

SupportAssist for Business PCs

Deployment Guide

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.....	5
Version.....	5
New and enhanced features.....	5
Audience.....	5
Document purpose.....	5
Getting started with SupportAssist.....	6
Chapter 2: Onboarding to TechDirect.....	7
Create a TechDirect account.....	7
Create a new company.....	7
Join an existing company.....	8
Activate the Connect and manage service.....	8
Add technicians.....	9
Chapter 3: Prerequisites to deploy SupportAssist.....	10
Chapter 4: Configure and connect SupportAssist downloaded from TechDirect.....	14
Create a new deployment.....	14
Manage deployment for an existing site.....	15
Configure the existing deployment.....	15
Download Deployment Package Manager.....	16
Download activation file.....	16
Managing SupportAssist preferences.....	17
General.....	17
PC updates.....	17
Schedule scans and optimizations.....	18
User interaction.....	19
Create the SupportAssist deployment package.....	19
Modify an existing SupportAssist deployment.....	21
Deploy SupportAssist on the PC fleet.....	23
Run the SupportAssist self-diagnosis test.....	26
Configure and deploy SupportAssist on new PCs.....	27
Install Central Resource Manager.....	27
Updating SupportAssist for Business PCs and software add-ons.....	28
Chapter 5: Deploy SupportAssist using Dell Management Portal and through Microsoft Intune... 30	
Chapter 6: Configure and connect SupportAssist installed through other Dell sources.....	31
Download the SupportAssist Deployment Package Manager.....	31
Generate the SupportAssist deployment package.....	32
Appendix A: Activate SupportAssist using Administrative Template Files (.admx/.adml).....	35
Securing the SupportAssist Deployment Registry Key Using Group Policy.....	36

Appendix B: Connect and manage roles in TechDirect.....	37
Appendix C: Version and validity.....	40
Appendix D: SupportAssist version and deployment product code.....	42
Appendix E: Features and enhancements in previous versions.....	43
Appendix F: Resources.....	46
Appendix G: Contact Dell.....	47

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.

SupportAssist allows you to update your Dell PC either automatically or manually.

SupportAssist can identify and self-heal commonly occurring issues using remediation scripts

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](#)
- [Getting started with SupportAssist](#)

Version

v5.2.1.2141

New and enhanced features

- Support for MS .NET 10.0.x Desktop Runtime version.
- Introduced Command Line Interface (CLI) support to automate Driver scans and Driver updates.
- New Reminder notifications with deferral options to end users when installed PC updates require mandatory restart.
- Improved audit trail messages for PC updates installation status.
- Easily identify IT-managed PCs in TechDirect using a registry key.
- Other enhancements: This update also includes performance improvements, security fixes, and bug fixes.

Audience

The information in this deployment guide is intended for administrators who manage the deployment of SupportAssist on PCs running the Windows operating system.

Document purpose

This document provides information about onboarding to TechDirect, and configuring and deploying SupportAssist on PCs running the Windows operating system.

Getting started with SupportAssist

SupportAssist is available through the following sources:

1. TechDirect—an online portal that enables you to configure SupportAssist, download a customized SupportAssist package, and manage your PC fleet with ProSupport suite capabilities.
2. Dell Management Portal - Publish SupportAssist for Business PCs from [management portal](#), to your Intune instance and deploy to your PC fleet via Intune security groups.
3. Ready Image—a clean simple image with no added software. You can include SupportAssist for Business PCs while purchasing the Ready Image solution.
4. SupportAssist page—manually download the latest version of SupportAssist from the [Connect to SupportAssist for Business PCs in TechDirect](#) page.
5. Intune Enterprise App Catalog - Deploy SupportAssist for Business PCs to your PC fleet directly from Intune Enterprise App Catalog.

For more information about configuring and connecting SupportAssist, see [Configure and connect SupportAssist downloaded from TechDirect](#) or [Configure and connect SupportAssist installed through other Dell sources](#).

Onboarding to TechDirect

TechDirect is an online portal that enables you to configure SupportAssist, download a customized SupportAssist package, and manage your PC fleet with ProSupport suite capabilities.

To start managing your PC fleet using SupportAssist, you must first onboard to TechDirect.

Related video: [How to onboard to TechDirect to set up and connect SupportAssist for Business PCs](#)

Topics:

- [Create a TechDirect account](#)
- [Create a new company](#)
- [Join an existing company](#)
- [Activate the Connect and manage service](#)
- [Add technicians](#)

Create a TechDirect account

About this task

You must create a user account to use Connect and manage in TechDirect.

Steps

1. Go to [TechDirect](#).
2. Click **Register at Dell.com**.
3. Enter the name, email address, and password.
4. Click **Create Account**.
A one-time verification code is sent to the email address you entered.
5. Enter the verification code and click **Verify and sign in**.

Results

Your TechDirect account is created.

Next steps

[Create a new company](#) or [Join an existing company](#).

Create a new company

About this task

To start managing your PC fleet, you must designate an administrator and your TechDirect account must be associated with a company. If your company does not exist in TechDirect, you can create a new company and assign administrator rights to your account. If your company exists, you can join the company. For information about joining an existing company, see [Join an existing company](#).

Steps

1. Sign in to [TechDirect](#).
2. Read the license agreement and click **Agree and continue**.
The **What's your role** page is displayed.
3. Select **Create a new company in TechDirect and assign myself as the administrator**.

The **Complete your profile** page is displayed.

4. Enter a company name, select the country or region, and then enter the address.
5. Select **For my company**.
6. Click **Submit**.

Results

A new company is created and you are assigned as the administrator. As a company administrator, you have full access to manage services and user permissions for the TechDirect account of your company.

Next steps

[Activate the Connect and manage service.](#)

Join an existing company

If your company exists in TechDirect, you can associate your TechDirect user account with the existing company.

Prerequisites

Ensure that your company is already created in TechDirect and is associated with a company administrator.

Steps

1. Sign in to [TechDirect](#).
2. Read the license agreement and click **Agree and continue**.
The **What's your role** page is displayed.
3. Select **Create a new account for myself and request to join my company's TechDirect account..**
The **Join Company** page is displayed.
4. Enter a company name and click **Search**.
The list of companies that match your search criteria is displayed.
5. Click **Join this Company**.
6. Complete or update your profile settings.

Results

The company administrator is notified and the administrator must approve your request to join the company. After your request is approved, the company administrator can assign you permissions to access certain TechDirect services and accounts.

Next steps

[Activate the Connect and manage service.](#)

Activate the Connect and manage service

To use SupportAssist in TechDirect, you must activate the Connect and manage service.

Steps

1. Sign in to [TechDirect](#) as a company administrator.
2. Select your username and click **My profile**.
The **Profile Settings** page is displayed.
3. In the **Activations** section, activate the **Connect and manage** service for your company.
The active TechDirect services are displayed in the **Roles** section.

Results

The Connect and manage service is activated, and you can start configuring SupportAssist.

Next steps

1. [Create a new deployment.](#)
2. Optional: [Add technicians.](#)
3. Optional: You can enable single sign-on for Connect and manage users in TechDirect. For information about enabling single sign-on, see [How to Set Up Single Sign-On](#) (available only in English).

Add technicians

Prerequisites

You must be signed in to TechDirect as a company administrator.

About this task

Optionally, a company administrator can add Connect and manage technicians to a TechDirect account and assign permissions to access certain TechDirect services and accounts.

The Connect and manage technicians have limited access to SupportAssist. By default, a technician can only view PC details and manage recommendations. However, these permissions can be configured by a Connect and manage administrator. For more information, see [Connect and manage roles in TechDirect](#).

Steps

1. Sign in to [TechDirect](#).
2. Go to **Utilities > Administrator Control Panel**.
3. Click **ADD TECHNICIAN**.
4. In the **Technician information** section, enter the technician information, select **Technician** for the Connect and manage role, and click **Next**.
5. In the **User Group (Branch) Information** section, select **Additional Groups** if required, and click **Next**.
6. Review the information provided and click **SUBMIT**.

Results

The technician is added to your account, and an email with login instructions is sent to the technician.

Next steps

[Create a new deployment.](#)

Prerequisites to deploy SupportAssist

Requirements

To deploy SupportAssist to a fleet of PCs, the target systems must meet the following requirements:

- Microsoft Windows 11 Operating System.
- PowerShell Script Execution.
- NET Desktop Runtime version 10.0.x. See [Microsoft .NET 10.0](#).
- Network requirements to enable and allow network traffic to [*.dell.com](#).

Network requirements

To deploy SupportAssist, the target PC must meet the following network requirements:

- Active Internet connection.
- Transport Layer Security (TLS) version 1.2.
- To allow SupportAssist for Business PCs to function properly and end user PCs able to communicate with TechDirect, we recommend to enable and allow network traffic to [*.dell.com](#) destination endpoint for listed ports and protocols in below table. Alternatively, you must enable the ports, communication modes, protocols, and specific endpoints listed in the table.
- The following table lists the ports, communication modes, protocols, and endpoints that must be enabled on end-user PCs to allow SupportAssist for Business PCs to function properly:

Table 1. Ports, communication mode, protocol, and endpoints

Port	Communication mode	Protocol	Destination	Purpose
443	Inbound and outbound secure connection to and from the destination	HTTPS	https://sacommercial.apis.dell.com	○ To communicate with Dell to retrieve the configuration settings. ○ To register Central Resource Manager to TechDirect, if applicable.
			https://saservices.dell.com	○ To register SupportAssist to TechDirect and upload SupportAssist log files to Dell. ○ To register Central Resource Manager to TechDirect, if applicable.
			○ https://downloads.dell.com ○ https://dl.dell.com ○ https://dellupdater.dell.com/	○ To scan for viruses and malware, and download catalog files. ○ To update SupportAssist automatically and

Table 1. Ports, communication mode, protocol, and endpoints (continued)

Port	Communication mode	Protocol	Destination	Purpose
				install drivers on the PC.
			https://apigtwb2c.us.dell.com	To retrieve the PC warranty data.
			https://hb.apis.dell.com	To collect and send the date on which the PC last connected to Dell.
			https://api.agent.dcca.dell.com	To collect and upload PC inventory and utilization data to Dell.
			https://raas.dell.com (Required from SupportAssist 4.5.2 or higher versions)	To diagnose the PCs for issues and remediate them.
			- o https://schashcheck.sutherlandglobal.com - o https://smartcheck.sutherlandglobal.com	To detect and remediate virus and malware issues. i NOTE: Enabling these endpoints is optional and only necessary if you have enabled the Remove viruses & malware option in SupportAssist preferences.
			- o https://www.yahoo.com - o https://www.google.com - o https://microsoft.com	To check and troubleshoot network issues. i NOTE: Enabling these endpoints is optional and only necessary if you have allowed PC users to use the SupportAssist user interface for troubleshooting network issues.
			https://cloud.blancco.com	To communicate the data erase progress. Access to this port is required only if you are using the remote Data Erase service.
			https://dotnet.microsoft.com/en-us/download/dotnet	To download the required .NET Desktop Runtime 10.0.x version.

Table 1. Ports, communication mode, protocol, and endpoints (continued)

Port	Communication mode	Protocol	Destination	Purpose
			https://coresvcs.amds.dell.com	To communicate with Dell to register device with secure Trusted Platform Module.
			Azure- - https://coresvcs.amds.dell.com (Required from SupportAssist 4.5.2 or higher versions.) - https://agent.api.astra.dell.com/ (Required from SupportAssist 4.5.2 or higher versions.)	For device registration and telemetry communication.
			DDC- https://csgdtm-svc-agent.dell.com/ (Required from SupportAssist 4.5.2 or higher versions.)	For event and blob intake.
			https://saupdates.dell.com (Required from SupportAssist 4.9 or higher versions.)	To download SupportAssist related files from Dell content delivery network.
			https://aka.ms (Required from SupportAssist 4.9 or higher versions.)	To download Microsoft windows app runtime.
9012 - 12012	localhost	WSS	localhost	For SupportAssist to communicate with the internal components in the end-user PC, using one of the available ports.
5700	localhost	HTTPS	localhost	For interprocess communication to open the SupportAssist user interface.
8883, 8884, 8885, or 8886	Inbound connection to and from the browser process running on the PC	HTTP	localhost	To communicate with Dell support website.
8883 and 443	Inbound and outbound secure connection to and from the destination MQTT	MQTT or HTTPS	*.azure-devices.net (Required from SupportAssist 4.5.2 or higher versions.) *.azure-devices-provisioning.net (Required from	To apply the latest changes made to SupportAssist preferences instantly and remotely optimize the PCs from TechDirect.

Table 1. Ports, communication mode, protocol, and endpoints (continued)

Port	Communication mode	Protocol	Destination	Purpose
			SupportAssist 4.5.2 or higher versions.)	○ To configure Central Resource Manager to retrieve BIOS passwords for PCs located outside the corporate network. ○ To run remediation scripts on the PCs.
5690	local host or over internet	HTTPS	local host or over internet.	To communicate with Dell support website.

NOTE: The SupportAssist installer does not explicitly modify folder permissions as part of its standard installation process. However, if the %ProgramData%\Dell directory has restricted access—due to environmental settings, group policies, or remnants from a previous uninstall—a manual or scripted adjustment of folder permissions may be required to allow the installation to complete successfully.

- **Gateway or firewall**—if the PC connects to the Internet through a proxy server and if you do not want to configure the proxy in system context mode, ensure that you configure the gateway or firewall to allow communication to the following destinations. These destinations validate certificates and securely connect the PCs to Dell.
 - <http://crl.entrust.net/level1k.crl>
 - <http://www.entrust.net/rpa>
 - <http://ocsp.entrust.net>
 - <http://aia.entrust.net/l1k-chain256.cer>
 - <http://crl3.digicert.com/DigiCertGlobalRootCA.crl>
 - <http://crl4.digicert.com/DigiCertGlobalRootCA.crl>
 - <http://ocsp.digicert.com>
 - <https://www.digicert.com/CPS>

NOTE: When configuring SSL encryption, ensure that traffic related to SupportAssist are excluded from decryption. Do not intercept or decrypt HTTPS traffic destined for Dell endpoints. Ensure that network, firewall and security settings allow direct HTTPS communication without SSL inspection for Dell endpoints.

Configure and connect SupportAssist downloaded from TechDirect

If you are deploying SupportAssist for the first time, you must download the Deployment Package Manager from the TechDirect dashboard. The Deployment Package Manager enables you to configure organization-specific settings and generate a customized SupportAssist deployment package. Once created, you can deploy the customized package across your fleet of managed PCs.

If SupportAssist is already deployed by other administrators on your PC fleet, you can add contact and shipping information, and configure any default SupportAssist preferences. See [Create a new deployment](#).

If you have already deployed SupportAssist on your PC fleet, you can manage deployments for your sites and sites that are created by other administrators, if permitted. You can also configure settings, download the Deployment Package Manager, or activate SupportAssist using an activation file. See [Manage deployment for an existing site](#).

Topics:

- [Create a new deployment](#)
- [Manage deployment for an existing site](#)
- [Managing SupportAssist preferences](#)
- [Create the SupportAssist deployment package](#)
- [Modify an existing SupportAssist deployment](#)
- [Deploy SupportAssist on the PC fleet](#)
- [Run the SupportAssist self-diagnosis test](#)
- [Configure and deploy SupportAssist on new PCs](#)
- [Install Central Resource Manager](#)
- [Updating SupportAssist for Business PCs and software add-ons](#)

Create a new deployment

Prerequisites

- Activate the Connect and manage service in TechDirect.
- Allow browser pop-ups from TechDirect.
- Sign in to TechDirect as a Connect and manage administrator.

About this task

If you are deploying, you must first download the deployment package manager from TechDirect and create a custom deployment package that you can deploy on your managed PCs.

After downloading the custom deployment package, you can add contact and shipping information and configure SupportAssist preferences.

Steps

1. From the [TechDirect](#) dashboard, go to **Connect and manage > Manage PC fleet**.
The **Manage PC fleet** page is displayed.
2. In the **Connect and manage PCs** card, click **MANAGE**.
The **Set up and connect with SupportAssist** page is displayed.
3. In the **Deployment Package Manager for SupportAssist** section, click **Download**.
The `SupportAssistDeploymentManager.zip` file is downloaded, and the **Deployment Instructions** page is displayed.

 **NOTE:** If you are unable to download the custom deployment package, clear the browser cookies and cache, and then retry.

 **NOTE:** All SupportAssist versions have end of support date. You can view the end of support date for your version from [Version and validity](#) and update to the latest version to ensure continued support.

4. In the **Add contact and shipping address** section, perform one of the following steps:
 - Click **Add new**, enter primary contact details, secondary contact details, shipping address, and then click **Save and next**.
 - Click **Choose from existing**, select the contact information and shipping address from the existing list, and click **Save**.

 **NOTE:** If the contact email addresses and the email address that is registered in TechDirect are the same, the preferred language is auto populated based on the TechDirect user profile language. If the email addresses are different, you can select the preferred language.

The contact and shipping information is saved. Dell Technical Support uses this information when SupportAssist automatically creates support request on your behalf and ship any replacement parts, when necessary.

5. In the **Preferences** section, if required, enable or disable the default [SupportAssist Preferences](#) and click **Save**.

 **NOTE:** The configuration is applied to the PCs within 30 minutes of establishing a connection with Dell.

Results

After you configure and deploy SupportAssist successfully on a PC, the first site and a **Default** group are created for your TechDirect account. You can create additional groups and organize your PCs within a site.

 **NOTE:** To create another site, sign in to TechDirect as another Connect and manage administrator, and then configure and deploy SupportAssist on the PC.

Next steps

[Create the SupportAssist deployment package.](#)

Manage deployment for an existing site

If you have already deployed SupportAssist on your PC fleet, you can manage deployments for your sites and sites that are created by other administrators, if permitted. You can also configure settings, download the Deployment Package Manager, or activate SupportAssist using an activation file.

Configure the existing deployment

About this task

You can update the contact and shipping details, and SupportAssist preferences in the configuration anytime. The updated configuration is applied to the PCs within 30 minutes of establishing a connection with Dell.

 **NOTE:** You do not have to redeploy SupportAssist when you modify the SupportAssist preferences in TechDirect.

Steps

1. From the [TechDirect](#) dashboard, go to **Connect and manage > Manage PC fleet**.
The **Manage PC fleet** page is displayed.
2. In the **Connect and manage PCs** card, click **MANAGE**.
3. Click **Set up and connect**.
4. Select **Manage deployment for an existing site**.
5. Select **Configure the existing deployment**.
The **Configure SupportAssist** page is displayed.
6. Select the site and group configuration.
7. In the **Add contact and shipping address** section, perform one of the following steps:
 - Click **Add new**, enter primary contact details, secondary contact details, shipping address, and then click **Save and next**.

- Click **Choose from existing**, select the contact information and shipping address from the existing list, and click **Save**.

NOTE: If the contact email addresses and the email address that is registered in TechDirect are the same, the preferred language is auto populated based on the TechDirect user profile language. If the email addresses are different, you can select the preferred language.

The contact and shipping information is saved. Dell Technical Support uses this information when SupportAssist automatically creates support request on your behalf and ship any replacement parts, when necessary.

8. In the **Preferences** section, if required, enable or disable the default [SupportAssist Preferences](#) and click **Save**.

NOTE: The configuration is applied to the PCs within 30 minutes of establishing a connection with Dell.

Download Deployment Package Manager

Prerequisites

Allow browser pop-ups from TechDirect.

About this task

If you have already deployed SupportAssist but you want to include software add-ons, configure proxy, and modify settings in your existing deployments, you can download the Deployment Package Manager and redeploy SupportAssist again. When a new version of SupportAssist is available, you can also manually update to the latest version using the Deployment Package Manager.

Steps

1. From the [TechDirect](#) dashboard, go to **Connect and manage > Manage PC fleet**.
The **Manage PC fleet** page is displayed.
 2. In the **Connect and manage PCs** card, click **MANAGE**.
 3. Click **Set up and connect**.
 4. Select **Manage deployment for an existing site**.
 5. Select **Download Deployment Package Manager**.
The **Download Deployment Package Manager** page is displayed.
 6. Select a site.
 7. In the **Deployment Package Manager for SupportAssist** section, click **Download**.
The SupportAssistDeploymentManager.zip file is downloaded, and the Deployment Instructions page is displayed.
- NOTE:** If you are unable to download the custom deployment package, clear the browser cookies and cache, and then retry.
- NOTE:** All SupportAssist versions have end of support date. You can view the expiry date for your version from [Version and validity](#) and update to the latest version to ensure continued support.
8. Create the SupportAssist deployment package using the Deployment Package Manager and deploy SupportAssist. See [Create the SupportAssist deployment package](#).

Download activation file

Prerequisites

Allow browser pop-ups from TechDirect.

About this task

Using the activation file, you can activate SupportAssist on your site or other sites by deploying SupportAssist. You can also create a SupportAssist deployment package by using the activation file in Deployment Package Manager. If your activation file is expired, missing, or invalid, you can download it anytime.

Steps

1. From the [TechDirect](#) dashboard, go to **Connect and manage > Manage PC fleet**.
The **Manage PC fleet** page is displayed.

2. In the **Connect and manage PCs** card, click **MANAGE**.
3. Click **Set up and connect**.
4. Select **Manage deployment for an existing site**.
5. Select **Download activation file**.
The **Download activation file** page is displayed.
6. Select a site.
7. In the **Activation file for SupportAssist** section, click **Download**.
8. Use the activation file in Deployment Package Manager to activate SupportAssist. See [Create the SupportAssist deployment package](#) or [Modify an existing SupportAssist deployment](#).

Managing SupportAssist preferences

SupportAssist enables you to perform automated and manual tasks on the target PCs. PC users can perform manual tasks only if the SupportAssist user interface is enabled. However, automated tasks are performed on the PCs even if the SupportAssist user interface is not enabled in preferences.

For information about using the SupportAssist user interface, see the *SupportAssist for Business PCs User's Guide* available on the [SupportAssist for Business PCs](#) documentation page.

 **NOTE:** The following options are configurable only if you have disabled the **Use default preferences** option.

General

Configure the following preferences for your PC fleet:

- **Auto update SupportAssist**—allows SupportAssist to automatically update to a later version.
- **Include software information in collected data**—allows Dell to collect information about installed applications, drivers, and operating system updates from your PCs.
- **Include identification information**—allows Dell to collect the identification information of a PC.

PC updates

To configure PC update settings, perform the following steps:

- Go to the **PC updates** section.
- Choose one of the following update options:
 1. Update manually from the Recommendations page allows you to choose and apply updates as they become available.
 2. Automated options to keep PC fleet's updates up to Dell-recommended versions.
- If you select **Automatically update**, SupportAssist installs only stable and verified driver updates with minimal user input.

 **NOTE:** Auto-update applies to SupportAssist version **4.9 or later**. PCs with valid warranties or entitlements are eligible. In a mixed environment, only PCs with version 4.9 or higher auto-update. Older versions require manual updates.

- To change your driver update preference from stable to the latest versions, toggle on the option labeled **Yes, install the most latest version of driver updates**.
- SupportAssist installs updates based on the selected preferences. By default, all options for importance, update type, and device category are selected. You can review and deselect any options you do not require.
- The types of updates included are BIOS updates, firmware updates, hardware drivers, utility software, application software (such as Dell Command | Power Manager), and all other relevant updates.
- Updates apply to a range of device categories, including audio, chipset, input devices (like mouse and keyboard), network and Bluetooth, storage devices (such as hard drives and CD/DVD drives), video, and all other components.
- In the **Additional preferences** section:
 - To restrict updates to a specific time range, check **Apply PC updates only within a time range** (optional), and set the time using the **From** and **To** dropdowns (default values are 00:00 Hrs to 23:00 Hrs).
- When a driver update requires a system restart to complete installation, SupportAssist displays a restart notification to the user. The notification informs the user that changes have been made to the PC by the IT administrator and a restart is required to complete the update.

The notification provides the following options:

Table 2. Options

Option	Description
Restart now	Restarts the system immediately to complete the update.
Remind me later	Defers the restart for 2 hours and dismisses the notification temporarily.

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.
- **Deferral Policy:**
 - **First notification** — The user can click **Remind me later** to defer the restart. The notification reappears after 2 hours.
 - **Second notification** — The user can click **Remind me later** to defer the restart a final time. The notification reappears after 2 hours.
 - **Third notification (final)** — The notification displays a 60-minute countdown timer. The deferral option is no longer available. The system performs a automatic restart when the countdown reaches zero.

 **NOTE:** You should save all open work before the countdown expires to prevent data loss. A maximum of two deferrals are permitted, allowing a total delay of up to 5 hours before the automatic restart is initiated.

Schedule scans and optimizations

Configure the following preferences to schedule scans and system optimization tasks that help manage the performance of managed PCs automatically:

- **Schedule your scans and optimizations**—allows SupportAssist to automatically scan your PCs to detect updates, hardware issues, and the required system optimizations.

 **NOTE:** The following options are configurable only if you have enabled the **Schedule your scans and optimizations** option.

- **Drivers & Downloads**—allows SupportAssist to perform the driver and downloads updates.
 - **Frequency**—select the frequency for SupportAssist to perform the drivers and downloads updates.
- **Hardware scans**—allows SupportAssist to perform the hardware scans.
 - **Frequency**—select the frequency for SupportAssist to perform the hardware scans.
- **Run system optimizations scans**—allows SupportAssist to optimize the PCs.
 - **Clean files**—allows SupportAssist to provide recommendations to optimize the PCs, by scanning and identifying the files that can be cleaned.
 - **Tune performance**—allows SupportAssist to provide recommendations to maximize the processing speed, by scanning and identifying the settings that can be adjusted on the PC.
 - **Optimize network**—allows SupportAssist to provide recommendations to maintain an efficient and reliable network, by scanning and identifying the network settings that can be updated on the PC.
 - **Remove viruses and malware**—allows SupportAssist to provide recommendations to optimize the PCs, by scanning and identifying the files infected by viruses and malware that can be removed from the PCs.

 **NOTE:** The virus and malware removal capability is:

- Available only for PCs with an active ProSupport Plus or ProSupport Flex for Client service plan.
- Not available in certain regions, for example, China.

- **Frequency**—select the frequency for SupportAssist to perform the system optimizations.

- **Automatic system optimizations**—allows SupportAssist to perform automatic software optimizations.

 **NOTE:** Auto-optimizations are applicable only for PCs with an active ProSupport Plus or ProSupport Flex for Client service plan.

- **Time range (Optional)**—select the time range for SupportAssist to perform the scans.
- **Run scans in background**—allows SupportAssist initiated schedule scans to run in the background without the need for end user interaction.

User interaction

Configure the following preferences to enable PC users to view and modify SupportAssist, and perform software optimizations manually:

- **Do not allow users to open and run SupportAssist on their PCs**—disables PC users to view and use the SupportAssist user interface.
- **Allow users with admin user rights**—enables PC users with administrator rights to view and use the SupportAssist user interface.
 - **Driver updates**—enables PC users with full or temporary administrator rights to update drivers. The term driver refers to drivers, firmware, BIOS, and Dell software application updates.

 **NOTE:** For PCs running SupportAssist 4.5.2 or higher version, you can configure the type of PC updates end users can install on their PCs based on Importance, Update type and Device category.

- **Hardware scans**—enables PC users with administrator rights to scan the PC hardware to check for and detect any hardware issues.
- **Boost performance**—enables PC users with administrator rights to improve PC fleet performance by removing unwanted files and registry entries, fine-tuning system features, and optimizing power settings and memory allocation.
- **Optimize network**—enables PC users with administrator rights to optimize network connectivity by adjusting the settings to have an efficient and reliable network.
- **Remove viruses & malware**—enables PC users with administrator rights to isolate, remove, and restore files that are corrupted by viruses and malware to keep the PC secure.
- **Display system notifications**—allows SupportAssist to display notifications about hardware and software issues, driver updates, support requests, and other alerts for the PC.

 **NOTE:** Ensure that you have enabled Windows **Notifications** in the **Notifications & action settings > System > Notifications** section.

Create the SupportAssist deployment package

Prerequisites

Configure and download the SupportAssist executable file from [TechDirect](#).

Steps

1. Go to the directory where you downloaded the Deployment Package Manager file from TechDirect, and then extract the files.
2. Double-click `SupportAssistDeploymentManager.exe` to launch the **Deployment Package Manager** wizard.
3. On the **Welcome** page, click **Next**.
The **Activation** page is displayed.

 **NOTE:** If a network connection is unavailable, an error message is displayed. To proceed with creating the deployment package, you can either connect to a network or enter the proxy details.
4. By default, the activation file is validated for a site. To activate a different site, perform the following steps:
 - a. From the [TechDirect](#) dashboard, go to **Connect and manage > Manage PC Fleet > Setup and connect > Download**.
 - b. Select the site and download the activation file.
 - c. Import the activation file in Deployment Package Manager and click **Validate activation file**.
The **Deployment Mode** page is displayed.

5. Choose one of the following option to create a SupportAssist package on your needs:

- **Install, upgrade or configure (EXE)**- Choose this option to install, upgrade, or configure and manage SupportAssist via Techdirect.
- **Install or upgrade (MSI)**- Choose this option to install or upgrade, SupportAssist (version 4.9.x and above) and manage it via Techdirect.
- **Configure or modify**- Choose this option to configure and manage SupportAssist via techdirect or modify existing settings.

NOTE: If optional group name is entered, only new PCs that are registering to TechDirect will be part of the group. Existing PCs that are upgrading to the latest version will not be part of the group.

a. If you choose **Install, upgrade or configure (EXE)**, perform the following steps to create an MSI Windows installer package:

- Choose the system type as **x64** or **Arm64**. You can choose one or both depending on the systems in your environment.
- Enter a deployment key to generate an encrypted deployment package.

NOTE: The deployment key is similar to a password that you must create for encrypting the deployment package. You must use the same deployment key while deploying SupportAssist on your PCs. The same deployment key can also be used to create multiple deployment packages.

NOTE: Ensure that you enter a key between four and ten characters that contain alphabets, numbers, and one of these special characters # & \$.

- To organize your PCs under specific groups in TechDirect, select **Organize your PCs in a group**, and enter the group name.

NOTE: The group configuration is applied to the PCs within 60 minutes after they connect to Dell.

b. If you choose **Install or upgrade (MSI)**, perform the following steps:

- Choose the system type as **x64** or **Arm64**. You can choose one or both depending on the systems in your environment.
- Enter a deployment key to generate an encrypted deployment package.

NOTE: The deployment key is similar to a password that you must create for encrypting the deployment package. You must use the same deployment key while deploying SupportAssist on your PCs. The same deployment key can also be used to create multiple deployment packages.

NOTE: Ensure that you enter a key between four and ten characters that contain alphabets, numbers, and one of these special characters # & \$.

c. If you choose **Configure or modify (MSI)**, perform the following steps:

- Enter a deployment key to generate an encrypted deployment package.

NOTE: The deployment key is similar to a password that you must create for encrypting the deployment package. You must use the same deployment key while deploying SupportAssist on your PCs. The same deployment key can also be used to create multiple deployment packages.

NOTE: Ensure that you enter a key between four and ten characters that contain alphabets, numbers, and one of these special characters # & \$.

6. Click **Next**.

The **Software add-ons** page is displayed.

7. Select your preferences for the following software add-ons and click **Next**:

- **Central Resource Manager**—enables you to store BIOS administrator passwords for your PC fleet. SupportAssist uses the stored passwords to install BIOS updates on BIOS password-configured PCs. If you chose to download Central Resource Manager, perform the following steps:

a. Enter the numeric seed value.

The seed value is used for encrypting the BIOS passwords. You can use the same seed value to reinstall the Central Resource Manager without redeploying SupportAssist.

- b. Enter the IP address, hostname, or fully qualified domain name (FQDN) of the system on which the Central Resource Manager is installed.

 **NOTE:** All Central Manager Resource versions have end of support date. You can view the expiry date for your version from [Version and validity](#) and update to the latest version to ensure continued support.

- **Dell Trusted Device**—a security agent that provides the security information for the connected PCs and enables you to verify the integrity of components in your PCs. For more information, see the *SupportAssist Administrator Guide* available on the [SupportAssist documentation](#) page or see the Trusted Device manuals available on the [Dell Trusted Device documentation](#) page.

The **Proxy** page is displayed.

8. If the PCs and the system on which the Central Resource Manager is installed, connects to the Internet through a proxy server, perform the following steps:

- a. Select **Connect to the internet through a proxy** and enter the address and port number.
- b. If the proxy server requires authentication, select **This proxy requires authentication**, and enter the username and password.

 **NOTE:** For proxy server authentication, it is recommended to use the username and password of a service account without an expiration date.

- c. Select **Allow other Dell applications to use these proxy details**.

Once selected, SupportAssist shares proxy details with other Dell applications running on the same PC.

- d. In the **Server certification validation** section, select one of the following options:

After deployment, SupportAssist validates the server certificates from remote servers, and verifies the certificate chain and certificate revocation status. If the certificate chain verification check fails, SupportAssist will not communicate with Dell, rendering it non-operational.

- **Perform check**—SupportAssist performs the certificate revocation check and is operational only when the check has passed. If the check fails, SupportAssist is non-operational.
- **Skip check and continue**—SupportAssist performs the certificate revocation check, and continues to be operational even if the revocation check fails.

- e. Click **Next**.

The **Output** page is displayed.

9. Perform the following steps:

- a. Select one of the preferred file formats for deployment—**Windows Installer Setup Transform (MST)** or **Administrative Template Files (ADMX/ADML)**.
- b. Browse and select the folder where you want to extract the deployment package.
- c. Click **Generate output**.

Results

The SupportAssist deployment package is generated and downloaded to the selected folder. You can review the `SupportAssistDeploymentInstructions.txt` to proceed with deploying SupportAssist.

Next steps

1. Verify the [Prerequisites to deploy SupportAssist](#).
2. [Deploy SupportAssist on the PC fleet](#).
3. Optional: [Install Central Resource Manager](#).

Modify an existing SupportAssist deployment

Steps

1. Go to the directory where you downloaded the Deployment Package Manager file from TechDirect, and then extract the files.
2. Double-click `SupportAssistDeploymentManager.exe` to launch the **Deployment Package Manager** wizard.
3. On the **Welcome** page, click **Next**.

The **Activation** page is displayed.

NOTE: If a network connection is unavailable, an error message is displayed. To proceed with creating the deployment package, you can either connect to a network or enter the proxy details.

4. By default, the activation file is validated for a site. To activate a different site, perform the following steps:
 - a. From the [TechDirect](#) dashboard, go to **Connect and manage > Manage PC Fleet > Setup and connect > Download**.
 - b. Select the site and download the activation file.
 - c. Import the activation file in Deployment Package Manager and click **Validate activation file**.

The **Deployment Mode** page is displayed.

5. To modify the existing settings, optionally install any software add-ons, and configure the proxy, select **Configure or modify (MSI)** and perform the following steps:
 - a. To generate an encrypted deployment package, enter a key for encryption

The deployment key is similar to a password that you must create for encrypting the deployment package. You must use the same deployment key while deploying SupportAssist on your PCs. The same deployment key can also be used to create multiple deployment packages.

NOTE: Ensure that you enter a key between four and ten characters that contain alphabets, numbers, and one of these special characters # & \$.

- b. Click **Next**.

The **Software add-ons** page is displayed.

6. Select your preferences for the following software add-ons and click **Next**:
 - **Central Resource Manager**—enables you to store BIOS administrator passwords for your PC fleet. SupportAssist uses the stored passwords to install BIOS updates on BIOS password-configured PCs. If you chose to download Central Resource Manager, perform the following steps:
 - a. Enter the numeric seed value.

The seed value is used for encrypting the BIOS passwords. You can use the same seed value to reinstall the Central Resource Manager without redeploying SupportAssist.

 - b. Enter the IP address, hostname, or fully qualified domain name (FQDN) of the system on which the Central Resource Manager is installed.

NOTE: All Central Manager Resource versions have end of support date. You can view the expiry date for your version from [Version and validity](#) and update to the latest version to ensure continued support.

- **Dell Trusted Device**—a security agent that provides the security information for the connected PCs and enables you to verify the integrity of components in your PCs. For more information, see the *SupportAssist Administrator Guide* available on the [SupportAssist documentation](#) page or see the Trusted Device manuals available on the [Dell Trusted Device documentation](#) page.

The **Proxy** page is displayed.

7. If the PCs and the system on which the Central Resource Manager is installed, connects to the Internet through a proxy server, perform the following steps:
 - a. Select **Connect to the internet through a proxy** and enter the address and port number.
 - b. If the proxy server requires authentication, select **This proxy requires authentication**, and enter the username and password.

NOTE: For proxy server authentication, it is recommended to use the username and password of a service account without an expiration date.

 - c. Select **Allow other Dell applications to use these proxy details**.
Once selected, SupportAssist shares proxy details with other Dell applications running on the same PC.
 - d. In the **Server certification validation** section, select one of the following options:

After deployment, SupportAssist validates the server certificates from remote servers, and verifies the certificate chain and certificate revocation status. If the certificate chain verification check fails, SupportAssist will not communicate with Dell, rendering it non-operational.

 - **Perform check**—SupportAssist performs the certificate revocation check and is operational only when the check has passed. If the check fails, SupportAssist is non-operational.
 - **Skip check and continue**—SupportAssist performs the certificate revocation check, and continues to be operational even if the revocation check fails.
 - e. Click **Next**.

The **Output** page is displayed.

8. Perform the following steps:
 - a. Select one of the preferred file formats for deployment—**Windows Installer Setup Transform (MST)** or **Administrative Template Files (ADMX/ADML)**.
 - b. Browse and select the folder where you want to extract the deployment package.
 - c. Click **Generate output**.

Results

The SupportAssist deployment package is generated and downloaded to the selected folder. You can review the `SupportAssistDeploymentInstructions.txt` to proceed with deploying SupportAssist.

Next steps

1. [Deploy SupportAssist on the PC fleet](#).
2. Optional: [Install Central Resource Manager](#).

Deploy SupportAssist on the PC fleet

Prerequisites

- [Create the SupportAssist deployment package](#).
- The PCs must meet the [Prerequisites to deploy SupportAssist](#).
- If the PCs connect to the Internet through a proxy server, ensure that you verify if the proxy is configured in system context mode, and if the Dell server certificate revocation check is successful. For more information about how to perform the verifications, see the *SupportAssist for Business PCs Frequently Asked Questions* available on the [SupportAssist for Business PCs documentation](#) page.
- Ensure the latest version of .NET Desktop Runtime 10.0.x is installed on the PCs.
- Verify the validity of the SupportAssist version. See [Version and validity](#).
- To install Dell Trusted Device:
 - Ensure that the required ports are open. For more information, see the *Ports* section in the Trusted Device manuals available on the [Dell Trusted Device](#) documentation page.

About this task

You can complete the SupportAssist deployment on PCs using one of the following methods:

- Deploy SupportAssist, and complete the configuration and activation together using a deployment tool of your choice, such as Microsoft System Center Configuration Manager (SCCM), or Microsoft Intune.
- Install SupportAssist without configurations as part of the corporate Windows image using a deployment tool of your choice, such as Microsoft System Center Configuration Manager (SCCM), or Microsoft Intune. You can independently configure and activate SupportAssist later using the activation file through generated administrative template file.

Steps

1. To deploy .Net Desktop Runtime, run the "`<path_of_the_DotNetDesktopRuntime.exe_file>\windowsdesktop-runtime-10.0.x-win-x64/Arm64.exe`" `/install /quiet /norestart` command.
The installer returns an exit code of 0 for success and an exit code of 3010 to indicate that a restart is required. Values other than zero and 3010 indicate an error.
2. Deploy SupportAssist on the PCs using one of the following commands depending on the file formats:

Table 3. Commands to deploy SupportAssist

Deployment file format and package format	Command	Deployment note
Windows installer 64-bit (.MSI) and Windows Installer Setup Transform (MST)	If you are creating a new SupportAssist deployment — <code>msiexec /i "[SupportAssist msi file path]\SupportAssistInstaller-x64.msi"</code>	To deploy SupportAssist, you must use the Windows Installer Setup Transform (MST) file that you created for the SupportAssist version you are deploying on the PC fleet. Do not use the MST files created for

Table 3. Commands to deploy SupportAssist (continued)

Deployment file format and package format	Command	Deployment note
	<pre>ADDLOCAL="BASE,CORE,FULL,SOF TWARE,DTM,HWDIAGS,RAAS" TRANSFORMS="[mst file path] \SupportAssistConfiguration. mst" DEPLOYMENTKEY="Uat123\$" SOURCE=TechDirect / norestart /qn /l+ "[msi log path]\SupportAssistMsi.log"</pre> If you are activating preinstalled SupportAssist or modifying an existing SupportAssist deployment— <pre>msiexec /i "[SupportAssist config msi file path] \SupportAssistConfigurator- x64.msi" TRANSFORMS="[mst file path] \SupportAssistConfiguration. mst" DEPLOYMENTKEY="[Deployment_K ey]" /norestart /qn /l+ "[msi log path] \SupportAssistConfigMsi.log"</pre> If you are upgrading SupportAssist to latest version— [SupportAssist for Business PCs Upgrade EXE file path] <pre>\SupportAssistDeployment_x64 .exe TRANSFORMS="[mst file path] \SupportAssistConfiguration. mst" DEPLOYMENTKEY="[Deployment_K ey]" SOURCE=TechDirect</pre>	other SupportAssist versions. Also, do not change any values in ADDLOCAL and SOURCE command line arguments, and all the provided options must be provided completely without alteration.
Windows installer 64-bit (.MSI) and Administrative Template Files (ADMX/ADML)	<pre>msiexec /i "[path_of_the_SupportAssist. msi_file] \SupportAssistInstaller- x64.msi" /norestart /qn /l+ "[path_to_save_the_msi_log_f ile]\SupportAssistMsi.log"</pre> NOTE: You must Activate SupportAssist using Administrative Template Files (.adm/.adml) to complete the SupportAssist deployment.	To deploy SupportAssist, you must use the Administrative Template Files (ADMX/ADML) file that you created for the SupportAssist version you are deploying on the PC fleet. Do not use the ADMX/ADML files created for other SupportAssist versions.
Windows executable 64-bit (.EXE) and Administrative Template Files (ADMX/ADML)	<pre>"[path_of_the_SupportAssist. exe_file] \SupportAssistInstaller- x64.exe"</pre> NOTE: You must Activate SupportAssist using Administrative Template Files (.adm/.adml) to complete the SupportAssist deployment.	To deploy SupportAssist, you must use the Administrative Template Files (ADMX/ADML) file that you created for the SupportAssist version you are deploying on the PC fleet. Do not use the ADMX/ADML files created for other SupportAssist versions.



NOTE: You must ensure that you provide the same deployment key that you entered while creating the deployment package.

- If you have included the Dell Trusted Device software add-on while creating the SupportAssist deployment package, run the `msiexec /i "[path_of_DellTrustedDevice.msi_file]\DellTrustedDevice-<version>.msi" /qn /norestart /l+ "[path_to_save_the_msi_log_file]\DtdMsi.log` command to deploy the security agent.

Results

SupportAssist is deployed on the PCs, and you can start managing and optimizing the PCs in TechDirect.



NOTE: The installation time varies depending on the network bandwidth and PC performance.

The following return codes may appear after upgrading SupportAssist to the latest version

Table 4. Status codes

Status code	Description	Action
0	The SupportAssist installation or upgrade completes successfully.	No action required.
1	The same or a newer version of SupportAssist is already installed on the system.	No action required.
2	An exception or unhandled error occurs during the SupportAssist installation or upgrade.	Retry the installation. If the issue persists, contact the Dell SupportAssist team.
3	A restart is required after uninstalling the older version of SupportAssist.	Instruct the end user to restart the system. The Task Scheduler resumes the installation automatically after reboot.
4	The SupportAssist installation fails.	Retry the installation. If unsuccessful, contact the Dell SupportAssist team.
5	Another instance of the deployment executable is already running.	No action required. Wait for the existing process to complete.
6	Task Scheduler creation fails. The Task Scheduler is necessary to retry installation in case of failure.	Retry the installation. If it continues to fail, contact the Dell SupportAssist team.
7	Backup of the SupportAssist database or essential folders fails during the upgrade. The upgrade process is aborted.	Retry the installation. If the issue persists, contact the Dell SupportAssist team.
8	The MSI installation file is missing or invalid.	Create a new deployment package and redeploy. If the issue remains, contact the Dell SupportAssist team.
9	The .NET framework installation fails.	Create a new deployment package and redeploy. If the issue persists, contact the Dell SupportAssist team.
10	Certificate validation fails for extracted resources.	Create a new deployment package and redeploy. If the issue persists, contact the Dell SupportAssist team.
11	A system restart is required after .NET installation.	Instruct the end user to restart the system. The Task Scheduler resumes the installation automatically after reboot.
12	The required .NET file is missing from the deployment package.	Create a new deployment package and redeploy. If the issue persists, contact the Dell SupportAssist team.

Table 4. Status codes (continued)

Status code	Description	Action
13	Extraction of embedded resources fails or the resources are missing.	Create a new deployment package and redeploy. If the issue persists, contact the Dell SupportAssist team.
14	The SupportAssist Config.MSI file is missing or corrupted.	Create a new deployment package and redeploy. If the issue persists, contact the Dell SupportAssist team.
15	The platform is not supported. Manufacturer or OEM may not be Dell or Alienware.	Ensure that deployment targets only supported platforms (Dell or Alienware systems).

After deploying SupportAssist successfully and registering your PCs with TechDirect, you can modify the SupportAssist configuration in TechDirect. The settings are automatically applied to the PCs when they connect to Dell. However, to modify an existing SupportAssist deployment, such as, proxy settings, you must manually update and deploy SupportAssist again. See [Modify an existing SupportAssist deployment](#).

 **NOTE:** SupportAssist is not supported on Federal Information Processing Standard (FIPS) enabled PCs.

For information about managing your PCs, see the *SupportAssist for Business PCs Administrator Guide* available on the [SupportAssist for Business PCs](#) documentation page.

Run the SupportAssist self-diagnosis test

Prerequisites

- The PC must have Internet connectivity.
- You must have administrator rights on the PC.
- Ensure that SupportAssist is deployed on the PCs. See [Deploy SupportAssist on the PC fleet](#).

About this task

For SupportAssist to function normally and as expected, SupportAssist must be connected to Dell. Run the self-diagnosis test on any of the PCs after deployment to determine if SupportAssist is successfully connected to Dell and is working as expected. You can also run the self-diagnosis test to verify if the system on which the Central Resource Manager is installed is accessible by SupportAssist.

Steps

1. Access the PC on which you want to perform the self-diagnosis test.
2. Click **Start** to open the **Programs** menu.
3. Find **Command Prompt** and click **Run as administrator**.
The **Command Prompt** window is displayed.
4. Change the directory to `\Program Files\DELL\SupportAssistAgent\bin`.
5. Type `SelfDiagnosis.exe` and press Enter.

Depending on the test result, one of the following messages is displayed for every test:

- **Available** or **Reachable**—SupportAssist is successfully connected to Dell and is working as expected.
- **Unavailable**—SupportAssist is not connected to Dell or is not working as expected. Perform one of the following steps:
 - Reboot the PC and retry performing the self-diagnosis test again.
 - Check the proxy, firewall, and network configurations in your environment, and retry performing the self-diagnosis test.

After performing the self-diagnosis tests, contact the technical support for assistance if:

- SupportAssist is not connected to Dell or is not working as expected.
- The system on which the Central Resource Manager is installed is not accessible by SupportAssist.

Configure and deploy SupportAssist on new PCs

To deploy SupportAssist on newer PCs or on PCs not running SupportAssist, use one of the following methods:

- Use a previously generated SupportAssist package created by other administrators using the Deployment Package Manager and deploy SupportAssist on the PCs. These PCs are added to the existing site as per the configurations in the SupportAssist package.
- Create a new site and then configure and deploy SupportAssist using the newly downloaded SupportAssist package. These PCs are added to the newly created site. To create a new site, sign in to TechDirect as another Connect and manage administrator who has never downloaded SupportAssist, and then configure and download SupportAssist.

Install Central Resource Manager

Prerequisites

- Ensure that a valid version of SupportAssist is installed on your PC fleet. See [Version and validity](#).
- [Create the SupportAssist deployment package](#).
- Ensure that Microsoft .NET Desktop Runtime version 10.0.x is installed on the system on which the Central Resource Manager is installed.
- Ensure that Transport Layer Security (TLS) version 1.2 is enabled on the system on which the Central Resource Manager is installed.
- Ensure that port 5690 is open on the system on which the Central Resource Manager is installed.
- Ensure that the <https://sacommercial.apis.dell.com> and <https://saservices.dell.com> destinations are open to register Central Resource Manager with TechDirect.
- To retrieve the BIOS administrator passwords, the PC fleet must be able to communicate with the system on which the Central Resource Manager is installed.
- A highly available system running the Windows operating system for successful BIOS updates. The system can be a server, virtual machine, desktop, and so on.
- Verify the validity of the Central Resource Manager version. See [Version and validity](#).

About this task

If you have included the Central Resource Manager while creating the SupportAssist deployment package, you can install the Central Resource Manager on a system running the Windows operating system. The Central Resource Manager stores BIOS administrator passwords that SupportAssist can use to install BIOS updates on your PC fleet.

After you install Central Resource Manager, you can either use a default password for BIOS updates or import the passwords using a spreadsheet.

You can install multiple Central Resource Manager instances in your PC fleet as required. However, only one Central Resource Manager instance can be externally accessible without a corporate network or VPN connection. For PCs that are outside the corporate network, not connected through VPN, or switching between corporate and external networks, ensure that you allow the PCs to access and retrieve BIOS password information over external networks. To enable the external network access, install and open Central Resource Manager, go to **Home > Settings**, and enable **Allow access** in the **External network access** section.

 **NOTE:** Central Resource Manager does not support ARM64 architecture.

Steps

1. Search for **Command Prompt** and click **Run as administrator**.
2. Type `msiexec /i "[CentralResourceManager.msi file path]\SupportAssistCentralResourceManager.msi" TRANSFORMS="[mst file path]\SupportAssistConfiguration.mst" DEPLOYMENTKEY="[deploymentKey]" /norestart /qn /l+ "[msi log path]\CrmMsi.log"` and press **Enter**.

 **NOTE:** You must ensure the seed value matches the one used in both SupportAssist and Central Resource Manager.

Results

The Central Resource Manager is installed on the system.

To verify if the PC fleet is communicating with the system on which the Central Resource Manager is installed, [Run the SupportAssist self-diagnosis test](#).

Next steps

Open Central Resource Manager as an administrator and use the following options to store the BIOS administrator passwords for your PC fleet:

- **Store default password**—if you have a common BIOS administrator password for most or all your PCs.
- **Store passwords via spreadsheet**—if you have different BIOS administrator passwords for each PC.

To store passwords using the spreadsheet, perform the following steps:

1. From the [TechDirect](#) dashboard, go to **Connect and manage > Manage PC fleet > Connect and manage PCs > Manage > PCs > Inventory**.
2. From the **Export** list, select **Central Resource Manager List**.
3. In the downloaded spreadsheet, enter the BIOS administrator passwords for each PC.
4. Import the spreadsheet in the Central Resource Manager.

NOTE:

- You can only enter the BIOS administrator passwords in the spreadsheet. Updates to other fields in the spreadsheet are not supported.
- The Central Resource Manager only stores the list of PCs and the associated BIOS administrator passwords that were last imported. Any previously stored information is not retained.
- When you update the BIOS administrator passwords for your PC fleet, you must also update the passwords in the Central Resource Manager.

Updating SupportAssist for Business PCs and software add-ons

SupportAssist for Business PCs

Updating SupportAssist ensures that the latest SupportAssist features are available on your PC. If you have opted to automatically update SupportAssist, SupportAssist automatically updates to the latest available version.

To manually update SupportAssist, download the Deployment Package Manager executable file from TechDirect and use any deployment tool to deploy SupportAssist.

After you download the Deployment Package Manager executable file, run the executable file to create the deployment package for the latest SupportAssist version which can be deployed on the PC fleet. See [Create the SupportAssist deployment package](#) and [Deploy SupportAssist on the PC fleet](#).

 **NOTE:** The update time varies depending on the network bandwidth and PC performance.

 **NOTE:** If SupportAssist has expired on your PC, you must manually update to the latest version. Automatic updates are not supported on expired versions. See [Version and validity](#).

 **NOTE:** SupportAssist updates are not available for PCs running the following operating systems—Windows 10, Windows 8.1, Windows 8, and Windows 7. To avail the full benefits of SupportAssist, it is recommended that you install SupportAssist on PCs running Windows 11.

Central Resource Manager

Updating Central Resource Manager ensures that the latest features are available to you. If you are running Central Resource Manager version 3.5 or later, it is automatically updated to the upcoming versions, by default.

To manually update Central Resource Manager when the latest version is available, open the **Central Resource Manager** application on your system and update to the next version from the **Settings** page or the **Home** page. Alternatively, you can

also select the **Central Resource Manager** software add-on in the Deployment Package Manager, download the deployment package, and manually install **Central Resource Manager**.

Dell Trusted Device

The Dell Trusted Device security agent is not automatically updated. You must manually download and update to the latest version when available. To download the latest version, select the **Dell Trusted Device** software add-on in the Deployment Package Manager, download the deployment package, and manually deploy it.

Deploy SupportAssist using Dell Management Portal and through Microsoft Intune

Prerequisites

- Ensure the .NET Desktop Runtime is pre-installed on all target devices.
- The PCs must meet the [Prerequisites to deploy SupportAssist](#).

Steps

1. Login to [Dell Management Portal](#) using your Microsoft Entra ID credentials which should be same as your MS Intune portal credentials.
2. In the **Apps** section of the Dell Management Portal, select **Dell SupportAssist**.
3. Choose **Dell SupportAssist** and publish it to your **Microsoft Intune** instance.
4. After publishing, confirm that Dell SupportAssist is available in **Windows application** section within your Intune environment for deployment.
5. Deploy SupportAssist to required PC fleet using Intune security groups.
6. Login to TechDirect and download the Deployment Package Manager and generate configuration ADMX/ADML file for your Techdirect tenant.
7. Upload the ADMX/ADML file in your intune instance for SupportAssist application to ensure PCs running SupportAssist are able to connect to TechDirect.
8. Create a device configuration policy using the imported ADMX files and assign it to the required PCs in the security group.

Configure and connect SupportAssist installed through other Dell sources

SupportAssist is also available through the following sources apart from TechDirect:

- Ready Image—a clean simple image with no added software. You can include SupportAssist for Business PCs while purchasing the Ready Image solution.
- SupportAssist page—manually download the latest version of SupportAssist from the [Connect to SupportAssist for Business PCs in TechDirect](#) page.
- Intune Enterprise App Catalog—deploy SupportAssist for Business PCs to your PC fleet directly from Intune Enterprise App Catalog.

If you have included SupportAssist version in your Ready Image, or manually obtained the latest version of SupportAssist from the [Connect to SupportAssist for Business PCs in TechDirect](#) page, you must configure SupportAssist to start managing your PC in TechDirect.

1. Create the deployment package to apply the configuration on preinstalled SupportAssist versions and connect SupportAssist to TechDirect:
 - a. Download the Deployment Package Manager.
 - b. In Deployment Package Manager Wizard, For Deployment mode select **Configure or Modify (MSI)** on an existing SupportAssist Deployment option and generate a new SupportAssist Deployment package to deploy in your PC fleet.
2. In TechDirect, Connect and manage, under Setup and connect, configure SupportAssist preferences:
 - a. Enter contact information and shipping details.
 - b. Configure SupportAssist preferences.

Topics:

- [Download the SupportAssist Deployment Package Manager](#)
- [Generate the SupportAssist deployment package](#)

Download the SupportAssist Deployment Package Manager

Prerequisites

- You must have a TechDirect account.
- You must have enabled browser pop-ups from TechDirect.
- You must be signed in to TechDirect as a Connect and manage administrator.

About this task

If you are deploying SupportAssist for the first time, you must first download the deployment package manager from TechDirect and create a custom deployment package that you can deploy on your managed PCs.

After downloading the custom deployment package, you can add contact and shipping information and configure SupportAssist preferences.

Steps

1. From the [TechDirect](#) dashboard, go to **Connect and manage > Manage PC fleet**. The **Manage PC fleet** page is displayed.
2. In the **Connect and manage PCs** card, click **MANAGE**. The **Set up and connect with SupportAssist** page is displayed.
3. In the **Deployment Package Manager for SupportAssist** section, click **Download**.

The `SupportAssistDeploymentManager.zip` file is downloaded, and the **Deployment Instructions** page is displayed.

NOTE: If you are unable to download the deployment package manager, clear the browser cookies and cache, and then retry.

NOTE: All SupportAssist versions have expiry dates. You can view the expiry date for your version from [Version and validity](#) and update to the latest version to ensure continued support.

4. Create the custom deployment package using deployment package manager and deploy SupportAssist. See [Create the SupportAssist deployment package](#).
 5. In the **Add contact and shipping address** section, perform one of the following steps:
 - Click **Add new**, enter primary contact details, secondary contact details, shipping address, and then click **Save and next**.
 - Click **Choose from existing**, select the contact information and shipping address from the existing list, and click **Save**.
- NOTE:** If the contact email addresses and the email address that is registered in TechDirect are the same, the preferred language is auto populated based on the TechDirect user profile language. If the email addresses are different, you can select the preferred language.

The contact and shipping information is saved. Dell Technical Support uses this information to create support requests on your behalf and ship any necessary replacement parts, when necessary.

6. In the **Preferences** section, if required, enable or disable the default [SupportAssist Preferences](#) and click **Save**.

NOTE: The configuration is applied to the PCs within 30 minutes of establishing a connection with Dell.

Next steps

[Generate the SupportAssist deployment package](#).

Generate the SupportAssist deployment package

Prerequisites

The PC must meet the [Prerequisites to deploy SupportAssist](#).

Steps

1. Go to the directory where you downloaded the Deployment Package Manager file from TechDirect, and then extract the files.
2. Double-click `SupportAssistDeploymentManager.exe` to launch the **Deployment Package Manager** wizard.
3. On the **Welcome** page, click **Next**.
The **Activation** page is displayed.

NOTE: If a network connection is unavailable, an error message is displayed. To proceed with creating the deployment package, you can either connect to a network or enter the proxy details.
4. By default, the activation file is validated for a site. To activate a different site, perform the following steps:
 - a. From the [TechDirect](#) dashboard, go to **Connect and manage > Manage PC Fleet > Setup and connect > Download**.
 - b. Select the site and download the activation file.
 - c. Import the activation file in Deployment Package Manager and click **Validate activation file**.The **Deployment Mode** page is displayed.
5. To configure the SupportAssist version installed through other sources, optionally install any software add-ons, and configure the proxy, select **Install or upgrade (MSI)** and click **Next**.
 - a. Enter a deployment key to generate an encrypted deployment package.

The deployment key is similar to a password that you must create for encrypting the deployment package. You must use the same deployment key while deploying SupportAssist on your PCs. The same deployment key can also be used to create multiple deployment packages.

NOTE: Ensure that you enter a key between four and ten characters that contain alphabets, numbers, and one of these special characters # & \$.
 - b. Click **Next**.

The **Software add-ons** page is displayed.

6. Select your preferences for the following software add-ons and click **Next**:
 - **Central Resource Manager**—enables you to store BIOS administrator passwords for your PC fleet. SupportAssist uses the stored passwords to install BIOS updates on BIOS password-configured PCs. If you chose to download Central Resource Manager, perform the following steps:
 - a. Enter the numeric seed value.

The seed value is used for encrypting the BIOS passwords. You can use the same seed value to reinstall the Central Resource Manager without redeploying SupportAssist.
 - b. Enter the IP address, hostname, or fully qualified domain name (FQDN) of the system on which the Central Resource Manager is installed.

 **NOTE:** All Central Manager Resource versions have end of support date. You can view the expiry date for your version from [Version and validity](#) and update to the latest version to ensure continued support.

- **Dell Trusted Device**—a security agent that provides the security information for the connected PCs and enables you to verify the integrity of components in your PCs. For more information, see the *SupportAssist Administrator Guide* available on the [SupportAssist documentation](#) page or see the Trusted Device manuals available on the [Dell Trusted Device documentation](#) page.

The **Proxy** page is displayed.

7. If the PCs and the system on which the Central Resource Manager is installed, connects to the Internet through a proxy server, perform the following steps:
 - a. Select **Connect to the internet through a proxy** and enter the address and port number.
 - b. If the proxy server requires authentication, select **This proxy requires authentication**, and enter the username and password.

 **NOTE:** For proxy server authentication, it is recommended to use the username and password of a service account without an expiration date.
 - c. Select **Allow other Dell applications to use these proxy details**.

Once selected, SupportAssist shares proxy details with other Dell applications running on the same PC.
 - d. In the **Server certification validation** section, select one of the following options:

After deployment, SupportAssist validates the server certificates from remote servers, and verifies the certificate chain and certificate revocation status. If the certificate chain verification check fails, SupportAssist will not communicate with Dell, rendering it non-operational.

 - **Perform check**—SupportAssist performs the certificate revocation check and is operational only when the check has passed. If the check fails, SupportAssist is non-operational.
 - **Skip check and continue**—SupportAssist performs the certificate revocation check, and continues to be operational even if the revocation check fails.
 - e. Click **Next**.

The **Output** page is displayed.

8. Perform the following steps:
 - a. Select one of the preferred file formats for deployment—**Windows Installer Setup Transform (MST)** or **Administrative Template Files (ADMX/ADML)**.
 - b. Browse and select the folder where you want to extract the deployment package.
 - c. Click **Generate output**.

Results

The custom deployment package is generated and downloaded to the selected folder. You can use this package to apply the configuration on preinstalled SupportAssist versions.

Next steps

1. Complete the SupportAssist deployment and activation using a deployment tool of your choice, such as Microsoft System Center Configuration Manager (SCCM), or Microsoft Intune. See the *SupportAssistDeploymentInstructions.txt* for the deployment commands and instructions. You can also manually install SupportAssist on each PC using the commands. After the configuration and deployment is complete, and the PCs connect to Dell, you can start managing your PC fleet in TechDirect centrally.

 **NOTE:** Historical data collected by SupportAssist before configuration and deployment is not available in TechDirect.

2. [Run the SupportAssist self-diagnosis test.](#)
3. Optional: [Install Central Resource Manager.](#)

Activate SupportAssist using Administrative Template Files (.admx/.adml)

Prerequisites

- SupportAssist must be preinstalled on the PC fleet.
- The PCs must be members of the Intune or Active Directory group.

About this task

When you [Create the SupportAssist deployment package](#) with Administrative Template Files (.admx/.adml), the SupportAssistConfiguration.admx and SupportAssistConfiguration.adml files are generated in your SupportAssist deployment package. These files are used to complete the deployment of SupportAssist using the Active Directory or Intune device configuration policy. When the group policy is updated to the PCs, SupportAssist is automatically configured with the latest configuration settings provided in the Administrative Template files and registers with TechDirect.

Perform the following steps to update the Active Directory:

Steps

1. Perform the following steps to copy the .admx and .adml files to the policy-specific folders in the Active Directory server:
 - a. Open **File Explorer** and go to the C:\Windows\PolicyDefinitions folder.
 - b. Copy the SupportAssistConfiguration.admx file to the PolicyDefinitions folder.
 - c. Go to the required language-specific folder within the PolicyDefinitions folder, for example, C:\Windows\PolicyDefinitions\en-US.
 - d. Copy the SupportAssistConfiguration.adml file to the language folder.
2. Perform the following steps to enable the group policy in the Active Directory server to deploy the SupportAssist configuration:
 - a. Open the **Group Policy Management Console (GPMC)**.
 - b. Go to the Group Policy Object (GPO) you want to configure (or create a new GPO).
 - c. Right-click the GPO and select **Edit**.
The **Group Policy Management Editor** is displayed.
 - d. Go to **Computer Configuration > Administrative Templates > SupportAssist Agent**.
 - e. Double-click **SupportAssist for Business PC**, select **Enabled**, and click **Apply**.
 - f. Close the **Group Policy Management Editor**.

Perform the following steps for intune device configuration policy:

- a. Upload the ADMX/ADML file in your intune instance for SupportAssist application to ensure PCs running SupportAssist are able to connect to TechDirect.
- b. Create a device configuration policy using the imported ADMX files and assign it to the required PCs in the security group.

NOTE:

When you apply an ADMX or AXML policy using Group Policy Management Console (GPMC) or Intune, a window appears with Key and Content fields populated automatically. Do not edit this field manually. It is automatically generated and must remain unchanged for the policy to function correctly.

- **Key field:** This field contains the deployment key defined during the creation of the SupportAssist (SA) package in Deployment Package Manager (DPM).
- **Content field:** This field contains an encrypted blob generated by the DPM tool. It includes the deployment key, proxy settings, group name, and other configuration values. Do not edit this field manually. It is auto-generated and must remain unchanged for the policy to work correctly.

3. After enabling the group policy, you can either wait for the Group Policy Object (GPO) or Intune device configuration policy to propagate in your environment or force an immediate update on the PC fleet.

Topics:

- [Securing the SupportAssist Deployment Registry Key Using Group Policy](#)

Securing the SupportAssist Deployment Registry Key Using Group Policy

About this task

The SupportAssist Deployment Group Policy stores deployment settings in the following registry

location: `Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Dell\SupportAssistAgent\Deployment`

To maintain security, IT administrators should enforce Access Control List (ACL) restrictions that grant access only to Administrators and System accounts. The following procedure describes how to use Group Policy Objects (GPOs) to secure registry keys, both for existing keys and for preemptive protection before key creation.

1. Open the Group Policy Management Editor by running the "gpedit.msc" command in the Run dialog (press Win + R) or by searching for "Edit Group Policy" in the Start menu.
2. Create a new GPO that applies to the target computers or users.
3. Navigate to Computer Configuration or User Configuration, depending on whether you want to apply the settings to computers or users respectively.
4. Expand **Policies** → **Windows Settings** → **Security Settings**.
5. Right-Click on Registry and select **Add Key**.
6. Specify the registry key path for which you want to set ACLs.

For example, if you want to protect `Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Dell\SupportAssist` key, enter the path accordingly.

7. Click OK to add the key.
8. Now, right-click on the added registry key and select Properties.
9. In the Security dialog box, you can add, remove, or modify the permissions for different groups or users, as seen below.

NOTE: If the Users group is removed from the "Group or user names" section, any normal user will not see the contents under "`Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Dell\SupportAssist`". The access will be restricted ONLY to the users who explicitly have Read permissions to the key. To allow only System to access the key, the access can be restricted accordingly as required

10. Click Add to add a new group or user.
11. Select the desired group or user and click OK.
12. Set the appropriate permissions for the selected group or user by checking or unchecking the Allow or Deny checkboxes for various permissions.
13. Click OK to save the changes.
14. Link the GPO to the appropriate organizational unit (OU) or apply it to the necessary Active Directory security group.
15. Wait for the GPO to propagate, or force a Group Policy update on the target computers by running the following command in Command Prompt or PowerShell: `gpupdate /force`.

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 5. 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 > Manage > Recommendations	Supported	Requires permissions from the Connect and manage administrator.
	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 >	Supported	Requires permissions from the Connect and manage administrator.

Table 5. SupportAssist capabilities and roles in TechDirect (continued)

Capability	Description	TechDirect navigation	Connect and manage administrator	Connect and manage technician
		Manage > Update catalogs		
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.
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.

Table 5. SupportAssist capabilities and roles in TechDirect (continued)

Capability	Description	TechDirect navigation	Connect and manage administrator	Connect and manage technician
	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.

Version and validity

SupportAssist for Business PCs

It is recommended to update to the latest version to ensure continued support and receive the full benefits of SupportAssist. The following table lists the validity and end of support date for each version of SupportAssist:

Table 6. SupportAssist version and validity

Release version	Validity
5.2.1.2141	Valid until February 29, 2028
v5.1.1.3567	Valid until November 30, 2027
v5.0.1.2516	Valid until August 31, 2027
v4.9.2.48875	Valid until January 31, 2027
v4.9.1.48804	Valid until January 31, 2027
4.9.0.40923	Valid until January 31, 2027
4.5.3.25254	Unsupported
4.5.2.24316	
4.5.1.23326	
4.5.0.18225 (Patch-2 update)	
4.5.0.17431 (Patch-1 update)	
4.5.0.11735	
3.6.0.56900 (Patch update) and earlier	

NOTE: If SupportAssist has expired on your PC, you must manually update to the latest version. Automatic updates are not supported on expired versions.

Central Resource Manager

It is recommended to update to the latest version to ensure continued support and receive the full benefits of the Central Resource Manager capabilities.

The following table lists the validity of each version of Central Resource Manager:

Table 7. Central Resource Manager version and validity

Release version	Validity
v5.2.1.2141	Valid until February 29, 2028
v5.1.1.3567	Valid until November 30, 2027
v4.9.2.48875	Valid until January 31, 2027
v4.9.1.48804	Valid until January 31, 2027
4.9.0.40923	Valid until January 31, 2027
4.5.3.25254	Unsupported

Table 7. Central Resource Manager version and validity (continued)

Release version	Validity
4.5.2.24316	
4.5.1.23326	
4.5.1.17488	
4.5.0.11735	
3.6.0.56884 and earlier	

SupportAssist version and deployment product code

The product code to be used during deployment varies depending on the version of SupportAssist you are deploying. The following table provides the product code for each SupportAssist version:

Table 8. SupportAssist version and product code

SupportAssist version	Product code
v5.2.1.x	• X64 = 65043213-393F-49BF-B658-5B06C5F713FF • Arm64 = D50198A2-7CD1-49A5-80B2-9B2A1FBF0231
v5.1.1.x	• X64 = 5E5B7C3B-96BE-4A47-B28D-CAA7D87F95A8 • Arm64 = E88D1016-9B01-49C0-841D-9E3391A0C098
v5.0.1.x	19A9EDD8-0C4D-4CF4-B0EA-D110407DF54B
4.9.2.x	F883F4A3-B6A9-40E8-907E-40B91097982E
4.9.1.x	216251D5-BF55-4775-80C4-99E2DDBC0FD
4.9.0.x	2CB737EA-4230-4605-A8EC-2233A2D3E7AE
4.5.3.x	46A18083-9AD3-4BA5-B451-2F690D0C7C89
4.5.2.x	D2C6C498-C603-40E5-8482-723FAFD44C75
4.5.1.x	0D35A1E8-EDF2-49B4-98AC-4BCBA842C445
4.5.0.x	93D44311-C3E0-4FCD-A924-BFAD0AD80525
3.6.0.x	FB5FA53F-5501-4E4C-A57A-6E96199AA22D
3.5.0.x	7622AC14-4D15-4C29-A56C-14A53FF246C7
3.4.1.x	193A0BA2-2FE7-4CC6-9E2D-AA98BF3A0955
3.4.0.x	550B9D53-29F0-44DB-9EBC-B39C4B6948FD

Features and enhancements in previous versions

v5.1.1.3567

- 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.

v5.0.1.2516

- Added Support for Windows 11 25H2.
- Added changes to DPM deployment mode page.
- More enhancements: This update includes performance improvements, security fixes, and bug resolutions.

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.

Resources

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

Documentation and others

Table 9. Resources

For more information about	See	Available at
Onboarding to TechDirect, configuring, downloading, and deploying SupportAssist on the PC fleet	IT Administrators— <i>SupportAssist for Deployment Guide</i> Partners— <i>SupportAssist for Deployment Guide for Partners</i>	SupportAssist documentation page
Using TechDirect to manage your PCs running SupportAssist	<i>SupportAssist for Administrator Guide</i>	
Frequently asked questions and answers about SupportAssist	<i>SupportAssist for Frequently Asked Questions</i>	
Setting up SupportAssist	<i>SupportAssist for Quick Setup Guide</i>	
Data collected from various components of your PC	<i>SupportAssist for Data Collected from Connected PCs</i>	
Summary of recent changes, enhancements, known issues, and limitations in the release	<i>SupportAssist for Release Notes</i>	
Using SupportAssist that is configured and deployed on your PC by your administrator	<i>SupportAssist for User's Guide</i>	
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
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.

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**.