



Boot Identity

This Dell technical white paper gives an overview of the Boot Identity feature and the associated operations

Dell Engineering
September 2015

THIS WHITE PAPER IS FOR INFORMATIONAL PURPOSES ONLY, AND MAY CONTAIN TYPOGRAPHICAL ERRORS AND TECHNICAL INACCURACIES. THE CONTENT IS PROVIDED AS IS, WITHOUT EXPRESS OR IMPLIED WARRANTIES OF ANY KIND.

Copyright © September 2015 Dell Inc. All rights reserved. Dell and the Dell logo are trademarks of Dell Inc. in the United States and/or other jurisdictions. All other marks and names mentioned herein may be trademarks of their respective companies.



Table of contents

Executive summary	4
1 Introduction	5
2 Pre-requisites For Boot Identity feature	6
3 Initial Setup	7
4 Saving Boot Identity Profile of NIC/FC Cards	10
5 Applying Boot Identity Profile to Select NIC/FC Partition	12
6 Bringing Up the Spare Server	15
6.1 Clearing Boot Identity Profiles	15
6.2 Deactivating MAC Addresses	16
6.3 Apply saved Boot Identity to new or spare server	16
7 Managing Stored Boot Identity Profiles	17
7.1 Viewing Stored Boot Identity Profiles	17
7.2 Importing Boot Identity Profile	18
7.3 Exporting Boot Identity Profile	18
7.4 Deleting Boot Identity Profile	19
8 Typical Customer used workflow	20
9 Appendix	21
9.1 Sample Boot Identity Profile	21
9.2 Boot Identity Attributes Associated with iSCSI/FCoE/FC Partitions	24
9.3 How to Create and Enable iSCSI/FCoE/FC partitions	27
9.4 Feature Constraint	27



Executive summary

The document provides details on creating and deploying a Boot Identity Profiles, from iSCSI, FC, or FCoE configurations, to enable quick restore of workload to a spare server in the event of server failure.



1 Introduction

The Dell Chassis Management Controller provides the feature to capture the identity of Network Interface Card/Fibre Channel (NIC/FC) partition of server in XML format referred as Boot Identity Profile. Boot Identity Profiles contains unique virtual MAC and WWN/WWPN addresses. The profiles are saved to NFS or CIFS network shares and applied to a spare server with identical NIC/FC card located in the same or different chassis. By applying the Boot Identity profile enables the spare server to SAN boot the operating system and applications of the failed server. However, this feature requires close attention to details on attributes in profile such as I/O Identity, target settings and other protocol specific configurations that could causes issues if misconfigured. The main advantage of this feature is the use of a virtual MAC address pool that is unique and shared across all chassis.

The Boot Identity feature involves creating locally administered virtual MAC address pool database (vmacdb.xml) in network share and saving the Boot Identity profiles from NIC/FC partition which contains the unique MAC address from the virtual MAC address pool. These Boot Identity profiles can be applied to spare server to enable iSCSI/FCoE/FC SAN booting. This feature is supported only with Enterprise license in **VRTX**, **FX2** and **FX2s** variants. No license is required for the **M1000e** Chassis.



2 Pre-requisites For Boot Identity feature

- CMC version **5.1** or later for M1000e, **2.1** or later for VRTX and **1.3** or later for FX2.
- iDRAC version 2.20.20 or later
- Enterprise license for CMC (Applicable only for VRTX and FX2 variants)
- User must have CMC Administrator privileges
- CIFS/NFS Network share to configure in CMC
- Backend connectivity setup for server through IOM to iSCSI/SAN targeted device



3 Initial Setup

The initial setup includes configuring CMC network share and creating locally administered virtual MAC Address Pool database (vmacdb.xml) in the network share.

To configure a network share:

1. Log in to CMC.
2. Navigate to **Server Overview**—>**Setup**—>**Network Share**. Refer Figure 1 Configure Network share.

Edit Network Share



Network Share Settings

Attribute	Value
Protocol	<input checked="" type="radio"/> CIFS <input type="radio"/> NFS
IP Address or Host Name	<input type="text" value="cifs"/>
Share Name	<input type="text" value="samba"/>
Update Folder	<input type="text" value="BI"/> <input type="button" value="Test Directory"/>
File Name (optional)	<input type="text"/>
Server Profile Folder	<input type="text"/> <input type="button" value="Test Directory"/>
Boot Identity Profile Folder	<input type="text" value="BI"/> <input type="button" value="Test Directory"/>
Chassis Profile Folder	<input type="text"/> <input type="button" value="Test Directory"/>
Domain Name	<input type="text"/>
User Name	<input type="text" value="albury"/>
Password	<input type="password" value="*****"/>
<input type="button" value="Test Network Connection"/> <input type="button" value="Apply"/>	

Figure 1 Configure Network share

3. Select the protocol, input network share ip address or host name, share name, boot identity profile folder, username and password and apply. Ensure that the "Test Directory" task is successful.

To create a virtual MAC Address Pool database:

1. Navigate to **Server Overview**—>**Setup**—>**Profiles**.
2. Click the **Boot Identity profiles** tab.
3. Ensure that the "Network Share" under **Stored profiles** displays the network path that was configured earlier.
4. Under **Manage Virtual MAC Address Pool**, the **Starting MAC Address** field displays the default starting MAC address as 0E:00:00:00:00:00. Refer Figure 2 Creating MAC pool

Stored Profiles ▲ Back to top

Options: [Import Profile](#) > [Export Profile](#) > [Delete Profile](#)

Network Share : cifs:// cifs/samba /BI [Edit](#)

Select	Profile Name	Profile Version	Profile Location	View Profile
There is no profile in the network share.				

Manage Virtual MAC Address Pool: ▲ Back to top

Options: [Add MAC Addresses](#) > [Remove MAC Addresses](#)

Create MAC Pool

Starting MAC Address: 0E:00:00:00:00:00 x

Number of MAC Addresses: 10

Create MAC Pool

Figure 2 Creating MAC pool

5. Enter the number of MAC address required in the pool. The default value is 1 . The number depends on the mac addresses required per profile and number of profiles. For example: the value is set to 10.
6. Click **Create MAC pool** tab. The CMC creates 10 virtual MAC addresses. Refer Figure 3 Created Mac Pool shows under Manage Virtual MAC Pool

Manage Virtual MAC Address Pool: ▲ Back to top

Options: [Add MAC Addresses](#) > [Remove MAC Addresses](#)

<input type="checkbox"/>	MAC Address	Node ID	FQDD	Boot File	Status
<input type="checkbox"/>	0E:00:00:00:00:00				unassign
<input type="checkbox"/>	0E:00:00:00:00:01				unassign
<input type="checkbox"/>	0E:00:00:00:00:02				unassign
<input type="checkbox"/>	0E:00:00:00:00:03				unassign
<input type="checkbox"/>	0E:00:00:00:00:04				unassign
<input type="checkbox"/>	0E:00:00:00:00:05				unassign
<input type="checkbox"/>	0E:00:00:00:00:06				unassign
<input type="checkbox"/>	0E:00:00:00:00:07				unassign
<input type="checkbox"/>	0E:00:00:00:00:08				unassign
<input type="checkbox"/>	0E:00:00:00:00:09				unassign

Deactivate MAC Address(es)

Recent Profile Log ▲ Back to top

Options: [Go to Profile Log](#)

Severity	Date/Time	Description
	2015-09-28T19:58:28-0500	A new Virtual MAC Address Pool is created with 10 addresses from 0E:00:00:00:00:00 for Boot Identity profile operations.

Figure 3 Created Mac Pool shows under Manage Virtual MAC Pool

7. The initial status of each MAC Address is 'unassign' as they are not associated with any profile.

NOTE:

The "Create MAC pool" tab is available only if no virtual MAC Address database is created in the network share. Once virtual MAC address database is created, only "Add MAC Addresses" and "Remove MAC Addresses" options will appear under "Manage Virtual MAC Address Pool".

Users can only use unicast MAC addresses in the Virtual MAC Address Pool. The following MAC address ranges are allowed for Boot Identity feature.

02:00:00:00:00:00 - F2:FF:FF:FF:FF:FF

06:00:00:00:00:00 - F6:FF:FF:FF:FF:FF

0A:00:00:00:00:00 - FA:FF:FF:FF:FF:FF

0E:00:00:00:00:00 - FE:FF:FF:FF:FF:FF



4 Saving Boot Identity Profile of NIC/FC Cards

1. Navigate to **Server Overview->Setup->Profiles->Boot Identity Profiles**.
2. Select the server and select the selective FQDD from the FQDD drop-down list.
3. Click **Save identity**.
4. Enter the **Base Profile Name** and **Number of Profiles** that you want to save.
5. Select a starting MAC Address for the base profile from the **Virtual MAC Address** drop-down and click **Save Profile**. Refer Figure 4 Saving Boot Identity profile

The screenshot displays the 'Boot Identity Profiles' configuration interface. At the top, there are tabs for 'Server Profiles', 'Profiles for QuickDeploy', and 'Boot Identity Profiles'. Below these, there are options to '> Save Identity', '-- Select Profile --', '> Apply Identity', and '> Clear Identity'. A table lists server slots with columns for Slot, Slot Name, Model, FQDD, Last Applied Profile, and Status. Slot 1c is selected, and its FQDD is 'NIC.Embedded'. Below the table, the 'Stored Profiles' section shows the 'Save Profile' form. The 'Base Profile Name' is 'FC430_1', the 'Number of Profiles' is '5', and the 'Virtual MAC Address' is '0E:00:00:00:00:00'. The 'Save Profile' button is highlighted.

Slot	Slot Name	Model	FQDD	Last Applied Profile	Status
1a	WIN-V3VCM9ADBLI	PowerEdge FC430	--Select FQD		
1b	SLOT-01b	PowerEdge FC430	--Select FQD		
1c	WIN-TOU0TES1EI2	PowerEdge FC430	NIC.Embedded		
1d	localhost	PowerEdge FC430	--Select FQD		
3a	WIN-O89E5SDFBIM	PowerEdge FM120	--Select FQD		
3b	SLOT-03b		--Select FQD		
3c	localhost.localdomain	PowerEdge FM120	--Select FQD		
3d	q1fy16stomp1d	PowerEdge FM120	--Select FQD		

Stored Profiles [Back to top](#)

Options: [Import Profile](#) > Export Profile > Delete Profile **Network Share :** cifs:// cifs/samba /BI [Edit](#)

Save Profile

Base Profile Name: FC430_1

Number of Profiles: 5

Virtual MAC Address: 0E:00:00:00:00:00

Cancel **Save Profile**

Figure 4 Saving Boot Identity profile

6. The number of templates created are based on the number of profiles the user specified. The format for the name file is -- <base profile name>_<profile number>_<MAC address>. For example: FC630_01_0E0000000000
7. The saved templates are listed under **Stored profiles**. The status of the used MAC address in "Manage Virtual MAC Address Pool" changes to **assign** from **unassign**. Refer Figure 5 Profiles saved under stored profiles and Mac address status changes to assign.

Stored Profiles

[▲ Back to top](#)

Options:
[> Import Profile](#)
[> Export Profile](#)
[> Delete Profile](#)
Network Share : cifs:// cifs/samba /BI
[Edit](#)

Select	Profile Name	Profile Version	Profile Location	View Profile
<input type="radio"/>	FC430_1_00_0E0000000000	Boot Identity	Network Share	> View
<input type="radio"/>	FC430_1_01_0E0000000003	Boot Identity	Network Share	> View

Manage Virtual MAC Address Pool:
[▲ Back to top](#)

Options:
[> Add MAC Addresses](#)
[> Remove MAC Addresses](#)

<input type="checkbox"/>	MAC Address	Node ID	FQDD	Boot File	Status
<input type="checkbox"/>	0E:00:00:00:00:00			FC430_1_00_0E0000000000	assign
<input type="checkbox"/>	0E:00:00:00:00:01			FC430_1_00_0E0000000000	assign
<input type="checkbox"/>	0E:00:00:00:00:02			FC430_1_00_0E0000000000	assign
<input type="checkbox"/>	0E:00:00:00:00:03			FC430_1_01_0E0000000003	assign
<input type="checkbox"/>	0E:00:00:00:00:04			FC430_1_01_0E0000000003	assign

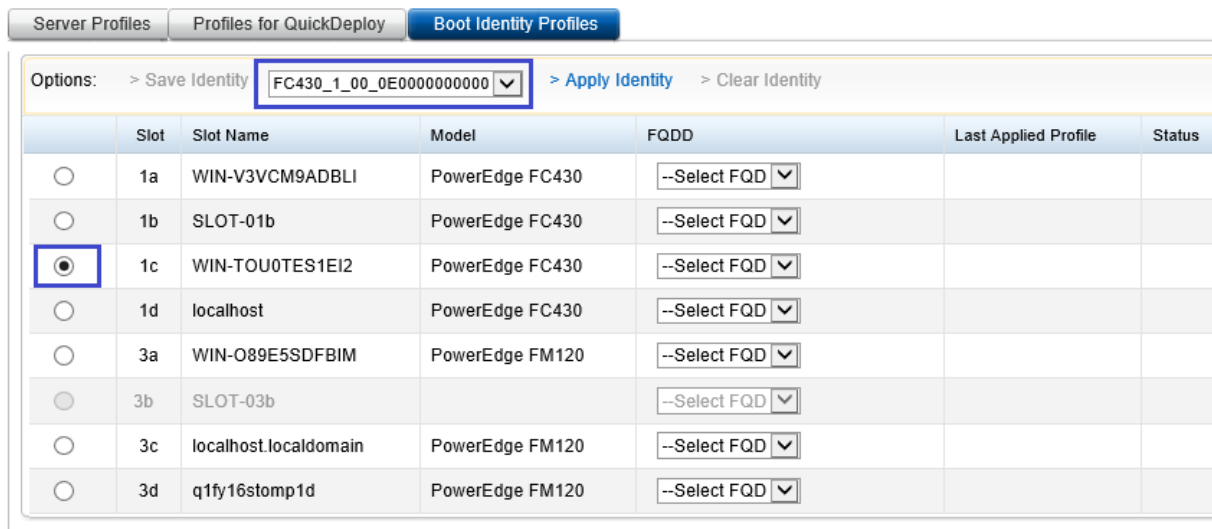
Figure 5 Profiles saved under stored profiles and Mac address status changes to assign

NOTE:

The CSIOR option must be enabled for the servers to complete CSIOR operation and to capture the profiles from the respective server.

5 Applying Boot Identity Profile to Select NIC/FC Partition

1. Edit the saved Boot Identity template from the network share and change values of the attributes for iSCSI/FCoE/FC SAN boot environment. This profile is used later to bring up the spare server.
2. Navigate to **Server Overview->Setup->Profiles->Boot Identity Profiles**.
3. Select the server and select the profile, that must be applied, from the drop-down list. Click **Apply identity**. Refer Figure 6 Applying profile identity to selective NIC/FC card



Options: > Save Identity **FC430_1_00_0E0000000000** > Apply Identity > Clear Identity

	Slot	Slot Name	Model	FQDD	Last Applied Profile	Status
<input type="radio"/>	1a	WIN-V3VCM9ADBLI	PowerEdge FC430	--Select FQD ▼		
<input type="radio"/>	1b	SLOT-01b	PowerEdge FC430	--Select FQD ▼		
<input checked="" type="radio"/>	1c	WIN-TOU0TES1EI2	PowerEdge FC430	--Select FQD ▼		
<input type="radio"/>	1d	localhost	PowerEdge FC430	--Select FQD ▼		
<input type="radio"/>	3a	WIN-089E5SDFBIM	PowerEdge FM120	--Select FQD ▼		
<input type="radio"/>	3b	SLOT-03b		--Select FQD ▼		
<input type="radio"/>	3c	localhost.localdomain	PowerEdge FM120	--Select FQD ▼		
<input type="radio"/>	3d	q1fy16stomp1d	PowerEdge FM120	--Select FQD ▼		

Figure 6 Applying profile identity to selective NIC/FC card

The server reboots and the Boot Identity is applied to the respective NIC partition through Life Cycle Controller. After the Boot Identity is applied, the server boots from iSCSI/FCoE/FC SAN target device. The Last applied profile column against the server displays the applied profile and the corresponding virtual MAC address status changes to "active" from "assign". Refer Figure 7 Assign status of MAC changes to active status.

Options: > Save Identity -- Select Profile -- > Apply Identity > Clear Identity

	Slot	Slot Name	Model	FQDD	Last Applied Profile	Status
<input type="radio"/>	1a	WIN-V3VCM9ADBLI	PowerEdge FC430	--Select FQ		
<input type="radio"/>	1b	SLOT-01b	PowerEdge FC430	--Select FQ		
<input type="radio"/>	1c	WIN-TOU0TES1EI2	PowerEdge FC430	--Select FQ	FC430_1_00_0E0000000000	
<input type="radio"/>	1d	localhost	PowerEdge FC430	--Select FQ		
<input type="radio"/>	3a	WIN-O89E5SDFBIM	PowerEdge FM120	--Select FQ		
<input type="radio"/>	3b	SLOT-03b		--Select FQ		
<input type="radio"/>	3c	localhost.localdomain	PowerEdge FM120	--Select FQ		
<input type="radio"/>	3d	q1fy16stomp1d	PowerEdge FM120	--Select FQ		

Stored Profiles [▲ Back to top](#)

Options: > Import Profile > Export Profile > Delete Profile **Network Share :** cifs:// cifs/samba /BI [Edit](#)

Select	Profile Name	Profile Version	Profile Location	View Profile
<input type="radio"/>	FC430_1_00_0E0000000000	Boot Identity	Network Share	> View
<input type="radio"/>	FC430_1_01_0E0000000003	Boot Identity	Network Share	> View

Manage Virtual MAC Address Pool: [▲ Back to top](#)

Options: > Add MAC Addresses > Remove MAC Addresses

	MAC Address	Node ID	FQDD	Boot File	Status
<input type="checkbox"/>	0E:00:00:00:00:00	1234567	NIC.Embedded.1-1-1	FC430_1_00_0E0000000000	active
<input type="checkbox"/>	0E:00:00:00:00:01	1234567	NIC.Embedded.1-1-1	FC430_1_00_0E0000000000	active
<input type="checkbox"/>	0E:00:00:00:00:02	1234567	NIC.Embedded.1-1-1	FC430_1_00_0E0000000000	active

Figure 7 Assign status of MAC changes to active status

- Navigate to the respective server- properties page and scroll down to the WWN Macaddress section and from the View drop-down list, select **advance and expand**.
- Verify if the virtual MAC addresses are active under IO identity/Remote assigned column. Refer Figure 8 Virtual Mac address are active in the server properties page.

WWN/MAC Addresses

[▲ Back to top](#)

Options: [> Export](#) [> Expand/Collapse All View: Advanced](#)

Server Slot	Fabric	Protocol	Server-Assigned	FlexAddress (Chassis-Assigned)	I/O Identity (Remote-Assigned)	Partition Status
SLOT-01c (WIN-TOU0TES1E12)	All Fabrics	All Protocols	Search by WWN/MAC Address	All WWN/MAC Addresses Type		All Partitions
SLOT-01c (WIN-TOU0TES1E12)	iDRAC A1	Management	✓ C8:1F:66:FF:1A:8F	34:E6:D7:D8:EE:89	Not Installed	Unknown
		10 GbE KR	34:17:EB:E6:3D:99	34:E6:D7:D8:E8:69	✓ 0E:00:00:00:00:00	Enabled
		iSCSI	34:17:EB:E6:3D:9A	34:E6:D7:D8:E8:6A	✓ 0E:00:00:00:00:01	Disabled
		FCoE-FIP	✓ 34:17:EB:E6:3D:9B	34:E6:D7:D8:E8:6B	Not Installed	Unknown
		FCoE-WWN	✓ 20:01:34:17:EB:E6:3D:9B	20:01:34:E6:D7:D8:E8:6B	Not Installed	Unknown
		10 GbE KR	✓ 34:17:EB:E6:3D:9F	34:E6:D7:D8:EE:8D	Not Installed	Unknown
		iSCSI	✓ 34:17:EB:E6:3D:A0	34:E6:D7:D8:EE:8E	Not Installed	Unknown
		FCoE-FIP	✓ 34:17:EB:E6:3D:A1	34:E6:D7:D8:EE:8F	Not Installed	Unknown
		FCoE-WWN	✓ 20:01:34:17:EB:E6:3D:A1	20:01:34:E6:D7:D8:EE:8F	Not Installed	Unknown
		10 GbE KR	✓ 34:17:EB:E6:3D:A5	34:E6:D7:D8:EE:93	Not Installed	Unknown
		iSCSI	✓ 34:17:EB:E6:3D:A6	34:E6:D7:D8:EE:94	Not Installed	Unknown

Figure 8 Virtual Mac address are active in server properties page

NOTE:

Ensure that identical cards are used in the spare server.

"If the NDC/FC card fails, the saved boot identity profile can be applied to the partition only after replacing the respective card."



6 Bringing Up the Spare Server

When an active server goes to failure state, the spare server must be configured to bring online state fast to avoid the downtime cost. To bring up the spare server, perform the following steps:

- i. Clear Boot Identity profile from failed server or deactivate the MAC Addresses
- ii. Apply saved Boot Identity to new or spare server

6.1 Clearing Boot Identity Profiles

Before applying a new Boot Identity profile to a server, clear the existing Boot Identity configurations from the selected server by using the Clear Identity option available in the CMC web interface.

To clear Boot Identity profiles:

1. Go to the **Server Profiles** page. In the **Boot Identity Profiles** section, select the server from which you want to clear the Boot Identity profile.
2. Click **Clear Identity**. Refer Figure 9 Clearing Boot Identity.
3. Click **OK** to clear the Boot Identity profile from the selected server.
4. The clear operation disables the IO Identity and persistence policy of the server. On completion of the clear operation, the server is powered off.

Options: > Save Identity -- Select Profile -- > Apply Identity > **Clear Identity**

	Slot	Slot Name	Model	FQDD	Last Applied Profile	Status
<input type="radio"/>	1a	WIN-V3VCM9ADBLI	PowerEdge FC430	--Select FQDD--		
<input type="radio"/>	1b	SLOT-01b	PowerEdge FC430	--Select FQDD--		
<input checked="" type="radio"/>	1c	WIN-TOU0TES1EI2	PowerEdge FC430	--Select FQDD--	FC430_1_00_0E0000000000	
<input type="radio"/>	1d	localhost	PowerEdge FC430	--Select FQDD--		
<input type="radio"/>	3a	WIN-O89E5SDFBIM	PowerEdge FM120	--Select FQDD--		
<input type="radio"/>	3b	SLOT-03b		--Select FQDD--		
<input type="radio"/>	3c	localhost.localdomain	PowerEdge FM120	--Select FQDD--		
<input type="radio"/>	3d	q1fy16stomp1d	PowerEdge FM120	--Select FQDD--		

Stored Profiles [Back to top](#)

Figure 9 Clearing Boot Identity

NOTE:

This option is enabled only if any of the servers are selected and Boot Identity profiles are applied to the selected servers.

6.2 Deactivating MAC Addresses

You can deactivate MAC addresses that are active by using the Deactivate MAC Address(es) option in the CMC web interface. This option is provided to retrieve the Boot Identity profile from the failed server which could not perform the clear identity method. The failed server needs to be removed from the network to avoid any MAC address conflict as the IO identity is not disabled properly from the server using clear identity operation.

To Deactivate MAC addresses in the virtual MAC Address pool:

1. Go to the Server Profiles page.
2. In the **Boot Identity Profiles** → **Manage Virtual MAC Address Pool** section, select the active MAC address(es) that you want to deactivate.
3. Click **Deactivate MAC Address(es)**. Refer Figure 10 Deactivate Virtual MAC Address.

Manage Virtual MAC Address Pool: [▲ Back to top](#)

Options: [> Add MAC Addresses](#) [> Remove MAC Addresses](#)

<input checked="" type="checkbox"/>	MAC Address	Node ID	FQDD	Boot File	Status
<input checked="" type="checkbox"/>	0E:00:00:00:00:00	1234567	NIC.Embedded.1-1-1	FC430_1_00_0E0000000000	active
<input checked="" type="checkbox"/>	0E:00:00:00:00:01	1234567	NIC.Embedded.1-1-1	FC430_1_00_0E0000000000	active
<input checked="" type="checkbox"/>	0E:00:00:00:00:02	1234567	NIC.Embedded.1-1-1	FC430_1_00_0E0000000000	active
<input type="checkbox"/>	0E:00:00:00:00:03			FC430_1_01_0E0000000003	assign
<input type="checkbox"/>	0E:00:00:00:00:04			FC430_1_01_0E0000000003	assign
<input type="checkbox"/>	0E:00:00:00:00:05			FC430_1_01_0E0000000003	assign
<input type="checkbox"/>	0E:00:00:00:00:06				unassign
<input type="checkbox"/>	0E:00:00:00:00:07				unassign
<input type="checkbox"/>	0E:00:00:00:00:08				unassign
<input type="checkbox"/>	0E:00:00:00:00:09				unassign

[Deactivate MAC Address\(es\)](#)

Figure 10 Deactivate Virtual MAC Address

NOTE:

Use the Deactivate MAC Address(es) option only if the server does not responding to the Clear Identity action..

6.3 Apply saved Boot Identity to new or spare server

1. Insert the spare server to the chassis NDC and FC card which is in spare server should be same as in failed server or replace NDC and FC card in failed server
2. [Refer section 5](#) and follow from step 2

7 Managing Stored Boot Identity Profiles

Saved profiles lists under Stored profiles section, from here profiles can be viewed, deleted, exported to management station and profiles available in management station can be imported to Stored profile section.

7.1 Viewing Stored Boot Identity Profiles

To view the Boot Identity profiles stored on the network share, go to the **Server Profiles** page. In the **Boot Identity Profiles** → **Stored Profiles** section, select the profile and click **View** in the **View Profile** column. The **View Settings** page is displayed. Refer Figure 11 Viewing stored Boot Identity profile and Figure 12 Sample Boot Identity page.

Stored Profiles [▲ Back to top](#)

Options: > Import Profile > Export Profile > Delete Profile Network Share : <code>cifs:// cifs/samba /BI</code> Edit				
Select	Profile Name	Profile Version	Profile Location	View Profile
<input type="radio"/>	FC430_1_00_0E0000000000	Boot Identity	Network Share	> View
<input type="radio"/>	FC430_1_01_0E0000000003	Boot Identity	Network Share	> View

Figure 11 Viewing stored Boot Identity profile

View Settings

[<< Return to Server Profile](#)

Profile: FC430_1_00_0E0000000000 - NIC.Embedded.1-1-1

Key	Value
BlinkLeds	0
VirtMacAddr	0E:00:00:00:00:00
VirtIscsiMacAddr	0E:00:00:00:00:01
VirtFIPMacAddr	0E:00:00:00:00:02
VirtWWN	20:00:0E:00:00:00:00:02
VirtWWPN	20:01:0E:00:00:00:00:02
TcpIpViaDHCP	Enabled
IscsiViaDHCP	Enabled
ChapAuthEnable	Disabled
IscsiTgtBoot	Enabled
DhcpVendId	BRCM ISAN
LnkUpDelayTime	0
TcpTimestamp	Disabled
FirstHddTarget	Disabled
LunBusyRetryCnt	0
IpVer	IPv4
WinHbaBootMode	Disabled
IscsiInitiatorId	0.0.0.0

Figure 12 Sample Boot Identity page

7.2 Importing Boot Identity Profile

You can import Boot Identity profiles that are stored on the management station to the network share. To import a stored profile on to the network share from the management station, perform the following tasks:

1. Go to the **Server Profiles** page.
2. In the **Boot Identity Profiles → Stored Profiles** section, click **Import Profile**. The **Import Profile** section is displayed.
3. Click **Browse** to access the profile from the required location and then click **Import Profile**. Refer Figure 13 Import profile to Network share.

Stored Profiles [▲ Back to top](#)

Options: [> Import Profile](#) [> Export Profile](#) [> Delete Profile](#) Network Share : cifs:// cifs/samba /BI [Edit](#)

Import Profile

Filename: [Browse...](#) [Cancel](#) [Import Profile](#)

Manage Virtual MAC Address Pool: [▲ Back to top](#)

Figure 13 Import profile to Network share

7.3 Exporting Boot Identity Profile

You can export Boot Identity profiles that are saved on the network share to a specified path on a management station. To export a stored profile, perform the following tasks:

1. Go to the **Server Profiles** page.
2. In the **Boot Identity Profiles → Stored Profiles** section, select the required profile and then click **Export Profile**. A File Download message is displayed prompting you to open or save the file.
3. Click **Save** to export the profile to the required location. Refer Figure 14 Exporting Boot Identity from Network share.

Stored Profiles

Options: > Import Profile > **Export Profile** > Delete Profile Network Share : cifs://cifs/samba/BI

Select	Profile Name	Profile Version	Profile Location	View
<input checked="" type="radio"/>	FC430_1_00_0E0000000000	Boot Identity	Network Share	> View
<input type="radio"/>	FC430_1_01_0E0000000003	Boot Identity	Network Share	> View

Manage Virtual MAC Address Pool:

Options: > Add MAC Addresses > Remove MAC Addresses

	MAC Address	Node ID	FQDD	Boot File	Status
<input type="checkbox"/>	0E:00:00:00:00:00	1234567	NIC.Embedded.1-1-1	FC430_1_00_0E0000000000	active
<input type="checkbox"/>	0E:00:00:00:00:01	1234567	NIC.Embedded.1-1-1	FC430_1_00_0E0000000000	active
<input type="checkbox"/>	0E:00:00:00:00:02	1234567	NIC.Embedded.1-1-1	FC430_1_00_0E0000000000	active
<input type="checkbox"/>	0E:00:00:00:00:03			FC430_1_01_0E0000000003	assign
<input type="checkbox"/>	0E:00:00:00:00:04			FC430_1_01_0E0000000003	assign
<input type="checkbox"/>	0E:00:00:00:00:05			FC430_1_01_0E0000000003	assign
<input type="checkbox"/>	0E:00:00:00:00:06				unassi

save FC430_1_00_0E0000000000.xml **Save** Cancel

Figure 14 Exporting Boot Identity profile from Network share

7.4 Deleting Boot Identity Profile

You can delete a Boot Identity profile that is stored on the network share. To delete a stored profile, perform the following tasks:

1. Go to the **Server Profiles** page.
2. In the **Boot Identity Profiles** → **Stored Profiles** section, select the required profile, and then click **Delete Profile**. A warning message is displayed indicating that deleting a profile deletes the selected profile permanently.
3. Click **OK** to delete the selected profile.

8 Typical Customer used workflow

INITIAL, FIRST or ONE-TIME SETUP

- Navigate to **Chassis Overview->Server Overview->Setup->Network Share** and enter the name for "Boot Identity Profile Folder". Click **Apply** button to save the settings. Click **Test Directory** button adjacent to the **Boot Identity Profile Folder** to make sure that the Network share and **Boot Identity Profile Folder** are accessible by CMC.
- Navigate to **Chassis overview->Server Overview->Setup->Profiles** and click the **Boot Identity Profiles** tab. Go to the **Manage Virtual MAC address Pool** section. The default MAC address (0E:00:00:00:00:00) is displayed in the **Starting MAC Address** field. Enter the **Starting MAC address** and the **Number of MAC Addresses**, and click **Create MAC Pool** to create a virtual MAC address pool.
- Make sure to create and enable NIC/FC partitions as needed in the blade servers by referring to the white papers listed in this document. The NIC/FC partitions are created and enabled using a Server Configuration Profile before the Boot Identity is assigned .
- Navigate to **Chassis Overview->Server Overview->Setup->Profiles** and click the **Boot Identity Profiles** tab. Make sure all available blade servers, which support IOIOpt and persistence policy, are displayed on this page.
- Click on a particular blade server, it will display the enabled NIC cards/partitions configured for iSCSI & FCoE and the enabled FC cards/partitions present in that blade server. Each NIC card/partition and FC card/partition is identified with a unique FQDD.
- Select a blade server and the appropriate FQDD and click the **Save Profile**. You are prompted to choose the number of profiles to be created. Enter the number of profiles to be created. The default number of profiles is 1. You can select or enter the base file name. A drop-down list has been provided to enable users to choose the available or unassigned MAC address from the pool for the first boot identity profile generated . The CMC captures a profile only once from iDRAC for the selected FQDD and generates multiple profiles from this captured profile. The names of the multiple profiles contain the base file name and the suffix XXXX. For example, if the base file name is "austindatacenter", then the profiles generated are austindatacenter_vmacaddr1.xml, ustindatacenter_vmacaddr2.xml and so on. The default MAC address are first available in the pool. You can choose the required MAC address from the drop-down list.
- The CMC administrator can then edit the Boot Identity profiles by accessing the profiles directly on the network share by using the required editor. The CMC GUI does not provide any interface to edit the Boot Identity profiles.
- The attributes that CMC administrator edits must be as per Section 9.2 that has a table with details on which attributes are applicable to various types of partitions that is, iSCSI, FCoE, and FC.
- The edited Boot Identity file must be applied to the blade server.



9 Appendix

9.1 Sample Boot Identity Profile

Initiator and target settings needs to be modified.

```
<?xml version="1.0"?>

<SystemConfiguration Model="PowerEdge M620" ServiceTag="2WQBH32" TimeStamp="Thu
Jul 16 08:56:01 2015">

    <!--Export type is Replace,Selective-->

    <!--Exported configuration may contain commented attributes. Attributes may be
commented due to dependency, destructive nature, preserving server identity or
for security reasons.-->

    <Component FQDD="NIC.Integrated.1-1-1">

        <Attribute Name="VirtualizationMode">NONE</Attribute>

        <Attribute Name="BlnkLeds">0</Attribute>

        <Attribute Name="VirtMacAddr">0E:00:00:33:00:0D</Attribute>

        <Attribute Name="VirtIscsiMacAddr">0E:00:00:33:00:0E</Attribute>

        <Attribute Name="VirtFIPMacAddr">0E:00:00:33:00:00</Attribute>

        <Attribute Name="VirtWWN">20:00:0E:00:00:33:00:00</Attribute>

        <Attribute Name="VirtWWPN">20:01:0E:00:00:33:00:00</Attribute>

        <Attribute Name="TcpIpViaDHCP">ashok</Attribute>

        <!-- <Attribute Name="IpAutoConfig">Enabled</Attribute> -->

        <Attribute Name="IscsiViaDHCP">Enabled</Attribute>

        <Attribute Name="ChapAuthEnable">Enabled</Attribute>

        <Attribute Name="IscsiTgtBoot">Enabled</Attribute>

        <Attribute Name="DhcpVendId">Dell ISAN</Attribute>

        <Attribute Name="LnkUpDelayTime">0</Attribute>

        <Attribute Name="TcpTimestamp">Disabled</Attribute>

        <Attribute Name="FirstHddTarget">Disabled</Attribute>
```



```

<Attribute Name="LunBusyRetryCnt">0</Attribute>

<Attribute Name="IpVer">IPv4</Attribute>

<Attribute Name="WinHbaBootMode">Disabled</Attribute>

<Attribute Name="IscsiInitiatorIpAddr">0.0.0.0</Attribute>

<Attribute Name="IscsiInitiatorSubnet">0.0.0.0</Attribute>

<!-- <Attribute Name="IscsiInitiatorSubnetPrefix"></Attribute> -->

<Attribute Name="IscsiInitiatorGateway">0.0.0.0</Attribute>

<Attribute Name="IscsiInitiatorPrimDns">0.0.0.0</Attribute>

<Attribute Name="IscsiInitiatorSecDns">0.0.0.0</Attribute>

<Attribute Name="IscsiInitiatorName">ValueCleared</Attribute>

<Attribute Name="IscsiInitiatorChapId">ValueCleared</Attribute>

<Attribute Name="IscsiInitiatorChapPwd">ValueCleared</Attribute>

<Attribute Name="ConnectFirstTgt">Disabled</Attribute>

<Attribute Name="FirstTgtIpAddress">0.0.0.0</Attribute>

<Attribute Name="FirstTgtTcpPort">3260</Attribute>

<Attribute Name="FirstTgtBootLun">0</Attribute>

<Attribute Name="FirstTgtIscsiName">ValueCleared</Attribute>

<Attribute Name="FirstTgtChapId">ValueCleared</Attribute>

<Attribute Name="FirstTgtChapPwd">ValueCleared</Attribute>

<Attribute Name="ConnectSecondTgt">Disabled</Attribute>

<Attribute Name="SecondTgtIpAddress">0.0.0.0</Attribute>

<Attribute Name="SecondTgtTcpPort">3260</Attribute>

<Attribute Name="SecondTgtBootLun">0</Attribute>

<Attribute Name="SecondTgtIscsiName">ValueCleared</Attribute>

<Attribute Name="SecondTgtChapId">ValueCleared</Attribute>

<Attribute Name="SecondTgtChapPwd">ValueCleared</Attribute>

<Attribute Name="LegacyBootProto">PXE</Attribute>

```



```

<Attribute Name="BootStrapType">AutoDetect</Attribute>

<Attribute Name="HideSetupPrompt">Disabled</Attribute>

<Attribute Name="BannerMessageTimeout">5</Attribute>

<Attribute Name="LnkSpeed">AutoNeg</Attribute>

<Attribute Name="WakeOnLan">Disabled</Attribute>

<Attribute Name="VlanMode">Disabled</Attribute>

<!-- <Attribute Name="VlanId">1</Attribute> -->

<Attribute Name="BootRetryCnt">NoRetry</Attribute>

<Attribute Name="SecondaryDeviceMacAddr">00:00:00:00:00:00</Attribute>

<Attribute Name="UseIndTgtPortal">Disabled</Attribute>

<Attribute Name="UseIndTgtName">Disabled</Attribute>

<Attribute Name="NicPartitioning">Disabled</Attribute>

<!-- <Attribute Name="FlowControlSetting">Auto</Attribute> -->

<Attribute Name="FCoETgtBoot">Disabled</Attribute>

<Attribute Name="FCoEFirstHddTarget">Disabled</Attribute>

<Attribute Name="FCoELnkUpDelayTime">0</Attribute>

<Attribute Name="FCoELunBusyRetryCnt">0</Attribute>

<Attribute Name="FCoEFabricDiscoveryRetryCnt">4</Attribute>

<Attribute Name="ConnectFirstFCoETarget">Disabled</Attribute>

<Attribute Name="FirstFCoEWWPNTarget">00:00:00:00:00:00:00:00</Attribute>

<Attribute Name="FirstFCoEBootTargetLUN">0</Attribute>

</Component>

</SystemConfiguration>

```



9.2 Boot Identity Attributes Associated with iSCSI/FCoE/FC Partitions

Attribute	NIC/CNA Personality	FC HBA
<i>Virtual Addresses</i>		
VirtMacAddr	NIC Port, NIC Partition	N/A
VirtIscsiMacAddr	ISOE	N/A
VirtFIPMacAddr	FCoE Initiator	N/A
VirtWWN	FCoE Initiator	FC Port Initiator
VirtWWPN	FCoE Initiator	FC Port Initiator
<i>iSCSI InitiatorSettings</i>		
IscsilInitiatorIpAddr	ISOE, NIC Port, NIC Partition	N/A
IscsilInitiatorIpv4Addr	ISOE, NIC Port, NIC Partition	N/A
IscsilInitiatorIpv6Addr	ISOE, NIC Port, NIC Partition	N/A
IscsilInitiatorSubnet	ISOE, NIC Port, NIC Partition	N/A
IscsilInitiatorSubnetPrefix	ISOE, NIC Port, NIC Partition	N/A
IscsilInitiatorGateway	ISOE, NIC Port, NIC Partition	N/A
IscsilInitiatorIpv4Gateway	ISOE, NIC Port, NIC Partition	N/A
IscsilInitiatorIpv6Gateway	ISOE, NIC Port, NIC Partition	N/A
IscsilInitiatorPrimDns	ISOE, NIC Port, NIC Partition	N/A
IscsilInitiatorIpv4PrimDns	ISOE, NIC Port, NIC Partition	N/A



IscsiInitiatorIpv6PrimDns	ISOE, NIC Port, NIC Partition	N/A
IscsiInitiatorSecDns	ISOE, NIC Port, NIC Partition	N/A
IscsiInitiatorIpv4SecDns	ISOE, NIC Port, NIC Partition	N/A
IscsiInitiatorIpv6SecDns	ISOE, NIC Port, NIC Partition	N/A
IscsiInitiatorName	ISOE, NIC Port, NIC Partition	N/A
IscsiInitiatorChapId	ISOE, NIC Port, NIC Partition	N/A
IscsiInitiatorChapPwd	ISOE, NIC Port, NIC Partition	N/A
<i>iSCSI Storage Target Settings</i>		
ConnectFirstTgt	iSCSI Target	N/A
FirstTgtIpAddress	iSCSI Target	N/A
FirstTgtTcpPort	iSCSI Target	N/A
FirstTgtBootLun	iSCSI Target	N/A
FirstTgtIscsiName	iSCSI Target	N/A
FirstTgtChapId	iSCSI Target	N/A
FirstTgtChapPwd	iSCSI Target	N/A
FirstTgtIpvVer	iSCSI Target	N/A
ConnectSecondTgt	iSCSI Target	N/A
SecondTgtIpAddress	iSCSI Target	N/A



SecondTgtTcpPort	iSCSI Target	N/A
SecondTgtBootLun	iSCSI Target	N/A
SecondTgtIscsiName	iSCSI Target	N/A
SecondTgtChapId	iSCSI Target	N/A
SecondTgtChapPwd	iSCSI Target	N/A
SecondTgtIplVer	iSCSI Target	N/A
<i>FCoE Storage Target Settings</i>		
FCoEBootScanSelection	FCoE Target	FC Target
FirstFCoEWWPNTarget	FCoE Target	FC Target
FirstFCoEBootTargetLUN	FCoE Target	FC Target
FirstFCoEFCFVLANID	FCoE Target	FC Target
FCoETgtTBoot	FCoE Target	FC Target
<i>FC Storage Target Settings</i>		
BootScanSelection	N/A	FC Target
FirstFCTargetConnect	N/A	FC Target
FirstFCTargetWWPN	N/A	FC Target
FirstFCTargetLUN	N/A	FC Target
SecondFCTargetConnect	N/A	FC Target



SecondFCTargetWWPN	N/A	FC Target
SecondFCTargetLUN	N/A	FC Target

9.3 How to Create and Enable iSCSI/FCoE/FC partitions

http://en.community.dell.com/techcenter/extras/m/white_papers/20242976/download.aspx	FCoE Boot Configuration Setup on Broadcom using Lifecycle Controller
http://en.community.dell.com/techcenter/extras/m/white_papers/20118779	FCoE Boot Configuration Setup on Intel Card using Lifecycle Controller

9.4 Feature Constraint

- The Boot Identity feature is limited to Dell 12th generation of blade servers with 13th generation iDRAC firmware, Dell's 13th generation of blade servers and later generation of blade servers.
- The IOIOpt (IO Identity Optimization) and persistence policy is supported from Dell 12th generation of blade servers onwards.
- Applying Boot Identity Profile to a server requires a server reboot.
- This feature is available only for blade servers that support IOIOpt and Persistence Policy.
- This feature is applicable only to already enabled NIC cards/partitions and FC Cards/Partitions.
- NIC cards/partitions should have their iSCSI/FCoE Protocol already enabled. Enable the NIC/FC card partitions using a preparation XML template profile. The preparation XML template profile is the profile that is used to configure the server when the blade server is inserted in the chassis.
- This feature is guaranteed to work only when an identical IOM with the same configuration is present both with failed blade and spare blade.
- This feature is guaranteed to work only when the same CNA is present both with failed blade and spare blade.
- This feature is guaranteed to work only when BIOS and CNA configuration settings are same with failed blade and spare blade.
- Persistence policy is set to retain virtual addresses for warm reset, cold reset, and AC power loss for the following attributes of iDRAC:



- *VirtualAddressPersistencePolicy*
 - *VirtualAddressPersistencePolicyAuxPwr* (*AuxPowered*)
 - *VirtualAddressPersistencePolicyNonAuxPwr* (*NonAux powered*)
- *InitiatorPersistencePolicy*
- *StorageTargetPersistencePolicy*

Set these policies in the preparation XML template profile. The preparation XML template profile is the profile that is used to configure the server when the blade server is inserted in the chassis.

- Some of the NIC/FC adaptors in Dell's 13th generation blade servers may not support IOI & Persistence Policy. CMC will find out capability to support IOIOpt and Persistence Policy programmatically by querying iDRAC.
- Chassis PCIe slots in the stomp/VRTX chassis are not included for this feature.
- You must not update any of the Boot Identity parameters including virtual MAC addresses after it is applied using CMC.
- The behavior of NIC/FC adaptors with any bugs in their implementation is out of scope of this document.
- Any runtime issues of iDRAC after applying Boot Identity profile is out of scope of this document.
- Changing virtual MAC address pool directly on the network share creates issues. Instead, use the interface provided for these tasks.
- Do not delete or rename profiles from network share as it results in the vmacdb.xml going out of sync. Instead, use the interface provided for these tasks.
- This feature works only when the SD card is present in the CMC.
- This feature is limited to primary partition of the network cards.

