



Quest® On Demand Migration

Active Directory Intune, Autopilot and BitLocker Cleanup Quick Start Guide



© 2025 Quest Software Inc. ALL RIGHTS RESERVED.

This guide contains proprietary information protected by copyright. The software described in this guide is furnished under a software license or nondisclosure agreement. This software may be used or copied only in accordance with the terms of the applicable agreement. No part of this guide may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying and recording for any purpose other than the purchaser's personal use without the written permission of Quest Software Inc.

The information in this document is provided in connection with Quest Software products. No license, express or implied, by estoppel or otherwise, to any intellectual property right is granted by this document or in connection with the sale of Quest Software products. EXCEPT AS SET FORTH IN THE TERMS AND CONDITIONS AS SPECIFIED IN THE LICENSE AGREEMENT FOR THIS PRODUCT, QUEST SOFTWARE ASSUMES NO LIABILITY WHATSOEVER AND DISCLAIMS ANY EXPRESS, IMPLIED OR STATUTORY WARRANTY RELATING TO ITS PRODUCTS INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. IN NO EVENT SHALL QUEST SOFTWARE BE LIABLE FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL, PUNITIVE, SPECIAL OR INCIDENTAL DAMAGES (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, BUSINESS INTERRUPTION OR LOSS OF INFORMATION) ARISING OUT OF THE USE OR INABILITY TO USE THIS DOCUMENT, EVEN IF QUEST SOFTWARE HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. Quest Software makes no representations or warranties with respect to the accuracy or completeness of the contents of this document and reserves the right to make changes to specifications and product descriptions at any time without notice. Quest Software does not make any commitment to update the information contained in this document.

If you have any questions regarding your potential use of this material, contact:

Quest Software Inc.

Attn: LEGAL Dept
20 Enterprise, Suite 100

Aliso Viejo, CA 92656

See our Web site (<https://www.quest.com>) for regional and international office information.


Patents

Quest Software is proud of our advanced technology. Patents and pending patents may apply to this product. For the most current information about applicable patents for this product, please visit our website at <https://www.quest.com/legal>.

Trademarks

Quest, the Quest logo, and Join the Innovation are trademarks and registered trademarks of Quest Software Inc. For a complete list of Quest marks, visit <https://www.quest.com/legal/trademark-information.aspx>. All other trademarks and registered trademarks are property of their respective owners.

Legend

 **CAUTION: A CAUTION icon indicates potential damage to hardware or loss of data if instructions are not followed.**

 **IMPORTANT, NOTE, TIP, MOBILE, or VIDEO:** An information icon indicates supporting information.

Contents

| | |
|-----------------------------------------------------------------------------------------------------------------------------------|-----------|
| Introduction | 4 |
| Requirements | 4 |
| Intune/Autopilot Workstation Cutover Process | 4 |
| High-Level Custom Task Explanation | 6 |
| Autopilot Cleanup | 6 |
| Intune Registry Cleanup | 6 |
| SetUserEmailValues | 7 |
| BitlockerBackupToEntraID (Optional) | 7 |
| CleanUpLocalAdministratorsGroup (Optional) | 10 |
| SetPrimaryUser (Optional) | 12 |
| Implementation Process | 13 |
| Step 1. Copy the Default EntraIDCutover Action | 13 |
| Step 2. Add BitlockerBackupToEntraID Task | 13 |
| Step 3. Add CleanUpLocalAdministratorsGroup Task | 14 |
| Intune Cutover Run Book | 15 |
| Step 1. Run Re-ACL Process | 15 |
| Step 2. Run Cutover Process | 15 |
| Frequently Asked Questions | 16 |
| Why isn't my device joining the target Entra ID, and why is it being removed automatically after a successful initial join? | 16 |
| About us | 17 |
| Technical support resources | 17 |

Introduction

On Demand Migration for Active Directory (ODMAD) supports Microsoft Entra ID Join device migration for devices running Windows 10 or Windows 11 while preserving the User Profiles and File/Folder Security Permissions.

ODMAD successfully migrates these devices to the target Microsoft Entra ID using the default ODMAD settings, including migrating devices that are already Intune-enrolled and devices that were originally provisioned using Autopilot. In addition to migrating the devices to Microsoft Entra ID, a best practice is to also clear previous Autopilot and Intune settings to allow successful Intune enrollment and management in the target.

This quick start guide describes how to perform Intune managed device migration between two Microsoft Entra ID (Cloud Only) tenants.

This guide is a supplementary document to the [Active Directory Entra-Joined Devices Quick Start Guide](#).

Requirements

General

- Client is licensed for On Demand Migration Active Directory and Directory Sync
- One Global Administrator Account for each Microsoft 365 tenant

Accounts

- Microsoft Entra ID Application Account
- An account with Global Administrator Role is required to grant permissions and establish connection when adding a Cloud Environment.
- Microsoft Entra ID PowerShell Accounts. Three PowerShell accounts are automatically created to read and update objects in the cloud. To do this an OAuth token is used from the account that is used to add the Cloud Environment. These PowerShell accounts do not require any Microsoft 365 licenses.

Intune/Autopilot Workstation Cutover Process

The migration process no longer requires the modification of the Default Microsoft Entra ID Cutover action in ODMAD. However, if BitLockerBackup is required for the migration, there is an additional task that needs to be added which will be noted below:

- **AutoPilot Cleanup** - Default Task, removes the Autopilot registry keys from the workstation. This should be done after the workstation has been removed from Enrolled Devices in the source tenant.
- **BT-DownloadReACLConfig** - Default Task
- **BT-ReACLPrepareWin10Profiles** - Default Task
- **BitlockerBackupToEntraID** (Only required if source workstations are BitLocker Enabled) - If the workstation is BitLocker enabled in the source, the Recovery key is not automatically transferred to the target Microsoft Entra ID. This task creates a PowerShell script on the workstation and creates a **Scheduled Task** that will run the script after the user has logged on post migration. The script will escrow the existing recovery key from workstation and write it to the target Microsoft Entra ID account.
- **CleanupLocalAdministratorsGroup** (Optional) - If the source user was an Administrator on the machine, the Re-ACL process will put the target user in the Administrators group. This task will remove users from the Local Administrator Group.
- **BT-EntraIDCutover** - Default Task

High-Level Custom Task Explanation

Autopilot Cleanup

This task must be submitted by the migration administrator for the auto-pilot device to remove the autopilot object in Entra ID.

To allow enrolling the workstation into the target Intune, it is important to remove the source Auto-Pilot Enrollment information. Otherwise, the workstation thinks that it is already part of an Intune/Auto-Pilot Enrollment and will not try to enroll in the target.

First, the AutoPilot Cleanup Action must be submitted by the migration administrator, prior to performing the cutover event, to remove the autopilot object in Entra ID. Additionally, the Auto-Pilot Cleanup option must be selected in the Entra ID Join Profile so the cutover process can clean up the Autopilot registry keys on the device.

Intune Registry Cleanup

To allow enrolling the workstation into the target Intune, it is important to remove the source Intune Enrollment information. Otherwise, the workstation thinks that it is already part of an Intune Enrollment and will not try to enroll in the target. To accomplish this, the **Intune Cleanup** option must be selected in the Entra ID Join Profile.

Edit Your Microsoft Entra Join Profile

✕

PROFILE NAME

Azure AD Join

BULK ENROLLMENT PACKAGE FILE NAME

Note: Microsoft Entra Join requires a provisioning package created in the target tenant, please visit [link](#) for details on how to create the provisioning page. ⓘ

AZJoin.ppkg

TARGET ENVIRONMENT

Lab2-LeagueTeam

DEVICE NAME OPTION

DEVICE NAME DEFINED PER PROVISIONING PACKAGE

KEEP ORIGINAL DEVICE NAME

ENROLL INTO INTUNE MANAGEMENT ⓘ

INTUNE CLEANUP ⓘ

AUTO-PILOT CLEANUP ⓘ

CLEAR

NEXT

SetUserEmailValues

When the machine enrolls in the target Intune, it will look for an Intune Licensed user in M365 using the **UserEmail** value found in the workstation registry. By default, this value is set to the Bulk Enrollment user, which does not have the relevant license, and prevents the Intune service from running correctly.

The product performs this automatically during Entra ID Device Join when the Enroll into Intune Management option is selected in EntraID Device Join Profile. The product will update the **UserEmail** value in the following registry key, setting it to the UPN of the logged-on target user.

- HKLM:\System\CurrentControlSet\Control\CloudDomainJoin\JoinInfo

BitlockerBackupToEntraID (Optional)

When a machine is BitLocker enabled in the source Environment, the key is stored in the source Microsoft Entra ID. During the Workstation migration process the BitLocker key is not automatically migrated into the target Environment. To ensure that the recovery key is stored in the target tenant, this task will escrow the BitLocker key from the workstation and push into the target tenant post migration.

This script creates a separate PowerShell script on the workstation called **BackupBitlockerKeyToADD.ps1** in the ODMAD agent folder and creates a Scheduled Task to execute **BackupBitlockerKeyToADD.ps1** when the first target user logs on.

When the BackupBitlockerKeyToADD script runs during the first login post-migration, it will escrow the BitLocker recovery keys from the machine and store them in the Microsoft Entra ID object of the logged-on user and become viewable in the target Intune tenant.

The script will also create a log file in the ODM agent Files folder and then perform cleanup to remove the Scheduled Task and remove the script itself.

BackupBitlockerKeytoAAD

```
Param (
)

$output = New-Object BinaryTree.ADM.Agent.PSHelpers.PSOutput

$ScriptName = "BackupBitlockerKeyToADD.ps1"

$BacktoAAD = @"

Try{
    `ODMADService = Get-Service -Name ODMActiveDirectory
}
Catch{
    Write-Output "Error Retrieving Service Status...Terminating with error:
`$(`$Error)"
    Exit 1
}
If(`$ODMADService){
    Write-Output "ODM AD Agent Service Found...Finding ODM AD Agent Service Path"
    `$ODMADServicePath = (Get-ItemProperty -Path
HKLM:SYSTEM\CurrentControlSet\Services\ODMActiveDirectory).ImagePath
    `$ODMAgentPath = Split-Path `$ODMADServicePath
    `$ODMAgentPath = `$ODMAgentPath.Trim("` `")
    Write-Output "ODM AD Service Path: `$(`$ODMAgentPath)"
}
Else{
    Write-Output "No ODM Agent Service Found...Terminating"
    Exit 1
}

`$TranscriptFile = "`$(`$ODMAgentPath)\Files\PowerShell-`$(Get-Date -f yyyyMMdd-HHMM)-
BackupBitlockerKeyToAAD.log"
Start-Transcript -Path `$TranscriptFile

`$DriveLetter = `$env:SystemDrive

#endregion declarations

#region functions

function Test-Bitlocker (`$BitlockerDrive) {
    #Tests the drive for existing Bitlocker keyprotectors
    try {
        Get-BitLockerVolume -MountPoint `$BitlockerDrive -ErrorAction Stop
    } catch {
        Write-Output "Bitlocker was not found protecting the `$BitlockerDrive drive.

```

BackupBitlockerKeytoAAD

```
Terminating script!"
    exit 0
}
}

function Get-KeyProtectorId (`$BitlockerDrive) {
    #fetches the key protector ID of the drive
    `$BitLockerVolume = Get-BitLockerVolume -MountPoint `$BitlockerDrive
    `$KeyProtector = `$BitLockerVolume.KeyProtector | Where-Object {
`$_.KeyProtectorType -eq 'RecoveryPassword' }
    return `$KeyProtector.KeyProtectorId
}

function Invoke-BitlockerEscrow (`$BitlockerDrive,`$BitlockerKey) {
    #Escrow the key into Azure AD
    try {
        BackupToAAD-BitLockerKeyProtector -MountPoint `$BitlockerDrive -KeyProtectorId
`$BitlockerKey -ErrorAction SilentlyContinue
        Write-Output "Attempted to escrow key in Azure AD - Please verify manually!"
        exit 0
    } catch {
        Write-Error "Error Occurred"
        exit 1
    }
}

#endregion functions

#region execute

Test-Bitlocker -BitlockerDrive `$DriveLetter
`$KeyProtectorId = Get-KeyProtectorId -BitlockerDrive `$DriveLetter
Invoke-BitlockerEscrow -BitlockerDrive `$DriveLetter -BitlockerKey `$KeyProtectorId

#endregion execute

Remove-Item -path "`$ODMADAgentPath\${$ScriptName}" -Force

Unregister-ScheduledTask -TaskName "${$TaskName}" -Confirm:`$false

Stop-Transcript

"@

#$output = New-Object BinaryTree.ADM.Agent.PSHelpers.PSOutput

### Get ODMAD Agent Information to determine path
Try{
    $ODMADService = Get-Service -Name ODMActiveDirectory -ErrorAction SilentlyContinue
}
Catch{
    Write-Output "Error Retrieving Service Status...Terminating with error: $($Error)"
}
```

BackupBitlockerKeytoAAD

```
Exit 1
}
If($ODMADService){
Write-Output "ODM AD Agent Service Found...Finding ODM AD Agent Service Path"
$ODMADServicePath = (Get-ItemProperty -Path
HKLM:SYSTEM\CurrentControlSet\Services\ODMActiveDirectory).ImagePath
$ODMAGENTPath = Split-Path $ODMADServicePath
$ODMAGENTPath = $ODMAGENTPath.Trim("`")
Write-Output "ODM AD Service Path: $($ODMAGENTPath)"
}
Else{
Write-Output "No ODM Agent Service Found...Terminating"
Exit 1
}

$AgentPath = "$ODMAGENTPath\"
$ScriptFullName = $AgentPath+$ScriptName
If(!(Test-Path $ScriptFullName)) {
New-item -path $ODMAGENTPath -Name $ScriptName -Type "File" -Value $BacktoAAD
}

# Create Scheduled Task
$TaskName = "Backup Bitlocker Key"
$Argument = "-ExecutionPolicy Bypass -File `"$($ODMAGENTPath)\$($ScriptName)`""
$action = New-ScheduledTaskAction -Execute "PowerShell.exe" -Argument $Argument
$Settings = New-ScheduledTaskSettingsSet -AllowStartIfOnBatteries
$Principal = New-ScheduledTaskPrincipal -UserId "LOCALSERVICE" -LogonType
ServiceAccount
$Trigger = New-ScheduledTaskTrigger -Atlogon
$Trigger.Delay = "PT20M"
$ScheduledTask = New-ScheduledTask -Action $Action -Trigger $Trigger -Settings
$Settings
# Register Scheduled Task
Register-ScheduledTask -TaskName $TaskName -InputObject $ScheduledTask -User "NT
AUTHORITY\SYSTEM" -Force

return ($output)
```

CleanUpLocalAdministratorsGroup (Optional)

If the ReACL profile is configured to process local users & groups, the ReACL process will add the target user's Microsoft Entra ID account to the local Administrators group if the source user is a member of that group. If this is not allowed by target security policies, then the target user accounts should be removed from the local Administrators group before migration, as local groups can be managed in the Target Intune environment post-migration.

This script will check the Local Administrators group (identified by SID in case the group has been renamed) and will remove any users where the domain portion of their username matches "Microsoft Entra ID"

CleanUp Local Administrators Group.ps1

```
Param (
)

$output = New-Object BinaryTree.ADM.Agent.PSHelpers.PSOutput

$CleanUnresolvedSIDS = $false
If($CleanUnresolvedSIDS -eq $true){Write-Output "Clean up of unresolved SIDs is Enabled"}
Else{Write-Output "Clean up of unresolved SIDs is Disabled"}

### Get Local Administrators Group
$Get_Local_AdminGroup = Get-WmiObject win32_group -Filter "Domain='$env:computername' and SID='S-1-5-32-544'"
$Get_Local_AdminGroup_Name = $Get_Local_AdminGroup.Name
Write-Output "Administrators group name is: $($Get_Local_AdminGroup_Name)"

## Get Local Administrators group owners
$group = [ADSI]"WinNT://$env:COMPUTERNAME/$(Get_Local_AdminGroup_Name)"
  $admins = $group.Invoke('Members') | % {
    $path = ([adsisearch]"($($group.Name) & $($_.path))".path
    [pscustomobject]@{
      Computer = $env:COMPUTERNAME
      Domain = $(Split-Path ($Split-Path $path) -Leaf)
      User = $(Split-Path $path -Leaf)
    }
  }

### Filter for AzureAD Accounts only - Ignore all other accounts

foreach($admin in $admins){
  If($admin.Domain -eq "AzureAD"){
    Write-Output "Removing AzureAD Users from Local Administrators Group"
    Write-Output "  Removing AzureAD User: $($admin.User)"
    Try{
      Remove-LocalGroupMember -Group $Get_Local_AdminGroup_Name -Member
"$($admin.domain)\ $($admin.user)"
    }
    Catch{
      Write-Output "Error occured removing $($admin.user) from $($Get_Local_AdminGroup_Name) group"
    }
  }
}

### OPTIONAL: Clean up unresolved SIDs - Controlled by status of the
$CleanUnresoldeSIDS Variable ($True=Enabled, $False=Disabled)

If($CleanUnresolvedSIDS -eq $True){
  Write-Output "Removing unresolved SIDs from Group"
  foreach($admin in $admins){
    $admin
```

CleanUp Local Administrators Group.ps1

```
##### Check if SID starts with S-1-12-1 (AzureAD objects) -If Yes then ignore
If($admin.user.StartsWith('S-1-12-1')){
    Write-Output "AzureAD User Found - Ignoring unresolved SID"
    Continue
}
ElseIf($admin.Domain -eq "WinNT:"){
    Write-Output " Removing unresolved SID: $($admin.User) from $($Get_Local_
AdminGroup_Name)"
    Try{
        Remove-LocalGroupMember -Group $Get_Local_AdminGroup_Name -Member
$admin.user
    }
    Catch{
        Write-Output "Error occured removing $($admin.user) from $($Get_Local_
AdminGroup_Name) group"
    }
}
}
}

return ($output)
```

SetPrimaryUser (Optional)

The Primary User value is automatically set in the target Microsoft Entra ID when performing a Microsoft Entra ID join. The product also provides the ability to set this value again via a default system action "Set Intune Primary User". The default system action will set the last logon target user as the device Primary Intune User.

Implementation Process

Refer to the below steps to configure the Optional BitlockerBackupToEntraID task to the custom EntraID Cutover action we are about to create.

Step 1. Copy the Default EntraIDCutover Action

1. In ODMAD using Select **CONFIGURATIONS** from the main ODMAD Menu.
2. Select **ACTIONS**.
3. In the ACTIONS section select click **SHOW SYSTEM**.
4. Find the EntraIDCutoverAction and select it.
5. Click **COPY**, which will open the Edit a Custom Action dialog window. Configure the action as follows:
 - a. ACTION NAME- IntuneMicrosoftEntraIDCutover
 - b. ACTION DISPLAY NAME- Intune Microsoft Entra ID Cutover
 - c. DESCRIPTION - Process to join an Intune/Autopilot workstation to an Microsoft Entra ID
 - d. ACTION TARGET - Computer
 - e. ACTION TYPE - Microsoft Entra ID Cutover
6. Click the **SAVE** to continue.

Step 2. Add BitlockerBackupToEntraID Task

(Optional: Only required if source workstations are BitLockerred)

1. Scroll down to the TASKS section of the Action window and click **NEW**.
2. The ADD A Custom Task window will appear. Configure this as follows:
 - a. TASK NAME: BitlockerBackupToEntraID
 - b. DESCRIPTION: Backups the Bitlocker key from the Workstation to Entra ID user that logged on to the workstation
 - c. TASK TYPE: PowerShell Script
3. Click **NEXT** to Continue.
4. Copy the [BackupBitlockerKeytoAAD.ps1](#) script into the SCRIPT section. There is no need to click the LOAD SCRIPT FRAMWORK as this is included in the PS1 file.
5. Run the PowerShell script
6. Leave all other settings as default and click the **SAVE**.

7. Select the Task just created and select the IntuneMicrosoftEntraIDCutover Action that was created earlier. Click the **ADD TO** to add this task to the action.
8. Scroll up the **ACTIONS** section and expand the IntuneMicrosoftEntraIDCutover Action. The task just added will appear as the last step of the action, click+hold on the task and drag to correct position in the script (after the SetUserEmailValues task, but before the BT-EntraIDCutover task). The change will be saved automatically.

Step 3. Add CleanupLocalAdministratorsGroup Task

(Optional: Only required if source administrator must be removed from the target Local Administrator Group.)

1. Scroll down to the **TASKS** section of the Action window and click **NEW**.
2. The **ADD A Custom Task** window will appear. Configure this as follows:
 - a. **TASK NAME** - CleanupLocalAdministratorsGroup
 - b. **DESCRIPTION** - Removes Microsoft Entra ID Domain users from the local Administrators group before cutover.
 - c. **TASK TYPE** - PowerShell Script
3. Click **NEXT** to continue.
4. Copy the [CleanUp Local Administrators Group.ps1](#) script into the **SCRIPT** section. There is no need to click the **LOAD SCRIPT FRAMEWORK** as this is included in the PS1 file.
5. Run the PowerShell script
6. Leave all other settings as default and click the **SAVE**.
7. Select the Task just created and select the IntuneMicrosoftEntraIDCutover Action that was created earlier. Click the **ADD TO** to add this task to the action.
8. Scroll up the **ACTIONS** section and expand the IntuneMicrosoftEntraIDCutover Action. The task just added will appear as the last step of the action, click+hold on the task and drag to correct position in the script (after the SetUserEmailValues task, but before the BT-EntraIDCutover task). The change will be saved automatically.

Intune Cutover Run Book

This run book assumes that the computer had been read in to On Demand and the workstation has the agent installed, configured, and registered.

Step 1. Run Re-ACL Process

1. In On Demand, navigate to **Devices and Servers**.
2. Select the Device and from the drop-down menu select **Re-ACL**.
3. Select the Re-ACL profile and follow the on-screen prompts.

Step 2. Run Cutover Process

a. Remove Workstation from Source Autopilot

The Autopilot Clean action must be completed and On Demand Migration Active Directory will automatically remove the serial number from the source tenant.

1. In On Demand, navigate to **Devices and Servers**.
2. Select the Device(s) to be cutover and from the drop-down menu select **Autopilot Cleanup**.
3. Once the job is completed, move to the next step.

b. Cutover the Device using ODMAD

1. In On Demand, navigate to **Devices and Servers**.
2. Select the Device(s) to be cutover and from the drop-down menu select **Intune Microsoft Entra ID Cutover**.
3. Select the **Microsoft Entra ID Cutover Profile** and follow the on-screen prompts.

Frequently Asked Questions

Why isn't my device joining the target Entra ID, and why is it being removed automatically after a successful initial join?

If you have enabled automatic enrollment for Windows devices, you may need to create an exclusion for the provisioning package account. This exclusion is necessary when auto-enrollment is active.

With these settings enabled, the device will be automatically joined when the provisioning package is installed. However, it may also be removed immediately if the computer or account is not compliant with policy requirements. This commonly occurs when Multi-Factor Authentication (MFA) is enforced, as the provisioning package account is typically not MFA-compliant.

To resolve this, you'll need to create an MFA exclusion. Check the target MFA policy and add an exclusion for the provisioning package. When adding the exclusion, search for "package ...", you should see a result similar to the provisioning package account.

Select excluded users and groups

Try changing or adding filters if you don't see what you're looking for.

Search

1 result found

All Users Groups

| | Name | Type | Details |
|--------------------------|---------------------------------|------|---------------------------------------------|
| <input type="checkbox"/> | package_854f91cb-9e7d-4526-9... | User | package_41786508-f623-4072-ba78-af3858af... |

Selected (0)

[Reset](#)

No items selected

Add the provisioning package to the exclusion list, wait approximately 10 minutes for the changes to replicate, and then try provisioning the device again. Finally, review the Audit Logs to see if the behavior has changed.

Quest Software creates technology and solutions that build the foundation for enterprise AI. Focused on data management and governance, cybersecurity and platform modernization, Quest helps organizations address their most pressing challenges and make the promise of AI a reality. Around the globe, more than 45,000 companies including over 90% of the Fortune 500 count on Quest Software. For more information, visit www.quest.com or follow Quest Software on [X \(formerly Twitter\)](#) and [LinkedIn](#).

Technical support resources

Technical support is available to Quest customers with a valid maintenance contract and customers who have trial versions. You can access the Quest Support Portal at <https://support.quest.com>.

The Support Portal provides self-help tools you can use to solve problems quickly and independently, 24 hours a day, 365 days a year. The Support Portal enables you to:

- Submit and manage a Service Request
- View Knowledge Base articles
- Sign up for product notifications
- Download software and technical documentation
- View how-to-videos
- Engage in community discussions
- Chat with support engineers online
- View services to assist you with your product