Using Lifecycle Controller to Configure UEFI Secure Boot and OS Deployment

This Dell technical white paper describes the capabilities of using Lifecycle Controller to configure UEFI Secure Boot and OS Deployment on Dell PowerEdge servers.

Dell Engineering
September 2014

Raghavendra Venkataramudu
Sumanth Vidyadhara
Nagaraju S
Using Lifecycle Controller to Configure UEFI Secure Boot and OS Deployment

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.

© 2014 Dell Inc. All rights reserved. Reproduction of this material in any manner whatsoever without the express written permission of Dell Inc. is strictly forbidden. For more information, contact Dell.

Dell, the DELL logo, and the DELL badge are trademarks of Dell Inc. Symantec, NetBackup, and Backup Exec are trademarks of Symantec Corporation in the U.S. and other countries. Microsoft, Windows, and Windows Server are registered trademarks of Microsoft Corporation in the United States and/or other countries. Other trademarks and trade names may be used in this document to refer to either the entities claiming the marks and names or their products. Dell disclaims any proprietary interest in the marks and names of others.

Trademarks used in this text:
Dell™, the Dell logo, Dell Boomi™, Dell Precision™, OptiPlex™, Latitude™, PowerEdge™, PowerVault™, PowerConnect™, OpenManage™, EqualLogic™, Compellent™, KACE™, FlexAddress™, Force10™ and Vostro™ are trademarks of Dell Inc. Other Dell trademarks may be used in this document. Cisco Nexus®, Cisco MDS®, Cisco NX-OS®, and other Cisco Catalyst® are registered trademarks of Cisco System Inc. EMC VNX®, and EMC Unisphere® are registered trademarks of EMC Corporation. Intel® Pentium®, Xeon®, Core® and Celeron® are registered trademarks of Intel Corporation in the U.S. and other countries. AMD® is a registered trademark and AMD Opteron™, AMD Phenom™ and AMD Sempron™ are trademarks of Advanced Micro Devices, Inc. Microsoft®, Windows®, Windows Server®, Internet Explorer®, MS-DOS®, Windows Vista® and Active Directory® are either trademarks or registered trademarks of Microsoft Corporation in the United States and/or other countries. Red Hat® and Red Hat® Enterprise Linux® are registered trademarks of Red Hat, Inc. in the United States and/or other countries. Novell® and SUSE® are registered trademarks of Novell Inc. in the United States and other countries. Oracle® is a registered trademark of Oracle Corporation and/or its affiliates. Citrix® Xen®, XenServer® and XenMotion® are either registered trademarks or trademarks of Citrix Systems, Inc. in the United States and/or other countries. VMware®, VMware Virtual SMP®, vMotion®, vCenter® and vSphere® are registered trademarks or trademarks of VMware, Inc. in the United States or other countries. IBM® is a registered trademark of International Business Machines Corporation. Broadcom® and NetXtreme® are registered trademarks of Broadcom Corporation. QLogic is a registered trademark of QLogic Corporation. Other trademarks and trade names may be used in this document to refer to either the entities claiming the marks and/or names or their products and are the property of their respective owners. Dell disclaims proprietary interest in the marks and names of others.
Contents

Executive summary .............................................................................................................................................. 4

Introduction .......................................................................................................................................................... 5

1. Enabling Secure boot using OMSA .............................................................................................................. 6
2. Enabling Secure boot using DTK .................................................................................................................. 8
3. Enabling Secure Boot using RACADM ....................................................................................................... 10
4. Enabling Secure Boot using WS-MAN ......................................................................................................... 14
5. Secure Boot in LC UI .................................................................................................................................... 18
   5.1 Workflow Diagram to Install Operating System with Secure Boot Enabled through Lifecycle Controller ...... 18
   5.2 Installing an operating system with Secure Boot enabled using Lifecycle Controller .................................. 19
6. Error Messages and Resolution ................................................................................................................ 35
7. Warning Messages and Resolution .......................................................................................................... 37
8. Best practices .................................................................................................................................................. 41
   A. List of operating systems that support Secure Boot ................................................................................ 42
   B. Configuration details .................................................................................................................................. 43
Executive summary

This white paper provides:
- Detailed information on configuring UEFI Secure Boot and deploying the operating system on Dell PowerEdge servers using Lifecycle Controller.
- An introduction on the Secure Boot feature and steps to enable Secure Boot using interfaces such as OMSA/DTK/RACADM/WS-MAN and Lifecycle Controller UI.
- A detailed work flow on installing a Secure Boot supported operating system by enabling the Secure Boot feature using Lifecycle Controller.

For a detailed information on the Unattended OS Installation in LC refer the Unattended OS Install white paper.

For a detailed information on the RAID Configuration refer the Raid Configuration white paper.

For a detailed information on the Secure Boot Settings refer to “Defining a Secure Boot Policy on Dell Servers” whitepaper.
Introduction

UEFI Secure Boot is a technology that eliminates a major security hole that may occur during a handoff between the UEFI firmware and UEFI operating system. In UEFI Secure Boot, each component in the chain is validated and authorized against a specific certificate before it is allowed to load or run. Secure Boot removes the legacy threat and provides software identity checking at every step of the boot – Platform Firmware, Option Cards, and OS Bootloader.

**NOTE:** You can upload the certificates only using the BIOS settings. For more information, see the Defining a Secure Boot Policy on Dell Servers white paper.

When set to Enabled, UEFI Secure Boot prevents the unsigned UEFI device drivers from being loaded, displays an error message and does not allow the device to function. You must disable Secure Boot to load the unsigned device drivers.

On the Dell 13th generation PowerEdge servers, you can enable or disable the Secure Boot feature using interfaces such as:
- Dell OpenManage Server Administrator (OMSA)
- Dell OpenManage Deployment Toolkit (DTK)
- Dell Lifecycle Controller (LC UI)
- Dell Remote Access Controller Admin (RACADM)
- iDRAC Web Services Management (WS-MAN)
- BIOS Settings
1. Enabling Secure boot using OMSA

1. On the OMSA home page, navigate to **System -> Main System Chassis -> BIOS**.
2. Click **Setup -> System Security**.

![OMSA System BIOS Settings Page](image-url)

**Figure 2 OMSA System BIOS Settings Page**
3. Under **Secure Boot**, select **Enabled** and click **Apply**.

![Figure 3 OMSA System BIOS Settings -> System Security Page](image)

4. Reboot the system.

![Figure 4 OMSA System BIOS Settings Success Message](image)
2. Enabling Secure boot using DTK

1. Boot to **System Setup** -> **System BIOS Settings** -> **Boot Settings** and set the **Boot Mode** to **UEFI**.
2. Boot into DTK Media.

![Figure 5 Boot Mode message while loading DTK](image)

3. Select the **Dell Deployment Toolkit** on the Boot Selection Page.

![Figure 6 Boot Selection page for DTK](image)
4. Type the following command to enable Secure Boot:

   `syscfg --secureboot=Enable`

   **Console Output:**

   ![Figure 7 Enabling Secure Boot on DTK Shell](image)

   Figure 7 Enabling Secure Boot on DTK Shell
3. Enabling Secure Boot using RACADM

1. Type the following command to set the Boot Mode as UEFI:

   racadm set bios.BiosBootSettings.BootMode Uefi

   **Console Output:**

   ![Figure 8 Command to set the Boot Mode to UEFI](image)

   Successfully modified the object value and the change is in pending state. To apply modified value, create a configuration job and reboot the system. To create the commit and reboot jobs, use “jobqueue” command. For more information about the “jobqueue” command, see RACADM help.
2. Type the following commands to get the Boot Mode and Secure Boot status:

```
racadm get bios.BiosBootSettings.BootMode
racadm get bios.SysSecurity
```

**Console Output:**

![Console Output Image]

Figure 9 Command to get the Boot Mode and Secure Boot Status
3. Type the following command to enable Secure Boot:

```
```

**Console Output:**

![Console Output](image)

Figure 10 Command to enable Secure Boot
The job remains in scheduled state till you restart the server. Restart the server to execute the job. Use “-r forced” at the end of Jobqueue create command to reboot the server immediately.

```
racadm jobqueue create BIOS.Setup.1-1
```

**Console Output:**

![Console Output](image)

Figure 11 Display the job status
4. Enabling Secure Boot using WS-MAN

1. Type the following commands to set the Boot Mode to UEFI:

```
winrm i SetAttribute http://schemas.dmtf.org/wbem/wscim/1/cim-schema/2/root/dcim/DCIM_BIOSService?__cimnamespace=root/dcim+SystemCreationClassName=DCIM_ComputerSystem+SystemName=DCIM:ComputerSystem+CreationClassName=DCIM_BIOSService+Name=DCIM:BIOSService-u:root -p:calvin -r:https://idrac_ip/wsman -SkipCNcheck -SkipCAcheck -encoding:utf-8 -a:basic @{Target="BIOS.Setup.1-1";AttributeName="BootMode";AttributeValue="Uefi"}
```

```
winrm i CreateTargetedConfigJob
http://schemas.dmtf.org/wbem/wscim/1/cim-schema/2/root/dcim/DCIM_BIOSService?__cimnamespace=root/dcim+SystemCreationClassName=DCIM_ComputerSystem+SystemName=DCIM:ComputerSystem+CreationClassName=DCIM_BIOSService+Name=DCIM:BIOSService-u:root -p:calvin -r:https://idrac_ip/wsman -SkipCNcheck -SkipCAcheck -encoding:utf-8 -a:basic @{Target="BIOS.Setup.1-1";RebootJobType="1";ScheduledStartTime="TIME_NOW"}
```

**Console Output:**

```
C:\Users\mmondap_dutta\Desktop\man\winrm i SetAttribute http://schemas.dmtf.org/wbem/wscim/1/cim-schema/2/root/dcim/DCIM_BIOSService?__cimnamespace=root/dcim+SystemCreationClassName=DCIM_ComputerSystem+SystemName=DCIM:ComputerSystem+CreationClassName=DCIM_BIOSService+Name=DCIM:BIOSService-u:root -p:calvin -r:https://idrac_ip/wsman -SkipCNcheck -SkipCAcheck -encoding:utf-8 -a:basic @{Target="BIOS.Setup.1-1";AttributeName="BootMode";AttributeValue="Uefi"}
```

```
C:\Users\mmondap_dutta\Desktop\man\winrm i CreateTargetedConfigJob http://schemas.dmtf.org/wbem/wscim/1/cim-schema/2/root/dcim/DCIM_BIOSService?__cimnamespace=root/dcim+SystemCreationClassName=DCIM_ComputerSystem+SystemName=DCIM:ComputerSystem+CreationClassName=DCIM_BIOSService+Name=DCIM:BIOSService-u:root -p:calvin -r:https://idrac_ip/wsman -SkipCNcheck -SkipCAcheck -encoding:utf-8 -a:basic @{Target="BIOS.Setup.1-1";RebootJobType="1";ScheduledStartTime="TIME_NOW"}
```

Figure 12 Set the Boot Mode to UEFI
2. Type the following commands to enable the Secure Boot settings:

```
```

```
```

**Console Output:**

![Console Output](image)

Figure 13 Enable Secure Boot
3. Type the following commands to schedule an OS deployment job:

```
winrm i BootToNetworkISO
http://schemas.dmtf.org/wbem/wscim/1/cim-schema/2/root/dcim/DCIM_OSDeploymentService?__cimnamespace=root/dcim+SystemCreationClassName=DCIM_ComputerSystem+SystemName=DCIM:ComputerSystem+CreationClassName=DCIM_OSDeploymentService+Name=DCIM:OSDeploymentService -u:root -p:calvin -r:https://idrac_ip/wsman -SkipCNcheck -SkipCAcheck -encoding:utf-8 -a:basic @{IPAddress="CIFS share IP";ShareName="Downloads\OS\Windows\Win_2008_R2";ImageName="image.iso";ShareType="2";Username="drac";Password="tiger"}
```

```
winrm i BootToNetworkISO
http://schemas.dmtf.org/wbem/wscim/1/cim-schema/2/root/dcim/DCIM_OSDeploymentService?__cimnamespace=root/dcim+SystemCreationClassName=DCIM_ComputerSystem+SystemName=DCIM:ComputerSystem+CreationClassName=DCIM_OSDeploymentService+Name=DCIM:OSDeploymentService -u:root -p:calvin -r:https://idrac_ip/wsman -SkipCNcheck -SkipCAcheck -encoding:utf-8 -a:basic @{IPAddress="NFS share IP";ShareName="nfs";ImageName="image.iso";ShareType="0"}
```

```
```
Using Lifecycle Controller to Configure UEFI Secure Boot and OS Deployment

Console Output:

```
C:\Users\nondeep_dutta\Desktop\webman> warp / BootToNetworkISO http://schemas.dmtf.org/wbem/wscim/1/cim-schema/2/root/cim/DCIM_OSDeploymentService?CreationClassName=DCIM_OSDeploymentService&Name=DCIM_OSDeploymentService&SystemCreationClassName=DCIM_ComputerSystem&SystemName=DCIM:ComputerSystem -w root -p picolvin -r http://10.94.195.162\%root -p443 -s Down\%Linux\%Windows\%USEFI-297551/ -h shareType=2 -d Username="liger" -P Password="liger" -i -n ImageName=4DF81_C9C_C3B144FR8DOS_G351100.FMT.IO
BootToNetworkISO_OUTPUT

Job
EndpointReference
  Address = http://schemas.xmlsoap.org/ws/2007/08/addressing/rel/anonymous
  SelectorSet = root/cim Bat: InstanceID = DCIM_OSDeploymentService; __namespace = __ns
  ReturnValue = 4096
```

```
C:\Users\nondeep_dutta\Desktop\webman> warp / http://schemas.dmtf.org/wbem/wscim/1/cim-schema/2/root/cim/DCIM_OSDeploymentService-ut="root" -p="calvin" -r=https://10.94.195.162\%root -p443 -s Down\%Linux\%Windows\%USEFI-297551/ -h shareType=2 -d Username="liger" -P Password="liger" -i -n ImageName=4DF81_C9C_C3B144FR8DOS_G351100.FMT.IO
DCIM_OSDeploymentService
  DeleteOnCompletion = false
  InstanceID = DCIM_OSDeploymentService1
  JobName = BootToNetworkISO
  JobStatus = Rebooting to ISO
  Message = null
  MessageID = null
  Name = BootToNetworkISO
```

```
C:\Users\nondeep_dutta\Desktop\webman> warp / http://schemas.dmtf.org/wbem/wscim/1/cim-schema/2/root/cim/DCIM_OSDeploymentService-ut="root" -p="calvin" -r=https://10.94.195.162\%root -p443 -s Down\%Linux\%Windows\%USEFI-297551/ -h shareType=2 -d Username="liger" -P Password="liger" -i -n ImageName=4DF81_C9C_C3B144FR8DOS_G351100.FMT.IO
DCIM_OSDeploymentService
  DeleteOnCompletion = false
  InstanceID = DCIM_OSDeploymentService1
  JobName = BootToNetworkISO
  JobStatus = Success
  Message = The command was successful
  MessageID = 0001
  Name = BootToNetworkISO
```

Figure 14 Schedule OS deployment job
5. Secure Boot in LC UI

5.1 Workflow Diagram to Install Operating System with Secure Boot Enabled through Lifecycle Controller

Figure 15 Workflow diagram to install operating system with Secure Boot enabled
5.2 Installing an operating system with Secure Boot enabled using Lifecycle Controller

1. Press **<F10>** during POST to start Lifecycle Controller.

Figure 16 Server POST screen
2. In the left pane, click **OS Deployment** and then click **Deploy OS**.

![OS Deployment page](image)

*Figure 17 OS Deployment page*
3. Click **Go Directly to OS Deployment** to continue with the OS deployment and click **Next**.

**NOTE:** You can also select **Configure RAID First** to re-configure RAID before installing the operating system. For more information on configuring RAID, see the [Creating RAID Using Lifecycle Controller](#) at Dell TechCenter.

![Figure 18 Step 1- 5: Select Deployment path page](image-url)
4. Set the **Boot Mode** as **UEFI** and **Secure Boot** as **Enabled**. The operating systems in the **Available Operating System** drop-down list box are populated depending on the boot mode selected.

5. Select the required operating system from the **Available Operating Systems** drop-down list box and click **Next**.

**NOTE:** The **Secure Boot** option is available only if the **Boot Mode** is set to **UEFI** and the **Load Legacy Video Option ROM** setting is set to disabled. To disable the **Load Legacy Video Option ROM** setting, click **System Setup → System BIOS Settings → Miscellaneous Settings → Load Legacy Video Option ROM → Disabled**.

**NOTE:** **Secure Boot Policy** is a read-only setting in Lifecycle Controller UI. You can change this setting only in the system BIOS settings.

**NOTE:** If **Secure Boot** is set to **Enabled**, make sure that you select an operating system that supports Secure Boot.
Figure 19 Step 2 of 5 Select an Operating System page

After you click **Next**, a progress bar displaying the composing OS drivers appears.
Figure 20 Composing OS Drivers
6. Select the installation mode — **Unattended Install** or **Manual Install** and click **Next**. If you select **Unattended Install**, then you must upload an OS configuration file to complete the installation. For more information on unattended OS installation, see the white paper on unattended install available at the Dell TechCenter.

![Figure 21 Step 3 of 5 Select Installation Mode page](image)
7. For manual installation, insert the OS media and click **Next**. The **Reboot the System** page with the summary of selections is displayed.

A warning message appears if the validation fails.

Figure 22 Step 4 of 5 Insert OS Media page
On the **Reboot the System** page, the summary of selections is displayed. Verify the selections and click **Finish**.

![Reboot the System page](image)

**Figure 23 Step 5 of 5 Reboot the System page**
The system reboots after the settings are applied successfully.

Figure 24 POST screen
The following message appears during the POST when the Secure Boot settings are modified.

Figure 25 POST message for Secure Boot Policy modification
The system boots from the OS media and displays the progress of the files loading.

![Loading files...](image)

**Figure 26 Loading files from OS media**
NOTE: The screen shots bellow illustrate the installation of Windows Server 2012 R2 as an example.

The Windows Setup screen appears after the drivers are loaded. Click Install now to begin installing the operating system.

Figure 27 Windows Setup page
Select the **Language to install**, **Time and currency format**, and **Keyboard or input method** and click **Next**.

![Windows Setup Page for Language and Keyboard settings](image)

**Figure 28 Windows Setup Page for Language and Keyboard settings**
The following screen appears when the installation begins. Your system may restart several times during the installation.

Figure 29 Installing Windows screen
After the installation is competed, restart the system and login. You will notice that all the drivers are successfully installed.

Figure 30 OS desktop screen
6. Error Messages and Resolution

The following message appears when the Boot Mode settings cannot be set in the BIOS.

![Lifecycle Controller](image)

**Figure 31 Critical error - Unable to apply the boot mode settings for BIOS**

**Resolution:**

1. Perform a system reboot and attach the OS media before entering Lifecycle Controller.
2. If the problem persists, perform an iDRAC reset from the iDRAC web interface.
The following error message appears when Secure Boot is Enabled and one of the device drivers fail the Secure Boot validation. This will prevent the device from being detected.

![Error message: driver validation failure with Secure Boot](image)

**Resolution:**

- If Secure Boot is not required, disable Secure Boot and proceed with loading the device driver.
- With Secure Boot enabled, flash the signed device driver for the failing device and continue with the process.
7. Warning Messages and Resolution

The following Secure Boot warning message appears when the Load Legacy Option ROM setting is enabled in BIOS Settings.

![Secure Boot warning message](Image)

Figure 33 Secure Boot warning message

**Resolution:**

- You can skip this message and continue if you do not require Secure Boot.
- To use Secure Boot, disable the Load Legacy Video Option ROM setting (System Setup → System BIOS Settings → Miscellaneous Settings → Load Legacy Video Option ROM → Disabled).
Using Lifecycle Controller to Configure UEFI Secure Boot and OS Deployment

Figure 34 Load Legacy Video Option ROM setting page
The following warning message appears when the inserted media fails the Dell custom validation criteria.

![Warning message for OS Media Validation](image)

**Figure 35: Warning message for OS Media Validation**

**Resolution:**

Click **Yes** and continue, if you are sure about the media provided for the selected operating system. Else, insert the right media and click **Next**.
The following warning message appears when Secure Boot is enabled and the operating system selected for installation does not support Secure Boot.

Figure 36 Secure Boot warning for unsupported OS media

**Resolution:**

- Press “d” to disable Secure Boot.
- Disable Secure Boot using any of the interfaces explained in the sections above.
8. Best practices

It is recommended to set the **Setup Password** in **System BIOS Settings** to prevent unauthorized disabling of Secure Boot.

![System Security in System BIOS Settings page](image)

**Figure 37 System Security in System BIOS Settings page**
A. List of operating systems that support Secure Boot

- Microsoft Windows Server 2012
- Microsoft Windows Server 2012 R2
- Red Hat Enterprise Linux 7.0 x64
B. Configuration details

The following table lists the components that support Secure Boot.

Table 1  Component table

<table>
<thead>
<tr>
<th>Component</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Firmware version</td>
<td>BIOS 1.0.XX, IDRAC 2.01.00.01, Driver pack 14.08.01, OM 8.0.1</td>
</tr>
<tr>
<td>Application</td>
<td>iDRAC, OMSA, Lifecycle Controller and BIOS Settings</td>
</tr>
<tr>
<td>Server</td>
<td>Dell 13th generation PowerEdge servers and later</td>
</tr>
</tbody>
</table>