Dell Active Fabric Manager for Microsoft Cloud Platform System 2.1(0.0)P2 Release Notes

This document describes the new features, enhancements, and fixed issues for Active Fabric Manager for Microsoft Cloud Platform (AFM-CPS).

Document Revision History

Table 1. Revision History

Revision	Date	Description
A00	2016–04	Updated fixed issues for AFM-CPS 2.0(0.0)P6 release.
A01	2016–05	Updated for AFM-CPS 2.0(0.0)P7 release.
A02	2016–06	Updated for AFM-CPS 2.1(0.0) release.
A03	2016–08	Updated for AFM-CPS 2.1(0.0)P1 release.
A04	2016–09	Updated for AFM-CPS 2.1(0.0)P2 release.

Contents

Requirements

The following requirements apply to AFM-CPS.

AFM-CPS Supported Hardware

AFM-CPS 2.1(0.0)P2 supports the following devices.

Rev. A04
2016 - 09

Table 2. CPS Supported Hardware

Hardware Version	Supported Devices	Version
CPS 2016	S3048-ON	9.10(0.1)P8
	S4048-ON	9.10(0.1)P8
CPS 2014	S4810	9.10(0.1)P8
	S55	8.3.5.6

AFM-CPS 2.1(0.0)P2 also supports CPS 2016 racks with S3048-ON and S4048-ON devices and CPS 2014.

Table 3. Supported Rack Deployments

AFM-CPS 2.1(0.0)P2	Supported Rack Deployments
CPS 2016	One to four racks. Each CPS 2016 rack can include: • One S3048-ON switch • Five S4048-ON switches (one for aggregation, two tenant switches configured as a VLT pair, and two data center switches)
CPS 2014	Each CPS 2014 rack can include: • One S55 switch • Five S4810 switches (one for aggregation, two tenant switches configured as a VLT pair, and two data center switches)

About CPS 2016 Racks

- The aggregation, tenant, and data center switches are connected using a distributed core mesh.
- AFM-CPS uses virtual link trunking (VLT) in the access fabric to connect the rack switches to the server and internal BGP (iBGP) for the traffic in the fabric.
- Each S4048-ON switch in the same rack connects to the S3048-ON switch from ports 37 to 41.
- Each aggregation switch connects to the S3048-ON switch from ports 7 to 52.
- Port 42 is reserved for the AFM-CPS 2.1(0.0)P2 laptop to connect to the S3048-ON switch in each rack for deployment and management of the switches.
- Each rack has its own subnet and default gateway.
- The S3048-ON in each rack is not directly connected to the switches in the other racks.
- The aggregation switch contains the L3 uplink running BGP connected to the edge router in the network.
- The edge router is not considered part of any single fabric because it is shared with multiple fabrics.
- To run validation checks on the racks and route traffic across the switches, manually configure any edge routers for AFM CPS.
- To validate the link between the management port on the S4048-ON switch and the S3048-ON switch, use the `ping` command.
- With AFM-CPS 2.1(0.0)P2, you can expand the racks to a maximum of four racks.

AFM-CPS Server and Client Requirements

The following tables describe the hardware requirements for the server and client switches.

Table 4. AFM-CPS Server Requirements

Hardware	Requirement
Processor	Intel® Xeon® E5620 2.4Ghz, 12M Cache, Turbo, HT, 1066 MHz Max Memory
Operating System	Windows Server 2012 R2
Memory	32GB Memory (8x4GB) minimum, 1333 MHz Dual Ranked LV RDIMMs for 2 processors, Advanced ECC
Disk Space	1TB 7.2K RPM SATA 3.5 hot plug Hard Drive

Table 5. AFM-CPS Client Requirements

Hardware	Requirement
Processor	Intel® Core (TM) i5-2520 M CPU @2.50Ghz
Operating System	Windows 8.1 64-bit
Memory	8 GB (minimum)

AFM-CPS Client Requirements

To install and deploy AFM-CPS and to deploy the racks, use a laptop as a host for the AFM-CPS virtual machine (VM). You install the AFM-CPS virtual hard disk (VHDx) on the laptop Hyper-V virtual machine. For information on how to import or export files using Hyper-V, see the Microsoft Hyper-V documentation.

Using AFM-CPS 2.1(0.0)P2, connect the laptop to each S3048-ON switch in the rack for the initial deployment or after replacement or redeployment of aggregation switches.

Table 6. AFM-CPS Client Requirements

Hardware	Requirement
Processor	Intel® Core (TM) i5-2520 M CPU @2.50Ghz
Operating System	Windows 8.1 64-bit OS or Windows Server 2012 R2
Memory	4 GB (minimum)
Software	Microsoft Hyper-V
	Microsoft System Center Virtual Machine Manager (SCVMM) (required for Hyper-V)

Software Requirements

This section describes information about the virtual machine, client, and server software.

Virtual Machine Requirements

AFM-CPS runs as a virtual machine and requires the following software.

Table 7. AFM-CPS Virtual Machine Software

Hypervisor	Version
Microsoft Hyper-V	6.3.9600.16384
Microsoft System Center Virtual Machine Manager (SCVMM) — Microsoft Hyper-V requires SCVMM.	

AFM Client Software Requirements

The AFM client and server requires the following software.

Table 8. AFM Client and Server Software

Software	Description
Server OS	Windows Server 2012 R2
	Windows requires Administrator permission on the target server. Make sure that you have modification permissions on the network service account for the system temp directory: **%systemroot%\temp**
Client OS	Windows 8.1 64-bit
	System Center 2012 R2
	Windows Azure
Browser	Internet Explorer 9 or higher
	Firefox 12 or higher

Rack Expansion

The rack expansion feature requires switches running CPS 2016.

IP Address Requirements

Before deployment, verify that you have the following IP address information available.

- The AFM-CPS laptop IP address
- The AFM-CPS IP address and default gateway for each rack — The IP addresses are different for each rack because each rack has its own subnet and default gateway.
- The final AFM-CPS IP address in the infrastructure rack.

Port Configuration Requirements

AFM-CPS requires the following AFM port configurations.

Table 9. Port Configuration

Port	Protocol
20 and 21	FTP
22	SSH and SCP (communication to the switches and CLI access to AFM)
23	Telnet (communication to the switches)
67 and 68	DHCP
69	TFTP
80	AFM server port listening for client connection and requests
123	NTP
161	SNMP get and set protocol between AFM server and switch.
162	SNMP trap listener between AFM and switch.
443	HTTPS communication protocol where the AFM takes requests from the client browser.

Port	Protocol
5432	Database server
8080	TCP/UDP
61616	ActiveMQ

New in This Release

AFM-CPS 2.1(0.0)P2 includes the following feature:

- SNMPv3 support.

  NOTE: Refer to Dell Networking OS 9.x Configuration and Command-Line Reference Guides for information on how to configure SNMPv3.

Upgrading AFM-CPS

The AFM-CPS browser client can be used to upgrade an earlier version of AFM-CPS to AFM-CPS 2.1(0.0)P2.
You can view and manage AFM-CPS updates on the **Server Update**.

1. From the AFM-CPS browser client menu, click **Administration** and then click the **Server Update** tab.
2. In the **Select RPM packing file location** area, select one of the following options:

   - **Local Drive (DVD, USB)**
   - **Remote Server**

     NOTE: If the location is a remote server, enter the URL location of the RPM file on the remote server.

     1. From the **Protocol Type** drop-down menu, select the protocol type:
        - **https**
        - **ftp**
        - **sftp**
     2. Specify the path of the RPM package using the following formats:

        NOTE: The RPM filename must start with AFM and must end with **.noarch.rpm** (for example, **AFM<version>.noarch.rpm**).

        - **https://***ipaddress|path_to_rpm.file*
        - **ftp**://*ipaddress|path_to_rpm.file*
        - **sftp**://*ipaddress|path_to_rpm.file*
3. From the **Select the server update method** area, select:

   - **AFM Upload/Download** — Copy the update to the standby partition on the server but do not apply it or restart. To update, manually start the update from the AFM-CPS server update page.
4. Click **Update**.

   An information note appears indicating that the server update job is scheduled. See the execution details in the **Job Results** tab. When the software image is available, it is listed in the Available Software Version column in the **Server Update** tab.
5. Click **Activate Available Version**.
6. Click **Yes** to enable the available AFM software and reboot the server. During the upgrade process, the AFM server restarts to enable the update in the standby partition. View the process details in the **Job Results** tab.

When the upgrade is complete, you can confirm the update listed in the **Current Software Version** column in the **Server Upgrade** tab.

Known Issues

Known issues are reported using the following definitions.

Category	Description
PR#	Problem Report number that identifies the issue.
Synopsis	Synopsis is the title or short description of the issue.
Release Notes	Release Notes description contains more detailed information about the issue.
Work around	Work around describes a mechanism for circumventing, avoiding, or recovering from the issue. It might not be a permanent solution. Issues listed in the "Closed Caveats" section should not be present, and the work around is unnecessary, as the version of code for which this release note is documented has resolved the caveat.
Severity	**S1** — Crash: A software crash occurs in the kernel or a running process that requires a restart of AFM, the router, switch, or process. **S2** — Critical: An issue that renders the system or a major feature unusable, which can have a pervasive impact on the system or network, and for which there is no work around acceptable to the customer. **S3** — Major: An issue that effects the functionality of a major feature or negatively effects the network for which there exists a work around that is acceptable to the customer. **S4** — Minor: A cosmetic issue or an issue in a minor feature with little or no network impact for which there might be a work around.

Category	Description
PR#	136879
Synopsis	AFM-CPS For any switches deployed after the initial full fabric deployment, user will need to manually enable Data collection Job for those switches
Release Notes	AFM-CPS For any switches deployed after the initial full fabric deployment, user will need to manually enable Data collection Job for those switches
Work around	User will have to use the "Jobs" menu in the left side panel, and select "Data Collection" tab to manually enable Data Collection support for the appropriate switches within the fabric.
Severity	S3

Category	Description
PR#	138430
Synopsis	AFM-CPS Once you deploy a switch in a fabric, you cannot change the management IP settings for that switch, including gateway/route
Release Notes	AFM-CPS Once you deploy a switch in a fabric, you cannot change the management IP settings for that switch, including gateway/route

Category	Description
Work around	There is no workaround for this issue, it will need to be addressed in a future release to allow user to update management network gateway / route values. Otherwise, if user really has to change this then they will have to delete this fabric from AFM and create a new one.
Severity	S3

Category	Description
PR#	158857
Synopsis	"python: not found" errors seen after upgrading with AFM.
Release Notes	Error messages might be seen when upgrading S4810 switches to a 9.9x software release. The "python: not found" errors were fixed after manually clearing all packages and reinstalling SmartScripts.
Work around	Uninstall existing packages from the S4810 switches using the CLI "package clear-all" before upgrading the switches using CPS.
Severity	S2

Category	Description
PR#	159322
Synopsis	AFM Predeployment Configuration wizard shows the prior software version as the correct version
Release Notes	The AFM Predeployment Configuration wizard incorrectly shows the previous software version even though the AFM upgrade completed successfully and the new switch firmware version is available.
Work around	None.
Severity	S2

Category	Description
PR#	159323
Synopsis	After switch upgrade, AFM validation shows config mismatch errors due to software version
Release Notes	Running validation on some switches after software upgrade might result in configuration mismatch errors in multiple tabs since the validation is using the previous version.
Work around	None.
Severity	S2

Category	Description
PR#	159339
Synopsis	IPv6 loopback ping validation on AFM may present false positive errors
Release Notes	During validation, AFM might ping an incorrect IPv6 address, resulting in AFM reporting the address is unreachable.
Work around	None.

Category	Description
Severity	S2

Category	Description
PR#	159344
Synopsis	"IOError [Errno 61] Connection refused" seen after upgrading with AFM
Release Notes	Error messages might be seen when upgrading S4810 switches to a 9.9x software release. These errors were seen in conjunction with "python: not found" errors and disappeared after clearing all packages with the CLI "package clear-all". This issue is not reproducible.
Work around	None.
Severity	S2

Category	Description
PR#	159750
Synopsis	Configuration changes during rack expansion is not pushed when deployed using Apply configuration option
Release Notes	Configuration changes during rack expansion is not pushed when deployed using "Apply configuration changes to the switch" option.
Work around	For redeployment of switches use "Overwrite entire configuration of the switch " option to push the configuration changes.
Severity	S2

Category	Description
PR#	160008
Synopsis	Activate Standby image Job scheduling not working for All Racks option
Release Notes	Standby software versions are not listed and job schedule fails when "All Racks" option selected for Standby partition upgrade
Work around	User should choose "All devices" option instead of "All Racks"
Severity	S3

Category	Description
PR#	160030
Synopsis	Config mismatch error report for logging source-interface ManagementEthernet command
Release Notes	Logging source-interface managementethernet 1/1 not accepted in switches when user upgrade the image from 9.9.x.x version to 9.10..0.1P3.
Work around	Push the configuration using custom templates
Severity	S2

Category	Description
PR#	160082
Synopsis	AFM database accessible from external system
Release Notes	AFM Database access currently available from external system with default port
Work around	None
Severity	S3

Category	Description
PR#	160084
Synopsis	AFM dependent management services like Telnet,ftp needs to be disabled
Release Notes	Ftp and telnet protocols support not disabled.
Work around	User should select secured protocol SSHV2 for deployment instead of telnet. No alternate option available for ftp.
Severity	S3

Category	Description
PR#	160085
Synopsis	Centos Security updates for Kernel and utilities
Release Notes	Centos 6 security updates like Kernel,ntp,openssl,wget,sudo,python,openssh are not addressed.
Work around	None.
Severity	S3

Category	Description
PR#	160806
Synopsis	Config Mismatch Error will be shown, when redeploy fabric with only “Apply configuration changes to the switch”
Release Notes	When AFM server upgraded from AFM-CPS build 2.0.0.P7 or below to build 2.1.0.0P2 and redeploy the existing fabric via “Apply configurations changes to switch” ,will get the configuration mismatch error.
Work around	Redeploy the existing fabric using “Overwrite entire configuration on the switch”
Severity	S3

Category	Description
PR#	160882
Synopsis	On multiple flips in SNMP version between v2 to v3, along with a password change, sometimes, the SNMP password change is not pushed to the device

Category	Description
Release Notes	On multiple flips in SNMP version between v2 to v3, along with a password change, sometimes, the SNMP password change is not pushed to the device. When this happens the device is not reachable.
Work around	There is no workaround, except to recreate the fabric.
Severity	S2

Category	Description
PR#	161062
Synopsis	Switching from SNMP V2 to SNMP v3 using "Apply Configuration" fails in AFM
Release Notes	When user flips from SNMP v2 to V3 and uses the "Apply Configuration" method, deployment is successful and Validation fails with message 'Switch not discovered'.
Work around	Always use "Overwrite Configuration" when changing from v2 to v3. If "Apply Configuration" is used by mistake, the recovery mechanism is re-deploy fabric using "Overwrite entire configuration on the switch" option.
Severity	S2

Fixed Issues

Fixed issues are reported using the following definitions.

Category	Description
PR#	Problem Report number that identifies the issue.
Synopsis	Synopsis is the title or short description of the issue.
Release Notes	Release Notes description contains more detailed information about the issue.
Work around	Work around describes a mechanism for circumventing, avoiding, or recovering from the issue. It might not be a permanent solution. Issues listed in the "Closed Caveats" section should not be present, and the work around is unnecessary, as the version of code for which this release note is documented has resolved the caveat.
Severity	**S1** — Crash: A software crash occurs in the kernel or a running process that requires a restart of AFM, the router, switch, or process. **S2** — Critical: An issue that renders the system or a major feature unusable, which can have a pervasive impact on the system or network, and for which there is no work around acceptable to the customer. **S3** — Major: An issue that effects the functionality of a major feature or negatively effects the network for which there exists a work around that is acceptable to the customer. **S4** — Minor: A cosmetic issue or an issue in a minor feature with little or no network impact for which there might be a work around.

Fixed Issues in this Release

Category	Description
PR#	160775
Synopsis	No TCA reported for fresh deployed fabric
Release Notes	On a Freshly deployed fabric, the dfmcron.py does not get executed. So TCA is not reported.
Work around	From Custom Configuration in AFM, we need to add the following two lines . no script execute /usr/pkg/home/dfmcron.py script execute /usr/pkg/home/dfmcron.py
Severity	S3

Category	Description
PR#	160881
Synopsis	On V3 credential configuration/Change, the AFM reports switch not reachable alerts.
Release Notes	The Trap v3 password is not updated in the cache maintained by the trap module. Hence even after the SNMP credential change, the trap module alone uses the old credential resulting in the errors. Other modules like performance monitor screen and summary screen work fine.
Work around	After Password change and deployment is complete, the AFM service has to be restarted.
Severity	S2

Category	Description
PR#	160904
Synopsis	Sender side loop detection default value change caused an issue with advertising AS number with the config "remove-private-as" in BGP
Release Notes	The default behavior for sender side route loop detection changed from enabled by default in Dell OS 9.9 to disabled by default in Dell OS 9.10. Sender side route loop detection must be explicitly enabled in CLI to enable loop detection. This CLI change has been made in the default configuration templates.
Work around	Sender side route loop detection can be enabled on the custom configuration screen.
Severity	S2

Category	Description
PR#	160987
Synopsis	Remove the provision to install the certificate signed by CA
Release Notes	There was a provision added in AFM-CPS-2.1p1 in the AFM console to install a certificate signed by CA along with the option to change the self signed certificate. The new feature to add the signed certificate was removed and the original option to change the self signed certificate was alone retained.
Work around	NONE

Category	Description
Severity	S3

SNMP Support

AFM-CPS 2.1(0.0)P2 supports SNMPv3 and retains support for SNMPv2.

You can configure the SNMPv2 or SNMPv3 credentials for designed and deployed fabrics. By default, AFM-CPS uses MD5 authentication and DES-56 encryption for SNMPv3 configuration. You can enable SNMPv3 in AFM-CPS in the following ways:

- A fresh installation with the AFM-CPS .VHDx image file.
- An RPM upgrade. See the *Active Fabric Manager for Microsoft Cloud Platform System User Guide* for more details.

You can configure SNMPv2 or SNMPv3 credentials for a fabric in the following ways:

- AFM Setup Wizard
- Administrative Settings
- Predeployment Configuration Wizard

Configuring the SNMP Version in the AFM Setup Wizard

You can configure the SNMP version — SNMPv2 or SNMPv3 — in the **AFM Setup** wizard.

1. In the SNMP and CLI screen of the **AFM Setup** wizard, you can select the version as **V2c** or **V3**.

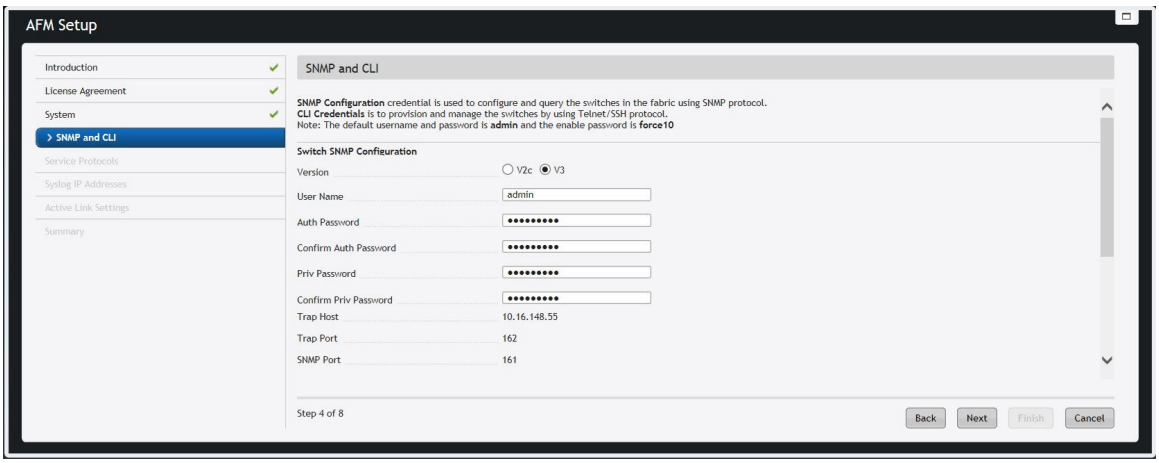

Figure 1. AFM Setup Wizard

2. In the **User Name** field, enter the user name.
3. In the **Auth Password** field, enter the auth password.
4. In the **Confirm Auth Password** field, confirm the auth password.
5. In the **Priv Password** field, enter the priv password.
6. In the **Confirm Priv Password** field, confirm the priv password.
7. Click **Next**.

Configuring SNMP Credentials Globally

You can configure SNMPv2 or SNMPv3 credentials globally in which AFM-CPS applies the settings to all fabrics designed in AFM-CPS.

NOTE: You cannot edit SNMP credentials after a fabric has been deployed.

1. From the menu, click **Administration** and then the **Settings** tab
2. In the SNMP configuration area, click **Edit**.
   The **SNMP Configuration** dialog box appears.

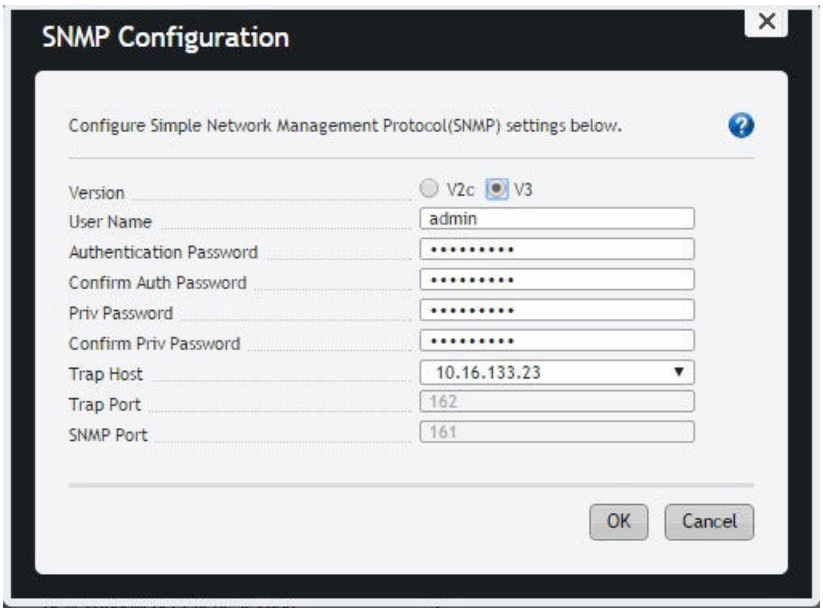

Figure 2. SNMP Configuration Dialog Box

3. In the **Version** field select one of the following options: **V2c** or **V3**.
4. In the **User Name** field, enter the user name.
5. In the **Authentication Password** field, enter the auth password.
6. In the **Confirm Auth Password** field, confirm the auth password.
7. In the **Priv Password** field, enter the priv password.
8. In the **Confirm Priv Password** field, confirm the priv password.
   - In **Trap Host** field, the default setting is the server IP.
   - In **SNMP Port** field, the default setting 161.
9. Click **OK**.

Configuring SNMP in the Predeployment Configuration Wizard

You can configure SNMPv2 or SNMPv3 credentials for each fabric during pre-deployment configuration.
You can edit these settings even after the fabric is deployed.

1. From the **SNMP and CLI Credentials** screen in the **Predeployment Configuration** wizard, in the **Version** field, select **V2c** or **V3**.

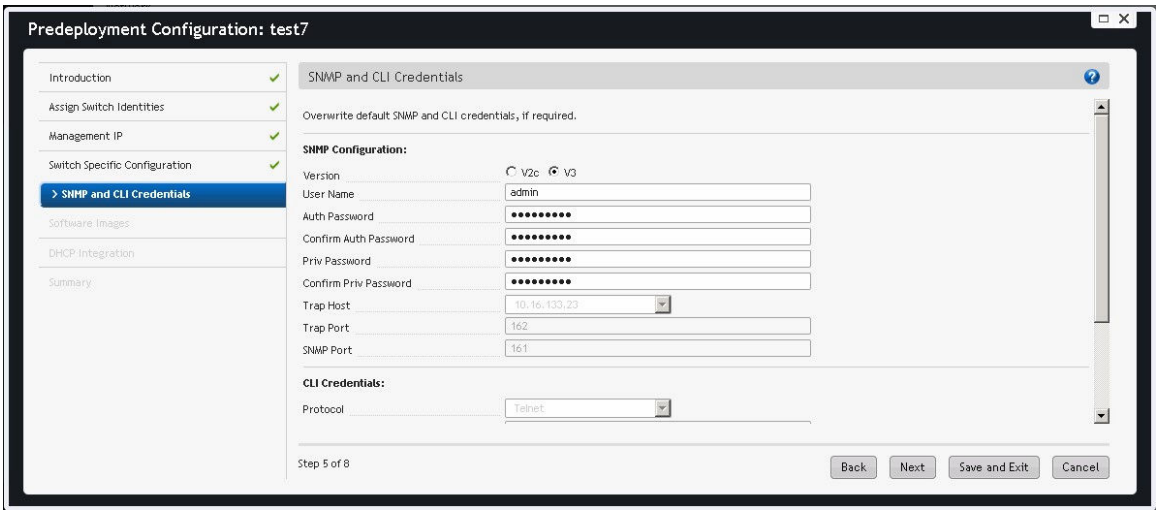

Figure 3. Predeployment Configuration Wizard

2. In the **User Name** field, enter the user name.
3. In the **Auth Password** field, enter the auth password.
4. In the **Confirm Auth Password** field, confirm the auth password.
5. In the **Priv Password** field, enter the priv password.
6. In the **Confirm Priv Password** field, confirm the priv password.
    - In the **Trap Host** field, by default is set as server IP.
    - In the **Trap Port** field, the default is set to 162.
    - In the **SNMP Port** field, the default is set to 161.
7. Click **Next**.

Converting from SNMPv2 to SNMPv3

You can convert from SNMPv2 to SNMPv3.

1. From the menu, select **Network** and then select the fabric.
2. Click the **Configure and Deploy** tab.
3. Click **Deploy Fabric**, and select **Pre-deployment Configuration**.
   The **Predeployment Configuration** wizard appears.
4. Navigate through the wizard to the **SNMP and CLI Credentials** screen.

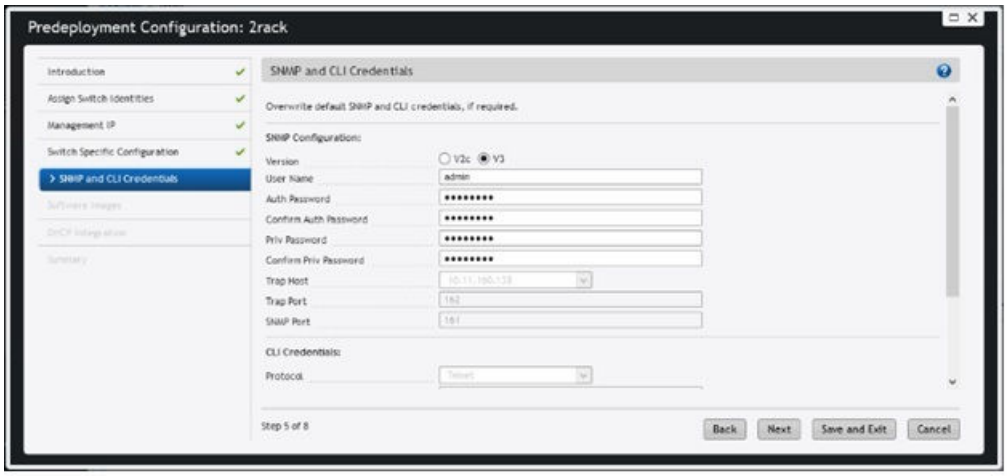

Figure 4. SNMP and CLI Credentials Screen

5. In the **Version** field, select **V3**.
6. Make entries for the **User Name**, **Auth Password**, **Confirm Auth Password**, **Priv Password**, and **Confirm Priv Password** fields.
7. Click **Next**.
8. Navigate through the remainder of the wizard and click **Finish**.
9. Return to the **Configure and Deploy** tab.
10. Click **Deploy Fabric** and select **Deploy and Validate**.
11. In the **Deploy and Validation** screen, select the switches to deploy and click **Deploy Selected**.

    The **Configuration deployment option** dialog box appears.
12. Select **Overwrite entire configuration on the switch** and click **OK**.

    AFM-CPS applies the SNMPv3 configuration to the switches and the reloads them. You must select **Overwrite** instead of **Apply** when changing between SNMPv2 and SNMPv3 to work around issue #161062. This issue can result in an error when applying the SNMP configuration to the switch that causes the AFM-CPS validation to fail with the error "Switch not discovered."
13. Deploy remaining switches using the previous steps.

Changing the SNMP Password

You can change the SNMPv2 or SNMPv3 password.

1. Navigate to the **SNMP and CLI Credentials** screen of the **Predeployment Configuration** wizard.

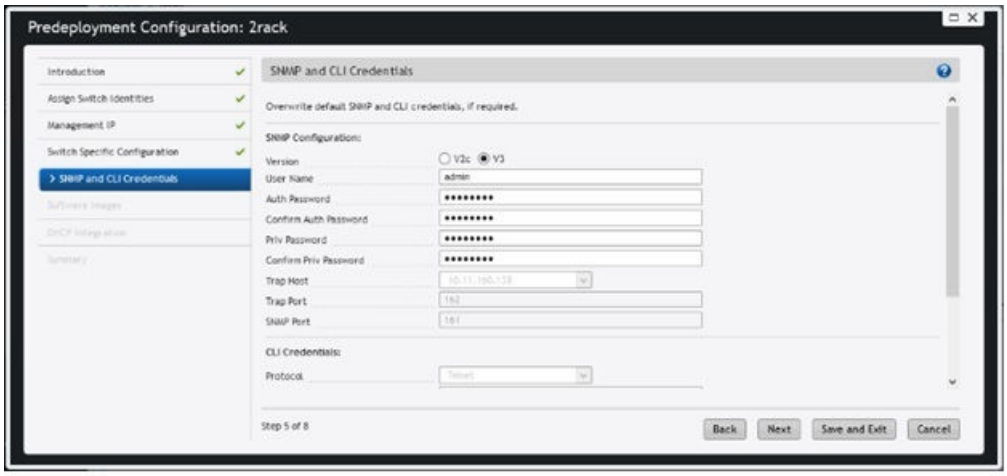

Figure 5. SNMP and CLI Credentials Screen

2. Navigate to the **SNMP Configuration** area.
3. In the **Version** field, make sure the correct SNMP version is selected: **V2c** or **V3**.
4. Edit any of the following fields as necessary: **User Name**, **Auth Password**, or **Priv Password**.
5. Navigate through the remainder of the wizard and click **Finish**.
6. Navigate to the **Deploy and Validation** dialog box.
7. Select the switches that you want to deploy and then click **Deploy Selected**.
   The **Configuration deployment option** dialog box appears.

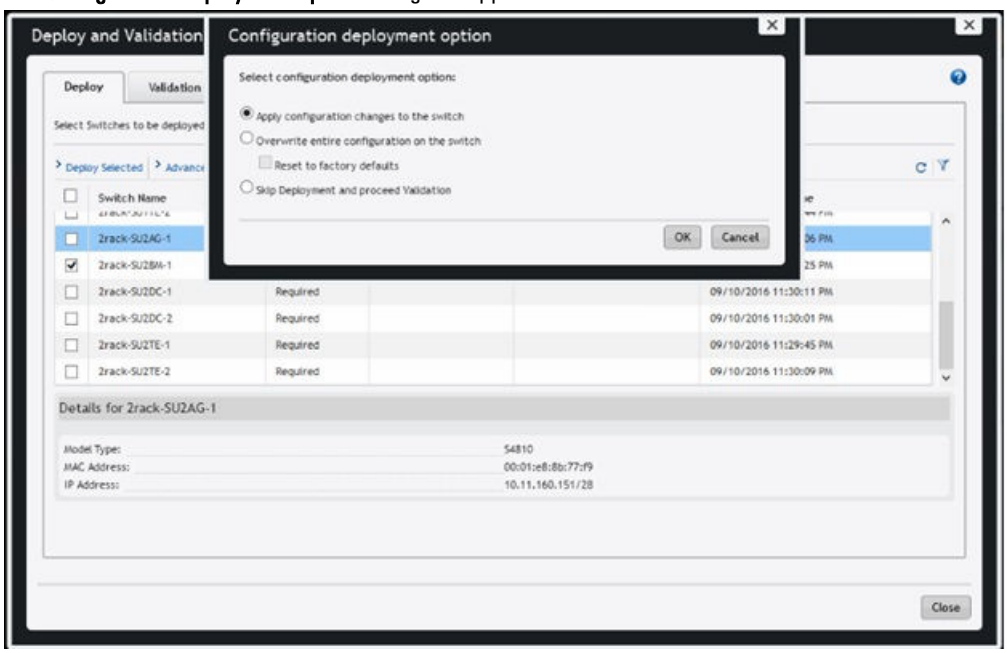

Figure 6. Configuration deployment option Dialog Box

8. Select **Apply configuration changes to the switch.**
9. Deploy remaining switches using the previous steps.

Changing CLI Credentials

You can change the CLI credentials.

1. Navigate to the **SNMP and CLI Credentials** screen of the **Predeployment Configuration** wizard.

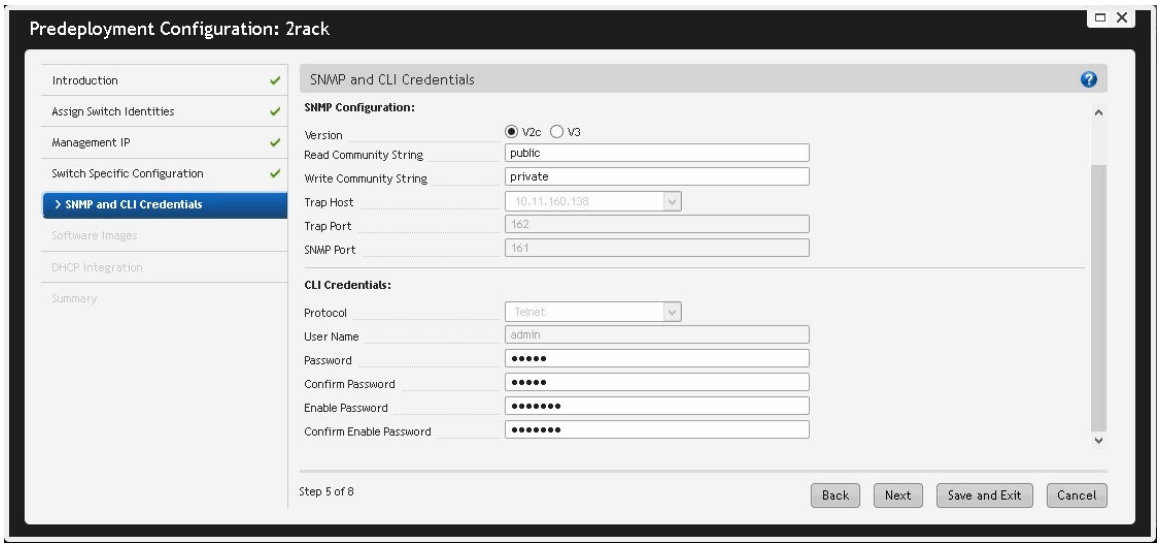

Figure 7. SNMP and CLI Credentials Screen

2. Navigate to the **CLI Credentials** area.
3. Edit any of the following fields as necessary: **Password** and **Confirm Password** or **Enable Password** and **Confirm Enable Password**.
4. Navigate through the remainder of the wizard and click **Finish**.
5. Navigate to the **Deploy and Validation** dialog box.
6. Select the switches that you want to deploy and then click **Deploy Selected**.

   The **Configuration deployment option** dialog box appears.

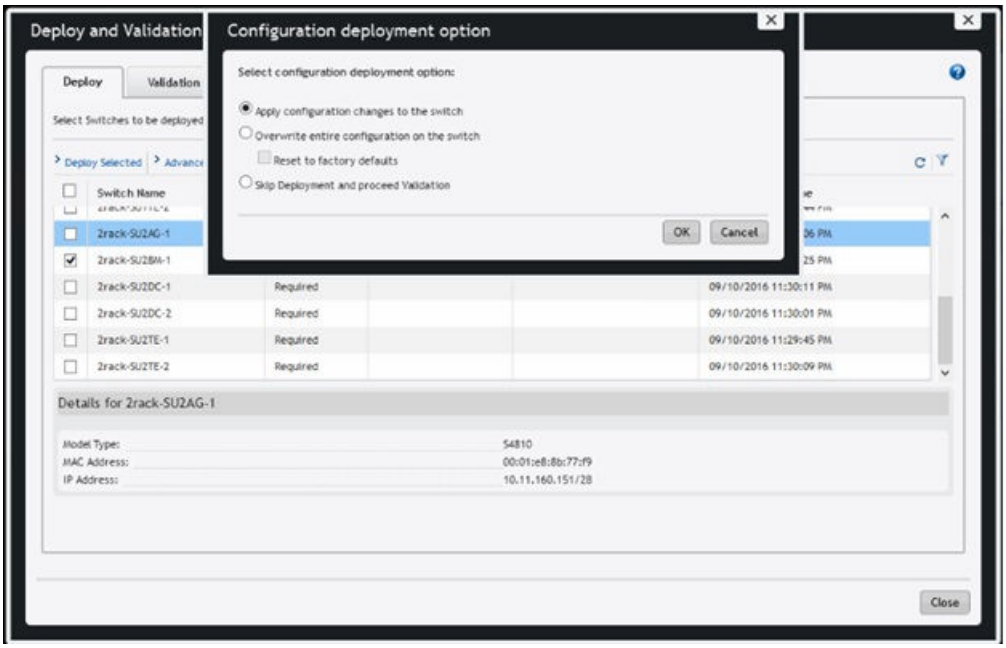

Figure 8. Configuration deployment option Dialog Box

7. Select **Apply configuration changes to the switch.**
8. Deploy remaining switches using the previous steps.

Support Resources

The following support resources are available for AFM-CPS.

Documentation Resources

This document contains operational information specific to Active Fabric Manager for Microsoft Cloud Platform System (AFM-CPS) 2.1(0.0).

For information about using AFM-CPS, see the following documents at http://www.dell.com/support:

- *AFM-CPS 2.1(0.0) Installation Guide*
- *AFM-CPS 2.1(0.0) User Guide*

You can view the AFM-CPS documentation in AFM by selecting the documentation option from the **Help** menu in the AFM user interface.

For more information about hardware features and capabilities, see the Dell Networking website at https://www.dell.com/networking.

For more information about the open network installation environment (ONIE)-compatible third-party operating system, see http://onie.org.

Issues

Issues are unexpected or incorrect behavior and are listed in order of Problem Report (PR) number within the appropriate sections.

NOTE: You can subscribe to issue update reports or use the BugTrack search tool to read current information about open and closed issues. To subscribe or use BugTrack, visit Support at: https://www.force10networks.com/CSPortal20/BugTrack/SearchIssues.aspx.

Finding Documentation

This document contains operational information specific to AFM-CPS.

- For information about using AFM-CPS, see the documents at http://www.dell.com/support.
- For more information about hardware features and capabilities, see the Dell Networking website at https://www.dell.com/networking.
- For more information about the open network installation environment (ONIE)-compatible third-party operating system, see http://onie.org.

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 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:

Go to support.dell.com.