Figure 33: Cabinet Junction Panel

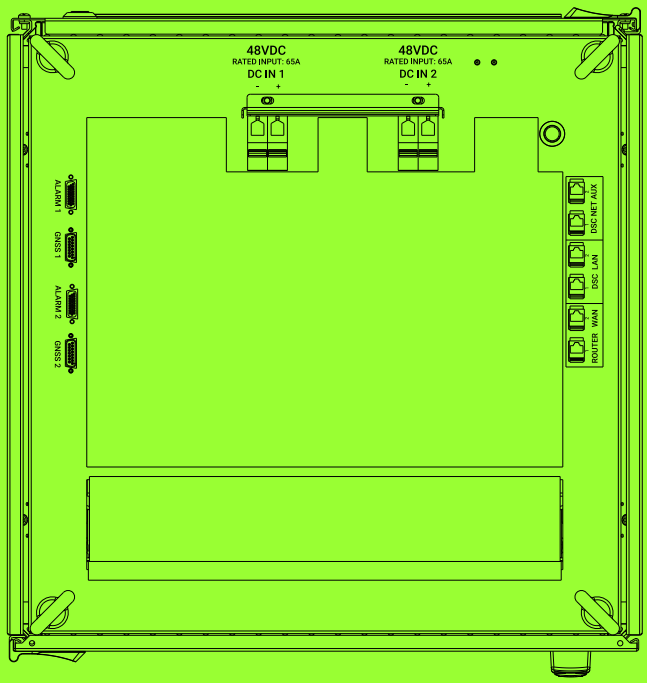


Figure 34: Rack Junction Panel Network Connections

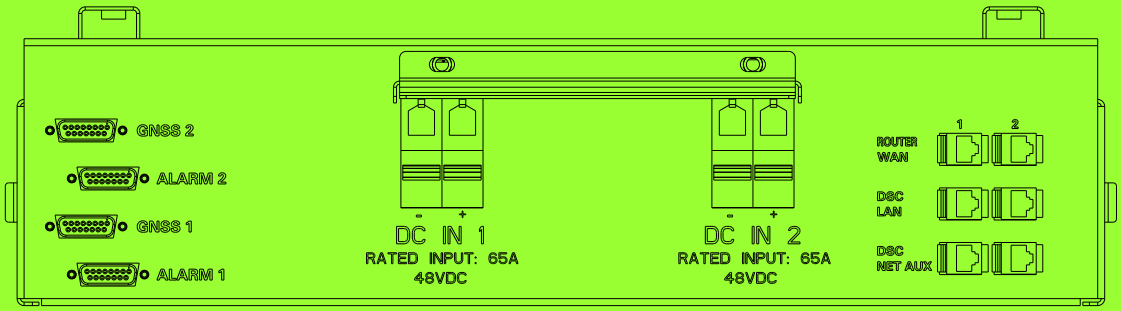
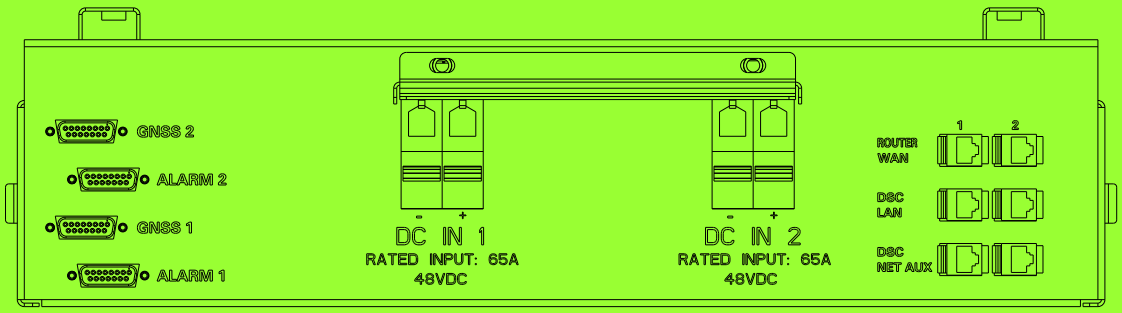


Table 8: Junction Panel Connections Description

Connection	Description
GNSS 1/2	Primary and redundant GNSS Antenna
ALARM 1/2	General-purpose input/output (GPIO) for the primary and redundant DSC 8500
DC IN 1/2	48VDC Power
DSC Net Aux	Net Aux connection for DSC 8500 1 and DSC 8500 2
DSC LAN	Site DSC 8500 to DSC 8500 connections
Router WAN	Edge Router connections

3.6.1
DSC 8500 Network Connections

Figure 35: Junction Panel Network Connections



When installing the DBR M12 MultiCarrier Site, you must ensure that the correct network connections are made at the top of the rack. The connections may differ, depending on whether it is a primary rack or one of the expansion racks. For the connections, you must use Cat5e or higher network cables.

NOTE: The maximum length of network cables connected to the DSC 8500 is 75 meters.

The following table provides information about the configuration.

Table 9: Top of Rack Site Controller Network Connections Configuration

Site Type	Primary DSC LAN 1	Primary DSC LAN 2	Expansion 1 DSC LAN 1	Expansion 1 DSC LAN 2	Expansion 2 DSC LAN 1	Expansion 2 DSC LAN 2
1 Primary	Primary DSC LAN 2	–	–	–	–	–
1 Primary 1 Expansion	Expansion 1 DSC LAN 2	Expansion 1 DSC LAN 1	Primary DSC LAN 2	Primary DSC LAN 1	–	–
1 Primary 2 Expansion	Expansion 2 DSC LAN 2	Expansion 1 DSC LAN 1	Primary DSC LAN 2	Expansion 2 DSC LAN 1	Expansion 1 DSC LAN 2	Primary DSC LAN 1

3.6.2
Optional AC Power Supply Unit Back Panel Connections

Figure 36: AC Power Supply Unit Rear View

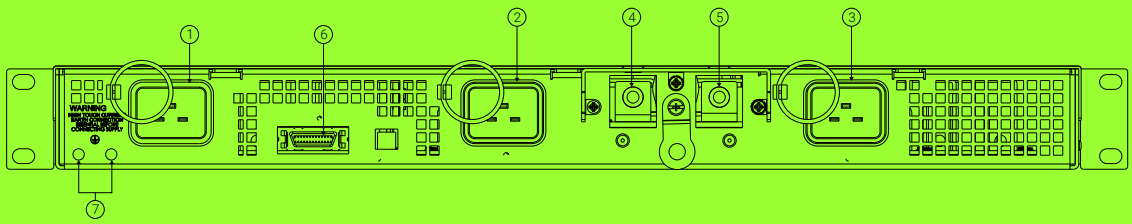


Table 10: Optional AC Power Supply Unit Rear Connections

Annotation	Designator	Description
1	J1	AC input connector
2	J2	AC input connector
3	J3	AC input connector
4	-	DC output
5	+	DC output
6	J16	PSU alarm
7	GND SYMB	Ground studs

3.7

RMC Attenuation Configuration

To adjust the RF gain for the different configuration, you can set the attenuation level applied to receivers from the DIP switches on the front of the Site RMC modules.

Figure 37: Site RMC

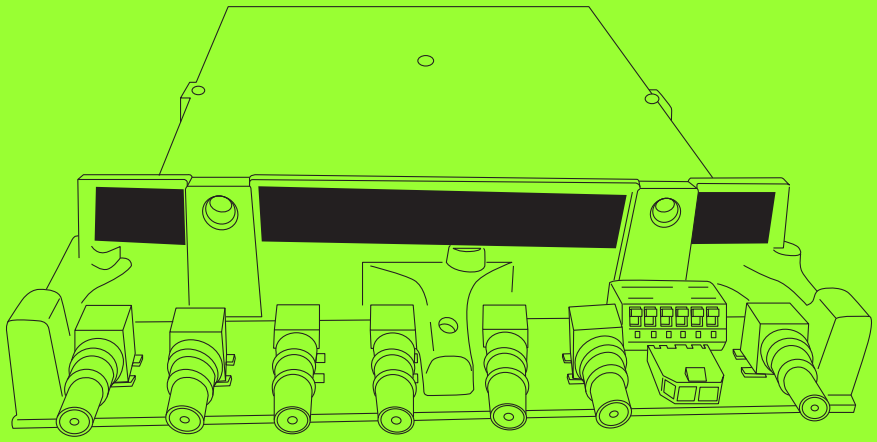
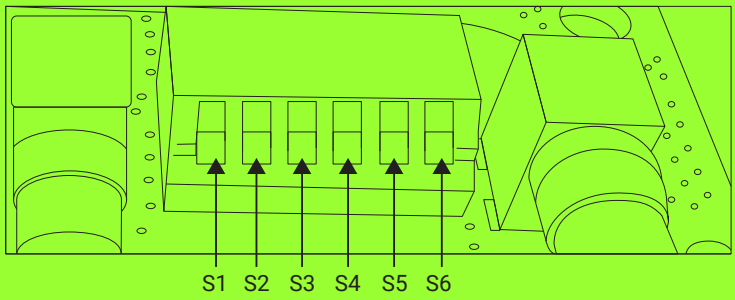


Figure 38: Site RMC DIP Switches



Annotation	Description
S1 – S5	Used to set the binary system dB attenuation values.
S6	Used to set RMC in normal mode or amp bypass mode.

dB Attenuation Values Configuration

The following figures, illustrate how the DIP switch positions (0 and 1) create a binary system for setting dB attenuation values for normal mode.

Figure 39: RMC DIP Switch Example - 0dB in a Normal Mode

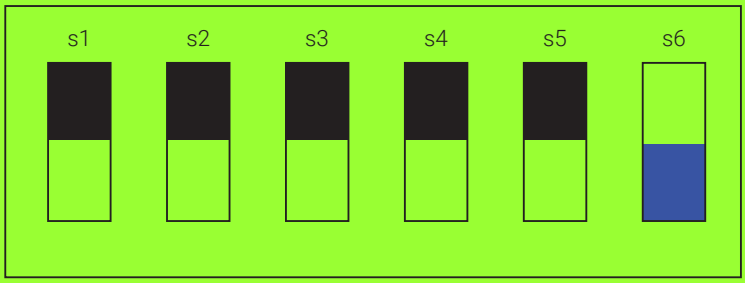


Figure 40: RMC DIP Switch Example - 10dB in a Normal Mode

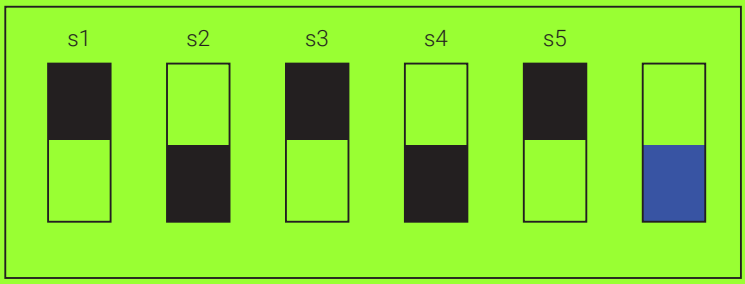
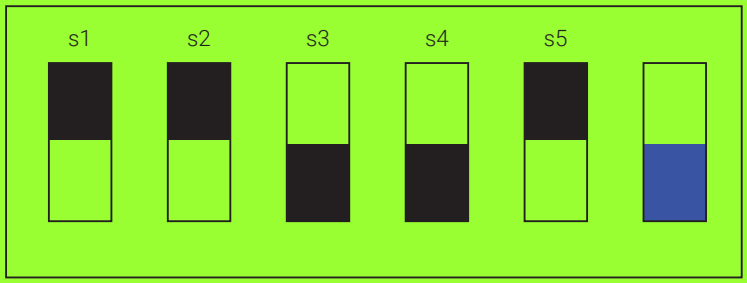
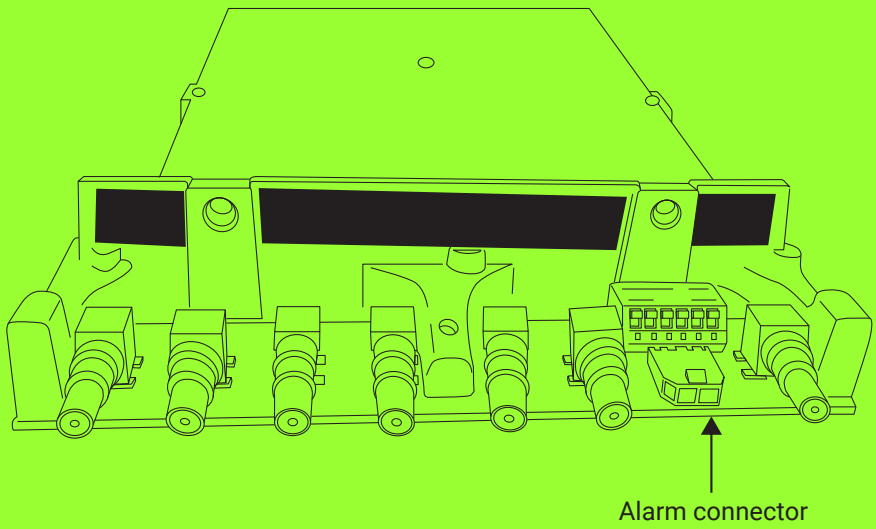


Figure 41: RMC DIP Switch Example - 12dB in a Normal Mode



Site RMC Alarm

Figure 42: Site RMC Alarm Connector Location



Site RMC provides an alarm in the form of relay closure through the alarm connector.

You can turn the RMC alarm on by disconnecting pin 1 and 2.

You can turn the RMC alarm off by connecting pin 1 and 2.

You can connect the Site RMC alarm relay to the DSC 8000/DSC 8500 auxiliary inputs to monitor the RMC alarm.

Chapter 4

On-Premises Software Hub Application

The On-Premises Software Hub application can be used to install, upgrade and recover software on DSC 8500s.

The installation and recovery procedures can be performed from a service laptop connected to the DSC 8500 service port. The upgrade procedure can be performed from the Network Management (NM) Client or a service laptop connected to a DSC 8500.

In some cases recovery procedures can be performed from the NM Client. If hardware failure occurs, recovery must be performed on site with service laptop connected.

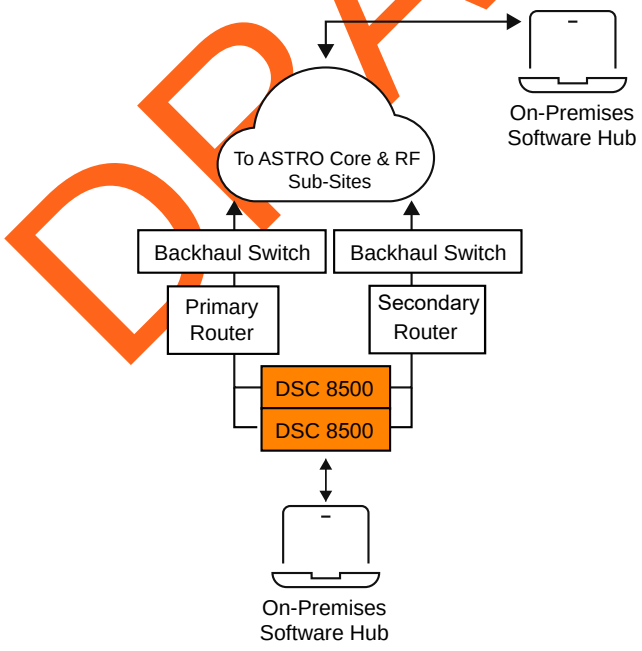
After you launch the On-Premises Software Hub application, you can select one of the following action items:

Bundle Management
Manages software versions and imports a new version into the local On-Premises Software Hub registry.

Device Management
Discovers and manages devices. Prepares and runs site operations (for example, installation or upgrade). Devices are grouped into sites that can also be grouped (for example a PrimeSite and a Subsite belonging to one site).

Task History
Shows the status of tasks that were run from the application.

Figure 43: On-Premises Software Hub at DSC 8500 Trunking RF Site



DRAFT

The On-Premises Software Hub Application can be installed on:

- Service laptop. See Installing On-Premises Software Hub on the Service Laptop on page 71.
- NM Client. See Installing On-Premises Software Hub on the NM Client on page 72.

4.1

Installing On-Premises Software Hub on the Service Laptop

During the installation, On-Premises Software Hub opens the following ports in Windows Defender Firewall so that the local computer and DSC 8500 can communicate with each other.

Table 11: Ports Required to Open in Firewall

Port Range	Used for
TCP 49690, 49714-49722	Connection to local docker registry (HTTPS)
UDP 67	Connection for DHCP traffic
UDP 69	Connection to local TFTP server

Prerequisites:
Obtain:

- Service laptop with minimum 4 GB of RAM and minimum 10 GB of disk space (each imported software bundle requires additional 2.5 GB)
- On-Premises Software Hub installation media
- *Windows Supplemental* media

From the *Windows Supplemental* media, install Motorola Solutions OpenJDK.

NOTE: The Motorola Solutions Password Vault, OpenSSL, and Certificate Generation and Distribution (CGD) packages are recommended to be installed before the installation of On-Premises Software Hub. If these packages are not present, On-Premises Software Hub creates and uses self-signed TLS certificates when connecting to the site.

Procedure:

1. Navigate to the location of the On-Premises Software Hub installation media.
2. Double click the `opsh-version.msi` file.
3. If you are prompted with a warning that the starting of an unrecognized application was prevented, perform the following actions:
   a. Right-click the `opsh-version.msi` file.
   b. Select **Properties**.
   c. Select **Unblock** check box.
   d. Click **Apply**.
4. If the **User Access Control** box appears, click **Yes**.
5. When the installation process completes, verify that the **On-Premises Software Hub** application appears on the desktop.
6. Open **On-Premises Software Hub**.
7. Verify that the version is correct by checking the footer.

DRAFT

4.2

Installing On-Premises Software Hub on the NM Client

Prerequisites:
Obtain the On-Premises Software Hub installation media.

NOTE:
The Motorola Solutions Password Vault, OpenSSL, and Certificate Generation and Distribution (CGD) packages are recommended to be installed before the installation of On-Premises Software Hub. If these packages are not present, On-Premises Software Hub creates and uses self-signed TLS certificates when connecting to the site.

Procedure:

1. Perform one of the following actions:

   NOTE: If the ASTRO 25 system uses Cortex XDR threat prevention on all endpoints, the system does not include a Core Security Management Server (CSMS).

If…	Then…
If the ASTRO 25 system uses Cortex XDR threat prevention on all endpoints,	go to step 3.
If the NM Client uses Trellix threat prevention,	perform the following actions: **a.** Check the CSMS version to ensure that the Network Management (NM) Client has the latest firewall rules. See Verifying CSMS and Windows Supplementary Versions on page 73. **b.** go to step 2.

2. Perform one of the following actions:

If…	Then…
If the CSMS OVF version is CSMS-HB-19.04.06 or later,	go to step 3.
If the CSMS OVF version is earlier than 19.04.06,	perform the following actions: **a.** Import new firewall rules. See Importing New Firewall Rules from CSMS Configuration Media on page 73. **b.** Push updates to endpoints. See Pushing Updates to Endpoints on page 75.

3. Navigate to the location of the On-Premises Software Hub installation media.
4. If the installer does not automatically start, double click the `opsh-version.msi` file.
5. If you are prompted with a warning that the starting of an unrecognized application was prevented, perform the following actions:
   a. Right-click the `opsh-version.msi` file.
   b. Select **Properties**.

DRAFT

   c. Select **Unblock** check box.
   d. Click **Apply**.
6. If the **User Access Control** box appears, click **Yes**.
7. When the installation process completes, verify that the **On-Premises Software Hub** application appears on the desktop.
8. Open **On-Premises Software Hub**.
9. Verify that the version is correct by checking the footer.

4.2.1
Verifying CSMS and Windows Supplementary Versions

Procedure:

1. Log on to the CSMS server.
2. Right-click **Start** and select **Run**.
3. In the **Run** window, enter `regedit`

   The **Registry Editor** window opens.
4. Perform one of the following actions:
   - If you want to verify the CSMS version, in the **Registry Editor** window, navigate to **Computer → HKEY_LOCAL_MACHINE → SOFTWARE → MotorolaSolutions**
     The displayed `OVF Version` is the CSMS version.
   - If you want to verify the CSMS supplementary version in the **Registry Editor** window, navigate to **Computer → HKEY_LOCAL_MACHINE → SOFTWARE → Motorola → Motorola Core Security Management Server**
     The displayed `Version` is the CSMS supplementary version.
   - If you want to verify Windows supplementary version in the **Registry Editor** window, navigate to **Computer → HKEY_LOCAL_MACHINE → SOFTWARE → MotorolaSolutions → AstroCSMS**
     The displayed `AWS_Version` is the Windows supplementary version.

DRAFT

4.2.2
Importing New Firewall Rules from CSMS Configuration Media

Perform this procedure to import the latest configuration to be applied out to endpoints.

CAUTION: Do not perform this procedure unless explicitly told to do so by Centralized Managed Support Operations (CMSO). If you use inappropriate version of the *CSMS Configuration Media*, Trellix ENS will block legitimate traffic throughout your ASTRO system, impacting calls.
ATTENTION: N'effectuez pas cette procédure à moins que le Centre des opérations de soutien centralisé Centralized Managed Support Operations (CMSO) ne vous le demande explicitement. Si vous utilisez une version inappropriée du support de configuration du CSMS, Trellix ENS bloquera le trafic légitime dans tout votre système ASTRO, ce qui aura un impact sur les appels.

Prerequisites:
Obtain the latest *CSMS Configuration Media*.

Procedure:

1. Log on to the CSMS as an administrator.

2. Insert the *CSMS Configuration Media* into the DVD drive.
3. Find the CSMS system release by performing the following actions:
   a. Right-click **Start** and select **Search**.
   b. Type: `regedit`
   c. Select **Run as administrator**.
   d. If the **User Account Control** window appears, click **Yes**.
   e. In the navigation tree, expand **HKEY_LOCAL_MACHINE** → **SOFTWARE** → **MotorolaSolutions**.
   f. Note down the `ovf` version.
4. From the *CSMS Configuration Media*, select one of the following folders:
   - If the `ovf` version contains `07.17` or `07.18`, select the `7.17-7.18` folder.
   - If the `ovf` version contains `19.02`, select the `2019.2` folder.
   - If the `ovf` version contains `19.03`, `19.04`, or `20.01`, select the `2020.1` folder.
5. Copy the folder you selected in step 4 to the desktop.
6. On the desktop, double-click **Launch McAfee ePolicy Orchestrator *<x.x.x>* Console**

   where ***<x.x.x>*** is the version number.
7. Log on to the **Trellix ePolicy Orchestrator Console** with the global administrator account.
8. From the toolbar, click the hamburger menu.
9. From the **Policy** area, select **Firewall Catalog**.
10. On the **Firewall Catalog** page, from the **Item type:** drop-down list, select **Rule**.
11. In the **Firewall Catalog** page, for **Catalog items:** select **Import**.
12. Click **Browse** and navigate to the folder that was copied to the desktop.
13. Navigate to: ***<release_folder>***`/XML_HB/Base/ENS Firewall Rules/Rule.xml`
14. Click **Open**.
15. Click **OK**.

    After some time a new window appears with your Review Affected Objects.
16. Click **OK**.

    The import of the Rules takes some time. When prompted with a pop-up window warning about the session timeout, you must click **OK**. After the import succeeds, you are returned to the **Firewall Catalog** page.
17. In the **Firewall Catalog**, from the **Item type:** drop-down list, select **Group**.
18. On the **Firewall Catalog** page, for **Catalog items:** select **Import**.
19. Click **Browse** and navigate to the folder that was copied to the desktop.
20. Navigate to: ***<release_folder>***`/XML_HB/Base/ENS Firewall Rules/Group.xml`
21. Click **Open**.
22. Click **OK**.

    After some time a new window appears with your Review Affected Objects.

DRAFT

23. Click **OK**.

    The import of the Groups takes some time. After the import succeeds, you are returned to the **Firewall Catalog** page.

24. From the toolbar, click the hamburger menu.
25. From the **Policy** area, select **Policy Catalog**.
26. From **Products**, select **Endpoint Security Firewall**.
27. Click the down arrow next to **New Policy** and select **Import**.
28. Click **Browse** and navigate to the folder that was copied to the desktop.
29. Navigate to: ***<release_folder>***`/XML_HB/Base/ENS Firewall Rules/Policies_For_Endpoint_Security_Firewall.xml`
30. Click **Open**.
31. Click **OK**.

    A review of conflicting policies appears. The Policies in red and marked in conflict will overwrite the existing policy and this is the required result.

32. Click **OK**.

    The import takes some time. After it succeeds, the import of new Firewall Rules completes and you are returned to the **Policy Catalog** page. The rules are updated on the endpoint the next time the endpoint communicates with the CSMS server.

33. If you want to force the update of the rules on the endpoint, perform Pushing Updates to Endpoints on page 75.

4.2.3
Pushing Updates to Endpoints

After the import of new Firewall Rules, it takes up to 30 minutes to update policies on endpoint. Perform this procedure to push policy updates to specific endpoints without waiting for an endpoint to communicate with the CSMS server.

Procedure:

1. Log on to the CSMS as an administrator.
2. On the desktop, double-click **Launch McAfee ePolicy Orchestrator *<x.x.x>* Console**

   where ***<x.x.x>*** is the version number.

3. Log on to the **Trellix ePolicy Orchestrator Console** with the global administrator account.
4. From the toolbar, click the hamburger menu.
5. From the **System Section** area, select **System Tree**.
6. Select the **System** tab.
7. In the **Preset** field, from the drop-down list, select **This Group and All Subgroups**.
8. Scroll down to navigate to the managed system that you want to update policies for and select the check box for the appropriate system.
9. Select **Actions** → **Agent** → **Wake Up Agents**.
10. In the **Force policy update** section, from the **Wake Up McAfee Agent** window, select **Force complete policy and task update**.

DRAFT

11. Click **OK**.

    The Agent wakes up in the next several seconds and pushes the updated policies.

12. Ensure that the **Agent Wake Up** took place by checking the **Last Communication time** in the **System Tree**.

    If the **Last Communication time** is updated, the policy was updated.

4.3

Importing the DSC 8500 Software Bundle

During the Software Bundle import, On-Premises Software Hub copies the installation scripts from the *DSC 8500 Software Installation* media and imports all DSC 8500 applications to its internal Docker Registry.

Prerequisites:
Obtain:

- The latest version of On-Premises Software Hub.
- The *DSC 8500 Software Installation* media.

Procedure:

1. Perform one of the following actions:
   - If you use an `.iso` image to import the Software Bundle, navigate to its location,right-click it, and select **Mount**.
   - If you use the *DSC 8500 Software Installation* media, insert it into the optical drive of the service laptop.
2. Select **Bundle Management** tab.
3. Click **Import Bundle**.
4. Navigate to the directory with the Software Bundle.
5. Select `manifest.json` file and click **Open**.

   After the software bundle is imported, a new entry appears in the Bundle's table.

6. Perform one of the following actions:
   - Unmount the imported Software Bundle `.iso` image by right-clicking it and selecting **Eject**.
   - Remove the *DSC 8500 Software Installation* media.
7. If you want to delete unnecessary software bundles, in the **Bundle Management** tab, click the trash icon next to the bundle you want to delete.

4.4

Discovering the Site

Prerequisites:
Ensure that:

- You use the latest version of On-Site Premises Software Hub.
- You imported the software bundle. See Importing the DSC 8500 Software Bundle on page 76.

Procedure:

1. Launch the On-Premises Software Hub.

DRAFT

2. Select the **Device Management** tab.
3. Click **Discover**.
4. In the **Device Discovery** window, enter zone and optional site numbers.

   NOTE: If the site field is left blank, the discovery process attempts to discover all available sites for the zone number entered.

5. Click **Start Discovery**.

   NOTE: If the site field was left blank, the process of scanning the whole zone may take up to 10 minutes.

6. If the site does not show the correct number of DSC 8500s after the discovery, perform the following actions:
   a. Check the fault status for each DSC 8500 in PCA or UEM.
   b. Verify that each DSC 8500 is enabled.
   c. Verify that the configuration of ports between DSC 8500s and routers are correct.

4.5 Connecting to the Site

The connection to the site is required prior to most site operations. It uses the SSH protocol to establish trust between the local host and the DSC 8500 host.

Prerequisites:
Ensure that:

- You use the latest version of On-Premises Software Hub.
- You discovered the site. See Discovering the Site on page 76.

Procedure:

1. Select the **Device Management** tab.
2. Select the site you want to connect to and click **Connect**.

   The **Connection** window with the user name and password prompt appears.

3. At the prompt, enter the domain (Active Directory) or local admin credentials for the DSC 8500.
4. To use the same credentials when connecting to other devices on the site, select the **Reuse credentials for other devices** check box.
5. If you connect for the first time, when prompted, accept a fingerprint key and host key. For details on the list of trusted hosts, see Managing Trusted Hosts List on page 78.

   To accept a new key fingerprint without prompting, Select the **On first, connection automatically accept SSH keys** check box

6. Click **Connect**.
7. If the connection to the DSC 8500 fails with a connection timeout message, perform one of the following:
   - Check the network connection to the DSC 8500 and click **Connect** to retry connection.
   - Connect to the next device in the site, by clicking **Skip**.

   If any of the sites was skipped after the last DSC 8500 connected, you have to click **Cancel** for the connect windows to disappear.

DRAFT

8. If the connection to the DSC 8500 fails with bad credentials message, perform one of the following actions:
   - Correct the credentials provided for the DSC 8500 and click **Connect** to retry connection.
   - Connect to the next device in the site, by clicking **Skip**.

   If any of the sites was skipped after the last DSC 8500 connected, you must click **Cancel** for the connect windows to disappear.

4.6

Managing Trusted Hosts List

During the first connection from On-Site Premises Software Hub to a site, key fingerprints of the DSC 8500 are displayed and they must be validated and accepted by the user. To increase security, it is possible to share or reuse a list of known and safe hosts between different machines on which On-Premises Software Hub is installed.

Procedure:

1. Navigate to `%USERPROFILE%\.ssh\known_hosts`
2. Copy the file.
3. Paste the copied file at the same location on another machine.

4.7

Site Actions

Actions are launched in the **Devices Management** view by using the **Actions** menu which is visible for each of the discovered sites. The exception is the **Initial Deployment** action, for which there is a separate **Install** button.

The **Actions** menu is inactive until you connect to the site. See Connecting to the Site on page 77. Depending on the state of the site, the list of available actions may be different.

There is a limit of 10 concurrently running, non-installation actions. After that limit is reached, new actions are queued.

Until the installation for one site is complete, it is not possible to start the installation for another site.

Actions can be stopped at any time by using the **Cancel** button.

NOTE: Interrupting the action is not recommended and may leave the devices in faulty state.

Java may be blocked by Windows Defender Firewall rule. In this case, a warning appears at the top of the **Action parameters** window. A manual change in Windows Defender Firewall is required before continuing.

4.8

Collecting Action Logs

For each operation, On-Premises Software Hub collects and stores application logs. Logs of completed tasks can be downloaded in the **Task History** view. Additionally, logs from recently completed operations can be downloaded by using the button visible on the right side of the of progress bar in the **Device Management** view.

Procedure:

1. Select the **Task History** tab.

DRAFT

2. Click **Download Logs** for selected tasks.
3. Select the destination and click **Save**.

DRAFT

Chapter 5

Provisioning and Configuration Agent Application

Provisioning and Configuration Agent (PCA) is a web interface for local configuration, status reporting and managing a site.

The PCA application can be used to perform the following actions:

- Configure operating parameters for infrastructure devices.
- Retrieve status and operational information from a device.
- Perform device configuration and servicing tasks through a direct Ethernet connection to the device or over the LAN from the Network Management subsystem.

5.1 PCA Users

Two predefined user accounts are available when you log on to the Provisioning and Configuration Agent (PCA) for the first time:

- **admin**
- **config**

They have initial passwords which you must change during the first login.

The **admin** user can perform the following actions:

- Add and delete local users
- Configure the existing local user accounts
- Configure Account Policies
- Configure security settings for SNMP Config and LDAP
- Define the custom login banner
- Configure a remote syslog server
- Set passwords for DSC 8500 logs

The **admin** user has access to the following menus:

- **Users Management**
- **Security Settings**
- **Configuration**
- **Help**

User management operations performed by the **admin** user are logged in the local `syslog` file and forwarded to the remote syslog server, if configured.

The **config** user can configure and modify the existing site parameters.

The **config** user has access to the following menus:

- **Configuration**
- **Pending Changes**

DRAFT

- **Export & Import**
- **Services**
- **Help** (includes the version information)

You can assign one of three roles to local users:

- **Network Security Administrator** with the **admin** account privileges
- **System Infrastructure Administrator** with the **config** account privileges
- **System Infrastructure Operator** with read-only access to the site configuration

5.2

Logging On to the PCA for the First Time

When you log on to the Provisioning and Configuration Agent (PCA) for the first time, you must change the predefined password following the rules of the password policy.

The password policy:

- Minimum password length: 15
- Minimum lowercase letters: 1
- Minimum uppercase letters: 1
- Minimum numeric digits: 1
- Minimum non-alphanumeric characters: 1 [!@#$%^&<>()+-=]
- Minimum changed characters: 8
- Password reuse history: 5
- Minimum password age: [day] 1
- Maximum password age: [day] 60

Prerequisites:
Obtain:

- Service laptop or the Network Management (NM) Client
- IP address or the host name of the DSC 8500. See Logon Information.
- *MSI CA Certs* package from *ASTRO Windows Supplemental* media
- Credentials for predefined admin or config users

Install the *MSI CA Certs* package on the service laptop to avoid certificate trust warnings from the web browser.

Procedure:

1. In the address bar of a web browser, enter one of the following:
   - IP address of your DSC 8500
   - Host name of your DSC 8500
2. Provide credentials for one of two predefined users.
3. Click **Log in**.
4. In the **Password** field, enter the password assigned to the predefined account you use.
5. In the **New password** field, enter your new password.

   The new password must meet the rules defined in the PCA Password Policy.

DRAFT

6. In the **Confirm new password** field, enter your new password.
7. Click **Update password and log in**.

   If your password does not follow the Password Policy rules, a message specifying the required changes appears.

5.2.1
Resetting SNMPv3 Passphrases to Default on DSC 8500

You can use this procedure to reset the SNMPv3 configuration in the Provisioning and Configuration Agent (PCA) if the configured SNMPv3 passphrases are lost.

Prerequisites:
Obtain:

- Service laptop or the Network Management (NM) Client
- IP address or the host name of the DSC 8500. See Logon Information.
- Credentials for the **Network Security Administrator** account

Install the *MSI CA Certs* package on the service laptop to avoid certificate trust warnings from the web browser.

Procedure:

1. In the address bar of a web browser, enter one of the following:
   - IP address of your DSC 8500
   - Host name of your DSC 8500
2. Log on to the PCA as the **Network Security Administrator**.
3. From the main menu bar, select **Security Settings**.
4. From the **Security Settings** drop-down list, select **SNMP Configuration**.
5. In the **SNMP Users** view, select **Factory Defaults** and set the **Redefault USM and VACM?** flag to active.
6. Click **Submit**.

DRAFT

5.2.1.1
Logon Information

DSC 8500 ASR Site

The IP address can be obtained from the following IP scheme:

`10.<Zone_no+100>.<Site_no>.<DSC>`

where:

<Zone_no> = Zone Number
<Site_no> = Site Number
<DSC> = DSC 1 = 228, DSC 2 = 229, DSC 3 = 230, DSC 4 = 231, DSC 5=232, DSC 6 = 233

The host name scheme can be obtained from the following host name scheme:

`z<zzz>s<sss>rfe<HH>.site<ss>.zone<z>`

where:

<zzz> is the Zone number, 1-7, 3 digit zero padded

<sss> is the RF Site number 1- 150, 3 digit zero padded
<HH> is the instance number used in host names and aliases, 2 digit zero padded
<ss> is the RF Site number 1- 150, 2 digit zero padded
<z> is the Zone number, 1-7

Example: `z001s001rfe01.site01.zone1`

DSC 8500 Subsite

The IP address can be obtained from the following IP scheme:

`101110ZZ.ZZZZZPPP.PPPSSSSS.SHHHHHHH`

where:

`ZZZZZZZ` = Zone Number
`PPPPPP` = Site Number
`SSSSSS` = Subsite Number
`HHHHHHH` = DSC 1 = 1101000 (104), DSC 2 = 1101001 (105), DSC 3 = 1101010 (106), DSC 4 = 1101011 (107), DSC 5 1101100 (108), DSC 6 = 1101101 (109)

The host name can be obtained from the following host name scheme:

`z{ZZ}ips{PP}s{RR}rfe{H}. ipss{subsite}.site{prime}.zone{zone}`

where:

<ZZ> is the Zone number, 1-7, 2 digit zero padded
<PP> is the RF Site number 1-64, 2 digit zero padded
<RR> is the IP Subsite number 1-64, 2 digit zero padded
<H> is the instance number used in host names and aliases, 1 digit zero padded
<subsite> is the IP Subsite number 1- 64, 2 digit zero padded
<prime> is the Prime Site number 1-64, 2 digit zero padded
<zone> is the Zone number, 1-7

Example: `z01ips01s01rfe1.ipss01.site01.zone1`

DRAFT

5.3
Setting Up PCA Users and Passwords

You can use this procedure to set up users and passwords in the Provisioning and Configuration Agent (PCA).

Prerequisites: Obtain:

- Service laptop or the Network Management (NM) Client
- IP address or the host name of the DSC 8500. See Logon Information.
- Credentials for the **Network Security Administrator** account

Procedure:

1. In the address bar of a web browser, enter one of the following:
   - IP address of your DSC 8500
   - Host name of your DSC 8500
2. Log on to the PCA as the **Network Security Administrator**.
3. From the main menu bar, select **Users Management**.

4. In the **Users Management** view, click the icon.
5. In the **New User** view, perform the following actions:
   a. In the **Login name** field, enter the user name.
   b. In the **Password** field, enter the user password.
   c. In the **Confirm password** field, confirm the user password.
   d. In the **Account locked** position, if you want to lock the user account, set the flag active.
   e. In the **Password change required** position, if you want to force the password change at the first login, set the flag active.
   f. In the **Roles** field, from the list of available roles, select the role of the user.
   g. Click **Submit**.

DRAFT

Chapter 6

DSC 8500 Trunking RF Site Configuration

6.1

Deploying the DSC 8500 Software

You can deploy the DSC 8500 software by using On-Premises Software Hub.

Prerequisites:
Obtain:

- Service laptop connected to the DSC 8500 service port
- DSC 8500 installation media

Procedure:

1. From the desktop, launch the **On-Premises Software Hub** application.
2. Import the DSC 8500 software bundle. See Importing the DSC 8500 Software Bundle on page 76.

DSC 8500 Software Installation

3. Select **Device Management** tab.
4. Enable PXE support by performing the following actions:
   a. Click **Menu**.
   b. Select **Settings**.
      The **Settings** window appears.
   c. Select **Enable PXE**.
   d. Click **OK**.
      The **Install** icon becomes active.
5. Manually assign IP addresses by performing the following actions:
   a. From the Windows start menu, select **Settings**.
   b. Click **Network and Internet**.
   c. In the navigation pane on the left, click **Ethernet**.
   d. Select the Ethernet connection used to connect to the DSC 8500.
   e. Scroll down to the **IP settings** and click **Edit**.
   f. From the **Edit IP settings** drop-down list, select **Manual**.
   g. From the **DSC ID** drop-down lists, select the numbers of DSC 8500s corresponding to the listed MAC addresses.
      The MAC address of the server is available in the upper left corner of the DSC 8500 front panel lip.
   h. Enable **IPv4**.
   i. Fill out **IP address** and **Subnet prefix length**.

DRAFT

IP addresses reserved for a service laptop in an ASR Site are `10.<Zone_no+100>.<Site_no>.<X>`, where `<X>` values from 236 to 239.

The subnet prefix is 24.

IP addresses reserved for a service laptop in a subsite are `101110ZZ.ZZZZZPPP.PPPSSSSS.SHHHHHHH`, where `HHHHHHH` values from 0110011 (51) to 0110111 (55).

NOTE: The IP address is represented in binary form.

The subnet prefix is 25.

j. Click **Save**.

6. Click **Install**.
7. In the **Initial Deployment** window perform the following actions:
   a. From the **Bundle** drop-down list, select the software bundle you want to install.
   b. From the **Site Type** drop-down list, select the type of your site.
   c. In the **Zone ID** field, enter the zone number.
   d. In the **Site ID** field, enter the site number.
   e. In the **Subsite ID** field, if applicable, enter the subsite number.
   f. Check the boxes for the DSC 8500s you want to install.
   g. From the **DSC ID** drop-down lists, select the numbers of DSC 8500s corresponding to the listed MAC addresses.

      In case of disaster recovery of one DSC 8500, you may indicate one DSC 8500.
   h. Click **Continue**.

      The DSC 8500 software installation process starts.

   NOTE: Until the installation for one site is complete, it is not possible to start the installation for another site.
8. Verify security configuration. See Verifying the DBR M12 MultiCarrier Site Security Configuration on page 126.
9. If you want to download installation logs, see Collecting Action Logs on page 78.

DRAFT

6.2 Configuring SNMPv3 Passphrases on DSC 8500 for MotoAdmin Account

When operating in AuthPriv mode, SNMPV3 passphrases are used to generate the necessary authentication and encryption keys for SNMPv3 communication between managers (such as UNC) and agents (like the DSC 8500). The MotoAdmin credentials protect the SNMPv3 communications path by which the manager can set and change the security level and passphrases for the agent's other SNMPv3 USM accounts.

For all user accounts with a security level that supports authentication, the SNMPv3 passphrases should be changed periodically. This includes MotoAdmin and other SNMPv3 USM accounts. The time period between passphrase changes is determined by system policy - contact your system administrator for guidance.

Prerequisites:

Ensure that credentials for new and current MotoAdmin accounts are added in the Unified Network Configurator (UNC). See "Adding Global Credentials in the VMware Smart Assurance Network Configuration Manager" in the *Unified Network Configurator User Guide*.

Procedure:

Changing the current SNMPv3 credentials for MotoAdmin account

1. Log on to the VMware Smart Assurance Network Configuration Manager.
2. In the left navigation pane of the VMware Smart Assurance Network Configuration Manager dashboard, select **Networks** → **Astro 25 Radio Network** → **Devices**.
3. Right-click the **DSC 8500 NM Agent** device on the right side of the window and select **Properties**.
4. In the **Device Properties** window, select the **Communication** tab.
5. Click **Update Credentials**.
6. In the **Update Credentials** window, select **In-Band** tab.
7. In the **SNMPv3** section, select the current MotoAdmin SNMPv3 credential and check the **Active** box.
8. Click **Save only**.
9. Right-click the **DSC8000 NM Agent** device on the right side of the window and select **Properties**.
10. In the **Device Properties** window, select the **Communication** tab.
11. Click **Update Credentials**.
12. In the **Update Credentials** window, select **In-Band** tab.
13. In the **SNMPv3** section, select the new MotoAdmin SNMPv3 credential.
14. For the new MotoAdmin SNMPv3 credential, check the **Active** box.
15. Click **Schedule**.

    The **Schedule Push Job** window appears.
16. Type the job name and schedule the job.
17. Click **Approve & Submit**.

    Clicking **Approve & Submit** closes the Schedule Job window and the job status can be viewed by using Schedule Manager available from the **Tools** menu on the VMware Smart Assurance Network Configuration Manager main window.

Restoring MotoMaster account credentials in UNC

18. Right-click the **DSC8000 NM Agent** device on the right side of the window and select **Properties**.
19. In the **Device Properties** window, select the **Communication** tab.
20. Click **Update Credentials**.
21. In the **Update Credentials** window, select **In-Band** tab.
22. In the **SNMPv3** section, select the current MotoMaster SNMPv3 credential.
23. For the new MotoMaster SNMPv3 credential, check the **Active** box.
24. Click **Save only**.
25. Right-click the **DSC8000 NM Agent** device on the right side of the window and select **Test Credentials**.
26. In the **Schedule Push Job** window, click **Approve & Submit**.
27. Verify that the scheduled job completed successfully:
    a. Open the schedule manager by pressing F7.

DRAFT

b. Sort the list by ascending job ID by clicking **Job ID** until an upward-pointing arrow appears.

c. Verify that the job is the top job on the list, select the job and verify that the target device is listed in the task list.

d. Verify the job completes without an error. The schedule manager will need to be refreshed manually by hitting F5 periodically.

   You need to refresh the schedule manager manually by hitting F5 periodically.

6.3 Configuring SNMPv3 Passphrases on DSC 8500 for Other USM Accounts

You can use this procedure to change current SNMPv3 credentials to new SNMPv3 AuthPriv credentials. Rolling credentials to NoAuthNoPriv or AuthNoPriv are not supported.

You can reset SNMP credentials to NoAuthNoPriv by performing Resetting SNMPv3 Passphrases to Default on DSC 8500 on page 82.

Procedure:

1. Log on to the VMware Smart Assurance Network Configuration Manager.
2. In the left navigation pane of the VMware Smart Assurance Network Configuration Manager dashboard, select **Networks** → **Astro 25 Radio Network** → **Devices**.
3. Right-click the DSC 8500 NM Agent device on the right side of the window and select **Saved Commands**.

   The **Select Item** dialog box appears.
4. Click the folder icon at the top of the dialog box, to the right of the **Look In** field. Continue to click this icon until the `System` folder displays on the list of folders, in the **Select Item** dialog box.
5. In the **Select Item** dialog box, go to **System** → **Motorola** → **SNMPv3**.

   A list of saved commands displays in the **Select Item** dialog box.
6. Select **Change SNMPv3 Users From Clear to AuthPriv**.
7. In the **Template Variable Substitution** dialog box, perform the following actions:

   a. Enter new newAuthPass and newPrivPass.

      NewAuthPass and newPrivPass - are the passphrases to be used for MotoMaster and MotoSWDL snmpv3 accounts on the device after this change

   b. Enter current adminAuthPass and adminPrivPass.

      AdminAuthPass and adminPrivPass are the passphrases currently configured on the device for MotoAdmin SNMPv3 account.

   c. Select the desired **targetInformUser**.

   d. Click **OK**.

   When successful, MotoMaster, MotoSWDL and selected Inform user accounts use new credentials.
8. Right-click the DSC 8500 NM Agent device on the right side of the window and select **Properties**.
9. In the **Device Properties** window, select the **Communication** tab.
10. Click **Update Credentials**.
11. In the **Update Credentials** window, select **In-Band** tab.

DRAFT

12. In the **SNMPv3** section, select the MotoMaster SNMPv3 account configured with new passphrases.
13. Check the **Active** box.
14. Click **Save only**.
15. Right-click the DSC 8500 NM Agent device on the right side of the window and select **Test Credentials**.
16. In the **Schedule Push Job** window, click **Approve & Submit**.

6.4 Setting up the Account Policies

You can use this procedure to configure password settings, define the values for maximum failed logon attempts, the account lockout duration in the Provisioning and Configuration Agent (PCA).

Prerequisites:
Obtain:

- Service laptop or the Network Management (NM) Client
- IP address or the host name of the DSC 8500. See Logon Information.
- Credentials for the **Network Security Administrator** account

Procedure:

1. In the address bar of a web browser, enter one of the following:
   - IP address of your DSC 8500
   - Host name of your DSC 8500
2. Log on to the PCA as the **Network Security Administrator**.
3. From the main menu bar, select **Security Settings**.
4. From the **Security Settings** drop-down list, select **Account Policies**.
5. In the **Account Policies list** view, select the account policies entry and click the icon.
6. In the **Edit Account policies** view, expand the **Password Complexity** node and define the values for the password settings.
7. In the **Edit Account policies** view, expand the **Account Lockout** node and define the values for maximum failed login attempts and the account lockout duration.
8. Click **Submit**.

6.5 Configuring the Login Banner

You can use this procedure to configure the login banner for the Linux platform, and Provisioning and Configuration Agent (PCA) web UI.

Prerequisites:
Obtain:

- Service laptop or the Network Management (NM) Client
- IP address or the host name of the DSC 8500. See Logon Information.
- Credentials for the **Network Security Administrator** account

DRAFT

Procedure:

1. In the address bar of a web browser, enter one of the following:
   - IP address of your DSC 8500.
   - Host name of your DSC 8500.
2. Log on to the PCA as **Network Security Administrator**.
3. From the main menu bar, select **Security Settings**.
4. From the **Security Settings** drop-down list, select **Login Banner**.
5. Enter the required Login Banner in the text box and select **Apply**.
6. To use the default Login Banner, select **Default** and **Apply**.
7. To undo any changes that are not applied, select **Revert**.

6.6

Configuring Centralized Authentication for PCA Users

DRAFT

You can use this procedure to configure Centralized Authentication in the Provisioning and Configuration Agent (PCA).

Users must be added to the system level dsc-provagent-login Active Directory group as well as one of the following system level role based groups.

Table 12: Active Directory Groups

System Level Group	PCA Access
dsc-provagent-secadm	Network Security Administrator manages local user accounts and security feature configuration.
dsc-provagent-infradm	System Infrastructure Administrator has read and write access to the DSC 8000/DSC 8500 configuration including the switch.
dsc-provagent-confgaud, dsc-provagent-infrsup	System Infrastructure Operator has read-only access to the DSC 8000/DSC 8500 configuration.
dsc-provagent-rftestoper	RF Coverage Test Operator account used to run RF coverage tests.
dsc-provagent-votingoper	Channel Voting Operator with read/write access to **Channel Voting Status** view.

You can configure up to five Lightweight Directory Access Protocol (LDAP) servers for Centralized Authentication. The number of available servers depends on the system configuration. An ASTRO® 25 system has two LDAP servers. Two more LDAP servers are available with DSR and one more is available for Tsub.

Table 13: LDAP Server Configuration

Order	Non-DSR	DSR
1	z<zzz>dc01.zone<z>	z<zzz>dc01.zone<z>
2	TSUB DC[1)]	TSUB DC[1)]

Order	Non-DSR	DSR
3	ucs-dc01.ucs	ucs-dc01.ucs
4	NA	z<zzz>dc03.zone<z>
5	NA	ucs-dc03.ucs

<zzz> is the Zone number, 1-7, 3 digit zero padded

<z> is the Zone number, 1-7

[1] Only configured if the site device is present in a Tsub.

Prerequisites:

CAUTION: The PCA application does not support SSO authentication, therefore AD User Smart Card enabled account is not able to log on to the PCA application. Possible solution is to temporarily enable password based authentication for the AD user account to enable service access to the PCA Application. You must revert back the Smart Card MFA authentication after post hardware services operations are completed.

ATTENTION: L'application PCA ne prend pas en charge l'authentification SSO. Ainsi, les comptes pour lesquels les cartes de connexion sur carte à puce AD sont activées ne peuvent pas se connecter à l'application PCA. Une solution possible est d'activer temporairement l'authentification par mot de passe pour le compte utilisateur AD afin d'activer l'accès par le service à l'application PCA. Vous devrez revenir à l'authentification multifacteurs par carte à puce une fois que les opérations des services matériels sont terminées.

Obtain:

- Service laptop or the Network Management (NM) Client
- IP address or the host name of the DSC 8000/DSC 8500. See Logon Information.
- Credentials for the **Network Security Administrator** account

Verify that the PCA active directory groups listed above are present on the Domain Controller. If not present, create them on the Domain Controller (DC) by performing "Adding Groups to a Domain" in *Authentication Services Feature Guide*. Assign roles to groups based on the last part of the group name. For example, the dsc-provagent-secadm group should be assigned the secadm system role.

Procedure:

1. In the address bar of a web browser, enter one of the following:
   - IP address of your DSC 8000/DSC 8500
   - Host name of your DSC 8000/DSC 8500
2. Log on to the PCA as the **Network Security Administrator**.
3. From the main menu bar, select **Security Settings**.
4. From the **Security Settings** drop-down list, select **LDAP Configuration**.
5. In the **LDAP Configuration list** view, select the LDAP you want to configure and click the icon.
6. In the **Edit LDAP Configuration** view, provide a domain, host name and port for the LDAP servers in your system, according to Table 13: LDAP Server Configuration on page 90.
7. Click **Submit**.
8. Log off from the PCA and log on as the **Network Security Administrator**.
9. Remove all local shared users by performing the following actions:
   a. From the main menu bar, select **User Management**.

DRAFT

b. In the **User Management** view, select all users.

c. Click the icon.

6.7

Verifying the Version of the Installed DC Plugin

If a Domain Controller (DC) Plugin on DCs is installed by using the version listed in the table (or later), the system is ready to use DSC 8000s and no corrective action is needed. If the installed version of the DC Plugin is not the same or newer than the ones listed in the following table, you must update the DC Plugin.

Table 14: DC Plugin Versions

Release	DC Plugin Version
2022.1, 2022.HS and later	12.00.57 or later
2020.1 and later	ADC_R11.00.89

Procedure:

1. Log in to the Domain Controller.
2. Run `regedit.exe`
3. Navigate to `HKEY_LOCAL_MACHINE\Software\Motorola\DCConfig`.
4. Verify value in CurrentVersion key.
5. If you have an outdated version of the DC Plugin, perform the following actions:
   a. Update groups in Active Directory and DNS records. See Updating Groups in Active Directory and DNS Records on page 92.
   b. Update DNS record. See Updating DNS Records on page 94.

6.7.1

Updating Groups in Active Directory and DNS Records

This procedure should be performed only on system level Domain Controller (UCS-DC01).

Prerequisites:
Obtain:

- Domain Administrator account name and password. See “User Input Requirements for Server Installation/ Configuration” in *Authentication Services Feature Guide* or contact your system administrator.
- DC Plugin `iso` image

Ensure that all Domain Controllers (DC) are in the correct state in the Unified Event Manager (UEM) and there are nor errors.

Procedure:

1. Mount the DC Plugin `iso` image to the virtual CD drive of the Domain Controller virtual machine.

   The DC Plugin `iso` file is present by default as an `E:` drive. For more details, see “Connecting a Drive or ISO to a Virtual Machine” in Windows Supplemental Configuration Setup Guide.

DRAFT

2. Log on to the Domain Controller by using your Active Directory account that is a member of the Domain Admins group.

   The domain administrator's desktop appears.

3. Open **File Explorer**, navigate to the DVD Drive and launch the DC Plugin package.

   The DC Plugin package is an ADC_R***<XX.YY.ZZ>*** file, where ***<XX.YY.ZZ>*** is a software version.

4. Wait for the installation window to disappear.
5. Open the **PowerShell** console by performing the following actions:
   a. From **Start**, click **Search**.
   b. In the search field, type: `powershell`
   c. Right-click **Windows PowerShell** and select **Run as administrator**.
   d. If the **User Account Control** window appears, click **Yes**.

      If you are not logged on with an administrative account, enter the Administrator credentials.

6. **System-level Domain Controller (UCS-DC01) in the primary core:** Update groups on Active Directory environment by entering the following commands:
   a. `cd "C:\Program Files\Motorola\AstroDC\AD\scripts"`
   b. `.\RemoveGroups.ps1`
   c. `.\CreatePasswordPolicy.ps1 -passPolicyFilePath ..\data\PasswordPolicies.xml`
   d. `.\CreateGroups.ps1`
7. Verify that the scripts are completed successfully.

   The last line should contain `"Exit with 0"` string.

8. Update DNS records on Active Directory environment by entering the following commands:
   a. `cd "C:\Program Files\Motorola\AstroDC\DNS\scripts"`
   b. `.\SetMigrationPath.ps1`
   c. `.\PerformMigration.ps1 -default -type ldif -primaryDCOnly`
   d. `.\DeleteGenDNSData.ps1`
9. Verify that the scripts are completed successfully.

   The last line should contain `"Exit with 0"` string.

10. Close the **PowerShell** console.
11. Unmount the DC Plugin `iso` image from the virtual CD/DVD drive of the Domain Controller.
12. Restart the DNS service by performing the following actions:
    a. From **Start**, click **Search**.
    b. Type `"dnsmgmt.msc"` and press ENTER.
    c. In the DNS Manager console, right click the Domain Controller name (UCS-DC01) and select **All Tasks** → **Restart**.
    d. Wait ten minutes to ensure that the service restarted and completed reloading of DNS Zones.

DRAFT

6.7.2
Updating DNS Records

This procedure should be performed on all zone-level Domain Controllers (z00*<z>*dc01) in the primary core. The Domain Controller host name of the zone-level DC in the primary core is z00*<z>*dc01 where *<z>* is the zone number.

Prerequisites:
Obtain:

- Domain Administrator account name and password. See “User Input Requirements for Server Installation/ Configuration” in *Authentication Services Feature Guide* or contact your system administrator.
- DC Plugin `iso` image

Ensure that all Domain Controllers (DC) are in the correct state in the Unified Event Manager (UEM) and there are nor errors.

Procedure:

1. Mount the DC Plugin `iso` image to the virtual CD drive of the Domain Controller virtual machine.

   The DC Plugin `iso` is present by default as an `E:` drive. For more details, see “Connecting a Drive or ISO to a Virtual Machine” in *Windows Supplemental Configuration Setup Guide*.
2. Log on to the Domain Controller by using your Active Directory account that is a member of the **Domain Admins** group.

   The domain administrator’s desktop appears.
3. Open **File Explorer**, navigate to the DVD Drive and launch the DC Plugin package.

   The DC Plugin package is an ADC_R*<XX.YY.ZZ>* file, where *<XX.YY.ZZ>* is a software version.
4. Wait for the installation window to disappear.
5. Open the **PowerShell** console with administrative privileges by performing the following actions:
   a. Right-click **Start** and select **Search**.
   b. Type in: `powershell`
   c. Right-click **Windows PowerShell** and select **Run as administrator**.
   d. If the **User Account Control** window appears, click **Yes**.
   e. If you are not logged on with an administrative account, enter the admin credentials.
6. Update DNS records on Active Directory environment by entering the following commands:
   a. `cd “C:\Program Files\Motorola\AstroDC\DNS\scripts”`
   b. `.\SetMigrationPath.ps1`
   c. `.\PerformMigration.ps1 -default -type ldif -primaryDCOnly`
   d. `.\DeleteGenDNSData.ps1`
7. Verify that the scripts are completed successfully.

   The last line should contain `"Exit with 0"` string.
8. Close the **PowerShell** console.
9. Unmount the DC Plugin `iso` image from the virtual CD/DVD drive of the Domain Controller.
10. Restart the DNS service by performing the following actions:
    a. From **Start**, click **Search**.

DRAFT

b. Type "`dnsmgmt.msc`" and press ENTER.

c. In the DNS Manager console, right click the Domain Controller name (Z001DC01 for example) and select **All Tasks** → **Restart**.

d. Wait ten minutes to ensure that the service restarted and completed reloading of DNS Zones.

6.8 Configuring the DBR M12 Trunking RF Site

Prerequisites:
Obtain:

- Service laptop or the Network Management (NM) Client
- IP address or the host name of the DSC 8500. See Logon Information.
- Credentials for the **System Infrastructure Administrator** account

Procedure:

1. In the address bar of a web browser, enter one of the following:
   - IP address of your DSC 8500
   - Host name of your DSC 8500
2. Log on to the PCA as the **System Infrastructure Administrator**.
3. Configure the system. See Configuring the System.
4. Configure the band plan. See Configuring the Band Plan.
5. Configure the zone. See Configuring the Zone on page 98.
6. Configure the site. See Configuring the Site on page 99.
7. Configure the channels. See Configuring the Channels on page 102.
8. Select the **Pending Changes** tab.
9. Apply the changes by clicking **Apply**.

DRAFT

6.8.1 Configuring the System

Procedure:

1. From the **Configuration** drop-down list, select **System**.
2. In the **System list** view, select the system entry and click .
3. In the **Edit System** view, provide appropriate values according to your system configuration.

   For information on the system parameters, see System on page 96.
4. Click **Submit**.

6.8.1.1
System

ASR Trunking Site

Table 15: ASR System Field Descriptions

Field	Description	Range	Default
WACN ID	This field is used to assign a unique ID to the network in a Wide Area Communications Network (WACN) system where this site controller is located. Hexadecimal range of values is 00001 through FFFFE with 00001 as the default value.	1..FFFFE	1
System ID	This field is used to assign a unique system ID for the communications system where this site controller is located. The possible range of hexadecimal values is 001 (the default) through FFE.	1..FFE	1
Active Band Plan ID	ID of the Band Plan that is currently active.	1..20	1
Active Band Plan Name	This field is used to enter a name or alias (up to 32 alphanumeric characters) for the current active band plan.	size (1 .. 32) List of allowed characters: White space, A-Z, a-z, 0-9, !#$()*+-_./\;:<>=?[]^~`	""

Table 16: Subsite System Field Descriptions

Field	Description	Range	Default
WACN ID	This field is used to assign a unique ID to the network in a Wide Area Communications Network (WACN) system where this site controller is located. Hexadecimal range of values is 00001 through FFFFE with 00001 as the default value.	1..FFFFE	1
System ID	This field is used to assign a unique system ID for the communications system where this site controller is located. The possible range of hexadecimal values is 001 (the default) through FFE.	1..FFE	1

DRAFT

6.8.2
Configuring the Band Plan

Procedure:

1. From the **Configuration** drop-down list, select **Band Plan**.
2. In the **Band Plan list** view, select the entry you want to configure and click .
3. In the **Edit Band Plan** view, perform the following actions:

a. From the **Identifier Enabled** drop-down list, select **Enable**.

b. Provide appropriate values according to you system configuration.

For information on the band plan parameters, see ASR Trunking Site Band Plan on page 97.

4. Click **Submit**.

6.8.2.1
ASR Trunking Site Band Plan

Table 17: ASR Trunking Site Band Plan Field Descriptions

Field Name	Description	Range	Default	Units
Band Plan ID Index	Band Plan ID index into frequency band plan table.	1-16	1 - Default for 1st instance of Band Plans.	N/A
Identifier Enabled	Flag to indicate if the frequency band plan table entry is valid or not.	Enable, Disable	Enable - Default for 1st instance of Band Plans.	N/A
Channel Type	This field specifies the channel type of the band plan entry, either FDMA or TDMA.	FDMA, TDMA	FDMA	N/A
Base Frequency [MHz]	Base frequency which corresponds to a band plan element. Used to calculate the channel number of a specific channel.	132.00000..940.99375	851.00625 Default for 1st instance of Band Plans.	MHz
Channel Spacing [kHz]	It is the frequency spacing used by the frequency band plan element. Frequency difference between consecutive channel numbers. (i.e. If channel 1 is 800 MHz, channel 2's frequency would be equal to 800 MHz + Channel Spacing).	0..12.5	6.25 - Default for 1st instance of Band Plans.	kHz
TX/RX Offset [kHz]	Frequency difference between the set of transmit frequencies and the set of receive frequencies. The actual range on the user screen is -64 MHz to 64 MHz.	-64MHz to 64Mhz	-45MHz	MHz
Receive Channel Bandwidth [kHz]	Channel bandwidth of the receiver. **NOTE:** This value is not utilized by any existing SC devices. This range is not enforced by the SC, but rather by the manager devices.	12.5	12.5 - Default for 1st instance of Band Plans.	kHz

DRAFT

6.8.3
Configuring the Zone

Procedure:

1. From the **Configuration** drop-down list, select **Zone**.
2. In the **Zone list** view, select the zone entry and click .
3. In the **Edit Zone** view, provide appropriate values according to your system configuration.

   For information on the zone parameters, see Zone on page 98.
4. Click **Submit**.

6.8.3.1
Zone

Table 18: ASR Trunking Site Zone Field Descriptions

Field	Description	Range	Default	Units
Zone ID	This is the Zone ID which uniquely identifies the zone in which this site resides.	1..7	1	N/A
ZC IP Address 1	The IP address for the first ZC IP address in Primary Core.	N/A	N/A	N/A
ZC IP Address 2	The IP address for the second ZC IP address in Primary Core.	N/A	N/A	N/A
DSR Voice and Mobility Capability	Parameter to enable or disable DSR Voice and Mobility Capability for the site.	enabled, disabled	disabled	N/A
Backup ZC IP Address 1	The IP address for the first ZC IP address in Backup Core.	N/A	N/A	N/A
Backup ZC IP Address 2	The IP address for the second ZC IP address in Backup Core.	N/A	N/A	N/A
Tsub Capable	This parameter configures a site for Tsub fallback operation (i.e., enables a site controller to link up with the Tsub ZC).	enabled, disabled	enabled	N/A
Tsub ZC IP Address 1	NIC1 IP address of the Tsub Zone Controller; needed for SC to establish connectivity to the Tsub ZC when operating in Tsub mode.	N/A	0.0.0.0	N/A
Tsub ZC IP Address 2	NIC2 IP address of the Tsub Zone Controller; needed for SC to establish connectivity to the Tsub ZC when operating in Tsub mode.	N/A	0.0.0.0	N/A
Grant Timeout Timer [msec]	This field is used to set the time period for which an assigned voice channel remains active after access to the	400... 6500 msec	1000	msec

DRAFT

Field	Description	Range	Default	Units
	channel is granted to a subscriber. If this timer expires before subscriber activity is received, the controller terminates the call.			
Fade Timeout Timer [msec]	This field is used to set the time period for which an assigned voice channel remains active without channel activity. If the timeout period expires without detecting activity, the channel is deassigned.	100... 6300 msec	1900	msec

6.8.4

Configuring the Site

Procedure:

1. From the **Configuration** drop-down list, select **Site**.
2. In the **Site list** view, select the site entry and click .
3. In the **Edit Site** view, provide appropriate values according to your system configuration.

   For information on the site parameters, see Site on page 99.
4. Click **Submit**.

6.8.4.1

Site

ASR Trunking Site

Table 19: ASR Trunking Site Field Description

Field Name	Description	Range	Default	Units
Site ID	This identifies the site. **NOTE:** The various types of Site Controllers have different system requirements for the Site ID range.	1..150	1	N/A
Site Name	This is the user name given to the site.	size (0 .. 16) List of allowed characters: White space A-Z a-z 0-9 !#$ ()*+-./\;:<>=? []^~`	N/A	N/A
Link Debounce Timer [sec]	This timer defines the period of time in seconds between at-	3 - 120	3	seconds

DRAFT

Field Name	Description	Range	Default	Units
	tempts to bring the site link backup. **NOTE:** Changing the value of the Link Debounce Timer field from its default value of 3 seconds may affect the site recovery time in a system configured for Dynamic System Resilience (DSR).			
Trunking Recovery Timeout Time [sec]	The amount of time that the site waits to enter a trunking state after it has the resources to do so.	1..99	5	seconds
Site Trunking Indication Holdoff Time [sec]	Delays the report of site trunking to subscribers in the site to 'debounce' any temporary transitions to site trunking.	0..129	0	seconds
Priority Monitoring During Site Trunking	This parameter enables or disables Priority Monitor Override, when enabled it allows all talkgroups to be priority monitor capable in Site Trunking.	Enable, Disable	Disable	N/A
Channel Access Holdoff Timer [sec]	Value used to determine how long a subscriber should hold off before registering with the system or performing a location update under failure conditions.	0..60	12	minutes
In-Call User Alert Enable	This specifies whether the In-Call User Alert feature is enabled.	Enabled, Disable	Disable	N/A
Site Call Load Capacity Override	This parameter determines if the current Site Call Load Capacity should be fixed based on number of explicit channels or 'overridden' by a user-specified value. ● Enabled - Site Call Load Call Capacity is user-specified. ● Disable - Site Load Capacity must be configured according to number of explicit channels (refer to help in Site Load Capacity for settings)	Enabled, Disable	Disable	N/A

DRAFT

Field Name	Description	Range	Default	Units
Site Call Load Capacity	This parameter defines the maximum limit of the number of simultaneous calls (both voice and data) handled by the site. If the Site Load Capacity Override is enabled the user can configure; if disabled by the prime site the parameter must be configured as follows: (# Explicit Chans -> Site Load Capacity) (0->36), (1->24), (2->22), (3->18), (4->16), (5->14), (6 or more -> 12)	10..36	36	N/A
BSI Interval [min]	This parameter specifies the interval of time for when the Base Station Identifier in analog Morse code is transmitted.	10 | 12 | 14 | 16 | 18 | 20 | 25 | 30 | 40 | 50 | 60	30	minutes
Minimum Repeaters to Trunk	This parameter specifies the minimum number of repeaters required to trunk.	2..28	2	N/A
Zone Core Link Minimum Jitter Buffer [msec]	Specifies the minimum outbound audio jitter buffer time to account for network jitter on the arriving XIS packets.	15, 30, 45, 60, 75		msec
UTC-TAI Value	Specifies current UTC Time and TAI Time offset.	-120...0	-37	seconds
Site Type	Read only field, that specifies Site type, defined during installation procedure.	ASR_SITE	ASR_SITE	N/A
Actual Access Code Index	Indicates the Access Code Index value currently active in the station.	(0..15)	0	N/A
Control Channel Slot Time	Defines the length of time allotted to microslots required for each control channel message packet.	1..40	6	microslots
Packet Data Channel Slot Time	Specifies the packet data channel slot time for the displayed channel.	1..40	10	microslots
Astro Fade Tolerance	Sets the number of missed frame syncs that are counted in a row before a call is terminated.	1..3	3	N/A

DRAFT

Subsite

Table 20: Subsite Site Field Description

Field Name	Description	Range	Default	Units
Site ID	This identifies the site. **NOTE:** The various types of Site Controllers have different system requirements for the Site ID range.	1..150	1	N/A
Site Name	This is the user name given to the site.	size (0 .. 16) List of allowed characters: White space A-Z a-z 0-9 !#$ ()*+-./\;:<>=? []^~`	N/A	N/A
UTC-TAI Value	Specifies current UTC Time and TAI Time offset.	-120...0	-37	seconds
Subsite Type	Read only field, that specifies subsite type, defined during installation procedure.	SUBSITE	SUBSITE	N/A
Actual Access Code Index	Indicates the Access Code Index value currently active in the station.	(0..15)	0	N/A
Control Channel Slot Time	Defines the length of time allotted to microslots required for each control channel message packet	1..40	6	microslots
Packet Data Channel Slot Time	Specifies the packet data channel slot time for the displayed channel.	1..40	10	microslots
Astro Fade Tolerance	Sets the number of missed frame syncs that are counted in a row before a call is terminated.	1..3	3	N/A

DRAFT

6.8.5

Configuring the Channels

Procedure:

1. From the **Configuration** drop-down list, select **Channel**.
2. In the **Channel list** view, select the entry you want to configure and click .
3. In the **Edit Channel** view, perform the following actions:
   a. From the **Common Channel Config State** drop-down list, select **configured**.

b. Provide appropriate values according to you system configuration.

For information on the channel parameters, see Channel.

4. Click **Submit**.

6.8.5.1
Channel

Table 21: Channel Field Descriptions – DSC 8500 ASR Trunking Site

Field	Description	Range	Default
Channel Number	The Channel Number is the ID of the Channel in the system.	1..28	1
Common Channel Config State	This field is used to indicate if this channel is configured for use in the site.	configured, unconfigured	unconfigured
ASTRO Classic Data Capable	This field specifies whether the channel is capable of supporting P25 Classic Data.	Enable, Disable	Enable
Reserved Access Data Capable	Specifies whether the channel is capable of supporting Enhanced Data. Setting this parameter to **Yes** enables the channel to be configured for Enhanced Data.	Yes, No	No
DFB Capable	This field is used to select whether the channel has the capability to use the Dynamic Frequency Blocking feature. When DFB capability is set, the channel cannot transmit control, voice, BSI, or failsoft information when the site is operating in site trunking mode. If the site is operating in wide-area trunking mode, the channel can transmit voice information when assigned by the zone controller. This channel is enabled to use the Dynamic Frequency Blocking feature. **1.** When this field is enabled, the following fields are disabled and read only: ● BSI Capable ● Failsoft Capable ● Control Channel Capable (for channels 1 to 4 only) **2.** When this field is disabled: this channel cannot use the Dynamic Frequency Blocking feature.	Enable, Disable	Disable
BSI Capable	This is the capability for a channel to transmit Base Station Identifier in the analog Morse code. Values:	Enable, Disable	Disable

Field	Description	Range	Default
	● enabled - indicates this channel can transmit the analog BSI. When this field is enabled, the following fields are disabled and are read-only: ○ DFB Capable ○ Control Channel Capable (for channels 1 to 4 only) ● disabled - indicates this channel cannot be assigned to transmit the analog BSI.		
BSI Callsign	BSI_Callsign is the base station identification signal. This is the assign radio call sign issued for the system by the local licensing authority. This call sign is used in the analog Morse code identifications sent over the air when BSI_capable is enabled. The first 8 characters are also sent over the control channel as part of the MOT_BSI_GRANT control channel message each time the analog BSI is initiated. The first 8 characters are also sent in digital format over the channels when assigned for voice or data.	size (0 .. 20) any upper-case letter or number	""
Failsoft Capable	This field is used to select whether this channel is capable of entering the site failsoft mode when the simulcast subsystem cannot support site trunking. The site failsoft feature is a fall-back mechanism that allows the comparator to operate in a standalone state. Enabled (default) - indicates the comparator can enter site failsoft mode if the subsystem cannot support site trunking. Disabled - indicates the comparator cannot enter site failsoft mode.	Enable, Disable	Enable
Control Channel Capable	For IVD, this field specifies whether or not the channel is capable of being the Control Channel. Only channels 1-4 can be set as control channel capable.	Enable, Disable	Disable
Control Channel Preference Level	This field is used to rank the channels that are enabled as control channel capable. This ranking determines the order the channels are used as a control channel at the site. The range is 1 through 4 with a preference level of 1 as the highest rank and 4 as the lowest preference level.	1-4	4

Field	Description	Range	Default
Protected Capable	This is the capability that protects the channel from being assigned a call unless it is the only channel available.	Enable, Disable	Disable
Voice Capable	This is the capability for a channel to be used for voice: ● enabled - indicates this channel can be assigned as a voice channel. ● disabled - indicates this channel cannot be assigned as a voice channel.	Enable, Disable	Enable
Sub-Band	This field is used to determine if this channel has the capability to be assigned to sub-band frequencies.	Enable, Disable	Enable
Channel Access Type	This attribute indicates whether the channel is: ● FDMAonly ● Dynamic Channel ● TDMAonly TDMA Only value indicates 2 slot TDMA operability of the channel.	FDMAonly/DynamicChannel/TDMAonly	FDMAonly
TX Channel Frequency [MHz]	This is the RF Frequency that the Base Radio will transmit.	132..174 380..524 762.00625..775.99375 851.00625..869.99375 935.00625..940.99375	132000000 Hz
RX Channel Frequency [MHz]	This field allows you to enter the receive frequency for this channel. **NOTE:** VHF: (132000000..174000000) UHF: (380000000..524000000) 700 MHz: (792006250..805993750) 800 MHz: (806006250..824993750) 900 MHz: (896006250..901993750) Dependency: The Rx Frequency must be even divisible by 5000 or 6250 Hz for UHF/700 MHz/ 800MHz/900MHz and by 2500 or 3125 Hz for VHF. The following VHF Rx Frequencies are also allowed: 154371250.00 Hz	132..174 380..524 792.00625..805.99375 806.00625..824.99375 896.00625..901.99375	132000000 Hz

Field	Description	Range	Default
	154463750.00 Hz 154471250.00 Hz 154478750.00 Hz 169172000.00 Hz 169807000.00 Hz 173203750.00 Hz 173396250.00 Hz 173435700.00 Hz The Rx Frequency must be within the Rx Minimum Frequency and Rx Maximum Frequency and between the limits listed in the Range above. In the 700 MHz or 800 MHz band, for IV&D, the frequency ranges starts 6250 Hz above the lower limit and end 6250 below the upper limit.		
Channel Assignment Type	The type of assignment CAI packet to be used for this channel. In explicit, both Rx and Tx OTA channel numbers are included in the CAI packet. In implicit, there is only one OTA channel number and a Tx/Rx Offset is applied to the Tx Frequency to determine the Rx Frequency.	Implicit, Explicit	Implicit
FDMA Tx Band Plan Element	Identifier for the band plan element. This identifies the band plan element used by the channel, encoded as the highest 4 bits of the Txchannel number (Tx channel number of SU) in the CAI packets.	1-16	1
TDMA Tx Band Plan Element	Identifier for the band plan element. This identifies the band plan element used by the channel, encoded as the highest 4 bits of the Tx channel number (Tx channel number of SU) in the CAI packets. **NOTE:** Applies for Phase 2.	1..16	3
FDMA Rx Band Plan Element	Band identifier for the element. This identifies the band plan element used by the channel, encoded as the highest 4 bits of the Rx channel number (Rx channel number of SU) in the CAI packets.	1-16	1
TDMA Rx Band Plan Element	Identifier for the band plan element. This identifies the band plan element used by the channel, encoded as the highest 4	1..16	3

Field	Description	Range	Default
	bits of the Rx channel number (Rx channel number of SU) in the CAI packets. **NOTE:** Applies for Phase 2.		
Service Mode	Indicates if field personnel can steer a serviceability talk group to this channel when marked for serviceability testing. Indicates if field personnel can do BER/out bound test pattern tests for coverage testing.	Enable, Disable	Disable
Tx Power Out Requested [W]	Specifies the desired output power from the transmitter.	2..44	2W
Phase 2 Tx Power Out Requested [W]	Specifies the desired output power from the transmitter.	2..44	2W
Illegal Carrier Determination	Specifies whether illegal carrier is enabled.	Enabled, Disabled	Enabled
RF Threshold (Illegal Carrier Level) [dBm]	Specifies the dBm level above which the received signal is considered to be an illegal carrier if this station is not assigned to a call.	-124..-50	-90
Threshold Timer (Carrier malfunction Time)	Selects the length of time (in seconds) a carrier must exceed the illegal carrier threshold on an unassigned channel before the controller removes the channel from system use.	1..254	50
Rx Dual Branch Receiver Operations	Enables or disables diversity receive.	Enable, Disable	Disable
Rx Branch Imbalance Delta [dB]	Specifies Signal Quality Estimate (SQE) delta in dB(s) between multiple receiver branches used for failure detection.	3..12	5
Rx Branch Imbalance Time to Failure	Specifies Signal Quality Estimate (SQE) time (in seconds) to failure when Signal Quality Delta difference between branches is met or exceeded.	(0,30..1200)	120

6.8.6
Configuring the Subsite

Procedure:

1. From the **Configuration** drop-down list, select **Subsite**.
2. In the **Subsite list** view, select the entry you want to configure and click .
3. In the **Edit Subsite** view, perform the following actions:
   a. From the **Subsite Configuration** drop-down list, select **configured**.

b. Provide appropriate values according to you system configuration.

For information on the subsite parameters, see Subsite on page 108.

4. Click **Submit**.

6.8.6.1
Subsite

Table 22: Subsite Channel Field Descriptions – DSC 8500 ASR Trunking Site

Field	Description	Range	Default
Channel Number	The Channel Number is the ID of the Channel in the system.	1..28	1
Common Channel Config State	This field is used to indicate if this channel is configured for use in the site.	configured, unconfigured	unconfigured
ASTRO Classic Data Capable	This field specifies whether the channel is capable of supporting P25 Classic Data.	Enable, Disable	Enable
DFB Capable	This field is used to select whether the channel has the capability to use the Dynamic Frequency Blocking feature. When DFB capability is set, the channel cannot transmit control, voice, BSI, or failsoft information when the site is operating in site trunking mode. If the site is operating in wide-area trunking mode, the channel can transmit voice information when assigned by the zone controller. This channel is enabled to use the Dynamic Frequency Blocking feature. **1.** When this field is enabled, the following fields are disabled and read only: ● BSI Capable ● Failsoft Capable ● Control Channel Capable (for channels 1 to 4 only) **2.** When this field is disabled: this channel cannot use the Dynamic Frequency Blocking feature.	Enable, Disable	Disable
BSI Capable	This is the capability for a channel to transmit Base Station Identifier in the analog Morse code. Values: ● enabled - indicates this channel can transmit the analog BSI. When this field is enabled, the following fields are disabled and are read-only:	Enable, Disable	Disable

Field	Description	Range	Default
	○ DFB Capable ○ Control Channel Capable (for channels 1 to 4 only) ● disabled - indicates this channel cannot be assigned to transmit the analog BSI.		
BSI Callsign	BSI_Callsign is the base station identification signal. This is the assign radio call sign issued for the system by the local licensing authority. This call sign is used in the analog Morse code identifications sent over the air when BSI_capable is enabled. The first 8 characters are also sent over the control channel as part of the MOT_BSI_GRANT control channel message each time the analog BSI is initiated. The first 8 characters are also sent in digital format over the channels when assigned for voice or data.	size (0 .. 20) any upper-case letter or number	""
Control Channel Capable	For IVD, this field specifies whether or not the channel is capable of being the Control Channel. Only channels 1-4 can be set as control channel capable.	Enable, Disable	Disable
Control Channel Preference Level	This field is used to rank the channels that are enabled as control channel capable. This ranking determines the order the channels are used as a control channel at the site. The range is 1 through 4 with a preference level of 1 as the highest rank and 4 as the lowest preference level.	1-4	4
Voice Capable	This is the capability for a channel to be used for voice: ● enabled - indicates this channel can be assigned as a voice channel. ● disabled - indicates this channel cannot be assigned as a voice channel.	Enable, Disable	Enable
TX Channel Frequency [MHz]	This is the RF Frequency that the Base Radio will transmit.	132..174 380..524 762.00625..775.99375 851.00625..869.99375 935.00625..940.99375	132000000 Hz

Field	Description	Range	Default
RX Channel Frequency [MHz]	This field allows you to enter the receive frequency for this channel. **NOTE:** VHF: (132000000..174000000) UHF: (380000000..524000000) 700 MHz: (792006250..805993750) 800 MHz: (806006250..824993750) 900 MHz: (896006250..901993750) Dependency: The Rx Frequency must be even divisible by 5000 or 6250 Hz for UHF/700 MHz/ 800MHz/900MHz and by 2500 or 3125 Hz for VHF. The following VHF Rx Frequencies are also allowed: 154371250.00 Hz 154463750.00 Hz 154471250.00 Hz 154478750.00 Hz 169172000.00 Hz 169807000.00 Hz 173203750.00 Hz 173396250.00 Hz 173435700.00 Hz The Rx Frequency must be within the Rx Minimum Frequency and Rx Maximum Frequency and between the limits listed in the Range above. In the 700 MHz or 800 MHz band, for IV&D, the frequency ranges starts 6250 Hz above the lower limit and end 6250 below the upper limit.	132..174 380..524 792.00625..805.99375 806.00625..824.99375 896.00625..901.99375	132000000 Hz
Tx Power Out Requested [W]	Specifies the desired output power from the transmitter.	2..44	2W
Phase 2 Tx Power Out Requested [W]	Specifies the desired output power from the transmitter.	2..44	2W
Illegal Carrier Determination	Specifies whether illegal carrier is enabled.	Enabled, Disabled	Enabled
RF Threshold (Illegal Carrier Level) [dBm]	Specifies the dBm level above which the received signal is considered to be an illegal carrier if this station is not assigned to a call.	-124..-50	-90

Field	Description	Range	Default
Threshold Timer (Carrier malfunction Time)	Selects the length of time (in seconds) a carrier must exceed the illegal carrier threshold on an unassigned channel before the controller removes the channel from system use.	1..254	50
Rx Dual Branch Receiver Operations	Enables or disables diversity receive.	Enable, Disable	Disable
Rx Branch Imbalance Delta [dB]	Specifies Signal Quality Estimate (SQE) delta in dB(s) between multiple receiver branches used for failure detection.	3..12	5
Rx Branch Imbalance Time to Failure	Specifies Signal Quality Estimate (SQE) time (in seconds) to failure when Signal Quality Delta difference between branches is met or exceeded.	(0,30..1200)	120
Local Failsoft	Configures the station to be capable of entering local failsoft mode when the link to the comparator fails.	Enabled, Disabled	Disabled
Local Failsoft Holdoff Time	Specifies the additional amount of time (in seconds) to wait before entering local failsoft after the link to the Comparator has failed.	0..600	0

Table 23: Subsite Field Description – DSC 8500 ASR Trunking Site

Field Name	Description	Range	Default	Units
Subsite ID	This identifies the Subsite. **NOTE:** The various types of subsite controllers have different system requirements for the site ID range.	1..64	1	N/A
Subsite Configuration	This field is used to indicate if this subsite is configured for use in the site.	Unconfigured, Configured	Unconfigured	N/A
Subsite Name	This field allows you to assign a name or alias to this subsite.	size (0 .. 16) List of allowed characters: White space AZ a-z 0-9 !#$ ()*+-./\;:<>=? []^~` (exluding |,@,%,&,”,’)	N/A	N/A
UTC-TAI Value	Specifies current UTC Time and TAI Time offset.	-120...0	-37	seconds

DRAFT

Field Name	Description	Range	Default	Units
Subsite Type	Read only field, that specifies subsite type, defined during installation procedure.	SUBSITE	SUBSITE	N/A
Actual Access Code Index	Indicates the Access Code Index value currently active in the station.	(0..15)	0	N/A
Control Channel Slot Time	Defines the length of time allotted to microslots required for each control channel message packet	1..40	6	microslots
Packet Data Channel Slot Time	Specifies the packet data channel slot time for the displayed channel.	1..40	10	microslots
Astro Fade Tolerance	Sets the number of missed frame syncs that are counted in a row before a call is terminated.	1..3	3	N/A

DRAFT

6.9 Updating SysName in PCA

Prerequisites:
Obtain:

- Service laptop or the Network Management (NM) Client
- IP address or the host name of the DSC 8500. See Logon Information.
- *MSI CA Certs* package from *ASTRO Windows Supplemental* media
- Credentials for predefined admin or config users

Procedure:

1. In the address bar of a web browser, enter one of the following:
   - IP address of your DSC 8500
   - Host name of your DSC 8500
2. Log on to the PCA as the **System Infrastructure Administrator**.
3. From the **Configuration** drop-down list, select **SNMP System**.
4. In the **SNMP System list** view, select the SNMP System entry and click .
5. In the **Edit SNMP System** view, in the **Contact** and **Location** fields, provide appropriate values according to your system configuration.
6. In the **Edit SNMP System** view, in the **SysName** field, provide one of the following SysNames:
   - For DSC 8500s at a non-Tsub ASR Site, enter: `dscnmagent01.siteYY.zoneZ`
   - For DSC 8500s at a Tsub ASR Site, enter: `dscnmagent01.ipssXX.tsubYY.zoneZ`
   - For DSC 8500s at a non-Tsub Subsite, enter: `dscnmagent01.ipssXX.siteYY.zoneZ`
   - For DSC 8500s at a Tsub Subsite, enter: `dscnmagent01.subsiteXX.tsubYY.zoneZ`

6. If the **Warning Discovery in progress** dialog box appears, to the view active jobs that are related to the object being deleted, click **Open Job View**.

   Once a managed resource is deleted, you cannot restore its alarms.

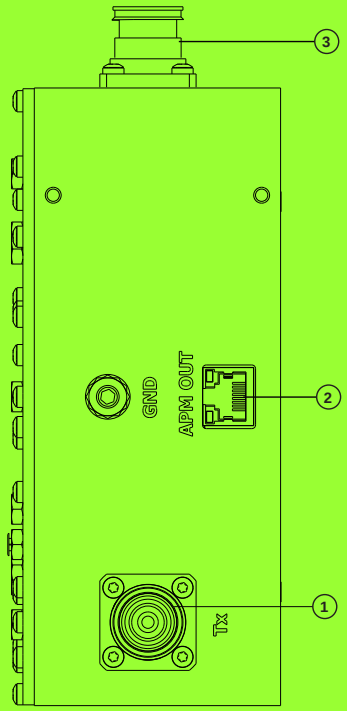
7.18

RFDS Transmit Filter (700/800)

The transmit filter removes any remaining noise in the receive sub-band between the combiner and the transmit antenna. The transmit band pass filter has a built-in power monitor on the output for monitoring the antenna system voltage standing wave ratio (VSWR) and the composite transmitter output power in reference to the top of the DBR M12 MultiCarrier Site cabinet/rack. The composite transmitter output power and VSWR can be viewed in the Provisioning and Configuration Agent (PCA). Additionally, the VSWR alarms are routed to the infrastructure as they occur.

The transmit filter is either 768–776 MHz or 851–870 MHz.

Figure 52: Transmit Filter (700/800/900 MHz)



Annotation	Description
1	Transmit in from the combiner (4.3-10 connector)
2	Transmit out to the antenna (4.3-10 connector)
3	Power monitor (Ethernet connection)

7.19

Setting the Transmitter Power

You can perform this procedure to set or verify the transmitter power during the commissioning of an RF site.

Prerequisites:
Obtain the service monitor.

Procedure:

1. Connect the service monitor to the -30 dB sample port of the Tx post filter with enough additional attenuation to protect the service monitor or the external power meter.

   NOTE: When you select **additional attenuation**, all of the DBR M12 MultiCarrier Site carriers can be keyed.

2. In the **Configuration/Channel** menu, set the transmitter power for all channels to the desired top of rack output level.
3. In the **Services/Requested State** menu, set the site to **Site Off**.
4. In the **Services/RF Channel Status** menu, perform the following actions:
   a. Select the desired channel.
   b. Ensure that **Real Time Session** is enabled.
   c. Start the V.52 FDMA test pattern.
   d. Ensure that the other channels are not transmitting.
5. In the **Configuration/Channel** menu, adjust the transmitter power of the desired channel to the desired accuracy as measured by the service monitor or external power meter in step 1.
6. Terminate the test pattern launched in step 4c.

   The top of the rack power, as measured by the service monitor or external power meter, should indicate that the carrier of the channel of interest is de-keyed.
7. For the rest of the channels, repeat step 4 to step 6.
8. In the **Services/Requested State** menu, set the site to the desired state.
9. In the **Services/RFDS Configuration** menu, key all of the enabled channels at once and save their composite power as a benchmark.

   You can compare the saved composite power benchmark with the future transmitter power out tests.

Chapter 9

DBR M12 MultiCarrier Site FRU Procedures

This chapter lists the Field Replaceable Units (FRUs) and includes replacement procedures applicable to the DBR M12 MultiCarrier Site.

9.1 DBR M12 MultiCarrier Site FRUs and Parts

The DBR M12 MultiCarrier Site is comprised of numerous field replaceable units (FRUs) and field replaceable parts.

When replacing a FRU or part, you must obtain the precise FRU Kit Number or Part Number and review the replacement procedures provided, including all safety precautions and system impact information.

When ordering FRUs, you must provide the FRU Kit Number. When ordering field replaceable parts, provide the Part Number. To obtain the numbers that are not provided in this section, you must contact Centralized Managed Support Operations (CMSO). If a part that you want to replace is not listed in this section, you must find the part number on the part or part label and contact Centralized Managed Support Operations (CMSO).

WARNING: To guard against personal injury and/or damage to equipment, switch a trunked base radio to Service Mode when performing service. The system periodically keys up to pseudo train its linear transmitter autonomously when it is not assigned by the zone controller. Tx Inhibiting the base radio also prevents the transmitter from keying. Remember to switch the base radio back to Normal Mode when service is complete.
AVERTISSEMENT: Pour prévenir les blessures ou les dommages à l'équipement, faites passer une radio de base commutée en mode Service lors de l'entretien. Le système se code périodiquement pour pseudo-entraîner son linéaire émetteur de manière autonome lorsqu'il n'est pas attribué par le contrôleur de zone. Le blocage d'émission de la radio de base empêche également l'émetteur de faire le codage. N'oubliez pas de remettre la radio de base en mode normal une fois l'entretien terminé.

Table 31: DBR M12 MultiCarrier Site Field Replaceable Units

Component Type	FRU Kit Number	Replacement Procedure
Transceiver Module (700/800 MHz)	DLN8065A	Replacing the Transceiver Module on page 176
Power Amplifier Module (800 MHz)	DLN8061A	Replacing the Power Amplifier on page 178
Power Amplifier Module (700 MHz)	DLN8062A	Replacing the Power Amplifier on page 178
Site RMC Module (700/800 MHz)	DLN8063A	Replacing the RMC Modules on page 189
Cabinet RMC Module (700/800 MHz)	DLN8064A	Replacing the RMC Modules on page 189
Power Amplifier Fan Filter Replacement Kit	DLN8042A	DBR M12 MultiCarrier Site Troubleshooting and Disaster Recovery on page 191

Component Type	FRU Kit Number	Replacement Procedure
Power Amplifier Fan Kit	DLN8032A	Replacing the DSC 8500 Fan Assembly on page 167
DSC 8500 without Rubidium Timing	DLN1446A	Replacing the DSC 8500 Hardware on page 165
DSC 8500 with Rubidium Timing	DLN1447A	Replacing the DSC 8500 Hardware on page 165
2-3 Way Combiner (800 MHz)	DLN8066A	Replacing the N-Way Combiner on page 185
2-3 Way Combiner (700 MHz)	DLN8067A	Replacing the N-Way Combiner on page 185
4-6 Way Combiner (800 MHz)	DLN8068A	Replacing the N-Way Combiner on page 185
4-6 Way Combiner (700 MHz)	DLN8069A	Replacing the N-Way Combiner on page 185
2-3 Way Splitter (800 MHz)	DLN8070A	Replacing the N-Way Splitter on page 187
2-3 Way Splitter (700 MHz)	DLN8071A	Replacing the N-Way Splitter on page 187
4-6 Way Splitter (800 MHz)	DLN8072A	Replacing the N-Way Splitter on page 187
4-6 Way Splitter (700 MHz)	DLN8073A	Replacing the N-Way Splitter on page 187
Rx Preselector (700/800 MHz)	DLN8074A	Replacing the Site Preselector on page 180
Tx post filter (800 MHz)	DLN8075A	Replacing the Transmit Filter on page 181
Tx post filter (700 MHz)	DLN8076A	Replacing the Transmit Filter on page 181
700Mhz 800MHz TX Phasing Harness	DLN8079A	Replacing the Phasing Harness on page 183

9.2

Replacing the DSC 8500 Hardware

If the DSC 8500 hardware fails, contact the Motorola Solutions Support Center for a replacement. Replacing the DSC 8500 is a process very similar to configuring the device at a site for the first time.

Prerequisites:
Obtain:

- Replacement DSC 8500 with known MAC address
- 2 mounting brackets
- 8 x M4x8 mm black screws (part no. 03009313001)
- T20 Torx driver with torque setting 1.7 Nm (15 in/lb)
- T30 Torx driver with torque setting 6.2 Nm (55 in/lb)
- 3/8" nut driver or socket and torque wrench set to 55 in-lbs
- 2 M6 star pan screw (part no. 0310909C91)
- 4x screw (not included): M6 or 12-24 UNC, depending on rack type
- Electrostatic discharge (ESD) wrist strap (Motorola Solutions part number RSX4015A, or equivalent) that must be worn during the removal and installation of the DSC 8500 in the rack. Its cable must be connected to a verified good ground

Process:

1. Wipe the software and sensitive data from the failed DSC 8500. See Wiping the Software and Sensitive Data on page 139.

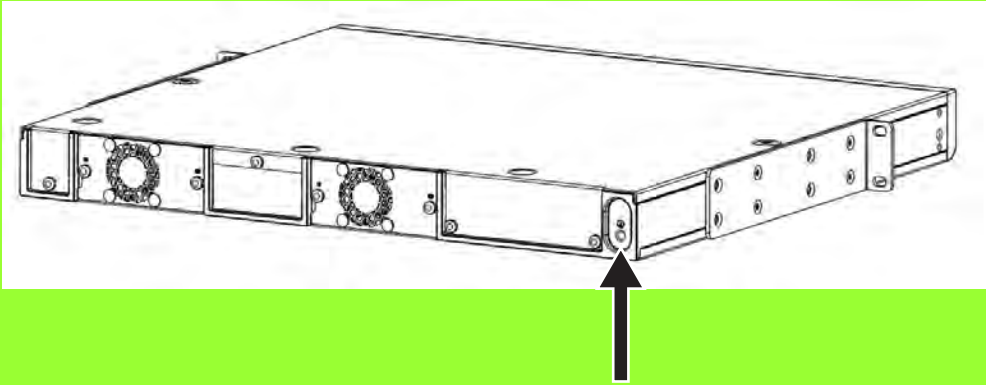
   NOTE: In case of serious hardware failure it might be impossible to wipe the software and sensitive data from the failed DSC 8500.

2. Disconnect all cables from the failed DSC 8500.

   If only one site router is present and connected to port DSCn_Port2_Router on the failed DSC 8500, communication with the site is lost after the cable is unplugged.

3. Remove the failed DSC 8500 from the rack.
4. Install the new DSC 8500 in the rack by performing one of the following actions:
   - Install DSC 8500s in a 2-post open rack. See Installing DSC 8000s in a 2-Post Open Rack.
   - Install DSC 8500s in a 4-post cabinet. See Installing DSC 8000s in a 4-Post Cabinet.
5. Ground the DSC 8500:
   a. Place the grounding cable with a right angle lug to the grounding point on the right, back side of the DSC 8500 and install an M6 star pan screw 0310909C91 by using a driver set to 55 in-lbs and a Torx T30 bit.

      Figure 53: DSC 8500 Grounding Point



   b. Secure the other end of the grounding cable to the busbar with an M6 star pan screw 0310909C91 by using a driver set to 55 in-lbs and a Torx T30 bit.
6. Connect the DSC 8500s to the power source. See Connecting Power to an AC Power Source or Connecting Power to a DC Power Source depending on site configuration.
7. Connect the DSC 8500 to other site elements. See DSC 8000 Trunking RF Site Cabling Scenarios.

   The cables must be connected to the new DSC 8500 the same way they were connected to the failed DSC 8500.

9.3

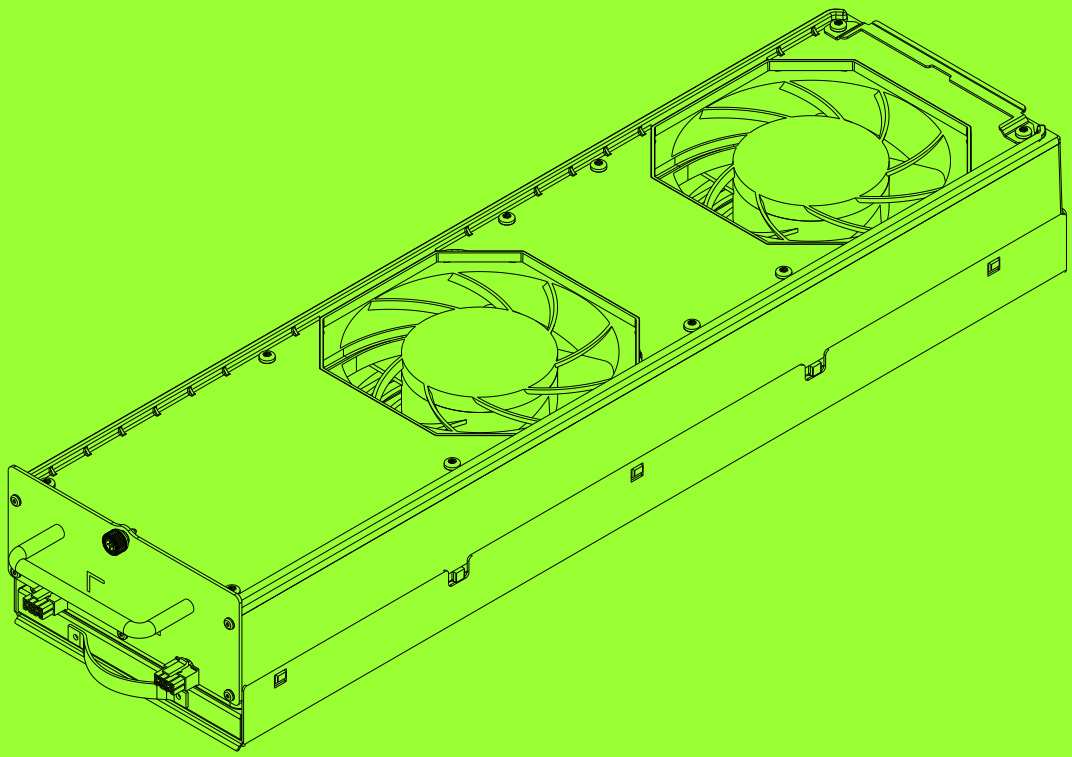
Replacing the DSC 8500 Fan Assembly

To prevent overheating, the fan must be in place at all times. You can remove the fan only for servicing purposes.

WARNING: Before and after the removal of the fan module, you must avoid touching the moving fan blades with tools, hands, or other objects. If you want to remove the fan module to access or replace the modules behind it, you must turn off the equipment power and allow the modules to cool before performing any work, as the surfaces of the modules can be hot.
AVERTISSEMENT: Avant et après le retrait du module de ventilateur, vous devez éviter de toucher les pales de ventilateur en mouvement avec des outils, les mains ou d'autres objets. Si vous souhaitez retirer le module de ventilateur pour accéder aux modules derrière lui ou les remplacer, vous devez couper l'alimentation de l'équipement et laisser les modules refroidir avant d'effectuer des travaux, car les surfaces des modules peuvent être chaudes.

IMPORTANT: You can swap out the fan assembly without shutting the power off. You must have the replacement fan assembly in place within a reasonable amount of time, so that the device module does not overheat and shut down.

Figure 54: DSC 8500 Fan Assembly



Prerequisites:
Obtain:

- Philips bit screwdriver
- Electrostatic discharge (ESD) wrist strap (Motorola Solutions part number RSX4015A, or equivalent) that must be worn throughout this procedure.

Procedure:

1. Wear an electrostatic discharge (ESD) strap and connect its cable to a verified good ground.

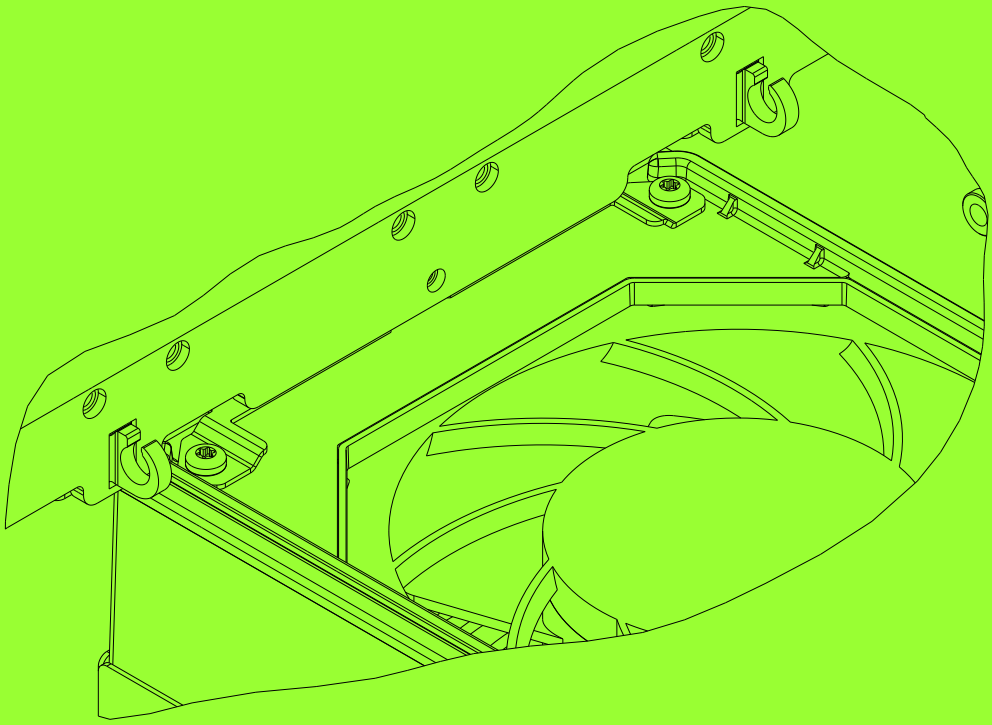
   CAUTION: Wear the ESD strap throughout the whole procedure to prevent ESD damage to any components.
   ATTENTION: Portez la dragonne ESD tout au long de la procédure pour éviter que les composants soient endommagés par les décharges électrostatiques.

2. Disconnect connections from the fan to the power amplifiers (PAs).
3. Using a Phillips bit screwdriver, loosen the captive screw on the front of the fan assembly that you want to replace.
4. Pull the fan module out of the card cage.

   You must support the bottom of the fan kit as it is removed.

5. Insert a new fan kit so that the retainer lines are aligned with the notch in the card cage.

   Figure 55: Fan Kit Retainer Lines and Card Cage Notch



6. Lift the fan kit up and push it forward until the front panel of the fan kit touches the card cage
7. Using a Phillips bit screwdriver, secure the new fan.
8. Ensure that the fan assembly operates properly, and that the fan Alarm LED is off.

   To verify the status of the equipment, you can also use software tools, such as Unified Event Manager (UEM) or Configuration/Service Software (CSS).

9.4

Replacing the Power Supply Unit Chassis

DANGER: High Leakage Current (12 mA). Earth connection is essential before connecting the power supply.
DANGER: Courant de fuite élevé (12 mA). La connexion à la terre est essentielle avant de connecter l'alimentation.

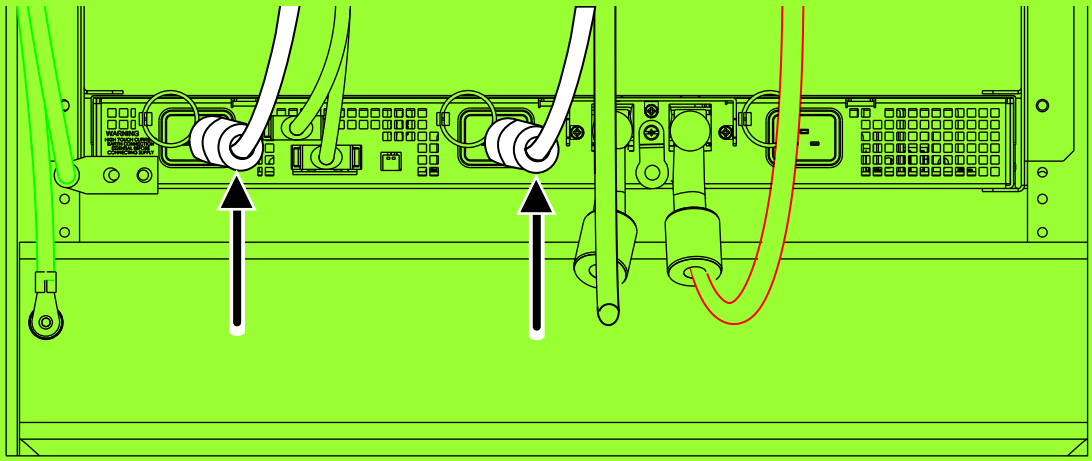
Prerequisites:
Obtain:

- PH1 screwdriver
- T30 driver set to 55 in-lb
- Electrostatic discharge (ESD) wrist strap (Motorola Solutions part number RSX4015A, or equivalent) that must be worn throughout this procedure. Its cable must be connected to a verified good ground.

Procedure:

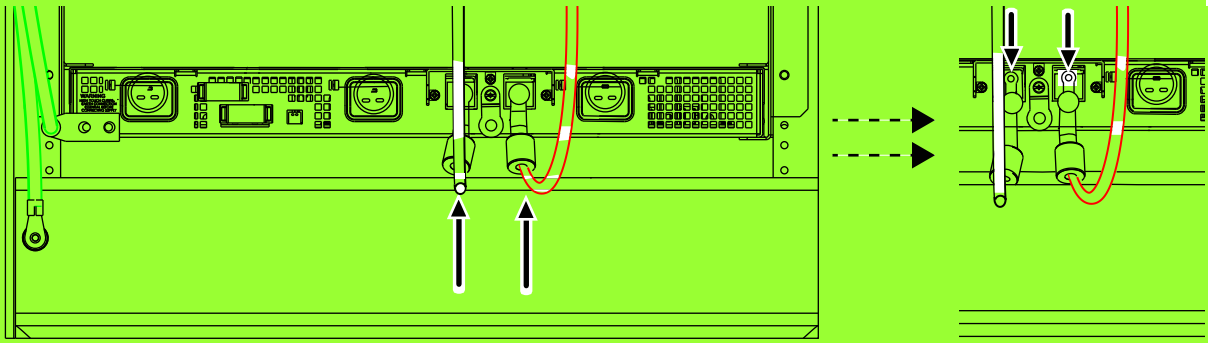
1. Unplug the power cord connectors from the Power Supply Units (PSUs).

   Figure 56: Power Cord Connectors



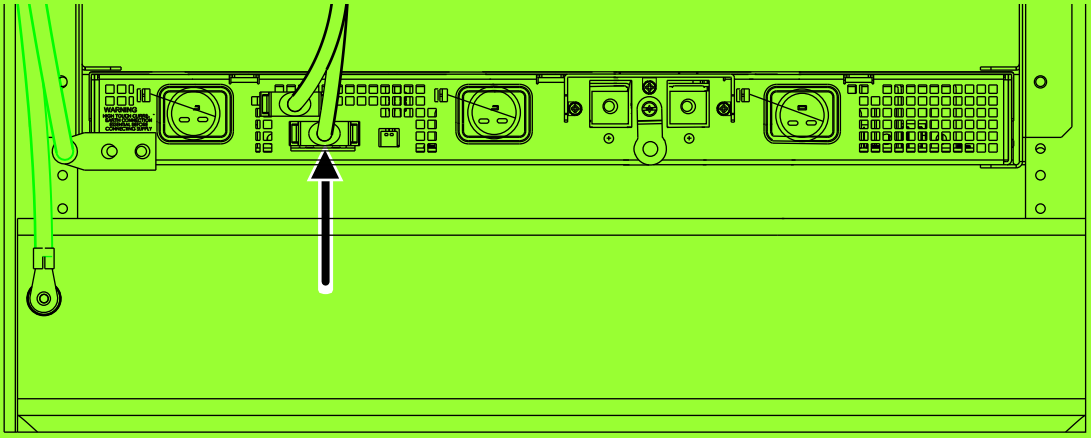
2. Disconnect the DC cables:
   a. Expose DC cable lugs by pushing terminal boots back.
   b. Unscrew the cable lugs of DC cables and remove them from the chassis.

   Figure 57: DC Cables



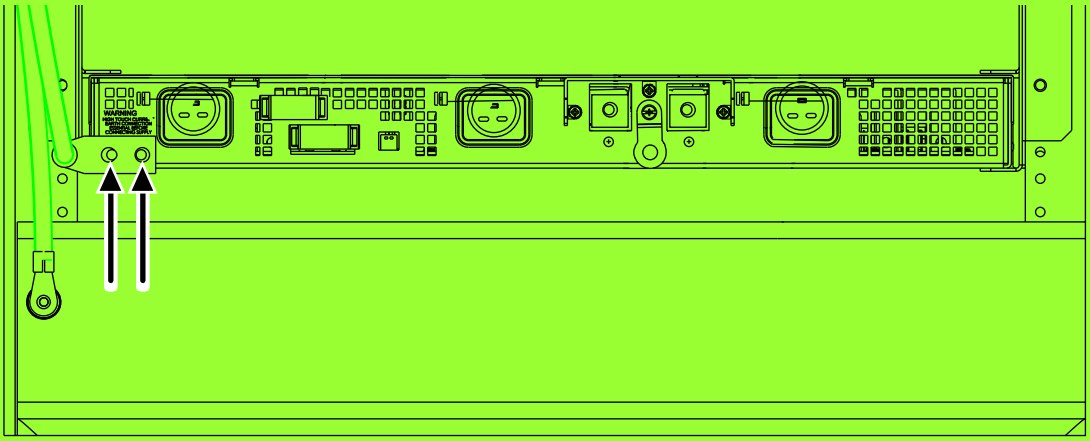
3. Disconnect the alarm cable from the frame.

Figure 58: Alarm Cable



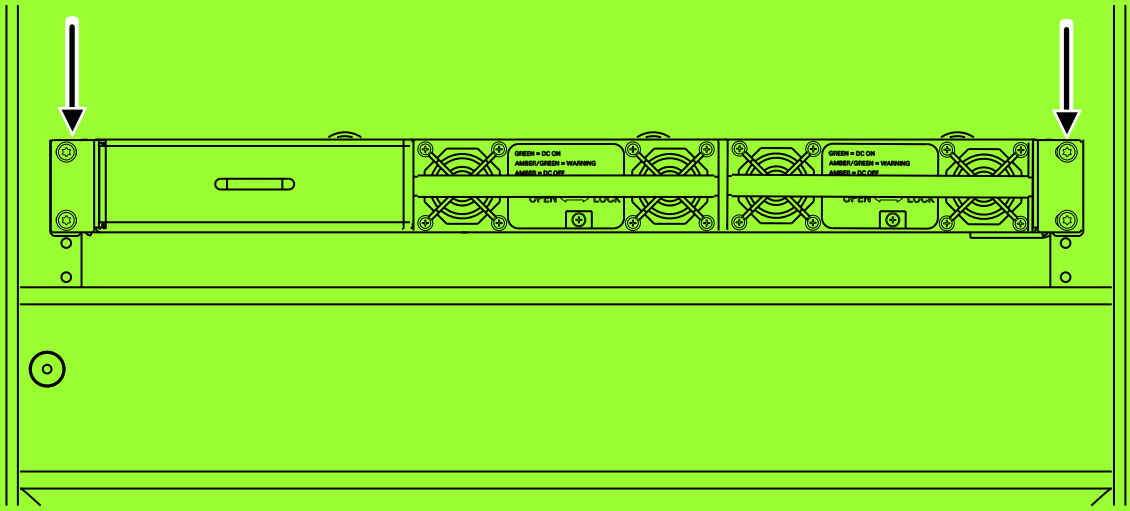
4. Disconnect the grounding cable by unscrewing the nuts on the double lug and pulling out the grounding cable connector.

Figure 59: PSU Chassis Grounding Cable



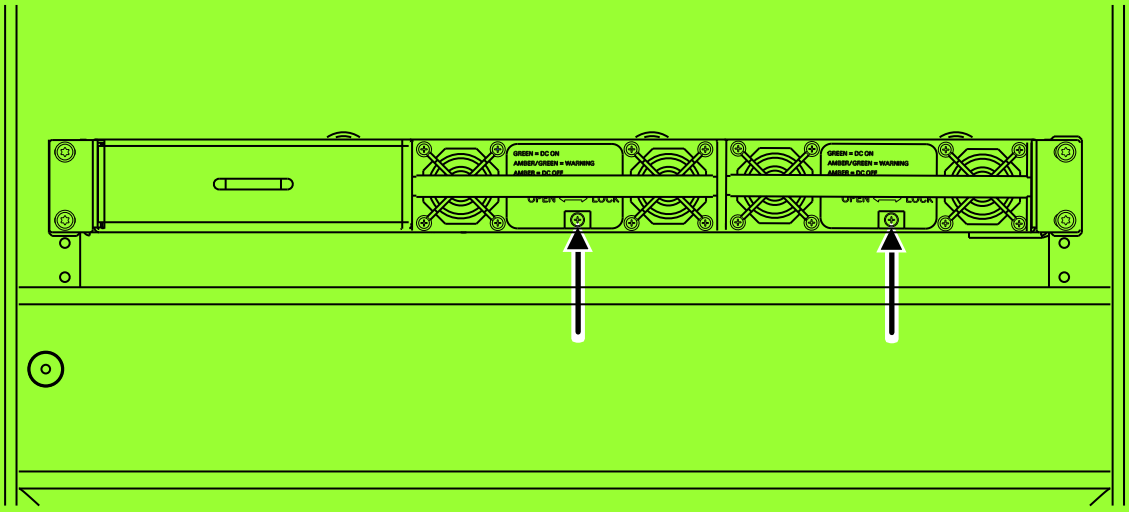
5. Disconnect the PSU chassis from the bracket:
   a. Remove four screws in the chassis corners.
   b. Slide the chassis out of the bracket on the rack.

Figure 60: PSU Chassis Screws Location



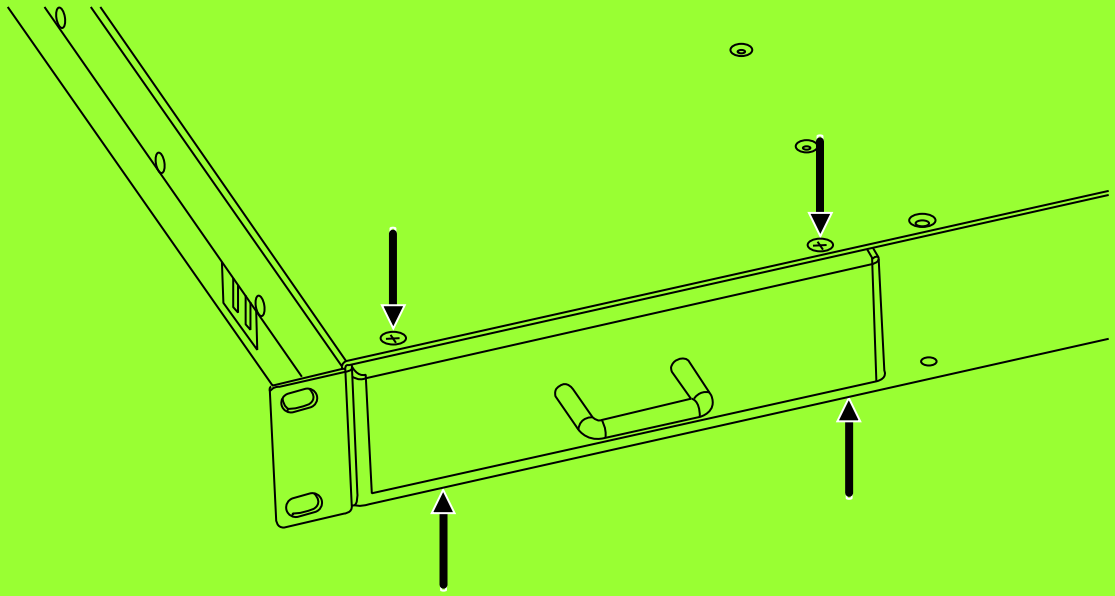
6. Retrieve PSUs:
   a. With a Phillips PH1 screwdriver, loose the screw on the front of the Power Supply Unit (PSU).
   b. Push the prong to the left with one hand.
   c. With the other hand, use the PSU handle to draw it out of the chassis.
   d. Repeat step 6a to step 6c for the other PSU.

Figure 61: Power Supply Units



7. Retrieve the PSU dummy panel by unscrewing four screws on top and bottom of the chassis and drawing it out of the chassis.

Figure 62: Retrieving the PSU Dummy Panel



8. With four short M3 screws provided with the panel, install the dummy panel on the unused slot of the new PSU chassis.

   The unused slot is the first one from the left. See Figure 61: Power Supply Units on page 171.

9. With four TORX screw, install the new PSU chassis into the bracket on the rack, and drive the screws to 55 in-lbs.

   See Figure 60: PSU Chassis Screws Location on page 171.

10. Install the PSUs in the chassis:

    a. Ensure that the lock screw is open.

    b. Slide each PSU into the chassis and ensure that each module clicks into place.

    c. With a Philips screwdriver tighten the lock screws.

    See Figure 61: Power Supply Units on page 171.

11. Connect DC cables to the new chassis:

    a. With the screws provided with the PSU chassis, screw the cable end with a log ring terminal to the PSU chassis.

    b. Draw the terminal boots up to cover the long ring terminals.

    See Figure 57: DC Cables on page 169.

12. Connect the grounding cable to the new PSU chassis by screwing the end with a double lug to the location in the bottom left corner of the chassis.

    See Figure 59: PSU Chassis Grounding Cable on page 170.

    WARNING: Do not disconnect the AC PSU alarm cable during operation. This cable must be connected to the PSU tray for the DC power to be provided to the DSC 8500. Removal of this cable from the AC Power Supply tray results in loss of power to the DSC 8500.
    AVERTISSEMENT: Ne débranchez pas le câble d'alarme du bloc d'alimentation CA pendant le fonctionnement. Ce câble doit être connecté au plateau d'alimentation CA pour que l'alimentation CC soit fournie au DSC 8500. Le retrait de ce câble du plateau d'alimentation CA entraîne une perte d'alimentation du DSC 8500.

13. Connect the PSU alarm cable to the back side of the PSU chassis.

    See Figure 58: Alarm Cable on page 170.

14. Plug in the power cords to the PSU chassis.

    See Figure 56: Power Cord Connectors on page 169.

9.5 Replacing the Power Supply Unit

Prerequisites:
Obtain:

- PH1 screwdriver
- Electrostatic discharge (ESD) wrist strap (Motorola Solutions part number RSX4015A, or equivalent) that must be worn throughout this procedure. Its cable must be connected to a verified good ground

Procedure:

1. Remove the faulty power supply unit from the rack:
   a. With a Phillips PH1 screwdriver, loose the screw on the front of the Power Supply Unit (PSU).
   b. Push the prong to the left with one hand.
   c. With the other hand, use the PSU handle to draw it out of the chassis.

   See Figure 6.
2. Install the new PSU in the rack:
   a. Ensure that the lock screw is open.
   b. Slide the PSU into the chassis and ensure that it clicks into place.
   c. With a Philips screwdriver tighten the lock screws.
3. To monitor the power supply status, connect the power supply presence output to the Aux In on the DSC 8500 or to other monitoring device (for example MC Edge). See Configuring the Auxiliary Inputs on page 129.

9.6 Replacing the DSC 8500 Site Controller Module

IMPORTANT: You can hot swap the DSC 8500 site controller module without losing functionality. The standby site controller automatically becomes the active site controller and takes over for the replaced site controller.

Prerequisites:
Ensure that you pulled the configuration and hardware information from the DSC 8500 to the Unified Network Configurator (UNC). See "Scheduling the Pull of Device Configurations" in the Unified Network Configurator User Guide.

NOTE: It may be impossible to pull the configuration and hardware information from the DSC 8500 to the UNC if the communication between the site controller and the UNC is severed.

Obtain:

- Replacement DSC 8500 with known a MAC address
- T30 Torx screwdriver with torque setting 6.2 Nm (55 in/lb)
- 3/8" socket and torque wrench set to 55 in-lbs

- Electrostatic discharge (ESD) wrist strap (Motorola Solutions part number RSX4015A, or equivalent) that must be worn during the removal and installation of the DSC 8500 in the rack.

Procedure:

1. Wear an electrostatic discharge (ESD) strap and connect its cable to a verified good ground.

   CAUTION: Wear the ESD strap throughout the whole procedure to prevent ESD damage to any components.
   ATTENTION: Portez la dragonne ESD tout au long de la procédure pour éviter que les composants soient endommagés par les décharges électrostatiques.

2. Perform one of the following actions:
   - If the DSC 8500 is non-operational, go to step 4.
   - If the DSC 8500 is operational, go to step 3.
3. Wipe the software and sensitive data from the failed DSC 8500. See Wiping the Software and Sensitive Data on page 139.

   NOTE: In case of serious hardware failure it might be impossible to wipe the software and sensitive data from the failed DSC 8500.

4. Label and disconnect all cables from the front of the failed DSC 8500.

   If only one site router is present and connected to port DSCn_Port2_Router port on the failed DSC 8500, communication with the site is lost after the cable is unplugged.

5. Perform one of the following actions:
   - If you remove the DSC 8500 from an open rack, remove the four screws that hold the DSC 8500 in brackets to the rails by using a 3/8" socket.
   - If you remove the DSC 8500 from a cabinet, remove the four screws that hold the DSC 8500 in brackets to the rails by using a T30 Torx screwdriver.
6. Partially remove the DSC 8500 and at the rear, remove the screw fastening the grounding cable to the module by using a T30 Torx screwdriver.
7. Fully remove the DSC 8500 module.
8. Partially insert the replacement DSC 8500 into position and at the rear, fasten the grounding cable to the DSC 85000 to 17 in-lbs by using a T30 Torx screwdriver.
9. Perform one of the following actions:
   - If you insert the replacement DSC 8500 to an open rack, fasten the four screws that hold the DSC 8500 in brackets to the rails to 55 in-lbs by using a 3/8" socket.
   - If you insert the replacement DSC 8500 to a cabinet, fasten the four screws that hold the DSC 8500 in brackets to the rails to 55 in-lbs by using a T30 Torx screwdriver.
10. Reconnect all the cabling to the correct replacement DSC 8500 ports, as labeled in step 4.

9.6.1
Deploying the DSC 8500 Software After the DSC 8500 Replacement

To avoid connectivity issues related to cabling the replacement DSC 8500 differently than the original, use the remaining DSC 8500 to disable MAC Port Lockdown on all ports of all DSC 8500s prior to connecting the replacement DSC 8500. After connecting the replacement DSC 8500, configure MAC Port lockdown for the desired ports. See Enabling/Disabling MAC Port Lockdown on the DSC 8500 on page 123.

Prerequisites:

Obtain:

- Service laptop with On-Premises Software Hub installed. Ensure that service laptop is connected to any enabled DSC 8500 service port. If not, enable service port on one of the working DSC 8500s. See Configuring the DSC 8500 Switch on page 121.
- DSC 8500 installation media
- IDs of the failed DSC 8500s
- MAC addresses of all replaced DSC 8500s

Ensure that:

- The latest version of On-Premises Software Hub is used.
- The software bundle deployed on the other DSC 8500s in the site is imported to On-Premises Software Hub.

Procedure:

1. From the desktop, launch the **On-Premises Software Hub** application.
2. Import the DSC 8500 software bundle. See Importing the DSC 8500 Software Bundle.

   After the software bundle is imported, a success message appears in the right bottom corner.
3. Discover the site. See Discovering the Site on page 76.
4. Connect to the site. See Connecting to the Site on page 77.
5. Go to **Device Management** screen in the On-Premises Software Hub.
6. For the site where the DSC 8500 is replaced or wiped, from the **Action** drop-down list, select **FRU Replacement-DSC***<DSC_ID>*.
7. In the **FRU Replacement** window, verify that software bundle version and site parameters are set correctly.
8. Set the DSC 8500 instance ID for the found MAC address of the new DSC 8500.

   IMPORTANT: It is required that the new DSC 8500 has the same ID as the replaced, failed DSC 8500.
9. Click **Continue** to start the installation process.

   Until the installation process for one site is complete, it is not possible to start the installation process for another site.
10. Wait for successful completion of **Initial Deployment** action on the replaced DSC 8500.
11. Verify security configuration. See Verifying the DBR M12 MultiCarrier Site Security Configuration on page 126.

9.6.2 Configuring DSC 8500 After Disaster Recovery Software Installation

This procedure configures DSC 8500 after successful hardware replacement and software deployment.

If disaster recovery is required for more than one DSC 8500s in the site, this procedure should be done when all DSC 8500s are replaced and the software on them is deployed.

Prerequisites:
Obtain:

- Service laptop or the Network Management (NM) Client

- IP address or the host name of the DSC 8500. See Logon Information.
- Credentials for the System Infrastructure Administrator account

Process:

1. Verify the DSC 8500 Trunking RF Site Security Configuration for each replaced DSC 8500. See Verifying the DBR M12 MultiCarrier Site Security Configuration on page 126.
2. In Provisioning and Configuration Agent, discover the DSC 8500s. See Discovering the Hardware on page 123.

9.7 Replacing the Transceiver Module

Figure 63: Transceiver Module

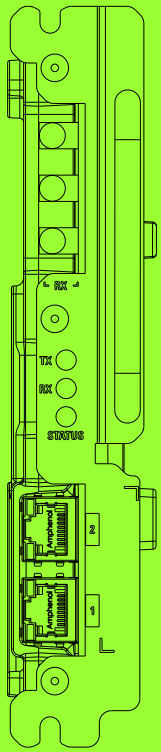
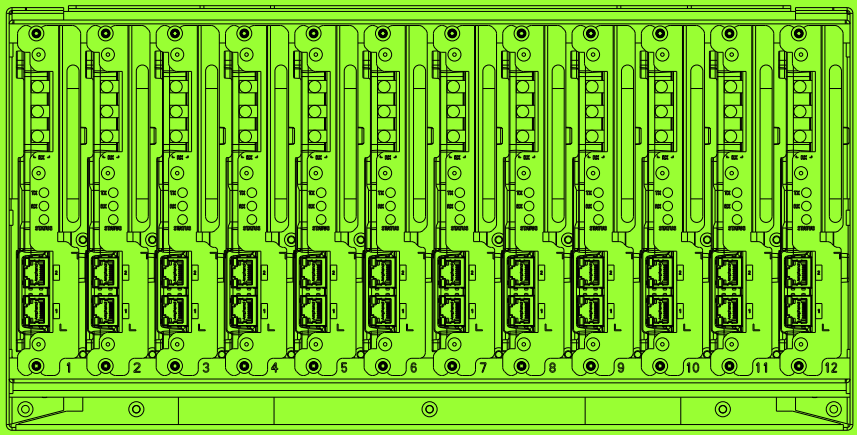


Figure 64: Transceiver Card Cage



NOTE: The IP address for the device is available through a serial port connection in Configuration/ Service Software (CSS) in the **Tools** menu.

Prerequisites:
Pull the configuration and hardware information from the transceiver into the Unified Network Configurator (UNC). See the “Scheduling the Pull of Device Configurations” section in the *Unified Network Configurator User Guide*.

The transfer may not be possible if communication is severed between the transceiver and the UNC, or if the transceiver is within a K core or non-networked site.

Obtain:

- The replacement transceiver module
- T20 bit
- Electrostatic discharge (ESD) wrist strap (Motorola Solutions part number RSX4015A, or equivalent) that must be worn during the removal and installation of the DSC 8500 in the rack.

Procedure:

1. Wear an electrostatic discharge (ESD) strap and connect its cable to a verified good ground.

   CAUTION: Wear the ESD strap throughout the whole procedure to prevent ESD damage to any components.
   ATTENTION: Portez la dragonne ESD tout au long de la procédure pour éviter que les composants soient endommagés par les décharges électrostatiques.

2. Locate the transceiver module that you want to replace.
3. In Provisioning and Configuration Agent (PCA), disable the XCVR by performing the following actions:
   a. Navigate to **Services** → **Requested States**.
   b. In the **Requested States** view, expand the **Transceiver** node.
   c. Expand the node for the rack where the XCVR is installed.
   d. From the drop-down list next to the XCVR, select **Disable**.
4. Label and disconnect all cables from the ports on the transceiver.
5. To disengage the two captive screws on the front of the transceiver module, loosen them by using a T20 bit.

6. Grab the handle on the transceiver module and gently pull the transceiver module straight out along the guides on which it sits.
7. Slide in the replacement transceiver module along the guiding rails until it is engaged.

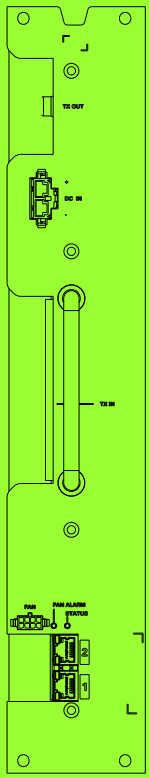
   A slight push may be necessary to securely engage the module in place.
   When the transceiver module is correctly engaged, the LEDs on the transceiver turn on.

   IMPORTANT: If the transceiver module stops before it is engaged, it is in an incorrect position. It is either in the wrong slot or is rotated 180°. The module has a keying feature that prevents it from going all the way into an incorrect slot, or going into the correct slot but rotated 180°. Do not try to force the module.
8. To secure the transceiver module to the card cage, insert the two captive screws on the front of the transceiver and tighten them to 17 in-lbs by using a T20 bit.
9. Reconnect all cables to the appropriate ports on the transceiver.
10. In PCA, discover the new XCVR. See Discovering the Hardware on page 123.
11. In PCA, check the records of the XCVR by performing the following actions:
    a. Navigate to **Services** → **Event Monitoring**.
    b. In the **Event Monitoring** view, expand the **Transceiver** node.

9.8

Replacing the Power Amplifier

Figure 65: Power Amplifier I/O Connections



Prerequisites:
Obtain:

- Replacement power amplifier (PA) module

- T20 bit screwdriver
- Electrostatic discharge (ESD) wrist strap (Motorola Solutions part number RSX4015A, or equivalent) that must be worn throughout this procedure.

Procedure:

1. Wear an electrostatic discharge (ESD) strap and connect its cable to a verified good ground.

   CAUTION: Wear the ESD strap throughout the whole procedure to prevent ESD damage to any components.
   ATTENTION: Portez la dragonne ESD tout au long de la procédure pour éviter que les composants soient endommagés par les décharges électrostatiques.

2. Perform one of the following actions:
   - If the PA is non-operational, go to step 4.
   - If the PA is operational, go to step 3.
3. In Provisioning and Configuration Agent (PCA), disable the PA by performing the following actions:
   a. Navigate to **Services** → **Requested States**.
   b. In the **Requested States** view, expand the **Power Amplifier** node.
   c. Expand the node for the rack where the PA is installed.
   d. From the drop-down list next to the PA, select **Disable**.
4. Remove the 4 screws that secure the PA module in place by using a T20 bit screwdriver.
5. Disconnect Ethernet cables.
6. Disconnect the power and the fan cable.
7. To allow for better reach to the RF connectors, partially remove the PA.
8. Remove Tx IN and Tx Out cables.

   NOTE: Do not disconnect any of the cables from the N-Way splitter or combiners.

   WARNING: Wait for the PA module to cool down before attempting to remove it.
   AVERTISSEMENT: Attendez que le module de l'amplificateur de puissance (AP) refroidisse avant de tenter de le retirer.

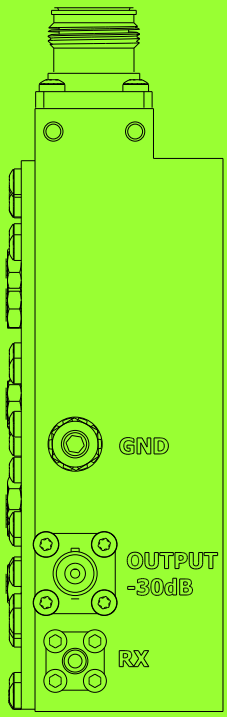
9. Fully remove the PA module from the card cage.
10. Partially insert the replacement PA module so that the retainer lines are aligned with the guides in the card cage, leaving room to access the RF connectors.
11. Reconnect the Ethernet cables, the power cable and the fan cable to the replacement PA module.
12. Fully insert the replacement PA module into the card cage.
13. Secure the PA module to the chassis by fastening the four screws to 17 in-lbs with a T20 bit screwdriver.
14. In PCA, discover the new PA module. See Discovering the Hardware on page 123.
15. In PCA, check the records of the XCVR by performing the following actions:
    a. Navigate to **Services** → **Event Monitoring**.
    b. In the **Event Monitoring** view, expand the **Power Amplifier** node.

9.9

Replacing the Site Preselector

You can replace the site preselector without shutting the power down.

Figure 66: Site Preselector Filter (700/800)



Prerequisites:
Obtain:

- Replacement site preselector
- T20 bit screwdriver
- 3/8" nut driver
- Electrostatic discharge (ESD) wrist strap (Motorola Solutions part number RSX4015A, or equivalent) that must be worn during the removal and installation of the site preselector.

Procedure:

1. Wear an electrostatic discharge (ESD) strap and connect its cable to a verified good ground.

   ⚠ **CAUTION:** Wear the ESD strap throughout the whole procedure to prevent ESD damage to any components.
   ATTENTION: Portez la dragonne ESD tout au long de la procédure pour éviter que les composants soient endommagés par les décharges électrostatiques.

2. Remove the site preselector from the rack by performing the following actions:
   a. Remove all cables from the site preselector.
   b. Remove the grounding cable from the site preselector by using the 3/8" nut driver.
   c. Remove the two screws that secure the site preselector tray to the Radio System Distribution System (RFDS) card cage by using the T20 bit screwdriver.

   d. Remove the four screws on the bottom of the site preselector tray by using the T20 bit screwdriver.

3. Install the replacement site preselector by performing the following actions:
   a. Secure the replacement site preselector to the tray by using the 4 screws tightened with the T20 bit screwdriver.
   b. Insert the replacement site preselector tray so that the retainer lines are aligned with the notch in the card cage and tighten the two screws by using the T20 bit screwdriver.
   c. Reconnect the grounding cable to the site preselector by using the 3/8" nut driver.
   d. Reconnect all cables to the site preselector.
4. Ensure that the system is operating properly by checking the receiver sensitivity.

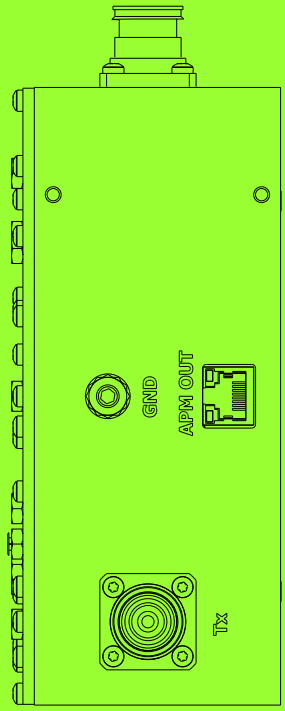
9.10 Replacing the Transmit Filter

WARNING: Shock hazard. The DBR M12 MultiCarrier Site contains dangerous voltages which can cause severe electrical shock or damage to equipment. You must disable power to the system before servicing the transmit filter.
AVERTISSEMENT: Risque d'électrocution. Le site DBR M12 MultiCarrier contient des tensions dangereuses qui peuvent provoquer une décharge électrique grave ou des dommages à l'équipement. Vous devez couper l'alimentation du système avant l'entretien de cette pièce.

IMPORTANT: Before you replace or remove the transmit filter, you must turn off the power to the site if the entire site is connected to the transmit filter that you want to replace or remove. Turning off the power to the site, causes any affiliated subscribers to relocate to another channel at an adjacent site. You must disable the site before powering down so the system does not attribute the loss of channel to a failure.

DRA

Figure 67: Site Transmit Filter



Prerequisites:
Obtain:

- Replacement site transmit filter
- T20 bit screwdriver
- 3/8" nut driver
- Electrostatic discharge (ESD) wrist strap (Motorola Solutions part number RSX4015A, or equivalent) that must be worn during the removal and installation of the transmit filter.

Procedure:

1. Wear an electrostatic discharge (ESD) strap and connect its cable to a verified good ground.

   ⚠ **CAUTION:** Wear the ESD strap throughout the whole procedure to prevent ESD damage to any components.
   AVERTISSEMENT: Risque d'électrocution. Le site DBR M12 MultiCarrier contient des tensions dangereuses qui peuvent provoquer une décharge électrique grave ou des dommages à l'équipement. Vous devez couper l'alimentation du système avant l'entretien de cette pièce.

2. In Provisioning and Configuration Agent (PCA), disable all of the power amplifiers (PAs) associated with the PMU/Tx post filter by performing the following actions:

   a. Navigate to **Services** → **Requested States**.

   b. In the **Requested States** view, expand the **Power Amplifier** node.

   c. Expand the node for the rack where the PA is installed.

   d. From the drop-down list next to the PA, select **Disable**.

   e. Repeat step 2d to be diabled.

3. Remove the site transmit filter from the rack, by performing the following actions:

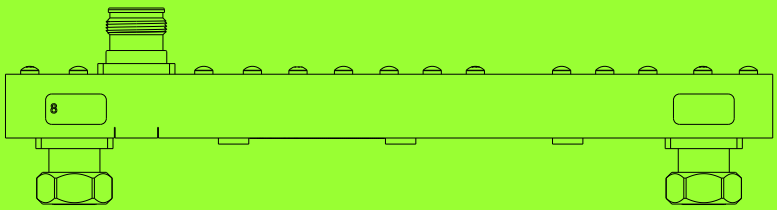
   a. Remove all cables from the site transmit filter.
   b. Remove the grounding cable from the site transmit filter by using the 3/8" nut driver.
   c. Remove the two screws that secure the site transmit filter tray to the Radio System Distribution System (RFDS) card cage by using the T20 bit screwdriver.
   d. Remove the four screws on the bottom of the site transmit filter tray by using the T20 bit screwdriver.
4. Install the replacement site transmit filter by performing the following actions:
   a. Secure the replacement site transmit filter to the tray by using the four screws tightened with the T20 bit screwdriver.
   b. Insert the replacement site transmit filter tray so that the retainer lines are aligned with the notch in the card cage and tighten the two screws by using the T20 bit screwdriver.
   c. Reconnect the grounding cable to the site transmit filter by using the 3/8" nut driver.
   d. Reconnect all cables to the site transmit filter.
5. In PCA, discover the new PMU/Tx post filter. See Discovering the Hardware on page 123.
6. In PCA, check the Tx Bank records by performing the following actions:
   a. Navigate to **Services** → **Event Monitoring**.
   b. In the **Event Monitoring** view, expand the **Transmit Bank** node.
7. In Provisioning and Configuration Agent (PCA), enable all of the power amplifiers (PAs) associated with the PMU/Tx post filter by performing the following actions:
   a. Navigate to **Services** → **Requested States**.
   b. In the **Requested States** view, expand the **Power Amplifier** node.
   c. Expand the node for the rack where the PA is installed.
   d. From the drop-down list next to the PA, select **Enable**.
   e. Repeat step 7d to be enabled.
8. In PCA, validate the associated Tx Bank, Tx power capability by performing the following actions:
   a. Navigate to **Services** → **RFDS Configuration**.
   b. In the **Transmit Path** view, click **Test**.

9.11 Replacing the Phasing Harness

WARNING: Shock hazard. The DBR M12 MultiCarrier Site contains dangerous voltages which can cause severe electrical shock or damage to equipment. You must disable power to the system before servicing this part.
AVERTISSEMENT: Risque d'électrocution. Le site DBR M12 MultiCarrier contient des tensions dangereuses qui peuvent provoquer une décharge électrique grave ou des dommages à l'équipement. Vous devez couper l'alimentation du système avant l'entretien de cette pièce.

IMPORTANT: Before you replace or remove the phasing harness, you must turn off the power to the site if the entire site is connected to the phasing harness that you want to replace or remove. Turning off the power to the site, causes any affiliated subscribers to relocate to another channel at an adjacent site. You must disable the site before powering down so the system does not attribute the loss of channel to a failure.

Figure 68: Phasing Harness



Prerequisites:
Obtain:

- Replacement phasing harness
- Electrostatic discharge (ESD) wrist strap (Motorola Solutions part number RSX4015A, or equivalent) that must be worn during the removal and installation of the phasing harness.

Procedure:

1. Wear an electrostatic discharge (ESD) strap and connect its cable to a verified good ground.

   CAUTION: Wear the ESD strap throughout the whole procedure to prevent ESD damage to any components.
   ATTENTION: Portez la dragonne ESD tout au long de la procédure pour éviter que les composants soient endommagés par les décharges électrostatiques.

2. In the Provisioning and Configuration Agent (PCA), disable all of the power amplifiers (PAs) by performing the following actions:
   a. Navigate to **Services** → **Requested States**.
   b. In the **Requested States** view, expand the **Power Amplifier** node.
   c. Expand the node for the rack where the PA is installed.
   d. From the drop-down list next to the PA, select **Disable**.
   e. Repeat step 5d to be disabled.
3. Remove the phasing harness from the rack, by performing the following actions:
   a. Remove antenna cable.
   b. On the phasing harness, disconnect the connectors that connect to each post filter.
4. Install the replacement phasing harness by performing the following actions:
   a. On the phasing harness, connect the connectors that connect to each post filter

      NOTE: You must install the replacement phasing harness in a way that the connectors labeled with a particular frequency band are connected to the appropriate post filters.

   b. Connect the antenna cable to the phasing harness.
5. In the Provisioning and Configuration Agent (PCA), enable all of the power amplifiers (PAs) by performing the following actions:
   a. Navigate to **Services** → **Requested States**.
   b. In the **Requested States** view, expand the **Power Amplifier** node.
   c. Expand the node for the rack where the PA is installed.
   d. From the drop-down list next to the PA, select **Enable**.

   e. Repeat step 5d for all PAs to be enabled.

6. In PCA, validate the associated Tx Bank, Tx power capability by performing the following actions:
   a. Navigate to **Services** → **RFDS Configuration**.
   b. In the **Transmit Path** view, click **Test**.

9.12 Replacing the N-Way Combiner

You can perform this procedure to replace the 2-3 Way combiner and the 4-6 Way combiner. The number of cables that you must disconnect and reconnect, varies between the 2-3 Way combiner and the 4-6 Way combiner.

WARNING: Shock hazard. The DBR M12 MultiCarrier Site contains dangerous voltages which can cause severe electrical shock or damage to equipment. You must disable power to the system before servicing this part.
AVERTISSEMENT: Risque d'électrocution. Le site DBR M12 MultiCarrier contient des tensions dangereuses qui peuvent provoquer une décharge électrique grave ou des dommages à l'équipement. Vous devez couper l'alimentation du système avant l'entretien de cette pièce.

IMPORTANT: Before you replace or remove the N-Way combiner, you must turn off the power to the site if the entire site is connected to the N-Way combiner that you want to replace or remove. Turning off the power to the site, causes any affiliated subscribers to relocate to another channel at an adjacent site. You must disable the site before powering down so the system does not attribute the loss of channel to a failure.
If the DBR M12 MultiCarrier Site has more than one N-Way combiner, you do not need to power off the remaining N-Way Combiner and its associated power amplifiers (PAs). If the DBR M12 MultiCarrier Site has only one N-Way combiner, replacing it shuts down the entire rack.

Figure 69: 2-3 Way Combiner

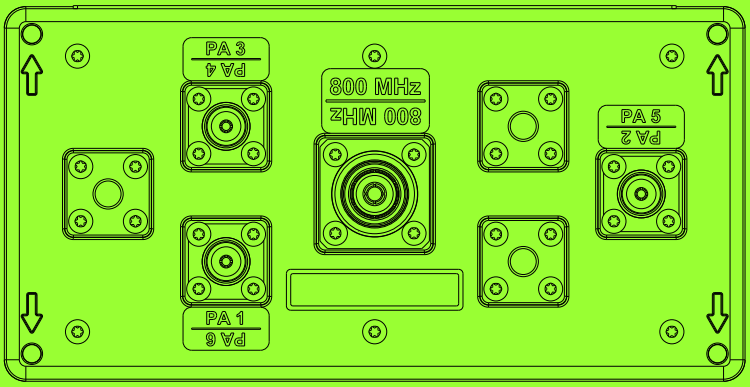
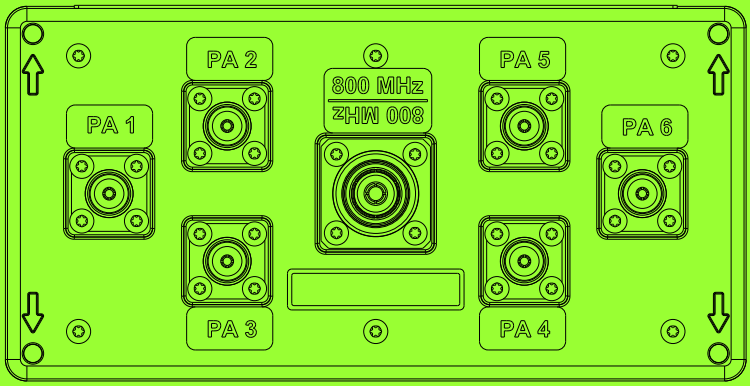


Figure 70: 4-6 Way Combiner



Prerequisites:
Obtain:

- Replacement N-Way combiner
- T20 bit screwdriver
- Electrostatic discharge (ESD) wrist strap (Motorola Solutions part number RSX4015A, or equivalent) that must be worn during the removal and installation of the N-Way combiner.

Procedure:

1. Wear an electrostatic discharge (ESD) strap and connect its cable to a verified good ground.

   ⚠ **CAUTION:** Wear the ESD strap throughout the whole procedure to prevent ESD damage to any components.
   ATTENTION: Portez la dragonne ESD tout au long de la procédure pour éviter que les composants soient endommagés par les décharges électrostatiques.

2. In the Provisioning and Configuration Agent (PCA), disable all of the power amplifiers (PAs) associated with the N-Way combiner that you want to replace by performing the following actions:
   a. Navigate to **Services** → **Requested States**.
   b. In the **Requested States** view, expand the **Power Amplifier** node.
   c. Expand the node for the rack where the PA is installed.
   d. From the drop-down list next to the PA, select **Disable**.
   e. Repeat step 2d for all PAs to be disabled.
3. Remove the N-Way combiner from the rack by performing the following actions:
   a. Label and disconnect all cables from the N-Way Combiner.

      You do not have to disconnect the other end of the cables from the power amplifier or the post filter.
   b. In the corner of the N-Way combiner, remove the four screws by using a T20 bit srewdriver.
4. Install the replacement N-Way combiner by performing the following actions:
   a. Secure the replacement N-Way combiner to the mounting bracket bu using the four screws tightened with a T20 bit screwdriver.
   b. Reconnect all cables to the N-Way combiner.
5. In PCA, enable all of the PAs associated with the PMU/Tx post filter Bank by performing the following actions:

a. Navigate to **Services** → **Requested States**.
b. In the **Requested States** view, expand the **Power Amplifier** node.
c. Expand the node for the rack where the PA is installed.
d. From the drop-down list next to the PA, select **Enable**.
e. Repeat step 5d for all PAs to be enabled.

6. In PCA, validate the associated Tx Bank, Tx power capability by performing the following actions:
   a. Navigate to **Services** → **RFDS Configuration**.
   b. In the **Transmit Path** view, click **Test**.

9.13

Replacing the N-Way Splitter

You can replace the N-Way splitter without shutting the power off.

Figure 71: 2-3 Way Splitter

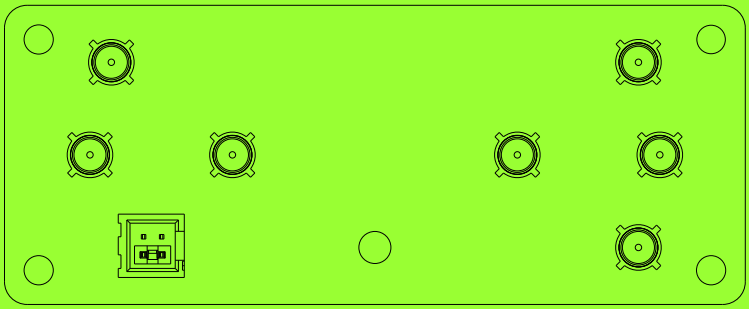
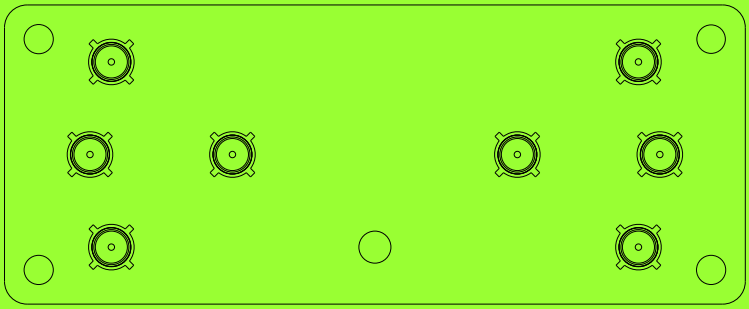


Figure 72: 4-6 Way Splitter



Prerequisites:
Obtain:

- Replacement N-Way splitter
- T20 bit screwdriver
- Electrostatic discharge (ESD) wrist strap (Motorola Solutions part number RSX4015A, or equivalent) that must be worn during the removal and installation of the N-Way splitter.

Procedure:

1. Wear an electrostatic discharge (ESD) strap and connect its cable to a verified good ground.

   CAUTION: Wear the ESD strap throughout the whole procedure to prevent ESD damage to any components.
   ATTENTION: Portez la dragonne ESD tout au long de la procédure pour éviter que les composants soient endommagés par les décharges électrostatiques.

2. Remove N-Way splitter from the power amplifier (PA) card cage by performing one of the following actions:

If…	Then…
If you want to remove the 2-3 way splitter,	perform the following actions: **a.** Label and disconnect all cables attached to the 2-3 Way splitter to be replaced. **b.** Note down the location of the shrouded header. **c.** Remove the RF jumper cable and the jumper in the shrouded header. **d.** Remove the screw that secures the board to the card cage by using a T20 bit screwdriver. **e.** Remove the 2-3 Way splitter board from the snap-in standoffs. Removing the splitter board may require some manual force to unseat.
If you want to remove the 4-6 way splitter,	perform the following actions: **a.** Label and disconnect all cables attached to the 4-6 Way splitter to be replaced. **b.** Remove the screw that secures the board to the card cage by using a T20 bit screwdriver. **c.** Remove the 4-6 Way splitter board from the snap-in standoffs. Removing the splitter board may require some manual force to unseat.

3. Install the N-Way combiner in the power amplifier (PA) card cage by performing one of the following actions:

If…	Then…
If you want to install the 2-3 way splitter,	perform the following actions: **a.** Place the replacement 2-3 Way splitter into the location of the removed one, and snap it into place. **b.** Secure the screw that secures the board to the card cage by using a T20 bit screwdriver. **c.** Reconnect the RF jumper cable and the jumper in the shrouded header. **d.** Reconnect the remaining cables to the 2-3 Way splitter.

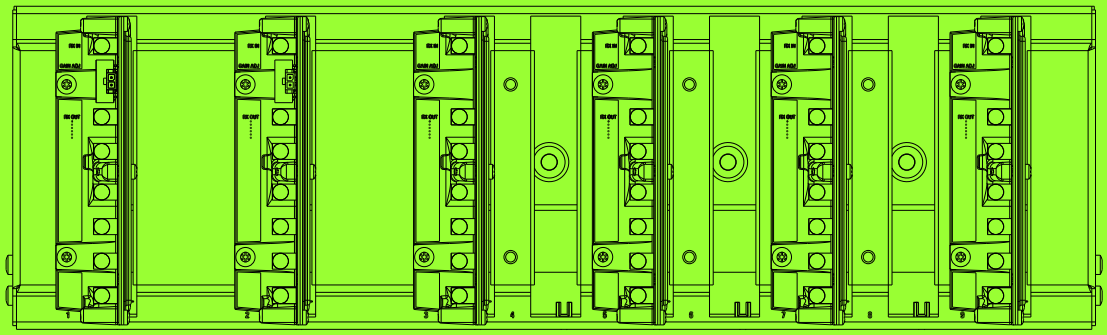
If…	Then…
If you want to install the 4-6 way splitter,	perform the following actions: **a.** Place the replacement 4-6 Way splitter into the location of the removed one, and snap it into place. **b.** Secure the screw that secures the board to the card cage by using a T20 bit screwdriver. **c.** Reconnect all the cables to the 4-6 Way splitter.

9.14

Replacing the RMC Modules

You can perform this procedure to replace the individual Site Receive Multi-Coupler (RMC) or Cabinet RMC.

Figure 73: RMC Cage for Site RMC and Cabinet RMC – Fully Populated



For each preselector in the rack, there is one Site RMC. For each Site RMC there is one Cabinet RMC per six or fewer transceiver modules. In case seven or more transceiver modules in the rack, there are two Cabinet RMCs.

Each Site RMC and its Cabinet RMCs are an independent receive branch. If service is required on a particular RMC in one branch, the other branch does not have to be disturbed. For more information on how to disable one branch for servicing purposes, see Replacing the Site Preselector on page 180.

Prerequisites:
Obtain:

- Replacement RMC module
- T20 bit screwdriver
- Electrostatic discharge (ESD) wrist strap (Motorola Solutions part number RSX4015A, or equivalent) that must be worn during the removal and installation of the RMC Modules.

Procedure:

1. Wear an electrostatic discharge (ESD) strap and connect its cable to a verified good ground.

   CAUTION: Wear the ESD strap throughout the whole procedure to prevent ESD damage to any components.
   ATTENTION: Portez la dragonne ESD tout au long de la procédure pour éviter que les composants soient endommagés par les décharges électrostatiques.

2. Perform one of the following actions:

If…	Then…
If you want to replace the Site RMC,	perform the following actions: **a.** Note down how the RF cables are connected to the RMC module. **b.** Note down the position of the DIP switch gain setting. **c.** Disconnect the RF cables from the RMC module. **d.** Remove the two screws that secure the RMC module by using the T20 bit screwdriver **e.** Slide the RMC module out of the rack. **f.** Install the replacement RMC module by tightening the two screws that secure the RMC module to 17 in-lbs with the T20 bit screwdriver. **g.** Reconnect all the cables to the RMC module. **h.** Ensure that the DIP switch settings are correct.
If you want to replace the Cabinet RMC,	perform the following actions: **a.** Note down how the RF cables are connected to the RMC module. **b.** Disconnect the RF cables from the RMC module. **c.** Remove the two screws that secure the RMC module by using the T20 bit screwdriver **d.** Slide the RMC module out of the rack. **e.** Install the replacement RMC module by tightening the 2 screws that secure the RMC module to 17 in-lbs with the T20 bit screwdriver. **f.** Reconnect all the cables to the RMC module.

Chapter 10

DBR M12 MultiCarrier Site Troubleshooting and Disaster Recovery

This chapter provides disaster recovery procedures for the DSC 8500 Trunking RF Site.

IMPORTANT:
Do not perform the DSC 8500 Trunking RF Site recovery if a DSC 8500 failed during **Software Upgrade** action. In this case, software upgrade must be recovered before starting the DSC 8500 Trunking RF Site disaster recovery. See Recovering the DSC 8500 Failed Software Upgrade on page 162.

It is recommended to perform every procedure, except for the Configuring DSC 8500 After Disaster Recovery Software Installation, device by device.

10.1 Power Amplifier Fan Air Filter Maintenance

The following section provides information about the power amplifier (PA) fan filter maintenance frequency, and the possible risk of not maintaining the fan filter.

WARNING: Failure to replace or clean the PA Fan Air filters results in PA thermal alarm events and eventual reduction or loss of TX power.
AVERTISSEMENT: Le fait de ne pas remplacer ou nettoyer les filtres à air du ventilateur de l'amplificateur de puissance (AP) entraîne des événements d'alarme thermique de l'AP et la réduction ou la perte éventuelle de la puissance d'émission.

The DBR M12 MultiCarrier Site is equipped with high performance RF multicarrier power amplifiers that utilize high density heatsink technologies to stay cool. These heatsinks are cooled by high power fans and are equipped with air filters to reduce debris accumulation in the heatsinks. Permanent removal of the air filters results in significant debris accumulation in the heatsink fins which reduce their thermal efficiency. Cleaning of the heatsinks requires the removal of the PAs from service which results in temporary loss of site performance and capacity.

The PA Fan Air filter is a replaceable and cleanable media filter, which can be easily changed without the need to take the PAs or fans out of service. For most R56-compliant sites equipped with environmental control and sufficient isolation from the outdoor environment, an annual service or replacement cycle can be expected. In harsh conditions with high levels of airborne dust or very high operating temperatures, a shorter (6 month or as needed) service or replacement cycle may be required.

The PA fan filters should be replaced, not cleaned. The expense of filter cleaning and the risk of not removing all debris must be weighed against the cost of full replacement. However, if replacement is not possible or if cleaning is highly desired, the filter may be cleaned with slightly compressed air, vacuumed, and/or rinsed with clean water. If a degreaser is required, you must use only a mild detergent, such as dishwashing liquid. You must avoid using harsh solvents or cleaning agents. If filters are cleaned with water, the filters should be completely dry before reinstalling. Even though this type of filter may be cleaned, replacement is recommended every two to three years on average, or after approximately every four to eight cleaning cycles, whichever comes first.

You can replace the fan filter by first pulling it from the slot in the fan module, using the flexible handle, and then sliding the replacement filter into its place.

You must push the replacement filter until it touches the back of the module.

DRAFT

10.2

DSC 8500 Troubleshooting

This section describes actions that can be taken to troubleshoot issues associated with DSC 8500s at the site.

You must start troubleshooting with identifying the faulty DSC 8500s In the Provisioning and Configuration Agent (PCA), from the **Services** drop-down menu, you can select one of the following:

Site Status

The **Site Status** view provides a graphical representation of the site with color and textual indications of the health of various elements at the site. This view provides information about the location of the faulty DSC 8500s within the site.

Event Monitoring

The **Event Monitoring** view provides a tabular or textual view of the current health of various elements at the site (including DSC 8500s). This view also provides hints at recovery action within the text of the fault. The **Event Archive** tab provides some level of historical information on the health of various elements at the site.

Logs

The **Logs** view provides information that you can use for further analysis of the problems observed at the site.

Network Capture

The **Network Capture** view provides information that you can use for further analysis of the problems observed at the site.

The DSC 8500 health can also be assessed by checking the DSC 8500 LEDs. See DSC 8500 Physical Description on page 24.

Table 32: Suggested DSC 8500 Troubleshooting Actions

Fault Cause	Fault Severity	Description	Suggested Troubleshooting Actions
Missing	Critical	The discovered DSC 8500 is not detected at the site.	• Check the DSC to DSC Ethernet connections. • Check the DSC 8500 switch port configurations. • Check the power connection to the DSC 8500. • Power cycle the DSC 8500. • Wipe and re-deploy the DSC 8500. See Wiping the Software and Sensitive Data on page 139 • Replace the DSC 8500. See Replacing the DSC 8500 Hardware on page 165.
Reference Lost	Critical	The DSC 8500 inventoried reference is missing.	1. In the PCA, check the DSC 8500 reference source by navigating to **Services** → **Time Reference Status**.

Fault Cause	Fault Severity	Description	Suggested Troubleshooting Actions
			2. Check the general reference. See Site Reference Troubleshooting on page 193.
Reference not Ready	Critical	The DSC 8500 inventoried reference is not locked.	1. If applicable, check the connected GPS. 2. Check the general reference. See Site Reference Troubleshooting on page 193.
RF not Available	Critical	The DSC 8500 cannot process the RF signals from the transceiver(s).	• In the PCA, restart the DSC 8500 by navigating to **Services** → **Requested States**, expanding the **DSC** node, and from the drop-down menu selecting **Hard reset**. • Replace the DSC 8500. See Replacing the DSC 8500 Hardware on page 165.
Not in Inventory	Minor	The DSC 8500 is detected at the site but is not added to the inventory.	Discover the hardware. See Discovering the Hardware on page 123.
Fan Unknown, Fan Fail	Minor	The DSC 8500 fan module detects an issue.	Replace the fan. See Replacing the DSC 8500 Fan Assembly on page 167.

10.3 Site Reference Troubleshooting

This section describes actions that can be taken to troubleshoot issues associated with references (GPS, extended holdover, external reference) utilized by the site to maintain call performance.

To troubleshoot issues associated with the site reference, in the Provisioning and Configuration Agent (PCA), from the **Services** drop-down menu, you can select one of the following:

Event Monitoring

The **Event Monitoring** view provides a tabular or textual view of the current health of the various site elements, including site reference. This view also provides hints for the recovery action within the text of the fault. The **Event Archive** tab provides some level of historical information on the health of various elements at the site.

Time Reference Status

The **Time Reference and Frequency Status** view provides real time insight into the state of available references and how they interact with the DSC 8500 at the site.

Table 33: Suggested GPS Troubleshooting Actions

Fault Cause	Fault Severity	Description	Suggested Troubleshooting Actions
Missing	Critical	The DBR M12 MultiCarrier Site hardware discovered GPS(s) that are no longer detected by the site.	• Check the GPS connection. • Check the GPS cable and antenna. • Replace GPS cable or antenna.
Not Ready	Major	The DBR M12 MultiCarrier Site detected a GPS that is not currently capable of providing a time reference.	• In the PCA, check the GNSS configuration by navigating to **Services → GNSS Configuration**. • Ensure that the GPS Antenna is capable of viewing satellites. • In the PCA check the time reference status by navigating to **Services → Time Reference Status**. • Wait for approximately 15 minutes for the reference to valid satellites to become ready. • Check the GPS connections. • Replace the GPS antenna.
Redundancy Missing	Minor	Two GNSS antennas are discovered but only one is available.	• Check the GPS connection. • Check the GPS cable and antenna. • Replace the GPS cable or antenna.
Present not Inventoried	Minor	The DBR M12 MultiCarrier Site detected a GPS receiver that is not added to the inventory through the hardware discovery option.	Discover the hardware. See Discovering the Hardware on page 123.

The troubleshooting actions described in the following table are only applicable to the sites with the DSC 8500 with the internal rubidium oscillator.

Table 34: Suggested Troubleshooting Actions for DSC 8500s with Extended Holdover Option

Fault Cause	Fault Severity	Description	Suggested Troubleshooting Actions
Missing	Critical	The DBR M12 Multi-Carrier Site detected one or both of the DSC 8500 with internal rubidium modules as missing.	• Check if the DSC 8500 with the extended holdover option is powered on and connected to the network. • Reboot or power cycle the DSC 8500 with the extended holdover option. • Replace the DSC 8500 with the extended holdover option. See Replacing the DSC 8500 Hardware on page 165.
Redundancy Missing	Minor		
Not Ready	Major	The DBR M12 Multi-Carrier Site discovered DSC 8500 with internal rubidium modules that are not trained by a GPS.	• In the PCA, check if the site has a locked GPS by navigating to **Services** → **Time Reference**). The extended holdover option requires the GPS for training If the DSC 8500 is powered on (cold), the training can take up to two and a half hours. If the DSC 8500 rubidium is locked and the GPS transitioned from locked to unlocked and back to locked (warm), the training can take up to 20 minutes. • In the PCA, check if the GPS is in the inventory by navigating to **Services** → **Hardware Discovery**.
Present not Inventoried	Minor	The DBR M12 Multi-Carrier Site inventoried the DSC 8500 with internal rubidium modules but the modules were not detected during the hardware discovery procedure.	Discover the hardware. See Discovering the Hardware on page 123.

Table 35: Suggested Troubleshooting Actions for External Reference (PPS)

Fault Cause	Fault Severity	Description	Suggested Troubleshooting Actions
Missing	Critical	The DBR M12 MultiCarrier Site inventoried the External Reference(s) (PPS) that are not detected.	• Check if the external reference is connected and if it produces a 1 PPS signal. • Check the cables connected to the reference source. • Discover the hardware. See Discovering the Hardware on page 123.
Missing Redundancy	Minor		
Not Ready	Major	The DBR M12 MultiCarrier Site detected and inventoried the external reference but the site is not trained to the reference or the Network Time Protocol (NTP) time is missing.	1. Check if the time reference source is available and configured properly. 2. In the PCA, check the time reference status by navigating to **Services → Time Reference Status** Training the site to the reference source may take up to 10 minutes.
Reference Invalid Input	Critical	The DBR M12 MultiCarrier Site inventoried the external reference but the detected signal is invalid (other than 1 PSS, 5 MHz, composite).	Ensure that the reference source is only 1 PPS (not composite PPS/5MHz or other).

10.4 Transceiver Troubleshooting

This section describes actions that can be taken to troubleshoot issues associated with transceivers

To identify the faulty transceivers, in the Provisioning and Configuration Agent (PCA), from the **Services** drop-down menu, you can select one of the following:

Site Status

The **Site Status** view provides a graphical representation of the site with color and textual indications of the health of various elements at the site. This view provides information about the location of the faulty transceiver within the site.

Event Monitoring

The **Event Monitoring** view provides a tabular or textual view of the current health of various elements at the site (including XCVRs). This view also provides hints at recovery action within the text of the fault. The **Event Archive** tab provides some level of historical information on the health of various elements at the site.

For more information about the transceiver front panel LEDs and ports, see .

The transceiver health can also be assessed by checking the transceiver LEDs. See XCVR Physical Description on page 28.

Table 36: Suggested Transceiver Troubleshooting Actions

Fault Cause	Fault State	Description	Suggested Troubleshooting Actions
Unknown	Critical	The DSC 8500s associated with the transceivers are not detected.	DSC 8500 Troubleshooting on page 192
Missing	Critical	A transceiver inventoried through hardware discovery procedure is no longer detected at the site.	• Check the Ethernet cables that connect the transceiver and the DSC 8500s. • Check the DSC 8500 switch port configurations of the transceiver ports. • Check if the transceiver is properly installed in the chassis. • In the PCA, reset the transceiver by navigating to **Services** → **Requested States**. • The connected DSC 8500 automatically attempts to recover the transceiver through a periodic 10 minute power reset (through the network switch ports). • Replace the transceiver. See Replacing the Transceiver Module on page 176.
Ex Fail, Tx Power Control	Critical	The transceiver cannot maintain the transmit power.	• The DSC 8500 attempts to recover the transceiver through a five minute periodic transmit test. • Check if the transceiver is properly installed in the chassis. • In the PCA, reset the transceiver by navigating to **Services** → **Requested States**, expanding the **Transceiver** node, and from the drop-down menu selecting **Reboot**. • Replace the transceiver. See Replacing the Transceiver Module on page 176.
Rx Fail	Critical	The transceivers have problems on the receive path.	• Check the transceivers RX1/2 Input connections. • In the PCA, reset the transceiver by navigating to **Services** → **Requested States**, expanding the **Transceiver** node, and from the drop-down menu selecting **Reboot**.

Fault Cause	Fault State	Description	Suggested Troubleshooting Actions
			• Replace the transceiver. See Replacing the Transceiver Module on page 176.
Branch xxx	Critical, Major	The transceiver detected an issue with one of the receive branches or detected an imbalance.	• Check the transceivers RX1/2 Input connections. • In the PCA, check the branch imbalance configuration on the associated channel by navigating to **Configuration → Channel** • Check the RMC and antenna: ○ Validate the receive paths by using the PCA (**Services → RF Channel Status**) for an Rx test pattern and a communication analyzer to generate a test pattern. ○ Check the site RMC dip switch settings.
Redundancy Missing	Major	The transceiver requires a specific network connection to each DSC 8500 in the rack.	Check the Ethernet cable and switch configuration connection with the associated DSC 8500.
Not in Inventory	Minor	A transceiver is detected at the site that is not currently inventoried.	Discover the hardware. See Discovering the Hardware on page 123.
Not Initialized	Critical	Transitional faults that are logged during the initialization of the transceiver.	If the faults persist: • In the PCA, reset the transceiver by navigating to **Services → Requested States**, expanding the **Transceiver** node, and from the drop-down menu selecting **Reboot**. • Replace the transceiver. See Replacing the Transceiver Module on page 176.
Reference Unlock	Major		

10.5

Power Amplifier Troubleshooting

This section describes actions that can be taken to troubleshoot issues associated with power amplifier(s) (PAs).

To identify the faulty PAs, in the Provisioning and Configuration Agent (PCA), from the **Services** drop-down menu, you can select one of the following:

Site Status

The **Site Status** view provides a graphical representation of the site with color and textual indications of the health of various elements at the site. This view provides information about the location of the faulty PA within the site.

Event Monitoring

The **Event Monitoring** view provides a tabular or textual view of the current health of various elements at the site (including PAs). This view also provides hints at recovery action within the text of the fault. The **Event Archive** tab provides some level of historical information on the health of various elements at the site.

The PA health can also be assessed by checking the PA LEDs. See MCPA Physical Description on page 30.

Table 37: Suggested Troubleshooting Actions for Power Amplifiers

Fault Cause	Fault State	Description	Suggested Troubleshooting Actions
Hardware Controlled Disabled	Disabled	The PA is internally disabled by diagnostic software. Most likely causes are temperature, reflected power or VSWR.	In the PCA, identify the alarm that possibly disabled the PA by navigating to **Services** → **Event Monitoring** → **Event Archive** and perform one of the following actions: ● Alarm caused by temperature: **1.** Check the fan. **2.** Check the fan filter. ● Alarm caused by VSWR, high or low power out: **1.** Check the phasing cables (VSWR, high/low power out) and connections. **2.** Check the N-Way combiner. **3.** Check the Tx post filter (In and Out). **4.** Check the Tx antenna. ● Faulty PA: Replace the PA. See Replacing the Power Amplifier on page 178.
Unknown	Critical	The DSC 8500s associated with the PA are not detected.	DSC 8500 Troubleshooting on page 192
Missing	Critical	The PA module added to inventory through the hardware discovery is not detected by the site.	● Check the Ethernet cables between the PA and the DSC 8500s ● Check the DSC 8500 switch port configurations for the PAs. ● In the PCA, reset the PA by navigating to **Services** → **Requested States**, expanding the **Power Amplifier** node, and from the drop-down menu selecting **Reboot**. ● Replace the PA. See Replacing the Power Amplifier on page 178.

Fault Cause	Fault State	Description	Suggested Troubleshooting Actions
Hardware Fail	Critical	There is an internal hardware issue in the PA or the PA is not synchronized to the requested transmit state.	• In the PCA, toggle the PA by performing the following actions: **1.** Navigate to **Services** → **Requested States**. **2.** Expand the Power Amplifier node **3.** From the drop-down list next to the PA select Disable and click Apply. **4.** From the drop-down list next to the PA select Enable and click Apply. • In the PCA, reset the PA by navigating to **Services** → **Requested States**, expanding the **Power Amplifier** node, and from the drop-down menu selecting **Reboot**. • Power off/on the PA by using the DC IN of the individual PA. • Replace the PA. See Replacing the Power Amplifier on page 178.
High Reverse Power, High VSWR	Critical	The PA module detected a high reverse power or a high VSWR.	• Check the combiner phasing cables for damage. • Check the N-Way combiner for damage. • Check the N-Way combiner connections. • Check the PA RF connections. • Check the Tx post filter connections. • Check the combiner phasing cables, the N-Way combiner, and the Tx post filter for the correct band of operation. • Check the Tx antenna. • In the PCA, reset the PA by navigating to **Services** → **Requested States**, expanding the **Power Amplifier** node, and from the drop-down menu selecting **Reboot**. • Replace the PA. See Replacing the Power Amplifier on page 178.
Power Out	Critical	The PA module detects a high power out.	• Check the splitter phasing cables for damage. • Check the N-Way splitter for damage. • Check the N-Way splitter connections.

Fault Cause	Fault State	Description	Suggested Troubleshooting Actions
			• Check the splitter phasing cables and the N-Way splitter for the correct band of operation. • In the PCA, reset the PA by navigating to **Services** → **Requested States**, expanding the **Power Amplifier** node, and from the drop-down menu selecting **Reboot**. • Replace the PA. See Replacing the Power Amplifier on page 178.
High Internal Temperature	Critical	The PA module detects a high temperature.	• Check the associated fans and replace if necessary. • Check the associated fan filter and replace if necessary. • Check for other airflow obstructions. • Replace the PA. See Replacing the Power Amplifier on page 178.
Redundancy Missing	Major	The PA module requires a specific network connection to each DSC 8500 in the rack.	Check the correct Ethernet cable and switch configuration connection with the associated DSC 8500.
Not in Inventory	Minor	The DBR M12 MultiCarrier Site detected a PA module that was not inventoried or was incorrectly connected through the hardware discovery process.	• In the PCA, check the bank ID by navigating to **Services** → **Event Monitoring** and expanding the **Transmit Bank** node. If the bank ID is not correct check the PA connection to the N-Way splitter. • Discover the hardware. See Discovering the Hardware on page 123.
Recovery in Progress	Warning Failed	The PA module is internally tested to check if it can be recovered.	No actions required.
Not Initialized	Critical	Transitional faults that are logged during the initialization of the transceiver.	If the faults persist: • In the PCA, reset the PA by navigating to **Services** → **Requested States**, expanding the **Power Amplifier** node, and from the drop-down menu selecting **Reboot**. • Replace the PA. See Replacing the Power Amplifier on page 178.
Reference Unlock	Major		

10.6

Transmit Bank Troubleshooting

This section describes actions that can be taken to troubleshoot issues associated with the transmit bank. A transmit bank consists of a Tx post filter or a Power Monitor Unit (PMU) and a group of associated MCPA modules.

To identify the faulty transmit bank, in the Provisioning and Configuration Agent (PCA), from the **Services** drop-down menu, you can select one of the following:

Site Status

The **Site Status** view provides a graphical representation of the site with color and textual indications of the health of various elements at the site. This view provides information about the location of the faulty transmit bank within the site.

Event Monitoring

The **Event Monitoring** view provides a tabular or textual view of the current health of various elements at the site (including transmit bank). This view also provides hints at recovery action within the text of the fault. The **Event Archive** tab provides some level of historical information on the health of various elements at the site.

Table 38: Suggested Troubleshooting Actions for Transmit Banks

Fault Cause	Fault State	Description	Suggested Troubleshooting Actions
		The transmit bank or PMU are not visible in the **Site Status** view.	• Ensure that the PMU network cable is connected to the correct DSC 8500 and switch port. • Ensure that the DSC 8500 switch port is enabled.
	Unconfigured		Ensure that the Tx post filter or the PMU Ethernet connection is connected to the correct port on the correct DSC 8500.
Unknown	Critical	The associated DSC 8500 is not detected, and the transmit bank attempts to recover the DSC 8500.	No actions required.
PMU Missing	Critical	The Tx post filter or PMU that is in inventory is no longer detected by the DBR M12 MultiCarrier Site.	• Ensure that the Tx post filter or the PMU Ethernet connection is connected to the correct port on the correct DSC 8500. • Ensure that the DSC 8500 PMU switch port is enabled.
High VSWR	Major	The Tx post filter or PMU reports a VSWR that is above the configured threshold.	• In the PCA, check the VSWR Threshold configuration by navigating to **Serv-**

Fault Cause	Fault State	Description	Suggested Troubleshooting Actions
			ices → RFDS Configuration → Transmit Path. ● Check the Tx post filter (Out). ● Check the Tx antenna.
Power Budget Exceeded	Minor	The transmit bank cannot support the channels that are capable of transmitting on the bank.	● In the PCA, check if the configured transmit power of the channels at the site are too high for the Tx bank to support by navigating to **Services → Site Status** and checking the value for Max TX Power/Chl. ● Check if the associated PA is user disabled, internally disabled or reports temperature and VSWR issues and recover the failed PA to restore the Tx bank to full budget.
PMU Not in Inventory	Minor	The DBR M12 MultiCarrier Site detected a PMU that was not added to inventory through the hardware discovery procedure.	Discover the hardware. See Discovering the Hardware on page 123.

10.7 Channel Troubleshooting

This section describes actions that can be taken to troubleshoot issues associated with a channel. A channel is a logical entity that represents the high level call processing capabilities of a given trunking channel.

To identify the faulty channels, in the Provisioning and Configuration Agent (PCA), from the Services drop-down menu, you can select one of the following:

Site Status

The Site Status view provides a graphical representation of the site with color and textual indications of the health of various elements at the site. This view provides information about the location of the faulty channel(s) within the site.

Event Monitoring

The **Event Monitoring** view provides a tabular or textual view of the current health of various elements at the site (including channel). This view also provides hints at recovery action within the text of the fault. The **Event Archive** tab provides some level of historical information on the health of various elements at the site.

Table 39: Suggested Channel Troubleshooting Actions

Fault Cause	Fault State	Description	Suggested Troubleshooting Actions
Hardware Failure	Critical	The logical channel has a problem with associated hardware.	In the PCA, check the channel hardware associations (DSC 8500, XCVR, PAs) by navigating to **Services** → **Site Status**.
Band Plan Mismatch	Major	The logical channel is misconfigured.	In the PCA, check the channel and band plan configuration by navigating to **Configuration** → **Channel** or **Configuration** → **Band Plan**.

10.8 RF Modem Troubleshooting

This section describes actions that can be taken to troubleshoot issues associated with an RF modem. An RF modem is a logical entity that represents the RF signal processing capabilities of a given trunking channel.

To identify the faulty RF modems, in the Provisioning and Configuration Agent (PCA), from the **Services** drop-down menu, you can select:

Event Monitoring

The **Event Monitoring** view provides a tabular or textual view of the current health of various elements at the site (including RF modem). This view also provides hints at recovery action within the text of the fault. The **Event Archive** tab provides some level of historical information on the health of various elements at the site.

Table 40: Suggested RF Modem Troubleshooting Actions

Fault Cause	Fault State	Description	Suggested Troubleshooting Actions
Unallocated	Disabled	The RF processing (RF modem) of a logical channel is not started or allocated.	• In the PCA, check if the transmit power of the channels are below the maximum by navigating to **Services** → **Site Status** and checking the value for Max TX Power/Chl. • Check the transmit bank or power amplifier(s) (PAs) associated with the RF modem. • Check the state of the associated XCVR. The disabled XCVR causes the unallocated fault state.
Tx/Rx Hardware Fail	Critical	The transceiver associated with the RF modem is not capable of receiving or transmitting.	Check the state of the associated XCVR.

Fault Cause	Fault State	Description	Suggested Troubleshooting Actions
Illegal Carrier	Critical	The RF Modem detected an illegal carrier.	• In the PCA, check the illegal carrier settings for the associated channel by navigating to **Services → Configuration → Channel**. • In the PCA, check the RSSI Measurement activity of the channel by navigating to **Services → RF Channel Status**. • Check the noise floor for the desired frequency. • Ensure that the Network Access Code (NAC) is configured correctly. • To get additional informational traps related to illegal carrier, enable **Serviceability Fault Reporting** for the desired channel by navigating to **Configuration → Channel**.
Launch Time Failure	Critical	The RF modem attempted to transmit several packets but failed due to issues with timing.	• In the PCA, check the subsite time reference by navigating to **Services → Time Reference Status**. • Check the prime site time reference. The subsite and prime site have different time. • Check for any site reference alarms • Check the technician logs for any RF modem alarms. • Check for Subsite Link Delay from Prime Site, and ensure that in the Prime Site value, the Launch Time offset is adjusted for the maximum subsite delay recorded across subsites.
RTP Link Failure	Critical	The RF modem lost the network link to the logical channel.	• Check the subsite network connectivity. • Check the prime site network connectivity.

Fault Cause	Fault State	Description	Suggested Troubleshooting Actions
			• Check for alarms on channels related to the subsite RF modem.
Tx Impaired	Minor Failed	The RF Modem is impaired because of an issue with the associated PAs.	Check the transmit bank and the associated PAs.

10.9

Logon Troubleshooting

Table 41: Logon Suggested Troubleshooting Actions

Issue Description	Suggested Troubleshooting Actions
Unable to log on to the Provisioning and Configuration Agent (PCA) by using an Active Directory account.	• Check the LDAP server configuration. See Configuring Centralized Authentication for PCA Users on page 90. You can check the available LDAP servers by using the following command: `nslookup -type=srv _ldap._tcp.<DOMAIN_NAME>` • Ensure that the users are members of the required Active Directory groups. See Configuring Centralized Authentication for PCA Users on page 90.
Unable to log on to the Linux platform by using an Active Directory account.	• Ensure that users are members of the required Active Directory groups. See Configuring DSC 8500 Active Directory Authentication on page 131. • Wait for the Active Directory join and Active Directory synchronization to finish. Active directory may not work until both Active Directory join and Active Directory synchronization are finished. Active Directory synchronization may require more time in systems with more domain controllers (DC) (it might take up to six hours).
PCA **admin** account password is invalid.	The PCA **admin** account is different from the Linux platform **admin** account. Changing the Linux platform **admin** account password does not change the password for the PCA **admin** account.
You forgot the PCA **admin** account password.	1. Connect to the DSC 8500s Linux platform through SSH or a serial connection.

Issue Description	Suggested Troubleshooting Actions
	2. Run the `service_entry host reset_pca_password` command. The PCA admin account password resets to default.
You forgot the Linux platform **admin** account password.	1. Log on to the DSC 8500s Linux platform serial connection by using the root password. 2. Reset the admin account password by running the `passwd admin` command.
You forgot the Linux platform **root** and **admin** account password.	1. Log on to the DSC 8500 by using your Active Directory account. 2. Wipe and reinstall the DSC 8500. See Wiping the Software and Sensitive Data on page 139 3. If the Active Directory is not configured, contact Centralized Managed Support Operations (CMSO).

10.10 On-Premises Software Hub Troubleshooting

Table 42: Suggested Troubleshooting Actions for On-Premises Software Hub

Issue Description	Suggested Troubleshooting Actions
On-Premises Software Hub displays the `The application failed to start because port 49691 was already in use` message.	Troubleshooting the On Premises Software Hub Failure to Start When the Port 49691 Is in Use on page 208
On-Premises Software Hub displays the `The device clock is not synchronized with the one on the local machine` message.	Ensure that the clock on the local PC is synchronized properly with the Network Time Protocol (NTP) time source.
Initial deployment, site expansion or FRU replacement action fails at around 4% with the `Failed at {'<IP_address>': 'Installing Platform via PXE'}` error message.	• Ensure that the service PC has IP address in the same subnet as the DSC 8500s • Deploy the DSC 8500 Software. See Deploying the DSC 8500 Software on page 85.
Software transfer procedure fails.	Software Transfer Failure Recovery on page 158
Software upgrade procedure fails.	Software Upgrade Failure Recovery on page 158

10.10.1

Troubleshooting the On Premises Software Hub Failure to Start When the Port 49691 Is in Use

Procedure:

1. Close the OPSH application.
2. Open the **PowerShell** console by performing the following actions:
   a. From **Start**, click **Search**.
   b. In the search field, type: `powershell`
   c. Right-click **Windows PowerShell** and select **Run as administrator**.
   d. If the **User Account Control** window appears, click **Yes**.

   If you are not logged on with an administrative account, enter the Administrator credentials.
3. At the **PowerShell** prompt, enter:

   ```
   Get-NetTCPConnection -LocalPort
   49690,49691,49714,49715,49716,49717,49718,49719,49720,49721,49722 2>$null
   ```
4. If the command lists any processes, identify and stop the processes in the **Windows Task Manager** by performing the following actions:
   a. Open the **Windows Task Manager**.
   b. In the search bar, enter the IDs of the processes displayed by the command in step 3.
   c. Right-click the desired processes and from the drop-down list select **End task**.
   d. Start the OPSH (OPSH) application.
5. If the command above does not list any processes, go to step 6.
6. Reserve OPSH port ranges from being used by other applications by performing the following actions:

   IMPORTANT: Reserving the OPSH port ranges may prevent other applications from working correctly.

   a. Open the Windows command prompt as an administrator and enter the following commands:

      ```
      netsh int ipv4 add excludedportrange protocol=tcp startport=49690
      numberofports=2
      ```

      ```
      netsh int ipv4 add excludedportrange protocol=tcp startport=49714
      numberofports=9
      ```

      ```
      netsh int ipv4 add excludedportrange protocol=udp startport=49690
      numberofports=2
      ```

      ```
      netsh int ipv4 add excludedportrange protocol=udp startport=49714
      numberofports=9
      ```

   b. Start the OPSH application.

Chapter 11

DBR M12 MultiCarrier Site Expansion

MultiCarrier Site expansion scenarios, you must refer to the ordering guide which contains a tool that generates a material list for expansion based on the current hardware and the desired final configuration.

Some expansions may require new full racks. The expansions that require a new full rack are noted in the expansion tool available in the ordering guide. You must order new racks from Motorola Solutions.

The following table provides a general reference of the possible expansion scenarios:

Table 43: DBR M12 MultiCarrier Site Expansion Scenarios

Functional Expansion	Hardware Impact
Increasing the top of rack power per channel or adding redundancy	Additional power amplifier (PA) required.
Adding channels without additional transmit path	Additional XCVRs and possibly additional PAs required. Adding channels may require a conversion from the 2-3 Way to the 4-6 Way, which requires an additional 4-6 Way combiner and 4-6 Way splitter.
Adding second transmit bank	Additional XCVRs, PAs, Tx Filter, 2-3 Way splitter, 2-3 Way combiner required.
Adding receive diversity	Additional preselector, site Receive Multi-Coupler (RMC), cabinet RMC(s) required.

11.1 DBR M12 MultiCarrier Site RFDS Equipment Specifications

This section provides specifications for the following RFDS equipment: transmit filter, preselector filter, and receiver Multi-Coupler / low noise amplifier.

IMPORTANT: Specifications are subject to change without notice.

11.1.1 DBR M12 MultiCarrier Site RFDS Elevation Derating

Above 3000 meters (9800’), the peak power derating for the Tx RFDS is 1dB/1km (0.3 dB/1000ft). So at 5000 meters (16400’) full power is limited to 9 carriers.

11.1.2
DBR M12 MultiCarrier Site Transmit Filter Specifications (700/800/900 MHz)

Table 44: DBR M12 MultiCarrier Site Transmit Filter Specifications (700/800/900 MHz)

	Tx Filter Spec Limit (700/800/900 MHz)	Typical	Notes
Frequency Range	762–776 MHz, 851–870 MHz		
Insertion Loss (700 or 800 MHz filter)	0.5 dB	0.3 dB	
Port Return Loss	14 dB	17 dB	
Rx Selectivity	60 dB		
RMS Input Power	650 W		
Peak Instantaneous Power	32k W		
Passive Intermodulation	–135 dBc		2 x 43 dBm
RF Connector Type			
Power Monitor Unit (PMU) Accuracy	+/- 10% (20–600 W), +/- 20% (1–20 W)		
Power Monitor Connector Type	RJ45 Ethernet		
Forward and Reflected Power Range	0–650 W		

11.1.3
DBR M12 MultiCarrier Site Preselector Filter Specifications (700/800 MHz)

Table 45: DBR M12 MultiCarrier Site Preselector Filter Specifications (700/800 MHz)

	DBR M 12 RF Site Preselector Spec Limit (700/800 MHz)	Typical
Frequency Range	792–825 MHz	
Insertion Loss	1 dB	0.8 dB
Return Loss	14 dB	17 dB
Tx Selectivity	75 dB	
Test Port Coupling	–30 dB	
Input Connector (Antenna)	4.3-10 female	

	DBR M 12 RF Site Preselector Spec Limit (700/800 MHz)	Typical
Output Connector	QMA female	
Test Port Connector	BNC	

11.2 Installing the DBR M12 MultiCarrier Site Expansion Rack

Procedure:

Content to be provided.

11.3 Deploying the DSC 8500 Software to the DBR M12 MultiCarrier Site Expansion Rack

You can deploy the DSC 8500 software by using On-Premises Software Hub.

Prerequisites:
Obtain:

- Service laptop connected to the DSC 8500 service port
- DSC 8500 installation media

Ensure that:

- All devices at the site are powered on, enabled, and functioning properly. Any faults, issues, or resetting of devices must be corrected before the software transfer.
  For details regarding any recent resets of site devices, see the Unified Event Manager (UEM). The Provisioning and Configuration Agent (PCA) shows details on the status of DSC 8500s.
- The latest version of On-Premises Software Hub is used.

Procedure:

1. From the desktop, launch the **On-Premises Software Hub** application.
2. Import the DSC 8500 software bundle. See Importing the DSC 8500 Software Bundle.

DSC 8500 Software Installation

3. Discover the site. See Discovering the Site on page 76.
4. Perform one of the following actions:

If…	Then…
If the expected site does not appear after the discovery,	in the Provisioning Configuration Agent (PCA) or the Unified Event Manager (UEM) verify the site status and the router port configuration and repeat step 3.

If…	Then…
If the site does not show the correct number of DSC 8500s after the discovery,	perform the following actions: **a.** In the PCA or the UEM, check the fault status of each DSC 8500. **b.** Ensure that each DSC 8500 is enabled. **c.** Ensure that the configuration of ports between the DSC 8500 and routers is correct.
If the expected site appears,	go to step 5.

5. Connect to the site. See Connecting to the Site on page 77.
6. Deploy the DSC 8500 software by performing the following actions:
   a. For the site where the DSC 8500 is replaced, from the **Action** drop-down list, select **Site Expansion**.
   b. In the **Site Expansion** window, from the **Bundle** drop-down list, select the DSC 8500 upgrade software bundle that you want to transfer.
   c. Click **Continue**.

   The DSC 8500 software installation process starts.

11.4 Adding a Transceiver

You can use this procedure to add a transceiver (channel) to a rack or bank.

Procedure:

1. Insert the XCVR module into a slot associated with the transmit (TX) bank.
2. Connect the XCVR network cables to both DSC 8000s/DSC 8500s in the rack.

   Cables must be connected to DSC 8000s/DSC 8500s associated with the XCVR slot.
3. In Provisioning and Configuration Agent (PCA), discover the hardware. See Discovering the Hardware on page 123.
4. In PCA, configure the new channel. See Configuring the Channels on page 102.
5. In PCA, validate the channel health by performing the following actions:
   a. Navigate to **Services** → **Event Monitoring**.
   b. In the **Event Monitoring** view, expand the **RF Modem** node.

11.5 Adding a Power Amplifier

Prerequisites:
Obtain:

- Torque driver with T20 bit that you can set to 17 in-lbs
- One of the following power amplifier (PA) expansion kit for frequency band:
  - DLNXXXX 800 MHz Band PA expansion kit
  - DLNXXXX 700 MHz Band PA expansion kit

- Additional power supply module DLN8001A is required, if the rack uses the T8926 AC supply system.
- Electrostatic discharge (ESD) wrist strap (Motorola Solutions part number RSX4015A, or equivalent).

Procedure:

1. Wear an electrostatic discharge (ESD) strap and connect its cable to a verified good ground.

   CAUTION: Wear the ESD strap throughout the whole procedure to prevent ESD damage to any components.
   A single fan kit cools adjacent PA pairs 1,2 / 3,4 / 5,6. If the adjacent PA where an expansion PA is added is not turned off, removing the PA blank panel and airflow plug temporarily exposes the potentially spinning fan blades. You must take extreme caution if the adjacent PA is not turned off after removing the airflow plug. Do not put hands inside the PA card cage.

   ATTENTION: Portez la dragonne ESD tout au long de la procédure pour éviter que les composants soient endommagés par les décharges électrostatiques. Un seul assemblage de ventilateur refroidit les paires adjacentes 1,2/3,4/5,6 de l'amplificateur de puissance (AP). Si l'AP adjacent où un AP d'extension est ajouté n'est pas éteint, le retrait du panneau vide de l'AP et du bouchon de circulation d'air expose temporairement les pales de ventilateur potentiellement en rotation. Vous devez être extrêmement prudent si l'AP adjacent n'est pas éteint après avoir retiré le bouchon de circulation d'air. Ne mettez pas les mains à l'intérieur du compartiment de la carte de l'AP.

2. Ensure that the breaker that corresponds to the PA that you want to add is in the OFF position.
3. Remove the four screws securing the blank panel in the slot where you want to add the expansion PA by using a driver with a T20 bit.

   WARNING: Disconnecting cables from an N-Way combiner or an N-Way splitter may cause damage to equipment.
   AVERTISSEMENT: La déconnexion des câbles du combineur N-Way ou du séparateur N-Way peut endommager l'équipement

4. Move cables connected from the N-Way combiner and the N-Way splitter out of the cavity covered by the blank panel.

   Do not disconnect the cables from the N-Way combiner or N-Way splitter.

5. With caution, grab the tab on the rubber airflow plug and remove it from the card cage.
6. Slide the new PA into the card cage and leave some room to connect the cables from the N-Way combiner and the N-Way splitter.
7. Connect the two cables from the N-Way combiner and the N-Way splitter to the Tx In and Tx Out.
8. Secure the PA to the card cage by tightening the four provided M4 to 17 in-lbs with a T20 bit.
9. Connect the PA to the two DSC 8500 by using the provided LAN cables.

   For more information about the DSC 8500 port connections, see DSC 8500 Physical Description on page 24.

10. Connect the fan connection from the fan to the PA.
11. Find the unused PA DC power cable labeled with the slot that the PA is added to and connect the DC power cable to the PA.

    The previously unused PA DC power cables are already in place secured to the side of the PA card cage.

12. Secure the Ethernet cables to the rack by using the provided velcro cable ties.
13. Secure the remaining cables to the rack by using the provided ratcheting cable ties.
14. Turn on the breaker that corresponds to the newly-added PA.

15. In the Provisioning and Configuration Agent (PCA), discover the new PA. See Discovering the Hardware on page 123.
16. In the PCA, check the records of the PA by performing the following actions:
    a. Navigate to **Services** → **Event Monitoring**.
    b. In the **Event Monitoring** view, expand the **Power Amplifier** node.
17. Optional: To update the Tx bank benchmark, in the PCA perform the Tx bank transmit test by performing the following actions:
    a. Navigate to **Services** → **RFDS Configuration**.
    b. In the **Transmit Path** view, click **Test**.

11.6 Adding an XCVR Module

Table 46: XCVR Connections – Primary Receive Path

XCVR	Connection
XCVR 1-6	Connects to Cabinet RMC 1
XCVR 7-12	Connects to Cabinet RMC 3
XCVR 1	Connects to RX out 1 on RMC 1
XCVR 2	Connects to RX out 2 on RMC 1
XCVR 7	Connects to Rx out 1 on RMC 3
XCVR 8	Connects to Rx out 2 on RMC 3

Table 47: XCVR Connections – Rx Diversity

XCVR	Connection
XCVR 1	Connects to RX out 1 on RMC 2
XCVR 2	Connects to RX out 2 on RMC 2
XCVR 7	Connects to RX out 1 on RMC 4
XCVR 8	Connects to Rx out 2 on RMC 4

Prerequisites:
Obtain:

- Torque driver with T20 bit that you can set to 17 in-lbs
- XCVR Bank 1 or Bank 2 expansion kit
  The only difference in the Bank 1 and Bank 2 expansion kit is the length of the included Ethernet cables. Bank 1 XCVRs (or XCVRs 1-6 in a 6+ XCVR 4-6 way system) route the Ethernet cables to the left on the rack. Bank 2 XCVRs (or XCVRs 7-12 in a 6+ XCVR 4-6 way system) route the Ethernet cables to the right on the rack.
- Electrostatic discharge (ESD) wrist strap (Motorola Solutions part number RSX4015A, or equivalent).

QMA to QMA coax cable (3066543B02), for systems with Rx diversity

Procedure:

1. Wear an electrostatic discharge (ESD) strap and connect its cable to a verified good ground.

   CAUTION: Wear the ESD strap throughout the whole procedure to prevent ESD damage to any components.
   ATTENTION: Portez la dragonne ESD tout au long de la procédure pour éviter que les composants soient endommagés par les décharges électrostatiques.

2. Determine the correct slot for the additional XCVR in the XCVR cage and slide the additional XCVR into place by pushing the module into the backplane connector.

   The XCVR front panel should be flush or close to flush with the card cage front panel. For more information about the slot for the additional XCVR, see DBR M12 MultiCarrier Site Expansion on page 209.

3. Insert the two provided M4 screws into the card cage and tighten them to 17 in-lbs with a T20 bit.
4. Connect the XCVR to the two DSC 8500 by using the provided Ethernet cables.

   For more information about the DSC 8500 port connections, see DSC 8500 Physical Description on page 24.

5. Secure the Ethernet cables to rack by using the provided velcro cable ties.
6. Connect the included QMA to QMA coax cable to port RX 1 on the XCVR.
7. Connect the second side of the QMA to QMA coax cable to port Rx Out on cabinet Receive Multi-Coupler (RMC) 1 or 3 depending on which slot the XCVR is in.

   For more information about the XCVR connections, see Table 46: XCVR Connections – Primary Receive Path on page 214.

8. **Systems with RX diversity:** Perform the following actions:
   a. Connect the included QMA to QMA coax cable to port RX 2 on the XCVR.
   b. Connect the second side to Rx Out on Cabinet RMC 2 or 4 depending on which slot the XCVR is in.

      For more information about the XCVR connections, see Table 47: XCVR Connections – Rx Diversity on page 214.

9. In the Provisioning and Configuration Agent (PCA), discover the new XCVR. See Discovering the Hardware on page 123.
10. In the PCA, check the records of the XCVR by performing the following actions:
    a. Navigate to **Services** → **Event Monitoring**.
    b. In the **Event Monitoring** view, expand the **Transceiver** node.

11.7 Adding a Cabinet RMC

The cabinet Receive Multi-Coupler (RMC) is not installed separately. It is always installed with other equipment.

Prerequisites:
Obtain:

- Torque driver with T20 bit that you can set to 17 in-lbs
- One or two cabinet RMC expansion kits depending on the expansion scenario
- One QMA to QMA coax cable (3066543B02), for each XCVR
- Electrostatic discharge (ESD) wrist strap (Motorola Solutions part number RSX4015A, or equivalent)

Procedure:

1. Wear an electrostatic discharge (ESD) strap and connect its cable to a verified good ground.

   CAUTION: Wear the ESD strap throughout the whole procedure to prevent ESD damage to any components.
   ATTENTION: Portez la dragonne ESD tout au long de la procédure pour éviter que les composants soient endommagés par les décharges électrostatiques.

2. Determine the correct slot for the additional cabinet RMC in the RMC card cage.
3. Ensure that the cabinet RMC position is correct.

   For more information about the correct XCVR position, see RMC Physical Description on page 31.

4. Slide the additional cabinet RMC into place.
5. Secure the cabinet RMC to the card cage by tightening the two provided M4 to 17 in-lbs with a T20 bit.
6. Connect the cabinet RMC to the site RMC with the included QMA cable.

   For more information about the RMC connections, see RMC Physical Description on page 31.

7. Connect the cabinet RMC to the XCVR with the QMA to QMA coax cable.

   For more information about the RMC connections, see RMC Physical Description on page 31.

11.8 Adding Receive Diversity

Prerequisites:
Obtain:

- Torque driver with T20 bit that you can set to 17 in-lbs
- Nut driver
- Preselector expansion kit
- Site Receive Multi-Coupler (RMC) expansion kit
- For six or less XCVRs, one cabinet RMC expansion kit
- For more than six XCVRs, two cabinet RMC expansion kits
- One QMA to QMA coax cable (3066543B02), for each XCVR
- Electrostatic discharge (ESD) wrist strap (Motorola Solutions part number RSX4015A, or equivalent)

Procedure:

1. Wear an electrostatic discharge (ESD) strap and connect its cable to a verified good ground.

   CAUTION: Wear the ESD strap throughout the whole procedure to prevent ESD damage to any components.
   ATTENTION: Portez la dragonne ESD tout au long de la procédure pour éviter que les composants soient endommagés par les décharges électrostatiques.

2. Insert the site RMC into the second site RMC slot in the RMC card cage.
3. Insert the cabinet RMC into the position for the cabinet RMC 2.
4. If the site has more than six XCVRs, insert the second cabinet RMC into the position for the cabinet RMC 4.

   For more information, see RMC Physical Description on page 31.

5. Secure each site and cabinet RMC by tightening the two included M4 screws to 17 in-lbs by using a T20 bit.

6. Secure the preselector to the included preselector bracket by tightening the included M4 screws to 17 in-lbs by using a T20 bit.
7. Slide the preselector bracket into the RFDS tray and secure it by tightening the two provided M4 screws to 17 in-lbs by using a T20 bit.
8. Remove the nut on the stud on the front of the site RMC by using a nut driver.
9. Attach one end of the included ground bond cable to the stud and secure the nut by using a nut driver.
10. Attach the other end of the included ground bond cable to the rack or cabinet busbar by using the included M6 screw.

    For more information, see RFDS Physical Description on page 37.
11. Connect the preselector to the newly-added site RMC with the included QMA cable.
12. Connect the cabinet RMC to the site RMC with the included QMA cable.
13. Connect the cabinet RMC to the XVCR with the QMA to QMA coax cable.

    For more information, see RMC Physical Description on page 31.
14. Connect the site RMC alarm cable to the site RMC.

    For more information, see RMC Physical Description on page 31.
15. Connect the receive antenna to the preselector.
16. For each channel, in the Provisioning and Configuration Agent (PCA) perform the following actions:
    a. Navigate to **Configuration** → **Channel**.
    b. In the **Channel list** view select the channel and click the icon.
    c. In the **Edit Channel** view, set the **Rx Dual Branch Receiver Operations** to **Enabled**.
    d. In the **Edit Channel** view, set **Rx Branch Imbalance Delta [dB]**.
    e. In the **Edit Channel** view, set **Rx Branch Imbalance Time to Failure [sec]**.

11.9 Adding a Transmit Bank

Prerequisites:
Obtain:

- Torque driver with T20 bit that you can set to 17 in-lbs
- Electrostatic discharge (ESD) wrist strap (Motorola Solutions part number RSX4015A, or equivalent)
- XCVR Bank 2 expansion kit for each channel that you want to add
- Cabinet RMC expansion kit
- Three 800 MHz or 700MHz band power amplifier (PA) expansion kits
- 800 MHz or 700MHz 2-3 Way combiner expansion kit
- 800 MHz or 700MHz 2-3 Way splitter expansion kit
- 800 MHz or 700MHz Tx filter expansion kit

For systems with Rx diversity, obtain:

- QMA to QMA coax cable (3066543B02) for each XCVR Bank 2 expansion kit
- Cabinet Receive Multi-Coupler (RMC) expansion kit

If the rack uses T8926 AC supply system, obtain 3 additional power supply modules (DLN8001A).

Process:

1. Wear an electrostatic discharge (ESD) strap and connect its cable to a verified good ground.

   CAUTION: Wear the ESD strap throughout the whole procedure to prevent ESD damage to any components.
   ATTENTION: Portez la dragonne ESD tout au long de la procédure pour éviter que les composants soient endommagés par les décharges électrostatiques.

2. Install Bank 2 Tx post filter by performing the following actions:
   a. Secure the Tx post filter to the included bracket by tightening the included M4 flathead screws to 17 in-lbs with a T20 bit.
   b. Slide Tx post filter bracket into the Radio Frequency Distribution System (RFDS) tray and secure it by tightening the two provided M4 pan head screws to 17 in-lbs with a T20 bit.

      For more information, see RFDS Physical Description on page 37.
   c. Connect the Ethernet cable to the power meter connection on Tx post fitler.
   d. Connect the other end of the Ethernet cable to the DSC 8500.

      For more information about the port connections, see DSC 8500 Physical Description on page 24.
   e. Secure the Ethernet cable to the rack by using the included velcro cable ties.
   f. Connect the transmit antenna to the Tx Out on the Tx filter.

      For more information, see RFDS Physical Description on page 37.

3. Install 2-3 Way combiner for Bank 2 by performing the following actions:
   a. Rotate the 2-3 Way combiner so that the PA 2, PA 4 and PA 6 labels are facing up.
   b. Secure the 2-3 Way combiner by tightening the four included screws to 17 in-lbs with a T20 bit.
   c. Connect the included coax cable with 4.3-10 connectors to the center connector of the 2-3 Way combiner.
   d. Connect the other end of the coax cable to the Tx In connector on the new Bank 2 Tx filter.
   e. Connect the three phasing cables to the three remaining connectors on the 2-3 Way combiner.
   f. Leave the other end of each phasing cable free.

      NOTE: The cables that connect the 2-3 Way combiner to the PA are sized for phase matching and are frequency dependent. You must ensure that the labels on the cables correspond to the frequency band of the newly-installed PAs.

   For more information about the 2-3 Way combiner, see N-Way Combiner Physical Description on page 34.

4. Install 2-3 Way splitter for Bank 2 by performing the following actions:
   a. Snap the 2-3 Way splitter into the PA card cage in the Bank 2 position.
   b. Tighten the included M4 screw to 17 in-lbs with a T20 bit.
   c. Connect the QMA to QMA coax cable to the two connectors on the 2-3 Way splitter.

      For more information, see N-Way Splitter Physical Description on page 35.
   d. Ensure that on the 2-3 Way splitter for Bank 2, there is **no** jumper connected in the 4 pin header.
   e. Ensure that on the 2-3 Way splitter for Bank 1, there is a jumper connected in the 4 pin header.
   f. On the 2-3 Way splitter for Bank 1, disconnect the cable connected to the connector labeled as **XCVR BANK B**.
   g. On the new 2-3 Way splitter for Bank 2, connect the disconnected cable to the connector labeled as **XCVR BANK B**.

The cable must be connected on the backplane board side the entire time the connection on the splitter board side is moved.

h. Connect the three coax cables with CMA connectors to the splitter board in MCPA 1, 2 and 3 connectors.

i. Leave the other end of each coax cable free.

NOTE: The cables that connect the 2-3 Way combiner to the PA are sized for phase matching and are frequency dependent. You must ensure that the labels on the cables correspond to the frequency band of the newly-installed PAs.

5. Install the cabinet RMC. See Adding a Cabinet RMC on page 215.

   For a second bank, you must install the new cabinet RMC in the position for the cabinet RMC 3. For the site with the Rx diversity, you must install a second cabinet RMC in the position for the cabinet RMC 4.

6. Install the XCVRs. See Adding an XCVR Module on page 214.

   You must install the Bank XCVRs in the position 7 in the XCVR cardcage.

7. Install the PAs. See Adding a Power Amplifier on page 212.

   You must install Bank 2 PAs in the positions 2, 4 and 6.

8. Ensure that all cables are connected properly.

   For more information about the cabling connections, see Module Physical Description on page 24.

9. In the Provisioning and Configuration Agent (PCA), discover the hardware. See Discovering the Hardware on page 123.

10. Configure the additional channels. See Configuring the Channels on page 102.

11. In the PCA, validate the newly-installed Tx Bank, PAs and XCVRs by performing the following actions:

    a. Navigate to **Services** → **Event Monitoring**.

    b. In the **Event Monitoring** view, expand the **Transmit Bank** node.

12. In the PCA, validate the health of the new channels by performing the following actions:

    a. Navigate to **Services** → **Event Monitoring**.

    b. In the **Event Monitoring** view, expand the **RF Modem** node.

13. If you want to update the Tx bank benchmark, in the PCA perform the Tx bank transmit test by performing the following actions:

    a. Navigate to **Services** → **RFDS Configuration**.

    b. In the **Transmit Path** view, click **Test**.

11.10 Converting from a 2-3 Way System to a 4-6 Way System

Prerequisites:
Obtain:

- Torque driver with T20 bit that you can set to 17 in-lbs
- Electrostatic discharge (ESD) wrist strap (Motorola Solutions part number RSX4015A, or equivalent)
- XCVR Bank 2 expansion kit for each channel that you want to add
- Cabinet RMC expansion kit

- Two or three 800 MHz band power amplifier (PA) expansion kits, or two or three 700 MHz PA expansion kits
- 800 MHz or 700MHz 2-3 Way combiner expansion kit
- 800 MHz or 700MHz 2-3 Way splitter expansion kit
- 800 MHz or 700MHz Tx filter expansion kit

For systems with Rx diversity, obtain:

- QMA to QMA coax cable (3066543B02) for each XCVR Bank 2 expansion kit
- Cabinet Receive Multi-Coupler (RMC) expansion kit

If the rack uses T8926 AC supply system, obtain 3 additional power supply modules (DLN8001A).

Process:

1. Wear an electrostatic discharge (ESD) strap and connect its cable to a verified good ground.

   CAUTION: Wear the ESD strap throughout the whole procedure to prevent ESD damage to any components.
   ATTENTION: Portez la dragonne ESD tout au long de la procédure pour éviter que les composants soient endommagés par les décharges électrostatiques.

2. In the Provisioning and Configuration Agent (PCA), disable all PAs by performing the following actions:
   a. Navigate to **Services** → **Requested States**.
   b. In the **Requested States** view, expand the **Power Amplifier** node.
   c. Expand the node for the rack where the PA is installed.
   d. From the drop-down list next to the PA, select **Disable**.
   e. Repeat step 2d for all PAs to be disabled.
3. Remove the 2-3 Way combiner by performing the following actions:
   a. Disconnect all the cables from the 2-3 Way combiner.

      Do not disconnect the other ends of the cables that are connected to the PAs.
   b. Disconnect the cable connected to the Tx filter.
   c. Remove the four screws on the 2-3 Way combiner by using the T20 bit screwdriver and set the 2-3 Way combiner aside.
4. Install the 4-6 Way combiner by performing the following actions:
   a. Secure the 4-6 Way combiner in the center position in the combiner bracket by tightening the four included screws to 17 in-lbs by using a T20 bit screwdriver.

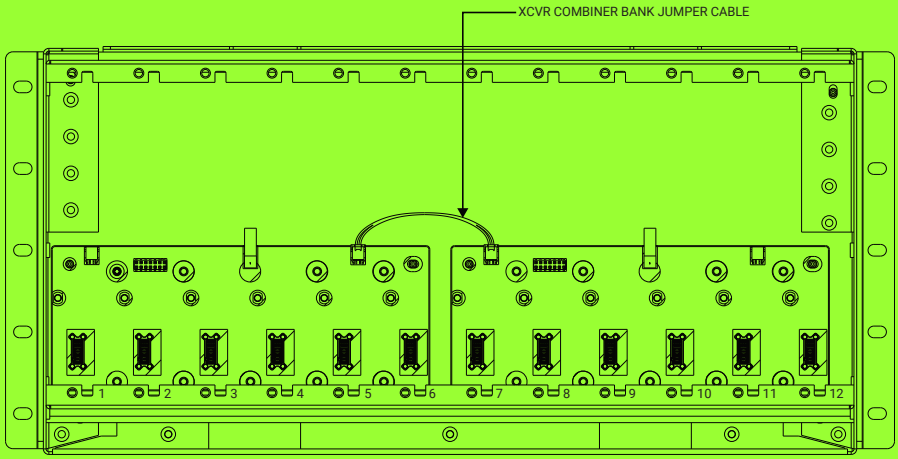
      For more information about the position of the 4-6 Way combiner, see N-Way Combiner Physical Description on page 34.
   b. Connect the three PA cables to the appropriate connectors on the 4-6 Way combiner.
   c. Connect the six phasing cables from the 4-6 Way expansion kit to the remaining PA connectors on the 4-6 Way combiner.

      IMPORTANT: Even if there are less than six PAs in the rack, you must connect all six phasing cables to the 4-6 Way combiner.
      If the cables are not connected properly, the system may not work well or it might result in damage to the system.
5. Install the XCVR combiner jumper cable by performing the following actions:
   a. If XCVR 5 and XCVR 6 are installed, temporarily remove them from the rack.

For more information on how to remove an XCVR module, see Adding an XCVR Module on page 214.

b. Install the included XCVR combiner jumper cable at the back of the rack.

Figure 74: XCVR Combiner Bank Cable



6. Remove the 2-3 Way splitter by performing the following actions:

a. Label and disconnect all cables attached to the 2-3-Way splitter.

b. Remove the screw that secures the board to the card cage by using a T20 bit screwdriver.

c. Remove the 2-3 Way splitter board from the snap-in standoffs.

Removing the splitter board may require some manual force to unseat.

7. Install the 4-6 Way splitter by performing the following actions:

a. On the bottom of the PA cardcage, snap the 4-6 Way splitter into position.

For more information about the location of the N-Way splitter, see N-Way Splitter Physical Description on page 35.

b. Tighten the M4 screw that secures the splitter board to the card cage to 17 in-lbs by using a T20 bit screwdriver.

c. Connect the three PA cables to the appropriate connectors on the 4-6 Way splitter.

d. Connect the six phasing cables from the 4-6 Way expansion kit to the remaining PA connectors on the 4-6 Way splitter.

IMPORTANT: Even if there are less than six PAs in the rack, you must connect all six phasing cables to the 4-6 Way splitter.
If the cables are not connected properly, the system may not work well or it might result in damage to the system.

8. Install the PAs by performing the following actions:

a. Remove the PA blank panels by using the T20 bit screwdriver.

b. Slide each new PA into the PA card cage, leaving room for the RF cables.

c. Connect the 4-6 Way combiner Tx cables to the newly-installed PAs.

d. Connect the 4-6 Way splitter Tx cables to the newly-installed PAs.

e. Route the cables from the 4-6 Way splitter so that they do not block the fans by using the included cable ties and secure the cables at the tie-down locations.

f. If there are any unused PA slots left, slide the unused phasing cables through the securing slots and reinstall the blank panle by using a T20 bit screwdriver set to 17 in-lbs.

g. Push each PA fully into place.

h. Secure each PA by tightening the four included M4 screws to 17 in-lbs by using a T20 bit screwdriver.

i. Connect the PA Ethernet connection to the DSC 1 and DSC 2 by using the included Ethernet cables.

   For more information, see DSC 8500 Physical Description on page 24 and MCPA Physical Description on page 30.

j. Connect the fan cables to the PAs.

k. From the side of the rack, cut the cable ties that secure the expansion PA DC Power cables.

   Each cable is labeled with the number of the PA that it connects to.

l. Connect the DC power cables.

9. Install XCVRs. See Adding an XCVR Module on page 214.
10. Install cabinet RMCs. See Adding a Cabinet RMC on page 215.
11. Ensure that all cables are connected properly.

    For more information about the cabling connections, see Module Physical Description on page 24.
12. Enable the PA breakers that were not previously enabled.
13. In the Provisioning and Configuration Agent (PCA), discover the hardware. See Discovering the Hardware on page 123.
14. Configure the additional channels. See Configuring the Channels on page 102.
15. In the PCA, validate the newly-installed Tx Bank, PAs and XCVRs by performing the following actions:
    a. Navigate to **Services** → **Event Monitoring**.
    b. In the **Event Monitoring** view, expand the **Transmit Bank** node.
16. In the PCA, validate the health of the new channels by performing the following actions:
    a. Navigate to **Services** → **Event Monitoring**.
    b. In the **Event Monitoring** view, expand the **RF Modem** node.
17. If you want to update the Tx bank benchmark, in the PCA perform the Tx bank transmit test by performing the following actions:
    a. Navigate to **Services** → **RFDS Configuration**.
    b. In the **Transmit Path** view, click **Test**.

11.11 Configuring the Expansion Rack

For a physical description of the rack, see DBR M12 MultiCarrier Site Installation on page 46.
For more information about network cabling, see DSC 8500 Network Connections on page 66.

Prerequisites:
Obtain:

- Service laptop with On-Premises Software Hub installed.
- DSC 8500 Installation media

Ensure that:

- The service laptop is connected to any enabled DSC 8500 service port. If not, enable service port on one of the working DSC 8500s. See Configuring the DSC 8500 Switch on page 121.
- All devices at the site are powered on, enabled, and functioning properly.
  Any faults, issues, or resetting of devices must be corrected before the software transfer.

  For details regarding any recent resets of site devices, see the Unified Event Manager (UEM). The Provisioning and Configuration Agent (PCA) displays details about the status of the DSC 8500s.
- The latest version of On-Site Premises Software Hub is used.

Procedure:

1. From the desktop, launch the **On-Premises Software Hub** application.
2. Import the DSC 8500 software bundle. See Importing the DSC 8500 Software Bundle.

   After the software bundle is imported, a success message appears in the right bottom corner.
3. Discover the site. See Discovering the Site on page 76.
4. If the site does not appear after the discovery, in the PCA or UEM verify the site status and the router port configuration and repeat step 3.
5. If the site does not display the correct number of the DSC 8500s after the site discovery, perform the following actions:
   a. In the PCA or UEM, check the fault status of each DSC 8500.
   b. Ensure that each DSC 8500 is enabled.
   c. Ensure that the configuration of ports between the DSC 8500s and routers is correct.
6. Connect to the site. See Connecting to the Site on page 77.
7. Deploy the DSC 8500 software by performing the following actions:
   a. For the site where the DSC 8500 is replaced, from the **Action** drop-down list, select **Site Expansion**.
   b. In the **Site Expansion** window, from the **Bundle** drop-down list, select the DSC 8500 upgrade software bundle that you want to transfer.
   c. Click **Continue**.

   The DSC 8500 software installation process starts.
8. In the PCA, Ensure that the newly-added rack is operational by navigating to **Services** → **Event Monitor**.