Product Correction Notice (PCN)

Issue Date: 13-December-2021
Supplement Date: 10-November-2025
Expiration Date: Not Applicable
PCN Number: 2135S

SECTION 1 - CUSTOMER NOTICE

Products affected by this PCN:

Avaya Aura® Session Manager 10.1 vAppliance running on Avaya provided servers: Avaya Solutions 130 R5.x (Dell® PowerEdge R640), Avaya Solutions Platform S8300E R5.1; and vAppliance running on customer provided VMware® certified hardware. Software Only deployments on VMware, Microsoft Hyper-V, KVM/AHV, AWS, IBM Cloud for VMware, Microsoft Azure, Google Cloud. Reference the Avaya Aura® Platform Offer Definition for details.

Description:

Effective 01-January-2026 Avaya will no longer provide Manufacturer Support for Avaya Aura® Platform Release 10.1 as noted in the *Product Lifecycle Notice*. Avaya is providing SM 10.1.3.7 as a final Service Pack and SM SSP37 as a final Security Service Pack on top of 10.1.x release.

10 November 2025 – Supplement 15 of this PCN introduces the following update:

- **REQUIRED Session Manager 10.1.3.7 (Service Pack 7 on Feature Pack 3)** (**Session_Manager_10.1.3.7.16.bin; PLDS ID**: **SM000000330**).
  This Service Pack applies to SM/BSM 10.1.x and is not applicable to any other SM/BSM software loads/releases. This Service Pack is applicable to all the 10.1 OVAs and ISO image and must be activated after SM 10.1.0.0.0 is deployed. Service Pack can be installed on top of any previously deployed Feature pack/Service Pack.
  Service pack or Feature pack must be installed prior to installing any Security Service Pack.
  SM 10.1.3.7 contains CRITICAL bug fixes.
- **Session Manager 10.1 Security Service Pack #37 launches coincident with SM 10.1.3.7.** Reference **PCN2136S** for the latest Session Manager 10.1 Security Service Pack.

  Note:
  - *PSN020636u* – Please refer to mentioned PSN for ASM expansion limitations.
  - *PSN020558u* - *Avaya Aura® 10.1.x Software-only RPM updates* will be updated with instructions specific to Aura® 10.1.3.7 once the Aura® 10.1.3.7 Certification for Software Only is completed.

16 June 2025 – Supplement 14 of this PCN introduces the following update:

- **REQUIRED Session Manager 10.1.3.6 (Service Pack 6 on Feature Pack 3)** (**Session_Manager_10.1.3.6.1013608.bin; PLDS ID**: **SM000000325**).
  This Service Pack applies to SM/BSM 10.1.x and is not applicable to any other SM/BSM software loads/releases. This Service Pack is applicable to all the 10.1 OVAs and ISO image and must be activated after SM 10.1.0.0.0 is deployed. Service Pack can be installed on top of any previously deployed Feature pack/Service Pack.
  Service pack or Feature pack must be installed prior to installing any Security Service Pack.
  SM 10.1.3.6 contains CRITICAL bug fixes.
- **Reference PCN2136S for the latest Session Manager 10.1 Security Service Pack.**

©2024-2025 Avaya LLC All Rights Reserved.

Avaya – Proprietary & Confidential.
Use pursuant to the terms of signed agreements or Avaya policy. All other trademarks are the property of their owners.

All trademarks identified by the ® or TM are registered trademarks or trademarks, respectively, of Avaya LLC.

Note:

- PSN020636u – Please refer to mentioned PSN for ASM expansion limitations.
- PSN020558u - *Avaya Aura® 10.1.x Software-only RPM updates* will be updated with instructions specific to Aura® 10.1.3.6 once the Aura® 10.1.3.6 Certification for Software Only is completed.

17 February 2025 – Supplement 13 of this PCN introduces the following update:

- **REQUIRED Session Manager 10.1.3.5 (Service Pack 5 on Feature Pack 3)** (**Session_Manager_10.1.3.5.1013508.bin; PLDS ID**: **SM000000322**).
  This Service Pack applies to SM/BSM 10.1.x and is not applicable to any other SM/BSM software loads/releases. This Service Pack is applicable to all the 10.1 OVAs and ISO image and must be activated after SM 10.1.0.0.0 is deployed. Service Pack can be installed on top of any previously deployed Feature pack/Service Pack.
  Service pack or Feature pack must be installed prior to installing any Security Service Pack.
  SM 10.1.3.5 contains CRITICAL bug fixes.
- **Session Manager 10.1 Security Service Pack #31 launches coincident with SM 10.1.3.5.** For further information on SSP contents and installation procedures for SM 10.1.x, reference **PCN2136S**.

Note:

- PSN020636u – Please refer to mentioned PSN for ASM expansion limitations.
- PSN020558u - *Avaya Aura® 10.1.x Software-only RPM updates* will be updated with instructions specific to Aura® 10.1.3.5 once the Aura® 10.1.3.5 Certification for Software Only is completed.

21 October 2024 – Supplement 12 of this PCN introduces the following update:

- **REQUIRED Session Manager 10.1.3.4 (Service Pack 4 on Feature Pack 3)** (**Session_Manager_10.1.3.4.1013410.bin; PLDS ID**: **SM000000315**).
  This Service Pack applies to SM/BSM 10.1.x and is not applicable to any other SM/BSM software loads/releases. This Service Pack is applicable to all the 10.1 OVAs and ISO image and must be activated after SM 10.1.0.0.0 is deployed. Service Pack can be installed on top of any previously deployed Feature pack/Service Pack.
  Service pack or Feature pack must be installed prior to installing any Security Service Pack.
  SM 10.1.3.4 contains CRITICAL bug fixes.
- **Session Manager 10.1 Security Service Pack #24 launches coincident with SM 10.1.3.4.** For further information on SSP contents and installation procedures for SM 10.1.x, reference **PCN2136S**.

Note:

- PSN020636u – Please refer to mentioned PSN for ASM expansion limitations.
- PSN020558u - *Avaya Aura® 10.1.x Software-only RPM updates* will be updated with instructions specific to Aura® 10.1.3.4 once the Aura® 10.1.3.4 Certification for Software Only is completed.

10 June 2024 – Supplement 11 of this PCN introduces the following update:

- **REQUIRED Session Manager 10.1.3.3 (Service Pack 3 on Feature Pack 3)**

©2024-2025 Avaya LLC All Rights Reserved.

Avaya – Proprietary & Confidential.
Use pursuant to the terms of signed agreements or Avaya policy. All other trademarks are the property of their owners.

All trademarks identified by the ® or TM are registered trademarks or trademarks, respectively, of Avaya LLC.

(**Session_Manager_10.1.3.3.1013305.bin; PLDS ID**: **SM000000302**).
This Service Pack applies to SM/BSM 10.1.x and is not applicable to any other SM/BSM software loads/releases. This Service Pack is applicable to all the 10.1 OVAs and ISO image and must be activated after SM 10.1.0.0.0 is deployed. Service Pack can be installed on top of any previously deployed Feature pack/Service Pack.
Service pack or Feature pack must be installed prior to installing any Security Service Pack.
SM 10.1.3.3 contains CRITICAL bug fixes.

- **Session Manager 10.1 Security Service Pack #24 launches coincident with SM 10.1.3.3.** For further information on SSP contents and installation procedures for SM 10.1.x, reference **PCN2136S**.

  Note:*PSN020558u - Avaya Aura® 10.1.x Software-only RPM updates* will be updated with instructions specific to Aura® 10.1.3.3 once the Aura® 10.1.3.3 Certification for Software Only is completed.

16 January 2024 – Supplement 10 of this PCN introduces the following update:

- **REQUIRED Session Manager 10.1.3.2 (Service Pack 2 on Feature Pack 3)**
  (**Session_Manager_10.1.3.2.1013201.bin**; **PLDS ID**: **SM000000295**).
  This Service Pack applies to SM/BSM 10.1.x and is not applicable to any other SM/BSM software loads/releases. This Service Pack is applicable to all the 10.1 OVAs and ISO image and must be activated after SM 10.1.0.0.0 is deployed. Service Pack can be installed on top of any previously deployed Feature pack/Service Pack.
  Service pack or Feature pack must be installed prior to installing any Security Service Pack.
  SM 10.1.3.2 contains CRITICAL bug fixes.
- **Session Manager 10.1 Security Service Pack #21 launches coincident with SM 10.1.3.2.** For further information on SSP contents and installation procedures for SM 10.1.x, reference **PCN2136S**.

  Note:*PSN020558u - Avaya Aura® 10.1.x Software-only RPM updates* will be updated with instructions specific to Aura® 10.1.3.2 once the Aura® 10.1.3.2 Certification for Software Only is completed.

13 October 2023 – Supplement 9-1 clarifies that the updated ASM/BSM 10.1 software only ISO updated with validation certificates has the same filename, but PLDS ID is changed. The checksum is updated as shown below.

- **Session Manager 10.1 Software Only ISO (updated)**
  (Session_Manager_10.1.0.0.1010009.iso PLDS ID: SM000000286)
  md5sum: c3531fbf59b0ab3b3f03c8ed479643a3
  sha256sum: 26698c18c9e294f3a15edcaa6b5fbc4921262faea70460ac7586a88364498483

09 October 2023 – Supplement 9 of this PCN introduces an updated Avaya Aura® Session Manager (SM) and Branch Session Manager (BSM) 10.1 software only ISO with updated ISO validation certificates.

The PLDS download IDs will remain same, but the ISO is updated.
Existing 10.1 deployments require no action. New software only installations beginning 9th October 2023 will require the updated ISO due to the certificate expiration (Certificate embedded in the old

©2024-2025 Avaya LLC All Rights Reserved.

Avaya – Proprietary & Confidential.
Use pursuant to the terms of signed agreements or Avaya policy. All other trademarks are the property of their owners.

All trademarks identified by the ® or TM are registered trademarks or trademarks, respectively, of Avaya LLC.

ISO was valid only till May 22, 2023).

The ISO file names have changed to reflect a new version number and the checksum is updated.

- ~~**Session Manager 10.1 Software Only ISO (updated) (Session_Manager_10.1.0.0.1010009.iso PLDS ID: SM000000213).**~~

Updated – See Supplement 9-1 above

28 August 2023 – Supplement 8 of this PCN introduces the following update:

- **REQUIRED Session Manager 10.1.3.1 (Service Pack 1 on Feature Pack 3)** (**Session_Manager_10.1.3.1.1013103.bin**; **PLDS ID**: **SM000000280**).
  This Service Pack applies to SM/BSM 10.1.x and is not applicable to any other SM/BSM software loads/releases. This Service Pack is applicable to all the 10.1 OVAs and ISO image and must be activated after SM 10.1.0.0.0 is deployed. Service Pack can be installed on top of any previously deployed Feature pack/Service Pack.
  Service pack or Feature pack must be installed prior to installing any Security Service Pack.
  SM 10.1.3.1 contains CRITICAL bug fixes.
- **Session Manager 10.1 Security Service Pack #16 launches coincident with SM 10.1.3.1.** For further information on SSP contents and installation procedures for SM 10.1.x, reference **PCN2136S**.

  Note:*PSN020558u - Avaya Aura® 10.1.x Software-only RPM updates* will be updated with instructions specific to Aura® 10.1.3.1 once the Aura® 10.1.3.1 Certification for Software Only is completed.

22 May 2023 – Supplement 7 of this PCN introduces the following update:

- **REQUIRED Session Manager 10.1.3 (Feature Pack 3)**
  (Session_Manager_10.1.3.0.1013007.bin; **PLDS ID**: SM000000269).
  This Feature Pack applies to SM/BSM 10.1.x and is not applicable to any other SM/BSM software loads/releases. This Feature Pack is applicable to all the 10.1 OVAs and ISO image and must be activated after SM 10.1.0.0.0 is deployed. Feature Pack 3 can be installed on top of any previously deployed Service Pack.
  Service Pack 1, Service Pack 2 or Feature Pack 2 or 3 must be installed prior to installing any Security Service Pack. SM 10.1.3 contains CRITICAL bug fixes.
- **Session Manager 10.1 Security Service Pack #13 launches coincident with SM 10.1.3.** For further information on SSP contents and installation procedures for SM 10.1.x, reference **PCN2136S**.

  Note:*PSN020558u - Avaya Aura® 10.1.x Software-only RPM updates* will be updated with instructions specific to Aura® 10.1.3 once the Aura® 10.1.3 Certification for Software Only is completed.

13 February 2023 – Supplement 6 of this PCN introduces the following update:

- **REQUIRED Session Manager 10.1.2 (Feature Pack 2)**
  (Session_Manager_10.1.2.0.1012016.bin; **PLDS ID**: SM000000257).
  This Feature Pack applies to SM/BSM 10.1.x and is not applicable to any other SM/BSM software loads/releases. This Feature Pack is applicable to all the 10.1 OVAs and ISO image and must be activated after SM 10.1.0.0.0 is deployed. Feature Pack 2 can be installed on top of any previously deployed Service Pack.

©2024-2025 Avaya LLC All Rights Reserved.

Avaya – Proprietary & Confidential.
Use pursuant to the terms of signed agreements or Avaya policy. All other trademarks are the property of their owners.

All trademarks identified by the ® or TM are registered trademarks or trademarks, respectively, of Avaya LLC.

There was no Feature Pack 1. Feature Pack 2 (10.1.2) is the first Feature Pack for 10.1.x. Service Pack 1, Service Pack 2 or Feature Pack 2 must be installed prior to installing any Security Service Pack. SM 10.1.2 contains CRITICAL bug fixes.

Note:*PSN020558u - Avaya Aura® 10.1.x Software-only RPM updates* will be updated with instructions specific to Aura® 10.1.2 once the Aura® 10.1.2 Certification for Software Only is completed.

24 January 2023 – Supplement 5 of this PCN introduces updated Avaya Aura® Session Manager (SM) and Branch Session Manager (BSM) 10.1 OVAs to address the expiration (February 20, 2023) of the Avaya signing certificate used for Avaya Aura OVAs.
The updated OVAs also provide support for SHA256.
The PLDS download IDs will be the same, but the OVAs are updated.
Existing 10.1 deployments require no action. New installations beginning February 20th, 2023 will require the updated OVAs due to the certificate expiration.
The OVA file names have changed to reflect a new version number and the checksum is updated.

- **Session Manager 10.1 OVA (updated)**
  (SM-10.1.0.0.1010009-e70-02.ova **PLDS ID**: SM000000211)
- **Branch Session Manager 10.1 OVA (updated)**
  (BSM-10.1.0.0.1010009-e70-02.ova **PLDS ID**: SM000000212)
- Reference ***PSN020586u - Avaya Aura® OVA Certificate Expiry February 2023*** for important information.

11 October 2022 – Supplement 4 of this PCN introduces an update/reissue of Session Manager 10.1.0.2.

- **REQUIRED Session Manager 10.1.0.2 (reissue of Service Pack 2)** (New build with necessary postgres security update.)
  (Session_Manager_10.1.0.2.1010219.bin; **PLDS ID**: SM000000246).
  This service pack applies to SM/BSM 10.1.x and is not applicable to any other SM/BSM software loads/releases. This Service Pack is applicable to all the 10.1 OVAs and ISO image and must be activated after SM 10.1.0.0.0 is deployed. Service Pack 2 can be installed on top of any previously deployed Service Pack.
  Service Pack 1 or Service Pack 2 must be installed prior to installing any Security Service Pack.
  SM 10.1.0.2 contains CRITICAL bug fixes.
- Those who already installed the 10.1.0.2 Service Pack provided in supplement 3, need to install SP **Session_Manager_10.1.0.2.1010219.bin** containing vulnerability fixes with respect to postgres (Refer to **Avaya Security Vulnerability Classification** section).

26 September 2022 – Supplement 3 of this PCN introduces the following update:

- **REQUIRED Session Manager 10.1.0.2 (Service Pack 2)**
  ~~(Session_Manager_10.1.0.2.1010215.bin; **PLDS ID**: SM000000243).~~
  ***Updated**: see **Supplement 4** above.*
  This service pack applies to SM/BSM 10.1.x and is not applicable to any other SM/BSM software loads/releases. This Service Pack is applicable to all the 10.1 OVAs and ISO image and must be activated after SM 10.1.0.0.0 is deployed. Service Pack 2 can be installed on top of any previously deployed Service Pack.
  Service Pack 1 or Service Pack 2 must be installed prior to installing any Security Service Pack.
  SM 10.1.0.2 contains CRITICAL bug fixes.

©2024-2025 Avaya LLC All Rights Reserved.

Avaya – Proprietary & Confidential.
Use pursuant to the terms of signed agreements or Avaya policy. All other trademarks are the property of their owners.

All trademarks identified by the ® or TM are registered trademarks or trademarks, respectively, of Avaya LLC.

- **Session Manager 10.1 Security Service Pack #2 launches coincident with SM 10.1.0.2.** Beginning with 10.1, a new Security Service Pack update process is introduced. For further information on SSP contents and installation procedures, reference **PCN2136S.**

18 April 2022 – Supplement 2 of this PCN introduces the following update:

- **REQUIRED Session Manager 10.1.0.1 (Service Pack 1)**
  (Session_Manager_10.1.0.1.1010105.bin; **PLDS ID**: SM000000228).
  This service pack applies to SM/BSM 10.1.x and is not applicable to any other SM/BSM software loads/releases. This Service Pack is applicable to all the 10.1 OVAs and ISO image and must be activated after SM 10.1.0.0.0 is deployed.
  Service Pack 1 replaces the original Service Pack 0.1 and Service Pack 0.
  Service Pack 10.1.0.1.0 is **mandatory.**
  SM 10.1.0.1.0 contains CRITICAL bug fixes.
  Service Pack 1 must be installed prior to installing any Security Service Pack.
- **Session Manager 10.1 Security Service Pack #1 launches coincident with SM 10.1.0.1.** Beginning with 10.1, a new Security Service Pack update process is introduced. For further information on SSP contents and installation procedures, reference **PCN2136S.**

24-December-2021 – Supplement 1 of this PCN introduces an updated, mandatory Session Manager Service Pack 0.1 that replaces the original required Session Manager Service Pack 0. This updated service pack include mitigation of the Log4j vulnerabilities. Reference PSN020550u for more details.

- **Required Session Manager 10.1 Service Pack 0.1** (Session_Manager_10.1.0.0.1010019.bin; **PLDS ID**: SM000000220). This service pack applies to SM and BSM 10.1 (10.1.0.0.1010009) OVA deployment and Software Only ISO deployment. This Service Pack is applicable and **mandatory** for the Session Manager/BSM 10.1 OVAs and Software Only ISO and must be activated after SM 10.1 is deployed. Service Pack 0.1 can be applied on top of Service Pack 0.

13-December-2021 – This PCN introduces Avaya Aura® Session Manager 10.1.0.0 and Branch Session Manager Release 10.1.0.0 and Service Pack 0 which is required to be activated once 10.1 is installed.

- **Session Manager 10.1 OVA** (~~SM-10.1.0.0.1010009-e70-01.ova~~ **PLDS ID**: SM000000211) *Updated – See Supplement 5 above.*
- **Branch Session Manager 10.1 OVA** (~~BSM-10.1.0.0.1010009-e70-01.ova~~ **PLDS ID**: SM000000212) *Updated – See Supplement 5 above.*
- **Session Manager /Branch Session Manager 10.1 Software Only ISO** (~~Session_Manager_10.1.0.0.1010009.iso **PLDS ID**: SM000000213~~)

Updated – See Supplement 9 above

- **Required Session Manager 10.1 Service Pack 0** (~~Session_Manager_10.1.0.0.1010012.bin~~ **PLDS ID**: ~~SM000000215~~)
- This service pack only applies to SM and BSM 10.1 (10.1.0.0.1010009) OVA deployment. This Service Pack is applicable and **mandatory** for the OVAs listed above and must be activated after SM 10.1 is deployed. This Service Pack is NOT required for the Software Only ISO deployment.
- **CRITICAL NOTE:** After application of Session_Manager_10.1.0.0.1010012.bin, the "security module" must be restarted. Restart the security module with the following command from the SM CLI with any customer admin account:
  restart secmod
- **Data Migration Utility for Session Manager / Branch Session Manager 10.1 (**dmutility-10.1.0.0.1010007.bin; **PLDS ID**: SM000000214) Use this utility for migrating data from a 7.x or 8.x based Session Manager Deployment to the 10.1 GA load if you are not using SDM for automated migration. If not using SDM, the data migration utility should be executed once

©2024-2025 Avaya LLC All Rights Reserved.

Avaya – Proprietary & Confidential.
Use pursuant to the terms of signed agreements or Avaya policy. All other trademarks are the property of their owners.

All trademarks identified by the ® or TM are registered trademarks or trademarks, respectively, of Avaya LLC.

	the OVA and Service Pack 0 have been successfully deployed. **Note**: The Avaya Aura® System Manager release/version must always be greater than or equal to the release/version of the components of the solution (Session Manager, Communication Manager, Application Enablement Services). **NOTE:** There is no Session Manager Security Service Pack being released coincident with Session Manager 10.1.
Level of Risk/Severity Class 1=High Class 2=Medium Class 3=Low	Class 2
Is it required that this PCN be applied to my system?	This PCN is required for servers running Session Manager and Branch Session Manager 10.1 GA or earlier software releases.
The risk if this PCN is not installed:	It is possible that service disruptions could occur on the Server, as well as some features not working as expected.
Is this PCN for US customers, non-US customers, or both?	This applies to both US and non-US customers.
Does applying this PCN disrupt my service during installation?	This software will disrupt service in that it requires a system reboot to take effect. Since Session Manager runs in an active-active environment, when multiple Session Manager instances are in a network, the servers should be updated one at a time to minimize any service impact. If only one Session Manager server is in the configuration, service will be impacted during the upgrade time, and should be planned for accordingly.
Installation of this PCN is required by:	Customer and/or (Avaya Remote or On-Site Services) and/or Avaya Authorized Business Partner.
Release notes and workarounds are located:	The Session Manager Release Notes contain the specific software updates and enhancements included in the release and can be obtained by performing the following steps from a browser: 1. Go to http://support.avaya.com then enter your **Username** and **Password** and select **LOG IN.** 2. Mouse over **Search Product** at the top of the page, select **Documents** in the menu.

©2024-2025 Avaya LLC All Rights Reserved.

Avaya – Proprietary & Confidential.
Use pursuant to the terms of signed agreements or Avaya policy. All other trademarks are the property of their owners.

All trademarks identified by the ® or TM are registered trademarks or trademarks, respectively, of Avaya LLC.

3. Begin to type **Session Manager** in the **Enter Your Product Here** box and when Avaya Aura® Session Manager appears as a selection below, select it.
4. Select **10.1.x** from the **Choose Release** pull down menu to the right.
5. Select **Product Documents** on the new page that is displayed. Scroll down (if necessary) and select **View All Product Documents**.
6. Under **Filters,** for category **TYPE** select **Manuals** and for category **SUB TYPE** select **Release Notes & Software Update Notes.**
7. Select the document titled **Avaya Aura® 10.1.x.x Release Notes**.

The What's New in 10.1.x document contains information on new features and important product changes for 10.1.x and can be obtained by performing the following steps from a browser:

1. Go to http://support.avaya.com then enter your **Username** and **Password** and select **LOG IN.**
2. Mouse over **Search Product** at the top of the page, select **Documents** in the menu.
3. Begin to type **Session Manager** and when Avaya Aura® Session Manager appears as a selection below, select it.
4. Select **10.1.x** from the **Choose Release** pull down menu to the right.
5. Select **Product Documents** on the new page that is displayed. Scroll down (if necessary) and select **View All Product Documents.**
6. Under **Filters,** for category **TYPE** select **Manuals** and for category **SUB TYPE** select **Overview.**
7. Select the document titled **What's New in Avaya Aura® Release 10.1.x**.

What materials are required to implement this PCN (If PCN can be customer installed):

All Session Manager 10.1.x.x GA software images are available via Avaya's PLDS software download system. Service Packs and Feature Packs are to be installed on top of the 10.1 GA OVA **"Session Manager 10.1 Installation OVA files, 10.1.x"** or **Branch Session Manager 10.1 OVA** for Core Session Manager or Branch Session Manager respectively**.**

This PCN is being issued as a customer installable PCN. The specified Session Manager files are required. To obtain the update files refer to the **How do I order this PCN** section of this PCN.

If unfamiliar with installing Session Manager software updates, the installation instructions are required. To obtain the installation instructions please refer to the **Finding the installation instructions** section of this PCN.

How do I order this PCN (If PCN can be customer installed):

The software updates can be downloaded by performing the following steps from a browser:

1. Go to http://support.avaya.com then enter your **Username** and **Password** and select **LOG IN.**
2. Mouse over **Search Product** at the top of the page.
3. Begin to type **Session Manager** and when Avaya Aura® Session Manager appears as a selection below, select it.
4. Select **10.1.x** from the **Choose Release** pull down menu to the right.
5. Select **Downloads** on the new page that is displayed. Scroll down (if necessary) and select **View**

©2024-2025 Avaya LLC All Rights Reserved.

Avaya – Proprietary & Confidential.
Use pursuant to the terms of signed agreements or Avaya policy. All other trademarks are the property of their owners.

All trademarks identified by the ® or TM are registered trademarks or trademarks, respectively, of Avaya LLC.

All Downloads.

6. Select the appropriate **Avaya Aura® Session Manager 10.1 Software** to download OVA, (OVA link includes ISO), feature pack/service pack.
7. Scroll down the page to find the download link for the appropriate deployment. This link will take you to the PLDS system with the **Download pub ID** already entered. This page also includes a link to this PCN and the Release Notes.
8. Select the **Download** link to begin the download.

Software updates can also be downloaded directly from the PLDS system at http://plds.avaya.com.

1. Enter your login ID and password. You may have to search for and enter your company name and/or accept the one-time EULA to gain access to software downloads.
2. Select **View Downloads.**
3. In the **Search by Download** tab enter the correct PLDS ID (corresponding PLDS IDs included in the Description section of this document) in the **Download pub ID** search field to access the download. Select the **Download** link to begin the download.

PLDS Hints:

1. In the PLDS **View Downloads** section under the **Suggested Downloads** tab, select **Session Manager** in the **Product Line** search field to display frequently downloaded Session Manager software, including recent Service Packs and other software updates.
2. All Session Manager 10.1 software downloads are available on PLDS. In the PLDS **View Downloads** section under the **Search by Download** tab, select **Session Manager** in the **Application** search field and **10.1** in the **Version** search field to display all available Session Manager 10.1 software downloads.

The MD5 sums are included in the Avaya Support and PLDS descriptions for the download files.

Finding the installation instructions (If PCN can be customer installed):

The Session Manager 10.1 GA software images are available via Avaya's PLDS software download system. **"Session Manager 10.1 OVA, 10.1.x"** or **"Branch Session Manager 10.1 OVA, 10.1.x"** for Core Session Manager or Branch Session Manager respectively**.**

1. Go to http://support.avaya.com then enter your **Username** and **Password** and select **LOG IN.**
2. Mouse over **Search Product** at the top of the page, select **Documents** in the menu.
3. Begin to type **Session Manager** and when Avaya Aura® Session Manager appears as a selection below, select it.
4. Select **10.1.x** from the **Choose Release** pull down menu to the right.
5. Select **Product Documents** on the new page that is displayed. Scroll down (if necessary) and select **View All Product Documents**.
6. Under **Filters,** for category **TYPE** select **Manuals** and for category **SUB TYPE** select **Installation Migrations Upgrades & Configurations.**
7. Select the appropriate deployment document based on the deployment platform.

Service Packs can be applied using SDM or by using *patchSM* from the command line.

©2024-2025 Avaya LLC All Rights Reserved.

Avaya – Proprietary & Confidential.
Use pursuant to the terms of signed agreements or Avaya policy. All other trademarks are the property of their owners.

All trademarks identified by the ® or TM are registered trademarks or trademarks, respectively, of Avaya LLC.

Post install instructions:	N/A

SECTION 1A – SOFTWARE SERVICE PACK INFORMATION

Note: Customers are required to backup their systems before applying the Service Pack.

How to verify the installation of the Software has been successful:	The **Upgrading Avaya Aura Session Manager** document contain details on how to ensure the update(s) installed correctly. You can also confirm the software was installed correctly by confirming the software version displayed for the Session Manager in the System Manger web interface. To determine the release of Session Manager software that is being run on a server you can: • Via a browser, log into the System Manager used to manage the targeted Session Manager server/instance. • Navigate to **Session Manager -> Dashboard.** The current Session Manager/Branch Session Manager version can be viewed in the "**Version**" column (e.g. **Session_Manager_10.1.3.7.16** indicates the Session Manager 10.1.3.7 (FP3SP7) load is running on the selected Session Manager).
What you should do if the Software installation fails?	Escalate to Avaya **Global Support Services (GSS)** or an Avaya authorized Business Partner. **NOTE: For the initial launch of Session Manager/Branch Session Manager 10.1 OVA deployment, there is a mandatory corresponding Service Pack to deploy**.
How to remove the Software if malfunction of your system occurs:	The **Upgrading Avaya Aura® Session Manager** document contains instructions on how to back out an upgrade, and can be obtained by performing the following steps from a browser: 1. Go to http://support.avaya.com 2. Click on **Documents** in the top menu bar 3. In the Enter Your Product Here box, enter "**Session Manager**", select release "**10.1"** in the pull-down list, and select **"Installation, Upgrades & Config"** checkbox in the Content Type box on the left. Then click the "**ENTER**" button to display a list of documents. 4. Search for the document titled "**Upgrading Avaya Aura® Session Manager"** **Contact Avaya Services for assistance if the system is not operating properly after the upgrade to this release. Alternatively, a rollback can be performed by re-installing all software on the Session Manager server per the server replacement procedures in the Maintenance and Troubleshooting guide.**

SECTION 1B – SECURITY INFORMATION

Are there any security risks involved?	Not Applicable
Avaya Security Vulnerability	Supplement 4 of PCN2135S contain fixes for postgres vulnerability mentioned in CVE-2021-23214 and CVE-2021-23222 (**Exception to the normal SSP Process where Security Updates are included in an**

©2024-2025 Avaya LLC All Rights Reserved.

Avaya – Proprietary & Confidential.
Use pursuant to the terms of signed agreements or Avaya policy. All other trademarks are the property of their owners.

All trademarks identified by the ® or TM are registered trademarks or trademarks, respectively, of Avaya LLC.

Classification:	**SSP**) Reference **PCN2136S** for Session Manager 10.1 Security Service Pack details.
Mitigation:	Not Applicable

SECTION 1C – ENTITLEMENTS AND CONTACTS

Material Coverage Entitlements:	Session Manager 10.1 is available free of charge to customers with a valid support contract for Session Manager 10.1.x.
Avaya Customer Service Coverage Entitlements:	Avaya is issuing this PCN as installable by the customer. If the customer requests Avaya to install this PCN, it is considered a billable event as outlined in Section 4 (*Software Updates and Product Correction Notices*) of the Avaya Service Agreement Supplement (Full Maintenance Coverage) unless the customer has purchased an Avaya Services enhanced offer such as the Avaya Services Product Correction Support offer. Additionally, Avaya on-site support is not included. If on-site support is requested, Avaya will bill the customer current Per Incident charges unless the customer has purchased an Avaya Services enhanced offer such as the Avaya Services Product Correction Support offer.

Customers under the following Avaya coverage: -Full Coverage Service Contract* -On-site Hardware Maintenance Contract*	
Remote Installation	Current Per Incident Rates Apply
Remote or On-site Services Labor	Current Per Incident Rates Apply

- Service contracts that include both labor and parts support – 24x7, 8x5.

Customers under the following Avaya coverage: -Warranty -Software Support -Software Support Plus Upgrades -Remote Only -Parts Plus Remote -Remote Hardware Support -Remote Hardware Support w/ Advance Parts Replacement	
Help-Line Assistance	Per Terms of Services Contract or coverage
Remote or On-site Services Labor	Per Terms of Services Contract or coverage

Avaya Product Correction Notice Support Offer
The Avaya Product Correction Support Offer provides out-of-hours support for remote and on-site technician installable PCNs, and Avaya installation for all

©2024-2025 Avaya LLC All Rights Reserved.

Avaya – Proprietary & Confidential.
Use pursuant to the terms of signed agreements or Avaya policy. All other trademarks are the property of their owners.

All trademarks identified by the ® or TM are registered trademarks or trademarks, respectively, of Avaya LLC.

	Avaya issued PCNs that are classified as "Customer-Installable". Refer to the PCN Offer or contact your Avaya Account Representative for complete details.
Avaya Authorized Partner Service Coverage Entitlements:	**Avaya Authorized Partner** Avaya Authorized Partners are responsible for the implementation of this PCN on behalf of their customers.
Who to contact for more information:	If you require further information or assistance please contact your Authorized Service Provider, or visit support.avaya.com. There you can access more product information, chat with an Agent, or open an online Service Request. Support is provided per your warranty or service contract terms unless otherwise specified in the Avaya support Terms of Use.

©2024-2025 Avaya LLC All Rights Reserved.

Avaya – Proprietary & Confidential.
Use pursuant to the terms of signed agreements or Avaya policy. All other trademarks are the property of their owners.

All trademarks identified by the ® or TM are registered trademarks or trademarks, respectively, of Avaya LLC.