you choose the **Assign PCs manually**, you can search for up to 30 PCs by choosing one of the following PC identifiers:
    - Service tag
    - Asset tag
    - Hostname

d. Click **Add PC**.

11. Click **Create rule** to finalize, or you can choose to **Save draft** if you need to make further modifications later.

Results

The remediation rule is saved and is displayed on the **Remediation rules** page.

NOTE: By default, the remediation rule is not applied to a new site or groups that are created after the creation of the remediation rule. You must edit the remediation rule to include PCs in the new site or group, to the rule. See Update a remediation rule.

Creating remediation rules using Custom Workflow scripts

Prerequisites

- You must be signed in to TechDirect as a Connect and manage administrator or Connect and manage technician.
- PCs must have an active ProSupport Plus or ProSupport Flex for Client service plan.
- To avoid issues with proxy connections, the PCs must connect to RaaS.
- The PC should run SupportAssist version 4.5.2 or higher.
- .NET Desktop Runtime version 8.0.x. See Microsoft .NET 8.0.

About this task

Remediation rules help identify and remediate issues within your PC fleet proactively. You can remediate the PCs by uploading diagnostic and remediation scripts to detect and resolve any issues that have occurred on the PC.

Steps

1. From the TechDirect dashboard, go to **Connect and manage** > **Manage PC fleet** > **Connect and manage PCs** > **Manage** > **Remediation rules**.
   The **Remediation rules** page is displayed.
2. Click **Create a rule**.
   The **Create a rule** page is displayed.
3. In the **Build workflow** section, enter a name for your rule in the **Name your rule** field.
4. In the **Select workflow type** section, choose **Custom Workflow**.
5. Click **Next**.
6. On the right side, in the **Skills and scripts library** use the search bar to find the skills you want to add.
7. Drag and drop the **Start event** to the main workflow area.
   This process initiates your custom workflow.
8. Drag and drop the **PowerShell** block into the workflow area where you want the skill to be performed and to configure the **PowerShell** skills, perform the following steps:
   a. Click the **PowerShell** skill block in the workflow area to open its properties on the right side of the screen.
   b. On the **Input** field, click the drop-down menu and select the appropriate input for the **PowerShell** script.
   c. If the execution of the **PowerShell** skill requires approval, click under the **Requires Approval** section, click the drop-down menu and, select the appropriate approval requirement.
   d. On the **User Context**, click the drop-down menu and select the appropriate user context for which the skill runs.
9. Click **Upload a PowerShell script**, if the specific script is not available in the library, select your script from your local system, assign it a name for reference, and click **Upload**.

   NOTE: Ensure that the PowerShell script you want to upload is saved in the **.PS1** format. Ensure that the file size does not exceed the maximum limit of **2 MB**.

   The system automatically signs the script using Dell certificates to validate its authenticity.
10. Select and drag the necessary skills and scripts from the skills library to your workflow. Some of the following available options to include:
    - **Product Owned actions**:
      - Disable Remote Desktop

- Enable ICMP Inbound
- Disable ICMP Inbound
- Enable Remote Desktop
- Enable USB Storage
- Disable USB Storage
- Dell Power Config
- Disable File Print and Share
- Enable File Print and Share
- Disable Hibernation
- Disable Hibernation on AC
- Disable Sleep on AC
- Disable Camera
- Enable Camera
- Enable Hibernation
- Enable Hibernation on AC
- Enable Sleep on AC

NOTE: Arrange all the above skills in the desired order based on your workflow requirements.

11. In the **Rule type and schedule** section, choose the occurrence and frequency at which a rule should be performed:
    - **Scheduled**—runs at specific intervals. You need to specify the frequency and time (AM or PM).
    - **Telemetry**—telemetry parameter allows users to set performance rules based on specific metric.
    - **Run Once Now**—runs immediately.
12. If you choose **Scheduled**, a drop-down menu appears to select the frequency daily or weekly, and then you select the specific time (AM or PM) for execution.
13. Click **Next** .
14. In the **Assign** section, choose the sites or groups to which you want to assign this rule. You can filter or search for specific sites or groups.

    NOTE: The **Sites & groups** list displays only PCs that have an active ProSupport Plus or ProSupport Flex for Client service plan.

15. Click **Create rule** to finalize, or you can choose to **Save draft** if you need to make further modifications later.
    The remediation rule is saved and is displayed on the **Remediation rules** page.

    NOTE: By default, the remediation rule is not applied to a new site or groups that are created after the creation of the remediation rule. You must edit the remediation rule to include PCs in the new site or group, to the rule. See Update a remediation rule.

Details of a specific rule

When you click a specific rule name on the **Remediation rules** page, the details of the selected rule are displayed. The status of the remediation rule is shown for the last 30 days.

Overview

The **Overview** provides a summary count of PCs in the following categories:

- PCs targeted with this rule: Displays the number of PCs targeted by the current rule.
- PCs detected with issues: Shows the number of PCs identified with issues.
- PCs remediated: Indicates the number of PCs successfully remediated.
- PCs failed to remediate: Shows the number of PCs that failed remediation.

This data helps evaluate how many PCs were able to self-heal using the remediation script and how many require your attention. You can also use this information to modify the remediation script as needed.

Details

The **Details** section information of the PCs on which the rule was triggered. The following table describes theinformation that is displayed in the **Details** section:

Table 18. Details

Column	Description
Service Tag	A unique five-to-seven digit alphanumeric code which is found on a white bar-coded label that is affixed on your Dell PC or peripheral.
Group	Group to which the asset is assigned.
Site	The name of the site to which the asset is assigned.
Model name	Model of the PC on which the rule was triggered, for example, Latitude 5400.
Incident creation date	Shows when the remediation rule created.
Execution Date	Shows when the remediation rule was executed.
Workflow	Describes the workflow associated with the remediation process. The **View** option under the workflow displays the execution workflow status for Dell workflow as well.
Execution Status	Status of the script execution. The status is categorized as follows: • **Success**—the diagnostic script that is executed successfully and no issues were found. • **Failed**—the diagnostic script execution failed due to various reasons, for example, unsigned script or expired certificate. **NOTE:** Success or failure is determined by the exit codes (zero or nonzero exit codes) that are generated after executing the diagnostic scripts. See Exit codes in PowerShell.
Remediation status	Status of the remediation script execution. The status is categorized as follows: • **Success**—the issues that were found during the diagnostic script execution were solved successfully using the remediation script. • **Failed**—the issues that were found during the diagnostic script execution were not solved successfully using the remediation script. • **Error**—the remediation script execution failed due to various reasons, for example, unsigned script or expired certificate. **NOTE:** Success or failure is determined by the exit codes (zero or nonzero exit codes) that are generated after executing the remediation scripts. See Exit codes in PowerShell.
Approval status	Shows the status of the approval. The status is categorized as follows: • **Pending Approval**—indicates that the workflow is awaiting approval. • **Approved**—indicates indicates that the workflow has been approved. • **Rejected**—indicates that the workflow has been rejected.
Rule Output	Shows the output of the rule applied.

Update a remediation rule

Prerequisites

You must be signed in to TechDirect as a Connect and manage administrator or Connect and manage technician.

Steps

1. From the TechDirect dashboard, go to **Connect and manage** > **Manage PC fleet** > **Connect and manage PCs** > **Manage** > **Remediation rules**.
   The **Remediation rules** page is displayed.
2. Locate the row where the details of the rule that you want to update are listed, click ⋮, and click **Edit**.
3. Update the rule details and click **Update rule**.
   The rule is successfully updated.

Delete a remediation rule

Prerequisites

You must be signed in to TechDirect as a Connect and manage administrator or Connect and manage technician.

Steps

1. From the TechDirect dashboard, go to **Connect and manage** > **Manage PC fleet** > **Connect and manage PCs** > **Manage** > **Remediation rules**.
   The **Remediation rules** page is displayed.
2. Locate the row where the rule that you want to delete is listed, click ⋮, and click **Delete**.
3. In the **Delete rule** window, click **Yes**.

Manage PowerShell scripts

About this task

In this section, you manage the uploading, tracking, and progress of PowerShell scripts for remediation.

Steps

1. From the TechDirect dashboard, go to **Connect and manage** > **Manage PC fleet** > **Connect and manage PCs** > **Manage** > **Remediation rules** > **Manage PowerShell scripts**.
   The **Manage PowerShell scripts** page is displayed.
2. To Manage PowerShell scripts, click **Upload a PowerShell script**, select your script from your local system.

   NOTE: Ensure that the PowerShell script you want to upload is saved in the **.PS1** format. Ensure that the file size does not exceed the maximum limit of **2 MB**.

3. Enter a descriptive name for the script in the **Name** field, and provide a brief summary of the script's functionality in the **Description** field.
4. Specify the script's signature status by selecting **Yes** or **No** under the **Is the script signed?** section.
5. To verify whether the script is signed, perform the following steps:
   - Right-click the `.ps1` file in Windows Explorer.
   - Select **Properties**, and go to the **Digital Signatures** tab.

   If the script is signed, the tab will display relevant signature details, including the signer name, certificate, and timestamp.

   NOTE: Dell does not validate or assume responsibility for scripts you upload. By continuing, you acknowledge and accept responsibility for any outcomes.

6. After completing all required fields and selecting the appropriate signature status, click **Upload** to submit the script.

The script is uploaded successfully.

10

Application experience for your PC fleet

Related video: How to view application experience for your PC fleet using SupportAssist for Business PCs

The **Applications** page enables you to track applications by usage, crashes, and memory utilization that helps understand the performance of each application across the fleet. The application experience data is collected only when the user has logged in and is actively using the PC. You can switch between the **Weekly** view or **Daily** view, based on your preference.

NOTE: You can view the application experience data only for PCs with an active ProSupport, ProSupport Plus, or ProSupport Flex for Client service plan. You can view limited data on PCs with the Basic service plan.

To view the application experience data for your PC fleet, from the TechDirect dashboard, go to **Connect and manage** > **Manage PC fleet** > **Connect and manage PCs** > **Manage** > **Applications**.

The following table describes the information that is displayed on the **Applications** page:

Table 19. Applications

Column	Description
Application name	Name of the application, for example, Zoom or Google Chrome. **NOTE:** To view the application utilization details and crash details, click the application name.
Version	Version number of the application.
Impacted PCs	Number of PCs on which the application stopped responding.
Crash count	Total number of times the application closed unexpectedly across the PC fleet.
Application froze count	Total number of times the application stopped responding across the PC fleet.
Average time in foreground	The average time duration in which the application is actively used.
Average total running time	The average time duration in which the application is running in the background or foreground.
CPU	The application load on the PC processor. The utilization is categorized as follows based on the criteria defined by Dell: • Normal—load on the CPU is normal. • Elevated—load on the CPU is increased. • High—load on the CPU is at the highest level and may affect the device performance.
Memory paged	The size of the paged pool. The paged pool is an area of the PC virtual memory that is used for objects that can be written to disk when they are not being used.
Memory non paged	The size of the non-paged pool. The non-paged pool is an area of the PC virtual memory that is used for objects that cannot be written to disk, and must remain in physical memory as long as they are allocated.
Memory (Working set)	The size of the private memory space that is in use by a particular application. This space is not shared or shareable with other processes.
Network I/O	The rate at which the applications are reading and writing data for network input-output operations.

Table 19. Applications (continued)

Column	Description
Disk I/O	The rate at which the applications are reading and writing data for disk input-output operations.

When you click the **Application name**, the following details about the application are displayed:

- **Application utilization**—provides insights about application usage.
- **Crash details**—provides details about the following:
  - **Process name**—the name of the application that has crashed.
  - **Process version**—the version number of the application that has crashed.
  - **Application error**—the error that has occurred on the application.
  - **Description**—the error description depicting the reason for the application crash.
  - **Impacted PCs**—the number of PCs that are impacted due to the application crash. Click the roll-up count to view details about the impacted PCs.

    NOTE: You can view limited data on PCs with the Basic service plan.

11

Security for your PC fleet

The **Security** page displays information about the security health of your PC fleet and enables you to verify the integrity of the components inside your Dell PC. See Security health and Component verification.

Topics:

- Security health
- Component verification

Security health

Related video: How to view security of your PC fleet using SupportAssist for Business PCs

The **Security** page displays information about the security of the PCs based on the security assessment that is performed periodically. This information helps assess the number of PCs at risk to ensure that the PCs are free from vulnerabilities and threats. You can switch between the **Weekly** view or **Daily** view, based on your preference.

NOTE: The security data is collected only if:

- You have deployed Dell Trusted Device on your PC fleet. For more information about Dell Trusted Device, see the Dell Trusted Device manuals available on the Dell Trusted Device documentation page.
- The PCs have an active ProSupport, ProSupport Plus, or ProSupport Flex for Client service plan. You can view limited data on PCs with the Basic service plan.

To view the application experience data for your PC fleet, from the TechDirect dashboard, go to **Connect and manage** > **Manage PC fleet** > **Connect and manage PCs** > **Manage** > **Security**, and click the **Security health** tab.

The following table describes the information that is displayed on the **Security** page:

Table 20. Security

Column	Description
Site	Name of the site to which the asset is assigned.
Group	Group to which the asset is assigned.
Service tag	A unique five-to-seven digit alphanumeric code which is found on a white bar-coded label affixed on your Dell PC or peripheral. **NOTE:** To view the security information for a single PC, click the Service Tag. See Security for a specific PC.
Asset tag	Asset tag of the PC that helps to easily track and inventory the PC. **NOTE:** This column is displayed if you have selected **Asset tag** as an asset identifier. See Set inventory identifiers. **NOTE:** To view the security information for a single PC, click the Service Tag. See Security for a specific PC.
Hostname	Unique hostname of the asset. **NOTE:** This column is displayed if you have selected **Hostname** as an asset identifier. See, Set inventory identifiers.
Warranty plan	Service plan of the asset, for example, ProSupport Plus.

Table 20. Security (continued)

Column	Description
Region	Region where the asset is present, for example, Americas.
Model	Model of the PC, for example, Latitude 5400.
Security score	The score that enables you to determine the security risk level of PCs in the fleet. The score is derived by performing the following assessment factors: ● Anti-virus solution detected and enabled? ● BIOS administrator password set? ● BIOS Verification pass? ● Disk encryption enabled? ● Firewall solution is detected and enabled? ● Indicators of attack detected? ● Trusted Platform Module is enabled? The score is categorized as follows: ● **70-100**—PCs are secure and the risk is minimal. ● **50-69**—PCs need attention. ● **0-49**—PCs are at risk. For more information about the security assessments that are performed on the PC and the associated results, see Security for a specific PC.
Weekly/Daily status	The overall security risk status for the PC fleet for the selected week or day. The status is categorized as follows: ● **Secure**—the security score is within 70-100 and therefore the PCs are secure. ● **Needs attention**—the security score is within 50-69 and therefore the PCs need attention. ● **Risk**—the security score is within 0-49 and the PCs are the risk to potential threats. ● **Data unavailable**—data was not received from the PC. **NOTE: Weekly/Daily status** is displayed for PCs with an active warranty.
Current status	The current or last updated security risk status for the PC fleet. The status is categorized as follows: ● **Secure**—the security score is within 70-100 and therefore the PCs are secure. ● **Needs attention**—the security score is within 50-69 and therefore the PCs need attention. ● **Risk**—the security score is within 0-49 and the PCs are the risk to potential threats. ● **Data unavailable**—data was not received from the PC. **NOTE: Current status** is displayed for PCs with an active warranty.

Component verification

Secured Component Verification (Cloud) is a supply-chain assurance offering that enables you to verify the integrity of the components inside your Dell PC. The **Component verification** page displays information about the internal components of the PCs based on the verification assessment that is performed. This information helps assess the number of PCs at risk and ensures that the PCs internal components are not modified after shipping from the Dell factory. Secured Component Verification (Cloud) verifies the following components:

- Processor (CPU)

- Trusted Platform Module (TPM)
- Fixed Storage
- Onboard Networking
- Memory (RAM)
- Motherboard
- System Information

NOTE: The component verification data is collected only if:

- You have deployed Trusted Device on your PC fleet. For more information about Trusted Device, see the Trusted Device manuals available on the Dell Trusted Device documentation page.
- The PCs have an active ProSupport, ProSupport Plus, or ProSupport Flex for Client service plan.

To view the component verification data of your PC fleet, from the TechDirect dashboard, go to **Connect and manage** > **Manage PC fleet** > **Connect and manage PCs** > **Manage** > **Security**, and click the **Component verification** tab.

The following table describes the information that is displayed on the **Component verification** page:

Table 21. Component verification

Column	Description
Sites	Name of the site to which the asset is assigned.
Groups	Group to which the asset is assigned.
Service tag	A unique five-to-seven digit alphanumeric code which is found on a white bar-coded label affixed on your Dell PC or peripheral. **NOTE:** To view the component verification information for a single PC, click the Service Tag. See Component verification for a specific PC.
Hostname	Unique hostname of the asset. **NOTE:** This column is displayed if you have selected **Hostname** as an asset identifier. See Set inventory identifiers.
Model	Model of the PC, for example, Latitude 5400.
Last Verified	The date and time on which Secured Component Verification Cloud was run on the PC.
Status	The current component verification status for the PC fleet. The status is categorized as follows: • **Verified**—the components inside your PCs match the factory configuration. • **Verification Error**—the components inside your PC do not match the factory configuration. • **Data unavailable**—data was not received from the PC.

12

Configuring settings

On the **Settings** page, you can configure the following settings:

- Select different options to identify your asset.
- Integrate the alerts with ServiceNow.
- View and modify Connect and manage technician roles and permissions.

To configure the settings, from the TechDirect dashboard, go to **Connect and manage** > **Manage PC fleet** > **Connect and manage PCs** > **Manage** > **Settings**.

NOTE: You require Connect and manage administrator rights to configure the settings.

Topics:

- Set inventory identifiers
- Enable or disable remote support
- Set alert rules
- Set PC update source
- Roles and permissions
- Connecting SupportAssist alerts with external solutions

Set inventory identifiers

Inventory identifier is a unique device identifier used by your company to identify the assets associated with your company.

Prerequisites

You must be signed in to TechDirect as a Connect and manage administrator.

Steps

1. From the TechDirect dashboard, go to **Connect and manage** > **Manage PC fleet** > **Connect and manage PCs** > **Manage** > **Settings** > **Inventory identifiers**.
   The **Inventory identifiers** page is displayed.
2. Select one of the following options:
   - **Asset tag**—asset tag of the PC that helps to easily track and inventory the PC.
   - **Hostname**—unique hostname of the asset.

   NOTE: Service Tag is a default identifier. Service Tag is a unique five-to-seven digit alphanumeric code which is found on a white bar-coded label affixed on your Dell PC or peripheral.
3. Click **Save**.

Results

Along with the Service Tag, the PC details associated with the selected identifier are displayed on multiple applicable pages, for example, **Inventory** page.

Enable or disable remote support

Prerequisites

You must be signed in to TechDirect as a Connect and manage administrator.

About this task

To expedite support and resolution during PC issues, you can enable remote support. This authorization allows Dell technical support to perform the following actions remotely:

- Scan and install PC updates.
- Scan the PC for hardware issues.
- Boost PC performance by freeing up hard drive space, removing clutter, and improving performance with file optimization.
- Optimize network connectivity by updating the PC settings to ensure that your network is efficient and reliable.
- Isolate, remove, and restore files that are corrupted by viruses and malware to keep PCs secure.

Steps

1. From the TechDirect dashboard, go to **Connect and manage** > **Manage PC fleet** > **Connect and manage PCs** > **Manage** > **Settings** > **Remote support**.
   The **Remote support from Dell** page is displayed.
2. Activate **Enable remote support**.
3. In the **Enable remote support** window, select **Yes, enable**.

Results

Remote support is enabled for your PC fleet. After the resolution of PC issues, you can disable and re-enable remote support as needed.

Set alert rules

Prerequisites

You must be signed in to TechDirect as a Connect and manage administrator.

About this task

You can configure rules to determine how SupportAssist alerts are handled in TechDirect. You can choose to retain the alerts in the **Alerts** page or send the alerts to a configured external solution such as ServiceNow. You can also set a standard set of rules for all PCs or customize the rules for a site and group.

Steps

1. From the TechDirect dashboard, go to **Connect and manage** > **Manage PC fleet** > **Connect and manage PCs** > **Manage** > **Settings** > **Alert rules**.
   The **Alert rules** page is displayed.
2. From the **Change alert rules** list, select one of the following options:
   - **Set a standard rule for all PCs**—set a common rule for all your PCs in the fleet.
   - **Customize rules for a group**—customize the rule for a specific group in a site.
3. In the **Inactivity period** section, enter the number of days an alert can reside in the queue with no activity.
   The alert resides in the queue for the number of days you have entered. After the inactivity period ends, a notification is sent to the administrator and alert owner, and the alert status is displayed as **Overdue** in the **Last activity** column of the **Alerts** page. See Alerts overview.
4. In the **Technical support alerts** section, perform one of the following steps:

   Technical support alerts are the alerts that are created for issues that may need further troubleshooting on your PCs. If required, the technical support agent contacts the PC user to understand and resolve the issues.

   - Select **Keep them in the Alerts page** to retain the alerts in the **Alerts** page. You can review and take various actions on the alert. See Alert actions.
   - Select **Forward them to another solution** to send all technical support alerts to the configured external solution.

     If you choose to forward the alerts to another solution, select the solution type and connected solution. For information about how to create a new connection, see Connect to an external solution.

     If the contact and shipping information is missing, you are prompted to add the information before you proceed.

     NOTE: If you want Dell Technologies to resolve the issue, select **Dell** from the **Solution type** list.

5. In the **Parts dispatch alerts** section, perform one of the following steps:

   Dispatch alerts are the alerts that are created for issues with a broken part or component. This issue may require shipment of a replacement part.

   - Select **Keep them in the Alerts page** to retain the alerts in the **Alerts** page. You can review and take various actions on the alert. See Alert actions.
   - Select **Forward them to another solution** to send all technical support alerts to the configured external solution.

     If you choose to forward the alerts to another solution, select the solution type and connected solution. For information about how to create a new connection, see Connect to an external solution.

     If the contact and shipping information is missing, you are prompted to add the information before you proceed.

     NOTE: If you want Dell Technologies to resolve the issue, select **Dell** from the **Solution type** list, and add or edit the user group rule in the **User group management** section.

6. If the **User group management** section is displayed, perform the following:

   Group rules are used for identifying the address for dispatch. When a SupportAssist alert is forwarded to Dell Technologies for parts dispatch, the address information in the alert is compared with the configured user group rules. If a match is found, the address information that is associated with that user group is used for parts dispatch.

   a. Click **Add user group rule**.
   b. Select the location, region, user group, time zone, relationship, and technician, and then click **Add rule**.

   The rule is added, and the **Alert rules** page is displayed.
7. Click **Save**.

Set PC update source

You can manage the updates for your PC fleet using Dell recommended updates or using the custom catalogs.

Prerequisites

You must be signed in to TechDirect as a Connect and manage administrator.

Steps

1. From the TechDirect dashboard, go to **Connect and manage** > **Manage PC fleet** > **Connect and manage PCs** > **Manage** > **Settings** > **Set PC update source**.
   The **Set PC update source** page is displayed.
2. Select one of the following options:
   - **Dell recommended updates**—get PC update recommendations automatically from Dell. See Recommendations for your PC fleet.
   - **Custom catalog updates**—update the PCs by creating, testing, downloading, and deploying custom catalogs on the PC fleet. See Custom catalogs for your PC fleet.
3. If you selected **Custom catalog updates**, perform the following steps:
   a. To automatically apply updates to new PCs and PCs moved to groups with custom catalogs, select the corresponding check box.
   b. To automatically apply updates when a new version of the custom catalog is available, select the corresponding check box.
   c. Enter a network path (\\server\share\folder) or an HTTPS URL (https://example.com/path) where updates are stored.

      NOTE: This setting is only applicable if you want to deploy updates remotely.

      NOTE: Updates stored in this location will be downloaded directly from it. If you choose a local path, updates are downloaded locally to save internet bandwidth.

4. Click **Save**.

Roles and permissions

TechDirect enables company administrators to designate Device Management Administrators and have Connect and manage technicians added for the company account. The Connect and manage administrator can access and manage all SupportAssist activities, whereas a Connect and manage technician has limited access to SupportAssist. The technicians can only manage SupportAssist based on the permissions configured by a Connect and manage administrator.

The **Define roles & permissions** page provides information about the users listed for your PC fleet, their assigned, roles, and so on.

To view and modify the roles and permissions, from the TechDirect dashboard, go to **Connect and manage** > **Manage PC fleet** > **Connect and manage PCs** > **Manage** > **Settings** > **Roles & permissions**.

User details and permissions

The **User details and permissions** section provides information about the following:

- **User**—username of the TechDirect user.
- **Roles**—roles assigned to the user, for example, Connect and manage administrator.
- **Email address**—registered email address of the user.
- **Site managed**—the site managed by the user.
- **Last visit**—date and time on which the user last visited the SupportAssist **Connect and Manage** pages.

Assign site ownership

By default, a new site is created automatically when an administrator deploys SupportAssist on a PC fleet for the first time and the site ownership is assigned to the administrator who deployed SupportAssist. An administrator can also manage multiple sites created by other administrators.

To reassign the site ownership between Connect and manage users or administrators, click ⋮, click **Assign site ownership**, select the user, and then click **Assign site ownership**.

NOTE:

- You can reassign the site ownership only if your PC fleet is running SupportAssist version 3.1 or later.
- You cannot assign site ownership if you are a partner or a client managed by a partner.
- When you upgrade SupportAssist from version 3.0 and earlier to the latest version, SupportAssist automatically creates a new site with the associated groups.

Manage user permissions

You can grant or revoke feature permissions for user roles.

1. Perform one of the following steps:
   - Click **Manage user permissions** and select the user from the **Select user** list.
   - Locate the user role for whom you want to manage the user permission, click ⋮, and then click **Manage user permissions**.
2. Modify the permissions.
3. Click **Save**.

Features, roles, and user permissions

By default, the Connect and manage administrator can access and manage all SupportAssist capabilities and features. You can grant or revoke the technician permissions by selecting or clearing the corresponding check boxes. For more information about SupportAssist capabilities and roles, see Connect and manage roles in TechDirect.

You can edit the feature permissions for required users by using one of the following methods:

- From the TechDirect dashboard, go to **Connect and manage** > **Manage PC fleet** > **Connect and manage PCs** and click **Manage permissions** in the left navigation pane. Select the site and group, edit the feature permissions, and then click **Save**.
- From the TechDirect dashboard, go to **Connect and manage** > **Manage PC fleet** > **Connect and manage PCs** > **Manage** > **Settings** > **Roles & permissions**. In the **User details and permissions** page, click **Manage user permissions**, Select the user, and site and group, edit the feature permissions, and then click **Save**.
- From the TechDirect dashboard, go to **Connect and manage** > **Manage PC fleet** > **Connect and manage PCs** > **Manage** > **Settings** > **Roles & permissions**. Go to the **Features, roles, and permissions** page, edit the permissions, and then click **Save**.

Connecting SupportAssist alerts with external solutions

If your organization uses ServiceNow for IT and Helpdesk management, you can integrate SupportAssist alerts with your ServiceNow solution. Integration with ServiceNow creates an incident in ServiceNow when a SupportAssist alert is generated.

Connect to an external solution

Prerequisites

You must be signed in to TechDirect as a Connect and manage administrator.

Steps

1. From the TechDirect dashboard, go to **Connect and manage** > **Manage PC fleet** > **Connect and manage PCs** > **Manage** > **Settings** > **External solutions**.
   The **External solutions** page is displayed.
2. Click **Connect to a solution**.
3. Enter a solution name.
   Ensure that you enter a unique name between 3-50 characters that contain letters, numbers, space, and one of these special characters . # -
4. For SupportAssist to automatically create an incident in ServiceNow, perform the following steps:
   a. Select **Use ServiceNow Instance**.
   b. Enter the ServiceNow instance ID, username, password, and failure notification email address.

      NOTE: If SupportAssist is unable to automatically create an incident in ServiceNow, an email is sent to the email address provided in the **Failure notification** box.

      NOTE: For a technical support alert, if an incident is already open in ServiceNow for a PC, the forwarded alert is appended to an existing incident in ServiceNow.

   c. Click **Create a test incident in ServiceNow** to send a test alert to your ServiceNow instance.
5. For SupportAssist to send alerts to ServiceNow by email, perform the following steps:
   a. Select **Use Email**.
   b. In the **Alerts Notification** box, enter the email address to which you want to send the SupportAssist alert details.

      NOTE: A forwarded alert creates a new incident in ServiceNow.

   c. Click **Create a test incident in ServiceNow** to send a test email to the email address entered in the **Alerts Notification** box.
6. Click **Connect**.

Results

An external solution connection is created.

Edit an external solution connection

Prerequisites

You must be signed in to TechDirect as a Connect and manage administrator.

Steps

1. From the TechDirect dashboard, go to **Connect and manage** > **Manage PC fleet** > **Connect and manage PCs** > **Manage** > **Settings** > **External solutions**.
   The **External solutions** page is displayed.
2. Locate the row where the details of the connection that you want to update is listed, click ⋮, and click **Edit**.
3. Update the solution name, instance Id, username, password, and failure notification email address, and click **Save**.

Delete an external solution connection

Prerequisites

- You must be signed in to TechDirect as a Connect and manage administrator.
- Ensure that the ServiceNow instance solution that you want to delete is not associated with any alert rule on the **Alerts** page.

Steps

1. From the TechDirect dashboard, go to **Connect and manage** > **Manage PC fleet** > **Connect and manage PCs** > **Manage** > **Settings** > **External solutions**.
   The **External solutions** page is displayed.
2. Locate the row where the details of the connection that you want to delete is listed, click ⋮, and click **Delete**.
3. Click **Ok**.

13

Data exports

In Connect and manage, you can download the data displayed on a specific page as a CSV file and work on the data offline.

If there are fewer than 5000 records, the data file is downloaded immediately to your PC. If there are 5000 or more records, the data is queued for processing and may take a few minutes to be processed. After the data is processed, you can download the data files from the **Data exports** page. A roll-up count denoting the number of data files that can be downloaded, is displayed beside **Data exports** in the left pane.

NOTE: The data files are available on the **Data exports** page only for 24 hours and are visible only to the requestor.

To go to the **Data exports** page, from the TechDirect dashboard, go to **Connect and manage** > **Manage PC fleet** > **Connect and manage PCs** > **Data exports**.

The status of the data exports and data downloads is displayed in the **Operations** view of the **Audit trail** page.

The following table describes the information that is displayed on the **Data exports** page:

Table 22. Data exports

Column	Description
Exported data	The page from which the data was exported, for example, Inventory - PC inventory.
Requested at	The date and time on which the data export request was initiated.
Download validity	The date and time on which the data files expire. The data files are available for download only for 24 hours from the time the data files were created.
Status	The status of the download request. The status is categorized as follows: • **Success**—the data was processed successfully and the data files are available for download. • **In progress**—the data processing is in progress. • **Failed**—the data processing failed.
Actions	The actions that you can take on the data file, for example, Download. If the data processing fails, an error message is displayed.

14

Performance indicators

The key performance indicators (KPIs) help evaluate the effectiveness of the PC fleet. The **Performance Indicators** page displays an overview of the KPIs that help determine the fleet behavior and overall impact on the productivity.

To view the KPIs, from the TechDirect dashboard, go to **Connect and manage** > **Manage PC fleet** > **Connect and manage PCs** > **Summary** > **Performance indicators (KPIs)**.

NOTE: You require Connect and manage administrator rights to view the key performance indicators. Connect and manage technicians can view the KPIs only if permitted by the administrator. See Roles and permissions.

You can view the KPIs for a selected duration and also download a PDF copy of the KPIs overview.

PC fleet

The **PC fleet** section displays the following information:

- Installed PCs—displays the total number of PCs from the start to end of the duration.
- Connected PCs—displays the total number of connected PCs at the end of the duration. Connected PCs are the PCs that have connected to Dell in last 30 days.

Alerts

The **Alerts** section displays the total number of predictive and proactive alerts that can lead to Technical Support alerts or Dispatch alerts.

Predictive alerts are for ProSupport Plus and ProSupport Flex for Client service plans and are based on the PCs telemetry data forecasting future events that may require your attention.

Proactive alerts are based on the current state of the fleet and may require additional action from your end.

PC updates

The **PC updates** section displays information about the following:

- Updates performed using Dell recommended updates—displays the total number of scans, total number of recommended updates, and total number of updates installed on the PC fleet.
- Updates performed using update catalogs—displays the total number of catalogs that are created, the total number of times the catalogs were deployed, and the total number of times the catalogs were downloaded.

Scans and optimization

The **Scans and optimization** section displays information about the scans and optimizations that ran on the PC fleet:

- The overall disk space that was recovered (in GB).
- The total number of unique PCs that were tuned for performance.
- The total number of unique PCs that were optimized for network settings.
- The total number of PUPs, virus, and malware removed from the PC fleet.

Remediation rules

The **Remediation rules** section displays information about the following:

- The total number of times rules were triggered to detect an issue.
- The total number of issues detected.
- The total number of issues remediated.

15

Audit trail

The **Audit trail** page provides a record of activities that are performed by SupportAssist, the Connect and manage administrator, and the Connect and manage technician in the last 30 days. This helps in tracking, monitoring, and reviewing all the actions performed on the PCs, when required.

To view the audit trail details, from the TechDirect dashboard, go to **Connect and manage** > **Manage PC fleet** > **Connect and manage PCs** > **Summary** > **Audit trail**.

You can select a time range and view the audit trail in either **Device** view or **Operations** view.

Device view

In the **Device** view, you can view the activities that are performed or events that have occurred on each PC.

The following table describes the information that is displayed in the **Device** view:

Table 23. Device view

Column	Description
Site	Name of the site to which the PC is assigned.
Group	Group to which the PC is assigned.
Service tag	A unique five-to-seven digit-alphanumeric code which is found on a white bar-coded label affixed on your Dell PC or peripheral.
Asset tag	Asset tag of the PC that helps to easily track and inventory the PC. **NOTE:** This column is displayed if you have selected **Asset tag** as an asset identifier.
Hostname	Unique hostname of the asset. **NOTE:** This column is displayed if you have selected **Hostname** as an asset identifier.
Activity	Type of activity performed by the administrator or technician, for example, Remote Action.
Sub activity	Type of sub activity that is associated with the **Activity**, for example, Tune Performance or Remove Virus and Malware.
Action initiator	The username of the administrator or technician who initiated the activity.
Start date & time	Date and time on which the action was initiated.
End date & time	Date and time on which the action was completed.
Activity details	The details about each activity performed on the PC.
Status	The status of the activity. The status is categorized as follows: • **Success**—the initiated activity was performed successfully. • **Canceled**—the initiated activity was canceled by the administrator, technician, or PC user. • **Expired** —the initiated activity was not executed by the PC.

Table 23. Device view (continued)

Column	Description
	• **Failed**—the initiated activity has failed to perform successfully.

Operations view

In the **Operations** view, you can view the activities that are performed or events that have occurred in the Connect and manage configuration, settings, or preferences.

The following table describes the information that is displayed in the **Operations** view:

Table 24. Operations view

Column	Description
Activity	Type of activity performed by the administrator or technician, for example, Remediation rules.
Sub activity	Type of sub activity that is associated with the **Activity**, for example, Rule activated.
Action initiator	The username of the administrator or technician who initiated the activity.
Start date & time	Date and time on which the action was initiated.
End date & time	Date and time on which the action was completed.
Activity details	The details about each activity performed on the PC fleet.
Status	The status of the activity. The status is categorized as follows: • **Success**—the initiated activity was performed successfully. • **Failed**—the initiated activity has failed to perform successfully.

16

Email notifications from SupportAssist

By default, SupportAssist notifies the primary and secondary contacts of a group configuration in Connect and manage.

NOTE: For alerts, email notifications are sent depending on the configured alert rules. See Set alert rules.

The following table provides a summary of the different types of email notifications that are sent by SupportAssist:

Table 25. Email notifications

Type of email notification	When the email notification is sent
Device registration	When a new site is created and when the first PC is registered with Dell Technologies after deployment by a Connect and manage administrator.
Support request creation for a technical support alert	When an issue is detected in your PC fleet, based on your service plan, SupportAssist automatically creates support requests. Dell technical support will proactively contact you for resolution.
Support request creation for a dispatch alert	When a failed component needs replacement, SupportAssist automatically creates a support request to get the component replaced.
Support request creation failed for a technical support alert	When an issue is detected in your PC fleet, but SupportAssist is unable to create an automated support request, based on your service plan. Contact Dell technical support for assistance.
Support request creation failed for an issue in your helpdesk	When an issue is detected in your PC fleet, but SupportAssist is unable to connect to the ServiceNow instance. Verify the configuration and connection between TechDirect and your ServiceNow instance.
Issue detected on PC with expired service plan	When an issue is detected in your PC fleet, but the service plan is expired.
Software update notification	When a newer version of SupportAssist is available or when new features and enhancements are available for the Connect and manage service in TechDirect.

17

Retrieve SupportAssist data using WMI

You can get information about the state of each system where SupportAssist is deployed by using Windows Management Instrumentation (WMI) classes. The namespace to access the SupportAssist profiles and classes is `root\supportassist`. The information that are exposed by WMI classes is as follows:

- Registration status
- Support request details
- Alert details
- Configuration and entitlement details

This section provides information about the available WMI classes.

DSA_RegistrationInformation

Table 26. DSA_RegistrationInformation

Property	Property Type	Description
InstanceID	CIM_STRING [KEY]	A string that uniquely identifies the instance of the class.
IsRegistrationDone	CIM_BOOLEAN	A Boolean value that indicates whether SupportAssist is registered with Dell. The possible values are: • True—SupportAssist is registered with Dell. • False—SupportAssist is not registered with Dell.
RegistrationErrorCode	CIM_STRING [KEY]	A string that provides information about registration failures.
RegistrationTime	CIM_DATETIME	Indicates the date and time when SupportAssist was registered.

DSA_CaseInformation

Table 27. DSA_CaseInformation

Property	Property Type	Description
InstanceID	CIM_STRING [KEY]	A string that uniquely identifies the instance of the class.
CaseID	CIM_STRING	A string that identifies the support request number created for an instance.
Description	CIM_STRING	A string that provides a description of the support request.
Type	CIM_UNIT16	An integer that indicates the type of the support request. The possible values are: • 0—any other support request. • 1—support request to get support from Dell technical support.

Table 27. DSA_CaseInformation (continued)

Property	Property Type	Description
		• 2—support request for parts dispatch.
Status	CIM_UNIT16	An integer that indicates the status of the support request. The possible values are: • 0—any other status. • 1—the support request has been submitted. • 2—the support request is open. • 3—the support request is reopened. • 4—the support request is in progress. • 5—the customer has deferred the support request. • 6—the support request is closed.
CaseCreationTime	CIM_DATETIME	Indicates the date and time when the support request was created.
AlertDetails	CIM_STRING	The string provides details of the alert for which the support request is created.

DSA_AlertInformation

Table 28. DSA_AlertInformation

Property	Property Type	Description
InstanceID	CIM_STRING [KEY]	A string that uniquely identifies the instance of the class.
TrapID	CIM_STRING	A string that identifies the trap ID of the alert.
EventID	CIM_STRING	A string that identifies the alert ID of the alert.
AlertDecription	CIM_STRING	A string that describes the alert.
AlertTime	CIM_DATETIME	Indicates the date and time when the alert was created.

DSA_SystemInformation

Table 29. DSA_SystemInformation

Property	Property Type	Description
Name	CIM_STRING [KEY]	A string that provides the name of the system.
IsConfigurationSet	CIM_BOOLEAN	A Boolean value that indicates whether the configuration is set on the system. The possible values are: • True—the configuration is set on the system. • False—the configuration is not set on the system.

Table 29. DSA_SystemInformation (continued)

Property	Property Type	Description
Entitlement	CIM_UNIT16	Indicates the service plan of the system. The possible values are: • 0—Other • 1—Basic • 2—ProSupport • 3—ProSupport Plus • 4—Premium • 5—Premium Support Plus • 6—ProSupport Flex for Client • 7—Unknown Warranty
EntitlementExpiryDate	CIM_DATETIME	Indicates the expiry date of the system service plan.
Version	CIM_STRING	A string that identifies the SupportAssist version installed on the system.

DSA_RemoteAction:

Table 30. DSA_RemoteAction:

Property	Property Type	Description
RemoteActionMgmtObject	DtVersion	A string that uniquely identifies remote action status information.
RemoteActionMgmtObject	CommandName	A string that uniquely identifies remote action status information.
RemoteActionMgmtObject	CommandSource	A string that uniquely identifies remote action status information.
RemoteActionMgmtObject	StatusCode	A string that uniquely identifies remote action status information.
RemoteActionMgmtObject	FileToken	A string that uniquely identifies remote action status information.
RemoteActionMgmtObject	StartTime	A string that uniquely identifies remote action status information.
RemoteActionMgmtObject	EndTime	A string that uniquely identifies remote action status information.
RemoteActionMgmtObject	NA	NA

18

Retrieve SupportAssist data using APIs

PC Management APIs in Connect and manage allow you to retrieve alerts, health, application, and security data of PCs in your fleet.

The PC Management APIs enables you to view:

- PC alert information such as alerts type, commodity name, last activity on alert, description, and so on, for a specific PC, group of PCs, and PC fleet.
- PC utilization information such as CPU, GPU, memory, battery, storage, and so on, for a specific PC, group of PCs, and PC fleet.
- PC security data and application experience data for a specific PC, group of PCs, and PC fleet.

NOTE: PC Management APIs are available for the PCs that have an active ProSupport, ProSupport Plus, or ProSupport Flex for Client service plan.

NOTE: APIs are not available for partners and their clients.

Prerequisites

To use the PC Management APIs in Connect and manage, perform the following steps:

1. Register and sign in to the TechDirect account.
2. Activate the Connect and manage service.
3. Activate the API service. To activate the service, go to **Services** > **Get support and replace parts** > **APIs**, and request for an API key.
4. Subscribe to the PC Managements APIs.
5. Deploy SupportAssist on the PC fleet.
6. Request the `client_id` and `client_secret` from the TechDirect API team.
7. Generate an access token. This token should be passed as the HTTPS request Headers - Authorization= Bearer < token>. To generate the access token, see the *OAuth document* available in the `APIs Technical Documents.zip` file.

For information about onboarding to TechDirect and deploying SupportAssist, see the *SupportAssist for Business PCs Deployment Guide* available on the SupportAssist for Business PCs documentation page.

For information about how to access SupportAssist data using APIs, see the PC Management APIs for Connect and Manage page.

A

Remote actions

Configure the following preferences to remotely optimize the connected PCs:

- **Run all remote scans and updates without end user interaction**—allows administrators to remotely optimize your managed PCs without user interaction.
  - **Suppress end user notification in case reboot is needed after installation**—allows SupportAssist to hide reboot notifications to users. If this option is enabled, the PCs are not rebooted automatically. The drivers, firmware, and BIOS updates are applied only when the user reboots the PC manually.
- **Apply PC updates only within a time range (Optional)**—allows SupportAssist to remotely update the PCs only during the selected time period.

B

Features and enhancements in previous versions

v4.9.2.48875

- More enhancements: This update includes performance improvements, security fixes, and bug resolutions.

v4.9.1.48804

- Automated updates: Keep your PC fleet up-to-date with BIOS, Drivers, Firmware by update type, device category or importance automatically.
- Automatic PC updates in your control: Flexibility to enable or disable Automatic PC updates and choose between latest (N) version or previous (N-1) version updates.
- Improved PC updates by adding a retry mechanism to handle temporary failures during driver installation.
- New Dell branded PCs support: SupportAssist for Business PCs can now be deployed on Dell, Dell Pro and Dell Pro Max branded PCs.
- More enhancements: This update includes performance improvements, security fixes, and bug resolutions.

4.5.3.25254

- Enhanced Remediation capabilities: Create custom workflows using your own PowerShell scripts, view the execution status at each step of the remediation workflow, optionally provide additional admin approval before remediation execution, and create draft remediation rules.
- Qualcomm platform support: SupportAssist is supported on Dell devices with Intel x64 and Qualcomm Arm64-based processors.
- PC updates enhancements: Automatically pauses PC updates initiated from TechDirect when the end user's PC is in an active audio or video call using Teams, Zoom, Avaya, and Skype apps. Updates resume automatically once the call ends.
- PC Update Configuration: Ability to configure the type and category of PC updates that end users can install on their PCs.
- Windows dark mode support: The supportAssist end-user interface enhances the user experience by supporting Windows Dark Mode.
- Group name configuration: Option to set or provide group names in the Deployment Package Manager.
- Additional enhancements: This update includes performance improvements, security fixes, and bug resolutions.

4.5.2.24316

- Enhanced Remediation capabilities: Create custom workflows using your own PowerShell scripts, view the execution status at each step of the remediation workflow, optionally provide additional admin approval before remediation execution, and create draft remediation rules.
- Qualcomm platform support: SupportAssist is supported on Dell devices with Intel x64 and Qualcomm Arm64-based processors.
- PC updates enhancements: Automatically pauses PC updates initiated from TechDirect when the end user's PC is in an active audio or video call using Teams, Zoom, Avaya, and Skype apps. Updates resume automatically once the call ends.
- PC Update Configuration: Ability to configure the type and category of PC updates that end users can install on their PCs.
- Windows dark mode support: The supportAssist end-user interface enhances the user experience by supporting Windows Dark Mode.
- Group name configuration: Option to set or provide group names in the Deployment Package Manager.
- Additional enhancements: This update includes performance improvements, security fixes, and bug resolutions.

4.5.1.23326

This update includes security fixes, and bug resolutions.

4.5.0.18225

- Custom groups: A new method for organizing PCs to apply updates. It allows you to define group membership using search criteria and provides the option to configure dynamic membership.
- PC updates: You can now update BIOS, drivers, firmware, and Dell applications across all PCs, regardless of their service plan or warranty.
- Staged PC updates: You can schedule an update to BIOS, drivers, firmware, and Dell applications in two stages and define a success threshold.
- New user interface: The end-user interface has been updated to provide an intuitive experience.
- Enhanced user permissions: IT administrators can configure preferences, to allow non-admin end users to perform tasks such as driver updates and hardware scans on their PCs.
- External network access: You can opt to configure the Central Resource Manager to retrieve BIOS passwords for PCs outside the corporate network.
- Dell library remediation scripts: A new library of Dell-developed remediation scripts is available in TechDirect.
- Enhanced remote support: Dell Technical Support agents can perform remote troubleshooting and resolve issues on managed PCs (subject to IT administrator approval).
- Other enhancements: This update also includes performance improvements, security fixes, and bug fixes.

3.6.0.56884

- Ability to download and deploy SupportAssist without configuring the preferences.
- Ability to include SupportAssist as part of Dell Image Assist or Dell Ready Image.
- Ability to provide contact and shipping details for groups when alerts are forwarded to another solution with incomplete or no contact information.
- For PCs running SupportAssist version 3.6—validity of the remote optimization task is extended from 72 hours to 30 days.

  NOTE: For PCs running SupportAssist version 3.5 and earlier, the validity of the remote optimization task remains as 72 hours.

- Ability to select language preference while entering the primary and secondary contact information.
- Availability of new Dell library remediation scripts—BSOD Remediation and Thermal Optimization.
- Ability to automatically apply updates when a new version of the custom catalog is available.
- Ability to search for information about the PCs by using rules or PC identifiers.
- Performance improvements, security fixes, and bug fixes.

3.5.0.46197

- New and improved deployment experience.
  - Ability to install and independently configure SupportAssist at a later time.
  - Ability to complete SupportAssist deployment using Administrative Template Files (.admx/.adml).
  - Ability to activate SupportAssist using the activation file, if not activated already.
  - Ability to independently download software add-ons like Dell Trusted Device and Central Resource Manager at any time.
- Ability to remotely initiate a system restore to rollback driver updates on a single PC.
- Ability to view the status of PC health, application experience, and security for PCs with Basic service plan.
- Support to create remediation rules using predefined Dell library scripts.
- Availability of context-sensitive help and online resources such as information about webinars, white papers, videos, and so on, in the **TechDirect** > **Connect and manage** user interface.
- Ability to manage user permissions for a required site and group.
- Enhancements to custom catalog capabilities.
  - Ability to view the status of catalog deployment for each PC.

  - Ability to view the status of individual updates deployed on a PC through custom catalogs.
  - Ability to automatically apply custom catalogs for PCs newly added to the site and group.
- Support to update Central Resource Manager to the upcoming version automatically.

  NOTE: This is supported only after Central Resource Manager is manually updated to version 3.5.

- Support for predictive hardware failure alerts from PCs with an active ProSupport service plan.
- User interface enhancements:
  - Option to view and export the BIOS version from the **PC inventory** page.
  - Option to view service plan and warranty details for a single PC.
  - Option to view details about Dell monitor and Dell docking station connected to a PC.
- Ability to search for information about the PCs by using rules or PC identifiers.
- Performance improvements, security fixes, and bug fixes.

3.4.1.42601

- Support to deploy SupportAssist for Business PCs using Microsoft Intune.
- Support to immediately apply updated configurations to the PC fleet.
- Ability to enable temporary administrator access for the PC users to use SupportAssist.
- Support to verify integrity of components on PCs that have the Secure Component Verification (Cloud) entitlement.
- Support for a newer version of Dell Trusted Device—version 5.6.
- Enhancements to custom catalog capabilities.
- User interface enhancements to sorting and filtering on various pages.
- Performance improvements and bug fixes.

C

Resources

This section lists the documentation resources and other useful links that provide more information about SupportAssist.

Documentation and others

Table 31. Resources

For more information about	See	Available at
Onboarding to TechDirect, configuring, downloading, and deploying SupportAssist on the PC fleet	IT Administrators—*SupportAssist for Deployment Guide*	SupportAssist documentation page
	Partners—*SupportAssist for Deployment Guide for Partners*	
Using TechDirect to manage your PCs running SupportAssist	*SupportAssist for Administrator Guide*	
Frequently asked questions and answers about SupportAssist	*SupportAssist for Frequently Asked Questions*	
Setting up SupportAssist	*SupportAssist for Quick Setup Guide*	
Data collected from various components of your PC	*SupportAssist for Data Collected from Connected PCs*	
Summary of recent changes, enhancements, known issues, and limitations in the release	*SupportAssist for Release Notes*	
Using SupportAssist that is configured and deployed on your PC by your administrator	*SupportAssist for User's Guide*	
Enrolling your organization, managing SupportAssist alerts, and parts dispatch requests in TechDirect	TechDirect dashboard	TechDirect
SupportAssist benefits and features	SupportAssist home page	SupportAssist home page
Using Image Assist Dynamic	*Image Assist Dynamic for Multiple Platforms User's Guide*	Image Assist documentation page
Ready Image current features and versions	Dell Ready Image Technical Specifications	Dell Ready Image Technical Specifications

Videos

- How to onboard to TechDirect to set up and connect SupportAssist—demonstrates how to onboard to TechDirect and activate the Connect and manage service.
- How to view health of your PC fleet using SupportAssist—demonstrates how to view the health of your PC fleet.
- How to view application experience for your PC fleet using SupportAssist—demonstrates how to view the application experience data for your PC fleet in Connect and manage.
- How to view security of your PC fleet using SupportAssist—demonstrates how to view the security data for your PC fleet.
- How to create remediation rules for your PC fleet using SupportAssist—demonstrates how you can create remediation rules that help proactively identify and automatically resolve issues or threats that occur on the PCs.

- How to create and manage catalogs for your PC fleet using SupportAssist—demonstrates how to create and manage catalogs and deploy PC updates remotely.

D

Contact Dell

About this task

To contact Dell for issues on the Connect and manage service and SupportAssist, perform the following steps:

Steps

1. Go to TechDirect and click **Contact us**.
   The **Contact us** page is displayed.
2. Enter the name, email address, phone, company, and select the region.
3. From the **Services** list, select **SupportAssist**.
4. From the **Subject** list, select a required subject.
5. Enter the Service Tag and a message, attach any helpful files, and then click **Submit**.