

Dell EMC OpenManage Integration for Microsoft System Center Version 7.2.1 for System Center Configuration Manager and System Center Virtual Machine Manager

Release Notes

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.

Chapter 1: OpenManage Integration Version 7.2.1 for Microsoft System Center Release Notes.....	4
Release type and definition.....	4
Importance.....	5
Important Notes.....	5
Platform(s) Supported.....	5
What's new?.....	5
Fixes.....	5
Installation prerequisites.....	5
Upgrade instructions.....	6
Known issues and resolutions.....	6
Limitations.....	12
Download instructions.....	13
Contacting Dell.....	13

OpenManage Integration Version 7.2.1 for Microsoft System Center Release Notes

This document describes the features, known issues, and resolutions in OpenManage Integration Version 7.2.1 for Microsoft System Center (OMIMSSC).

Topics:

- [Release type and definition](#)
- [Importance](#)
- [Important Notes](#)
- [Platform\(s\) Supported](#)
- [What's new?](#)
- [Fixes](#)
- [Installation prerequisites](#)
- [Upgrade instructions](#)
- [Known issues and resolutions](#)
- [Limitations](#)
- [Download instructions](#)
- [Contacting Dell](#)

Release type and definition

OpenManage Integration Version 7.2.1 for Microsoft System Center

OpenManage Integration for Microsoft System Center (OMIMSSC) is an appliance-based integration into System Center suite of products. OMIMSSC enables full lifecycle management of Dell EMC PowerEdge servers by using integrated Dell Remote Access Controller (iDRAC) with Lifecycle Controller (LC).

OMIMSSC offers operating system deployment, Storage Spaces Direct cluster creation, hardware patching, firmware update, and maintenance of servers and modular systems. Integrate OMIMSSC with Microsoft System Center Configuration Manager (SCCM) for managing the Dell PowerEdge servers in traditional data center, integrate OMIMSSC with Microsoft System Center Virtual Machine Manager (SCVMM) for managing The Dell PowerEdge servers in virtual and cloud environments.

This release is the immediate successor of OMIMSSC version 7.2 for SCCM and SCVMM.

For information about SCCM and SCVMM, see the Microsoft documentation.

Version

7.2.1 Rev.A01

Release date

September 2020

Previous versions


OMIMSSC v7.2

Importance

URGENT: Dell EMC recommends applying this update as soon as possible. The update contains changes to improve the reliability and availability of your Dell system.

Important Notes

- The associated Dell EMC Deployment Tool Kit (DTK) v6.4 is made available for latest iDRAC9 x5 based PowerEdge Servers, to be used with the OMIMSSC Pack only.
- DTK is End of Life product from Dell EMC. This version of DTK is supported for use only with OMIMSSC version 7.2.1

 **NOTE:** For more information, see *the Dell EMC OpenManage Integration for Microsoft System Center Version for Microsoft System Center Configuration Manager and System Center Virtual Machine Manager User's Guide*.

Platform(s) Supported

- 12th generation of Dell EMC PowerEdge servers and later
- Dell EMC PowerEdge MX 7000 chassis and its components
- Dell EMC PowerEdge R640, R740xd, and R740xd2 Storage Spaces Direct Ready Node

 **NOTE:** Support for 11th generation of PowerEdge servers is deprecated.

What's new?

- Support for System Center Configuration Manager (SCCM) version 1910.
- Support for System Center Configuration Manager (SCCM) version 2002.
- Support for System Center Virtual Machine Manager (SCVMM) 2016 UR8.
- Support for System Center Virtual Machine Manager (SCVMM) 2016 UR9.
- Support for System Center Virtual Machine Manager (SCVMM) 2019 UR1.
- Simplified user document. (Installation guide, User's guide, and Troubleshooting information consolidated in a single unified document).
- Reduced installer file size to support faster appliance download.
- Security fixes for Improper Authentication, Information disclosure for appliance logs, and Use of Hard-coded Cryptographic Key vulnerabilities have been implemented. For additional details on the security fixes, refer dell.com/support/security.
- Support for latest iDRAC9 based PowerEdge servers.

Fixes

- Firmware update issue of iDSDM component on Dell EMC PowerEdge R630 model.
- RAID configuration of BOSS device on Dell EMC Storage Spaces Direct R740XD Ready Node with S2D predefined operational template.

Installation prerequisites

To install the Dell EMC OMIMSSC 7.2.1, deploy the Dell EMC OMIMSSC 7.2.1 available as .vhd and enroll the Management Server in Appliance Web Console.

For detailed installation, pre-requisites, configuration, upgrade, and uninstallation instructions, see the Dell EMC OpenManage Integration for Microsoft System Center Version 7.2.1 for System Center Configuration Manager and System Center Virtual Machine Manager User's Guide at Dell.com/openmanagemanuals.

Upgrade instructions

- You can upgrade to OMIMSSC version 7.2.1 from previous versions by using backup and restore appliance capability of OMIMSSC.
- Ensure OMIMSSC for SCCM and SCVMM version 7.1, 7.1.1, or 7.2 is deployed before restoring to OMIMSSC for SCCM and SCVMM version 7.2.1
- Ensure that no jobs are running. If running, wait till the jobs are completed.
- Backup the OMIMSSC appliance data of previous release from the appliance black console.
- Restore the data into OMIMSSC version 7.2.1 from Admin Portal.

Service Pack upgrade from previous versions of OMIMSSC to OMIMSSC version 7.2.1 is not available.

Note:

- For more information about the backup procedure in previous versions, see the **Back up OMIMSSC Appliance** section in **Dell EMC OpenManage Integration for Microsoft System Center for System Center Configuration Manager and System Center Virtual Machine Manager Installation Guide**.
- For more information about the restore procedure in OMIMSSC version 7.2.1, see the Restore OMIMSSC appliance section in **Dell EMC OpenManage Integration for Microsoft System Center Version for Microsoft System Center Configuration Manager and System Center Virtual Machine Manager User's Guide**.

Known issues and resolutions

- **Issue 1 Description:**


System Center Administrator console will crash while importing OMIMSSC console extension in certain System Center versions. System Center versions where the issue may be seen : SC2016 VMM RTM build 4.0.1662.0, SC2012 VMM UR5 or later.

Workaround: As a workaround for SC2016 VMM RTM build 4.0.1662.0 version, upgrade SCVMM using the 4094925 KB article available at support.microsoft.com/kb/4094925, and then import the OMIMSSC console extension. For information about this issue in SC2012 VMM UR5 or later and resolving the issue, see issue 5 in the knowledge base URL: support.microsoft.com/kb/2785682.

- **Issue 2 Description:**

Login to OMIMSSC Console extension for SCCM fails with following error message: `Username or Password is incorrect`

Workaround: As a workaround, login to the system where SCCM site server is installed with the credentials used to login to OMIMSSC console extension and then retry logging in to the OMIMSSC console extension with the same credentials.

 **NOTE:** This is a onetime activity.

- **Issue 3 Description:**

If user names are same and the passwords are different for the domain user account and local user account, then the test connection between Microsoft console and OMIMSSC Appliance fails.

For example, domain user account is: `domain\user1` and password is `pwd1`. And local user account is `user1` and password is `Pwd2` . When you try to enroll with the above domain user account, the test connection fails.

Workaround:

As a workaround, use different user names for the domain user and local user accounts, or use a single user account as local user and during Microsoft console enrollment in OMIMSSC Appliance.

- **Issue 4 Description:**

When accessing the OMIMSSC admin portal by using Mozilla Firefox browser, you get the following warning message: `"Secure Connection Failed"`.

Workaround:

As a workaround, delete the certificate created from a previous entry of the admin portal in the browser. For information about deleting certificate from Mozilla Firefox browser, see support.mozilla.org

- **Issue 5 Description:**

When the OMIMSSC admin portal is launched on a Windows 2016 default IE browser, the admin portal is not displayed with the Dell EMC logo.

Workaround:

As a workaround, do one of the following:

- Upgrade IE browser to the latest version.
- Delete the browsing history, and then add the OMIMSSC admin portal URL to browser's favorite list.

● **Issue 6 Description:**

When modular servers that were previously in another chassis are added to a VRTX chassis and discovered in OMIMSSC, the modular servers carry previous chassis service tag information. Hence, a VRTX chassis group with old chassis information is created in the Appliance instead of the latest chassis information.

Workaround:

As a workaround, do the following:

1. Enable CSIOR, and reset iDRAC on the newly added modular server.
2. Manually delete all the servers in the VRTX chassis group, and then rediscover the servers.

● **Issue 7 Description:**

When a cluster is discovered in OMIMSSC, a cluster update group gets created in the **Maintenance Center** with all the servers listed in the cluster update group. Later, if all the servers are removed from this cluster through SCVMM, and an autodiscovery or synchronization with SCVMM operation is performed, the empty cluster update group is not deleted in **Maintenance Center**.

Workaround:

As a workaround, to delete the empty server group, rediscover the servers.

● **Issue 8 Description:**

When the Domain Name System (DNS) network configuration of the Appliance is changed, creation of HTTP or FTP type of update source fails.

Workaround:

As a workaround, restart the Appliance, and then create the update source of type HTTP or FTP.

● **Issue 9 Description:**

Creating DRM update source on management server running on Windows 10 Operating System (OS) may fail, displaying the following error message: `Failed to reach location of update source. Please try again with correct location and/or credentials.`

Refer the `dlicappliance_main` log in OMIMSSC Admin portal, if the error message displayed is: `Unix command failed SmbException: com.dell.pg.tetris.business.samba.smbclient.SmbException: session setup failed: NT_STATUS_IO_TIMEOUT where EnableSMB1Protocol = false.`

Workaround:

As a workaround, see to the following KB article: support.microsoft.com/en-us/help/4034314

● **Issue 10 Description:**

The same components on identical servers get updated during a firmware update irrespective of the selection of components made on these individual servers. This behavior is observed for 12th and 13th generation of PowerEdge servers with Enterprise license of iDRAC.

Workaround:

As a workaround, do one of the following:

- First apply updates for common components on identical servers, and then apply updates for specific components on individual servers.
- Perform staged updates with planned outage time to accommodate the firmware update.

Issue 11

Description:

After providing the details of a local update source, the test connection may fail as the required files may be not accessible.

Workaround: As a workaround, ensure that `catalog.gz` file is present in the following folder structure.

- For local HTTP update source: http:\\IP address\catalog\catalog.gz
- For local FTP update source: ftp:\\IP address\catalog\catalog.gz
- For local DRM update source: \\IP address\catalog\<catalogfile>.xml
- **Issue 12 Description:**

The **Deploy** option is not displayed in an existing task sequence after uninstalling and reinstalling OMIMSSC console extension for SCCM.

Workaround:

As a workaround, open the task sequence for editing, re-enable the **Apply** option, and click **OK**. The **Deploy** option is displayed again.

- **Issue 13 Description:**

If the DHCP lookup fails while operating system deployment, then the server times out and the server is not moved into Managed Lifecycle Controller Lifecycle Controller (ESXi) collection in SCCM.

Workaround:

As a workaround, install the SCCM client server, and then perform a synchronization to add the servers in Managed Lifecycle Controller Lifecycle Controller (ESXi) collection.

- **Issue 14 Description:**

Hypervisor deployment fails displaying the following error message in activity log: `Error New-SCVMHost failed with following error : An out of band operation (SMASH) for the BMC <IP ADDRESS> failed on IDRAC IP : <IP ADDRESS>.`

Workaround:

This error may occur due to one of these reasons:

- Dell Lifecycle Controller's state is bad.

As resolution, log in to iDRAC user interface and reset Lifecycle Controller.

After resetting Lifecycle Controller, if you still face the problem try the following alternative:

- The antivirus or firewall may restrict the successful run of the WINRM command.

See the following KB article for workaround: support.microsoft.com/kb/961804

- **Issue 15 Description:**

While adding servers to Active Directory, SCVMM error 21119 is displayed. `Error 21119: The physical computer with <SMBIOS GUID> did not join Active Directory in time. The comptuer was expected to join Active Directory using the computer name <host.domain>.`

Workaround:

As a workaround, do the following:

1. Wait for some time to see if the server is added to the Active Directory.
2. If the server is not added to the Active Directory, then manually add the servers to the Active Directory.
3. Add the server in to SCVMM.
4. After the server is added in to SCVMM, rediscover the server in OMIMSSC.

The server will now be listed under the **Host** tab.

- **Issue 16 Description:**

When deploying OS and injecting LC drivers using SC2012 VMM, the OS is deployed successfully but, the LC drivers are not injected.

Workaround:

To resolve the issue, apply the latest rollup for SCVMM.

- **Issue 17 Description:**

After scheduling an export server profile job, the server profile is not exported, and the following error message is displayed: `The selectors for the resource are not valid.`

Workaround:

As a workaround, reset iDRAC, and then schedule the export server profile job. For more information, see iDRAC documentation available at dell.com/support.

- **Issue 18 Description:**

After submitting the import server profile job in OMIMSSC, the job gets timed out after two hours.

Workaround:

As a workaround, perform the following steps:

1. Start the server, press F2, and then enter **BIOS Settings**.
2. Click **System Setup**, and select **Miscellaneous Settings**.
3. Disable **F1/F2 Prompt on Error**.

After performing the following steps, export the server profile again, and use the same server profile to import on that server.

- **Issue 19 Description:**

After collecting the LC logs, when you try to view the LC log file for a server, the following error message is displayed: "Failed to perform the requested action. For more information see the activity log".

Workaround:

As a workaround, reset iDRAC, and then collect and view the LC logs. For information about resetting iDRAC, see iDRAC documentation available at dell.com/support.

- **Issue 20 Description:**

After discovering the servers in OMIMSSC for SCCM console extension, the server may not get added into **All Dell Lifecycle Controller Servers** collection.

Workaround:

As a workaround, delete the **All Dell Lifecycle Controller Servers** collection and then discover the server. The collection is automatically created in SCCM and the server is added to this group.

- **Issue 21 Description:**

When you create a Storage Spaces Direct cluster on nodes that were part of an existing cluster, then the storage pool and the disk configurations have the configurations of the existing cluster. Hence, the cluster storage pool might not be created and if the cluster storage pool is created the health status may be displayed as unknown.

Workaround:

As a workaround, clear the storage pool and disk configuration having existing cluster details and then create the Storage Spaces Direct cluster. For more information on clearing the storage pool, see *Troubleshoot Storage Spaces Direct health and operational states* section from Microsoft documentation.

- **Issue 22 Description:**

When multiple Microsoft consoles are enrolled to an OMIMSSC Appliance, and you try to discover a server, if even one of the SCCM consoles are not reachable, then the server discovery job will fail.

Workaround:

As a workaround, de-enroll the SCCM console that is not reachable, or fix the errors and ensure that the SCCM console is reachable from OMIMSSC Appliance.

- **Issue 23 Description:**

When using Windows 2012 R2 operating system, the context sensitive online help content is launched displaying an error message.

Workaround:

As a solution, update the operating system using the latest KB articles, and then view the online help content.

- **Issue 24 Description:**

When you delete a server or all the servers in an update group from OMIMSSC, and rediscover them you cannot perform any other operations on these servers like updating firmware, exporting and importing LC logs, exporting and importing server profiles.

Workaround:

As a workaround, after rediscovering the deleted server or servers, perform firmware updates using the **Deploy Operational Template** feature in **Server View** and for other maintenance scenarios use iDRAC.

- **Issue 25 Description:**

When you are creating an Operational Template, if you select and clear a dependent attribute's check box having pool value, you are not able to save the Operational Template with the following error message:

```
Select atleast one attribte, under the selected components, before creating the Operational Template.
```

Workaround:

As a workaround, perform any one of the following:

- Select any other dependent attribute having pool value or the same dependent attribute and save the Operational Template.
- Create a new Operational Template.

- **Issue 26 Description:**

After the firmware update of PowerEdge MX7000 components, the comparison report under **Available Updates** in the **Maintenance Center** page, displays incorrect number of updates even if the firmware update is successful.

Workaround: As a work-around, go to **Maintenance Settings** and click **Test Connection** of update source that is used while updating the firmware. Go to **Maintenance Center** to view the correct number of updates.

- **Issue 27 Description:**

After de-enrolling SCVMM from the appliance, OMIMSSC page can still be opened through SCVMM console.

Workaround: As a work-around, ensure to uninstall SCVMM console plug-in after de-enrolling SCVMM from the appliance.

- **Issue 28 Description:**

If the update source does not contain update for the selected device, the firmware update for complete MX chassis group does not complete.

Workaround: Ensure to select devices for which updates are available in the selected update source.

Or

Select only the devices that have applicable updates which are based on the selected update source for firmware update job to complete.

- **Issue 29 Description:**

The Dell EMC Repository Manager (DRM) stops when repository of complete MX7000 chassis group is created using its inventory.xml file.

Workaround: Select only MX7000 chassis and servers. Ensure that the inventory does not contain IOMs and storage sleds.

- **Issue 30 Description:**

While discovering servers using **IP Address Range** and specifying the IP addresses to exclude, if you change any IP value specified in the **IP Address Range** after specifying the IP address to exclude, the following error is displayed, The IP address range that you want to exclude is not within the specified IP address range.

Workaround: As a workaround, do not change the **IP Address Range** values after you have specified the exclude IP address range to discover the servers.

- **Issue 31 Description:**

In the **Modular System View** page, the **Firmware Version** is not displayed after restoring the MX7000 modular system which is discovered in the previous version of OMIMSSC.

Workaround: As a workaround, rediscover the MX7000 modular system to view the firmware version.

- **Issue 32 Description:**

In the **Maintenance Center** page, if disk attached to AHCI controller is attempted for an update through cluster aware method, the updated **Post Successful Update Version** of the disk component will not be reflected.

Workaround: As a workaround, after the CAU job is completed, restart the cluster node or nodes where AHCI controller is an applicable update and refresh the inventory.

- **Issue 33 Description:**

In the **Maintenance Center** page, while performing **Run Update** using **Cluster Aware Update** method, user cannot update the firmware version of operating system driver pack.

Workaround: As a workaround, you can update the operating system driver pack from iDRAC console, or can directly run the DUP on the node operating system.

- **Issue 34 Description:**

In **Modular Systems** view, Operational Template **Compliance Summary** displays noncompliant with zero noncompliant attributes for MX7000.

Cause:

If MX7000 discovered in OMIMSSC is at 1.10.00 firmware version, attributes present under following specified groups cannot be configured using modular system type Operational Template and these attributes should be modified outside of OMIMSSC.

- LocalAccessConfiguration
- TimeConfig
- Power
- SessionConfiguration

Workaround: Recapture the Operational Template and rerun the compliance.

- **Issue 35 Description:**

In the **Maintenance Center** page, on performing import device profile, using vFlash as a **Protection Vault**, imported firmware version of few components may not reflect .

Workaround: As a workaround, perform a refresh inventory after successful import of device profile.

- **Issue 36 Description:**

Operating system deployment in SCVMM fails with an error message: `Invalid data manager state found for host` . Reason being, managed node does not boot to installed operating system since the WinPE image is not disconnected.

Workaround: On completion of operating system installation in SCVMM, before the manage node boots to installed operating system, disconnect the attached WinPE image.

NOTE: To disconnect run the following WinRM command: `winrm i DetachISOImage http://schemas.dmtf.org/wbem/wscim/1/cim-schema/2/root/dcim/DCIM_OSDeploymentService?CreationClassName=DCIM_OSDeploymentService+Name=DCIM:OSDeploymentService+SystemCreationClassName=DCIM_ComputerSystem+SystemName=DCIM:ComputerSystem -u:<username> -p:<password>-r:https://<ip address> -SkipCACheck -SkipCNCheck -encoding:utf-8 -a:basic`

- **Issue 37 Description:**

After applying Update Rollup for SC2012 R2 VMM, SC2016 UR9, and SC2019 UR1, if you try to open the already installed OMIMSSC console, SCVMM displays an error message for security reasons, and you cannot access the OMIMSSC console.

Workaround: As a workaround, do the following:

1. Delete the folder at default path: `C:\Program Files\Microsoft System Center 2012 R2\Virtual Machine Manager\Bin\AddInPipeline\AddIns\<username>`
2. Restart SCVMM.
3. Remove the console extension, and then import the console extension as mentioned in **Importing OMIMSSC console extension for SCVMM section of Dell EMC OpenManage Integration for Microsoft System Center for System Center Configuration Manager and System Center Virtual Machine Manager Installation Guide**.

- **Issue 38 Description:**

While creating Storage Spaces Direct cluster, the **Quality of Service** policy for the Mellanox/Qlogic card on each cluster node is recommended at 50% bandwidth to the SMB traffic, but the current setup is allocating only 30% bandwidth.

Workaround: For information on how to configure QoS policy for SMB traffic, refer to [Storage Spaces Direct deployment guide](#).

- **Issue 39 Description:**

Console Integration workflow triggered from DRM to connect to OMIMSSC appliance fails with password that includes special characters such as `<, >, ' , " , &`

Workaround: As a work around, change the appliance password from OMIMSSC black console to ensure the above mentioned special characters are not part of the password.

- **Issue 40 Description:**

In the **Maintenance Center** page, even after updating Intel(R) Ethernet Converged Network Adapter X710 component the current version will not be displayed as compliant with baseline version.

Workaround: As a work around, login to iDRAC life cycle controller logs page to confirm if the Intel(R) Ethernet Converged Network Adapter X710 component has been updated with the appropriate baseline version.

- **Issue 41 Description:**

Windows operating system deployment from SCCM console fails on Dell servers at "Format and Partition disk" step of task sequence with PERC H730, H330 Adapter, H730 mini, H330 mini controller in BIOS boot mode.

Workaround: As a work around, deploy windows operating system using WinPE image created with base image of SCCM without injecting DTK drivers.

or

Deploy windows operating system in UEFI boot mode.

Limitations

- **Issue 1**

Description:

Operational Template compliance is not displayed for Active Directory attribute, since the attribute value is present in managed device and not in Operational Template.

- **Issue 2**

Description:

If you are accessing local FTP using proxy credentials that are created by CCProxy server, then the local FTP site is not accessible.

- **Issue 3**

Description:

In **BIOS Settings**, the snoop mode attribute does not support **ClusterOnDie** option.

- **Issue 4**

Description:

While creating a logical switch or a hypervisor profile and selecting host groups in OMIMSSC, the groups are not listed in nested form as present in SCVMM.

- **Issue 5**

Description:

If you delete multiple credential profiles, the SCVMM and OMIMSSC consoles may be unresponsive until the profiles are deleted.

- **Issue 6**

Description:

Synchronizing OMIMSSC with enrolled Microsoft console takes sometime depending on the number of servers discovered.

- **Issue 7**

Description:

Filter on **Maintenance Center** is not available for MX7000 Modular Systems.

- **Issue 8**


Description:

In **Server View** page, under **Hosts** tab, the **Select Console Hosts** drop-down menu lists all the host groups present in SCCM with an internal group name. If you select the internal group name, all the hosts that are discovered and managed in SCCM and OMIMSSC are displayed.

- **Issue 9**

Description:

Modified date of a credential profile on creation is set to created date.

 **NOTE:** On consequent edits, modified dates are updated appropriately.

- **Issue 10**

Description:

While deploying Operational Template, if **RAID** is selected as **Device Component**, the attributes of hardware and software components do not get updated in the target server.

- **Issue 11**

Description:

In **Credential Profile** page, the device credential profile can be edited and reused but cannot be deleted. If you choose to delete, the following error message is displayed: `One or more Credential Profile cannot be deleted. One or more Credential Profile are locked and could not be deleted.`

- **Issue 12**

Description:

In Storage Spaces Direct operational template, power cap policy setting is disabled and **Power Cap Value** is predefined. Because of this predefined value, even with power cap policy setting being disabled, the compliance comparison report with predefined operational template will display as **Non-compliant**.

- **Issue 13**

Description:


If user copies the already logged in Admin Portal page URL in to a new browser window, the browser does not redirect the user to the login page.

Download instructions

You can download an evaluation version of OMIMSSC from Dell support page. However, to download a production version, contact your local Dell EMC Sales representative, purchase the appliance license, and then import to the required file location.

For more information about importing the OMIMSSC appliance license file, see the OpenManage Integration for Microsoft System Center User's Guide.

Contacting Dell

 **NOTE:** If you do not have an active Internet connection, you can find contact information on your purchase invoice, packing slip, bill, or Dell product catalog.

Dell EMC provides several online and telephone-based support and service options. Availability varies by country and product, and some services may not be available in your area. To contact Dell for sales, technical support, or customer service issues:

1. Go to **Dell.com/support**.
2. Select your support category.
3. Verify your country or region in the **Choose a Country/Region** drop-down list at the bottom of the page.
4. Select the appropriate service or support link based on your need.