DELL™

A Dell Technical White Paper

Unified Server Configurator Security Overview

By Raja Tamilarasan, Wayne Liles, Marshal Savage and Weijia Zhang

Table of Contents

Introduction

Dell introduces the Unified Server Controller (USC) as a part of the latest PowerEdge server embedded management capability that facilitates IT administrators to perform various operations without the use of any media. USC is a one stop shop that enables operating system deployment with integrated driver installations, firmware updates, hardware configuration, and diagnostics. USC is available even when the operating system is not functional or installed which allows added flexibility in provisioning the system and customizing it to suit customer requirements.

USC is an embedded software application that runs in the UEFI (Unified Extensible Firmware Interface) environment. UEFI is a pre-boot environment that is integrated into the system BIOS. For more information on UEFI, visit www.uefi.org. USC is an embedded extension of the iDRAC6 firmware and can only be invoked when iDRAC6 is functional.

This paper discusses the security features that were carefully considered and implemented as a part of the USC solution. The first section discusses the development process that was used to engineer security into the solution. The remaining sections deal with the various security-related configuration and authentication options available in USC.

Engineering Security in the Unified Server Configurator Solution

With the introduction of the latest PowerEdge Servers, Dell now offers Embedded Management, which dramatically reduces the time it takes to perform several common management tasks. Embedded Management is comprised of several interdependent components, including Lifecycle Controller and the Unified Server Configurator (USC) interface.

USC was designed using a development process that is intended to ensure appropriate security due diligence is conducted prior to the product release. The Dell Product Group has embedded security check points into appropriate phases of Dell's ISO9000 certified product development and quality program management process. In 2008, Dell was recognized for its SDL@Dell (Security Development Life Cycle) program which manages the integration of security activities in Dell business unit development methodologies.

The first security activity, occurring during the initial product development planning phases, is the compilation and analysis of the product's risk profile. The purpose of the risk profile is to permit prioritization of security assurance activities and spend. The risk profile bases risk on:

- What the product "is"
- What the product does
- Where it is located
- How it is intended to function
- What kind of data the application stores or processes
- The degree of architecture change from prior versions
- The "security history" of the product
- Whether the product has been previously assessed
- The quality of any assessment work

- Any vulnerability identified in the field, etc.

The risk profile function results in a high level risk classification for each product and, although each product is uniquely considered, generally results in the following security recommendations per risk level classification:

- ***High Risk Mitigations***
  - External assessment
  - Dell security expert assigned to product — active
  - Security requirements added to all third party developed content contracts

- ***Medium Risk Mitigations***
  - Internal threat model and code review
  - External penetration test may be recommended
  - Dell security expert assigned to product — passive
  - Security requirements added to all third-party developed content contracts

- ***Low Risk Mitigations***
  - Internal threat model and code review
  - Security requirements added to all third party developed content contracts

The USC components used threat modeling, static code analysis, manual code review, and penetration testing to find and mitigate security issues. The high risk components were also reviewed and penetration tested by an independent external security consulting company, while medium risk components were reviewed by internal Dell security experts. The external review found relatively few implementation issues which is a direct reflection of Dell's commitment to developing secure software and a reflection of Dell's iterative phase approach to integrating security into the development lifecycle. The developers ensured that all these issues were carefully considered and resolved prior to product launch.

Unified Server Configurator Best Practices

The USC is considered as an administrative tool and is protected by the BIOS administrator password which prevents unauthorized access. The principle features of USC are:

a. Operating system deployment
b. Diagnostics
c. Updates
d. Hardware configuration

As far as these features are concerned, USC interacts only with the local platform and hence does not require any network connectivity. The firmware update, on the other hand, requires network access to connect to **FTP.Dell.com** either directly or via a proxy. USC verifies that any content that is downloaded from the FTP site has been digitally signed with Dell's GPG private key. If access to the external Dell FTP site is not allowed, USC can be configured to download content from a local or internal FTP server.

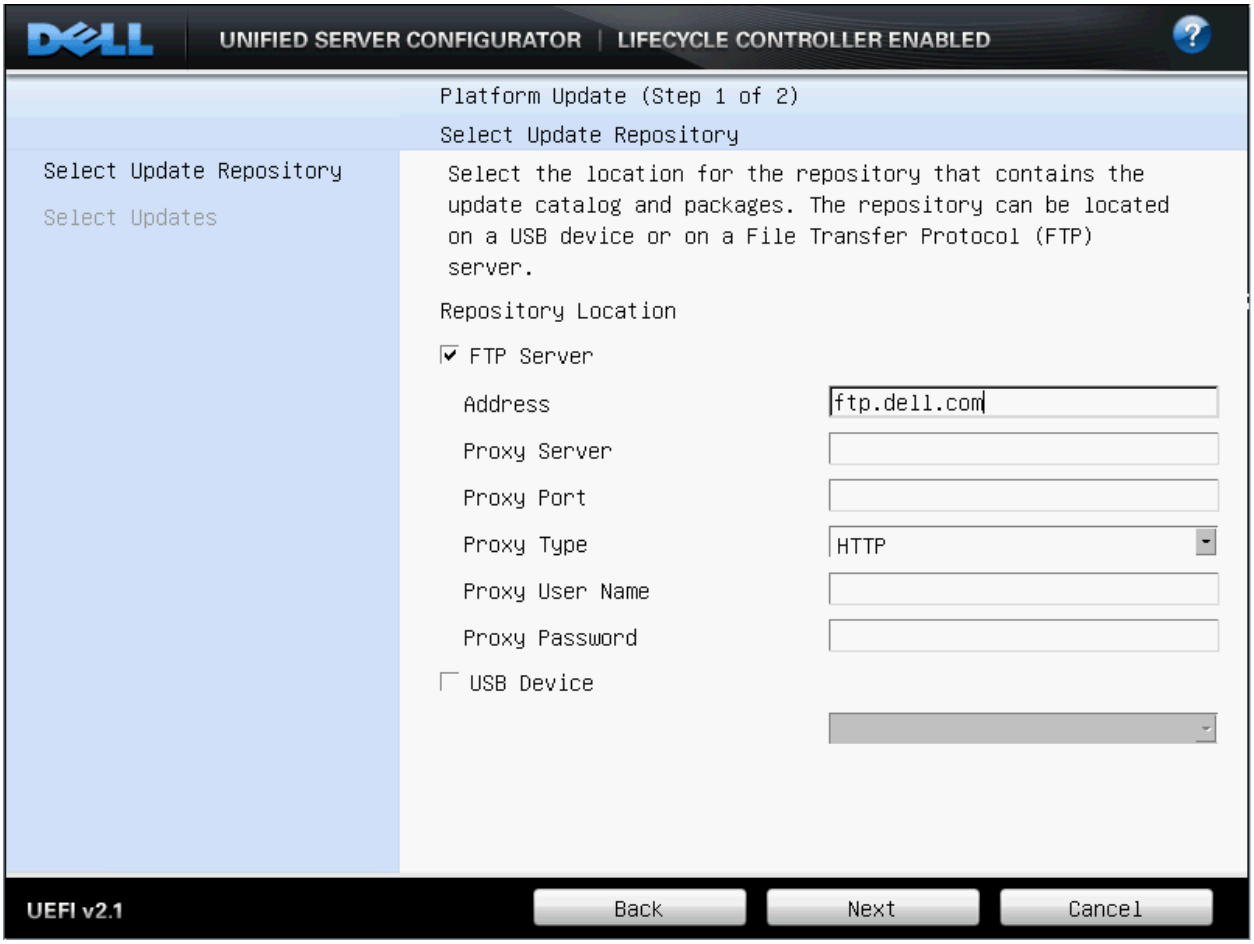

Figure 1 : Unified Server Configurator Updates Repository

USC also participates in the Trusted Platform Module (TPM) boot measurement process. The TPM that is installed on all USC-enabled platforms conform to TPM version 1.2. There are various TPM configuration options such as *On with pre-boot measurement*, *On without pre-boot measurement*, and *Off*. When the TPM is set to *On with pre-boot measurements*, USC participates in the boot chain measurements.

The TPM configuration changes can be made using different options such as F2 BIOS-boot, USC's Hardware Configuration and Dell OpenManage™ tools.

Configuration Options

USC provides the user various security-related configurable options.

Accessing Unified Server Configurator

During system boot, an F10 hotkey option is presented unless otherwise disabled as discussed in this document. Pressing F10 instructs the BIOS to invoke the UEFI pre-boot environment and USC. The F10 option is only available through BIOS and only then with permission and confirmation from iDRAC6. All BIOS security and authentication measures must be met before USC is started.

Authentication

Only users with administrator access to the BIOS will be able to access USC. The BIOS password can be managed by entering the BIOS settings during system startup (F2) or by using any of the OpenManage products to provision the server. A screenshot of the BIOS password setup is shown below.

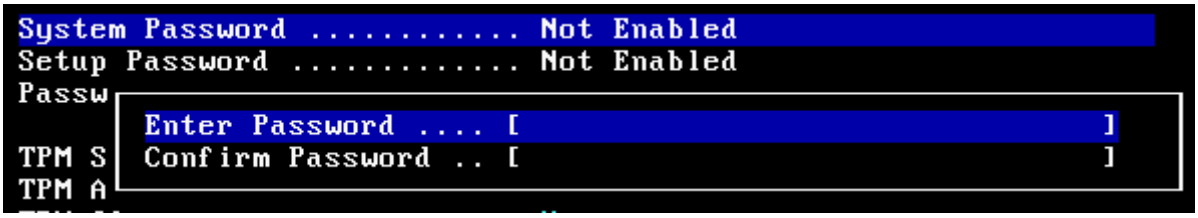

Figure 2 : BIOS Password Setup

Enable / Disable Unified Server Configurator

The USC can be enabled/disabled from the iDRAC option ROM. You can enter the iDRAC option ROM by using Ctrl+E when the system is booting. Once you are in the iDRAC option ROM, go to **System Services**.

Figure 3 : iDRAC Option ROM

Usually, system services are enabled as factory default settings.

Figure 4 : System Services Enabled

Setting **System Services** to **Disabled** will completely disable USC and all its functionalities. Once set to disabled, the F10 option to enter USC will also be disabled. Post will show `System Services disabled` as shown in the figure below.

Figure 5 : System Services Disabled

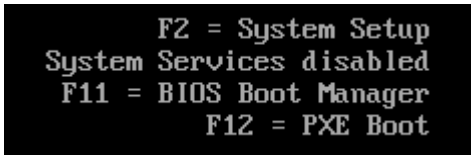

Figure 6 : POST

Virtual Flash

The VFlash or Virtual Flash is an optional SD card present with the iDRAC6 Enterprise solution. Unlike the embedded firmware used by USC, this card can be accessed (removed or inserted) from the back of the system. When enabled, Virtual Flash is configured as a virtual drive and appears in the boot order, allowing a user to boot from the Virtual Flash or access Virtual Flash from the host OS. User data stored on VFlash is the responsibility of the user to secure. Access to the Virtual Flash can be disabled by going through the iDRAC option ROM menu and selecting "Virtual Media Configuration" and choosing the enable/disable option.

Figure 7 : Virtual Media Configuration

Summary

Dell encourages security evaluations at every level of its software development lifecycle and as a result, USC software has high security standards and in addition adheres to various industry security standards and principles. The software has been configured with options for customers to configure security settings according to their IT environments. Unified Server Configurator was designed to provide secure and safe operation and is most secure when used in environments that adhere to established security best practices.