

Introdução a Conecte e gerencie com o TechDirect

Conecte-se ao TechDirect para ter o suporte mais inteligente quando mais precisar

O desempenho do PC é muito importante quando você trabalha em casa. Caso sua equipe enfrente desafios, ela precisa que os PCs sejam rápidos, inclusive na resolução de problemas. No entanto, com pouca noção sobre o desempenho do PC em tempo real, você pode estar reagindo aos problemas depois que seus funcionários já foram afetados por frustração e tempo de inatividade.

Conquiste a proatividade. Conecte-se ao TechDirect implementando o SupportAssist para PCs empresariais e tenha acesso a informações e ferramentas que oferecem o melhor desempenho aos PCs de sua equipe, para que ela possa trabalhar a qualquer hora e em qualquer lugar sem o estresse dos contratempos tecnológicos.

Gerencie e monitore seus PCs centralmente — a qualquer hora e em qualquer lugar — para obter desempenho ininterrupto dos PCs



Inscreva-se para ter uma conta gratuita no TechDirect, nosso portal do cliente on-line



Implemente remotamente o SupportAssist em sua frota de PCs



Gerencie e monitore PCs centralmente, desbloqueando recursos adicionais com o [ProSupport Suite for PCs](#)

Assim que tiver a conexão, libere esse potencial para:

Oferecer uma experiência descomplicada a qualquer hora e em qualquer lugar

- **Garantir a produtividade** com drivers, BIOS e firmware atualizados
- **Otimizar a experiência de PC** de sua equipe
- **Proteger seu ambiente** com remoção automatizada de vírus e malware

Obter suporte mais inteligente com a inteligência artificial que prevê problemas

- **Poupar tempo e esforço** com um monitoramento em tempo real que identifica e soluciona problemas proativamente, até 84% mais rápido que a concorrência²
- **Praticamente eliminar o tempo de inatividade não planejado** prevenindo problemas antes que aconteçam³

Prever as necessidades da equipe com percepções orientadas por dados

- **Antecipar-se às interrupções** com a percepção de problemas que afetam o desempenho
- **Tomar decisões melhores, orientadas por dados**, monitorando o uso e a atualização



Coletar com segurança apenas as informações necessárias para resolver problemas

Com a segurança e a privacidade integradas, você tem o controle para autorizar a coleta de informações de diagnóstico. Os diagnósticos são mantidos em segurança durante o transporte e o armazenamento com criptografia de 256 bits e uma comunicação unidirecional protegida por firewall de seus locais para a Dell.

Saiba mais sobre [como o SupportAssist monitora seus PCs Dell com segurança](#).

Use as seguintes etapas para se conectar

Antes de começar, analise o [Guia de implementação](#).

Você tem tudo o que é necessário para implementar?

- ✓ Atender aos [requisitos mínimos do sistema](#)
- ✓ Uma conta do TechDirect com acesso de administrador
- ✓ Detalhes de seu proxy
- ✓ Uma ferramenta de implementação (por exemplo, SCCM)

- 1** **Faça login no TechDirect** com suas atuais credenciais ou configure uma nova conta em minutos, se for um usuário que está acessando pela primeira vez.
- 2** **Configure sua empresa para se conectar e gerenciar no TechDirect.**
 - Se você estiver começando, deve associar a conta à sua empresa e se inscrever como administrador da empresa.
 - Registre-se no serviço lendo e aceitando os Termos e condições.
 - Adicione usuários técnicos e designe funções de administração.
- 3** **Configure o pacote de download** definindo como você vai monitorar e gerenciar PCs em todo o seu ambiente.
- 4** **Faça download** do pacote personalizado, **inicie** o gerenciador de pacotes de implementação e **salve** o pacote em seu PC.
- 5** **Use sua ferramenta preferida de implementação** para instalar o SupportAssist em sua frota.
- 6** **Comece a usar o TechDirect** para gerenciar facilmente seus PCs e os alertas da Dell, começar a atualizar e otimizar sistemas e obter informações sobre o desempenho de sua frota.

Alguma dúvida? [Participe de um webinar](#) para entrar em contato com um especialista ou visualizar uma gravação.

Dicas e sugestões

- **Ative a atualização automática** durante a configuração para ter sempre a versão mais recente em execução no ambiente
- É possível **configurar grupos** para implementar várias configurações com base nos requisitos de localização, departamentos, personas ou grupos de teste
- Por padrão, o agente do SupportAssist é executado em segundo plano e não interrompe os funcionários. Se você quiser conceder permissão para os usuários interagirem independentemente com o TechDirect, poderá **ativar a interface do usuário final** durante a configuração
- **Encaminhe alertas** para suas ferramentas existentes, como o ServiceNow
- O **Google® Chrome** fornece a melhor experiência com o TechDirect

Como acessar os recursos do TechDirect?

Os recursos variam conforme o nível de serviço. Você pode desfrutar do conjunto completo de recursos com o ProSupport Plus.

	Manutenção básica de hardware	ProSupport	ProSupport Plus	ProSupport Flex ⁴
Autoatendimento no gerenciamento de casos e no despacho de peças	•	•	•	•
Deteção de problemas, notificação e criação de casos — tudo automatizado e proativo		•	•	•
Visibilidade da base de ativos para facilitar o gerenciamento e os alertas		•	•	•
Deteção antecipada de problemas de desempenho com utilização de hardware e software		•	•	•
Otimização de PCs por meio de resolução remota (incluindo BIOS e drivers)			•	•
Deteção automatizada e preditiva de problemas para prevenção de falhas			•	•

Recursos

- [Portal on-line do TechDirect](#)
- [Documentação técnica](#)
- [White paper: Como o TechDirect monitora os PCs Dell com segurança](#)
- [Participe de um webinar](#)
- Entre em contato com a equipe de vendas ou com seu Gerente de contas de serviços para saber mais sobre o [ProSupport Suite for PCs](#)

1. Recursos do TechDirect que exigem conectividade do SupportAssist não estão disponíveis para Linux, Windows RT, Android, Ubuntu nem para alguns produtos baseados no Chrome. O TechDirect, quando conectado pelo SupportAssist, detecta automaticamente e alerta proativamente a Dell sobre: problemas do sistema operacional, upgrades de software, atualizações e patches de driver, malware, arquivos infectados por vírus, falhas em discos rígidos, baterias, memória, cabos internos, sensores térmicos, dissipadores de calor, ventiladores, unidades de estado sólido e placas de vídeo. O TechDirect, quando conectado por meio do SupportAssist, permite a detecção de falha de análise preditiva para discos rígidos, unidades de estado sólido, baterias e ventiladores.

2. Com base em um relatório de testes da Principled Technologies, "Dell ProSupport Plus warns you about hardware issues so you can fix them before they cause downtime", abril de 2019. Testes encomendados pela Dell e conduzidos nos Estados Unidos. Os resultados reais podem variar. Relatório completo em: <http://facts.pt/0xvze8>.

3. Com base em um relatório de testes da Principled Technologies de abril de 2020, "Diagnose and resolve a hard drive issue in less time with Dell ProSupport Plus". Testes encomendados pela Dell e conduzidos nos Estados Unidos. Os resultados reais podem variar. Relatório completo em: <http://facts.pt/ddv0ne9>.

4. Os clientes devem se comprometer a adquirir 1.000 ativos client Dell com o ProSupport Flex no prazo de 12 meses.

Direitos autorais © 2022 Dell Inc. ou suas subsidiárias. Todos os direitos reservados. Dell Technologies, Dell, EMC, Dell EMC e outras marcas comerciais são marcas comerciais da Dell Inc. ou de suas subsidiárias. Outras marcas comerciais podem pertencer a seus respectivos proprietários. Junho de 2021 | Dell Technologies TechDirect Getting Started Connect Manage

Produtos
Soluções
Serviços
Suporte
 Voltar
Página de suporte
Base de conhecimento
Garantia e contratos
Chamados e status de despacho
Suporte a pedidos
Entre em contato com o suporte
Comunidade

Bem-vindo ao Suporte Dell



Problemas técnicos



Identifique o dispositivo

Latitude 3420

Etiqueta de servi#xE7;o: 6H6GSK3



Descreva o problema

Problema não listado



Veja as opções de suporte

Opções de suporte disponíveis

O plano de serviço tem  Básica



Seu produto está coberto pela Garantia básica de hardware da Dell, que oferece acesso a suporte especializado durante o horário comercial. O suporte em outros horários e no fim de semana pode não estar disponível.

RECOMENDADO



Recursos de suporte on-line

Pesquise manuais, artigos e vídeos práticos para encontrar uma solução rápida.

[Suporte à pesquisa](#)



Localizador do serviço de entrega

Para obter o serviço de entrega, entre em contato conosco para receber o diagnóstico e o número de autorização obrigatório.

Encontrar centro de reparo



Entre em contato conosco

0-800 970- 3355 Seg - Sex, das 8h às 20h

Nota: você será solicitado a inserir seu código de serviço expresso **14099480211**



Chat

Converse com um de nossos especialistas técnicos.

Configure o navegador para aceitar cookies a fim de acessar o chat.

Iniciar chat

Tempo de espera no momento: 22 segundos.



Fale conosco pelo WhatsApp

Faça a varredura abaixo para [Chat com um técnico certificado pela Dell](#) ou adicione + 55 19 99335-5566 no WhatsApp.

O suporte está disponível 8 a.m. às 8 p.m., de segunda a sexta-feira.

Fale conosco pelo WhatsApp



TechDirect

Acompanhe e gerencie as solicitações de suporte da sua empresa.

TechDirect

[← Selecione problema diferente](#)

Mapa do site

Conta

[Minha conta](#)

[Status do pedido](#)

[Meus Produtos](#)

Suporte

[Página de suporte](#)

[Entre em contato com o suporte](#)

Fale conosco

[Comunidade](#)

[Fale conosco](#)

[Facebook](#)

[Twitter](#)

[Instagram](#)

[YouTube](#)

Nossas ofertasNossa empresa

[APEX](#)

[Quem somos](#)

[Produtos](#)

[Carreiras profissionais](#)[Localize um Varejista](#)[Eventos](#)

[Sobre nós](#)

[Notícias](#)

Nossos parceiros Recursos

[Encontre um parceiro](#)[Blog](#)

[Soluções de OEM](#)[Glossário](#)

Serviços	Reciclagem	Programa de parceria	Centro de privacidade
Promoção	Impacto social		Biblioteca de recursos
			Downloads de teste de software

Dell.com	Dell Technologies	Premier
-----------------	--------------------------	----------------

Copyright © 2022 Dell Inc.	Termos e Condições	Declaração de Privacidade	Cookies, Anúncios e e-mails
Informações Legais e Regulatórias	Políticas	Cumprimento dos Requisitos Regulatórios	

Acesso à configuração do sistema UEFI (BIOS) no Windows no sistema Dell

Resumo: Etapas e informações sobre como acessar o BIOS do sistema a partir do Windows.

Conteúdo do artigo

Sintomas

Este guia mostra como acessar a configuração UEFI (BIOS) do Windows. Use as guias abaixo para selecionar o sistema operacional instalado no seu computador.

Nota: alguns sistemas podem não ter essa opção, pois o BIOS não consegue alterar as configurações UEFI ou SATA.

Windows 10

Windows 8 ou 8,1

Windows 7

Inicialização de UEFI (BIOS) no Windows 10

Nota: para inicializar no BIOS UEFI sem entrar no Windows, siga as etapas a seguir:

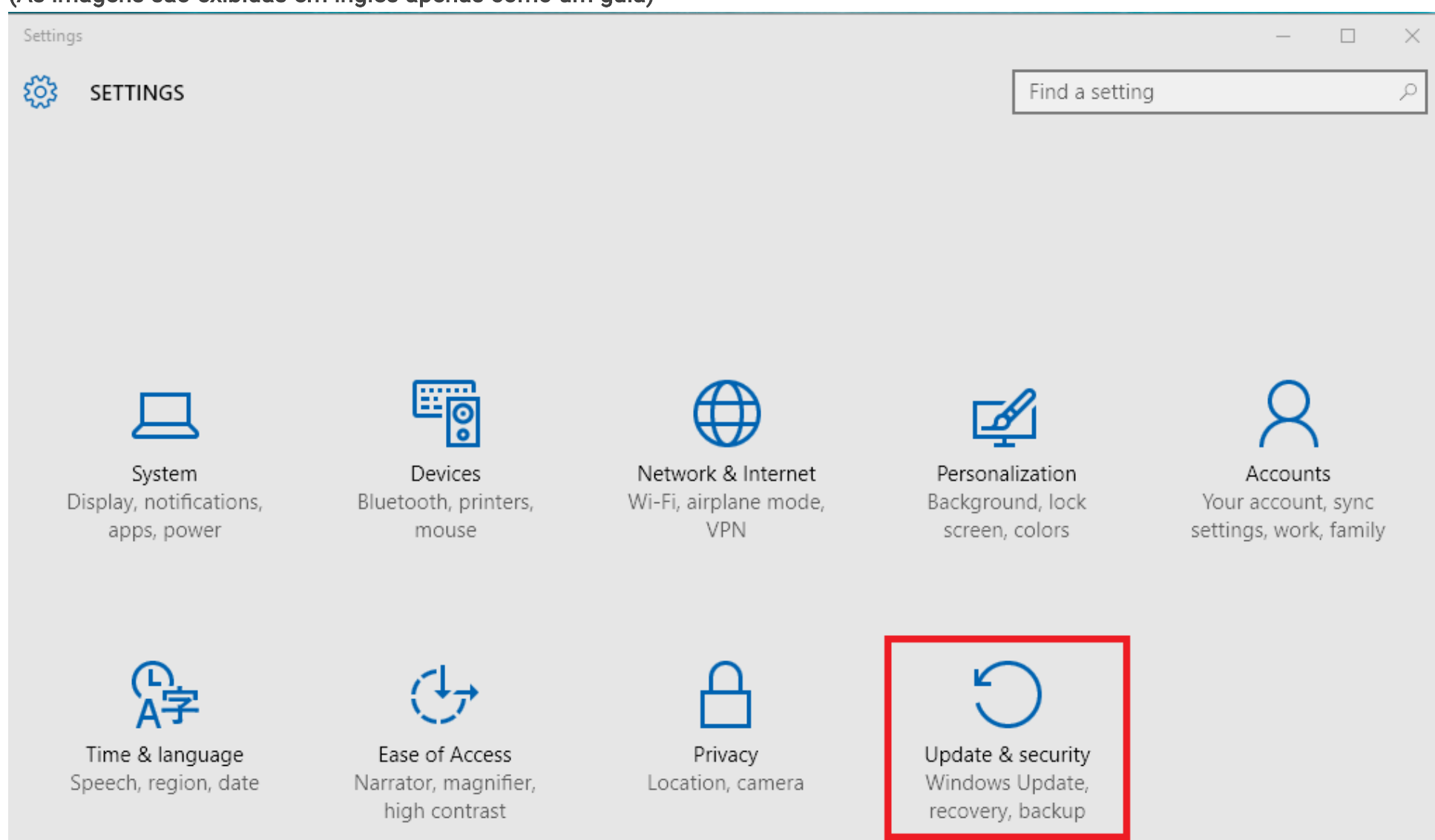
Ligue o sistema.

Pressione a tecla **F2** para entrar na Configuração do sistema quando o logotipo da Dell for exibido. Caso tenha dificuldade em acessar as Configurações utilizando esta tecla, pressione **F2** quando os LEDs do teclado piscarem pela primeira vez.

Tente não manter pressionada a tecla **F2**, pois isso às vezes pode ser interpretado pelo sistema como uma tecla presa.

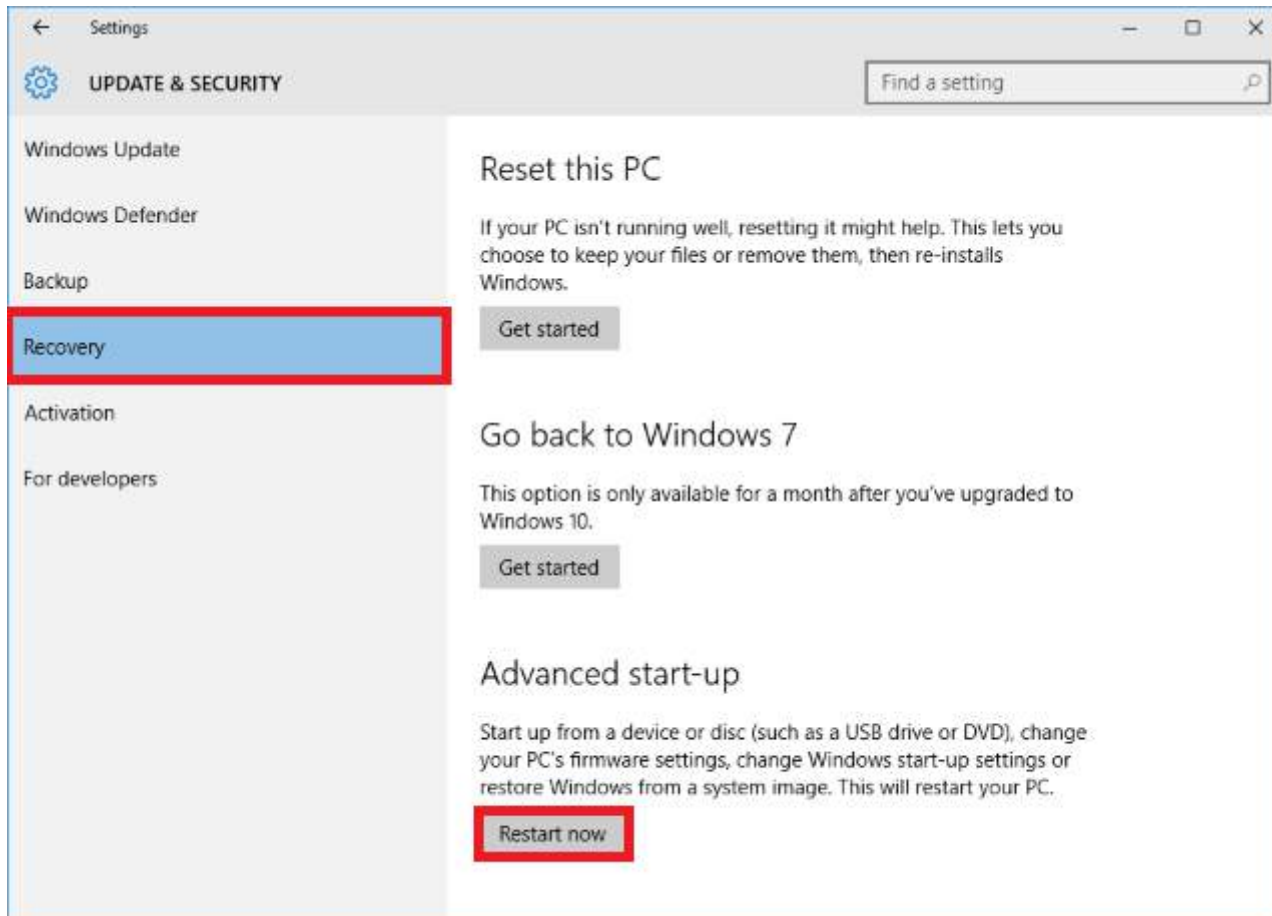
1. Clique no menu do botão sinalizador Iniciar e selecione **Configurações**.
2. Selecione **Atualização e Segurança**.

(As imagens são exibidas em inglês apenas como um guia)

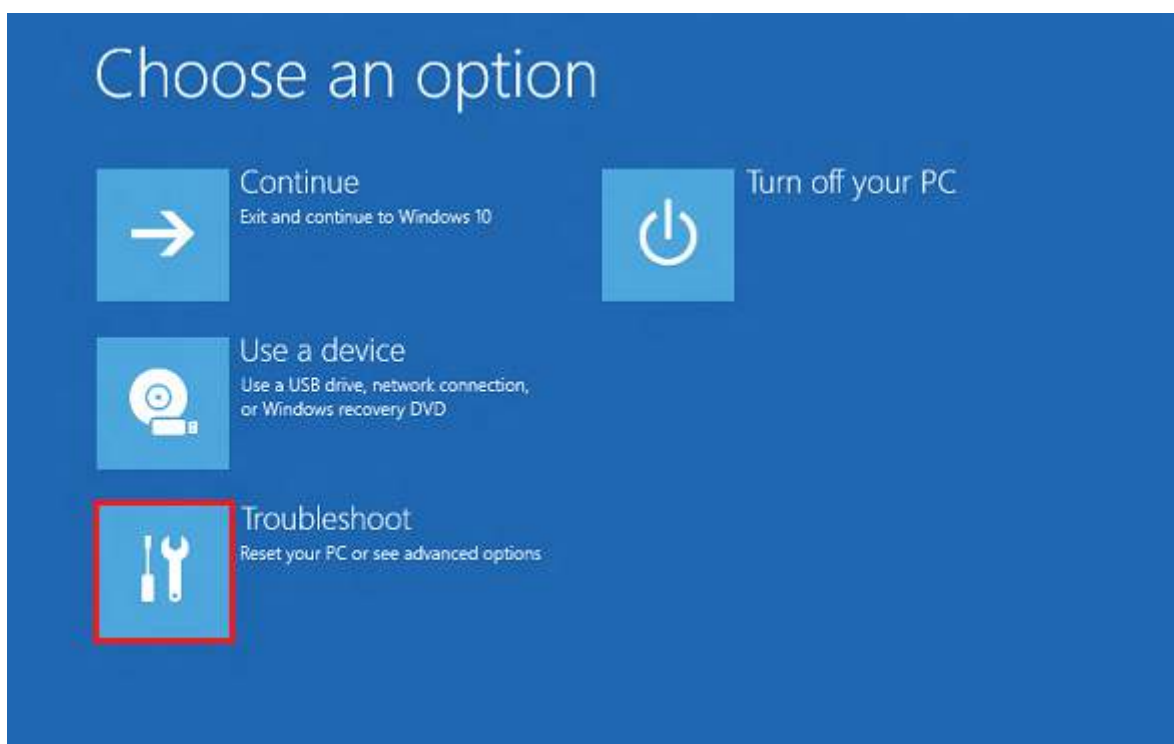


3. Clique em **Recuperação** no menu à esquerda.

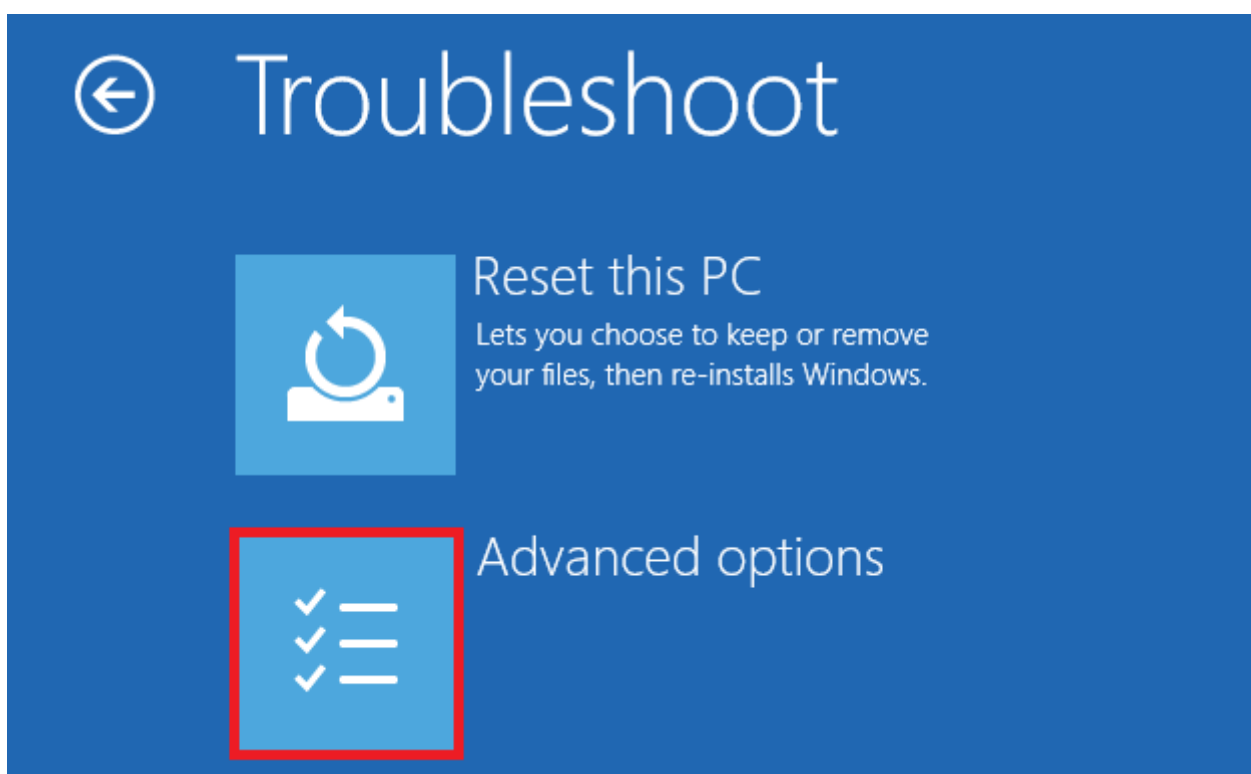
4. Em **Inicialização avançada**, clique em **Reiniciar agora**.



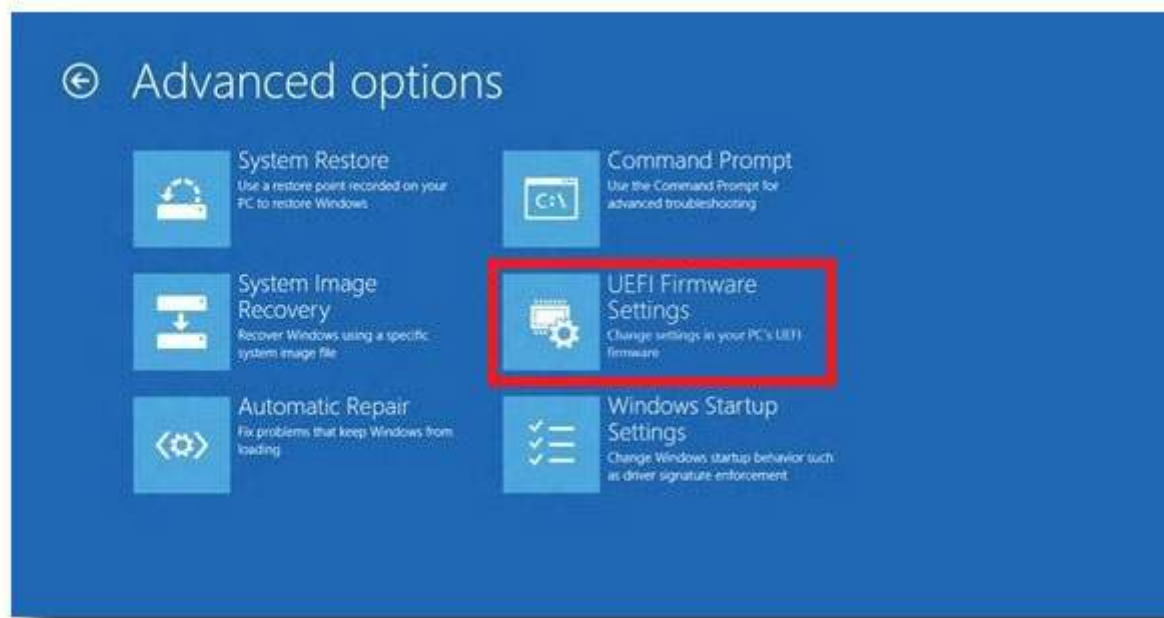
5. Selecione **Solução de problemas**.



6. Escolha **Opções avançadas**.



7. Selecione **Configurações de firmware UEFI**.



8. Clique em **Reiniciar** para reiniciar o sistema e entre no UEFI (BIOS).

Propriedades do artigo

Data da última publicação

04 Oct 2021

Versão

4

Tipo de artigo

Solution



Ministério do Meio Ambiente
Instituto Brasileiro do Meio Ambiente e dos Recursos Naturais Renováveis



CADASTROS TÉCNICOS FEDERAIS
CONSULTA PÚBLICA A CERTIFICADO DE REGULARIDADE - CR

Registro n.º: Data da consulta: CR emitido em: CR válido até:

[Dados básicos](#)

CNPJ:
Razão social:
Nome fantasia:
Data de abertura:

[Endereço](#)

Logradouro: Complemento:
N.º: Município:
Bairro: UF:
CEP:

Cadastro Técnico Federal de Atividades Potencialmente Poluidoras e Utilizadoras de Recursos Ambientais – CTF/APP

Categoria	Detalhe
5 - Indústria de material Elétrico, Eletrônico e Comunicações	2 - Fabricação de material elétrico, eletrônico e equipamentos para telecomunicação e informática

Conforme dados disponíveis na presente data, a pessoa jurídica acima possui Certificado de Regularidade em conformidade com as obrigações cadastrais e de prestação de informações ambientais sobre as atividades desenvolvidas sob controle e fiscalização do Ibama, por meio do CTF/APP.

O certificado de regularidade emitido pelo CTF/APP não desobriga a pessoa inscrita de obter licenças, autorizações, permissões, concessões, alvarás e demais documentos exigíveis por instituições federais, estaduais, distritais ou municipais para o exercício de suas atividades.

O Certificado de Regularidade do CTF/APP não habilita o transporte e produtos e subprodutos florestais e faunísticos.

[Fechar](#)

Dell OpenManage Client Instrumentation (OMCI) Standards and Protocols

CONTEÚDO DO ARTIGO

PROPRIEDADES DO ARTIGO

AVALIE ESTE ARTIGO

Conteúdo do artigo

Sintomas

OMCI uses Microsoft Windows Management Instrumentation (WMI) and enables Web Services-Management (WSMAN) protocols. OMCI uses Simple Network Management Protocol (SNMP) to describe several variables of the system.

CIM, SNMP, WMI and WSMAN Technology Overview

The Desktop Management Task Force (DMTF) is the industry-recognized standards body that leads the development, adoption, and unification of management standards (including CIM and ASF), and initiatives for desktop, enterprise, and Internet environments.

CIM

The CIM, created by the DMTF as part of the Web-based Enterprise Management (WBEM) initiative, provides a unified view of physical and logical objects in the managed environment. The following are important CIM details:

- CIM is an object-oriented data model for describing management information. CIM describes the way the data is organized, not necessarily the transport model used to transport the data. The most prevalent transport method is the WMI.
- CIM-capable management applications gather information from a variety of CIM objects and devices, including client and server systems, network infrastructure devices, and applications.
- The CIM specification details mapping techniques for improved compatibility with other management protocols.
- The CIM data model abstracts and describes all elements in a network environment. The CIM schema provides the actual data model descriptions and arranges the network into a series of managed objects, all interrelated and broadly classified.
- The CIM schema is defined by the Managed Object Format (MOF) file, which provides a standardized model for describing management information between clients in a management system. The MOF file is not bound to a particular implementation, and it allows the interchange of management information among different management systems and clients.

SNMP

Simple Network Management Protocol (SNMP) is a widely accepted solution to manage devices on IP networks. SNMP is developed and maintained by Internet Engineering Task Force (IETF). OMCI access information and monitor client systems using SNMP. Devices that typically support SNMP include routers, switches, servers, workstations, most of the hardware components and more. It consists of a set of standards for network management, including an application layer protocol, a database schema, and a set of data objects. SNMP exposes management data in the form of variables on the managed systems, which describe the system configuration. These

variables can then be queried by managing applications.

SNMP does not define which information (which variables) a managed system should offer.

Rather, SNMP uses an extensible design, where the list of available information is defined by management information bases (MIBs). MIBs describe the structure of the management data of a device and its subsystems. MIBs use a hierarchical namespace containing object identifiers (OID). Each OID identifies a variable that can be read via SNMP.

WMI

WMI is Microsoft's implementation of the Web-based Enterprise Management (WBEM) effort. It is implemented on the Microsoft Windows platforms. WMI supports CIM and Microsoft-specific CIM extensions.

WMI includes:

- A powerful set of native services such as query-based information retrieval and event notification.
- Extensive scripting capabilities via the Windows Scripting Host (WSH).
- The CIMOM, which is the interface and manipulation point for CIM objects and information.
- The repository, where CIMOM stores management data.

In the OMCI architecture, CIMOM and the repository are represented by the Microsoft WMI Object Manager. The CIMOM is the interface and manipulation point for CIM objects and information. It acts as a facilitator in gathering information and manipulating object properties. Microsoft has implemented this component as the Windows management (winmgmt) service. The CIMOM is a software middle layer that mediates interactions between high-level management applications and the low-level instrumentation, such as OMCI and other providers. The CIMOM ensures that data supplied by providers is presented to management applications in a uniform and provider-independent way. The CIMOM does this by using the Component Object Model (COM) Application Programming Interface (API).

The repository is a binary file where the CIMOM stores management data. The data includes information from the compiled Managed Object Format (MOF) file(s), including the CIM class definitions, properties, qualifiers, and hierarchical relationships. Instance data, as it becomes available, is also stored here.

WMI provides a scripting interface. Using VBScript or JScript, you can write scripts, connect to WMI services locally or remotely, retrieve information, or execute methods. You can script most of the OMCI tasks as OMCI is implemented through WMI. For the sample VBScript scripts, see the Dell OpenManage Client Instrumentation Reference Guide available at support.dell.com/manuals. For more information about WMI, see thetech.net.microsoft.com.



NOTE: To connect remotely to WMI services, you must have administrative rights on both the local and remote systems.

WSMAN

The WSMAN protocol is a DMTF open standard defining a Simple Object Access Protocol (SOAP)-based protocol for managing servers, devices, applications, and web services. It uses data from CIMOM to facilitate the management.

WSMAN is a protocol that provides an abstraction layer to access the CIM information. The reason is that the console can use WSMAN to communicate with in-band or out-of-band systems to gather asset inventory and to set information or run methods. In in-band systems, the WSMAN layer also abstracts the operating system present underneath. However, OMCI does not require WSMAN and it does not directly enable WSMAN as it is only a protocol.

Propriedades do artigo

Produto afetado

Desktops & All-in-Ones, Laptops, Servers

Data da última publicação

21 fev 2021

Versão

3

Tipo de artigo

Solution

Avalie este artigo

Fale conosco

Preciso

Úteis

Fácil de entender

Este artigo foi útil?

☐ Sim ☐ Não

Mais informações (opcional)

0/3000 characters

Enviar feedback

Artigos vistos por último

[Dell Command Update](#)

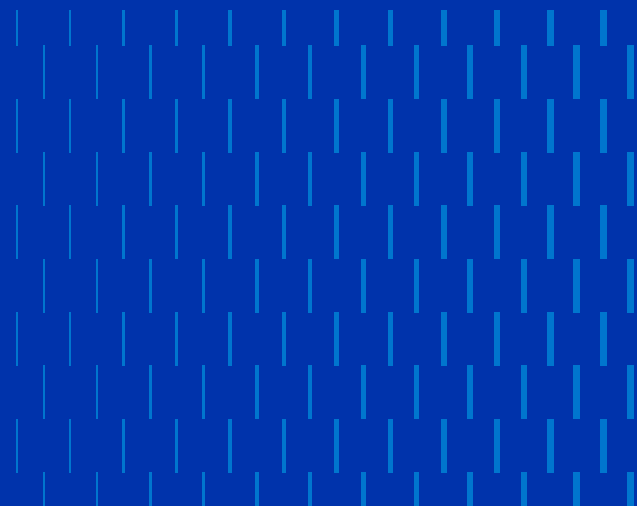
[Dell Command | Monitor: Simple Network Management Protocol \(SNMP\).](#)

[O que é BIOS e como atualizar o BIOS do seu sistema Dell](#)

[Dell Data Wipe](#)

[Ações de limpeza de unidade de disco rígido suportadas de Dell de limpeza de dados \(NIST 800 88r1\).](#)

Dell Trusted Device Below the OS White Paper



**A deep dive into the foundational, BIOS-level security of
Dell Trusted Devices, the world's most secure commercial
PCs***

January 2026



© 2026 Dell Inc. or its subsidiaries. All Rights Reserved. Dell, EMC, Dell EMC and other trademarks are trademarks of Dell Inc. or its subsidiaries. Other trademarks may be trademarks of their respective owners.

*Based on Dell internal analysis, October 2025 (Intel) and March 2025 (AMD). Applicable to PCs on Intel and AMD processors. Not all features available with all PCs. Additional purchase required for some features. Intel-based PCs validated by [Principled Technologies](#), July 2025.

Table of Contents

Preface	5
Introduction	6
Sidebar on Quantum-Readiness in Device Security.....	8
The Key Elements of Dell Built-In Security.....	8
The Role of BIOS (and what is UEFI?)	8
Secure Design Processes and SDL	10
Supply Chain Security	10
Industry Affiliations	11
Built-In “Below the OS” Security	12
Dell Trusted Device (DTD) Application.....	13
The Importance of Built-In “Below the OS” Security	14
Understanding Dell Cybersecurity Using the NIST Framework	14
Identify	16
Device Identity	17
<i>HBOM and SBOM</i>	18
Credential Protection: Dell SafeID	19
“Below the OS” Threat Modeling	20
Protect.....	20
Protecting the PC Boot Process.....	21
Securing the Boot Chain	22
The “Root of Trust”	22
TCG and the Root of Trust	22
UEFI Secure Boot.....	23
UEFI Secure Boot Expert Key Management.....	24
Signed Firmware Update.....	24
NIST SP800-147 Support	25
System Management Mode (SMM) For x86 Systems.....	25
Trusted Firmware for ARM Systems – Secure Partition Manager (SPM).....	27
BIOS Patch Management.....	28
BIOS Downgrade Protection	29
Embedded Controller: Signed Firmware	29

Dell Trusted Device Below the OS White Paper

Protecting BIOS Configuration	29
Configuration Side-Channels	32
Best Practices for Secure Configuration	33
Protecting BIOS at Runtime	33
Runtime BIOS Resilience (Intel Only)	33
Runtime BIOS Resilience (AMD Only)	34
Detect	34
Dell Physical Security Features	35
Physical Security – Chassis Intrusion	35
Ability to Block Boot after Chassis Intrusion	35
TPM integration for Chassis Intrusion events	36
Battery Removal Detection	36
SPI Flash Anti-Tamper features	36
Dell Built-In “Below the OS” Detection Capabilities	36
Dell off-Host BIOS and Firmware Verification	36
Indicators of Attack	38
How Off-Host Verification Is Performed	39
BIOS Image Capture	40
Common Vulnerabilities and Exposures (CVE) Detection and Remediation	40
Security Risk Protection Score	41
TCG Measured Boot	42
Intel® vPro Additions to Built-In Security	43
Code, Configuration, and the TPM Event Log	43
NIST 800-155 Measurements	44
Advanced: NIST 800-155 Measurements Extraction, Conversion, and Comparison	45
Dell Integrations with Hardware Providers	46
Intel Boot Guard	46
Intel Management Engine (ME) Firmware Verification	46
Intel vPro Integration for Out of Band Management (OOBM)	46
Microsoft Intune Integration	47
Hardware-Assisted Security with CrowdStrike and Intel	47
Below-the-OS Integration with CrowdStrike for Dell on AMD	48
Below-the-OS Integration with Absolute	48
Other Integrations for SafeBIOS	49

Respond and Recover 49

 Embedded Controller Recovery 49

 BIOS Recovery 50

 BIOS Recovery Image Update Flow 50

 Auto Recovery Flow 51

 Customer Flexibility: Manual Recovery 51

 Confirming BIOS Integrity 51

 Dell Data Sanitization 51

Additional Dell Security Capabilities 52

Protected Signing Infrastructure 52

The Future of Security 53

References 54

Dell and Partner References 54

Industry Organizations 54

Standards and Guidelines 55

Quoted Stats 55

Preface

Since the original release of this paper, which focused on Dell PCs with Intel x86 processors, Dell is now offering PCs with processors from AMD, Qualcomm and NVIDIA.

Our goal is to provide a high level of security for all commercial PCs. However, there are some differences in how this is implemented from platform to platform. When there is a difference, it will be noted in the text.

The paper also reflects revisions for:

- Naming conventions – Dell introduced a restructure of its PC naming, and this paper has been updated for this;
- Introductions and refinements in current solutions, including Secured Component Verification (SCV).
- New strategic software partnerships and deepening of existing partnerships (these software solutions leverage Dell Trusted Device and BIOS telemetry, improving prevention, detection, response and recovery/remediation).

Introduction

Computer security is a multi-billion-dollar business with thousands of companies competing for organizations' attention and enterprise dollars, and with good reason: it can provide a healthy payday for the attacker. The cost of cybercrime worldwide continues to grow at a brisk rate – [from \\$5.49 trillion USD in 2021 to a projected \\$10.5 to 12 trillion USD in 2025](#). These figures reflect the impact of increasingly sophisticated attacks, including ransomware. Governments are also witnessing growing nation-state level cyberattacks, as countries do battle using these weapons of warfare. The increasing adoption of zero trust methodologies and architectures reinforces that security remains a fundamental aspect of ensuring that an organization can secure its key assets and prevent the damage that even a simple cyberattack can wreak upon its operations.

One of the most critical and fundamental tenets in computer security is transparency. Though highly effective, security features deeply embedded within a client are not always visible. The intent of this publication is to provide transparency into the Dell device security features and technology implementations as provided and enforced by the code responsible for device boot and other fundamental device functions, which we refer to as our BIOS (Basic Input/Output System).

Dell Technologies has created [Dell Trusted Workspace](#), an innovative portfolio of technologies and solutions spanning both hardware and software, and dedicated to helping organizations effectively secure their enterprises while providing visibility to threats. One of the areas where Dell has substantially invested over the last decade is in the security of the endpoint itself, in this case the “client” device (desktops, workstations, and notebooks). The collection of innovative ‘built-in’ security features native to Dell hardware strengthens the ability of Dell client devices to detect, respond to and mitigate stealthy attacks which operate below the purview of the operating system – or ‘below-the-OS’ as it is often called. Dell takes this a step further through integration with software (e.g., EDR/XDR and SIEM) and device management solutions such as Microsoft Intune to enable organizations to take appropriate action and analyze a threat to improve response effectiveness.

Dell's leading commercial device security is offered on both Intel- and AMD-based devices. There are additional built-in security features from Intel® vPro, an option for Intel-equipped PCs. Though mention will be made, for more in-depth information there is a separate paper dedicated to those features that may be [downloaded here](#).

Even with the latest news about the increase in cyberattacks, there are still organizations that believe that security equals encryption plus antivirus, and that software is all it takes to be secure. They may recognize and appreciate Dell's significant investment in endpoint security but question the need. Why don't firewalls, IDS/IPS, SIEMs, NGAV, EDR and all the various alphabet soup of enterprise-level security tools already cover everything?

Well, those tools may be good at what they do. But they don't do everything. Dell believes that overall infrastructure security not only depends on these tools but also on the built-in security of each endpoint: that each endpoint should serve both as a point of security defense and as a security “sensor”, with both approaches supporting the overall zero-trust posture of the organization. From this perspective, the endpoints, and subsequently each individual device, collectively become the foundation of security for the entire enterprise. Further, as attackers develop more stealthy threats which work at the hardware level, existing security software simply isn't enough to detect and respond to them. Hardware-generated telemetry such as that provided by the Dell Trusted Device (DTD) Application provides a valuable source of information that can

be used to offset these increasing threat vectors – in essence, built-in security. This domain can only be implemented and supported by the OEM, and Dell continues to advance the abilities of its products to protect, detect, respond, and recover from cyberattacks.

This paper was written to provide a thorough introduction to the Dell device BIOS security features and hardening. The BIOS remains an extremely important component in a modern PC, and some of the more foundational (and critical) security hardening aspects of the device start with and depend on the BIOS. This document will unwrap the terminology and lexicon that has tightly attached itself to this area of technology and explain the individual features and components of the BIOS that help to secure enterprise infrastructure from the device up to the cloud.

The audience for this document includes security operation center (SoC) analysts, IT admins and decision makers (ITDMs), IT support personnel, compliance and risk/governance teams, security researchers and analysts, and anyone else interested in learning more about the built-in security offered by the Dell devices via security and hardening of the underlying BIOS and firmware.

Contextually this document is broken into sections that map to specific outcomes described in the [NIST Cybersecurity Framework \(CSF\)](#): Identify, Protect, Detect, Respond and Recover. This should help put each feature included in Dell devices into the perspective of the overall goal of helping to secure each organization's enterprise.

- **Identify:** Develop an organizational understanding to manage cybersecurity risk to systems, people, assets, data, and capabilities. Within the Dell security schema, this refers to tools to help customers categorize these classifications, including asset management and those secure design principles which proactively contribute to security (e.g., Dell Service Tag, Dell SafeID, Threat Modeling).
- **Protect:** Develop and implement appropriate safeguards to ensure delivery of critical services. These include defensive technologies to harden non-volatile storage and the boot process (e.g., Signed Firmware Update, BIOS Passwords).
- **Detect:** Develop and implement appropriate activities to identify the occurrence of a cybersecurity event. This includes the ability to convey status when unauthorized changes occur (e.g., SafeBIOS Verification, Intel® Boot Guard).
- **Respond:** Develop and implement appropriate activities to respond to a detected cybersecurity incident. Action is taken by the organization using tools and data (telemetry) provided by Dell capabilities described in this paper.
- **Recover:** Develop and implement appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity incident. This includes advanced mitigations to quickly remediate issues (e.g., BIOS Recovery, Dell Data Wipe).

Govern was introduced in the 2024 version of the CSF and intended to underlie each of these activities, which are critical for incorporating cybersecurity into an organization's broader enterprise risk management (ERM) strategy. From the perspective of an OEM such as Dell, Govern concerns work to be performed by the customer organization to understand organizational context; establish cybersecurity strategy and cybersecurity supply chain risk management; roles, responsibilities, and authorities; policy; and provide for the oversight of

cybersecurity strategy. It is not covered in the scope of this document, although it is essential for any organization seeking to implement and manage a robust cybersecurity strategy.

This document concludes with a brief section on our commitment to the ongoing Dell investments helping to shape the future of security. This document is not the end of the conversation about Dell device security; hopefully it's the continuation of a long and bi-directional discourse beneficial to the industry overall.

Sidebar on Quantum-Readiness in Device Security

Quantum computing is poised to revolutionize industries—but it also introduces unprecedented cybersecurity challenges. Current encryption methods, which safeguard sensitive data and device integrity, rely on algorithms that quantum computers will eventually break with ease. This means that the very foundation of trust in devices could be compromised if organizations fail to prepare.

The risk isn't theoretical. Threat actors are already employing "harvest now, decrypt later" (HNDL) tactics—collecting encrypted data today with the intent to decrypt it once quantum capabilities mature. For businesses, this translates into a ticking clock: intellectual property, confidential communications, and even firmware-level protections could be exposed retroactively.

Building a quantum-ready foundation starts at the deepest layer of device security—the BIOS. Advanced BIOS security features, such as secure boot and hardware root of trust, must evolve to support crypto-agility and post-quantum cryptography (PQC). Crypto-agility ensures that organizations can rapidly update cryptographic algorithms as standards change, while PQC introduces quantum-resistant algorithms designed to withstand future attacks.

Dell Technologies is leading this transition by integrating advanced BIOS security measures that anticipate quantum threats. By adopting these capabilities now, organizations can protect endpoints, maintain compliance, and preserve trust in an era where traditional cryptography will no longer suffice.

Quantum readiness isn't a future consideration—it's a present-day imperative. The organizations that act today will be the ones best positioned to safeguard their data and devices against tomorrow's most disruptive cybersecurity threat.

The Key Elements of Dell Built-In Security

The Role of BIOS (and what is UEFI?)

The "BIOS" in a modern PC remains one of the most misunderstood components of the firmware and software stack. The mere mention of "BIOS" to anyone that's been in the industry for more than a decade evokes memories of resetting the CMOS battery or toggling jumpers on the motherboard to make configuration changes. Many still refer to the BIOS configuration menu, or "BIOS Setup" as the BIOS, but there is so much more to it than that!

For the purposes of this document, the BIOS refers to the pre-boot firmware that the main processor executes at the beginning of every boot and any code that remains resident at runtime that was deployed by the pre-boot firmware. The role of this pre-boot firmware is to initialize memory, configure chipset and discrete devices on the motherboard, provide PC OEM unique features, and to enforce any customer specific configuration settings

managed by BIOS Setup. BIOS is largely OS agnostic and persists across OS installs, this means that most of the built-in features and capabilities described in this document work whether the system has Windows, Linux, or even without an operating system at all.

Additionally, more recently the term “UEFI” has become much more prominent when discussing pre-boot firmware on PCs. While architecturally the UEFI ecosystem has had a net positive effect on compatibility and ease of deployment, the term itself has managed to confuse the issue. UEFI, or the Unified Extensible Firmware Interface, is an industry specification that defines the various optional interfaces and protocols used by pre-boot firmware to configure a PC (in most cases). Many experts pedantically correct others that “UEFI has replaced BIOS!” but that’s only partly true. The truth is, PC OEMs and most subject matter experts in the field still use the term “BIOS” to refer to any pre-boot firmware designed to bootstrap a modern PC, regardless of whether it is UEFI-based, Linux-based, or completely custom.

One of the other net positive effects of UEFI has been the opportunity to integrate features and device drivers directly into the BIOS development flow that are compatible with the UEFI specification. An excellent example of this in practice is the [UEFI Tianocore](#) project on GitHub. Tianocore is the current reference implementation for UEFI and is completely open source. Dell and other OEMs use some of this project code as the foundation or “core” BIOS and add differentiated features on top of the open-source core. Another benefit of this open architecture is that UEFI supports multiple instruction sets such as x86-based and ARM-based PCs.

Secure Design Processes and SDL

Dell's Secure Development Lifecycle (SDL) shown in Figure 1 integrates standards and best practices from a variety of industry consortiums and standards bodies. A primary consideration in SDL is to blend data sources from both internally discovered and externally reported issues, allowing Dell to focus on the most prevalent issues in the Dell device technology space. A second major consideration is industry practices. Dell participates in many industry standards organizations such as SAFECODE, TCG and IEEE Center for Secure Design to ensure alignment to industry practices. Lastly, Dell's Secure Development Lifecycle is aligned with the principles outlined in [ISO/IEC 27034 'Information technology, Security techniques, Application security'](#). These practices are tightly integrated into the design and manufacture of Dell products.



Figure 1: Dell Technologies Secure Development Lifecycle

Supply Chain Security

Supply chain assurance and the broader supply chain security concept are complex topics that demand their own volume. Fortunately, the Dell device supply chain falls under the scope of a previously published comprehensive paper on this subject. The latest version of Dell Supply Chain Assurance is available for download [here](#).

Dell Trusted Device Below the OS White Paper

The following excerpt is a high-level description of many of the Dell device BIOS protection mechanisms that have been covered in-depth in this document:

- Dell has implemented procedures across our commercial servers, desktops, and laptops in accordance with the guidance and recommendations outlined in [NIST SP 800-147](#), Basic Input/Output System (BIOS) Protection Guidelines. Dell's protected BIOS and signed update mechanism help prevent unauthorized modification of the platform firmware and reduce the risk of pre-boot malware or unwanted functionality. From the Dell perspective, "supply chain security" covers more than suppliers, manufacturing sites, and logistics. Dell design, development, validation, and sustaining phases all equate to some parts of the supply chain from the customer perspective. This means that the investments in the features covered in this document can help assist and augment traditional supply chain security. For example, the BIOS verification check is part of the manufacturing process of every Intel and AMD-based commercial PC that Dell produces.

Industry Affiliations

Dell is active in multiple industry-wide groups to collaborate with other leading vendors in defining, evolving, and sharing best practices on product security, and in further enhancing the cause of secure development. Examples of industry collaboration include:

- Dell co-founded and currently chairs the Board of Directors of The Software Assurance Forum for Excellence in Code ([SAFECode](#)). Board members include representatives from Microsoft, Adobe, SAP, Intel®, Siemens, CA and Symantec. SAFECode members share and publish software assurance practices and training.
- Dell is an active participant in and long-time member of the Trusted Computing Group ([TCG](#)), a not-for-profit organization formed to develop, define, and promote open, vendor-neutral, global industry specifications and standards, supportive of a hardware-based root of trust, for interoperable trusted computing platforms. TCG's core technologies include specifications and standards for the Trusted Platform Module (TPM – a part of Dell SafeID), Trusted Network Communications (TNC) and network security and self-encrypting drives.
- Dell is an active member of the Forum of Incident Response and Security Teams ([FIRST](#)). FIRST is a premier organization and a recognized global leader in incident and vulnerability response.
- Dell is an active participant in The Open Group Trusted Technology Forum ([OTTF](#)). OTTF leads the development of a global supply chain integrity program and framework.
- Dell employees were founding members of the [IEEE Center for Secure Design](#), which was launched under the IEEE cyber security initiative to help software architects understand and address prevalent security design flaws.

Built-In “Below the OS” Security

	Dell Unique	Industry Standard
Identify	Dell Identity and Asset Management Tags	• Service Tag • Asset Tag
Detect	• Discrete TPM • Dell SafeBIOS Verification • Dell SafeBIOS IoA/IoC • Dell Secured Component Verification (SCV) • Intel® ME Firmware Verification • CVE Detection	• Runtime BIOS Resilience • TCG Measured Boot • Downgrade Protection
Respond	• Dell SafeBIOS Image Capture • Dell Trusted Device telemetry	Dell BIOS Recovery
Protect	• Fused Root of Trust • Dell UEFI Secure Boot • BIOS Passwords	• Intel® BIOS Guard • Intel® Boot Guard • Authenticated Updates • BIOS Public Keys
Recover	• Dell BIOS Connect • Dell Support Assist	Windows OS Recovery

The security of endpoints collectively forms the foundation of the entire enterprise. Consider the analogy of a house to represent endpoint security. An organization’s most valuable assets – data and sensitive information – are like the family inside this house. Houses however are not intrinsically secure, so homeowners must build or buy additional protection like deadbolts, security cameras, and motion sensors to help secure them. Jumping back to the enterprise: there are plenty of players in the security ecosystem which offer these additional protections, but what’s the remaining gap in this scenario? The foundation. Any dwelling must be built on a stable foundation to protect the homeowner’s investment in security from being subverted from below. That’s where the Dell commercial client protections and Dell SafeBIOS security comes in.

Dell refers to this stable foundation as Built-In, “Below the OS” security. Based on the analogy above, it’s clear that the endpoints and this below the OS foundation are valuable targets for adversaries attempting to get a foothold into an enterprise. This critical role in our customers’ security is why Dell has invested in “below the OS” security for over a decade and why it’s important that we publicly document SafeBIOS and associated features, along with some of the rationale behind their development.

Dell Trusted Device (DTD) Application

Among PC OEMs, only Dell integrates device telemetry with industry-leading software to improve fleet-wide security.* Designed for use on Windows PCs, telemetry data is captured and made available through the Dell Trusted Device (DTD) Application. The DTD App is free, downloadable software that provides maximum BIOS protections within the Dell SafeBIOS product portfolio. The DTD App can also be downloaded in an automated method for fleet management using [Dell Client Device Manager \(DCDM\)](#). It is also available to download from [Dell.com](#). The DTD App maximizes SafeBIOS capabilities by communicating endpoint telemetry between the device and a secure Dell cloud, providing unique below-the-OS insights into security “health.” The data transmitted provides assurance that the BIOS is being measured. If any feature reports unexpectedly change, the IT administrator is notified of possible tampering.

The DTD App provides telemetry to enable several features under Dell SafeBIOS such as Indicators of Attack (IoA) and BIOS Verification, which detect tampering of BIOS firmware and BIOS configuration.

- For Intel-equipped PCs using vPro, it also provides Intel Management Engine (ME) Firmware Verification, which verifies the integrity of highly privileged ME firmware by comparing ME firmware found on the platform with previously measured hashes (stored off-host), and our Security Score, a feature that aggregates various indicators into one easy-to-read KPI.
- For AMD-equipped PCs, it provides off-host verification of the AMD Platform Security Processor – PSP - to verify the integrity of this highly privileged firmware using the same methodology, and a Security Score is also determined and provided.

The administrator can find notifications in the Windows Event Viewer, a log of application and system messages, including errors, information messages and warnings. It's a useful tool for troubleshooting problems and analyzing potential threats as well as attacks that may be ongoing. They can also find this information in their endpoint management tool or SIEM, as Dell integrates device telemetry with industry-leading software to improve fleet-wide security. Our list of extensive partner integrations includes third-party security software such as CrowdStrike Falcon, as well as endpoint managers such as Microsoft Intune, and SIEMs such as Splunk. They can also view elements in Dell TechDirect, and as of the DTD 6.1 release, local users can view this information via a Dell Trusted Device local console.

Not only do these integrations improve threat detection and response with a brand-new set of device-level data: they also help customers make the most of their software investments by extending security-related PC data from ‘below the OS’ into tools which increase visibility and support action. Knowing how much our customers value the ability to view notifications such as security alerts within their preferred environments, Dell’s approach provides not just control and defense – it provides visibility to attack activities, and the DTD App is key to this.

Dell continues to release updates to the DTD App, enabling greater integration capabilities. For example, recent releases expanded key feature integrations in the Intune environment for both visibility and effective management for security. Now, Intune administrators can view additional data from BIOS verification, Intel ME Firmware Verification, AMD PSP verification (included in the BIOS verification report) and Secured Component Verification (or SCV, a Dell component integrity check), with added capabilities coming in future DTD releases.

Dell has worked with selected software providers to further integrate Dell built-in security with their applications, providing an even higher degree of defense, control and visibility that adds to the existing 'security in layers, security in depth'. These are discussed in detail within the "Detect" section of this paper. The integration of DTD telemetry with Intune supports extensible compliance and enables organizations to use this telemetry to maintain policies they choose to apply.

* Based on Dell internal analysis, October 2025 (Intel) and March 2025 (AMD). Applicable to PCs on Intel and AMD processors. Not all features available with all PCs. Additional purchase required for some features. Intel-based PCs validated by [Principled Technologies](#), July 2025.

The Importance of Built-In "Below the OS" Security

Industry standards bodies, policy makers, and security researchers have recently started to focus on built-in, below the OS security as well. Dell has been very involved in contributing to, and building devices that adhere to, recommendations from NIST around firmware security and resilience. [NIST Special Publication SP 800-193](#) outlines overall resilience guidelines for device firmware (including BIOS) and has been helpful in confirming the value in Dell's below the OS security investments and direction.

Other NIST Special Publications that are relevant in this space include [NIST SP 800-147](#), which defines guidelines for protecting the BIOS and specifies that only signed and authorized BIOS should run on the device (see the Dell Client Signed Firmware Update whitepaper [here](#)). [NIST SP 800-88](#) provides direction for data sanitization on hard drives and solid-state drives.

It's clear that industry and customer interest for built-in, "Below the OS" and firmware/BIOS security has risen in the last few years. This awareness is incredibly valuable because it allows Dell to continue to improve these areas year over year and help protect Dell device customers from the most sophisticated adversaries.

Understanding Dell Cybersecurity Using the NIST Framework

Cyber security capabilities can be categorized according to the five functions of the NIST Cybersecurity Framework: Identify, Protect, Detect, Respond, and Recover. These provide a shared understanding and methodology for classifying technologies and identifying gaps in an organization's cyber security architecture. In the sections which follow, we'll provide details of those features and below the OS security technologies that align to these functions and explain how they work and why they are important. There are other frameworks which can be used – Dell has selected the NIST framework for its simplicity and its widespread acceptance within the cybersecurity community. More information about the NIST Cybersecurity Framework can be found here: <https://www.nist.gov/cyberframework>.

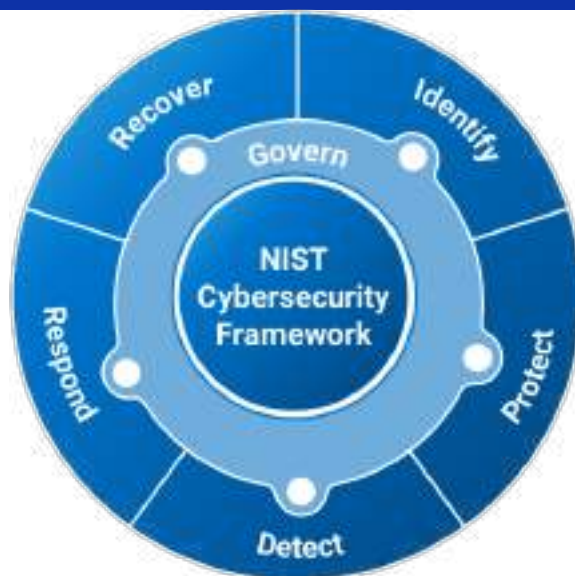


Figure 2: CSF Functions

Dell implements this framework using both Industry Standard and Dell Unique capabilities.

	Dell Unique	Industry Standard
 Identify	Dell Identity and Asset Management Tags	• Service Tag • Asset Tag
 Detect	• Discrete TPM • Dell SafeBIOS Verification • Dell SafeBIOS IoA/IoC • Dell Secured Component Verification (SCV) • Intel® ME Firmware Verification • CVE Detection	• Runtime BIOS Resilience • TCG Measured Boot • Downgrade Protection
 Respond	• Dell SafeBIOS Image Capture • Dell Trusted Device telemetry	Dell BIOS Recovery
 Protect	• Fused Root of Trust • Dell UEFI Secure Boot • BIOS Passwords	• Intel® BIOS Guard • Intel® Boot Guard • Authenticated Updates • BIOS Public Keys
 Recover	• Dell BIOS Connect • Dell Support Assist	Windows OS Recovery

Identify

From the NIST Framework: “Develop an organizational understanding to manage cybersecurity risk to systems, people, assets, data, and capabilities.”

The Dell built-in security features map directly to the Protect, Detect, and Recover/Respond functions of the NIST Cybersecurity Framework. The Identify function maps closely as well but the interaction is a bit more complex. For most enterprises, the Cybersecurity Framework is an effective tool for assessing security risk in their environments, where identifying assets and risk is a broad but valuable exercise. For Dell client devices, the Identify function has four separate and important roles:

- Includes features designed to help identify and asset-manage Dell devices within a customer infrastructure.
- Platform certificate-based machine identity which enables device health through proof of authenticity and supply chain assurance.
- Human identity secured via dedicated NIST certified biometrics and certificate-based authentication processing and storage SoC.
- Addresses processes and tools used by Dell to Identify customer security risks and threat models of the application and deployment of these devices.

Device Identity

Service & Asset Management Tags

The Dell BIOS supports two independent persistent identifiers (or “tags”) to allow customers to discover and manage their devices in their infrastructure.

- **Service Tag**

The Service Tag is programmed into the BIOS NVRAM (non-volatile random-access memory) during the manufacturing process and is locked in place for the life of the device. This allows the customer and Dell to identify the device for overall asset management in the customer enterprise and enables Dell to confirm the device information for service and warranty support. The BIOS is responsible for displaying the Service Tag in BIOS Setup and in management interfaces such as SMBIOS. The Service Tag is not changeable by the customer.

More information about the Service Tag can be found in the Dell Knowledgebase [here](#).

- **Asset Tag**

The Asset Tag is also stored into BIOS NVRAM and can be set, changed, or cleared by the end customer. The Asset Tag is displayed in text on the Dell boot splash screen on every boot and can be used for additional customer-specific tracking information, logistical messages, or unique branding. The BIOS Administrator password can be used to provide authentication and authorization controls to control Asset Tag modification.

More information about the Asset Tag can be found in the Dell Knowledgebase [here](#).

Platform Certificates for Machine Identity & Supply Chain Assurance (Secured Component Verification)

Supply chains can be vulnerable to disruptions such as tampering, theft, counterfeiting. Recent geopolitical tensions have thrust supply chain into the spotlight, causing customers to question their electronic product providers and demand visibility as to where products are developed, created, manufactured, and handled.

The US White House issued Executive Order in 2021 to strengthen the resilience of the US supply chain. Extending government action, the DoD recently released a ‘blueprint’ for the [secure procurement of devices](#), which effectively calls out platform certificates as mandatory for verifying and proving device authenticity, including the criteria for deploying an acceptance test. It provided qualified examples from NIST’s NCCoE supply chain assurance program, where Dell was one of the eight industry leaders which participated in developing examples, providing hardware and specifying solutions. Dell used its [Secured Component Verification \(SCV\)](#) solution as the foundation of [NIST Special Publication SP 1800-34](#) – Validating the Integrity of Computing Devices, which builds platform attribute certificates in the factory during manufacturing, thus aligning SCV with the DoD’s procurement guidelines.

Platform certificates create secure identities bound to the products during manufacturing which are used to seamlessly connect Dell devices to customer infrastructure or Dell services, creating a foundation from which Dell provides secure attestation methods to our supply chain for the customer. Today SCV enables dock to dock security by creating a certified manifest of device components bound to the device via TPM. The customer can validate that the device they ordered is the device Dell built and sent them. It ensures that the

device was not intercepted or changed at any point during the delivery process. Dell will continue to expand function and capabilities built into the platform certificate and the methods of attesting device hardware, components, software, and firmware to become the root-of-trust for device identity, health, and authenticity.

SCV certificates may be deployed in two ways:

- On cloud, which stores the certificate in a cloud service known as My Account (formerly Dell Digital Locker).
- On device , which stores the certificate on the device drive (HDD or SSD) within the system EFI partition

[Validation of the SCV certificate](#) upon receipt may be accomplished in several ways:

- Through [Dell Trusted Device](#) and extensible to [Microsoft Intune](#), CrowdStrike, or [SIEM](#)
- Through manual or open-source tools such as HIRS. Detailed instructions on how to use this tool can be found at <https://github.com/nsacyber/HIRS>

HBOM and SBOM

The emergence of SBOM (Software Bill of Materials) and HBOM (Hardware Bill of Materials) reflects a growing regulatory and operational need for transparency in the supply chain. SBOMs list software components used in a system, while HBOMs extend this concept to hardware, detailing the origin, manufacturer, and attributes of physical components. Both CISA's HBOM and TCG's Platform Attribute Certificate used by Dell's SCV to describe hardware composition/ Though they differ in purpose, structure, and security guarantees they are the same in providing a hardware manifest.

CISA HBOM

- Purpose: Supply chain transparency and risk management.
- Format: Extends SBOM formats (SPDX, CycloneDX) to include hardware attributes.
- Use Case: Primarily for documentation and procurement compliance.

TCG Platform Attribute Certificate

- Purpose: Cryptographic attestation of device identity and composition.
- Format: Signed certificate using Object Identifiers (OIDs) to describe component attributes (e.g., serial numbers, manufacturer, bus location)
- Security: Cryptographically signed by the manufacturer, ensuring integrity and authenticity from factory to field ("dock to dock")
- Use Case: Enables secure attestation and Zero Trust architecture

Dell's SCV platform certificate is a direct implementation of the TCG Platform Attribute Certificate. It is signed in a hardened datacenter during manufacturing and used to verify device integrity post-deployment

Credential Protection: Dell SafeID

Dell SafeID keeps user credentials safe at user and device levels and helps customers stay protected from malware attacks. This hardware-based, storage solution for credentials better protects your information by keeping it isolated and out of attackers' reach.

SafeID leverages a hardware based Trusted Platform Module, or discrete TPM, a specialized chip designed to store highly privileged information such as cryptographic keys, provide platform device authentication and protect other secrets and authorizations required for secure operation of the endpoint. The latest version, TPM 2.0, is required for devices running the Windows 11 operating system.

SafeID plays a role in multi-factor authentication, or MFA, through means of the fingerprint reader, a Personal Identity Verification (PIV) card, the camera, or a FIDO2 key on a Dell device. With Dell's Pro and Pro Max (Precision) series there is an option to add ControlVault as a part of the device's configuration. With this feature, the end user can perform Certificate-based email signing via S/MIME and smartcard sign-in to mission critical applications or workspaces. For the ITDM, a policy can be set for the device to use multiple means of authenticating into the device, an application (or workspace).

- **Isolated Processing & Storage: Dell ControlVault**

ControlVault's ARM Cortex A7 1GHz processor and storage is not only outside-validated, FIPS 140-3 Level 3 – it is a dedicated security chip, unique to Dell, providing a protective and secure boundary for credential processing and storage enabling multifactor authentication via fingerprint biometrics, smartcard & NFC modalities.

- **Support**

ControlVault works with industry leaders and standards bodies to ensure adherence to customer enterprise needs. Today it supports Windows Hello Enhanced Sign-in Security, Linux fingerprint biometrics, FIDO2 specifications and Imprivata One-Sign, Digital Persona and EntraID.

- **Certifications**

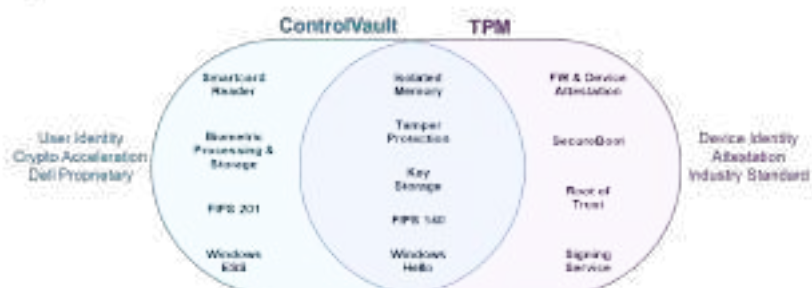
EMVco v4.3d, WQHL, NFC Forum, PCI PTS POI, FIPS 140-3 Level 3, FIPS 201-3

To learn more about Dell SafeID, read our [datasheet](#) or [blog](#).

SafeID ControlVault & TPM

Isolated security processing – the credential handshake occurs within the boundaries of a dedicated security chip, unique to Dell, providing a protective and secure boundary.

Secure credential storage – protected hardware boundary to store keys keeping them out of sight from attackers.



SafelD: TPM and Microsoft Pluton

Microsoft developed a security solution known as Pluton, intended as a security processor built into the System on Chip (SoC) that offers enhanced integrated security features in coexistence with an existing hardware TPM.

Dell will continue to include a hardware TPM in its commercial devices alongside enabling Pluton where it is available in SoC hardware. Pluton can serve as a security processor for additional OS features. Dell views this as a healthy co-exist strategy, which leverages the advantages of both TPM and Pluton for enabling OS security while also supporting discrete industry standard TPM 2.0 hardware for credential protection.

“Below the OS” Threat Modeling

Threat modelling is the exercise of using an adversarial mindset to evaluate computer architectures to determine potential vulnerabilities or attack surface early in the development phase. These exercises are critical to ensuring that any latent vulnerabilities are identified and remedied during development. Ongoing programs address client devices in-use as attackers develop new targeted threats.

Most publicly available threat modelling information is focused on software designed to be deployed as web applications or to cloud architectures. Dell uses this powerful tool not only for web and application software, but also as part of the SDL process for BIOS and firmware. Dell includes physical threats, time-based risk analysis, and persistent storage in the threat model assumptions for Dell devices. These expanded assumptions have proven to be significant improvements in finding and mitigating potential vulnerabilities in BIOS, firmware, and hardware design.

Dell includes physical threats, time-based risk analysis, and persistent storage in the threat model assumptions.

Just as hardware and software threat models differ, so do Dell customers' threat models. For example, not every customer includes “Below the OS” threats in their own threat models, but a growing number do. Using the most security-sensitive customers' threat models as a baseline for our own allows Dell to design devices that are resilient against the most sophisticated adversaries in addition to the more common threats. Penetration testing, or ‘pen-testing’, is a form of product validation where authorized attacks are performed for internal evaluation. This has become synonymous with mature security practices across the industry. Dell leverages both in-house teams and external vendors to pen-test Dell devices while these products are still in the engineering phases of development. Like the threat model assumptions made above, these tests focus on physical access and are prioritized based on risk assessments of individual components integrated into Dell devices.

Protect

From the NIST Framework: “Develop and implement appropriate safeguards to ensure delivery of critical services.”

Dell Trusted Device Below the OS White Paper

The Protect stage of the NIST framework has been an area of significant investment for Dell over the last decade. All the context described in the previous 'Identify' section with respect to portfolio details, threat models, and security research has been pulled into the overall direction, strategy, and architecture for protecting the lowest levels of code in Dell devices. These features are truly the “first line of defense” for modern PCs against sophisticated adversaries.

Protecting the PC Boot Process

In theory, bootstrapping a modern personal computer may seem relatively simple. Pull the processor out of reset or low-power sleep state, initialize memory and motherboard hardware devices, enumerate storage, and find a bootloader to load the customer's operating system of choice. Simple, right? In practice there is much more to it than that, and much of the complexity and additional features in the pre-boot timeframe is there to help protect the PC from executing unauthorized code. Ultimately, the BIOS boot process provides a safe foundation for the operating system and user applications.

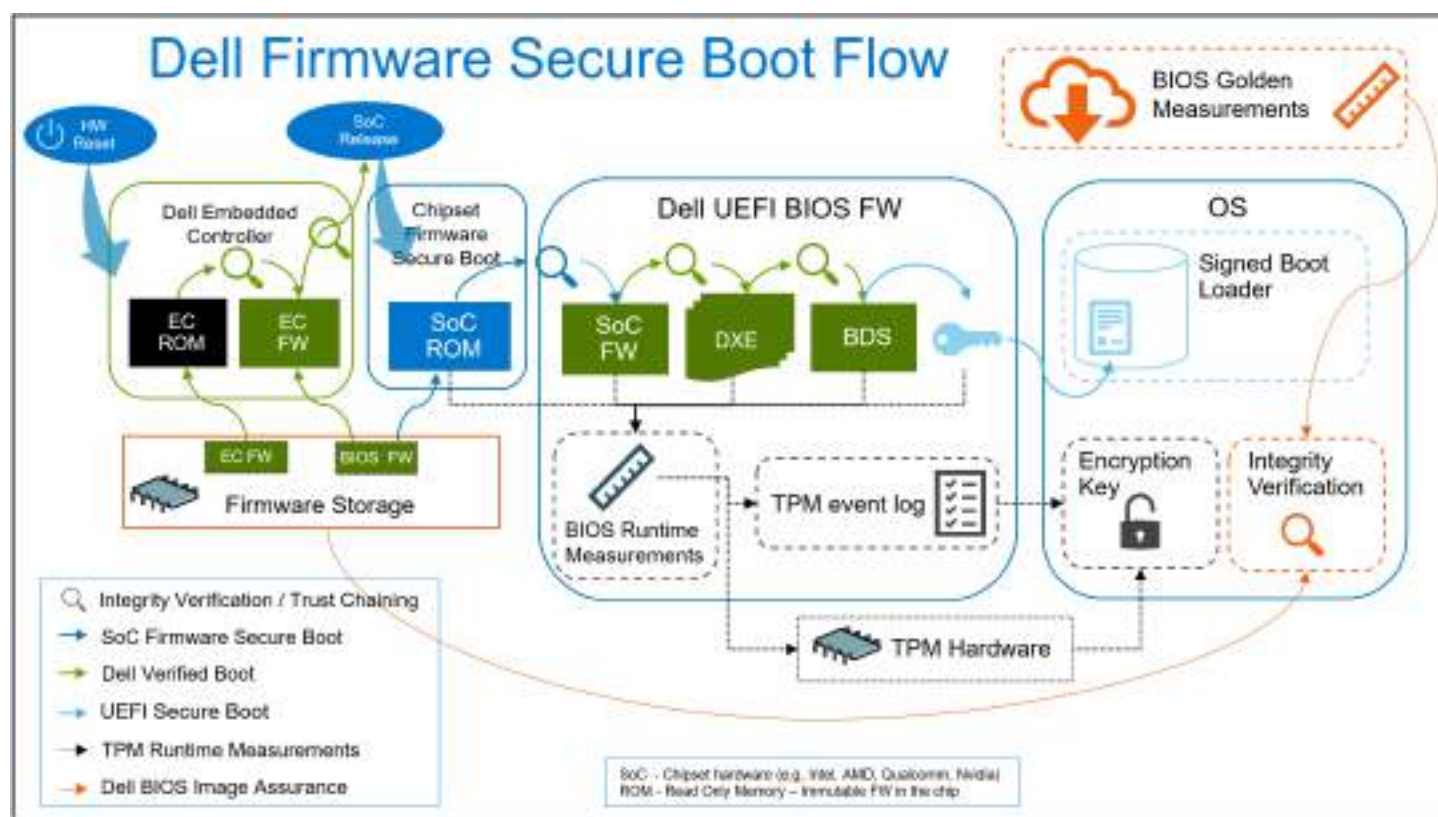


Figure 3: Dell Trusted Device Boot Chain

Securing the Boot Chain

The PC boot process is a series of configuration steps, events, and procedures that combine to create a tightly linked chain, from the point of time when the Embedded Controller (EC) and/or main processor come out of reset, to the point of handoff to an operating system like Microsoft Windows™, Linux, or Canonical Ubuntu™. Links in this chain protect the boot process by cryptographically verifying each subsequent link using either hashes or digital signatures. 'Golden' or reference hashes are protected by encoding them into an already verified section of code and digital signatures use public keys embedded in the firmware for verification.

The illustration in Figure 3 depicts a high-level overview of the major components in the Dell device boot chain. Many of these components, like the Embedded Controller, will be covered in more depth in other sections of this document and this illustration should serve as a helpful reference in understanding how everything ties together.

Like the roots of a tree, the root of trust is the origin point upon which all subsequent trusted events are built. For modern PC's, the processor reset vector is often considered the root of trust.

The "Root of Trust"

Like the roots of a tree, the root-of-trust serves as the foundational starting point for all subsequent trusted operations in a modern PC. Typically, this begins with the processor reset vector—the very first instruction the processor executes after coming out of reset.

In practice it's a bit more complicated than that. Dell devices support multiple roots-of-trust, including both an Embedded Controller and a chipset SoC (System-on-a-chip) security processor, such as Intel's Converged Security and Management Engine (CSME), and AMD's Security Processor (ASP) that executes verified boot firmware prior to releasing the chipset and executing BIOS firmware. The EC acts as Dell's primary hardware root-of-trust, running cryptographically verified code to manage the power controls which bring the chipset out of its low-power state. The boot flow begins with the EC verifying its own firmware and the integrity of the SoC chipset firmware

before releasing the chipset. Once released, the SoC chipset continues the boot chain by verifying the integrity of the BIOS firmware, ensuring that only trusted code is executed as the platform boots.

TCG and the Root of Trust

The Trusted Computing Group (TCG) provides definitions and specifications for developing secure products. The TCG glossary defines a root of trust as "A component that performs one or more security specific functions, such as measurement, storage, reporting, verification, and/or update. It is trusted always to behave in the expected manner because its misbehavior cannot be detected (such as by measurement) under normal operation." TCG specifications build on this to define several roots of trust that describe how the BIOS and Trusted Platform Module (TPM) must coordinate during the boot process to maintain authenticity of BIOS measurements; most importantly a Root of Trust for Measurement (RTM) and a Root of Trust for Reporting (RTR).

The Detect section of this document will cover the TCG Measured Boot feature in much more depth but first let's clarify a few words in the context of the boot process and root of trust. TCG Measured Boot uses the PC's

TPM as a protected area for storing hashes of BIOS and firmware code that is loaded and executed in the boot process. The TPM is designed to store these events in a secure way that can be verified post-boot through a process called attestation. Both Windows and Linux include TPM software stacks that support measured boot attestation.

All Dell commercial PCs use a dedicated TPM chip, as described in the SafeID section of this paper.

UEFI Secure Boot

One of the most powerful improvements in the last decade for protecting the pre-boot process from executing unauthorized code is UEFI Secure Boot. Unfortunately, there is some confusion in the industry about the benefits and scope of UEFI Secure Boot since the feature name tends to be conflated with the more general “secure boot” concept of executing signed pre-boot code. To avoid this confusion, this document will use the term “verified boot” when referring to executing cryptographically signed code in the pre-boot context when it is outside of the scope of UEFI Secure Boot.

That clarification is not intended to diminish the value of UEFI Secure Boot at all - it's an effective feature for mitigating threats and exploits that may be delivered via unsigned bootloaders, UEFI shells, or UEFI drivers on add-in devices. To protect against these threats, Dell provisions trusted default certificates into the UEFI Secure Boot databases to allow Dell to manage the UEFI authenticated variables that protect the allowed database – the “db” – and the disallowed database “dbx”. Default provisioning also enforces verification of Windows 10/Windows 11 bootloaders and signed shims for Linux using trusted certificates from Microsoft. Also included by default is a Microsoft Key Exchange Key or “kek” to allow Microsoft-signed db and dbx updates from Windows.

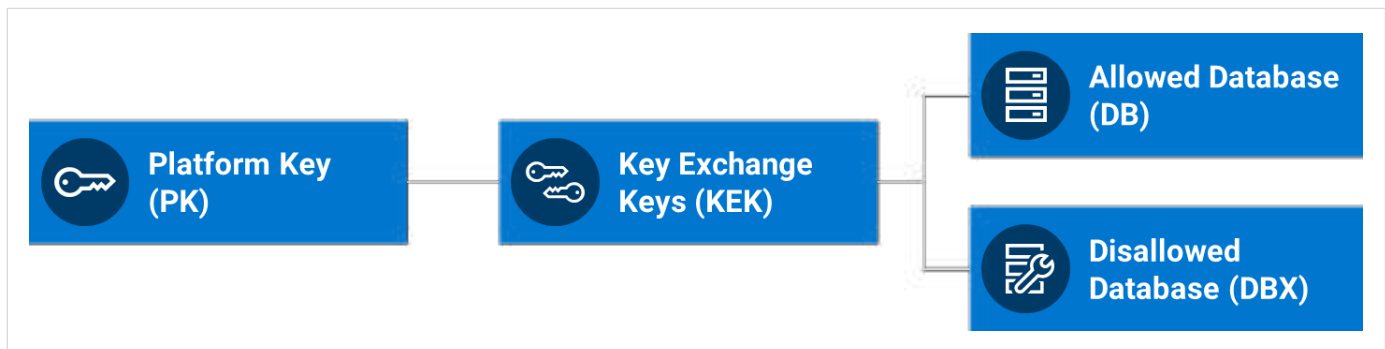


Figure 5: Secure Boot Key Hierarchy

UEFI Secure Boot Expert Key Management

Depending on customer and enterprise threat models, some administrators may want to restrict UEFI Secure Boot to only allow specific bootloaders and/or UEFI drivers. To support this, the Dell BIOS Setup interface supports Custom Mode Key Management settings that allows administrators to modify the contents of the UEFI Secure Boot key management databases through interfaces such as Microsoft’s PowerShell. This privileged operation is available with local physical access only and will temporarily disable UEFI Secure Boot while the certificate databases are being repopulated with custom keys supplied by the administrator. Key databases can also be reset back to the factory default values (including reinstallation of the original Dell PK) by using this interface.

The US DoD issued “[UEFI Secure Boot Customization](#)”, a Cybersecurity Technical Report, in September 2020. The document provides a comprehensive guide for customizing a Secure Boot policy to meet several use cases. Customization enables administrators to realize the benefits of boot malware defenses, insider threat mitigations, and data-at-rest protections, while overcoming incompatibility with hardware and software.

Signed Firmware Update

Previous sections detailed how the Dell BIOS protects itself from running unauthorized code during the boot process, but how does it ensure that code cannot be tampered with or replaced on the motherboard BIOS flash storage device (e.g. the Serial Peripheral Interface, or SPI flash storage device) in between boots and during updates? Guidelines for protecting the BIOS against these threats were published by NIST in 2011 as Special Publication 800-147. This NIST document describes requirements for cryptographic authentication of BIOS updates, integrity protection of currently running BIOS, as well as guidelines to prevent bypass which further harden the BIOS against unauthorized modification via “backdoors”. Dell devices implemented these

requirements in 2011 and a full whitepaper describing the support is linked in the References section of this document.

NIST SP800-147 Support

Dell puts significant effort into hardening the BIOS protection and authentication capabilities on its client devices in accordance with [NIST SP800-147](#) to support Dell's customers.

BIOS running on a device that supports Signed Firmware Update contains information in its Root of Trust for Update (RTU) that supports a cryptographically hardened verification mechanism which allows only approved BIOS update utilities to modify the BIOS code in storage:

- **BIOS Update Authentication**

All BIOS update images are signed using the RSA PKCS #1 v1.5/v2.1 algorithm with RSA 2048-bit keys as per [FIPS Publication 186-5 Digital Signature Standard \(DSS\)](#). The SHA-256 algorithm was selected to hash the payload in the signing and integrity verification process based on this algorithm's acceptance in NIST Special Publication 800-131A. Update images are verified by the BIOS using the public key contained in the RTU before the BIOS or other firmware currently running on the device is modified.

- **Integrity Verification**

The RTU and BIOS are protected from unauthorized modification using Dell proprietary flash write cycle trapping and locking mechanisms supported by the device hardware. All programmatic code update attempts that are not approved by the RTU verification mechanisms and any attempts to update BIOS data not approved by the BIOS storage handler are blocked from accessing the device flash memory using flash disable mechanisms.

- **Non-Bypassability**

The Signed Firmware Update mechanism in the RTU that enforces authenticated updates is the exclusive mechanism for modifying the BIOS. This enforcement cannot be bypassed by any firmware or software running on the device that is not controlled by the RTU.

System Management Mode (SMM) For x86 Systems

System Management Mode, or SMM, is a privileged mode of the processor architectures for x86 devices to support handling of high-availability, manufacturer-specific tasks independent of the operating system. Think of SMM as a component of the BIOS that remains resident underneath the operating system (reference the "ring" architecture where ring 3 refers to user mode code, ring 0 is the root, supervisory, or kernel mode of the operating system, and "ring -2" is applied to SMM to highlight the additional privileges that it is allowed over the device). Dell uses SMM to support persistent storage (e.g., UEFI variables), BIOS configuration interfaces, thermal handling, and other critical-priority events.



Figure 6: Modern PC Ring Architecture

SMM has been the target of dozens of disclosed vulnerabilities, security conference presentations, and media reports over the years. This has been welcomed attention from a security perspective because it provides helpful insights for SMM threat modeling and security improvements. For example, even though Dell BIOS uses SMM for system management activities, there has been significant investment in hardening the SMM environment and overall reduction in reliance on SMM. Additionally, Dell has integrated several technological advancements to incrementally deprive the SMM code that must be present on the system and mitigate potential impact to other parts of the operating system.

- **Threat: SMM Over-Reliance for BIOS Locking and Signed Update Verification**

The Signed Firmware Update whitepaper released in 2013 is still applicable and relevant to all Dell devices today. It's the baseline for protecting the BIOS from tampering or other unauthorized modification. While the NIST 800-147 specification requires non-bypassability in operation, it does not necessarily consider vulnerabilities that may exist in the code that enforces non-bypassability. In many implementations System Management Mode, or SMM, is the entity that enforces BIOS locking and signed update verification.

- **Mitigation: Intel BIOS Guard**

For Intel x86 equipped PCs, Dell decided to mitigate this reliance on SMM by moving the authority to unlock and update BIOS from SMM to device hardware. Dell devices have implemented Intel BIOS Guard since 2015, which explicitly verifies all BIOS code region writes using public keys fused into the Intel Platform Controller Hub (or PCH). Since the PCH operates between the processor and the flash storage where the BIOS is located, logic within the PCH can block all writes to the BIOS code region before flashing. Intel® BIOS Guard integration required considerable resources and infrastructure to implement, and because of this, was only adopted by a few OEMs. Dell considers this feature a must-have in the current below the OS threat landscape.

- **Threat: SMM Access to Hypervisor Memory**

One high-profile threat highlighted by security researchers is the potential for a rogue or malicious SMM handler or code to use SMM privilege to arbitrarily read and write to main memory. Turning this threat from theoretical to practical requires exploiting an unknown or unpatched vulnerability in SMM itself to gain code execution. As a demonstration of potential impact, researchers created proof of concept code that would interact with hypervisor memory and context that was designed to isolate and protect user applications. The end goal for an adversary with this level of access and sophistication could be credential or data theft from applications that were presumed secure.

- **Mitigation: Windows SMM Security Mitigations Table (WSMT)**

The Windows SMM Security Mitigations Table (WSMT) enumerates various methods that BIOS vendors can implement to mitigate SMM threats. Since some of the mitigations in WSMT can cause compatibility issues with legacy systems management software, Dell devices support a WSMT option in BIOS Setup to allow the administrator to enable or disable these mitigations. Once enabled, WSMT mitigations provide strict boundaries for memory access from SMM, e.g. the BIOS SMM handler can only use specific pre-allocated memory address ranges to communicate with system management software. The WSMT structure published by the BIOS provides affirmation to the operating system that the Dell device has implemented and enabled these features.

- **Mitigation: Memory Attribute Table and No Execute (MAT/NX)**

Protecting operating system memory from modification by SMM is just one piece of the runtime defense puzzle. UEFI Runtime Services are supported by BIOS and run within the OS context. To isolate these services, the BIOS implements the `EFI_MEMORY_ATTRIBUTES_TABLE`, which describes runtime memory organization for the operating system's consumption. This allows the OS to accurately configure page tables to block code execution from EFI data areas and prevent code areas from being overwritten from other potentially malicious code. These may seem like fundamental security features from an OS perspective but the handoff between pre-boot and operating system requires specific coordination to ensure these protections are accurate and do not introduce compatibility issues.

...the handoff between pre-boot and operating system requires specific coordination to ensure these protections are accurate and do not introduce compatibility issues.

Trusted Firmware for ARM Systems – Secure Partition Manager (SPM)

For ARM-based Architecture(s) for Qualcomm and NVIDIA-based PCs, the Secure Partition Manager, or SPM, would be applied by Trusted Firmware.

Privilege Elevation Comparison: SMI vs. Secure World

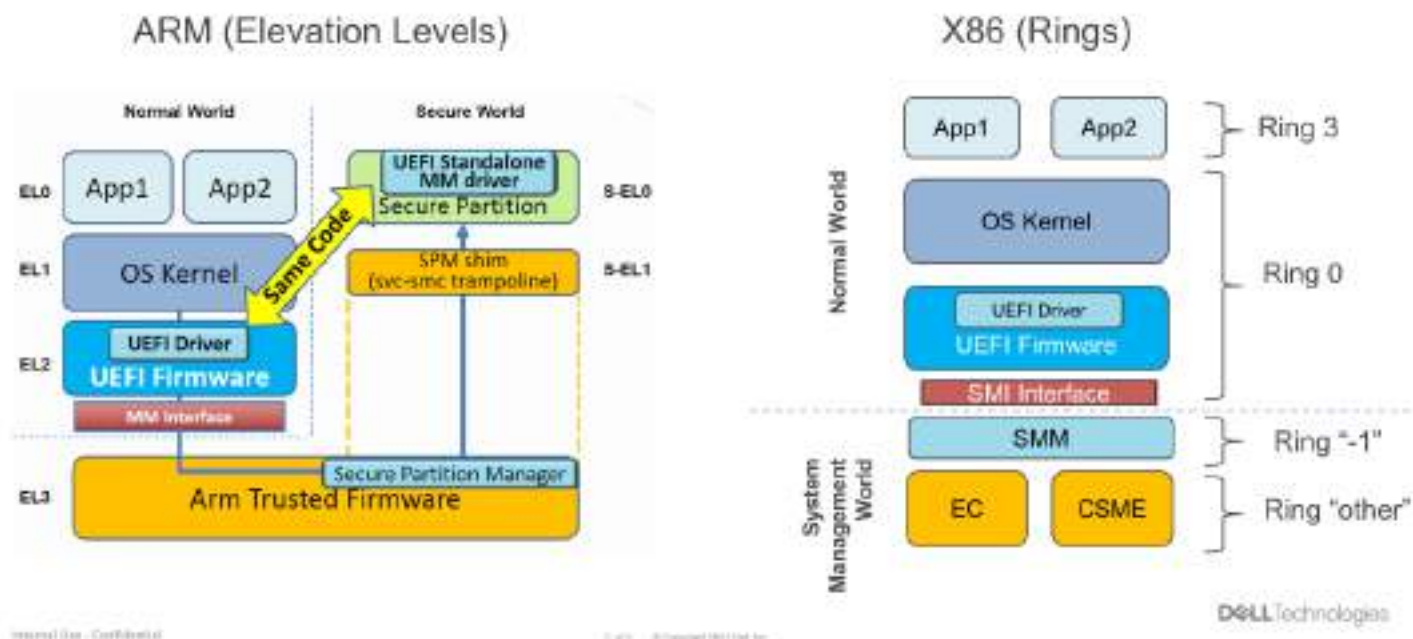


Figure 7: Privilege Elevation Comparison

BIOS Patch Management

Best practices in enterprise security should always include a comprehensive software patch management strategy to ensure that any software updates to mitigate vulnerabilities are deployed as soon as they are available. BIOS upgrades are often overlooked or delayed in the overall patch management strategy, but that's rapidly changing as customer awareness for built-in "Below the OS" security continues to increase. To support this overall initiative, Dell device BIOS updates are posted to both Windows Update (or WU) for Windows 11 systems, and to the Linux Vendor Firmware Service (or LVFS) for Linux systems. This allows seamless integration of BIOS updates into the OS ecosystem without the need for separate BIOS update utilities.

BIOS updates are also provided as a part of the [Dell Trusted Update Experience \(DTUE\)](#), designed to help organizations more easily manage updates to keep devices at optimal operation and security. Of course, updating the BIOS using the Dell BIOS update utility is still supported.

BIOS Downgrade Protection

Sometimes adversaries will attempt to revert or 'rollback' software/firmware to a known vulnerable previous version as an initial step in their attack. A Dell commercial device with SafeBIOS can be configured in the BIOS setup program or remotely using the Dell Command Tool Suite to prevent BIOS reversions, thus mitigating this threat. By default, the Enable BIOS Downgrade BIOS setup option is turned on to support full flexibility for customers to choose the BIOS image appropriate for their infrastructure. However, once this setting is disabled (locally or remotely) only newer BIOS versions will be allowed to flash onto the device and physical presence (i.e. a user in front of the keyboard) is required to revert the setting.

Embedded Controller: Signed Firmware

The embedded controller, or EC, is included on all Dell commercial device notebooks and most modern commercial desktops and workstations. As explained in the section on root of trust, the EC is responsible for low level hardware interface functions such as power and reset management. Dell devices protect the EC firmware updates at two layers while performing firmware updates. First, the BIOS verifies the EC firmware signature prior to sending the update to the EC and blocks any unauthorized direct access to the EC firmware at runtime. Second, the EC update payload is subsequently verified by the EC firmware using public keys embedded in the EC context, independent of the BIOS. Modern Dell devices include cryptographic acceleration and verification capabilities integrated directly into the EC. These capabilities include verified boot support that will block any EC execution of unsigned firmware even if it was programmed onto the device via an unauthorized side-channel, such as direct physical access. This is a good example of the benefits of including physical access into the Dell device threat model and helps to protect this critical root of trust from tampering.

Protecting BIOS Configuration

Security research and media coverage of "Below the OS" threats focus largely on firmware tampering and/or escalation of privilege, but the configuration of the client device can also be a potential threat surface. Attackers may use BIOS configuration settings to attempt to manipulate or reconfigure the device into a state that may be at higher risk for exploitation depending on the environment. Dell devices are shipped in a "secure by default" state and customers can protect this state from unauthorized access or modification by enabling a few important features.

Option	Description
Admin Password	Allows you to set, change, or delete the administrator (admin) password. The entries to set password are: • Enter the old password: • Enter the new password: • Confirm new password: Click OK once you set the password



NOTE: For the first time login, “Enter the old password:” field is marked to “Not set”. The password must be set for the first time you login and then you can change or delete the password

Figure 8: BIOS Password Reset

The BIOS Admin Password is the Dell device authorization mechanism for protecting BIOS configuration (such as BIOS settings) and the ability to upgrade or downgrade the BIOS. From a protection perspective, Dell recommends that all customers set a complex BIOS Admin Password to minimize the risk of unauthorized BIOS configuration modifications. The BIOS Admin Password can be set locally through BIOS Setup or remotely using the Dell Command Tool Suite. More information is available in individual device owner’s manuals and administrator guides.

- **Local vs. Remote Configuration**

The BIOS Admin Password protects against local and remote modification of BIOS settings that could be used by adversaries to open an attack surface on the device. Dell devices go one step further to classify specific security settings that are only available with local physical presence (i.e. a user in front of the keyboard) using BIOS Setup. These settings are locked from remote access even if the BIOS Admin Password is supplied through the remote interface. An example list appears in Table 1 below (not exhaustive):

BIOS Configuration Option	Local Access	Remote Access
Secure Boot	Yes	No
Allow BIOS Downgrade	Yes	No
Master Password Lockout	Yes	No
TPM Clear	Yes	No

Table 1: Example Local-only BIOS Options

- **Dell Master Password**

The Dell Master Password is a lesser-known feature of the Dell commercial client device. The Master Password feature is available for commercial device customers who may have forgotten or misplaced the BIOS Administrator Password on their device or fleet of devices. The Dell Master Password uses a shared secret algorithm (i.e. the BIOS and the unlock tool share a common secret) integrated into the BIOS or EC to allow Dell Customer Support to offer a device-specific unlock password only for customers that contact technical support and can provide proof of ownership of the device. Once provided by customer service, the master password must be typed into the device locally to unlock the system, as it cannot be used over any remote BIOS interface. The Master Password feature can also be disabled through a Lockout feature, for situations where the threat profile warrants it.

To the security practitioner, this feature may seem a bit antiquated, especially in a largely connected world running on a firm base of public key cryptography. Dell Customer Support must cover a varied commercial customer base across the world with a large set of challenges, not the least of which are language

Dell Trusted Device Below the OS White Paper

barriers, connectivity issues, and infrastructure availability. These requirements and overall customer scale combine to drive the need for this somewhat low-tech solution that can be exercised even when network-based remediation is not available.

- **Threat: Online Password Generators**

Dell is aware of several unauthorized online password generators that claim to generate Dell Master Passwords for devices. These generators include algorithms that duplicate the shared secret algorithm that is integrated into the BIOS and can often generate valid passwords for older devices. To combat this activity, Dell has redesigned the Master Password feature using modern cryptographic capabilities and best practices. For example, on newer devices this threat is mitigated by using secure encrypted storage when supported by the Dell commercial device, with broader portfolio coverage increasing year over year.

- **Mitigation: Master Password Lockout**

Certain customers may include targeted attacks against BIOS configuration with direct physical access in their threat model. A successful exploit within this threat model would require an adversary to discover a specific device identification information code and then have direct physical access to BIOS Setup to input the master password without being detected. This is a perfectly valid threat model, especially with today's prevalence of mobile systems. In these cases, Dell recommends enabling the Master Password Lockout feature to completely disable the Dell generated master password. Customers that enable this feature must employ their own independent password management processes since Dell Customer Support can no longer help with misplaced passwords for systems configured in this mode.

Configuration Side-Channels

Investments in protecting the configuration of the Dell device extend beyond interface and feature definitions. Protecting against “side-channels” or attempts to attack the implementation outside the bounds of the intended usage is also part of the Dell device threat model.

- **Threat: Physical Access**

As discussed, direct physical access to a Dell device is a part of the threat model of many customers, but more importantly, it's an assumption that the Dell security teams make during the secure development process. In other words, Dell uses this highest risk profile to promote the broadest resilience capability of the Dell device. Physical access from the device perspective includes not only access to the local keyboard and display, but also potentially to the motherboard in an extended ‘evil maid’ class of attack. Adversaries may attempt to tamper with BIOS configuration settings by directly accessing the storage on the motherboard.

- **Mitigation: Encrypted Storage**

To protect against this level of physical access, Dell has incrementally moved BIOS configuration settings that control security policy to encrypted storage within the embedded controller (the EC). The EC includes root keys and cryptographic accelerators to provide resilience against direct physical attacks directed at the EC non-volatile storage. As an additional layer of security, these variables are encrypted with a device specific encryption key to protect against “break once” types of attack scenarios and further reduce the value of this type of attack.

Best Practices for Secure Configuration

BIOS configurations can be managed at scale in the enterprise with the Dell Client Command Suite. Customers interested in securely configuring their systems using the most restrictive policies can consult the [National Security Agency Cybersecurity Report UEFI Defensive Practices Guidance document](#) for overall recommendations. Please see the Dell Client Command Suite tool documentation to deploy and manage policies aligned to these guidelines.

Protecting BIOS at Runtime

A common misconception in the PC industry is that the BIOS is completely out of the picture once the bootloader and kernel take over execution of the boot process at the point in time where the BIOS hands control over to an operating system which has called the UEFI runtime service `ExitBootServices()`. Of course, this is not the case and even the “Basic Input/Output System” acronym is a reference to this role. A small subset of the BIOS code must persist while the operating system is running to support system management interfaces, UEFI interfaces, and overall system health components like event logging, as well as OEM hardware-specific functionality for power/thermal management.

- **UEFI Runtime Services**

The Dell BIOS allocates and assigns main memory during the boot process as `EFI_MEMORY_RUNTIME` to support specific UEFI services needed by the operating system. These services allow the OS to invoke capsule updates to update BIOS and/or device firmware, set general purpose UEFI variables, and manage the authenticated variables used for Secure Boot configuration. Most of these services are defined by standards (such as UEFI) but may include customization specific to Dell hardware and enhanced security features.

Runtime BIOS Resilience (Intel Only)

Intel has been another valuable ally in the Dell device security story providing foundational security technologies in processors and chipsets, also extending trusted computing concepts into new architectural areas of Dell devices. One example of this partnership is Runtime BIOS Resilience, which is part of the Intel Hardware Shield group of security features.

Runtime BIOS resilience builds another layer of security within the BIOS by hardening the SMM environment against attacks and protecting the operating system (and ultimately user code and data) from tampering by SMM. The Dell device sets up runtime BIOS resilience early in the boot process by enabling memory paging in SMM and configuring the SMM page tables to only allow access to the memory pages specifically allocated to SMM (in an area of memory called TSEG). This brings architectural capabilities of the processor that have been best practice for operating system memory safety into the realm of BIOS and SMM. These protections help prevent malicious code injection and redirection in the valuable SMM execution environment as well as ensure SMM code cannot affect the operating system (regardless of whether the code is legitimate or potentially rogue).

For more information about other Intel vPro capabilities, visit:

<https://www.intel.com/content/www/us/en/architecture-and-technology/vpro/what-is-vpro.html>.

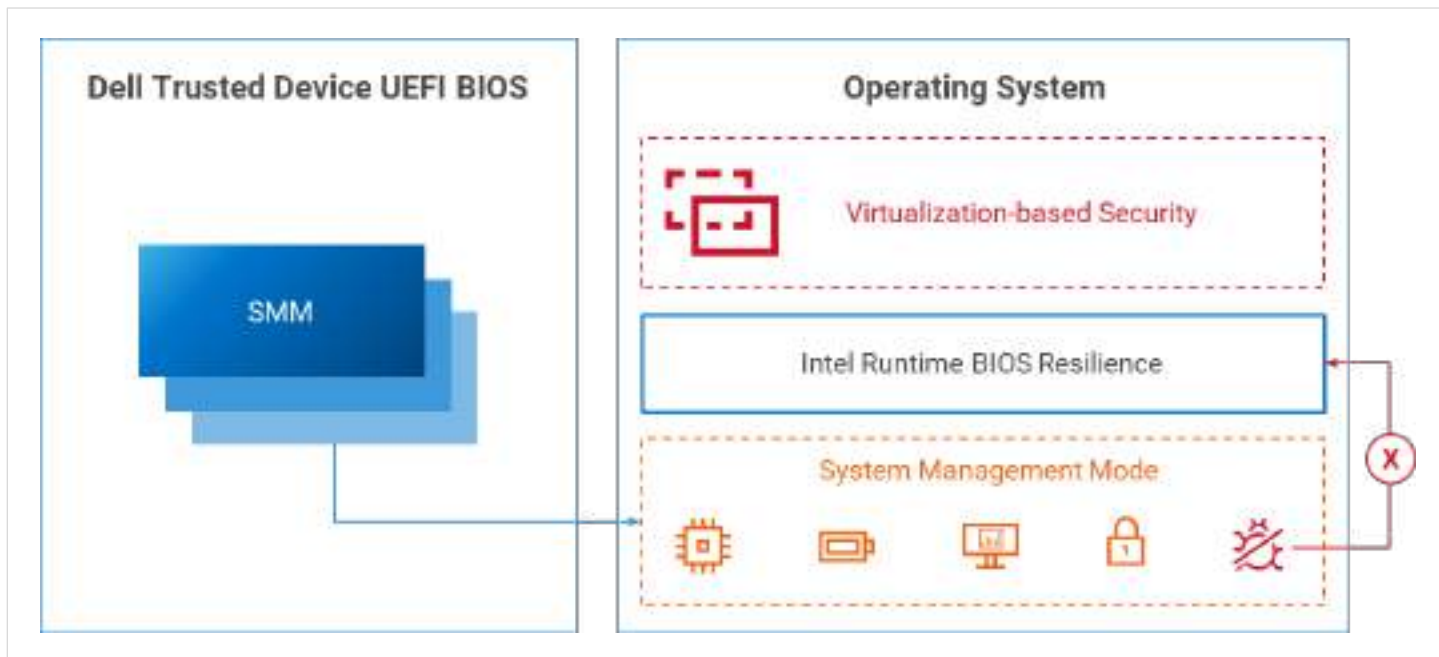


Figure 9: Intel Runtime BIOS Resilience

Runtime BIOS Resilience (AMD Only)

AMD-based Dell devices implement runtime BIOS resilience by embedding protections below the operating system that continuously monitor, detect, and recover the BIOS against unauthorized changes. Dell leverages NIST SP 800-193 Platform Firmware Resiliency guidelines and AMD security features to ensure that the BIOS can self-heal during runtime, preventing persistent compromise. These AMD features include:

- **AMD Secure Processor (ASP):** A dedicated, integrated security co-processor that establishes a hardware root of trust during the boot process, which helps ensure system integrity from boot to runtime.
- **AMD Memory Guard:** Enables comprehensive, full system memory encryption to protect data in the event of physical access to the machine.
- **AMD Shadow Stack:** A hardware-based security feature that helps prevent malware from redirecting the flow of commands, a common exploit technique.

These features are integrated within the Dell BIOS resilience framework to strengthen runtime protections and help mitigate vulnerabilities.

Detect

From the NIST Framework: Develop and implement appropriate activities to identify the occurrence of a cybersecurity event.

Even a 100% effective protection strategy both above and below the OS may not be enough to thwart the most sophisticated adversaries. Adversaries with this skill level and incentive can move and evolve quickly. Thus, having built-in (not bolted on) detection mechanisms help fill the gap between prevention and response and can provide much needed visibility into new adversarial techniques targeting client PCs.

In line with the expressed goal of 'transparency', Dell provides both hardware and firmware-based checks and detections which enable the customer to know when a device is compromised. These fall into two broad categories:

- Physical security detections and protections, and
- Built-in 'below-the OS' detection capabilities.

Dell Physical Security Features

Keeping PCs secure requires addressing all potential attack vectors. One important aspect is the physical security of the PC. This area of security aims to detect, alert and ultimately prevent an attacker from gaining physical access to the system, including its data and the credentials and secrets that it stores.

Dell provides physical security for its PCs in several ways:

- **Detecting when the chassis is opened and/or the battery is removed** and allowing the IT manager to decide what actions to take (from stopping boot to alerting via DTD to securely recording and reporting the event to wiping the TPM).
- **Inhibiting exploits which may connect directly to key parts of the circuitry**, providing highly privileged access to BIOS (SPI Tamper).
- **Protecting key credentials** – such as smart card and fingerprint reader – with hardware-based security that's equal to or better than provided by the TPM (with Dell ControlVault, which is unique to Dell and a part of SafeID).

Key components of each of the physical security features are described in the following paragraphs.

Physical Security – Chassis Intrusion

Dell commercial devices – including Dell Pro and Dell Pro Max systems (fixed and mobile) - include chassis intrusion detection circuitry and logging capability that can be monitored via Microsoft Intune/SCCM, Dell Client Command Suite, and other common systems management platforms. Chassis intrusion combines with other built-in, below the OS security features to strengthen the Dell device defense in depth layered strategy. Complementary features already implement layers of security for defending below the operating system, such as protecting against and detecting tampering, but it's important to also support early detection as soon as the chassis has been opened, which is typically the first sign of a physical attack.

Ability to Block Boot after Chassis Intrusion

An optional BIOS setting prevents system boot when chassis intrusion is detected. This new option, called "Block Boot Until Cleared", will prevent the system from booting when a chassis intrusion event is detected. This option is only available when Chassis Intrusion is set to "Enabled". When the POST message is displayed,

the only option will be to enter setup, where a user can use the “Clear IntrusionWarning” checkbox to acknowledge the intrusion event.

TPM integration for Chassis Intrusion events

When chassis intrusion is detected, an event is recorded in the TPM event log and extended to TPM PCR1. This can be used to protect TPM-sealed keys, such as Microsoft Windows Bitlocker encryption keys, preventing Bitlocker decryption of the hard drive when a chassis intrusion event is detected. The BIOS will record an EV_ACTION event with string “Chassis Intrusion” to the crypto agile log. The event digest will be a hash of the event string and extended to PCR1. When the chassis intrusion warning is cleared, the EV_ACTION event will not be recorded.

Optionally, a BIOS setting can be enabled to completely wipe TPM if a chassis intrusion is detected.

Battery Removal Detection

Removing the battery from a system results in an event being logged in the BIOS event log. To supplement Chassis Intrusion detection events, this new battery removal event can be used by security analysts to detect potential system tampering. When a battery is removed or replaced, this event will appear in the log on the subsequent normal boot: “Alert! Battery previously removed.”

SPI Flash Anti-Tamper features

Dell Commercial Devices also include new technology which detects and prevents tampering with BIOS SPI flash chips on the motherboard. While the system is powered on, the Dell Embedded Controller (EC) monitors electrical signals controlling the BIOS SPI Flash storage chip. If BIOS SPI flash chip tampering is detected by the EC, an event is logged in the BIOS event log, and a warning may optionally be displayed. When the system is powered off, the Dell Embedded Controller will shunt the electrical signals, such that BIOS SPI flash data cannot be accessed with an offline flash programming “chip clip”.

Dell Built-In “Below the OS” Detection Capabilities

Dell’s “below the OS” detection capabilities are designed to detect tampering, malware or unauthorized changes at the firmware level, before the OS loads. This helps to protect against advanced threats like rootkits and BIOS-level attacks. This extra layer of defense against firmware-level attacks is particularly valuable in enterprise environments where these threats could bypass traditional antivirus or OS-level defenses. Through the DTD App, data from these detections and defenses can be shared with EDR/XDR solutions, SIEMs and management solutions like Intune.

Dell off-Host BIOS and Firmware Verification

Dell’s off-host BIOS verification and firmware verification is a SafeBIOS capability that verifies the integrity of the system BIOS (and, on supported platforms, Intel vPro ME/CSME firmware and AMD PSP firmware) against a known good reference stored in Dell’s cloud, instead of trusting only what’s stored on the endpoint itself.

Unlike pure “self-healing BIOS” designs that only compare to a local backup image, Dell’s approach validates against external, OEM controlled reference measurements and exposes that telemetry outward, which is what makes it “off host”.

At a high level, the workflow involves three main components:

Dell Trusted Device Below the OS White Paper

- **Endpoint firmware and BIOS:** Dell commercial PC with a signed, NIST 800 193–aligned BIOS and platform firmware stack.
- **On-host telemetry and agent:**
 - o Dell Trusted Device (DTD) Application or Dell Client Device Manager Security module installed in the OS.
 - o This module reads BIOS/firmware measurements and sends telemetry/verification results.
- **Off-host verification backend:**
 - o The Dell secure cloud that stores known-good BIOS images and firmware measurements per platform and version/SKU.
 - o It maintains cryptographic reference hashes and metadata, along with approved Intel ME/CSME firmware builds and AMD PSP firmware builds for relevant platforms.
 - o Verification logic that compares endpoint measurements and returns pass/fail, plus events for SIEM/management tools (Intune, CrowdStrike Falcon, TechDirect, etc.).

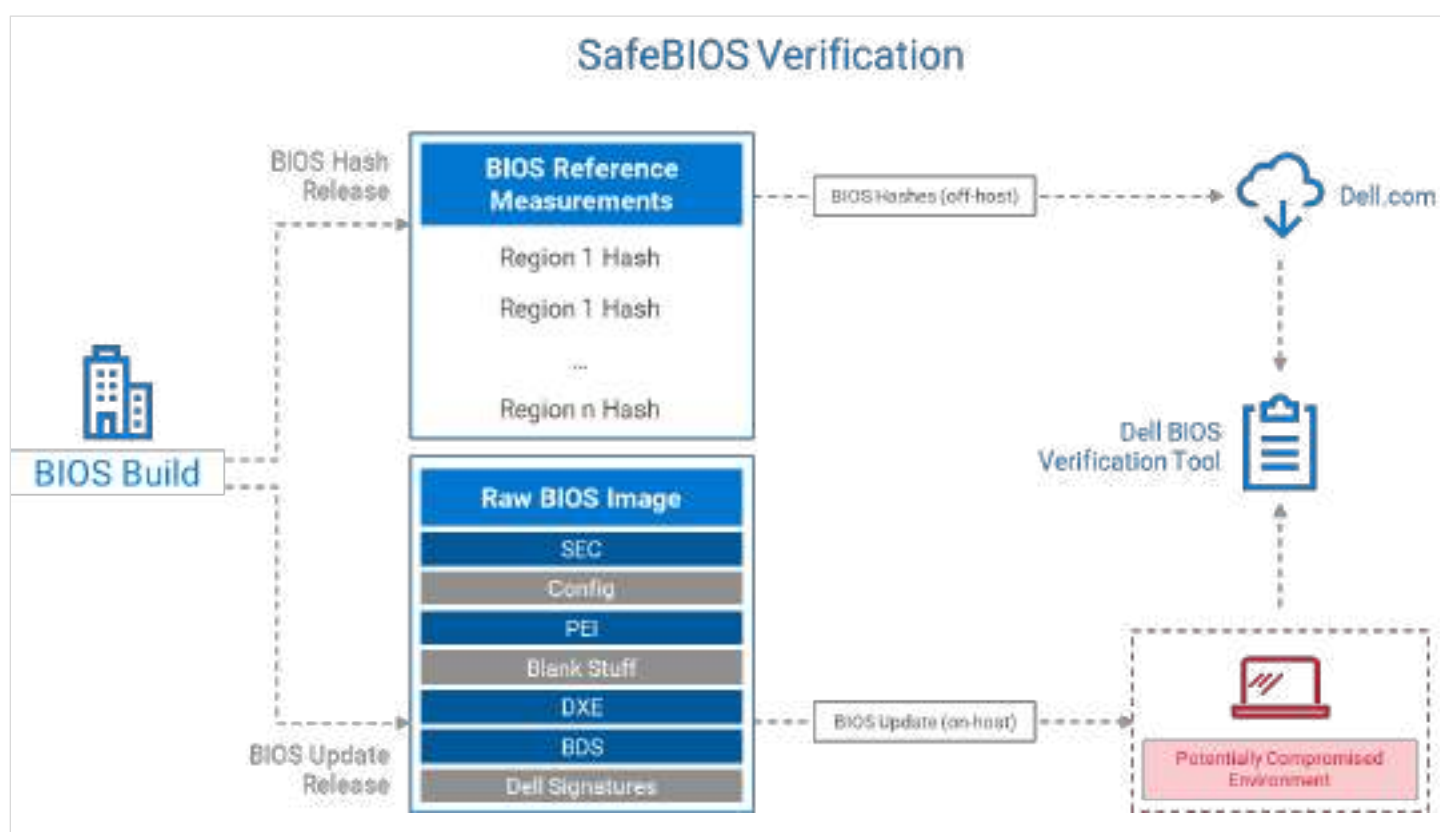


Figure 10: SafeBIOS Verification Flow

Dell BIOS verification now utilizes SHA-512 verification algorithms that are resistant to quantum computing hacks, providing an increased level of protection for the off-host process. More information can be found [here](#).

Indicators of Attack

Dell SafeBIOS Indicators of Attack (IoA) extends tamper detection capabilities beyond the code into the BIOS configuration arena. Various compliance and security tools have been able to detect changes to operating system settings and a small subset of BIOS settings (typically only Secure Boot) in the past, but these tools usually lack any kind of temporal context for these detections. These prior solutions were designed for compliance or drift detection and may still allow an attacker to carry out multiple configuration changes and then revert to a “known good” state to avoid detection.

The Dell SafeBIOS IoA feature addresses this gap by using Dell threat modelling exercises and expertise to define specific chains of multiple configuration changes that could introduce risk to the system or signal the early signs of an in-progress attack. These may include behavioral signals and sequences which may indicate a below the OS attack (e.g., repeated failed verification, unusual update patterns, suspicious configuration drift). The configuration attributes in each of these chains are continuously monitored by the Dell Trusted Device Application, and risk evaluations are logged as these chains are traversed on the system. This allows the administrator or security analyst to take remediation actions as needed based on incremental risk associations and potentially before the next stage of the attack is deployed against the weakened configuration.

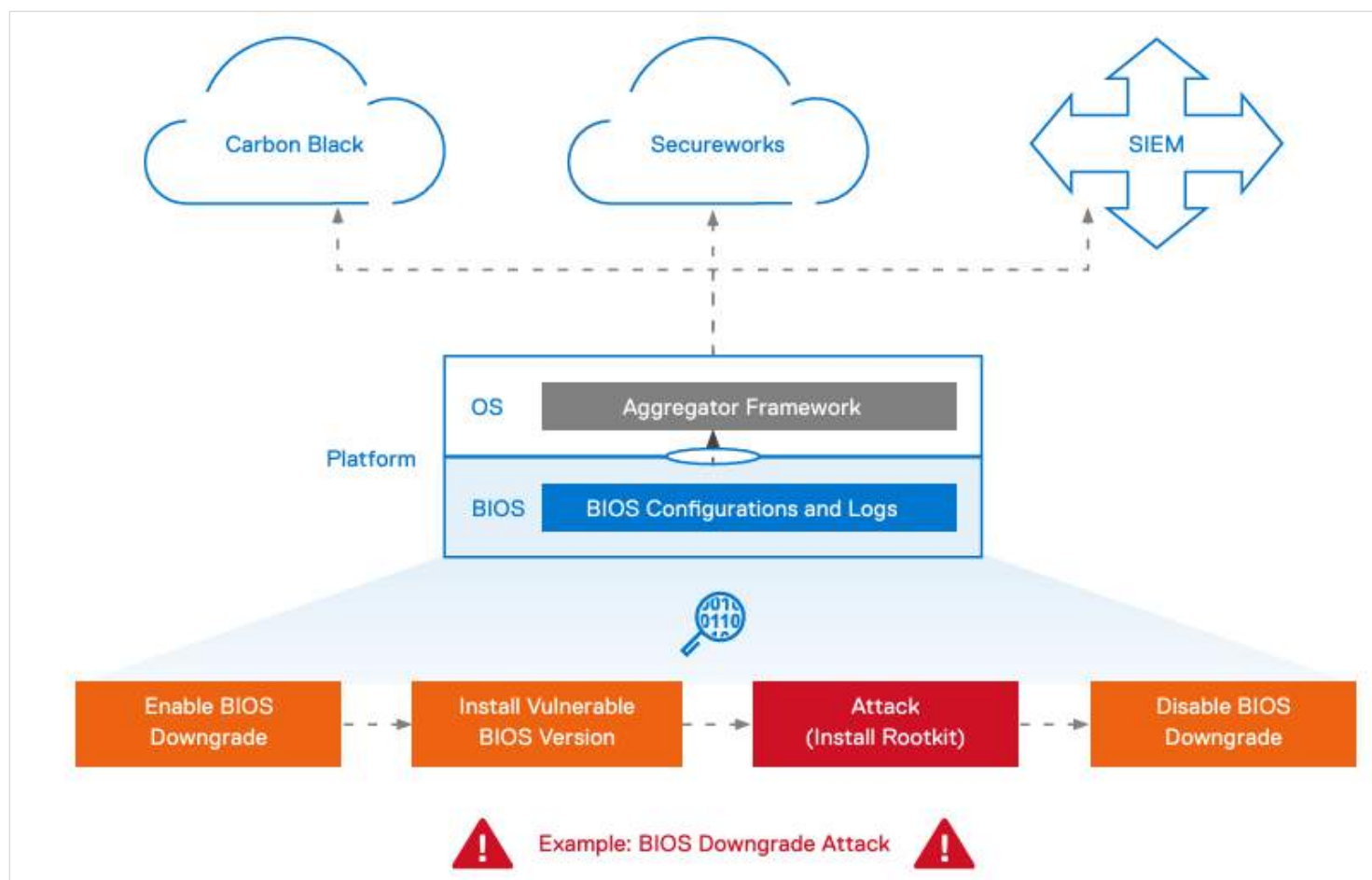


Figure 11: SafeBIOS Indicators of Attack

How Off-Host Verification Is Performed

The DTD App (or Client Device Manager Security module) runs at each boot and/or per policy (typically scheduled, e.g., every 24 hours or on-demand). On the endpoint, the DTD App (or DCDM):

- Reads the current BIOS/firmware image and configuration metrics from the endpoint.
- Calculates hashes (e.g., SHA-2, SHA-5 family; exact algorithm choice is not specified publicly but is consistent with Dell's cryptographic practices).
- Packages the measurements along with device identifiers (service tag, model, BIOS version, etc.).

It then sends a telemetry/verification request to Dell's secure cloud over an authenticated, encrypted channel.

In the Dell cloud the verification service takes the following steps:

- Locates the correct reference entry for the device (maps platform ID + BIOS version + ME version → reference record).
- Compares endpoint hashes to these off-host stored hashes:
 - o If `H_bios_image == H_bios_image_ref` and `H_me_fw == H_me_fw_ref` (where applicable) and there are no policy violations in configuration, the BIOS/firmware is considered verified.
- Produces a pass/fail result and may also calculate a risk score or attach specific error codes:
 - o "Pass" → BIOS (or firmware) is intact, matches known good copy.
 - o "Fail - version mismatch" → outdated but not necessarily tampered.
 - o "Fail - integrity mismatch" → hash mismatch indicating possible tampering or unapproved modification.

Verification results are pushed back and made available in several ways:

- Windows Event Viewer on the endpoint – detailed event IDs, pass/fail, error details.
- Management and security consoles:
 - o Microsoft Intune (via Dell Client Device Manager & DTD integration).
 - o Dell TechDirect / Dell Management Portal for fleet wide views, especially when using Client Device Manager and Secured Component Verification (SCV) on Cloud.
 - o CrowdStrike Falcon, Absolute – integrated BIOS-level telemetry streams IoA, off-host BIOS verification failures, component tampering alerts into third-party security consoles.

Dell is the only PC OEM documented as providing firmware level threat detection and visibility directly within third party security consoles using this off-host telemetry.

If off-host BIOS verification detects an issue, the DTD / DCDM logs BIOS Verification failure events locally and surfaces them to the configured management plane (Intune, Dell TechDirect, CrowdStrike Falcon, Absolute, etc.).

These can then trigger:

- Conditional access policies (e.g., in Intune).
- Incident workflows in XDR/SIEM.
- Remediation playbooks.

BIOS Image Capture

If BIOS corruption or tampering is detected, SafeBIOS can capture the compromised BIOS image for forensic analysis, rather than simply overwriting it immediately. Customers that are concerned about sophisticated adversaries tampering with BIOS would likely also be concerned about the intention, and even identity, of those adversaries. To support this, the Dell SafeBIOS Recovery feature includes an image capture function to save the tampered or corrupted BIOS to the system drive (HDD/SSD) during any recovery operation. This image is saved as a simple binary file that can be harvested by system security software such as the Dell Trusted Device Application.

To accomplish this, the DTD App/DCDM security module queries the EFI partition for a corrupt or tampered image.

- If found, copies it to \\%PROGRAMDATA%\Dell\TrustedDevice\ImageCapture.
- If off-host verification fails and tampering is suspected, it can copy images from memory as well to the same location.

Image capture is retained for a defined period (e.g., 200 days) to support investigations. This image can be collected by a compatible app for analysis at scale. Experienced analysts within customers' security operations control (SoC) can evaluate this file using methods that already exist for analyzing malware during more common hunting operations.

Common Vulnerabilities and Exposures (CVE) Detection and Remediation

This feature permits identification of known vulnerabilities on a Dell device with a built-in security check.

- CVE Detection uses an intelligent, built-in monitoring feature that scans for publicly reported security flaws on a Dell device and provides recommendations on how to fix them. It proactively assesses device health against a database of publicly disclosed computer security flaws maintained in the U.S. National Vulnerability Database by the National Cybersecurity's federally funded research and development center (FFRDC), operated by the MITRE Corporation and funded in part by the U.S. Department of Homeland Security. It also uses Dell Security Advisories (DSAs) which map specific CVEs to affected Dell models and BIOS/Firmware verifications, as well as the recommended fixed versions and mitigation guidance.
- CVE Detection scans for vulnerabilities based on specific PC models and BIOS versions, recommending the relevant patch for swift remediation.
- On each endpoint, the agent collects:
 - Platform identity (model, service tag).
 - Installed BIOS version.
 - Installed firmware versions tracked by DCU/DCDM (as applicable).
- The version is mapped to a CVE, informed by the NVD/MITRE CVE database and Dell security advisories. For each component, the DTD (DCDM) app determines whether or not there are open CVEs (unpatched on the device) and if there is a remediating BIOS/firmware update existing from Dell. It then aggregates this into a per-component vulnerability status and provides an overall view of outstanding DSAs and CVEs for the device.

- The results are written in the Windows Event Viewer, the DTD local console and/or Dell TechDirect and DMP portal dashboards. These results can also be provided to Intune, CrowdStrike, Absolute, etc. depending on the configuration.
- CVE identification can run as 'detect only' (unmanaged) where it does not automatically patch, and logs which CVEs/DSAs apply, providing recommendations on which BIOS/firmware updates to apply.
- In managed environments such as Intune, CVE auto-remediation can orchestrate the updates for the detected CVEs using the DCDM Update Module or the DCU backend. This data can be used to prioritize patching for high-impact CVEs and critical platforms, to provide a compliance signal and implement conditional access and to implement a CVE Auto-Remediation process through DCDM to reduce the need for manual patching.

Dell CVE Detection and Remediation turns each Dell PC into a self-reporting sensor for BIOS/firmware vulnerabilities, with the option (via DCDM) to make remediation more automatic. It bridges the usual gap between traditional patch management and the firmware layer, which is typically opaque to standard endpoint tools.

Dell CVE Detection and Remediation works today for BIOS vulnerabilities and is being extended to cover all firmware and eventually applications and drivers.

Security Risk Protection Score

Dell's Security Risk Protection Score (or more simply the Security Score) is a composite endpoint-level KPI generated by the DTD App or DCDM. It's meant to provide a single, quantitative signal to plug into policy engines (Intune, SIEM, SOAR, etc.), but it's explicitly derived from several underlying security controls rather than being a black box.

The Security Risk Protection Score is an endpoint-level KPI that expresses how well a device is protected at and below the OS, based on the presence and health of specific controls as observed by the DTD agent.

- It is not a generic "vulnerability score" like CVSS.
- It is not a behavior-based risk score (e.g., "this device is under active attack").
- It is a configuration-/control-centric score that answers: "Given what I can see about this endpoint's foundational protections, how exposed is it?"

It should be treated as a device-hardening and control-coverage signal, not as a replacement for EDR risk scores or SIEM detections.

The score is based on a fixed set of security "solutions" / controls that the agent checks on each endpoint. Currently this list includes:

- Anti-virus status
- Firewall status
- Disk encryption (e.g., BitLocker) status
- TPM use (TPM 2.0, enabled & in use, required for some Dell capabilities)
- BIOS administrator password presence/enforcement
- BIOS Verification state (off-host BIOS integrity attestation)

- Intel ME Verification state (for Intel platforms)
- AMD PSP Verification state (for AMD platforms)
- Indicators of Attack (IoA) / BIOS Events status (whether IoA has flagged issues or if BIOS configuration has suspicious changes)

For each of these controls, the DTD App/DCDM determines:

- Whether the control is present and correctly configured.
- Whether it has recently passed its own internal checks (e.g., BIOS verification passed, Intel ME verification passed).
- Whether there are warnings or failures (e.g., control missing, disabled, or showing signs of compromise/misconfiguration).

For each control, DTD computes a per-control assessment (Pass, Pass with warnings or Fail) and aggregates them into the Security Risk Protection Score (per device), written as a comprehensive score event along with the detailed per-control statuses.

While Dell does not expose the exact mathematical formula, you can safely assume that high-impact controls (e.g., BIOS Verification, disk encryption, Intel ME verification) are weighed more heavily than softer ones (e.g., AV presence), given the emphasis on below-the-OS security in SafeBIOS and DTD. Additionally, a single Fail on a critical foundational control typically has a material negative impact on the overall score, even if less critical items pass.

DTD scans for the presence and status of each component every 24 hours, and also 15 minutes after the DTD App/DCDM service restarts.

Results persist as timestamped events in Windows Event Viewer under the Dell Trusted Device logs and are also available via integrations (Intune, SIEM, etc.).

The score can be disabled via registry (HKLM\SOFTWARE\Dell\TrustedDevice\DWORD=SecurityScore, 1=enabled, 0=disabled). This is useful if you want to control telemetry volume or prefer to rely solely on raw control-level events.

There are Security Score web service APIs with JWT authentication, indicating that the score is also consumable via Dell's backend or TechDirect-like services for dashboards/fleet KPIs.

TCG Measured Boot

As mentioned in an earlier section, TCG Measured Boot on the Dell device uses the TPM as a protected area for storing hashes of BIOS, firmware, and bootloader code and configuration that is loaded and/or executed in the boot process. The TPM is designed to store these events in a secure way that can be cryptographically verified after the boot completes through a process called attestation. More information about how the TPM works can be found in the TCG [TPM 2.0 Library Specification](#).

The functionality needed to support TCG Measured Boot is built into the TPM using registers with very specific properties called PCRs (Platform Configuration Registers). These PCRs cannot be written to directly: they can only be 'extended.' Extending is a relatively simple operation in practice but is incredibly useful for code integrity. Internal to the TPM, each PCR extension operation takes the current state of the PCR, concatenates it with the incoming message or data to extend, and then hashes it using the selected algorithm, e.g., SHA-256,

before recording it to the PCR. This creates a PCR value cryptographically dependent on all extended operations (and their order) that occurred since the PC was reset.

Intel® vPro Additions to Built-In Security

With Intel vPro enabled on Intel-equipped PCs and supplementing Dell SafeBIOS protections, Dell and Intel® provide another routine for managing fleet of Dell platforms. With Intel® Active Management Technology, ITDMs can diagnose issues remotely in a hybrid work scenario. Along with Intel® AMT, vPro has additional features such as a Platform Service Record and Unique Platform Identity (or UPID). Both features rely on one another to play key roles in Dell SafeBIOS prompting tamper detection on Dell platforms through the SafeBIOS IoA.

Code, Configuration, and the TPM Event Log

Each Dell commercial device extends code and configuration information to the TPM PCRs during every boot in accordance to the [TCG PC Client Platform Firmware Profile Specification](#).

There are many PCRs in each TPM. Table 2 provides a high-level overview of some of the TPM PCRs used on the platform. To maximize compatibility across PC vendors, the TCG PC Client Platform Firmware Profile Specification describes which specific PCR indexes in the TPM should be included in each type of measurement during the boot process. For example, pre-boot BIOS code that executes from the internal SPI flash is extended to PCR0 while UEFI drivers that execute from add-in devices are extended to PCR2. Dell devices extend BIOS Setup options that are security related to PCR1 in addition to hardware information such as memory configuration.

PCR Number	Function / Allocation
0	BIOS Code
1	BIOS Settings / Platform Configuration
2	UEFI Option ROMs
3	UEFI Option ROM Configuration
4	Boot Loader / Master Boot Loader (MBR)
5	Boot Loader / Master Boot Loader (MBR) Configuration
6	Platform Manufacturer Specific Measurements

PCR Number	Function / Allocation
7	Secure Boot
8-15	Static Operating System
16	Debug
23	Application Support

Table 2: Standard PCR Allocations

The Dell device BIOS creates a TPM event log entry each time a new measurement is extended to any TPM PCR during the boot process. The TPM event log allows verifiers such as the OS or remote entities to reconstruct the record of code in the event of a mismatch to an expected or known-good value. The TPM measurements persist for one boot cycle. Upon reboot, the TPM PCRs are 'reset', and the TPM event log is cleared. The TPM PCR measurements and the event log are recreated on every boot.

NIST 800-155 Measurements

One unpublicized feature of Dell devices with Intel processors that may be interesting to readers is the inclusion of PCR0 "reference measurements" directly embedded into each BIOS update utility. This feature aligns to the NIST SP800-155 BIOS Integrity Measurement Guidelines (still in draft revision) and can be used to determine the Dell authorized values for the BIOS code region measurement that the BIOS extends to PCR0. The value can then be compared to the measured value in the TPM event log on the device to verify the BIOS code running on the platform. To export these reference measurements, use the /BIOSMeasurement command line option on any Dell device BIOS update utility. An example of the content and format of the output of this command appears below:

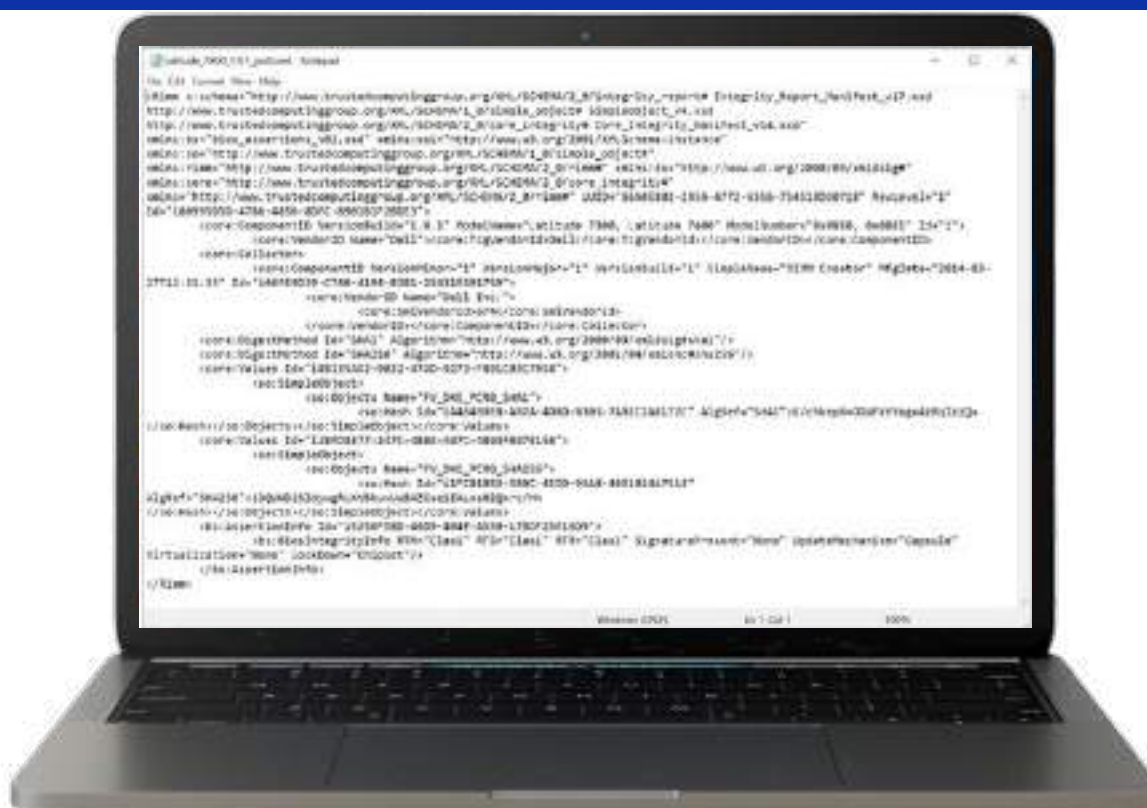


Figure 12: Example BIOS Measurements

Advanced: NIST 800-155 Measurements Extraction, Conversion, and Comparison

Use the following steps to extract and compare the NIST 800-155 measurements from the BIOS update utility with the device's TPM PCR event log measurement.

- Create a NIST800-155 xml output file from the BIOS firmware update utility
 - At a command prompt, execute: Latitude_7X00_1.9.1.exe /BiosMeasurement
 - Locate the output file. e.g., Latitude_7X00_1.9.1_pcr0.xml from the above step.
 - This is the NIST 800-155 Measurement XML file
 - Open the file, and find the SHA1 and / or SHA256 PCR 0 values
 - Convert the BASE64 PCR 0 value to HEX (use an online tool)
 - Save value for comparison.
- Get the TPM PCR Event Log from the device (booted to the OS).
 - Use a tool to read the device's TPM PCR Event Log.
 - Find the PCR0 'EV_Post_Code' entry in the log.
 - Compare this value to 1.e). The values should match.

Dell Integrations with Hardware Providers

Intel Boot Guard

When Intel introduced Boot Guard technology, Dell client PCs implemented it as an additional hardware root of trust for BIOS. Intel Boot Guard serves as an incredibly effective detection mechanism for verifying the integrity of the earliest and most critical code executed by the processor is still intact. Any tampering or corruption of the initial boot block (IBB), the very first piece of BIOS code to be executed by the processor, will be detected by the chipset before the processor comes out of reset. Dell devices are configured with the most restrictive policy for Boot Guard which blocks all code access if the boot block verification fails during the Boot Guard check. This policy “bricks” the system, to limit any further adversary activity, and to reduce the overall incentive for tampering.

While technologies like Intel Boot Guard offer effective protection and detection capabilities for the root of trust, some customers may be concerned that the Boot Guard checks are only enforced once per boot or that the digital certificates used for verifying the boot block are resident on the endpoint. The BIOS verification included in Dell commercial PCs addresses both concerns. BIOS verification uses an OS-resident application – the Dell Trusted Device, or DTD – to verify the integrity of the BIOS against known-good off-host reference measurements at any time. These reference measurements are generated for each BIOS version during the BIOS build process inside Dell infrastructure. Invoking this capability at a regular cadence greatly reduces the window of time that malicious code can be present on a system before detection, even in the extremely unlikely event that all boot-time prevention capabilities were somehow bypassed.

Intel Management Engine (ME) Firmware Verification

As previously mentioned, the Intel vPro Converged Security and Management Engine (CSME or just “Intel ME”) plays an important and privileged role in the boot process and the overall operation of the system below the OS. The Intel ME Firmware Verification component of Dell Trusted Device detects unauthorized tampering of the early boot stages of this highly privileged firmware. Built exclusively for Dell commercial PCs as an off-host check, this built-in feature within the SafeBIOS framework provides this additional level of insight for Intel vPro systems.

Intel vPro Integration for Out of Band Management (OOBM)

Dell has an integration with Intel vPro which provides enhanced security and the ability to remediate and securely wipe a device. The Dell Client Command Suite uses the Intel vPro platform's out of band management capabilities to equip administrators with remote keyboard/video/mouse (KVM) to wake a device, wipe its main drive, or initiate an Intel® Firmware Guard assisted firmware update to reliably reduce the possibility of in-the-field system crashes. The integration of these capabilities provides a unique, multilayer defense-in-depth that improves a SecOps team's effectiveness and efficiency as they protect, correct, and respond to evolving cyberthreats. These capabilities come standard with all Intel vPro equipped devices.

Microsoft Intune Integration

Microsoft Intune is a flexible platform that integrates various services for IT administrators, enabling them to oversee and control a range of devices, including mobile devices, desktop computers, virtual machines, embedded devices, and servers.

Administrators can create compliance policies in the Intune admin center to ensure that SafeBIOS and other Dell 'built-in' capabilities – through the DTD application – are protecting Dell computers below the operating system. DTD uses PowerShell scripts and agent-level configuration to communicate endpoint compliance and transmit results to Microsoft Intune.

The DTD Script folder contains the required script and configuration file which can be imported to create and deploy custom policy in Intune. The result is displayed on the Intune compliance page.

More information and instructions are available here: [Dell Trusted Device – Installation and Administration Guide v6.0 | Dell US](#)

Hardware-Assisted Security with CrowdStrike and Intel

To provide faster threat detection, Dell worked with CrowdStrike and Intel to deliver an endpoint security solution that brings together the power of hardware and software to enhance threat detection and response. The joint "hardware-assisted security" solution allows administrators to combine CrowdStrike's threat intelligence database with below-the-OS device telemetry for greater insight into potential breaches. With the Dell Trusted Device (DTD) Application enabled, Dell commercial PCs push data from multiple built-in security features to the OS, and surface that data for integration with third-party software solutions. With CrowdStrike Falcon XDR added on-the-box, an admin can collect device security data coming from SafeBIOS alerts for further investigation within the CrowdStrike console.

This collaboration enhances software security by providing another layer of defense with improved visibility and observability at the firmware level – an area of the device where we have seen an uptick in malicious and persistent threats in recent years. CrowdStrike software can catch activity deviating from the known good, but Dell device telemetry will also surface rapid alerts from, e.g., SafeBIOS Indicators of Attack, to ensure timely response and remediation of an affected device.

Dell PCs provide the visibility and actionability needed to disrupt attacks by leveraging BIOS/firmware protections and (when using Intel vPro) Intel® Control-flow Enforcement Technology (Intel® CET) to help shut down the entire class of ROP attacks. CrowdStrike's Hardware Enhanced Exploit Detection (HEED) integrates Intel® Processor Trace (Intel® PT) CPU telemetry to extend memory safety protections for coded injection techniques, across PC fleet generations.

In addition, CrowdStrike has re-imagined how to stop fileless attacks early in the kill chain by using the accelerated memory scanning algorithms of Intel TDT and its ability to offload processing to the Intel® Graphics Technology integrated graphics processor. The resulting 4-7x performance⁹ acceleration helps ensure a performant user experience while applying CrowdStrike's dynamic, earlier, IOAs to the memory layer – and it's only available on Intel® processor-based PCs. As fileless attacks attempt to move down the stack, Dell

SafeBIOS uses the Intel vPro platform's Intel® System Resource Defense technology to restrict system privileges and malicious access to the OS.

These capabilities are [described in this solution brief](#).

Below-the-OS Integration with CrowdStrike for Dell on AMD

A similar threat detection capability exists for AMD devices. This joint solution allows administrators to combine CrowdStrike's threat intelligence database with Dell below-the-OS device telemetry for greater insight into potential breaches. With the Dell Trusted Device (DTD) Application enabled, Dell commercial PCs push data from multiple built-in security features to the OS, and surface that data for integration with third-party software solutions. With CrowdStrike Falcon XDR added on-the-box, an admin can collect device security data coming from BIOS alerts for further investigation within the CrowdStrike console.

This collaboration enhances software security by providing another layer of defense with improved visibility and observability at the firmware level. CrowdStrike software can catch activity deviating from the known good, but Dell device telemetry will also surface rapid alerts from, e.g., Indicators of Attack, to ensure timely response and remediation of an affected device.

Below-the-OS Integration with Absolute

To strengthen endpoint resilience and improve visibility, Dell partnered with Absolute to deliver a solution that combines Dell's hardware-based security with Absolute's firmware-embedded persistence technology. This integration ensures that security controls remain active and tamper-proof, even if the operating system is reinstalled or the device is wiped.

With Dell Trusted Device (DTD) capabilities enabled, Dell commercial PCs provide telemetry from below-the-OS security features, which Absolute leverages to maintain continuous visibility and control. Absolute's Persistence® technology, embedded in the Dell BIOS, guarantees that the Absolute agent can self-heal if removed or corrupted—providing IT teams with an unbreakable connection to every endpoint.

This collaboration enhances endpoint security by delivering real-time insights into device health, compliance, and risk posture. Administrators can monitor critical security applications, detect anomalies, and remediate threats remotely, even when devices are off-network. By combining Dell's hardware root of trust and BIOS protections with Absolute's resilience platform, organizations gain a layered defense that extends beyond traditional software-based approaches.

The result is a security foundation that is both persistent and adaptive—helping businesses maintain compliance, reduce risk, and respond quickly to emerging threats. Together, Dell and Absolute deliver the visibility and control needed to protect endpoints in today's dynamic threat landscape.

Other Integrations for SafeBIOS

Security Information and Event Management (SIEM) solutions play a critical role in enhancing the cybersecurity posture of organizations by providing comprehensive tools for real-time monitoring, analyzing, and responding swiftly to security events. These solutions collect and aggregate log data generated throughout the organization's technology infrastructure, including networks, applications, and endpoints. SIEM tools leverage advanced analytics and correlation algorithms to identify patterns and anomalies in the data, helping security teams detect and investigate potential security incidents.

Dell Trusted Device (DTD) can interoperate with SIEM solutions and supports the following features:

- BIOS Verification
- Intel ME Verification
- BIOS Events & Indicators of Attack
- Image Capture
- Security Score
- CVE Detection & Auto-remediation
- Secured Component Verification

The Dell Event Repository must be installed to deliver DTD results to a SIEM solution.

Respond and Recover

From the NIST framework:

Respond: Develop and implement appropriate activities to respond to a detected cybersecurity incident.

Recover: Develop and implement appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity incident.

Respond and Recover are often overlooked functions within the NIST Cybersecurity Framework. Admitting that a failure or attack has occurred or that an unknown vulnerability has been exploited by an adversary can be uncomfortable at times. Being well prepared to handle these incidents and having the confidence to be able to restore the Dell device back to normal operating status as quickly and efficiently as possible can help to minimize the overall cost of these events.

Embedded Controller Recovery

As mentioned previously the Dell device embedded controller, or "EC", operates as the root of trust of the system at the very lowest level of hardware enablement. This privileged context and critical role requires a high degree of fault tolerance to avoid false positives and keep the beginning of the chain of trust intact, secure, and resilient. To address this, the Dell device EC supports dual firmware images and a failover mode to allow backup firmware to recover the primary image if needed.

BIOS Recovery

In addition to having a secure and resilient EC, it is also critical for the next stage of the boot process that the BIOS, also has a robust recovery mechanism. Dell PCs have a sophisticated set of flexible and tunable features that ensure that the BIOS can be reverted to a known-good copy if compromised. Additionally, once BIOS recovery is invoked, it will securely capture the state of tampering for offline analysis (described in the previous sections) for those customers that require deep insight into their adversaries' techniques.

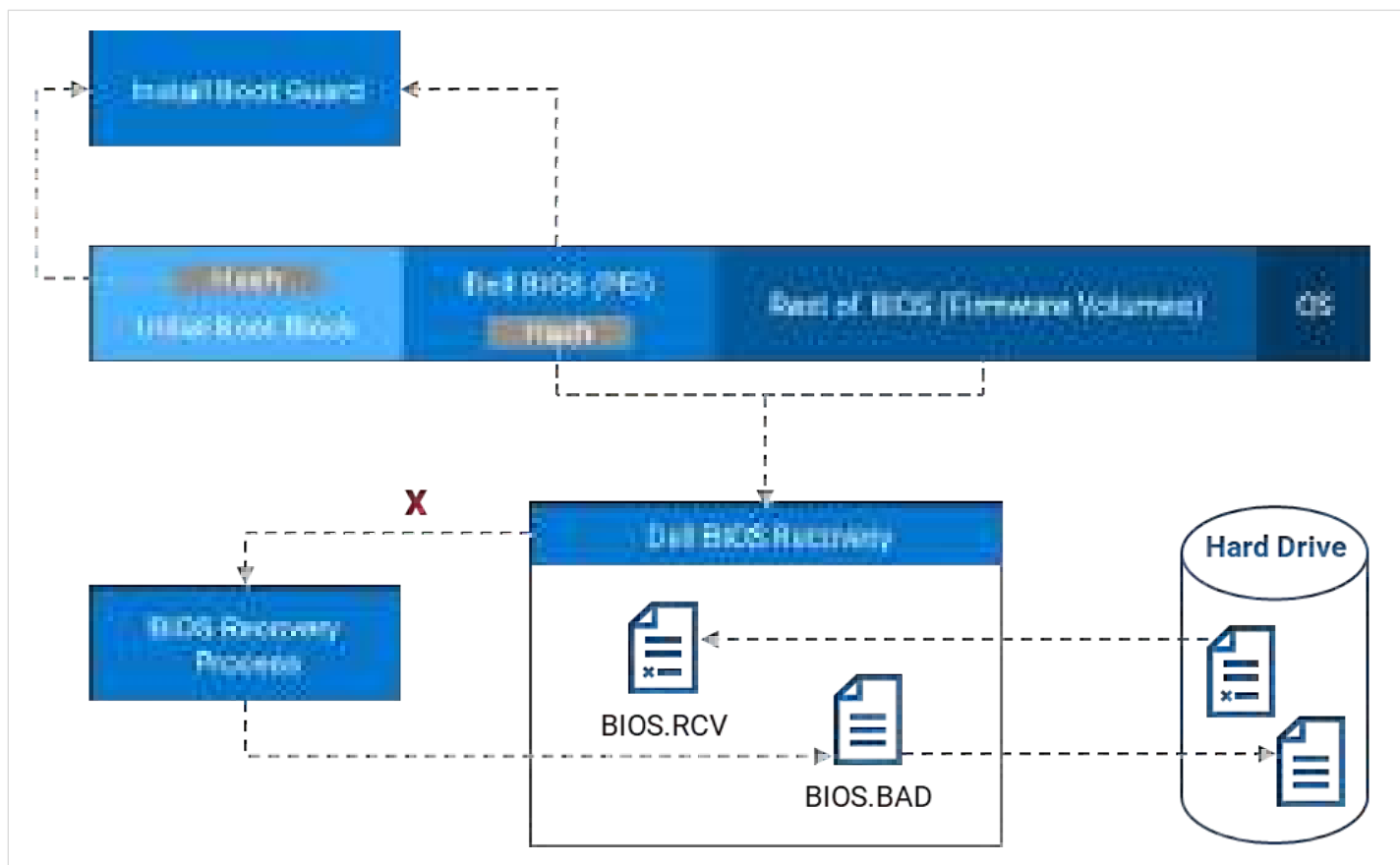


Figure 13: SafeBIOS Recovery Flow

BIOS Recovery Image Update Flow

BIOS recovery is engineered right into the Dell BIOS update architecture. Each Dell device is prepared days, months, or even years before any potential trigger to recover is ever required. Essentially this is part of every BIOS update on the system. In addition to updating the BIOS running on the system the BIOS update tool will copy a recovery version of the new BIOS to the secure EFI partition on the hard drive. The EFI partition is a hidden partition that is independent of the operating system hard drive partitions. Microsoft Windows uses the EFI System Partition (ESP) as the critical storage area for boot-related files. When a PC with BIOS (UEFI) firmware starts, the firmware loads boot files from the EFI partition, which contain the Windows Boot Manager, boot configuration data, and other utilities needed to initialize the operating system.

Dell Trusted Device Below the OS White Paper

This partition is modifiable with physical or OS administrative access, so it's important to note that the recovery image is signed in the same manner as the updated version and verified by the BIOS RTU prior to performing recovery.

BIOS Recovery

BIOS Recovery from Hard Drive – This option is set by default. Allows you to recover the corrupted BIOS from a recovery file on the HDD or an external USB key.

BIOS Auto-Recovery – Allows you to recover the BIOS automatically.



NOTE: BIOS Recovery from Hard Drive field should be enabled

Auto Recovery Flow

Dell devices can be configured to automatically recover the BIOS to a known-good copy when the early BIOS code detects an integrity violation during pre-boot. To support this, the early BIOS (the Pre-EFI Initialization phase, or PEI, in UEFI terminology) can read the BIOS recovery image from the hard drive or USB and verify the signature of the recovery image using the same Root of Trust for Update (RTU) that protects the BIOS update process (i.e. NIST 800-147).

Customer Flexibility: Manual Recovery

The BIOS Auto-Recovery option is disabled by default on Dell devices. This may at first seem misaligned with the overall security and threat model assumptions of the Dell device. However, this default was designed to support customers whose threat models prioritize detection of BIOS tampering or corruption well above the need for high availability/resilience that may mask potential adversarial activity.

Confirming BIOS Integrity

All Dell commercial BIOS are checked during boot (or per schedule in managed environments) against an off-host, Dell hosted 'golden image' using the SafeBIOS BIOS verification capability. This ensures that whatever the source may be for the replacement BIOS image, that the code is always secure and correct for that specific PC. This removes the need to protect a BIOS image with a level of hardware protection used, for instance, for personal credentials, since this off-host check ensures the validity of the code.

Dell Data Sanitization

Dell devices produced since 2017 include the Dell Data Sanitization feature. Dell Data Sanitization allows customers to securely delete data on the internal storage devices in their Dell device. This allows efficient erasure for repurpose or redeployment using industry standard commands based on the NIST 800- 88r1 and IEEE-2883 standards. The feature is supported on internal SATA, SSD, NVMe and eMMC storage devices. It uses industry standard methods such as Enhanced Security Erase for SATA, format NVM for NVMe, and Sanitize for eMMC based devices. (See [NIST Special Publication 800-88r1](#) Guidelines for Media Sanitization and [IEEE Standard for Sanitizing Storage](#) for more details.)

Dell Data Sanitization removes all user data from the storage device. To protect the device from unauthorized wipe of media, the feature is only accessible by a physically present user through the BIOS Setup (F2)

interface. Any user who has access to the BIOS Setup Menu can initiate the wipe. The user interface includes multiple confirmation prompts to ensure data wipe cannot be triggered accidentally. So, the user must be physically present until data wipe begins. Once initiated, the data wipe will proceed until all storage devices are wiped.

- Allows user-initiated data wipe of internal storage devices (SATA/SSD/NVMe/eMMC) using industry standard technology.
- Invokes acceptable media purge per NIST SP 800-88 r1 and IEEE-2883 by invoking media specific commands.
- User interface includes multiple confirmation prompts to ensure data wipe cannot be triggered accidentally.
- Commonly referenced DoD 5520.22-m “multi-pass” requirements were defined before ATA SECURITY ERASE and sanitization method table has been removed from 5520-m. NIST SP800-88r1 and IEEE-2883 both widely accepted as more relevant data sanitization standards, include storage technologies such as NVMe, SSD, etc.

More information about Dell Data Sanitization is available [here](#).

Additional Dell Security Capabilities

Protected Signing Infrastructure

Code signing and protecting access to private keys and certificates within the signing infrastructure is a critical piece of any software or firmware supply chain. Once again, this vital component of the supply chain is also an area most targeted by sophisticated adversaries.

- **Threat: Unauthorized Code Signing**

There are countless examples of supply chain attacks that resulted in stolen digital signing certificates or credentials being used to sign malware. The danger in this scenario is that it is challenging for customers, anti-virus software, and existing tools to differentiate between legitimate and potentially malicious code signed with the same certificate. One example of this activity can be found [here](#).

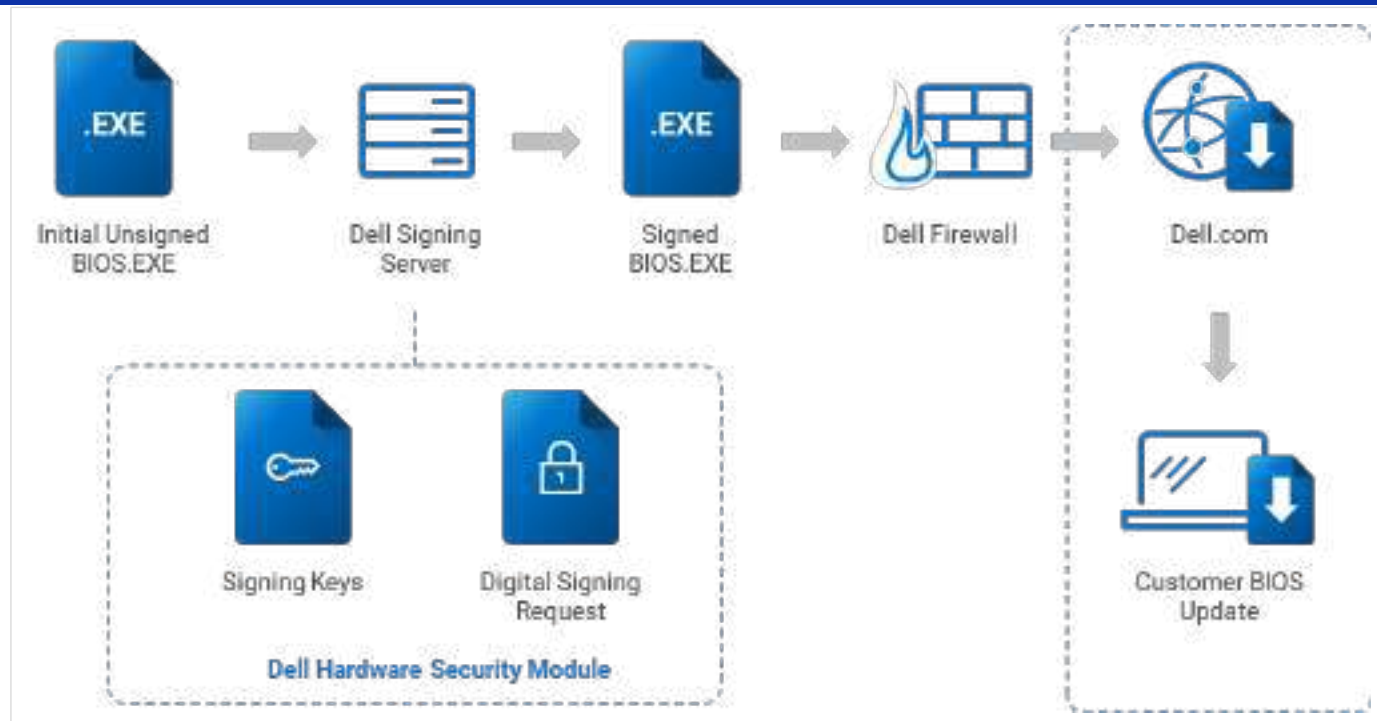


Figure 14: Dell SafeBIOS Signing

- **Mitigation: Signing Infrastructure**

Dell devices use secure signing infrastructure and hardware security modules, or HSMs, for code signing. This infrastructure is managed by Dell Cybersecurity, includes disaster recovery mechanisms, and is protected from unauthorized access using user access control and hardware binding. The Dell device BIOS signing capability is integrated directly into the automated build processes and developers do not have direct access to sign BIOS updates. This infrastructure signs the outer encapsulated BIOS update, Intel Boot Guard IBB, and Intel BIOS Guard code updates.

The Future of Security

Organizations rely on hardened endpoints to defend against modern and sophisticated adversaries and Dell has invested heavily in the security and resilience of the Dell devices to meet this demand. Transparency remains a critical tenet in computer security and hopefully this document has served to provide a comprehensive look into not only the details and intentions behind these features but also some of the limitations.

We understand that Dell devices are only one piece of the security puzzle for our customers. While our investments in device hardening are an important foundation for overall ecosystem security, we continue to prioritize integrations with security software and solutions that help customers maximize the benefits of what we've built. Integrating into security ecosystems and architectures such as Zero Trust ensure Dell telemetry

can be used to enrich user and network access policy tied to the health of the device. This rich telemetry evolves as the landscape evolves and it's exciting to help build the future integrations across not only Zero Trust but to create the basis of data to take full advantage of the AI security evolution over the coming years.

References

Dell and Partner References

- [A Partnership of Trust: Dell Supply Chain Security](#)
- [Achieving pervasive security above, within and below the OS](#) – Dell Technologies and Intel, June 2025
- [Dell, Intel and CrowdStrike – Joint Solution Brief](#)
- [BIOS Security – The Next Frontier for Endpoint Protection](#) – A Forrester Consulting Thought Leadership Paper Commissioned by Dell – June 2019
- [UEFI on Dell BizClient Platforms](#)
- [Intel Hardware Shield](#)
- Dell KB [Find Your Service Tag or Serial Number](#)
- Dell KB [Using Dell Command Configure to Set the Asset Tag Information of Your Dell Computer](#)
- Dell KB [Dell Data Wipe](#)
- Dell [Secured Component Verification \(SCV\) Datasheet](#)
- [Dell Trusted Device – Installation and Administration Guide – v6.0](#)
- [Dell Trusted Workspace](#)
- [Dell Client Signed Firmware Update](#)
- [Principled Technologies Most Secure Study ft. Intel](#)
- [Dell Device Security Practices](#)
- [Dell Secure AI PC Design](#)

Industry Organizations

- UEFI Tiancore Project – <https://github.com/tianocore/edk2>
- [SAFECode](#) – The Software Assurance Forum for Excellence in Code
- [TCG](#) – Trusted Computing Group
- [FIRST](#) – Forum of Incident Response and Security Teams
- [OTTF](#) – Open Group Trusted Technology Forum
- [IEEE Center for Secure Design](#)

Standards and Guidelines

- [NIST Cybersecurity Framework](#) – NIST Publication "The NIST Cybersecurity Framework (CSF) 2.0" - February 26, 2024
- [NIST Cybersecurity Framework](#) – Main Page
- [NIST Special Publication SP 800-193](#) – Platform Resiliency Guidelines
- [NIST Special Publication SP 800-147](#) – BIOS Protection Guidelines
- [NIST Special Publication SP 800-88 \(r1\)](#) – Guidelines for Media Sanitization
- [NIST Special Publication SP 1800-34](#) – Validating the Integrity of Computing Devices
- [FIPS Publication 186-5](#) – Digital Signature Standard (DSS)
- [National Security Agency Cybersecurity Report UEFI Defensive Practices Guidance](#)
- NSA Cybersecurity Information Sheet: [Procurement and Acceptance Testing Guide for Servers, Laptops, and Desktop Computers](#)
- [ISO/IEC 27034-1:2011](#) – Information Security Techniques for Application Security

Quoted Stats

- [Estimated cost of cybercrime worldwide 2017 – 2028](#) – Statistica.com

Diagnostics

If you experience a problem with your computer, run the ePSA diagnostics before contacting Dell for technical assistance. The purpose of running diagnostics is to test your computer's hardware without requiring additional equipment or risking data loss. If you are unable to fix the problem yourself, service and support personnel can use the diagnostics results to help you solve the problem.

Enhanced Pre-Boot System Assessment (ePSA) diagnostics

The ePSA diagnostics (also known as system diagnostics) performs a complete check of your hardware. The ePSA is embedded with the BIOS and is launched by the BIOS internally. The embedded system diagnostics provides a set of options for particular devices or device groups allowing you to:

- Run tests automatically or in an interactive mode
- Repeat tests
- Display or save test results
- Run thorough tests to introduce additional test options to provide extra information about the failed device(s)
- View status messages that inform you if tests are completed successfully
- View error messages that inform you of problems encountered during testing



CAUTION: Use the system diagnostics to test only your computer. Using this program with other computers may cause invalid results or error messages.



NOTE: Some tests for specific devices require user interaction. Always ensure that you are present at the computer terminal when the diagnostic tests are performed.

1. Power-on the computer.
2. As the computer boots, press the F12 key as the Dell logo appears.
3. On the boot menu screen, select the **Diagnostics** option.
The **Enhanced Pre-boot System Assessment** window is displayed, listing all devices detected in the computer. The diagnostics starts running the tests on all the detected devices.
4. To run a diagnostic test on a specific device, press Esc and click **Yes** to stop the diagnostic test.
5. Select the device from the left pane and click **Run Tests**.
6. If there are any issues, error codes are displayed.
Note the error code and contact Dell.

Lista de Membros

Borda

Broadcom Inc. (<http://www.broadcom.com>)
Cisco (<http://www.cisco.com>)
Dell Technologies (<http://www.dell.com>)
Hewlett Packard Enterprise (<http://www.hpe.com>)
Intel Corporation (<http://www.intel.com>)
Lenovo (<http://www.lenovo.com>)
NetApp (<http://www.netapp.com>)
Positivo Tecnologia SA (<https://www.positivotecnologia.com.br/>)
Verizon (<http://www.verizon.com>)

Liderança

Micro dispositivos avançados (<http://www.amd.com/>)
Alibaba (China) Co., Ltd
Daten Tecnologia Ltda (<http://www.daten.com.br>)
Ericsson AB (<http://www.ericsson.com>)
Google LLC (<http://www.google.com>)
HP, Inc (<http://www.hp.com/>)
Huawei (<http://www.huawei.com/>)
IBM (<http://www-03.ibm.com/systems/power/>)
Inspur (<http://en.inspur.com>)
NVIDIA Corporation (<http://www.nvidia.com>)
Seagate Technology (<http://www.seagate.com/>)
Supermicro (<http://www.supermicro.com>)
Vertiv (<http://www.avocent.com>)
VMware Inc. (<http://www.vmware.com>)

Participação

American Megatrends, Inc. (<http://www.ami.com>)
Ampere Computing LLC (<https://amperecomputing.com/>)
ARM, Inc (<http://www.arm.com>)
Atos (<https://atos.net/>)
Eaton (<http://www.eaton.com/us/en-us.html>)
Fujitsu (<http://www.fujitsu.com/>)
Futurewei (<https://www.futurewei.com/>)

Empresas membros do conselho DMTF



Veja todas as empresas membros da DMTF » (</about/list>)

Members List

Board

Broadcom Inc. (<http://www.broadcom.com>)
Cisco (<http://www.cisco.com>)
Dell Technologies (<http://www.dell.com>)
Hewlett Packard Enterprise (<http://www.hpe.com>)
Intel Corporation (<http://www.intel.com>)
Lenovo (<http://www.lenovo.com>)
NetApp (<http://www.netapp.com>)
Positivo Tecnologia S.A. (<https://www.positivotecnologia.com.br/>)
Verizon (<http://www.verizon.com>)

Leadership

Advanced Micro Devices (<http://www.amd.com/>)
Alibaba (China) Co., Ltd
Daten Tecnologia Ltda (<http://www.daten.com.br>)
Ericsson AB (<http://www.ericsson.com>)
Google LLC (<http://www.google.com>)
H3C (<http://www.h3c.com>)
HP, Inc (<http://www.hp.com/>)
Huawei (<http://www.huawei.com/>)
IBM (<http://www-03.ibm.com/systems/power/>)
Inspur Electronic Information Industry Co.,Ltd. (<https://zh.ieisystem.com/>)
Microsoft Corporation (<http://www.microsoft.com>)
NVIDIA Corporation (<http://www.nvidia.com>)
Supermicro (<http://www.supermicro.com>)
VMware Inc. (<http://www.vmware.com>)
xFusion Digital Technologies Co., Ltd. (<http://www.xfusion.com>)

Participation

American Megatrends, Inc. (<http://www.ami.com>)
Ampere Computing LLC (<https://amperecomputing.com/>)
ARM, Inc (<http://www.arm.com>)
Atos (<https://atos.net/>)
Code Construct (<https://codeconstruct.com.au>)
CoreWeave (<https://www.coreweave.com/>)

DMTF Board Member Companies



See all DMTF Member Companies
» (</about/list>)

DELL TECHNOLOGIES INC (GROUP)

WESTHOFFEN -United States of America | Manufacture of computers and peripheral equipment
Publication date:18 Dec 2025
Valid until:18 Dec 2026



CERTIFICATIONS & ENDORSEMENTS

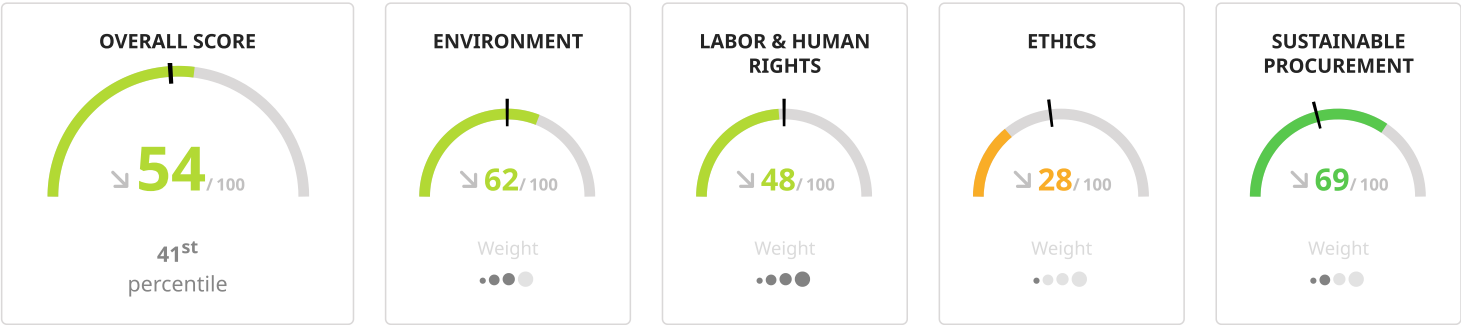
- At least one site is ISO 14001 certified
- Carbon disclosure project (CDP) respondent

SUSTAINABILITY PERFORMANCE OVERVIEW

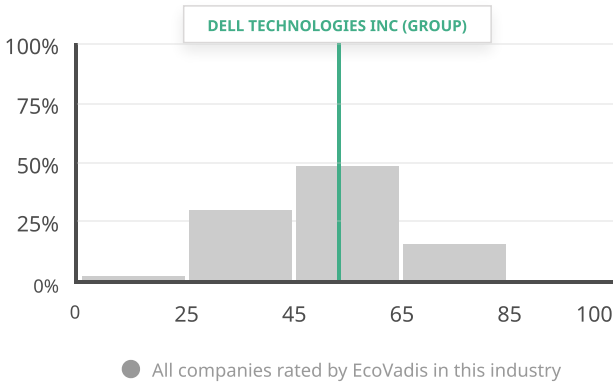
Score breakdown

DELL TECHNOLOGIES INC (GROUP) sustainability performance is: **Good**

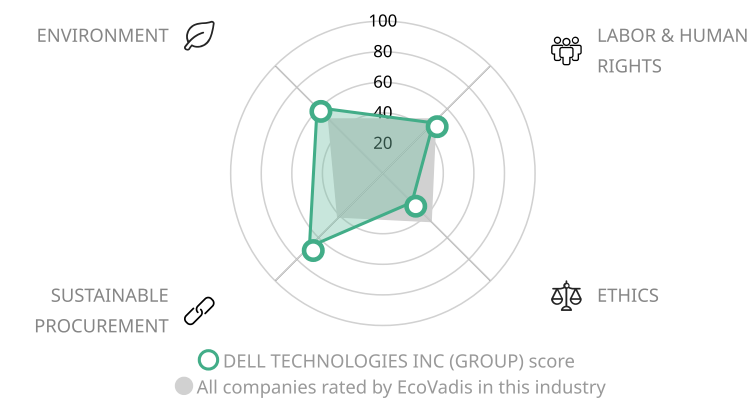
Sustainability performance Insufficient Partial Good Advanced Outstanding Average score



Overall score distribution



Theme score comparison



*You are receiving this score/medal based on the disclosed information and news resources available to EcoVadis at the time of assessment. Should any information or circumstances change materially during the period of the scorecard/medal validity, EcoVadis reserves the right to place the business' scorecard/medal on hold and, if considered appropriate, to re-assess and possibly issue a revised scorecard/medal.

ABOUT ECOVADIS

EcoVadis provides the leading solution for monitoring sustainability in global supply chains. Using innovative technology and sustainability expertise, we strive to engage companies and help them adopt sustainable practices.

Our Mission

To reliably assess companies' sustainability performance, providing them with comprehensive feedback, benchmarking and tools allowing them to embark upon a journey of continuous improvement.

Our Expertise

- Sustainability: our team of international sustainability experts analyze and crosscheck companies' data (supporting documents, 360° Watch Findings, etc.) in order to create reliable ratings, taking into account each company's industry, size and geographic location.
- Innovative technology: we offer access to web-based solutions, where companies can access the EcoVadis Scorecard and share information. These are highly secure online solutions which guarantee the safety of our users' data.

Our Methodology

The EcoVadis methodology is based on international sustainability standards (Global Reporting Initiative, United Nations Global Compact, ISO 26000), and supervised by a scientific committee of sustainability and supply chain experts, to ensure reliable third-party sustainability assessments.

Our Users

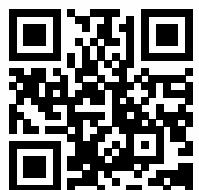
- Thousands of companies use the EcoVadis Ratings platform every month to respond to sustainability assessment requests from customers, set and maintain corrective action plans and centralize sustainability-related documents.
- Over 700 multinational companies use EcoVadis to monitor the sustainability performance of their trading partners, including:



Contact

contact@ecovadis.com

www.ecovadis.com



• Melhor compra

• BMW Group

• Bose Corporation

• Brother Industries Ltd.

• BT plc

Portal de atendimento ao membro (<https://responsiblebusiness.sharefile.com/>) [RBA-Online](#)

(<https://www.rba-online.org/>), [eLearning Academy](#) (<https://rbaacademy.litmos.com>).



([HTTP://WWW.RESPONSIBLEBUSINESS.ORG/](http://www.responsiblebusiness.org/))

CÓDIGO DE CONDUTA

VAP

FERRAMENTAS

INICIATIVAS

ÁREAS DE FOCO

C

EVENTOS E TREINAMENTO

NOTÍCIAS

SECA DE

CONTATO (CONTACT/)

• Cadence Design Systems

• Ciena

• Canon Inc.

• Cirrus Logic, Inc.

• Celestica

• Cisco

• Chicony Electronics Co., Ltd

• Citrix

• Ciara

• Compal Electronics

D

• Dell Inc.

• Dustin AB

E

• Edwards Ltd.

• Ericsson

• EIZO Corporation

F

• Fabrinet

• Ford Motor Company

• Facebook

• Foxconn

• Fairphone BV

• Fujitsu Limited

• Fitbit, Inc.

• Funai Electric Co., Ltd.

• Flex

G

• GlobalFoundries



ELETRÔNICOS

Eles estão cada vez mais presentes na nossa vida.

Você sabe o que fazer com eles quando não os precisa mais?

Veja como fazer o descarte correto.

[SAIBA MAIS](#)

O QUE É LIXO ELETRÔNICO?

Lixo Eletrônico: mitos e verdades - Episódio 1



ONDE DESCARTAR?

Termo utilizado para se referir a qualquer equipamento elétrico ou eletrônico, pilhas e baterias que não têm mais utilidade. Quando é alcançada a fim da vida útil destes produtos, eles são considerados lixo eletrônico.

[Saiba mais](#)

O QUE PODE SER DESCARTADO?

Os pontos de entrega voluntária recebem notebooks, impressoras, eletrônicos de escritório, eletrônicos de pequeno porte, tablets e celulares, acessórios de informática, câmeras, cabos e carregadores, eletroportáteis, ferramentas Elétricas e muitos outros



[Acesse a lista completa](#)

CICLO DA LOGÍSTICA REVERSA

Engajamento de todos para promover
o uso eficiente dos recursos



Localize o Ponto de Entrega
Voluntária do programa Descarte
Green mais perto de você!

Pontos de entrega



ASSOCIADAS ELETRÔNICOS

Confira quem garante o descarte sustentável de seus equipamentos eletroeletrônicos



ASSOCIADAS PILHAS

Confira quem garante o descarte sustentável de suas pilhas e baterias portáteis



Guia de download e instalação de atualizações do BIOS e da UEFI da Dell

Resumo: Informações sobre como fazer download e instalar as atualizações mais recentes do BIOS ou da UEFI em um computador Dell. Este guia aborda como acessar o BIOS ou a UEFI, atualizá-lo usando USB ou Windows e recuperar o BIOS ou a UEFI corrompidos em computadores Dell.

Artigo detalhado

Instruções

Atualizar seu BIOS ou UEFI é mais fácil do que você imagina. Para obter a experiência mais simplificada com instruções passo a passo, vídeos úteis e suporte abrangente para solução de problemas, visite nosso [Guia de atualização do BIOS/UEFI](#). Este recurso dedicado orienta você em cada método de atualização e responde a perguntas comuns em um local conveniente.

Continue lendo abaixo para obter informações essenciais sobre atualizações do BIOS ou vá direto para o Guia de atualização do BIOS/UEFI para obter instruções detalhadas.

Noções básicas sobre BIOS e UEFI

BIOS (Basic Input/Output System, Sistema Básico de Entrada/Saída) e UEFI (Unified Extensible Firmware Interface, Interface Unificada de Firmware Extensível) são os firmwares que conectam o hardware do computador ao sistema operacional. Pense nele como a base que ajuda seu computador a iniciar e se comunicar com seus componentes.

Os computadores modernos da Dell usam UEFI, que oferece:

- Tempos de inicialização mais rápidos
- Recursos de segurança aprimorados
- Melhor compatibilidade com o novo hardware
- Maior estabilidade do sistema

Por que atualizar o BIOS ou a UEFI?

A Dell lança regularmente atualizações do BIOS que podem melhorar o desempenho e a confiabilidade do computador. As atualizações normalmente incluem:

- **Aprimoramentos de segurança** – Proteção contra vulnerabilidades recém-descobertas
- **Melhorias de desempenho** – otimizações para melhor velocidade e eficiência
- **Compatibilidade de hardware** – Suporte para novos componentes e periféricos
- **Correções de bugs** – Soluções para problemas conhecidos que afetam a estabilidade do sistema
- **Adições de recursos** – Novos recursos e configurações

A Dell recomenda atualizar o BIOS como parte da manutenção regular do sistema para manter o computador funcionando sem problemas.

Antes de atualizar: Precauções importantes

Seguir algumas etapas simples antes de atualizar pode ajudar a garantir um processo tranquilo:

Etapas essenciais

- **Faça backup dos dados** – Embora raras, as interrupções de atualização podem afetar a estabilidade do sistema
- **Carregue seu notebook** – Certifique-se de pelo menos 10% da bateria (recomendamos o uso de energia CA)
- **Mantenha-se conectado à energia** – Mantenha os notebooks conectados durante toda a atualização
- **Feche todos os programas** – Isso evita interferências durante a atualização
- **Desconectar dispositivos externos** – Remover unidades USB, impressoras e outros periféricos

Usuários do BitLocker: Leia isso primeiro

Se o computador usar a criptografia BitLocker, você precisará suspendê-la temporariamente antes de atualizar:

1. Pesquise "BitLocker" no Windows
2. Selecione "Gerenciar BitLocker"
3. Selecione "Suspender proteção"
4. Continue com a atualização do BIOS
5. Reative o BitLocker após a conclusão da atualização

Nota: Se você não suspender o BitLocker, precisará da chave de recuperação após a reinicialização. Localize sua chave de recuperação em sua [conta da Microsoft](#), em Dispositivos.

Como atualizar o BIOS: Vários métodos fáceis

A Dell oferece várias maneiras convenientes de atualizar o BIOS. Para obter instruções completas sobre cada método, visite nosso [Guia de atualização do BIOS/UEFI](#).

- [SupportAssist \(recomendado para a maioria dos usuários\)](#). A opção automatizada mais fácil que verifica e instala atualizações para você.
- [Atualização do Windows](#) As atualizações do BIOS são exibidas como atualizações opcionais nas Configurações do Windows.
- [O Dell Command | Atualização](#) Projetado para computadores empresariais, como Latitude, OptiPlex e Precision.
- [Utilitário de atualização independente](#) Faça download e execute o arquivo de atualização diretamente do site da Dell no Windows.
- [Unidade flash USB](#) Perfeito para usuários do Linux ou quando o Windows não está acessível.
- [Atualização over-the-air \(OTA\)](#) Disponível em sistemas modernos para atualizações remotas do BIOS.
- [Dell Update ou Alienware Update](#) Ferramentas pré-instaladas para sistemas Inspiron, XPS, Série G e Alienware.

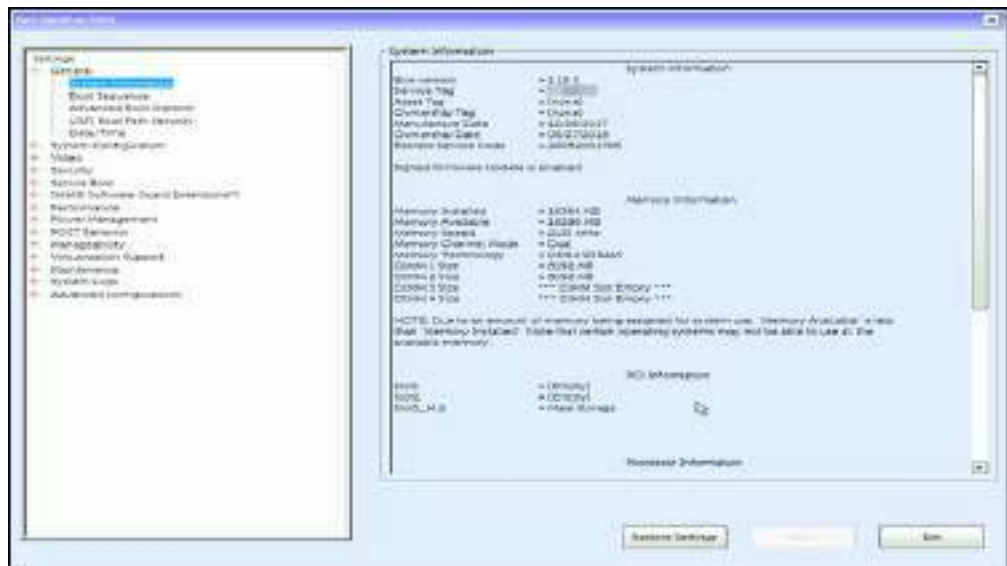
Cada método funciona bem, escolha aquele que se adapta à sua situação. O [Guia de atualização do BIOS/UEFI](#) fornece orientações detalhadas para todas as abordagens.

Como verificar a versão atual do BIOS

Antes de atualizar, verifique a versão atual do BIOS para ver se há atualizações disponíveis:

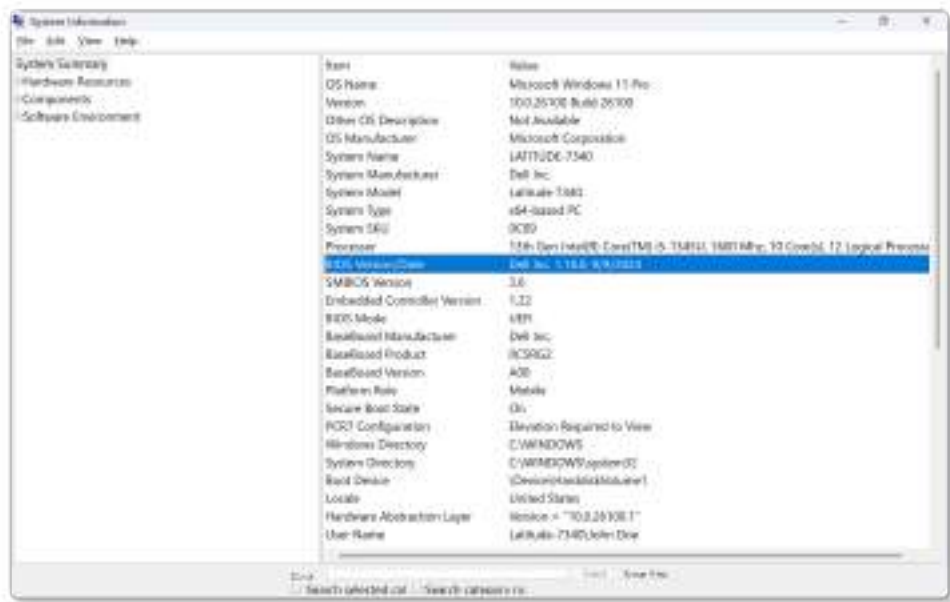
Método 1: Configurações do BIOS/UEFI

1. Reinicie o computador
2. **Pressione F2** repetidamente quando vir o logotipo da Dell
3. Procure a versão do BIOS em **System Information** ou **Overview**



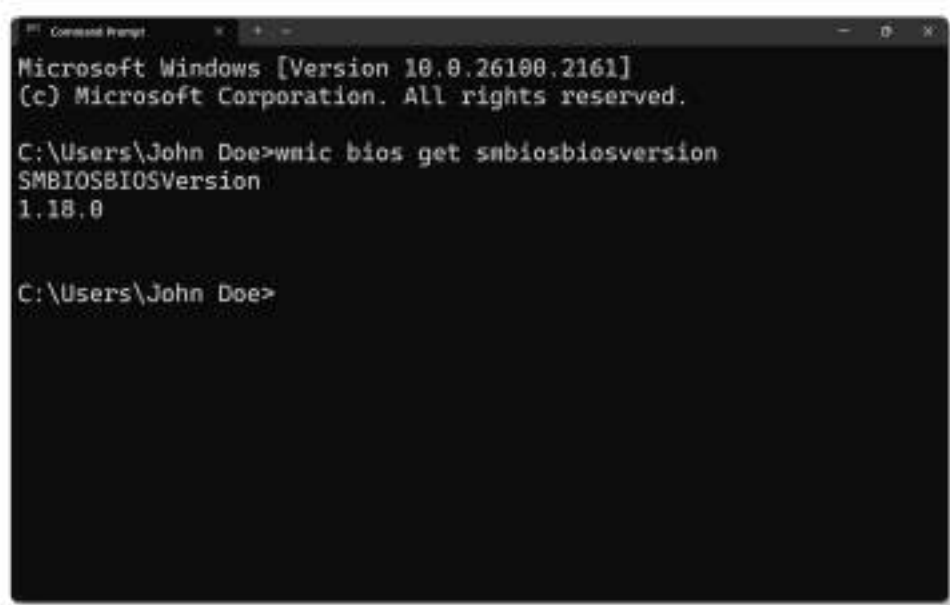
Método 2: Informações do sistema Windows

1. Pressione Windows + R
2. Digite msinfo32 e pressione Enter
3. Encontre "Versão/Data do BIOS" na lista



Método 3: Tela de comandos

1. Abra o Prompt de Comando
2. Digite `wmic bios get smbiosbiosversion`
3. Pressione Enter para ver sua versão



Acessando as configurações do BIOS/UEFI

Precisa alterar as configurações do BIOS? Veja como:

1. Ligue ou reinicie o computador
2. Pressione **F2** várias vezes assim que vir o logotipo da Dell
3. A tela de configuração do BIOS será exibida

Método alternativo:

1. Pressione **F12** no logotipo da Dell
2. Selecione "BIOS Setup" ou "System Setup" no menu

Se F2 não funcionar, tente pressionar **Fn + F2** juntos ou pressione F2 repetidamente em vez de mantê-lo pressionado.

Nota: A interface do BIOS pode ser diferente, dependendo do modelo do seu computador Dell. As configurações são projetadas para usuários experientes, portanto, altere apenas o que você precisa ajustar.

Solução de problemas de atualização

Se a atualização do BIOS encontrar problemas:

- **Garanta uma energia estável** : conecte seu notebook à corrente alternada
- **Carregue a bateria** — pelo menos 50% para notebooks
- **Remover dispositivos externos** – Desconecte dock stations, unidades externas e periféricos
- **Tente um método diferente** – Se um método de atualização falhar, tente usar o [utilitário de atualização do BIOS independente](#)

- **Verificar compatibilidade** – Verifique se você baixou o arquivo de BIOS correto para o seu modelo específico

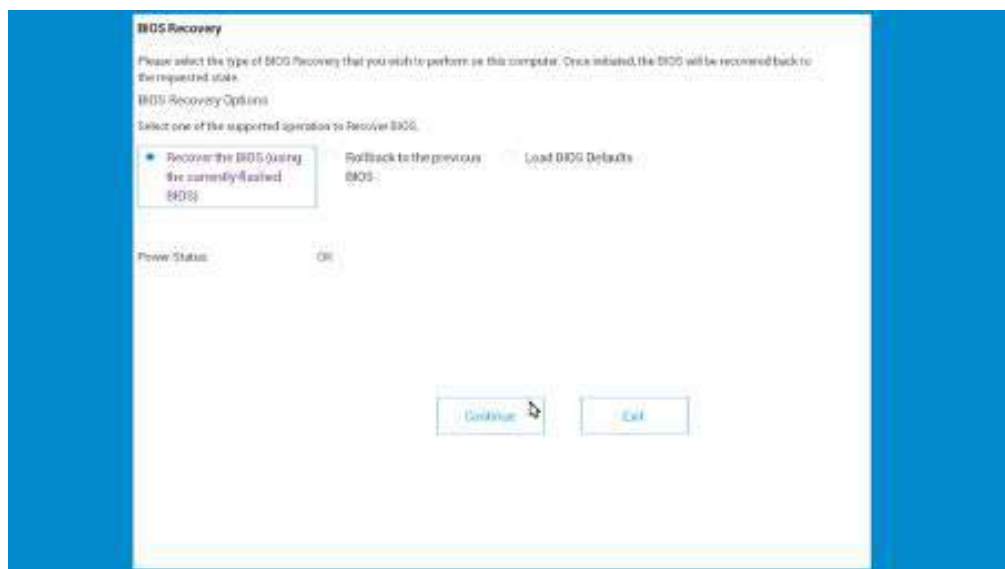
Recuperação do BIOS

Se o computador não iniciar após uma atualização com falha, a Dell fornecerá o recurso de recuperação do BIOS em sistemas Dell modernos. Esse recurso pode restaurar o BIOS usando arquivos de recuperação armazenados no disco rígido ou em uma unidade USB.

A recuperação está disponível por meio de:

- **BIOS Recovery Tool** – Software projetado para corrigir o BIOS corrompido em sistemas Dell modernos

Para obter instruções completas de recuperação e orientação passo a passo, consulte nosso [guia de recuperação do BIOS](#).



Recursos de segurança do BIOS

O BIOS oferece proteção por senha para proteger o computador:

- [Senha de supervisor/administrador](#) – Impede alterações não autorizadas do BIOS
- [Senha do sistema/usuário](#) – necessária para iniciar o computador
- [Senha do disco rígido/SSD](#) – Protege os dados nas unidades internas

Perguntas frequentes

P: Com que frequência devo atualizar meu BIOS?

R: Atualize durante a manutenção regular ou quando a Dell lança atualizações críticas para problemas de segurança ou específicos que você está enfrentando.

P: A atualização excluirá meus dados?

R: Não, as atualizações do BIOS não afetam seus arquivos. No entanto, fazer backup dos dados antes de qualquer atualização do sistema é sempre uma prática recomendada.

P: Posso fazer downgrade para uma versão mais antiga do BIOS?

R: Às vezes. A Dell poderá restringir os downgrades quando versões mais recentes incluírem correções essenciais de segurança. Verifique as notas da versão específicas do BIOS.

P: Preciso de direitos de administrador?

R: Sim, você deve estar conectado como administrador para instalar as atualizações do BIOS.

P: E se minha atualização falhar?

R: Não se preocupe, tente um método de atualização diferente. A [biblioteca de suporte](#) abrange várias abordagens e etapas de solução de problemas.

Como atualizar o BIOS ou a UEFI

Assista a este vídeo para saber como fazer download e instalar o BIOS ou a UEFI mais recente em um computador Dell.



Duração: 03:46

Quando disponíveis, as configurações de idioma de legendas podem ser escolhidas usando o ícone de CC ou Configurações deste player de vídeo.

Como realizar a atualização de firmware pelo ar usando o Dell BIOSConnect



Duração: 02:02

Legendas: Este vídeo está disponível em vários idiomas. Clique no ícone Legenda e selecione o idioma desejado.

Mais informações

Como atualizar o BIOS ou a UEFI

Assista a este vídeo para saber como fazer download e instalar o BIOS ou a UEFI mais recente em um computador Dell.



Duração: 03:46

Quando disponíveis, as configurações de idioma de legendas podem ser escolhidas usando o ícone de CC ou Configurações deste player de vídeo.

Como realizar a atualização de firmware pelo ar usando o Dell BIOSConnect



Duração: 02:02

Legendas: Este vídeo está disponível em vários idiomas. Clique no ícone Legenda e selecione o idioma desejado.

Produtos afetados

Alienware, Dell All-in-One, Dell Pro All-in-One, Dell Pro Max Micro, Dell Pro Max Slim, Dell Pro Max Tower, Dell Pro Micro, Dell Pro Slim, Dell Pro Tower, Dell Slim, Dell Tower, Inspiron, Legacy Desktop Models, OptiPlex, Vostro, XPS, G Series, G Series, Alienware, Dell Laptops, Dell Plus, Dell Pro, Dell Pro Max, Dell Pro Plus, Dell Pro Premium, Inspiron, Latitude, Dell Pro Rugged, Vostro, XPS, Legacy Laptop Models, XPS Tablets, Fixed Workstations, Mobile Workstations, Dell Pro Max Micro XE FCM2250, Dell Pro Max Slim XE FCS1250, Dell Pro Max Tower T2 XE FCT2250, Dell Pro Max 16 XE MC16250, Dell Pro Micro Plus XE QBM1250, Dell Pro Slim Plus XE5 QBS1250, Dell Pro Tower Plus XE5 QBT1250

Propriedades do artigo

Número do artigo: 000124211

Tipo de artigo: How To

Último modificado: 06 nov. 2025

Versão: 38



Certificate of Registration of Quality Management System to ISO 9001:2015

The National Standards Authority of Ireland Inc. certifies that:

**Dell Technologies Inc.
Dell Marketing L.P.
One Dell Way
Round Rock, TX 78682
USA**

has been assessed and deemed to comply with the
requirements of the above standard in respect of the scope of
operations given below:

**The Design, Development, Manufacture, Procurement,
Fulfillment, Delivery, Sales, Sales Operations, Customer
Service, Support, Deployment, Consulting, Take-Back
and Recycling, Refurbishment and Supporting Functions
of Technology Products, Services and Solutions**

**Additional sites covered under this multi-site certification are listed on the
Annex (File No. 19.5000)**

Geraldine LarkinChief
Executive Officer

Lisa Greenleaf
Technical Operations Officer

Registration Number: 19.5000
Certification Granted: January 25, 2011
Effective Date: January 25, 2026
Expiry Date: January 24, 2029



National Standards Authority of Ireland Inc., 20 Trafalgar Square, Nashua, New Hampshire, NH 03063, USA T +1 603 882 4412



Annex to Certificate Number: 19.5000

Scope of Registration:

The Design, Development, Manufacture, Procurement, Fulfillment, Delivery, Sales, Sales Operations, Customer Service, Support, Deployment, Consulting, Take-Back and Recycling, Refurbishment and Supporting Functions of Technology Products, Services and Solutions

Activity

Location

Central Function,
Design/Development, Manufacture,
Procurement, Fulfillment, Delivery,
Sales, Service, Take-Back &
Recycling, Refurbishment, Supporting
Functions

Dell Technologies Inc.
Dell Marketing L.P.
One Dell Way
Round Rock, TX 78682
USA
File No.: 19.5000

Manufacture, Fulfillment, Delivery,
Refurbishment, Service, Support

Dell Technologies Inc.
Dell Computadores do Brasil Ltda. (BRH1)
Av da. Emancipação, 5000
Hortolândia
SP 13.184-654
Brasil
File No.: 19.5000/R1/A

Service, Support, Sales

Dell Technologies Inc.
Dell Computadores do Brazil Ltda.
Avenida Industrial Belgraf, 400
(Service and Support,
Sales/Marketing and CC)
Bairro Medianeira
Eldorado do Sul – CEP 92990-000
Brazil
File No.: 19.5000/R1/B

Service, Support, Sales

Dell Technologies Inc.
Park Plaza Tower 1
Javier Barros Sierra 540, 10th Floor
Santa Fe, Del. Alvaro Obregon
Mexico City, C.P. 01210
Mexico
File No.: 19.5000/R1/C



Annex to Certificate Number: 19.5000

Scope of Registration:

The Design, Development, Manufacture, Procurement, Fulfillment, Delivery, Sales, Sales Operations, Customer Service, Support, Deployment, Consulting, Take-Back and Recycling, Refurbishment and Supporting Functions of Technology Products, Services and Solutions

Activity

Location

Service, Support, Sales

Dell Technologies Inc.
Area Especial Economica Panama – Pacifico
Avenida Bryant
Building No. 255, Arraijan
Panama City
Panama
File No.: 19.5000/R1/D

Design/Development, Delivery, Sales,
Fulfillment, Service, Support

Dell Technologies Inc.
One Dell Way
Round Rock, Texas 78682
USA
File No.: 19.5000/R1/E

Sales, Service

Dell Technologies Inc.
Federal Systems, L.P.
One Dell Way
Round Rock, Texas 78682
USA
File No.: 19.5000/R1/F

Fulfillment, Delivery, Sales

Dell Technologies Inc.
One Dell Parkway
Nashville, Tennessee 37217
USA
File No.: 19.5000/R1/L



Annex to Certificate Number: 19.5000

Scope of Registration:

The Design, Development, Manufacture, Procurement, Fulfillment, Delivery, Sales, Sales Operations, Customer Service, Support, Deployment, Consulting, Take-Back and Recycling, Refurbishment and Supporting Functions of Technology Products, Services and Solutions

Activity

Location

Service, Support, Sales

Dell Technologies Inc.
Oklahoma Business Center - A & B
3501 S.W. 15th Street
Buildings A, B
Oklahoma City, Oklahoma 73108
USA
File No.: 19.5000/R1/M

Service, Support, Sales

Dell Technologies Inc.
Dell Canada Inc.
155 Gordon Baker Road
Suite 501
North York, Ontario M2H 3N5
Canada
File No.: 19.5000/R1/Q

Design/Development, Support

Dell Technologies Inc.
Dell Digital IT (DDIT)
401 Dell Way
Round Rock, TX 78682
USA
File No.: 19.5000/R1/Z

Support

Dell Technologies Inc.
Del Mall Real Cariari
600 MTS N. Zona Franca America
Heredia, Costa Rica S.A.
File No.: 19.5000/R1/GG

Design/Development

Dell Technologies Inc.
Dell Silicon Valley Design Center (SVDC)
5450 & 5480 Great America Parkway
Buildings 1 & 2
Santa Clara, CA 95054
USA
File No.: 19.5000/R1/JJ



Annex to Certificate Number: 19.5000

Scope of Registration:

The Design, Development, Manufacture, Procurement, Fulfillment, Delivery, Sales, Sales Operations, Customer Service, Support, Deployment, Consulting, Take-Back and Recycling, Refurbishment and Supporting Functions of Technology Products, Services and Solutions

Activity

Location

Design/Development, Service

Dell Technologies Inc.
176 South Street
Hopkinton, MA 01748
USA
File No.: 19.5000/R1/MM

Manufacture and Supply

Dell Technologies Inc.
EMC Corporation
5800 Technology Drive
Apex, NC 27539
USA
File No.: 19.5000/R1/QQ

Design/Development, Service

Dell Technologies Inc.
505 1st Avenue South
Seattle, WA 98104
USA
File No.: 19.5000/R1/UU

Manufacture and Supply

Dell Technologies Inc.
EMC Corporation
50 Constitution Blvd
Franklin, MA 02038
USA
File No.: 19.5000/R1/VV

Service

Dell Technologies Inc.
DELL EMC UTAH
13197 South Frontrunner Boulevard
Draper, UT 84020
USA
File No.: 19.5000/R1/XX



Annex to Certificate Number: 19.5000

Scope of Registration:

The Design, Development, Manufacture, Procurement, Fulfillment, Delivery, Sales, Sales Operations, Customer Service, Support, Deployment, Consulting, Take-Back and Recycling, Refurbishment and Supporting Functions of Technology Products, Services and Solutions

Activity

Location

Sales

Dell Technologies Inc.
Dell NV
BEWML164
Koningin Astridlaan 164
Equinox North
1780, Wemmel
Belgium
File No.: 19.5000/R2/A

Sales

Dell Technologies Inc.
Dell A/S
Arne Jacobsens Allé 15 -17
Copenhagen
Denmark
DK-2300
File No.: 19.5000/R2/C

Service, Support, Sales

Dell Technologies Inc.
Dell SAS
1 Rond Point,
Benjamin Franklin 34938
Montpellier 34000
France
File No.: 19.5000/R2/E

Service, Support, Sales

Dell Technologies Inc.
Dell SAS
River Ouest
80 Quai Voltaire
Bezons, 95870
France
File No.: 19.5000/R2/F



Annex to Certificate Number: 19.5000

Scope of Registration:

The Design, Development, Manufacture, Procurement, Fulfillment, Delivery, Sales, Sales Operations, Customer Service, Support, Deployment, Consulting, Take-Back and Recycling, Refurbishment and Supporting Functions of Technology Products, Services and Solutions

Activity

Location

Sales

Dell Technologies Inc.
Dell GmbH
Unterschweinstiege 10
60549 Frankfurt am Main
Germany
File No.: 19.5000/R2/H

Service, Support, Sales

Dell Technologies Inc.
Dell GmbH
Raffineriestraße 28
06112 Halle (Saale)
Germany
File No.: 19.5000/R2/I

Design/Development, Service,
Support, Sales

Dell Technologies Inc.
Dell Products Unlimited Company
Innovation House
Cherrywood Science & Technology Park
Cherrywood
Dublin 18, D18 XP84
Ireland
File No.: 19.5000/R2/J

Service, Support, Sales

Dell Technologies Inc.
Dell Products Unlimited Company
Raheen Business Park
Limerick
Ireland
File No.: 19.5000/R2/K



Annex to Certificate Number: 19.5000

Scope of Registration:

The Design, Development, Manufacture, Procurement, Fulfillment, Delivery, Sales, Sales Operations, Customer Service, Support, Deployment, Consulting, Take-Back and Recycling, Refurbishment and Supporting Functions of Technology Products, Services and Solutions

Activity

Location

Service, Support, Sales

Dell Technologies Inc.
Dell S.p.A.
Via Luisa Battistotti Sassi 11B
20133 Milano
Italy
File No.: 19.5000/R2/L

Service, Support, Sales

Dell Technologies Inc.
Dell SAS
Shore12
Casaneareshore Park
1100 Bd Qods
Sidi Maarouf
20270 Casablanca
Morocco
File No.: 19.5000/R2/M

Service, Support, Sales

Dell Technologies Inc.
Dell B.V.
Transformatorweg 12
38-72 1014, AK Amsterdam
Netherlands
File No.: 19.5000/R2/N

Service, Support, Sales

Dell Technologies Inc.
Dell AS
Lilleakerveien 2B, 0283
Oslo
NO-0275
Norway
File No.: 19.5000/R2/O



Annex to Certificate Number: 19.5000

Scope of Registration:

The Design, Development, Manufacture, Procurement, Fulfillment, Delivery, Sales, Sales Operations, Customer Service, Support, Deployment, Consulting, Take-Back and Recycling, Refurbishment and Supporting Functions of Technology Products, Services and Solutions

Activity

Location

Service, Support, Sales

Dell Technologies Inc.
Dell Corporation Ltd.
City Park
368 Alexandra Parade
Glasgow
G31 3AU
United Kingdom
File No.: 19.5000/R2/R

Service, Support, Sales

Dell Technologies Inc.
Dell s.r.o.
Fazulova 7
811 07
Bratislava, Slovak Republic
File No.: 19.5000/R2/S

Service, Support, Sales

Dell Technologies Inc.
Dell Computers S.A. (South Africa)
The Campus, Wembley Building, Ground Floor
Cnr Main and Sloan Streets
Bryanston 2021
Johannesburg
South Africa
File No.: 19.5000/R2/T

Sales

Dell Technologies Inc.
Dell AB
Frösundaviks Allé 1
SE-169 70
Solna
Sweden
File No.: 19.5000/R2/U



Annex to Certificate Number: 19.5000

Scope of Registration:

The Design, Development, Manufacture, Procurement, Fulfillment, Delivery, Sales, Sales Operations, Customer Service, Support, Deployment, Consulting, Take-Back and Recycling, Refurbishment and Supporting Functions of Technology Products, Services and Solutions

Activity

Location

Sales

Dell Technologies Inc.
Dell SA
Route de l'Aéroport 29-31
Case postale 216
1215 Genève 15
Switzerland CH-1215
File No.: 19.5000/R2/V

Service, Support, Sales

Dell Technologies Inc.
Dell Computer, S.A.U.
Calle Ribera del Loira n8
Paris Building
28042 Madrid
Spain
File No.: 19.5000/R2/W

Sales, Sales Support

Dell Technologies Inc.
Dell Corporation Ltd.
Dell House
1st & 2nd Floor
One Creechurch Place
London EC3A 5AF
United Kingdom
File No.: 19.5000/R2/X

Design/Development

Dell Technologies Inc.
Dell Technology & Solutions Israel Ltd.
7 Hamada Street
Herzliya 46733
Israel
File No.: 19.5000/R2/Z



Annex to Certificate Number: 19.5000

Scope of Registration:

The Design, Development, Manufacture, Procurement, Fulfillment, Delivery, Sales, Sales Operations, Customer Service, Support, Deployment, Consulting, Take-Back and Recycling, Refurbishment and Supporting Functions of Technology Products, Services and Solutions

Activity

Location

Sales, Sales Support

Dell Technologies Inc.
Dell Technology S.R.L.
George Constantinescu Street,
No. 4B and 2-4 lot 2,
Building B, District 2
Bucharest
Romania
File No.: 19.5000/R2/BB

Manufacture, Fulfillment

Dell Technologies Inc.
Dell Products (Poland) Sp.z.o.o.
Informatyczna Street No 1
92-410 Łódź
Poland
File No.: 19.5000/R2/DD

Manufacture and Supply

Dell Technologies Inc.
EMC Information Systems International
Unlimited Company
Unit B IDA Industrial Estate
Ovens
Co. Cork P31 D253
Ireland
File No.: 19.5000/R2/EE



Annex to Certificate Number: 19.5000

Scope of Registration:

The Design, Development, Manufacture, Procurement, Fulfillment, Delivery, Sales, Sales Operations, Customer Service, Support, Deployment, Consulting, Take-Back and Recycling, Refurbishment and Supporting Functions of Technology Products, Services and Solutions

Activity

Customer Support, Deploy Services
and Sales Operations

Location

Dell Technologies Inc.
EMC Egypt Service Center Limited
Dell Technologies Egypt Limited
90th Street no. 39
First Section City Center
New Cairo
Helwan
Egypt
&
El Sewedy Building
North 90th Street, Plot No. 39
5th District Centre
Cairo 11835
Egypt
File No.: 19.5000/R2/II

Design/Development, Sales,
Sales Support

Dell Technologies Inc.
EMC Information Systems International
Unlimited Company
IDA Industrial Estate
Ovens
Co. Cork P31 D253
Ireland
File No.: 19.5000/R2/JJ

Customer Service, Support, Sales,
Customer Care

Dell Technologies Inc.
Dell S.p.A.
Via Amsterdam, 125
00144 Roma
Italy
File No.: 19.5000/R2/KK



Annex to Certificate Number: 19.5000

Scope of Registration:

The Design, Development, Manufacture, Procurement, Fulfillment, Delivery, Sales, Sales Operations, Customer Service, Support, Deployment, Consulting, Take-Back and Recycling, Refurbishment and Supporting Functions of Technology Products, Services and Solutions

Activity

Location

Sales, Customer Service

Dell Technologies Inc.
Dell SA
EMC Computer Systems AG
Hardturmstrasse 161
8005 Zürich
Switzerland
File No.: 19.5000/R2/LL

Sales

Dell Technologies Inc.
Dell III – Comercio de Computadores,
Unipessoal Lda
Lagos Park Edificio 5B, 3º,
Andar 2740-298 Porto Salvo
Lisboa
Portugal
File No.: 19.5000/R2/MM

Service, Support

Dell Technologies Inc.
Dell Technology Products and Services
Single Member S.A.
90 Kifissias Avenue
15125 Maroussi
Athens
File No.: 19.5000/R2/NN

Sales

Dell Technologies Inc.
Dell Computer, spol. s r.o.
V Parku 2325/16
148 00 Prague 11 - Chodov
Czech Republic
File No.: 19.5000/R2/OO



Annex to Certificate Number: 19.5000

Scope of Registration:

The Design, Development, Manufacture, Procurement, Fulfillment, Delivery, Sales, Sales Operations, Customer Service, Support, Deployment, Consulting, Take-Back and Recycling, Refurbishment and Supporting Functions of Technology Products, Services and Solutions

Activity

Location

Design/Development, Sales

Dell Technologies Inc.
Dell Sp. z o.o.
4a Inflancka Street
1st & 8th Floor, Building A
Warsaw 00-189
Poland
File No.: 19.5000/R2/QQ

Service, Support, Sales

Dell Technologies Inc.
Dell Australia Pty Limited
The Zenith
Tower A, Levels 1-5
821-843 Pacific Highway
Chatswood, Sydney
New South Wales
2067
Australia
File No.: 19.5000/R3/A

Design/Development

Dell Technologies Inc.
Dell International Services India, Pvt. Ltd.
Bagmane Parin, Katha No.65/2,
Bagmane Tech Park, Byrasandra,
C.V. Raman Nagar,
Bengaluru 560093
India
File No.: 19.5000/R3/B



Annex to Certificate Number: 19.5000

Scope of Registration:

The Design, Development, Manufacture, Procurement, Fulfillment, Delivery, Sales, Sales Operations, Customer Service, Support, Deployment, Consulting, Take-Back and Recycling, Refurbishment and Supporting Functions of Technology Products, Services and Solutions

Activity

Location

Service, Support, Sales

Dell Technologies Inc.
Dell International Services India Pvt. Ltd.
Crystal Downs
Survey no. 7/1, 7/2, 7/3
Embassy Golf Links Business Park,
Off-Intermediate Ring Road, Domlur,
Challaghatta Village, Varthur Hobli,
Bengaluru Karnataka
560071 India
File No.: 19.5000/R3/C1

Manufacture, Delivery

Dell Technologies Inc.
Dell International Services India Pvt. Ltd.
M-4, SIPCOT Industrial Park
Sunguvarchatram Post, Sriperumbudur Taluk
Kancheepuram District
Tamil Nadu 602106
India
File No.: 19.5000/R3/E

Service, Support, Sales

Dell Technologies Inc.
Dell International Services India Pvt. Ltd.
Vipul Tech Square, Golf Course Road
Sector - 43, Gurgaon
Haryana 122 002
India
File No.: 19.5000/R3/F

Sales, Sales Support

Dell Technologies Inc.
Dell International Services India Pvt. Ltd.
Plot No. 42
HITEC City Layout
Madhapur, Hyderabad
Telangana 500081
India
File No.: 19.5000/R3/G



Annex to Certificate Number: 19.5000

Scope of Registration:

The Design, Development, Manufacture, Procurement, Fulfillment, Delivery, Sales, Sales Operations, Customer Service, Support, Deployment, Consulting, Take-Back and Recycling, Refurbishment and Supporting Functions of Technology Products, Services and Solutions

Activity

Location

Service, Support, Sales

Dell Technologies Inc.
Dell Technologies Japan Inc.
Miyazaki Customer Center
Carino Miyazaki 5F
4-8-1 Tachibana-dori-Higashi
Miyazaki-shi
Miyazaki, Japan
880-0805
File No.: 19.5000/R3/J

Customer Service, Delivery Service,
Customer Care, Inside Sales, Support

Dell Technologies Inc.
Dell Technologies Japan Inc.
Headquarters
Otemachi One Tower 17F
1-2-1 Otemachi, Chiyoda-ku,
Tokyo 1008159
Japan
File No.: 19.5000/R3/K

Customer Service, Delivery Service,
Customer Care, Inside Sales

Dell Technologies Inc.
Dell Global Business Centre Sdn. Bhd.
(Cyberjaya)
2900 Persiaran APEC, Floor 1-4
63000 Cyberjaya. Selangor Darul Ehsan
Malaysia
File No.: 19.5000/R3/L

Service, Support, Sales

Dell Technologies Inc.
Dell Global Business Center Sdn. Bhd.
(742481-H)
Plot P27, Bayan Lepas Industrial Zone
Phase IV 11900
Bayan Lepas
Penang
Malaysia
File No.: 19.5000/R3/M



Annex to Certificate Number: 19.5000

Scope of Registration:

The Design, Development, Manufacture, Procurement, Fulfillment, Delivery, Sales, Sales Operations, Customer Service, Support, Deployment, Consulting, Take-Back and Recycling, Refurbishment and Supporting Functions of Technology Products, Services and Solutions

Activity

Location

Service, Manufacturing, Fulfillment, Delivery

Dell Technologies Inc.
Dell Global Business Center Sdn. Bhd. (APCC)
Plot 76
Mukim 11
Bukit Tengah Industrial Park
14000 Bukit Mertajam
Pulau Pinang
Malaysia
File No.: 19.5000/R3/N

Service, Support, Sales

Dell Technologies Inc.
Dell International Services Philippines, Inc.
17th Floor World Plaza Building
5th Avenue Bonifacio Global City
Taguig City, 1634
Philippines
File No.: 19.5000/R3/O

Sales, Sales Support

Dell Technologies Inc.
Dell (China) Co. Ltd.
Beijing Branch
Unit 507, 5/F, Tower A
Full Link Plaza No.18
Chao Yang Menwai Avenue
Beijing
China 100020
File No.: 19.5000/R3/P

Sales, Sales Support

Dell Technologies Inc.
Dell (China) Co. Ltd.
Dell (Xiamen) Co. Ltd.
Dalian Branch
IC Building,
No. 56 Huoju Road,
Hi-Tech Industrial Zone
Dalian China 116023
File No.: 19.5000/R3/Q



Annex to Certificate Number: 19.5000

Scope of Registration:

The Design, Development, Manufacture, Procurement, Fulfillment, Delivery, Sales, Sales Operations, Customer Service, Support, Deployment, Consulting, Take-Back and Recycling, Refurbishment and Supporting Functions of Technology Products, Services and Solutions

Activity

Location

Manufacture, Fulfillment, Sales,
Service, Support

Dell Technologies Inc.
Dell (China) Co. Ltd. (CCC2)
Dell (Xiamen) Co. Ltd. (CCC4)
Nos. 2388 & 2366 Jinshang Road
Information Photo-Electronic Park
Xiamen Torch Hi-Tech Zone
Fujian
China 361011
File No.: 19.5000/R3/T

Design, Development

Dell Technologies Inc.
Dell International Services India Pvt. Ltd.
Dell Networking Research and Development
8th & 9th Floor
Fortius Block
Olympia Tech Park, Plot No:1
SIDCO Industrial Estate
Guindy, Chennai
Tamil Nadu 600032
India
File No.: 19.5000/R3/T3

Sales, Service, Support

Dell Technologies Inc.
Dell (China) Co. Ltd. (CCC5)
No. 613 Sishui Road
Haicang Building #1
Wuyuan Bay
Business Operation Center
Xiamen Fujian
China 361015
File No.: 19.5000/R3/U2



Annex to Certificate Number: 19.5000

Scope of Registration:

The Design, Development, Manufacture, Procurement, Fulfillment, Delivery, Sales, Sales Operations, Customer Service, Support, Deployment, Consulting, Take-Back and Recycling, Refurbishment and Supporting Functions of Technology Products, Services and Solutions

Activity

Location

Design/Development, Service, Support

Dell Technologies Inc.
Dell Taiwan B.V.
Taiwan Branch
No. 216 and No. 218, Sec. 2
Tun Hua S. Road
Taipei
Taiwan, R.O.C.
File No.: 19.5000/R3/V

Service, Support, Customer Care, Sales

Dell Technologies Inc.
Dell International Inc. (Korea)
Gangnam Finance Center,
17th, 18th Floors,
152 Teheran-ro, Gangnam-Gu
Seoul, Republic of Korea
06236
File No.: 19.5000/R3/Y

Design/Development, Sales, Sales Support

Dell Technologies Inc.
Dell Global B.V. (Singapore Branch)
Singapore Design Center
2 International Business Park
The Strategy Tower 2, #01-34
Singapore 609930
File No.: 19.5000/R3/Z

Sales

Dell Technologies Inc.
Dell Corporation (Thailand) Co., Ltd.
22nd Floor Empire Tower
1 South Sathorn Road
Yannawa, Sathorn
Bangkok 10120
Thailand
File No.: 19.5000/R3/BB



Annex to Certificate Number: 19.5000

Scope of Registration:

The Design, Development, Manufacture, Procurement, Fulfillment, Delivery, Sales, Sales Operations, Customer Service, Support, Deployment, Consulting, Take-Back and Recycling, Refurbishment and Supporting Functions of Technology Products, Services and Solutions

Activity

Location

Manufacture, Fulfillment

Dell Technologies Inc.
Dell (Chengdu) Company Limited
No. 800 Tianqin Road
Hi-Tech Zone West
Chengdu
Sichuan 611731
China
File No.: 19.5000/R3/NN

Design/Development, Service,
Support

Dell Technologies Inc.
Dell International Services India Pvt. Ltd.
Moonstone - Block B
Bagmane World Technology Centre - SEZ
Krishnarajapuram Marathahalli Outer Ring
Road
Mahadevapura, Dodannekundi Village
Bengaluru, Karnataka
560048
India
File No.: 19.5000/R3/SS

Design/Development

Dell Technologies Inc.
Dell International Services India Pvt. Ltd.
9th Floor, No.154/6, IT8 & IT-9, M/S
Qubix SEZ,
Rajiv Gandhi Infotech Park,
Hinjewadi Phase-1,
Pune, Maharashtra
411 057
India
File No.: 19.5000/R3/TT



Annex to Certificate Number: 19.5000

Scope of Registration:

The Design, Development, Manufacture, Procurement, Fulfillment, Delivery, Sales, Sales Operations, Customer Service, Support, Deployment, Consulting, Take-Back and Recycling, Refurbishment and Supporting Functions of Technology Products, Services and Solutions

Activity

Location

Design/Development

Dell Technologies Inc.
EMC Information Technology
Research & Development (Beijing) Co., Ltd.
8 & 19/F, Block D, Qidi Science Park, No.1
Zhongguancun East Road,
Haidian District,
Beijing 100084
China
File No.: 19.5000/R3/VV

Design/Development

Dell Technologies Inc.
EMC Information Technology
Research & Development (Chengdu) Co., Ltd.
17-18/F Building C11
Tianfu Software Park,
No.219 Tianhua Second Street, Hi-Tech Zone,
Chengdu, 610041 China
File No.: 19.5000/R3/YY

Design/Development, Sales, Support

Dell Technologies Inc.
EMC Information Technology
Research & Development (Shanghai) Co., Ltd.
3-5F, Building #1, KIC Plaza, No.234
2-3F, Building #2, KIC Plaza, No.252
2-3F, Building #5, KIC Plaza, No.316
Songhu Road, Yangpu District
Shanghai, 200433
China
File No.: 19.5000/R3/ZZ

**Verified by:
Technical Operations Officer**



NSAI

Certificate of Registration of Environmental Management System to ISO 14001:2015

The National Standards Authority of Ireland Inc. certifies that:

**Dell Technologies Inc.
Dell Marketing L.P.
One Dell Way
Round Rock, TX 78682
USA**

has been assessed and deemed to comply with the
requirements of the above standard in respect of the scope of
operations given below:

**The Development, Manufacture, Supply, and
Takeback Services of Computers, Storage and
Server Products and Technology Products.**

**Additional sites covered under this multi-site certification are listed on the
Annex. (File No. 14.5000)**

Geraldine Larkin
Chief Executive Officer

Lisa Greenleaf
Technical Operations Officer

Registration Number: 14.5000
Certification Granted: January 25, 2011
Effective Date: January 25, 2026
Expiry Date: January 24, 2029





National Standards Authority of Ireland Inc., 20 Trafalgar Square, Nashua, New Hampshire, NH 03063, USA T +1 603 882 4412

Annex to Certificate Number: 14.5000

Scope of Registration:

The Development, Manufacture, Supply, and Takeback Services of Computers, Storage and Server Products and Technology Products.

Activity

Location

Central Function, Manufacture and Supply, Takeback Services, Product Development

Dell Technologies Inc.
Dell Marketing L.P.
One Dell Way
Round Rock, TX 78682
USA
File No.: 14.5000

Manufacture and Supply

Dell Technologies Inc.
Dell Computadores do Brasil Ltda.
(BRH1)
Av da. Emancipação, 5000
Hortolândia
SP 13.184-654
Brazil (Brasil)
File No.: 14.5000/R1/A

Global Product Environmental Lifecycle Management

Dell Technologies Inc.
(Product Development)
One Dell Way
Round Rock, TX 78682
USA
File No.: 14.5000/R1/S

Global Product Environmental Lifecycle Management

Dell Technologies Inc.
(Takeback Services)
One Dell Way
Round Rock, Texas 78682
USA
File No.: 14.5000/R1/EE

Manufacture and Supply

Dell Technologies Inc.
EMC Corporation
5800 Technology Drive
Apex, NC 27539
USA



File No.: 14.5000/R1/QQ

Annex to Certificate Number: 14.5000

Scope of Registration:

The Development, Manufacture, Supply, and Takeback Services of Computers, Storage and Server Products and Technology Products.

Activity

Location

Manufacture and Supply

Dell Technologies Inc.
EMC Corporation
50 Constitution Blvd
Franklin, MA 02038
USA
File No.: 14.5000/R1/VV

Manufacture and Supply

Dell Technologies Inc.
Dell Products (Poland) Sp.z.o.o.
Informatyczna Street No 1
92-410 Łódź
Poland
File No.: 14.5000/R2/DD

Manufacture and Supply

Dell Technologies Inc.
EMC Information Systems International
Unlimited Company
Unit B IDA Industrial Estate
Ovens
Co. Cork P31 D253
Ireland
File No.: 14.5000/R2/EE

Manufacture and Supply

Dell Technologies Inc.
Dell International Services India Pvt. Ltd.
M-4, SIPCOT Industrial Park
Sunguvarchatram Post, Sriperumbudur
Taluk
Kancheepuram District
Tamil Nadu 602106
India
File No.: 14.5000/R3/E



Annex to Certificate Number: 14.5000

Scope of Registration:

The Development, Manufacture, Supply, and Takeback Services of Computers, Storage and Server Products and Technology Products.

Activity

Location

Manufacture and Supply

Dell Technologies Inc.
Dell Global Business Center Sdn. Bhd.
(APCC)
Plot 76
Mukim 11
Bukit Tengah Industrial Park
14000 Bukit Mertajam
Pulau Pinang
Malaysia
File No.: 14.5000/R3/N

Manufacture and Supply

Dell Technologies Inc.
Dell (China) Co. Ltd. (CCC2)
Dell (Xiamen) Co. Ltd. (CCC4)
Nos. 2388 & 2366 Jinshang Road
Information Photo-Electronic Park
Xiamen Torch Hi-Tech Zone
Fujian
China 361011
File No.: 14.5000/R3/T

Manufacture and Supply

Dell Technologies Inc.
Dell (Chengdu) Company Limited
No. 800 Tianqin Road
Hi-Tech Zone West
Chengdu
Sichuan 611731
China
File No.: 14.5000/R3/NN

Verified by:



Technical Operations Officer



Certificate of Registration of Information Security Management System to ISO 27001:2022

The National Standards Authority of Ireland Inc. certifies that:

**Dell Technologies Inc.
Dell Marketing L.P.
One Dell Way
Round Rock, TX 78682
USA**

has been assessed and deemed to comply with the requirements of the above standard in respect of the scope of operations given below:

The Information Security Management System for Dell Technologies Inc. encompasses activities which enable the protection of information assets across the enterprise including Dell Technology Services (DTS), Sales, Dell Financial Services (DFS), Dell Infrastructure Solutions Group (ISG) and supporting functions inclusive of the Security & Resiliency Organization (SRO); Dell IT; Facilities Management, Human Resources and Legal, in accordance with the Statement of Applicability, Version 9.1.

Additional sites covered under this multi-site certification are listed on the Annex. (File No. 27.5000)

Geraldine Larkin
Chief Executive Officer

Lisa Greenleaf
Technical Operations Officer

Registration Number: 27.5000
Certification Granted: January 05, 2022
Effective Date: October 29, 2025
Expiry Date: January 04, 2028





Annex to Certificate Number: 27.5000

Scope of Registration:

The Information Security Management System for Dell Technologies Inc. encompasses activities which enable the protection of information assets across the enterprise including Dell Technology Services (DTS), Sales, Dell Financial Services (DFS), Dell Infrastructure Solutions Group (ISG) and supporting functions inclusive of the Security & Resiliency Organization (SRO); Dell IT; Facilities Management, Human Resources and Legal, in accordance with the Statement of Applicability, Version 9.1.

Activity

Location

Central Function

Dell Technologies Inc.
Dell Marketing L.P.
One Dell Way
Round Rock, TX 78682
USA
File No.: 27.5000

The Information Security Management System for Dell Technologies Inc. encompasses activities which enable the protection of information assets across the enterprise including Dell Technology Services (DTS), Sales, Dell Financial Services (DFS), Dell Infrastructure Solutions Group (ISG) and supporting functions inclusive of the Security & Resiliency Organization (SRO); Dell IT; Facilities Management, Human Resources and Legal, in accordance with the Statement of Applicability, Version 9.1.

The provision of Managed Services.

Dell Technologies Inc.
176 South St.
Hopkinton, MA 01748
USA
File No.: 27.5000/R1/MM

Global Design and Development of Dell AIOps.

Dell Technologies Inc.
62 TW Alexander Drive
Research Triangle Park
Durham, NC 27709
USA
File No.: 27.5000/R1/NN



Annex to Certificate Number: 27.5000

Scope of Registration:

The Information Security Management System for Dell Technologies Inc. encompasses activities which enable the protection of information assets across the enterprise including Dell Technology Services (DTS), Sales, Dell Financial Services (DFS), Dell Infrastructure Solutions Group (ISG) and supporting functions inclusive of the Security & Resiliency Organization (SRO); Dell IT; Facilities Management, Human Resources and Legal, in accordance with the Statement of Applicability, Version 9.1.

Activity

Location

The provision of Managed Services and Supporting Services for as-a-service offers.

Dell Technologies Inc.
13197 South Frontrunner Boulevard
Draper, UT 84020
USA
File No.: 27.5000/R1/XX

The provision of Managed, Professional and Field Services.

Dell Technologies Inc.
Dell Corporation Limited
1st & 2nd Floor
One Creechurch Place
London EC3A 5AF
United Kingdom
File No.: 27.5000/R2/A

Provision of Professional Services and Field Support Services.

Dell Technologies Inc.
Dell SAS
1 Rond Point Benjamin Franklin
34000 Montpellier
France
File No.: 27.5000/R2/E

The provision of Professional & Field Services.

Dell Technologies Inc.
Dell GmbH
Unterschweinstiege 10
Frankfurt am Main
60549
Germany
File No.: 27.5000/R2/H



Annex to Certificate Number: 27.5000

Scope of Registration:

The Information Security Management System for Dell Technologies Inc. encompasses activities which enable the protection of information assets across the enterprise including Dell Technology Services (DTS), Sales, Dell Financial Services (DFS), Dell Infrastructure Solutions Group (ISG) and supporting functions inclusive of the Security & Resiliency Organization (SRO); Dell IT; Facilities Management, Human Resources and Legal, in accordance with the Statement of Applicability, Version 9.1.

Activity

Location

The Provision of Professional Services, Field Services, Sales and Supporting functions.

Dell Technologies Inc.
Dell S.p.A.
Dell Soluzioni Finanziarie S.r.l.
Via Luisa Battistotti Sassi 11
Milano 20133
Italy
File No.: 27.5000/R2/L

The Provision of Professional and Field Services

Dell Technologies Inc.
Dell Computer, S.A.U.
Calle Ribera del Loira n8
Paris Building
28042 Madrid
Spain
File No.: 27.5000/R2/W

The Provision of Professional Services, Managed Services and Global Asset Management.

Dell Technologies Inc.
EMC Egypt Service Center Limited
Dell Technologies Egypt Limited
90th Street no. 39
First Section City Center
New Cairo
Helwan
Egypt
&
El Sewedy Building
North 90th Street, Plot No. 39
5th District Centre
Cairo 11835
Egypt
File No.: 27.5000/R2/II



Annex to Certificate Number: 27.5000

Scope of Registration:

The Information Security Management System for Dell Technologies Inc. encompasses activities which enable the protection of information assets across the enterprise including Dell Technology Services (DTS), Sales, Dell Financial Services (DFS), Dell Infrastructure Solutions Group (ISG) and supporting functions inclusive of the Security & Resiliency Organization (SRO); Dell IT; Facilities Management, Human Resources and Legal, in accordance with the Statement of Applicability, Version 9.1.

Activity

Location

The provision of Managed Services: Global Services Site Reliability Engineering (SRE) and Global Design and Development supporting cloud services and as-a-service offers.

Dell Technologies Inc.
EMC Information Systems International
Unlimited Company
IDA Industrial Estate
Ovens, Co. Cork P31 D253
Ireland
File No.: 27.5000/R2/JJ

The provision of Professional & Field Services.

Dell Technologies Inc.
Dell SA
Hardturmstrasse 161
8005 Zürich
Switzerland
File No.: 27.5000/R2/LL

The provision of payment solutions to end users of products and services sold by Dell Technologies.

Dell Technologies Inc.
Dell Products Unlimited Company
Dell Bank International Designated Activity
Company
Innovation House
Cherrywood Science & Technology Park
Cherrywood
Dublin 18, D18 XP84
Ireland
File No.: 27.5000/R2/MM



Annex to Certificate Number: 27.5000

Scope of Registration:

The Information Security Management System for Dell Technologies Inc. encompasses activities which enable the protection of information assets across the enterprise including Dell Technology Services (DTS), Sales, Dell Financial Services (DFS), Dell Infrastructure Solutions Group (ISG) and supporting functions inclusive of the Security & Resiliency Organization (SRO); Dell IT; Facilities Management, Human Resources and Legal, in accordance with the Statement of Applicability, Version 9.1.

Activity

Location

The provision of Managed Services.

Dell Technologies Inc.
Dell GmbH
Osterfeldstrasse 84
Ismaning
85737
Germany
File No.: 27.5000/R2/PP

The provision of Managed Services.

Dell Technologies Inc.
Dell International Services India Pvt. Ltd.
9th Floor, No.154/6, IT8 & IT-9, M/S Qubix
SEZ,
Rajiv Gandhi Infotech Park,
Hinjewadi Phase-1,
Pune, Maharashtra
411 057
India
File No.: 27.5000/R3/A

The provision of Managed Services.

Dell Technologies Inc.
Dell Australia Pty Limited
The Zenith
Tower A, Levels 1-5
821-843 Pacific Highway
Chatswood, Sydney
New South Wales
2067
Australia
File No.: 27.5000/R3/B



Annex to Certificate Number: 27.5000

Scope of Registration:

The Information Security Management System for Dell Technologies Inc. encompasses activities which enable the protection of information assets across the enterprise including Dell Technology Services (DTS), Sales, Dell Financial Services (DFS), Dell Infrastructure Solutions Group (ISG) and supporting functions inclusive of the Security & Resiliency Organization (SRO); Dell IT; Facilities Management, Human Resources and Legal, in accordance with the Statement of Applicability, Version 9.1.

Activity

Location

Activities of Dell Technologies Japan, including Sales and Service of Dell Technologies Products.

Dell Technologies Inc.
Dell Technologies Japan Inc.
Headquarters
Otemachi One Tower 17F
1-2-1 Otemachi,
Chiyoda-ku,
Tokyo
1008159
Japan
File No.: 27.5000/R3/I

Activities of Dell Technologies Japan, including Sales and Service of Dell Technologies Products.

Dell Technologies Inc.
Dell Technologies Japan Inc.
Miyazaki Customer Center
Carino Miyazaki 5F
4-8-1 Tachibana-dori-Higashi,
Miyazaki-shi,
Miyazaki
880-0805
Japan
File No.: 27.5000/R3/J



Annex to Certificate Number: 27.5000

Scope of Registration:

The Information Security Management System for Dell Technologies Inc. encompasses activities which enable the protection of information assets across the enterprise including Dell Technology Services (DTS), Sales, Dell Financial Services (DFS), Dell Infrastructure Solutions Group (ISG) and supporting functions inclusive of the Security & Resiliency Organization (SRO); Dell IT; Facilities Management, Human Resources and Legal, in accordance with the Statement of Applicability, Version 9.1.

Activity

Location

The provision of Managed Services.

Dell Technologies Inc.
Dell Global Business Center Sdn. Bhd.
Cyberjaya 1
Global Business Center
2900 Persiaran APEC
Floors 1-4
63000 Cyberjaya
Selangor Darul Ehsan
Malaysia
File No.: 27.5000/R3/L

The provision of Managed Services
and CSG Support Services.

Dell Technologies Inc.
Dell (China) Co. Ltd.
Dell (Xiamen) Co. Ltd.
Dalian Branch
IC Building,
No. 56 Huoju Road,
Hi-Tech Industrial Zone
Dalian China 116023
File No.: 27.5000/R3/Q



Annex to Certificate Number: 27.5000

Scope of Registration:

The Information Security Management System for Dell Technologies Inc. encompasses activities which enable the protection of information assets across the enterprise including Dell Technology Services (DTS), Sales, Dell Financial Services (DFS), Dell Infrastructure Solutions Group (ISG) and supporting functions inclusive of the Security & Resiliency Organization (SRO); Dell IT; Facilities Management, Human Resources and Legal, in accordance with the Statement of Applicability, Version 9.1.

Activity

Location

The provision of Managed Services.

Dell Technologies Inc.
Dell International Services India Pvt. Ltd.
Moonstone - Block B
Bagmane World Technology Centre - SEZ
Krishnarajapuram Marathahalli Outer
Ring Road
Mahadevapura, Dodanekundi Village
Bengaluru, Karnataka
560048
India
File No.: 27.5000/R3/SS

Provision of Configuration Services,
Technical Support, Global Command
Center, Account Management
Services, Infrastructure Delivery
Services, Global Field Services,
Global Service Parts Planning and
Operations.

Dell Technologies Inc.
Dell (China) Company Limited
No. 2388 Jinshang Road,
Xiamen, Fujian
China 361009 (CCC2)
&
No. 37-1, Banshang She, Building 1, Xinke
Plaza, Torch Hi-Tech Zone,
Xiamen, Fujian
China 361009 (CCC7)
File No.: 27.5000/R3/U2

Verified by:
Technical Operations Officer

Online Browsing Platform (OBP)



Sign in

Language ▾

Help ▾

Search

Search

ISO/IEC 19678:2015(en) ×

ISO/IEC 19678:2015(en) Information Technology — BIOS Protection Guidelines

Table of contents

Foreword

Introduction

1 Scope

2 Conformance

3 Normative references

4 Terms and definitions

5 Symbols (and abbreviated terms)

▼ 6 Background

6.1 System BIOS

▶ 6.2 Role of system BIOS in the boot process

6.3 Updating the system BIOS

6.4 Importance of BIOS integrity

6.5 Threats to the system BIOS

▼ 7 Threat mitigation

7.1 Overview

▶ 7.2 Security requirements for system BIOS

▶ 7.3 Recommended practices for BIOS recovery

Bibliography

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) are the two international organizations responsible for the development of International Standards through technical committees established by the respective organs and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental or non-governmental, in liaison with ISO and IEC, also take part in the work. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of the joint technical committee is to prepare International Standards for publication. The project is initiated by a proposal from a member body of the joint technical committee and the project is approved by the joint technical committee. The project is then developed by the joint technical committee and the project is approved by the joint technical committee. Publication of an International Standard requires the approval of a 75 % of the national bodies casting a vote.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO and IEC accept no liability for any loss or damage caused by the use of the information contained in this document.

Note: ITTF will provide the document number needed below

ISO/IEC 19678 was prepared by the U.S. National Institute of Standards and Technology (NIST) in accordance with the requirements of the NIST publication (available at <http://csrc.nist.gov/publications/nistpubs/800-147>). The NIST publication was adopted under a special “fast-track procedure”, by Joint Technical Committee 1, in parallel with its approval by the national bodies of ISO and IEC.

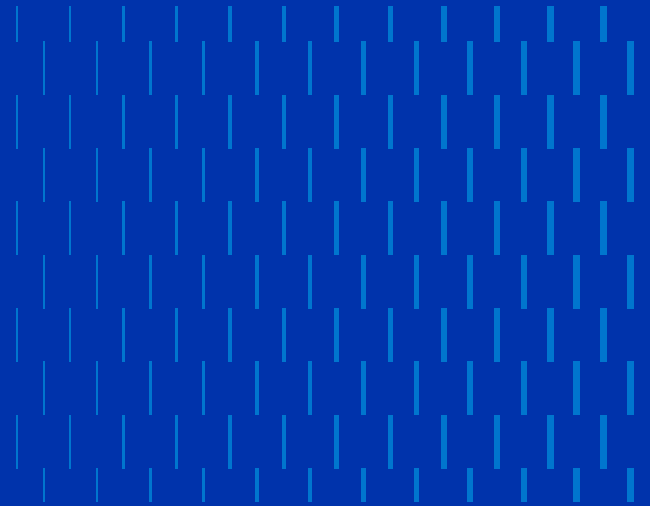
Introduction

Modern computers rely on fundamental system firmware, commonly known as BIOS, to facilitate the hardware initialization process and transition control to the operating system. Original equipment manufacturers (OEMs) and independent BIOS vendors, as well as manufacturers, frequently update system firmware to fix bugs, improve performance, and add new features. This International Standard provides security requirements and guidance for preventing unauthorized modification of BIOS in PC client systems.

Unauthorized modification of BIOS firmware by malicious software constitutes a security vulnerability. A malicious BIOS modification can be used to either a permanent denial of service (if the BIOS is corrupted) or to gain access to the system's resources.

Figures

Client Solutions Dell Trusted Device: BIOS Security



A deep dive into the foundational, BIOS-level security of Dell Trusted Devices, the world's most secure commercial AI PCs*

May 2025



© 2025 Dell Inc. or its subsidiaries. All Rights Reserved. Dell, EMC and other trademarks are trademarks of Dell Inc. or its subsidiaries. Other trademarks may be trademarks of their respective owners.

*Based on Dell internal analysis, October 2024. Applicable to PCs on Intel processors. Not all features available with all PCs. Additional purchase required for some features. Validated by Principled Technologies. [A comparison of security features](#), April 2024.

Table of Contents

Introduction 4

The Key Elements of Dell Built-In Security..... 6

The Role of BIOS (and what is UEFI?) 6

Secure Design Processes and SDL 7

Supply Chain Security 7

Industry Affiliations 8

Built-In, “Below the OS” Security..... 9

Dell Trusted Device (DTD) Application..... 10

The Importance of Built-In Security 10

Intel® vPro Additions to Built-In Security 11

Understanding Dell Cybersecurity Using the NIST Framework 11

Identify 12

 Device Identity 13

 User Identity: Dell SafeID..... 14

 “Below the OS” Threat Modeling 16

Protect..... 16

 Protecting the PC Boot Process..... 17

 Securing the Boot Chain 17

 The “Root of Trust” 18

 TCG and the Root of Trust 18

 UEFI Secure Boot..... 18

 UEFI Secure Boot Expert Mode 19

 Signed Firmware Update..... 19

 NIST SP800-147 Support 20

 System Management Mode (SMM) 20

 BIOS Patch Management..... 22

 BIOS Downgrade Protection 23

 Embedded Controller: Signed Firmware 23

 Protecting BIOS Configuration 23

 Configuration Side-Channels 25

 Best Practices for Secure Configuration 26

 Protecting BIOS at Runtime 26

Runtime BIOS Resilience.....	26
Detect.....	27
Intel Boot Guard.....	27
Intel Management Engine (ME) Firmware Verification.....	28
Hardware-Assisted Security with CrowdStrike and Intel.....	29
Intel® vPro Integration for Out of Band Management.....	29
Microsoft Intune Integration.....	30
Other Integrations for SafeBIOS.....	30
SafeBIOS Indicators of Attack.....	30
Common Vulnerabilities and Exposures (CVE) Detection.....	32
TCG Measured Boot.....	32
Code, Configuration, and the TPM Event Log.....	32
NIST 800-155 Measurements.....	33
Advanced: NIST 800-155 Measurements Extraction, Conversion, and Comparison.....	34
Physical Security Features – Chassis Intrusion.....	35
Respond and Recover.....	35
Embedded Controller Recovery.....	36
BIOS Recovery.....	36
BIOS Recovery Image Update Flow.....	37
Auto Recovery Flow.....	38
Customer Flexibility: Manual Recovery.....	38
SafeBIOS Image Capture.....	38
Dell Data Wipe.....	38
Additional Dell Security Capabilities.....	39
Protected Signing Infrastructure.....	39
The Future of Security.....	40
References.....	40
Dell and Partner References.....	40
Industry Organizations.....	41
Standards and Guidelines.....	41
Quoted Stats.....	41

Introduction

Computer security is a multi-billion-dollar business with thousands of companies competing for organizations' attention and enterprise dollars, and with good reason: it can provide a healthy payday for the attacker. The cost of cybercrime worldwide continues to grow at a brisk rate – [from \\$5.49 trillion USD in 2021 to an estimated \\$8.15 trillion USD in 2023](#). Governments are also witnessing growing nation-state level cyberattacks, as countries do battle using these weapons of warfare. The increasing adoption of zero trust methodologies and architectures reinforces that security remains a fundamental aspect of ensuring that an organization can secure its key assets and prevent the damage that even a simple cyberattack can wreak upon its operations.

One of the most critical and fundamental tenets in computer security is transparency. Though highly effective, security features deeply embedded within a client are not always visible. The intent of this publication is to provide transparency into the Dell device security features and technology implementations as provided and enforced by the code responsible for device boot and other fundamental device functions, which we refer to as our BIOS (Basic Input/Output System).

Dell Technologies has created [Dell Trusted Workspace](#), an innovative and effective portfolio of technologies and solutions – both hardware and software – in this industry to help organizations strive to secure their enterprises. One of the areas where Dell has substantially invested over the last decade is in the security of the endpoint itself, in this case the “client” device (desktops, workstations, and notebooks). The collection of innovative ‘built-in’ security features native to Dell hardware strengthens the ability of Dell client devices to detect, respond to and mitigate stealthy attacks which operate below the purview of the operating system – or ‘below-the-OS’ as it is often called. Dell takes this a step further through integration with software (EDR/XDR and SIEM) and device management solutions such as Microsoft Intune to enable organizations to take appropriate action and analyze a threat to improve response effectiveness.

Since this paper was originally published, Dell device security has expanded to include additional built-in security features from Intel® vPro. Though mention will be made, for more in-depth information there is a separate paper dedicated to those features that may be [downloaded here](#).

Even with the latest news about the increase in cyberattacks, there are still organizations that believe that security equals encryption plus antivirus, and that software is all it takes to be secure. They may recognize and appreciate Dell's significant investment in endpoint security but question the need. Why don't firewalls, IDS/IPS, SIEMs, NGAV, EDR and all the various alphabet soup of enterprise-level security tools already cover everything?

Well, those tools may be good at what they do. But they don't do everything. Dell believes that overall infrastructure security not only depends on these tools but also on the built-in security of each endpoint. From this perspective, the endpoints, and subsequently each individual device, collectively become the foundation of security for the entire enterprise. Further, as attackers develop more stealthy threats which work at the hardware level, existing security software simply isn't enough to detect and respond to them. Hardware-generated telemetry such as that provided by the Dell Trusted Device (DTD) Application provides a valuable source of information that can be used to offset these increasing threat vectors – in essence, built-in security. This domain can only be implemented and supported by the OEM, and Dell continues to advance the abilities of its products to protect, detect, respond, and recover from cyberattacks.

This paper was written to provide a thorough introduction to the Dell device BIOS security features and hardening. The BIOS remains an extremely important component in a modern PC, and some of the more foundational (and critical) security hardening aspects of the device start with and depend on the BIOS. This document will unwrap the terminology and lexicon that has tightly attached itself to this area of technology and explain the individual features and components of the BIOS that help to secure enterprise infrastructure from the device up to the cloud.

The audience for this document includes security operation center (SoC) analysts, IT admins and decision makers (ITDMs), IT support personnel, compliance and risk/governance teams, security researchers and analysts, and anyone else interested in learning more about the built-in security offered by the Dell devices via security and hardening of the underlying BIOS and firmware.

Contextually this document is broken into sections that map to specific outcomes described in the [NIST Cybersecurity Framework \(CSF\)](#): Identify, Protect, Detect, Respond and Recover. This should help put each feature included in Dell devices into the perspective of the overall goal of helping to secure each organization's enterprise.

- **Identify:** Develop an organizational understanding to manage cybersecurity risk to systems, people, assets, data, and capabilities. Within the Dell security schema, this refers to tools to help customers categorize these classifications, including asset management and those secure design principles which proactively contribute to security (e.g., Dell Service Tag, Dell SafeID, Threat Modeling).
- **Protect:** Develop and implement appropriate safeguards to ensure delivery of critical services. These include defensive technologies to harden non-volatile storage and the boot process (e.g., Signed Firmware Update, BIOS Passwords).
- **Detect:** Develop and implement appropriate activities to identify the occurrence of a cybersecurity event. This includes the ability to convey status when unauthorized changes occur (e.g., SafeBIOS Verification, Intel® Boot Guard).
- **Respond:** Develop and implement appropriate activities to respond to a detected cybersecurity incident. Action is taken by the organization using tools and data (telemetry) provided by Dell capabilities described in this paper.
- **Recover:** Develop and implement appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity incident. This includes advanced mitigations to quickly remediate issues (e.g., BIOS Recovery, Dell Data Wipe).

Govern was introduced in the 2024 version of the CSF and intended to underlie each of these activities, which are critical for incorporating cybersecurity into an organization's broader enterprise risk management (ERM) strategy. From the perspective of an OEM like Dell, Govern concerns work to be performed by the customer organization to understand organizational context; establish cybersecurity strategy and cybersecurity supply chain risk management; roles, responsibilities, and authorities; policy; and provide for the oversight of cybersecurity strategy. It is not covered in the scope of this document, although it is essential for any organization seeking to implement and manage a robust cybersecurity strategy.

This document concludes with a brief section on our commitment to the ongoing Dell investments helping to shape the future of security. This document is not the end of the conversation about Dell device security; hopefully it's the continuation of a long and bi-directional discourse beneficial to the industry overall.

The Key Elements of Dell Built-In Security

The Role of BIOS (and what is UEFI?)

The "BIOS" in a modern PC remains one of the most misunderstood components of the firmware and software stack. The mere mention of "BIOS" to anyone that's been in the industry for more than a decade evokes memories of resetting the CMOS battery or toggling jumpers on the motherboard to make configuration changes. Many still refer to the BIOS configuration menu, or "BIOS Setup" as the BIOS, but there is so much more to it than that!

For the purposes of this document, the BIOS refers to the pre-boot firmware that the main processor executes at the beginning of every boot and any code that remains resident at runtime that was deployed by the pre-boot firmware. The role of this pre-boot firmware is to initialize memory, configure chipset and discrete devices on the motherboard, provide PC OEM unique features, and to enforce any customer specific configuration settings managed by BIOS Setup. BIOS is largely OS agnostic and persists across OS installs, this means that most of the built-in features and capabilities described in this document work whether the system has Windows, Linux, or even without an operating system at all.

Additionally, more recently the term "UEFI" has become much more prominent when discussing pre-boot firmware on PCs. While architecturally the UEFI ecosystem has had a net positive effect on compatibility and ease of deployment, the term itself has managed to confuse the issue. UEFI, or the Unified Extensible Firmware Interface, is an industry specification that defines the various optional interfaces and protocols used by pre-boot firmware to configure a PC (in most cases). Many experts pedantically correct others that "UEFI has replaced BIOS!" but that's only partly true. The truth is, PC OEMs and most subject matter experts in the field still use the term "BIOS" to refer to any pre-boot firmware designed to bootstrap a modern PC, regardless of whether it is UEFI-based, Linux-based, or completely custom.

One of the other net positive effects of UEFI has been the opportunity to integrate features and device drivers directly into the BIOS development flow that are compatible with the UEFI specification. An excellent example of this in practice is the [UEFI Tianocore](#) project on GitHub. Tianocore is the current reference implementation for UEFI and is completely open source. Dell and other OEMs use some of this project code as the foundation or "core" BIOS and add differentiated features on top of the open-source core. Another benefit of this open architecture is that UEFI supports architectures well beyond Intel® x86-based PCs.

Secure Design Processes and SDL

Dell's Secure Development Lifecycle (SDL) shown in Figure 1 integrates standards and best practices from a variety of industry consortiums and standards bodies. A primary consideration in SDL is to blend data sources from both internally discovered and externally reported issues, allowing Dell to focus on the most prevalent issues in the Dell device technology space. A second major consideration is industry practices. Dell participates in many industry standards organizations such as SAFECode, TCG and IEEE Center for Secure Design to ensure alignment to industry practices. Lastly, Dell's Secure Development Lifecycle is aligned with the principles outlined in [ISO/IEC 27034 'Information technology, Security techniques, Application security'](#). These practices are tightly integrated into the design and manufacture of Dell products.



Figure 1: Dell EMC Secure Development Lifecycle

Supply Chain Security

Supply chain assurance and the broader supply chain security concept are complex topics that demand their own volume. Fortunately, the Dell device supply chain falls under the scope of a previously published comprehensive paper on this subject. The latest version of Dell Supply Chain Assurance is available for download [here](#).

The following excerpt is a high-level description of many of the Dell device BIOS protection mechanisms that have been covered in-depth in this document:

- Dell has implemented procedures across our commercial servers, desktops, and laptops in accordance with the guidance and recommendations outlined in [NIST SP 800-147](#), Basic Input/Output System (BIOS) Protection Guidelines. Dell's protected BIOS and signed update mechanism help prevent unauthorized modification of the platform firmware and reduce the risk of pre-boot malware or unwanted functionality. From the Dell perspective, "supply chain security" covers more than suppliers, manufacturing sites, and logistics. Dell design, development, validation, and sustaining phases all equate to some part of the supply chain from the customer perspective. Luckily, this means that the investments in the features covered in this document can help assist and augment traditional supply chain security. For example, the SafeBIOS verification check is part of the manufacturing process of every commercial device that Dell produces.

Industry Affiliations

Dell is active in multiple industry-wide groups to collaborate with other leading vendors in defining, evolving, and sharing best practices on product security, and in further enhancing the cause of secure development. Examples of industry collaboration include:

- Dell co-founded and currently chairs the Board of Directors of The Software Assurance Forum for Excellence in Code ([SAFECode](#)). Board members include representatives from Microsoft, Adobe, SAP, Intel®, Siemens, CA and Symantec. SAFECode members share and publish software assurance practices and training.
- Dell is an active participant in and long-time member of the Trusted Computing Group ([TCG](#)), a not-for-profit organization formed to develop, define, and promote open, vendor-neutral, global industry specifications and standards, supportive of a hardware-based root of trust, for interoperable trusted computing platforms. TCG's core technologies include specifications and standards for the Trusted Platform Module (TPM – a part of Dell SafeID), Trusted Network Communications (TNC) and network security and self-encrypting drives.
- Dell is an active member of the Forum of Incident Response and Security Teams ([FIRST](#)). FIRST is a premier organization and a recognized global leader in incident and vulnerability response.
- Dell is an active participant in The Open Group Trusted Technology Forum ([OTTF](#)). OTTF leads the development of a global supply chain integrity program and framework.
- Dell employees were founding members of the [IEEE Center for Secure Design](#), which was launched under the IEEE cyber security initiative to help software architects understand and address prevalent security design flaws.

Built-In, “Below the OS” Security

	Dell Unique	Industry Standard
Identify	Dell Identity and Asset Management Tags	• Service Tag • Asset Tag
Detect	• Discrete TPM • Dell SafeBIOS Verification • Dell SafeBIOS IoA/IoC • Dell Secured Component Verification (SCV) • Intel® ME Firmware Verification • CVE Detection	• Runtime BIOS Resilience • TCG Measured Boot • Downgrade Protection
Respond	• Dell SafeBIOS Image Capture • Dell Trusted Device telemetry	Dell BIOS Recovery
Protect	• Fused Root of Trust • Dell UEFI Secure Boot • BIOS Passwords	• Intel® BIOS Guard • Intel® Boot Guard • Authenticated Updates • BIOS Public Keys
Recover	• Dell BIOS Connect • Dell Support Assist	Windows OS Recovery

As mentioned in the introduction, the security of endpoints collectively forms the foundation of the entire enterprise. Consider the analogy of a house to represent endpoint security. An organization’s most valuable assets – data and sensitive information – are like the family inside this house. Houses however are not intrinsically secure, so homeowners must build or buy additional protections like deadbolts, security cameras, and motion sensors to help secure them. Jumping back to the enterprise: there are plenty of players in the security ecosystem which offer these additional protections, but what’s the remaining gap in this scenario? The foundation. Any dwelling must be built on a stable foundation to protect the homeowner’s investment in security from being subverted from below. That’s where the Dell commercial client protections and Dell SafeBIOS security comes in.

Dell refers to this stable foundation as Built-In, “Below the OS” security. Based on the analogy above, it’s clear that the endpoints and this below the OS foundation are valuable targets for adversaries attempting to get a foothold into an enterprise. This critical role in our customers’ security is why Dell has invested in “below the OS” security for over a decade and why it’s important that we publicly document SafeBIOS and associated features, along with some of the rationale behind their development.

Dell Trusted Device (DTD) Application

Among PC OEMs, only Dell integrates device telemetry with industry-leading software to improve fleet-wide security.* This data is captured and made available through the Dell Trusted Device (DTD) Application. The DTD App is free, downloadable software that provides maximum BIOS protections within the Dell SafeBIOS product portfolio. The DTD App maximizes SafeBIOS capabilities by communicating endpoint telemetry between the device and a secure Dell cloud, providing unique below-the-OS insights into security “health.” The data transmitted provides assurance that the BIOS is being measured. If any feature reports unexpectedly change, the IT administrator is notified of possible tampering.

The DTD App provides telemetry to enable several features under Dell SafeBIOS such as Indicators of Attack (IoA) and BIOS Verification, which detect tampering of BIOS firmware and BIOS configuration. It also provides Intel Management Engine (ME) Firmware Verification, which verifies the integrity of highly privileged ME firmware by comparing ME firmware found on the platform with previously measured hashes (stored off-host), and our Security Score, a feature that aggregates various indicators into one easy-to-read KPI.

The administrator can find notifications in the Windows Event Viewer, a log of application and system messages, including errors, information messages and warnings. It’s a useful tool for troubleshooting problems. They can also find this information in their endpoint management tool or SIEM, as Dell integrates device telemetry with industry-leading software to improve fleet-wide security. Our list of extensive partner integrations includes third-party security software, such as CrowdStrike Falcon and Absolute, as well as endpoint managers, such as Microsoft Intune, and SIEMs, such as Splunk. They can also view elements in Dell TechDirect, and as of the DTD 6.1 release, local users can view this information via a Dell Trusted Device local console.

Not only do these integrations improve threat detection and response with a brand-new set of device-level data, but they also help customers make the most of their software investments. Knowing how much our customers value the ability to view (e.g., security alerts) within their preferred environments, Dell continues to release updates to the DTD App, enabling greater integration capabilities. For example, recent releases expanded key feature integrations in the Intune environment. Now, Intune administrators can view additional data from BIOS Verification, Intel ME Firmware Verification and Secured Component Verification (or SCV, a Dell-unique component integrity check), with added capabilities coming in future DTD releases. The integration of DTD telemetry with Intune supports extensible compliance and enables organizations to use this telemetry to maintain policies they choose to apply.

The Importance of Built-In Security

Industry standards bodies, policy makers, and security researchers have recently started to focus on built-in, below the OS security as well. Dell has been very involved in contributing to, and building devices that adhere to, recommendations from NIST around firmware security and resilience. [NIST Special Publication SP 800-193](#) outlines overall resilience guidelines for device firmware (including BIOS) and has been helpful in confirming the value in Dell’s below the OS security investments and direction.

* Based on Dell internal analysis, September 2023. Applicable to PCs on Intel processors. Not all features available with all PCs. Additional purchase required for some features.

Other NIST Special Publications that are relevant in this space include [NIST SP 800-147](#), which defines guidelines for protecting the BIOS and specifies that only signed and authorized BIOS should run on the device (see the Dell Client Signed Firmware Update whitepaper [here](#)). [NIST SP 800-88](#) provides direction for data sanitization on hard drives and solid-state drives.

It's clear that industry and customer interest for built-in, "Below the OS" and firmware/BIOS security has risen in the last few years. This awareness is incredibly valuable because it allows Dell to continue to improve these areas year over year and help protect Dell device customers from the most sophisticated adversaries.

Intel® vPro Additions to Built-In Security

With Intel vPro enabled and supplementing Dell SafeBIOS protections, Dell and Intel® provide another routine for managing fleet of Dell platforms. With Intel® Active Management Technology, ITDMs can diagnose issues remotely in a hybrid work scenario. Along with Intel® AMT, vPro has additional features such as a Platform Service Record and Unique Platform Identity (or UPID). Both features rely on one another to play key roles in Dell SafeBIOS prompting tamper detection on Dell platforms through the SafeBIOS IoA.

Understanding Dell Cybersecurity Using the NIST Framework

Cyber security capabilities can be categorized according to the five functions of the NIST Cybersecurity Framework: Identify, Protect, Detect, Respond, and Recover. These provide a shared understanding and methodology for classifying technologies and identifying gaps in an organization's cyber security architecture. In the sections which follow, we'll provide details of those features and below the OS security technologies that align to these functions and explain how they work and why they are important. There are other frameworks which can be used – Dell has selected the NIST framework for its simplicity and its widespread acceptance within the cybersecurity community. More information about the NIST Cybersecurity Framework can be found here: <https://www.nist.gov/cyberframework>.

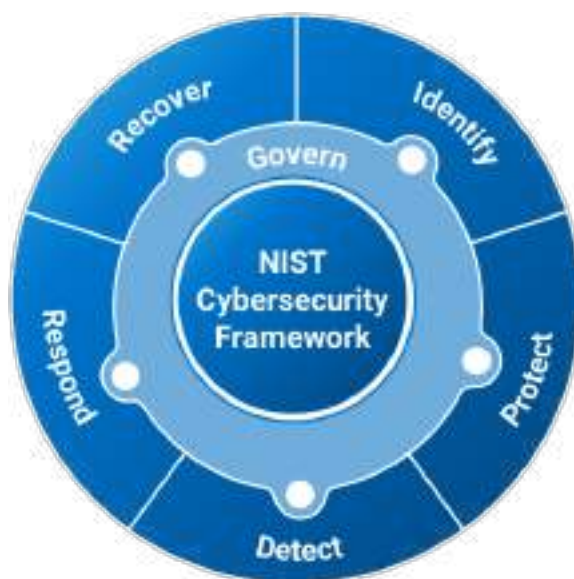


Figure 2: CSF Functions

Dell implements this framework using both Industry Standard and Dell Unique capabilities.

	Dell Unique	Industry Standard
 Identify	Dell Identity and Asset Management Tags	• Service Tag • Asset Tag
 Detect	• Discrete TPM • Dell SafeBIOS Verification • Dell SafeBIOS IoA/IoC • Dell Secured Component Verification (SCV) • Intel® ME Firmware Verification • CVE Detection	• Runtime BIOS Resilience • TCG Measured Boot • Downgrade Protection
 Respond	• Dell SafeBIOS Image Capture • Dell Trusted Device telemetry	Dell BIOS Recovery
 Protect	• Fused Root of Trust • Dell UEFI Secure Boot • BIOS Passwords	• Intel® BIOS Guard • Intel® Boot Guard • Authenticated Updates • BIOS Public Keys
 Recover	• Dell BIOS Connect • Dell Support Assist	Windows OS Recovery

Identify

From the NIST Framework: “Develop an organizational understanding to manage cybersecurity risk to systems, people, assets, data, and capabilities.”

The Dell built-in security features map directly to the Protect, Detect, and Recover/Respond functions of the NIST Cybersecurity Framework. The Identify function maps closely as well but the interaction is a bit more complex. For most enterprises, the Cybersecurity Framework is an effective tool for assessing security risk in their environments, where identifying assets and risk is a broad but valuable exercise. For Dell client devices, the Identify function has four separate and important roles:

- Includes features designed to help identify and asset-manage Dell devices within a customer infrastructure.
- Platform certificate-based machine identity which enables device health through proof of authenticity and supply chain assurance.
- Human identity secured via dedicated NIST certified biometrics and certificate-based authentication processing and storage SoC.
- Addresses processes and tools used by Dell to Identify customer security risks and threat models of the application and deployment of these devices.

Device Identity

Service & Asset Management Tags

The Dell BIOS supports two independent persistent identifiers (or “tags”) to allow customers to discover and manage their devices in their infrastructure.

- **Service Tag**

The Service Tag is programmed into the BIOS NVRAM (non-volatile random-access memory) during the manufacturing process and is locked in place for the life of the device. This allows the customer and Dell to identify the device for overall asset management in the customer enterprise and enables Dell to confirm the device information for service and warranty support. The BIOS is responsible for displaying the Service Tag in BIOS Setup and in management interfaces such as SMBIOS. The Service Tag is not changeable by the customer.

More information about the Service Tag can be found in the Dell Knowledgebase [here](#).

- **Asset Tag**

The Asset Tag is also stored into BIOS NVRAM and can be set, changed, or cleared by the end customer. The Asset Tag is displayed in text on the Dell boot splash screen on every boot and can be used for additional customer-specific tracking information, logistical messages, or unique branding. The BIOS Administrator password can be used to provide authentication and authorization controls to control Asset Tag modification.

More information about the Asset Tag can be found in the Dell Knowledgebase [here](#).

Platform Certificates for Machine Identity & Supply Chain Assurance

Supply chains can be vulnerable to disruptions such as tampering, theft, counterfeiting. Recent geopolitical tensions have thrust supply chain into the spotlight, causing customers to question their electronic product providers and demand visibility as to where products are developed, created, manufactured, and handled.

The US White House issued Executive Order in 2021 to strengthen the resilience of the US supply chain. Extending government action, the DoD recently released a ‘blueprint’ for the [secure procurement of devices](#), which effectively calls out platform certificates as mandatory for verifying and proving device authenticity, including the criteria for deploying an acceptance test. It provided qualified examples from NIST’s NCCoE supply chain assurance program, where Dell was one of the eight industry leaders which participated in developing examples, providing hardware and specifying solutions. Dell used its [Secured Component Verification \(SCV\)](#) solution as the foundation of [NIST Special Publication SP 1800-34](#) – Validating the Integrity of Computing Devices, which builds platform attribute certificates in the factory during manufacturing, thus aligning SCV with the DoD’s procurement guidelines.

Platform certificates create secure identities bound to the products during manufacturing which are used to seamlessly connect Dell devices to customer infrastructure or Dell services, creating a foundation from which Dell provides secure attestation methods to our supply chain for the customer. SCV enables dock to dock security by creating a certified manifest of device components bound to the device via TPM. The customer can validate that the device they ordered is the device Dell built and sent them. It ensures that the device was not intercepted or changed at any point during the delivery process. Dell will continue to expand function and

capabilities built into the platform certificate and the methods of attesting device hardware, components, software, and firmware to become to root-of-trust for device identity, health, and authenticity.

Dell manages the entire SCV solution in-house, from collection of component information and certificate creation to storage and retrieval. This is because root of trust (the first code that runs in a PC when it's turned on) is foundational to Dell Endpoint Security. By taking on this end-to-end ownership and not ceding our processes or customers' data to outside parties, we maintain tighter control on our supply chain and mitigate potential risk introduced by outside parties. Available today:

- **Dell SCV on Device:** As the name indicates, this solution includes a platform certificate on the device itself, eliminating the need for customers to connect to the internet to collect the certificate. With this solution, Dell provides an option for air gapped environments, as well as cloud-based environments.
- **Dell SCV on Cloud:** This solution is an ecosystem one, providing a fleet-wide view and an automated and seamless method of verification. Our in-house verification method (the Dell Trusted Device Application) integrates with Dell TechDirect and third-party partners. For example, with SCV on Cloud, admins can view results and reports within the Microsoft Intune environment, as well as within Dell TechDirect – *without* the use of a third-party HIRS tool.

User Identity: Dell SafeID

Dell SafeID keeps user credentials safe and helps customers stay protected from malware attacks. This hardware-based, storage solution for credentials better protects your information by keeping it isolated and out of attackers' reach.

Two options are available:

- **Dell SafeID with discrete TPM**
- **Dell SafeID with ControlVault 3+.** CV3+ is unique to Dell* and FIPS 140-3 level 3 certified.

Dell SafeID with discrete TPM: SafeID leverages a hardware based Trusted Platform Module, or discrete TPM, a specialized chip designed to store highly privileged information such as cryptographic keys, provide platform device authentication and protect other secrets and authorizations required for secure operation of the endpoint. The latest version, TPM 2.0, is required for devices running the Windows 11 operating system.

Dell SafeID with ControlVault: SafeID plays a role in multi-factor authentication, or MFA, through means of the fingerprint reader, a Personal Identity Verification (PIV) card, the camera, or a FIDO2 key on a Dell device. With Dell's Precision Mobile and Latitude series there is an option to add ControlVault as a part of the device's configuration. With this feature, the end user can perform Certificate-based email signing via S/MIME and smartcard sign-in to mission critical applications or workspaces. For the ITDM, a policy can be set for the device to use multiple means of authenticating into the device, an application (or workspace).

- **Isolated Processing & Storage: Dell ControlVault**

ControlVault's ARM Cortex A7 1GHz processor and storage is not only outside-validated, FIPS 140-3 level 3 certified – it is a dedicated security chip, unique to Dell, providing a protective and secure boundary for credential processing and storage enabling multifactor authentication via fingerprint biometrics, smartcard & NFC modalities.

- **Support**

ControlVault works with industry leaders and standards bodies to ensure adherence to customer enterprise needs. Today it supports Windows Hello Enhanced Sign-in Security, Linux fingerprint biometrics, FIDO2 specifications and Imprivata One-Sign (on certain platforms with FIPS fingerprint reader).

- **Certifications**

EMVco v4.3d, WQHL, NFC Forum, PCI PTS POI, FIPS 140-3 lvl3 & FIPS 201-3

No other embedded PC biometric solution has achieved this level of external validation from NIST.*

**Based on Dell internal analysis, October 2024. Applicable to PCs on Intel processors. Not all features available with all PCs. Additional purchase required for some features. Validated by Principled Technologies. A comparison of security features, April 2024.*

To learn more about Dell SafeID, read our [datasheet](#).

“Below the OS” Threat Modeling

Threat modeling is the exercise of using an adversarial mindset to evaluate computer architectures to determine potential vulnerabilities or attack surface early in the development phase. These exercises are critical to ensuring that any latent vulnerabilities are identified and remedied during development. Ongoing programs address client devices in-use as attackers develop new targeted threats.

Most threat modeling information that is publicly available is focused on software designed to be deployed as web applications or to cloud architectures. Dell uses this powerful tool not only for web and application software, but also as part of the SDL process for BIOS and firmware. Dell has started to include physical threats, time-based risk analysis, and persistent storage in the threat model assumptions for Dell devices. These expanded assumptions have proven to be significant improvements in finding and mitigating potential vulnerabilities in BIOS, firmware, and hardware design.

Dell has started to include physical threats, time-based risk analysis, and persistent storage in the threat model assumptions

Dell includes physical threats, time-based risk analysis, and persistent storage in the threat model assumptions.

Just as hardware and software threat models differ, so do Dell customers' threat models. For example, not every customer includes “Below the OS” threats in their own threat model, but a growing number do. Using the most security-sensitive customers' threat models as a baseline for our own allows Dell to design devices that are resilient against the most sophisticated adversaries in addition to the more common threats. Penetration testing, or ‘pen-testing’, is a form of product validation where authorized attacks are performed for internal evaluation. This has become synonymous with mature security practices across the industry. Dell leverages both in-house teams and external vendors to pen-test Dell devices while these products are still in the engineering phases of development. Like the threat model assumptions made above, these tests focus on physical access and are prioritized based on risk assessments of individual components integrated into Dell devices.

Protect

From the NIST Framework: “Develop and implement appropriate safeguards to ensure delivery of critical services.”

The Protect stage of the NIST framework has been an area of significant investment for Dell over the last decade. All the context described in the previous ‘Identify’ section with respect to portfolio details, threat models, and security research has been pulled into the overall direction, strategy, and architecture for protecting the lowest levels of code in Dell devices. These features are truly the “first line of defense” for modern PCs against sophisticated adversaries.

Protecting the PC Boot Process

In theory, bootstrapping a modern personal computer may seem relatively simple. Pull the processor out of reset or low-power sleep state, initialize memory and motherboard hardware devices, enumerate storage, and find a bootloader to load the customer's operating system of choice. Simple, right? In practice there is much more to it than that, and much of the complexity and additional features in the pre-boot timeframe is there to help protect the PC from executing unauthorized code. Ultimately, the BIOS boot process provides a safe foundation for the operating system and user applications.

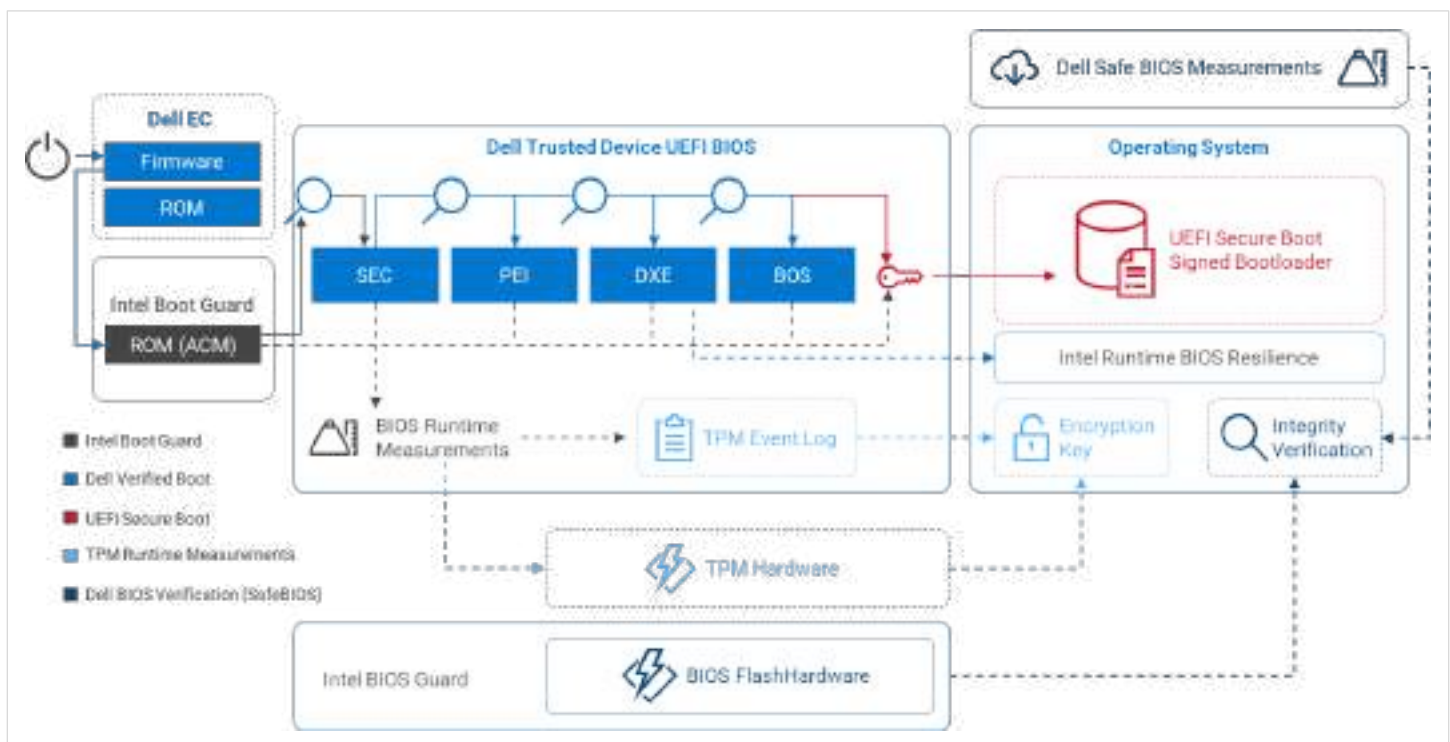


Figure 3: Dell Trusted Device Boot Chain

Securing the Boot Chain

The PC boot process is a series of configuration steps, events, and procedures that combine to create a tightly linked chain, from the point of time when the embedded controller and/or main processor come out of reset, to the point of handoff to an operating system like Microsoft Windows™ or Canonical Ubuntu™. Links in this chain protect the boot process by cryptographically verifying each subsequent link using either hashes or digital signatures. 'Golden' or reference hashes are protected by encoding them into an already verified section of code and digital signatures use public keys embedded in the firmware for verification.

The illustration in Figure 3 depicts a high-level overview of the major components in the Dell device boot chain. Many of these components, like the Embedded Controller (or EC), will be covered in more depth in other sections of this document and this illustration should serve as a helpful reference in understanding how everything ties together.

Like the roots of a tree, the root of trust is the origin point upon which all subsequent trusted events are built. For modern PC's, the processor reset vector is often considered the root of trust.

The “Root of Trust”

Like the roots of a tree, the root of trust is the origin point upon which all subsequent trusted events are built. For modern PCs, the processor reset vector is often considered the root of trust. This is the first instruction that the processor fetches after coming out of reset.

Again, in practice it's a bit more complicated than that. Dell devices include both an embedded controller (EC) and typically an Intel® Converged Security and Management Engine (CSME) or AMD® Platform Security Processor (PSP) that execute firmware before the processor wakes up. The Dell EC is the hardware root of trust for these devices since it runs cryptographically verified code that manages the power controls which bring the x86 chipset out of its low-power state. This root of trust boot flow continues by chaining the Intel CSME or AMD PSP to the Dell EC, followed by the BIOS. This flow is like that in Dell devices that contain ARM-based architecture(s).

TCG and the Root of Trust

The Trusted Computing Group (TCG) provides definitions and specifications for developing secure products. The TCG glossary defines a root of trust as “A component that performs one or more security specific functions, such as measurement, storage, reporting, verification, and/or update. It is trusted always to behave in the expected manner because its misbehavior cannot be detected (such as by measurement) under normal operation.” TCG specifications build on this to define several roots of trust that describe how the BIOS and Trusted Platform Module (TPM) must coordinate during the boot process to maintain authenticity of BIOS measurements; most importantly a Root of Trust for Measurement (RTM) and a Root of Trust for Reporting (RTR).

The Detect section of this document will cover the TCG Measured Boot feature in much more depth, but first let's clarify a few words in the context of the boot process and root of trust. TCG Measured Boot uses the PC's TPM as a protected area for storing hashes of BIOS and firmware code that is loaded and executed in the boot process. The TPM is designed to store these events in a secure way that can be verified post-boot through a process called attestation. Both Windows and Linux include TPM software stacks that support measured boot attestation.

UEFI Secure Boot

One of the most powerful improvements in the last decade for protecting the pre-boot process from executing unauthorized code is UEFI Secure Boot. Unfortunately, there is some confusion in the industry about the benefits and scope of UEFI Secure Boot since the feature name tends to be conflated with the more general “secure boot” concept of executing signed pre-boot code. To avoid this confusion, this document will use the term “verified boot” when referring to executing cryptographically signed code in the pre-boot context when it is outside of the scope of UEFI Secure Boot.

That clarification is not intended to diminish the value of UEFI Secure Boot at all - it's an effective feature for mitigating threats and exploits that may be delivered via unsigned bootloaders, UEFI shells, or UEFI drivers on add-in devices. To protect against these threats, Dell provisions trusted default certificates into the UEFI Secure Boot databases to allow Dell to manage the UEFI authenticated variables that protect the allowed database – the “db” – and the disallowed database “dbx”. Default provisioning also enforces verification of Windows 10/Windows 11 bootloaders and signed shims for Linux using trusted certificates from Microsoft. Also included by default is a Microsoft Key Exchange Key or “kek” to allow Microsoft-signed db and dbx updates from Windows.

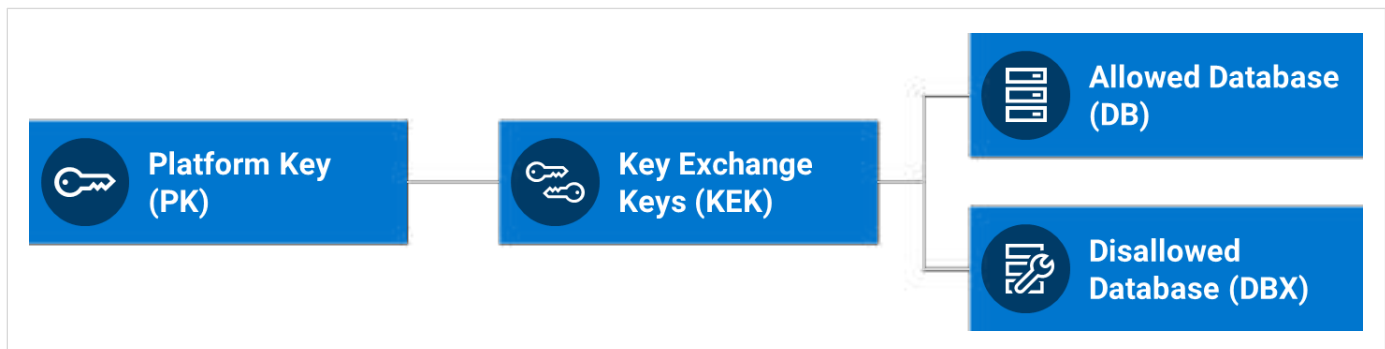


Figure 4: Secure Boot Key Hierarchy

UEFI Secure Boot Expert Mode

Depending on customer and enterprise threat models, some administrators may want to restrict UEFI Secure Boot to only allow specific bootloaders and/or UEFI drivers. To support this, the Dell BIOS Setup engine integrates Custom Mode Key Management that allows administrators to modify the entire contents of the UEFI Secure Boot key management database directly. This privileged operation is available with local physical access only and will temporarily disable UEFI Secure Boot while the certificate databases are being repopulated with custom keys supplied by the administrator. Key databases can also be reset back to the factory default values (including reinstallation of the original Dell PK) by using this interface.

The US DoD issued “[UEFI Secure Boot Customization](#)”, a Cybersecurity Technical Report, in September 2020. The document provides a comprehensive guide for customizing a Secure Boot policy to meet several use cases. Customization enables administrators to realize the benefits of boot malware defenses, insider threat mitigations, and data-at-rest protections, while overcoming incompatibilities with hardware and software.

Signed Firmware Update

Previous sections detailed how the Dell BIOS protects itself from running unauthorized code during the boot process, but how does it ensure that code cannot be tampered with or replaced on the motherboard BIOS flash storage device (e.g. the Serial Peripheral Interface, or SPI flash storage device) in between boots and during updates? Guidelines for protecting the BIOS against these threats were published by NIST in 2011 as Special Publication 800-147. This NIST document describes requirements for cryptographic authentication of BIOS updates, integrity protection of currently running BIOS, as well as guidelines to prevent bypass which further harden the BIOS against unauthorized modification via “backdoors”. Dell devices implemented these requirements in 2011 and a full whitepaper describing the support is linked in the References section of this document.

NIST SP800-147 Support

Dell puts significant effort into hardening the BIOS protection and authentication capabilities on its client devices in accordance with [NIST SP800-147](#) to support Dell's customers.

BIOS running on a device that supports Signed Firmware Update contains information in its Root of Trust for Update (RTU) that supports a cryptographically hardened verification mechanism which allows only approved BIOS update utilities to modify the BIOS code in storage:

- **BIOS Update Authentication**

All BIOS update images are signed using the RSA PKCS #1 v1.5/v2.1 algorithm with RSA 2048-bit keys as per [FIPS Publication 186-5 Digital Signature Standard \(DSS\)](#). The SHA-256 algorithm was selected to hash the payload in the signing and integrity verification process based on this algorithm's acceptance in NIST Special Publication 800-131A. Update images are verified by the BIOS using the public key contained in the RTU before the BIOS or other firmware currently running on the device is modified.

- **Integrity Verification**

The RTU and BIOS are protected from unauthorized modification using Dell proprietary flash write cycle trapping and locking mechanisms supported by the device hardware. All programmatic code update attempts that are not approved by the RTU verification mechanisms and any attempts to update BIOS data not approved by the BIOS storage handler are blocked from accessing the device flash memory using flash disable mechanisms.

- **Non-Bypassability**

The Signed Firmware Update mechanism in the RTU that enforces authenticated updates is the exclusive mechanism for modifying the BIOS. This enforcement cannot be bypassed by any firmware or software running on the device that is not controlled by the RTU.

System Management Mode (SMM)

System Management Mode, or SMM, is a privileged mode of the processor architected to support handling of high-availability, manufacturer-specific tasks independent of the operating system. Think of SMM as a component of the BIOS that remains resident underneath the operating system (reference the "ring" architecture where ring 3 refers to user mode code, ring 0 is the root, supervisory, or kernel mode of the operating system, and "ring -2" is applied to SMM to highlight the additional privileges that it is allowed over the device). Dell uses SMM to support persistent storage (e.g., UEFI variables), BIOS configuration interfaces, thermal handling, and other critical-priority events. For Arm-based Architecture(s) the Secure Partition Manager, or SPM, would be applied by Trusted Firmware.



Figure 5: Modern PC Ring Architecture

SMM has been the target of dozens of disclosed vulnerabilities, security conference presentations, and media reports over the years. This has been welcomed attention from a security perspective because it provides helpful insights for SMM threat modeling and security improvements. For example, even though Dell BIOS uses SMM for system management activities, there has been significant investment in hardening the SMM environment and overall reduction in reliance on SMM. Additionally, Dell has integrated several technology advancements to incrementally deprive the SMM code that must be present on the system and mitigate potential impact to other parts of the operating system.

- **Threat: SMM Over-Reliance for BIOS Locking and Signed Update Verification**

The Signed Firmware Update whitepaper released in 2013 is still applicable and relevant to all Dell devices today. It's the baseline for protecting the BIOS from tampering or other unauthorized modification. While the NIST 800-147 specification requires non-bypassability in operation, it does not necessarily consider vulnerabilities that may exist in the code that enforces non-bypassability. In many implementations System Management Mode, or SMM, is the entity that enforces BIOS locking and signed update verification.

- **Mitigation: Intel BIOS Guard**

Dell decided to mitigate this reliance on SMM by moving the authority to unlock and update BIOS from SMM to device hardware. Dell devices have implemented Intel BIOS Guard since 2015, which explicitly verifies all BIOS code region writes using public keys fused into the Intel Platform Controller Hub (or PCH). Since the PCH operates between the processor and the flash storage where the BIOS is located, logic within the PCH can block all writes to the BIOS code region before flashing. Intel® BIOS Guard integration required considerable resources and infrastructure to implement, and because of this, was only adopted by a few OEMs. Dell considers this feature a must-have in the current below the OS threat landscape.

- **Threat: SMM Access to Hypervisor Memory**

One high-profile threat highlighted by security researchers is the potential for a rogue or malicious SMM handler or code to use SMM privilege to arbitrarily read and write to main memory. Turning this threat from theoretical to practical requires exploiting an unknown or unpatched vulnerability in SMM itself to gain code execution. As a demonstration of potential impact, researchers created proof of concept code that would interact with hypervisor memory and context that was designed to isolate and protect user applications. The end goal for an adversary with this level of access and sophistication could be credential or data theft from applications that were presumed secure.

- **Mitigation: Windows SMM Security Mitigations Table (WSMT)**

The Windows SMM Security Mitigations Table (WSMT) enumerates various methods that BIOS vendors can implement to mitigate SMM threats. Since some of the mitigations in the WSMT can cause compatibility issues with legacy systems management software, Dell devices support a WSMT option in BIOS Setup to allow the administrator to enable or disable these mitigations. Once enabled, WSMT mitigations provide strict boundaries for memory access from SMM, e.g. the BIOS SMM handler can only use specific pre-allocated memory address ranges to communicate with system management software. The WSMT structure published by the BIOS provides affirmation to the operating system that the Dell device has implemented and enabled these features.

- **Mitigation: Memory Attribute Table and No Execute (MAT/NX)**

Protecting operating system memory from modification by SMM is just one piece of the runtime defense puzzle. UEFI Runtime Services are supported by the BIOS and run within the OS context. To isolate these services, the BIOS implements the `EFI_MEMORY_ATTRIBUTES_TABLE`, which describes runtime memory organization for the operating system's consumption. This allows the OS to accurately configure page tables to block code execution from EFI data areas and prevent code areas from being overwritten from other potentially malicious code. These may seem like fundamental security features from an OS perspective but the handoff between pre-boot and operating system requires specific coordination to ensure these protections are accurate and do not introduce compatibility issues.

...the handoff between pre-boot and operating system requires specific coordination to ensure these protections are accurate and do not introduce compatibility issues.

BIOS Patch Management

Best practices in enterprise security should always include a comprehensive software patch management strategy to ensure that any software updates to mitigate vulnerabilities are deployed as soon as they are available. BIOS upgrades are often overlooked or delayed in the overall patch management strategy, but that's rapidly changing as customer awareness for built-in "Below the OS" security continues to increase. To support this overall initiative, Dell device BIOS updates are posted to both Windows Update (or WU) for Windows 10/Windows 11 systems and to the Linux Vendor Firmware Service (or LVFS) for Linux systems. This allows seamless integration of BIOS updates into the OS ecosystem without the need for separate BIOS update utilities. BIOS updates are also provided as a part of the [Dell Trusted User Experience \(DTUE\)](#), designed to help organizations more easily manage updates to keep devices at optimal operation and security. Of course, updating the BIOS using the Dell BIOS update utility is still supported.

BIOS Downgrade Protection

Sometimes adversaries will attempt to revert or 'rollback' software/firmware to a known vulnerable previous version as an initial step in their attack. A Dell commercial device with SafeBIOS can be configured in the BIOS setup program or remotely using the Dell Command Tool Suite to prevent BIOS reversions, thus mitigating this threat. By default, the Enable BIOS Downgrade BIOS setup option is turned on to support full flexibility for customers to choose the BIOS image appropriate for their infrastructure. However, once this setting is disabled (locally or remotely) only newer BIOS versions will be allowed to flash onto the device and physical presence (i.e. a user in front of the keyboard) is required to revert the setting.

Embedded Controller: Signed Firmware

The embedded controller, or EC, is included on all Dell commercial device notebooks and most modern commercial desktops and workstations. As explained in the section on root of trust, the EC is responsible for low level hardware interface functions such as power and reset management. Dell devices protect the EC firmware updates at two layers while performing firmware updates. First, the BIOS verifies the EC firmware signature prior to sending the update to the EC and blocks any unauthorized direct access to the EC firmware at runtime. Second, the EC update payload is subsequently verified by the EC firmware using public keys embedded in the EC context, independent of the BIOS. Modern Dell devices include cryptographic acceleration and verification capabilities integrated directly into the EC. These capabilities include verified boot support that will block any EC execution of unsigned firmware even if it was programmed onto the device via an unauthorized side-channel, such as direct physical access. This is a good example of the benefits of including physical access into the Dell device threat model and helps to protect this critical root of trust from tampering.

Protecting BIOS Configuration

Security research and media coverage of "Below the OS" threats focus largely on firmware tampering and/ or escalation of privilege, but the configuration of the client device can also be a potential threat surface. Attackers may use BIOS configuration settings to attempt to manipulate or reconfigure the device into a state that may be at higher risk for exploitation depending on the environment. Dell devices are shipped in a "secure by default" state and customers can protect this state from unauthorized access or modification by enabling a few important features.

Option	Description
Admin Password	Allows you to set, change, or delete the administrator (admin) password. The entries to set password are: • Enter the old password: • Enter the new password: • Confirm new password: Click OK once you set the password  NOTE: For the first time login, "Enter the old password:" field is marked to "Not set". Hence, password has to be set for the first time you login and then you can change or delete the password

The BIOS Admin Password is the Dell device authorization mechanism for protecting BIOS configuration (such as BIOS settings) and the ability to upgrade or downgrade the BIOS. From a protection perspective, Dell recommends that all customers set a complex BIOS Admin Password to minimize the risk of unauthorized BIOS configuration modifications. The BIOS Admin Password can be set locally through BIOS Setup, or remotely using the Dell Command Tool Suite. More information is available in individual device owner's manuals and administrator guides.

- **Local vs. Remote Configuration**

The BIOS Admin Password protects against local and remote modification of BIOS settings that could be used by adversaries to open an attack surface on the device. Dell devices go one step further to classify specific security settings that are only available with local physical presence (i.e. a user in front of the keyboard) using BIOS Setup. These settings are locked from remote access even if the BIOS Admin Password is supplied through the remote interface. An example list appears in Table 1 below (not exhaustive):

BIOS Configuration Option	Local Access	Remote Access
Secure Boot	Yes	No
Allow BIOS Downgrade	Yes	No
Master Password Lockout	Yes	No
TPM Clear	Yes	No

Table 1: Example Local-only BIOS Options

- **Dell Master Password**

The Dell Master Password is a lesser-known feature of the Dell commercial client device. The Master Password feature is available for commercial device customers who may have forgotten or misplaced the BIOS Administrator Password on their device or fleet of devices. The Dell Master Password uses a shared secret algorithm (i.e. the BIOS and the unlock tool share a common secret) integrated into the BIOS or EC to allow Dell Customer Support to offer a device-specific unlock password only for customers that contact technical support and can provide proof of ownership of the device. Once provided by customer service, the master password must be typed into the device locally to unlock the system, as it cannot be used over any remote BIOS interface. The Master Password feature can also be disabled through a Lockout feature, for situations where the threat profile warrants it.

To the security practitioner, this feature may seem a bit antiquated, especially in a largely connected world running on a firm base of public key cryptography. Dell Customer Support must cover a varied commercial customer base across the world with a large set of challenges, not the least of which are language barriers, connectivity issues, and infrastructure availability. These requirements and overall customer scale combine to drive the need for this somewhat low-tech solution that can be exercised even when network-based remediation is not available.

- **Threat: Online Password Generators**

Dell is aware of several unauthorized online password generators that claim to generate Dell Master Passwords for devices. These generators include algorithms that duplicate the shared secret algorithm that is integrated into the BIOS and can often generate valid passwords for older devices. To combat this activity, Dell has redesigned the Master Password feature using modern cryptographic capabilities and best practices. For example, on newer devices this threat is mitigated by using secure encrypted storage when supported by the Dell commercial device, with broader portfolio coverage increasing year over year.

- **Mitigation: Master Password Lockout**

Certain customers may include targeted attacks against BIOS configuration with direct physical access in their threat model. A successful exploit within this threat model would require an adversary to discover a specific device identification information code, and then have direct physical access to BIOS Setup to input the master password without being detected. This is a perfectly valid threat model especially with today's prevalence of mobile systems. In these cases, Dell recommends enabling the Master Password Lockout feature to completely disable the Dell generated master password. Customers that enable this feature must employ their own independent password management processes since Dell Customer Support can no longer help with misplaced passwords for systems configured in this mode.

Configuration Side-Channels

Investments in protecting the configuration of the Dell device extend beyond interface and feature definitions. Protecting against "side-channels" or attempts to attack the implementation outside the bounds of the intended usage is also part of the Dell device threat model.

- **Threat: Physical Access**

As discussed, direct physical access to a Dell device is a part of the threat model of many customers, but more importantly, it's an assumption that the Dell security teams make during the secure development process. In other words, Dell uses this highest risk profile to promote the broadest resilience capability of the Dell device. Physical access from the device perspective includes not only access to the local keyboard and display, but also potentially to the motherboard in an extended 'evil maid' class of attack. Adversaries may attempt to tamper with BIOS configuration settings by directly accessing the storage on the motherboard.

- **Mitigation: Encrypted Storage**

To protect against this level of physical access, Dell has incrementally moved BIOS configuration settings that control security policy to encrypted storage within the embedded controller (the EC). The EC includes root keys and cryptographic accelerators to provide resilience against direct physical attacks directed at the EC non-volatile storage. As an additional layer of security, these variables are encrypted with a device specific encryption key to protect against "break once" types of attack scenarios and further reduce the value of this type of attack.

Best Practices for Secure Configuration

BIOS configurations can be managed at scale in the enterprise with the Dell Client Command Suite. Customers interested in securely configuring their systems using the most restrictive policies can consult the [National Security Agency Cybersecurity Report UEFI Defensive Practices Guidance document](#) for overall recommendations. Please see the Dell Client Command Suite tool documentation to deploy and manage policies aligned to these guidelines.

Protecting BIOS at Runtime

A common misconception in the PC industry is that the BIOS is completely out of the picture once the bootloader and kernel take over execution of the boot process at the point in time where the BIOS hands control over to an operating system which has called the UEFI runtime service `ExitBootServices()`. Of course, this is not the case and even the “Basic Input/Output System” acronym is a reference to this role. A small subset of the BIOS code must persist while the operating system is running to support system management interfaces, UEFI interfaces, and overall system health components like event logging, as well as OEM hardware-specific functionality for power/thermal management.

- **UEFI Runtime Services**

The Dell BIOS allocates and assigns main memory during the boot process as `EFI_MEMORY_RUNTIME` to support specific UEFI services needed by the operating system. These services allow the OS to invoke capsule updates to update BIOS and/or device firmware, set general purpose UEFI variables, and manage the authenticated variables used for Secure Boot configuration. Most of these services are defined by standards (such as UEFI) but may include customization specific to Dell hardware and enhanced security features.

Runtime BIOS Resilience

Intel has been another valuable ally in the Dell device security story providing foundational security technologies in processors and chipsets, also extending trusted computing concepts into new architectural areas of Dell devices. One example of this partnership is Runtime BIOS Resilience which is part of the Intel Hardware Shield group of security features.

Runtime BIOS resilience builds another layer of security within the BIOS by hardening the SMM environment against attacks and protecting the operating system (and ultimately user code and data) from tampering by SMM. The Dell device sets up runtime BIOS resilience early in the boot process by enabling memory paging in SMM and configuring the SMM page tables to only allow access to the memory pages specifically allocated to SMM (in an area of memory called TSEG). This brings architectural capabilities of the processor that have been best practice for operating system memory safety into the realm of BIOS and SMM. These protections help prevent malicious code injection and redirection in the valuable SMM execution environment as well as ensure SMM code cannot affect the operating system (regardless of whether the code is legitimate or potentially rogue).

For more information about other Intel Hardware Shield capabilities, [refer to this paper](#).

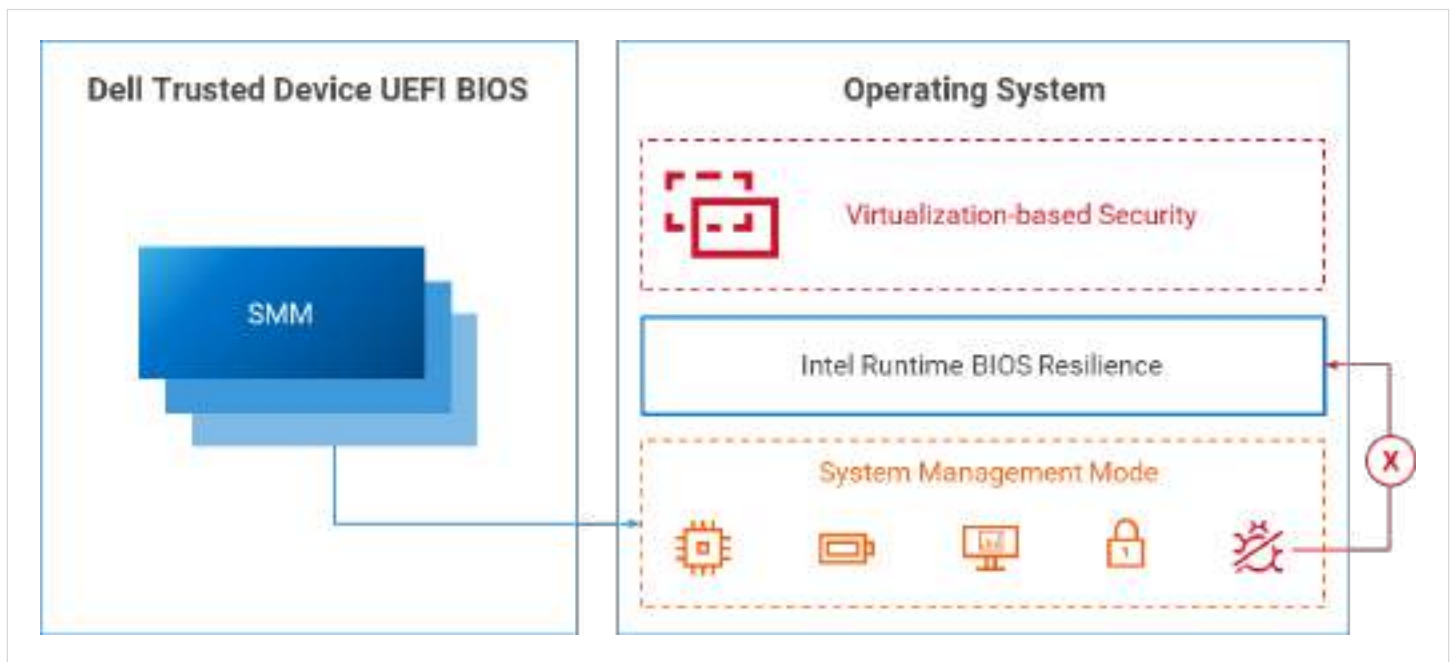


Figure 6: Intel Runtime BIOS Resilience

Detect

From the NIST Framework: Develop and implement appropriate activities to identify the occurrence of a cybersecurity event.

Even a 100% effective protection strategy both above and below the OS may not be enough to thwart the most sophisticated adversaries. Adversaries with this skill level and incentive can move and evolve quickly. Thus, having built-in (not bolted on) detection mechanisms help fill the gap between prevention and response and can provide much needed visibility into new adversarial techniques targeting client PCs.

Intel Boot Guard

When Intel introduced Boot Guard technology, Dell client PCs implemented it as an additional hardware root of trust for BIOS. Intel Boot Guard serves as an incredibly effective detection mechanism for verifying the integrity of the earliest and most critical code executed by the processor is still intact. Any tampering or corruption of the initial boot block (IBB), the very first piece of BIOS code to be executed by the processor, will be detected by the chipset before the processor comes out of reset. Dell devices are configured with the most restrictive policy for Boot Guard which blocks all code access if the boot block verification fails during the Boot Guard check. This policy “bricks” the system, to limit any further adversary activity, and to reduce the overall incentive for tampering.

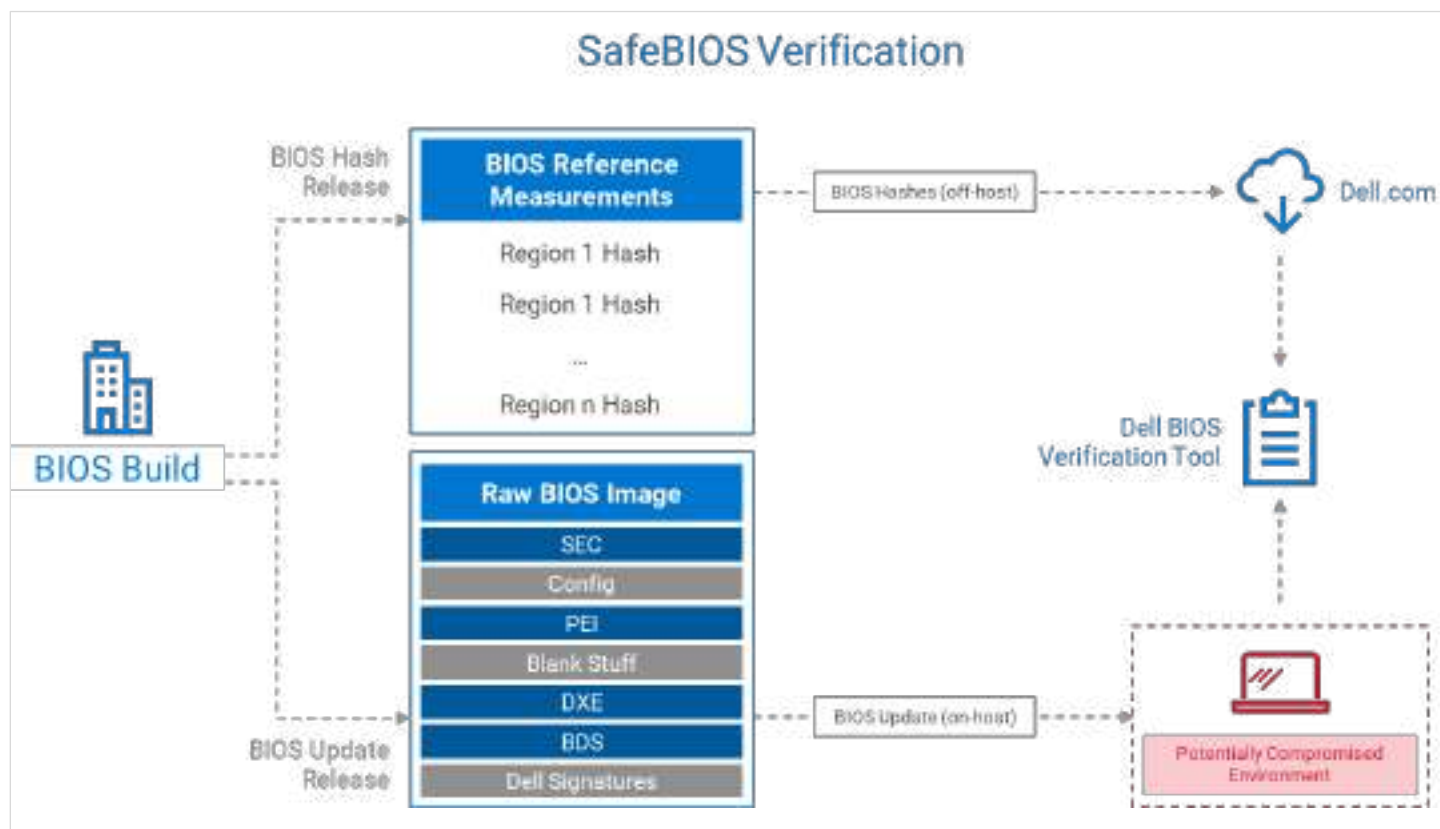


Figure 7: SafeBIOS Verification Flow

While technologies like Intel Boot Guard offer effective protection and detection capabilities for the root of trust, some customers may be concerned that the Boot Guard checks are only enforced once per boot or that the digital certificates used for verifying the boot block are resident on the endpoint. Dell commercial PCs have a feature called SafeBIOS Verification that addresses both concerns. SafeBIOS Verification uses an OS-resident application – the Dell Trusted Device, or DTD – to verify the integrity of the BIOS against known-good off-host reference measurements at any time. These reference measurements are generated for each BIOS version during the BIOS build process inside Dell infrastructure. Invoking this capability at a regular cadence greatly reduces the window of time that malicious code can be present on a system before detection, even in the extremely unlikely event that all boot-time prevention capabilities were somehow bypassed.

Intel Management Engine (ME) Firmware Verification

As previously mentioned, the Intel Converged Security and Management Engine (CSME or just “Intel ME”) plays an important and privileged role in the boot process and the overall operation of the system below the OS. The Intel ME Firmware Verification component of Dell Trusted Device detects unauthorized tampering of the early boot stages of this highly privileged firmware. Built exclusively for Dell commercial PCs as an off-host check, this built-in feature within the SafeBIOS framework provides this additional level of insight for Intel vPro systems.

Hardware-Assisted Security with CrowdStrike and Intel

To provide faster threat detection, Dell worked with CrowdStrike and Intel to deliver an endpoint security solution that brings together the power of hardware and software to enhance threat detection and response. The joint “hardware-assisted security” solution allows administrators to combine CrowdStrike’s threat intelligence database with below-the-OS device telemetry for greater insight into potential breaches. With the Dell Trusted Device (DTD) Application enabled, Dell commercial PCs push data from multiple built-in security features to the OS, and surface that data for integration with third-party software solutions. With CrowdStrike Falcon XDR added on-the-box, an admin can collect device security data coming from SafeBIOS alerts for further investigation within the CrowdStrike console.

This collaboration enhances software security by providing another layer of defense with improved visibility and observability at the firmware level – an area of the device where we have seen an uptick malicious and persistent threats in recent years. CrowdStrike software can catch activity deviating from the known good, but Dell device telemetry will also surface rapid alerts from, e.g., SafeBIOS Indicators of Attack, to ensure timely response and remediation of an affected device.

Dell PCs provide the visibility and actionability needed to disrupt attacks by leveraging BIOS/firmware protections and Intel® Control-flow Enforcement Technology (Intel® CET) to help shut down the entire class of ROP attacks. CrowdStrike’s Hardware Enhanced Exploit Detection (HEED) integrates Intel® Processor Trace (Intel® PT) CPU telemetry to extend memory safety protections for coded injection techniques, across PC fleet generations.

In addition, CrowdStrike has re-imagined how to stop fileless attacks early in the kill chain by using the accelerated memory scanning algorithms of Intel TDT and its ability to offload processing to the Intel® Graphics Technology integrated graphics processor. The resulting 4-7x performance acceleration helps ensure a performant user experience while applying CrowdStrike’s dynamic, earlier, IOAs to the memory layer – and it’s only available on Intel® processor-based PCs. As fileless attacks attempt to move down the stack, Dell SafeBIOS uses the Intel vPro platform’s Intel® System Resource Defense technology to restrict system privileges and malicious access to the OS.

The solution is [described in this solution brief](#).

Intel® vPro Integration for Out of Band Management

Dell has an integration with Intel vPro which provides enhanced security and the ability to remediate and securely wipe a device. The Dell Client Command Suite uses the Intel vPro platform's out of band management capabilities to equip administrators with remote keyboard/video/mouse (KVM) to wake a device, wipe its main drive, or initiate an Intel® Firmware Guard assisted firmware update to reliably reduce the possibility of in-the-field system crashes. The integration of these capabilities provides a unique, multilayer defense-in-depth that improves a SecOps team’s effectiveness and efficiency as they protect, correct, and respond to evolving cyberthreats. These capabilities come standard with all Intel vPro equipped devices.

Microsoft Intune Integration

Microsoft Intune is a flexible platform that integrates various services for IT administrators, enabling them to oversee and control a range of devices, including mobile devices, desktop computers, virtual machines, embedded devices, and servers.

Administrators can create compliance policies in the Intune admin center to ensure that SafeBIOS and other Dell 'built-in' capabilities – through the DTD application – are protecting Dell computers below the operating system. DTD uses PowerShell scripts and agent-level configuration to communicate endpoint compliance and transmit results to Microsoft Intune.

The DTD Script folder contains the required script and configuration file which can be imported to create and deploy custom policy in Intune. The result is displayed in Intune compliance page.

More information and instructions are available here: [Dell Trusted Device – Installation and Administration Guide v6.0 | Dell US](#)

Other Integrations for SafeBIOS

Security Information and Event Management (SIEM) solutions play a critical role in enhancing the cybersecurity posture of organizations by providing comprehensive tools for real-time monitoring, analyzing, and responding swiftly to security events. These solutions collect and aggregate log data generated throughout the organization's technology infrastructure, including networks, applications, and endpoints. SIEM tools leverage advanced analytics and correlation algorithms to identify patterns and anomalies in the data, helping security teams detect and investigate potential security incidents.

Dell Trusted Device (DTD) can interoperate with SIEM solutions and supports the following features:

- BIOS Verification
- Intel ME Verification
- BIOS Events & Indicators of Attack
- Image Capture
- Security Score
- CVE Detection

The Dell Event Repository must be installed to deliver DTD results to a SIEM solution.

SafeBIOS Indicators of Attack

Dell SafeBIOS Indicators of Attack (IoA) extends tamper detection capabilities beyond the code into the BIOS configuration arena. Various compliance and security tools have been able to detect changes to operating system settings and a small subset of BIOS settings (typically only Secure Boot) in the past, but these tools usually lack any kind of temporal context for these detections. These prior solutions were designed for compliance or drift detection and may still allow an attacker to carry out multiple configuration changes and then revert to a "known good" state to avoid detection.

The Dell SafeBIOS IoA feature addresses this gap by using Dell threat modeling exercises and expertise to define specific chains of multiple configuration changes that could introduce risk to the system or signal the early signs of an in-progress attack. The configuration attributes in each of these chains are continuously monitored by the Dell Trusted Device Application, and risk evaluations are logged as these chains are traversed on the system. This allows the administrator or security analyst to take remediation actions as needed based on incremental risk associations and potentially before the next stage of the attack is deployed against the weakened configuration.

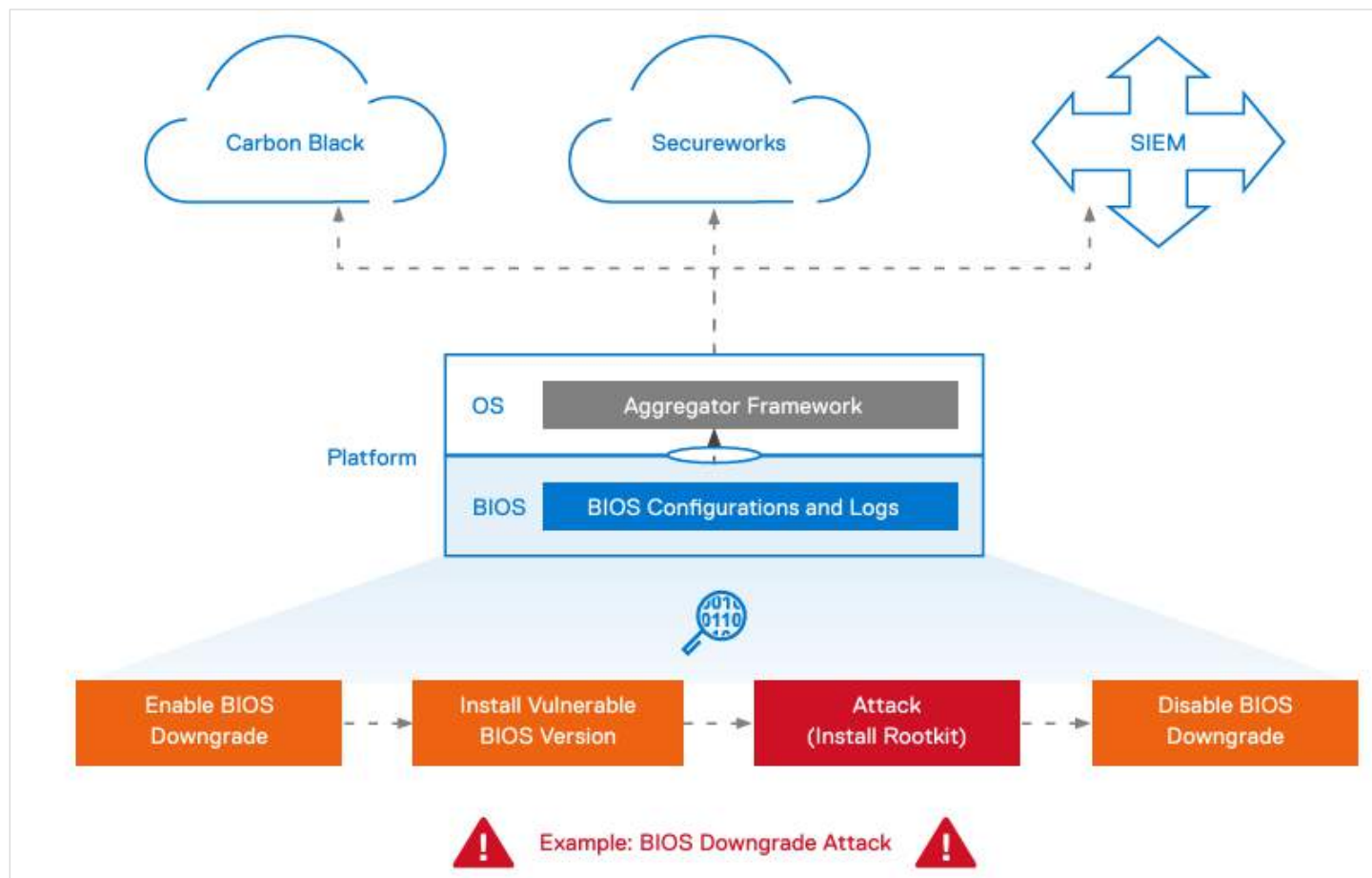


Figure 8: SafeBIOS Indicators of Attack

Common Vulnerabilities and Exposures (CVE) Detection

This feature permits identification of known vulnerabilities on a Dell device with a built-in security check.

- CVE Detection uses an intelligent, built-in monitoring feature that scans for publicly reported security flaws on a Dell device and provides recommendations on how to fix them. It proactively assesses device health against a database of publicly disclosed computer security flaws maintained in the U.S. National Vulnerability Database by the National Cybersecurity's federally funded research and development center (FFRDC), operated by the MITRE Corporation and funded in part by the U.S. Department of Homeland Security.
- CVE Detection also scans for vulnerabilities based on specific PC models and BIOS versions, recommending the relevant patch for swift remediation. While CVE Detection will eventually be available for BIOS, firmware, applications, and drivers, it will initially launch for BIOS vulnerabilities only.

TCG Measured Boot

As mentioned in an earlier section, TCG Measured Boot on the Dell device uses the TPM as a protected area for storing hashes of BIOS, firmware, and bootloader code and configuration that is loaded and/or executed in the boot process. The TPM is designed to store these events in a secure way that can be cryptographically verified after the boot completes through a process called attestation. More information about how the TPM works can be found in the TCG [TPM 2.0 Library Specification](#).

The functionality needed to support TCG Measured Boot is built into the TPM using registers with very specific properties called PCRs (Platform Configuration Registers). These PCRs cannot be written to directly: they can only be 'extended.' Extending is a relatively simple operation in practice but is incredibly useful for code integrity. Internal to the TPM, each PCR extension operation takes the current state of the PCR, concatenates it with the incoming message or data to extend, and then hashes it using the selected algorithm, e.g., SHA-256, before recording it to the PCR. This creates a PCR value cryptographically dependent on all extended operations (and their order) that occurred since the PC was reset.

Code, Configuration, and the TPM Event Log

Each Dell commercial device extends code and configuration information to the TPM PCRs during every boot in accordance to the [TCG PC Client Platform Firmware Profile Specification](#).

There are many PCRs in each TPM. Table 2 provides a high-level overview of some of the TPM PCRs used on the platform. To maximize compatibility across PC vendors, the TCG PC Client Platform Firmware Profile Specification describes which specific PCR indexes in the TPM should be included in each type of measurement during the boot process. For example, pre-boot BIOS code that executes from the internal SPI flash is extended to PCR0 while UEFI drivers that execute from add-in devices are extended to PCR2. Dell devices extend BIOS Setup options that are security related to PCR1 in addition to hardware information such as memory configuration.

PCR Number	Function / Allocation
0	BIOS Code

PCR Number	Function / Allocation
1	BIOS Settings / Platform Configuration
2	UEFI Option ROMs
3	UEFI Option ROM Configuration
4	Boot Loader / Master Boot Loader (MBR)
5	Boot Loader / Master Boot Loader (MBR) Configuration
6	Platform Manufacturer Specific Measurements
7	Secure Boot
8-15	Static Operating System
16	Debug
23	Application Support

Table 2: Standard PCR Allocations

The Dell device BIOS creates a TPM event log entry each time a new measurement is extended to any TPM PCR during the boot process. The TPM event log allows verifiers such as the OS or remote entities to reconstruct the record of code in the event of a mismatch to an expected or known-good value. The TPM measurements persist for one boot cycle. Upon reboot, the TPM PCRs are 'reset', and the TPM event log is cleared. The TPM PCR measurements and the event log are recreated on every boot.

NIST 800-155 Measurements

One unpublicized feature of Dell devices with Intel processors that may be interesting to readers is the inclusion of PCR0 "reference measurements" directly embedded into each BIOS update utility. This feature aligns to the NIST SP800-155 BIOS Integrity Measurement Guidelines (still in draft revision) and can be used to determine the Dell authorized values for the BIOS code region measurement that the BIOS extends to PCR0. The value can then be compared to the measured value in the TPM event log on the device to verify the BIOS code running on the platform. To export these reference measurements, use the /BIOSMeasurement command line option on any Dell device BIOS update utility. An example of the content and format of the output of this command appears below:



Figure 9: Example BIOS Measurements

Advanced: NIST 800-155 Measurements Extraction, Conversion, and Comparison

Use the following steps to extract and compare the NIST 800-155 measurements from the BIOS update utility with the device's TPM PCR event log measurement.

- Create a NIST800-155 xml output file from the BIOS firmware update utility
 - At a command prompt, execute: Latitude_7X00_1.9.1.exe /BiosMeasurement
 - Locate the output file. e.g., Latitude_7X00_1.9.1_pcr0.xml from the above step.
 - This is the NIST 800-155 Measurement XML file
 - Open the file, and find the SHA1 and / or SHA256 PCR 0 values
 - Convert the BASE64 PCR 0 value to HEX (use an online tool)
 - Save value for comparison.
- Get the TPM PCR Event Log from the device (booted to the OS).
 - Use a tool to read the device's TPM PCR Event Log.
 - Find the PCR0 'EV_Post_Code' entry in the log.
 - Compare this value to 1.e). The values should match.

Physical Security Features – Chassis Intrusion

Dell commercial devices – including Latitude, OptiPlex and Precision Workstation systems (fixed and mobile) include chassis intrusion detection circuitry and logging capability that can be monitored via Intune/SCCM, Client Command Suite, VMware Workspace ONE and other common systems management platforms. Chassis intrusion combines with other built-in, below the OS security features to strengthen the Dell device defense in depth layered strategy. Complementary features already implement layers of security for defending below the operating system, such as protecting against and detecting tampering, but it's important to also support early detection as soon as the chassis has been opened, which is typically the first sign of a physical attack.

Ability to Block Boot after Chassis Intrusion

A new optional BIOS setting prevents system boot when chassis intrusion is detected. This new option, called "Block Boot Until Cleared", will prevent the system from booting when a chassis intrusion event is detected. This option is only available when Chassis Intrusion is set to "Enabled". When the POST message is displayed, the only option will be to enter setup, where a user can use the "Clear IntrusionWarning" checkbox to acknowledge the intrusion event.

TPM integration for Chassis Intrusion events

When chassis intrusion is detected, an event is recorded in the TPM event log, and extended to TPM PCR1. This can be used to protect TPM-sealed keys, such as Microsoft Windows Bitlocker encryption keys, preventing Bitlocker decryption of the hard drive when a chassis intrusion event is detected. The BIOS will record an EV_ACTION event with string "Chassis Intrusion" to the crypto agile log. The event digest will be a hash of the event string and extended to PCR1. When the chassis intrusion warning is cleared, the EV_ACTION event will not be recorded.

Battery Removal Detection

Removing the battery from a system results in an event being logged in the BIOS event log. To supplement Chassis Intrusion detection events, this new battery removal event can be used by security analysts to detect potential system tampering. When a battery is removed or replaced, this event will appear in the log on the subsequent normal boot: "Alert! Battery previously removed."

SPI Flash Anti-Tamper features

Dell Commercial Devices also include new technology which detects and prevents tampering with BIOS SPI flash chips on the motherboard. While the system is powered on, the Dell Embedded Controller (EC) monitors electrical signals controlling the BIOS SPI Flash storage chip. If BIOS SPI flash chip tampering is detected by the EC, an event is logged in the BIOS event log, and a warning may optionally be displayed. When the system is powered off, the Dell Embedded Controller will shunt the electrical signals, such that BIOS SPI flash data cannot be accessed with an offline flash programming "chip clip".

Respond and Recover

From the NIST framework:

Respond: Develop and implement appropriate activities to respond to a detected cybersecurity incident.

Recover: Develop and implement appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity incident.

Respond and Recover are often the most overlooked functions within the NIST Cybersecurity Framework. Admitting that a failure or attack has occurred or that an unknown vulnerability has been exploited by an adversary can be uncomfortable at times. Being well prepared to handle these incidents and having the confidence to be able to restore the Dell device back to normal operating status as quickly and efficiently as possible can help to minimize the overall cost of these events.

Embedded Controller Recovery

As mentioned previously the Dell device embedded controller, or “EC”, operates as the root of trust of the system at the very lowest level of hardware enablement. This privileged context and critical role requires a high degree of fault tolerance to avoid false positives and keep the beginning of the chain of trust intact, secure, and resilient. To address this, the Dell device EC supports dual firmware images and a failover mode to allow a backup firmware to recover the primary image if needed.

BIOS Recovery

In addition to having a secure and resilient EC, it is also critical that the next stage of the boot process, the BIOS, also has a robust recovery mechanism. While it may not have been previously included in the overall security conversation, the Dell device has a sophisticated set of flexible and tunable features that ensure that the BIOS can be reverted to a known good copy if compromised. Additionally, once BIOS recovery is invoked, it will securely capture the state of tampering for offline analysis for those customers that require that deep insight into their adversaries’ techniques.

Dell devices have a sophisticated set of flexible and tunable features that ensure that the BIOS can be reverted to a known good copy if compromised.

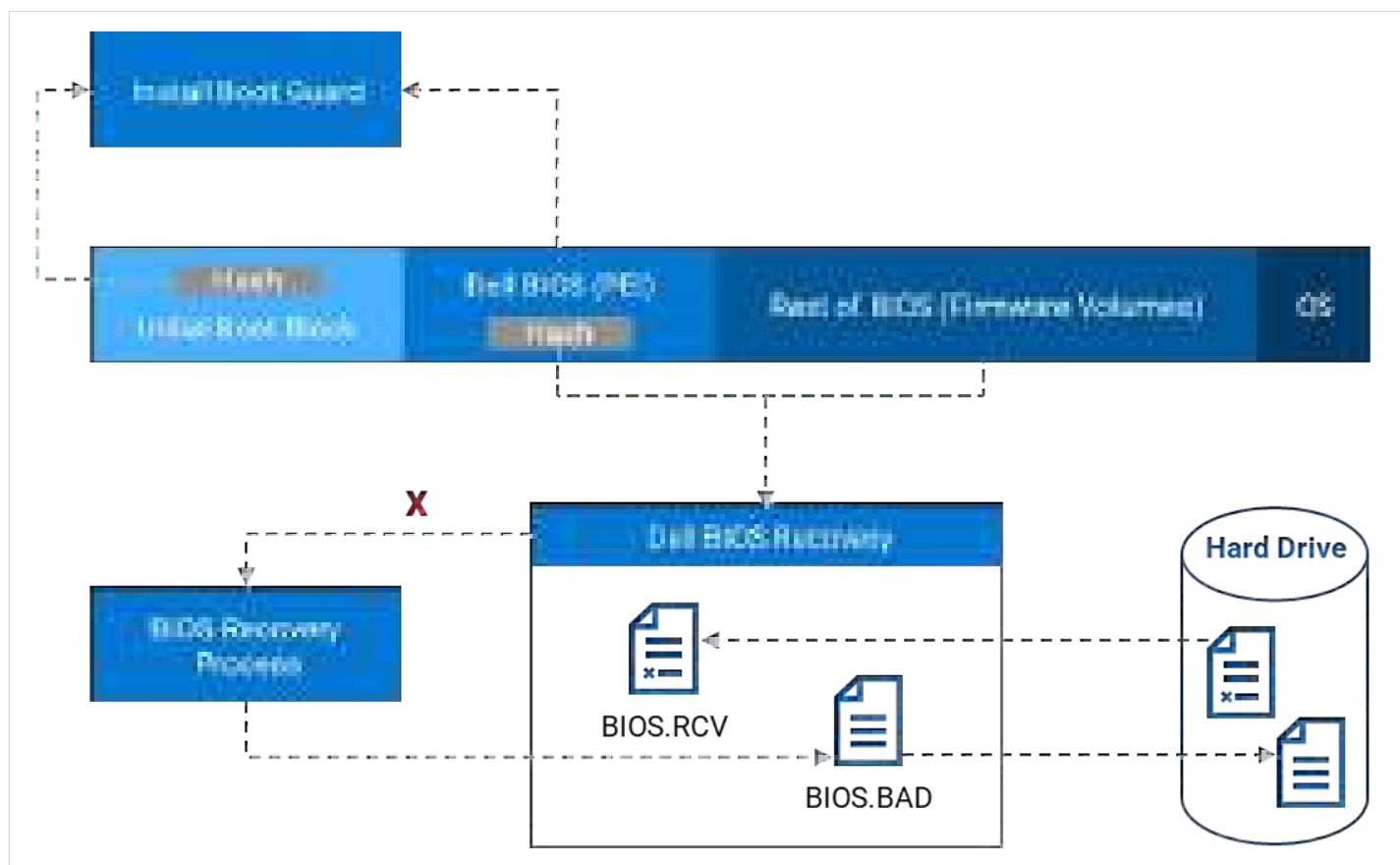


Figure 10: SafeBIOS Recovery Flow

BIOS Recovery Image Update Flow

BIOS recovery is engineered right into the Dell BIOS update architecture, each Dell device can prepare days, months, or even years before any potential trigger to recover is ever required. Essentially this is part of every BIOS update on the system; in addition to updating the BIOS running on the system the BIOS update tool will copy a recovery version of the new BIOS to the EFI partition on the hard drive. The EFI partition is a hidden partition that is independent of the operating system hard drive partitions. This partition is modifiable with physical or OS administrative access, so it's important to note that the recovery image is signed in the same manner as the updated version and verified by the BIOS RTU prior to performing recovery.

BIOS Recovery

BIOS Recovery from Hard Drive – This option is set by default. Allows you to recover the corrupted BIOS from a recovery file on the HDD or an external USB key.

BIOS Auto-Recovery – Allows you to recover the BIOS automatically.



NOTE: BIOS Recovery from Hard Drive field should be enabled

Auto Recovery Flow

Dell devices can be configured to automatically recover the BIOS to a known good copy when the early BIOS code detects an integrity violation during pre-boot. To support this, the early BIOS (the Pre-EFI Initialization phase, or PEI, in UEFI terminology) can read the BIOS recovery image from the hard drive or USB and verifying the signature of the recovery image using the same Root of Trust for Update (RTU) that protects the BIOS update process (i.e. NIST 800-147).

Customer Flexibility: Manual Recovery

The BIOS Auto-Recovery option is disabled by default on Dell devices. This may at first seem misaligned with the overall security and threat model assumptions of the Dell device. However, this default was designed to support customers whose threat models prioritize detection of BIOS tampering or corruption well above the need for high availability/resilience that may mask potential adversarial activity.

SafeBIOS Image Capture

As previously discussed, Dell devices include built-in features available to all customers that were designed to support the most advanced customer threat models. Customers that are concerned about sophisticated adversaries tampering with BIOS would likely also be concerned about the intention, and even identity, of those adversaries. To support this, the Dell SafeBIOS Recovery feature includes an image capture function to save the tampered or corrupted BIOS to the system hard drive during any recovery operation. This image is saved as a simple binary file that can be harvested by system security software such as the Dell Trusted Device Application. Once again, this image can be collected by a compatible app for analysis at scale. Experienced analysts within customers' security operations control (SoC) can evaluate this file using methods that already exist for analyzing malware during more common hunting operations.

Dell Data Wipe

Dell devices produced since 2017 include the Dell Data Wipe feature. Dell Data Wipe allows customers to securely delete data on the internal storage devices in their Dell device. This allows efficient erasure for repurpose or redeployment using industry standard commands based on the NIST 800- 88r1 standard. The feature is supported on internal SATA, SSD, NVMe and eMMC storage devices. It uses industry standard methods such as Enhanced Security Erase for SATA, format NVM for NVMe, and Sanitize for eMMC based devices. (See [NIST Special Publication 800-88r1](#) Guidelines for Media Sanitization for more details.)

Dell Data Wipe removes all user data from the storage device. To protect the device from unauthorized wipe of media, the feature is only accessible by a physically present user through the BIOS Setup (F2) interface. Any user who has access to the BIOS Setup Menu can initiate the wipe. The user interface includes multiple confirmation prompts to ensure data wipe cannot be triggered accidentally. So, the user must be physically present until data wipe begins. Once initiated, the data wipe will proceed until all storage devices are wiped.

- Allows user-initiated data wipe of internal storage devices (SATA/SSD/NVMe/eMMC) using industry standard technology.
- Invokes acceptable media purge per NIST Special Publication 800-88 Revision 1 Guidelines for Media Sanitization by invoking media specific commands.

- User interface includes multiple confirmation prompts to ensure data wipe cannot be triggered accidentally.
- Commonly referenced DoD 5520.22-m “multi-pass” requirements were defined before ATA SECURITY ERASE and sanitization method table has been removed from 5520-m. NIST SP800-88r1 widely accepted as more relevant data sanitization standard, most recent update (Dec 2014) includes storage technologies such as NVMe, SSD, etc.

More information about Dell Data Wipe is available [here](#).

Additional Dell Security Capabilities

Protected Signing Infrastructure

Code signing and protecting access to private keys and certificates within the signing infrastructure is a critical piece of any software or firmware supply chain. Once again, this vital component of the supply chain is also an area most targeted by sophisticated adversaries.

- **Threat: Unauthorized Code Signing**

There are countless examples of supply chain attacks that resulted in stolen digital signing certificates or credentials being used to sign malware. The danger in this scenario is that it is challenging for customers, anti-virus software, and existing tools to differentiate between legitimate and potentially malicious code signed with the same certificate. One example of this activity can be found [here](#).

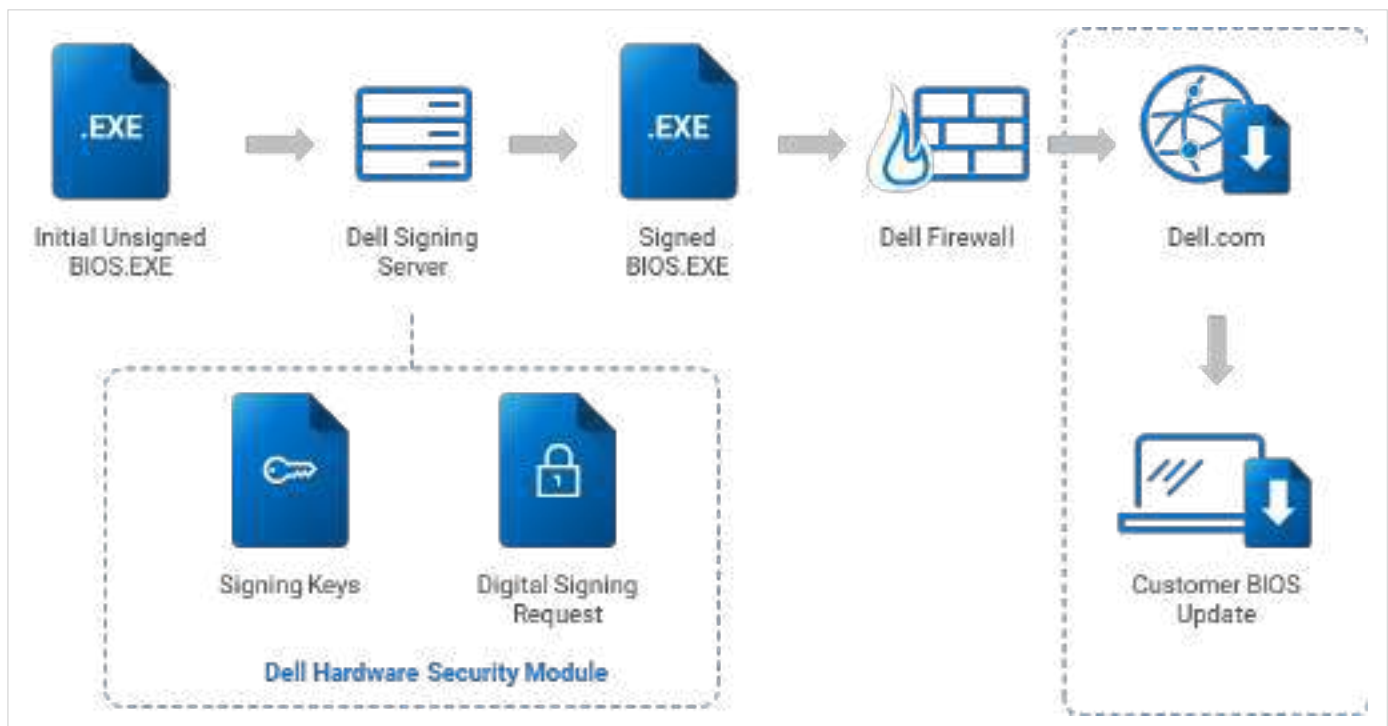


Figure 11: Dell SafeBIOS Signing

- **Mitigation: Signing Infrastructure**

Dell devices use secure signing infrastructure and hardware security modules, or HSMs, for code signing. This infrastructure is managed by Dell Cybersecurity, includes disaster recovery mechanisms, and is protected from unauthorized access using user access control and hardware binding. The Dell device BIOS signing capability is integrated directly into the automated build processes and developers do not have direct access to sign BIOS updates. This infrastructure signs the outer encapsulated BIOS update, Intel Boot Guard IBB, and Intel BIOS Guard code updates.

The Future of Security

Organizations rely on hardened endpoints to defend against modern and sophisticated adversaries and Dell has invested heavily in the security and resilience of the Dell devices to meet this demand. Transparency remains a critical tenet in computer security and hopefully this document has served to provide a comprehensive look into not only the details and intentions behind these features but also some of the limitations.

We understand that Dell devices are only one piece of the security puzzle for our customers. While our investments in device hardening are an important foundation for overall ecosystem security, we continue to prioritize integrations with security software and solutions that help customers maximize the benefits of what we've built. Integrating into security ecosystems and architectures such as Zero Trust ensure Dell telemetry can be used to enrich user and network access policy tied to the health of the device. This rich telemetry evolves as the landscape evolves and it's exciting to help build the future integrations across not only Zero Trust but to create the basis of data to take full advantage of the AI security evolution over the coming years.

References

Dell and Partner References

- [A Partnership of Trust: Dell Supply Chain Security](#)
- [Achieving pervasive security above, within and below the OS](#) – Dell Technologies and Intel, July 2023
- [Dell, Intel and CrowdStrike – Joint Solution Brief](#)
- [BIOS Security – The Next Frontier for Endpoint Protection](#) – A Forrester Consulting Thought Leadership Paper Commissioned by Dell – June 2019
- [UEFI on Dell BizClient Platforms](#)
- [Intel Hardware Shield](#)
- Dell KB [Find Your Service Tag or Serial Number](#)
- Dell KB [Using Dell Command Configure to Set the Asset Tag Information of Your Dell Computer](#)
- Dell KB [Dell Data Wipe](#)

- Dell [Secured Component Verification \(SCV\) Datasheet](#)
- [Dell Trusted Device – Installation and Administration Guide – v6.0](#)
- [Dell Trusted Workspace](#)
- [Dell Client Signed Firmware Update](#)

Industry Organizations

- UEFI Tianocore Project – <https://github.com/tianocore/edk2>
- [SAFECode](#) – The Software Assurance Forum for Excellence in Code
- [TCG](#) – Trusted Computing Group
- [FIRST](#) – Forum of Incident Response and Security Teams
- [OTTF](#) – Open Group Trusted Technology Forum
- [IEEE Center for Secure Design](#)

Standards and Guidelines

- [NIST Cybersecurity Framework](#) – NIST Publication "The NIST Cybersecurity Framework (CSF) 2.0" - February 26, 2024
- [NIST Cybersecurity Framework](#) – Main Page
- [NIST Special Publication SP 800-193](#) – Platform Resiliency Guidelines
- [NIST Special Publication SP 800-147](#) – BIOS Protection Guidelines
- [NIST Special Publication SP 800-88](#) (r1) – Guidelines for Media Sanitization
- [NIST Special Publication SP 1800-34](#) – Validating the Integrity of Computing Devices
- [FIPS Publication 186-5](#) – Digital Signature Standard (DSS)
- [National Security Agency Cybersecurity Report UEFI Defensive Practices Guidance](#)
- NSA Cybersecurity Information Sheet: [Procurement and Acceptance Testing Guide for Servers, Laptops, and Desktop Computers](#)
- [ISO/IEC 27034-1:2011](#) – Information Security Techniques for Application Security

Quoted Stats

- [Estimated cost of cybercrime worldwide 2017 – 2028](#) – Statistica.com

Dell Data Wipe

Resumo: Saiba como implementar, gerenciar, proteger e virtualizar soluções de BYOD, de Enterprise Client e de mobilidade com especialistas e colegas

Conteúdo do artigo

Sintomas

Dell Data Wipe é um recurso no BIOS do Dell Enterprise Client que possibilita que nossos clientes solicitem uma limpeza de dados dos dispositivos de armazenamento interno em seu sistema. Isso possibilita uma eliminação eficiente para fins de realocação ou nova implementação usando os recursos de limpeza de dados padrão do setor já compatíveis com os dispositivos de armazenamento da Dell.

Como os dados do cliente são uma prioridade para a Dell, desenvolvemos esse recurso para garantir a máxima compatibilidade e o potencial mínimo de eliminação não intencional de dados.

- Oferece suporte apenas para dispositivos de armazenamento interno: disco rígido SATA, SSD e eMMC, dependendo dos tipos de dispositivos compatíveis com o sistema.
- Usa métodos aprovados padrão do setor para limpeza de dados, como Secure Erase para SATA e Sanitize para eMMC. Consulte as diretrizes da NIST Special Publication 800-88 sobre limpeza de mídia para obter mais detalhes.
- Pode ser acessado somente por um usuário presente fisicamente. O usuário deve estar fisicamente presente até que a limpeza da unidade comece. (Os clientes podem usar o Dell vPro Extensions para fazer a limpeza remotamente. Consulte [Gerenciamento de sistemas Dell Business Client fora de banda usando o Intel AMT vPro](#) para obter mais informações sobre limpeza remota.)
- Todas as unidades internas no sistema passam pela limpeza, sem a opção de limpar apenas determinados dispositivos de armazenamento.

O recurso Data Wipe é acessado na configuração do BIOS. Na tela inicial da Dell, pressione F2 para entrar na configuração do BIOS.

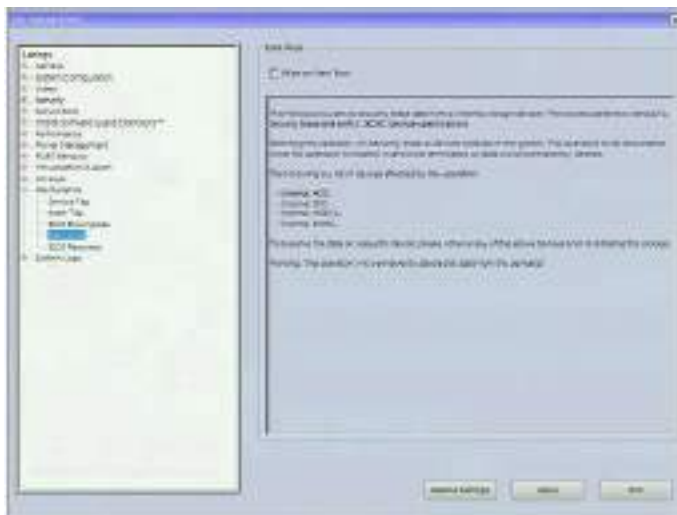


Figura 1: Dell Latitude E7470

No aplicativo de configuração do BIOS, o usuário pode selecionar "Limpar na próxima inicialização" na opção **Manutenção -> Data Wipe** para chamar a limpeza de dados para todas as unidades internas após a reinicialização.

O BIOS solicitará a confirmação do usuário duas vezes antes de permitir que ele saia da configuração com a opção "Limpar na próxima inicialização" selecionada. O objetivo disso é garantir que o usuário realmente pretende limpar todos os dispositivos de armazenamento.

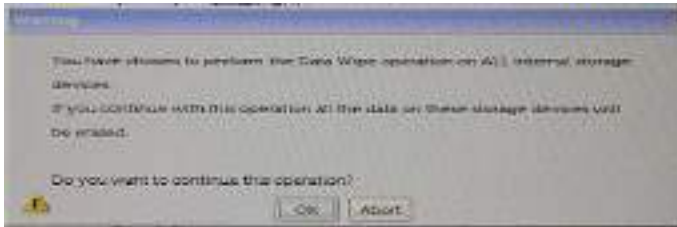


Figura 2: operação do Data Wipe

Como medida de segurança adicional, o BIOS ajustará a seleção padrão para um prompt final a fim de reforçar ainda mais a aceitação direta dessa operação por parte do usuário.



Figura 3: dispositivos de armazenamento interno

Depois que a opção for selecionada e os prompts forem confirmados, o usuário sairá da configuração do BIOS para forçar uma reinicialização do sistema e iniciar o processo de limpeza de dados.

Após a reinicialização, o BIOS solicitará novamente várias confirmações antes de enviar as instruções de limpeza de dados para os dispositivos de armazenamento do cliente.

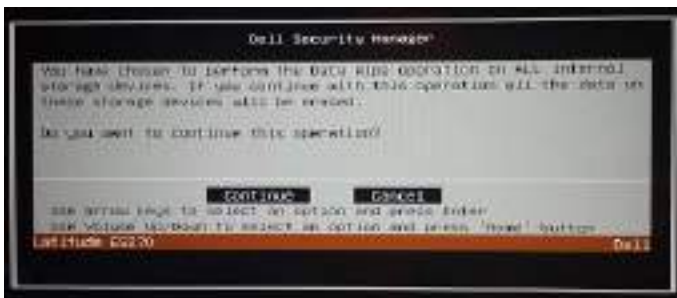


Figura 4: Dell Security Manager

O usuário pode optar por cancelar o procedimento de limpeza da unidade em qualquer um desses prompts. Se isso ocorrer, o acionador da limpeza de dados será reiniciado. O processo deverá ser reiniciado na configuração do BIOS para reiniciar o procedimento de limpeza, se desejado.



Figura 5: Latitude E5270

Assim que o usuário confirmar todos os prompts, o BIOS começará a limpeza das unidades internas. Será exibida uma barra de andamento, pois algumas tecnologias de unidade podem levar de vários minutos a muitas horas para limpar a unidade.



Figura 6: dispositivos SATA internos

A exibição de uma caixa de diálogo verde com a mensagem "Data Wipe Completed Successfully" (Limpeza de dados concluída com sucesso) relata o êxito na execução de um procedimento de limpeza. Se houver falhas, elas serão apresentadas em vez da caixa de diálogo de sucesso na limpeza.



Figura 7: reinicie o sistema

Você encontrará mais informações sobre como fazer a limpeza dos dados no artigo da Base de conhecimento Dell [Como limpar os dados de meu disco rígido?](#)

Propriedades do artigo

Data da última publicação

10 Apr 2021

Versão

3

Tipo de artigo

Solution

Tudo pronto para a TI com o Ready Image



Em todo o mundo,
81 mil unidades de
imagens a cada
semana.

Eleve seus recursos
de imagem com a
capacitação em nuvem.

Dell Ready Image — integrando e aperfeiçoando

Pronta quando você estiver

Um número cada vez maior de clientes quer opções para carregar uma imagem. Seja uma imagem limpa sem software adicionado ou um sistema operacional estável para provisionamento sem erros, a Dell tem o Ready Image — pronta para você.

Aperfeiçoando

O Dell Ready Image da Dell está enriquecendo nossa capacidade atual para torná-la uma oferta independente, pronta para pedidos. O que isso significa para você, cliente de TI? Significa que você pode acessar, habilitar, implementar e recuperar sua imagem por meio da nuvem.

Capacidades

Aproveitando a nuvem, estamos acelerando a entrega de imagens. Oferecida como independente ou em conjunto com outra oferta, o Ready Image é uma solução projetada para beneficiar seus esforços de TI.

Sabemos que não é fácil dar suporte a uma força de trabalho cada vez mais remota. Por isso, a Dell integrou o Ready Image ao nosso serviço Self-Healing Image Recovery, que oferece aos administradores de TI o controle da recuperação remota de imagens na nuvem. Os usuários podem iniciar a recuperação, mas os administradores têm todo o controle.

Principais benefícios

- Idioma de sua escolha
- Carregue a versão do sistema operacional de sua escolha
- Apenas sistema operacional MSFT — reduzindo aplicativos de caixa de entrada e software de terceiros
- Integra-se a soluções da Dell como ProDeploy Client Suite, Connected Provisioning e outros serviços de configuração.

Entre em contato hoje mesmo com seu representante de vendas

Recuperar o BIOS em um computador ou tablet Dell após uma falha de inicialização ou POST

Resumo: Guia de recuperação do BIOS da Dell: Corrigir falha de inicialização, tela preta ou erros de POST. Fáceis instruções por etapas para os métodos de recuperação por disco rígido e por USB.

Artigo detalhado

Instruções

A recuperação do BIOS restaura o firmware corrompido do BIOS em computadores Dell. Use este procedimento se o computador não iniciar, exibir uma tela preta, mostrar padrões piscantes de LED ou falhar no autoteste de inicialização (POST).

 **Nota:** A recuperação do BIOS afeta apenas o firmware do BIOS/UEFI. Os dados e a instalação do Windows permanecem inalterados.

Como recuperar-se de problemas de inicialização usando a ferramenta de recuperação do BIOS



Duração: 03:49

Quando disponíveis, as configurações de idioma de legendas podem ser escolhidas usando o ícone de CC ou Configurações deste player de vídeo.

Quando usar a recuperação do BIOS

Use a recuperação do BIOS se o computador Dell apresentar qualquer um destes sintomas:

- Liga, mas não inicia ou não mostra a tela de inicialização (ausência de POST)
- Mostra uma tela preta na inicialização, sem o logotipo da Dell
- As luzes de LED piscam em padrões (especialmente padrões 3,6 ou 3,7, indicando um BIOS corrompido)
- Exibe mensagens de erro "BIOS corrupted" ou semelhantes
- Reinicia continuamente sem inicializar

Não use a recuperação do BIOS se:

- O computador inicializa no Windows normalmente. Em vez disso, use o procedimento padrão de atualização do BIOS.
- Você vê mensagens de erro do hardware. Em vez disso, execute o diagnóstico.
- O computador apresenta danos físicos ou derramamento de líquido.

Noções básicas sobre métodos de recuperação

Os computadores Dell oferecem suporte a dois métodos de recuperação do BIOS:

Método 1: Recuperação por disco rígido (método recomendado; tente esse primeiro)

- Usa um arquivo de recuperação armazenado no disco rígido do computador
- Nenhuma preparação necessária
- Ativado por padrão em sistemas compatíveis
- Método mais rápido e fácil

Método 2: Recuperação por unidade USB (use se o Método 1 não funcionar)

- Usa um arquivo de recuperação em uma unidade USB
- Requer preparação em um computador que esteja funcionando
- Use esse método se a recuperação por disco rígido falhar ou não estiver disponível

Como funciona o recurso de recuperação do BIOS

Ao iniciar a recuperação do BIOS:

1. Se uma unidade USB estiver conectada, o sistema a procurará primeiro
2. Se nenhuma unidade USB estiver presente ou nenhum arquivo de recuperação for encontrado na USB, o sistema procurará o disco rígido
3. Se nenhum arquivo de recuperação for encontrado nesses locais, a recuperação apresentará falha

Embora o sistema procure a unidade USB primeiro, quando ela estiver presente, nós recomendamos tentar realizar primeiro a [recuperação por disco rígido](#) porque ela não requer preparação. Somente crie uma unidade de recuperação USB se necessário.

O que é necessário

Para todos os dispositivos:

- Bateria carregada em pelo menos 25% para notebooks (50% para tablets)
- Adaptador CA ou cabo de alimentação conectado durante a recuperação

Para desktops e all in ones:

- Teclado USB com fio (teclados Bluetooth ou sem fio não funcionam)

Para recuperação por USB (se necessário):

- Outro computador que esteja funcionando com acesso à Internet
- Insira a etiqueta de serviço ou o código de serviço expresso da Dell
- Unidade flash USB vazia (pelo menos 2 GB)

Método 1: Recuperação do BIOS por disco rígido (recomendado)

Tente esse método primeiro. Os computadores Dell mais recentes já têm um arquivo de recuperação do BIOS armazenado no disco rígido.

 **Nota:** Não crie uma unidade USB ainda. Tente primeiro a recuperação por disco rígido para economizar tempo.

A recuperação por disco rígido funcionará se o computador atender a estas condições:

- Tem o disco rígido original de fábrica (não foi substituído)
- O sistema operacional não foi reinstalado ou a unidade não foi reformatada

- O modo de inicialização do BIOS está definido como UEFI (não Legacy)
- A unidade não está criptografada com o BitLocker ou não tem uma [senha de disco rígido do BIOS](#)

Se você não tiver certeza se essas condições se aplicam ou não, tente primeiro fazer a recuperação por disco rígido. O processo indicará se não encontrar um arquivo de recuperação.

Etapa 1: Iniciar a recuperação do BIOS

Localize o tipo de dispositivo abaixo e siga estas etapas:

Desktop ou all in one

1. Certifique-se de que nenhuma unidade USB esteja conectada
2. Ligue o computador
3. Pressione juntas as teclas `Ctrl` + `Esc` e as mantenha pressionadas
4. Solte-as quando vir a tela de recuperação.

Se nada acontecer, tente novamente ou verifique se o computador oferece suporte à recuperação do BIOS.

Notebooks

1. Certifique-se de que nenhuma unidade USB esteja conectada
2. Certifique-se de que a bateria esteja carregada a pelo menos 25%
3. Desconecte o cabo de alimentação
4. Pressione juntas as teclas `Ctrl` + `Esc` e as mantenha pressionadas
5. Enquanto pressiona as teclas, conecte o cabo de alimentação
 - Para notebooks Alienware, pressione o botão liga/desliga uma vez.
6. Solte-o quando vir a tela de recuperação

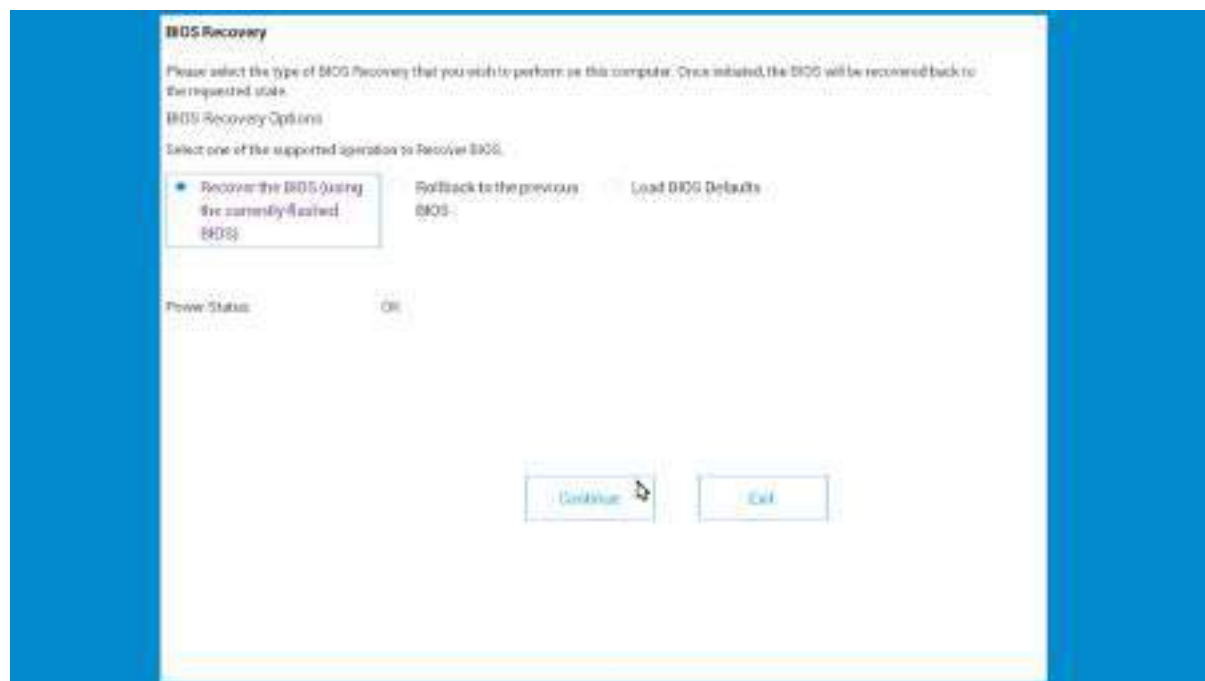
Você precisará usar o teclado integrado do notebook. Teclados externos não funcionam.

Etapa 2: Verificar se o arquivo de recuperação foi encontrado

Depois que o computador inicializar na recuperação do BIOS, analise a tela:

Se você vir um menu de recuperação com opções, avance para a Etapa 3.

Se você vir a mensagem "No recovery image found" ou apenas luzes piscando, isso significará que o computador não tem o arquivo de recuperação. Tente recuperar o BIOS por meio da unidade USB.





Etapa 3: Concluir a recuperação

Agora que você vê o menu de recuperação:

-
1. Selecione **Recover BIOS** (também pode dizer "Recover the BIOS")
 2. Selecione **Continue** ou pressione **Enter** para iniciar
 3. Aguarde a recuperação do computador. O computador será reiniciado várias vezes, e esse é um comportamento normal.
 4. Não desligue o computador

Alguns sistemas podem mostrar a tela BIOS Setup. Se isso acontecer, pressione `Esc` para sair e inicializar normalmente.

Método 2: Recuperação do BIOS por unidade USB (método de fallback)

Somente use esse método se a recuperação por disco rígido falhar ou não estiver disponível.

Quando usar a recuperação por USB:

-
- Falha na recuperação por disco rígido (exibiu a mensagem "No recovery image found")
 - O disco rígido foi substituído após a compra
 - O sistema operacional foi reinstalado ou a unidade foi reformatada
 - O modo de inicialização do BIOS foi alterado de UEFI para Legacy
 - A unidade é criptografada ou tem uma senha de disco rígido do BIOS

Visão geral do processo de recuperação por USB

A criação e o uso de uma unidade de recuperação USB envolvem estas etapas:

-
1. Fazer download do arquivo de recuperação do BIOS em um computador que esteja funcionando
 2. Formatar uma unidade USB como FAT32
 3. Copiar o arquivo de recuperação na unidade USB
 4. Usar a unidade USB para recuperar o BIOS no computador afetado

Etapa 1: Fazer download do arquivo de recuperação do BIOS

Conclua estas etapas em um computador que esteja funcionando.

-
1. Acesse [Drivers e downloads da Dell](#).
 2. Identifique seu computador:
 - Selecione **Detectar produto** para detectar o computador automaticamente ou
 - Digite a etiqueta de serviço do computador que não funciona.
 3. Selecione **Drivers e downloads**.
 4. Em **Categoria**, selecione **BIOS**.
 5. Encontre a atualização mais recente do BIOS para seu modelo e faça download do arquivo do BIOS.

Renomear o arquivo do BIOS

Mostrar extensões de arquivo no Windows

1. Abra o Explorador de arquivos. Para abrir o Explorador de Arquivos, pressione a **tecla com o logotipo do Windows + E**.
2. No menu **Mostrar**, selecione **Extensões de nomes de arquivos**.

Renomear o arquivo para BIOS_IMG.rcv

1. Acesse a pasta em que você fez download do arquivo do BIOS. Exemplo de nome de arquivo: Latitude_5420_1.18.0.exe
2. Clique no arquivo com o botão direito e selecione **Renomear**.
3. Altere o nome do arquivo inteiro para **BIOS_IMG.rcv**. Make sure to:
 - Excluir todo o nome do arquivo, inclusive a extensão .exe
 - Digitar o novo nome exatamente como exibido: BIOS_IMG.rcv
 - Usar letras maiúsculas, incluir o sublinhado e usar a extensão .rcv
4. Pressione Enter.
5. Na caixa de diálogo de advertência, selecione **Sim**. Agora, o arquivo aparece como BIOS_IMG.rcv.

Etapa 2: Preparar a unidade USB

Formatar a unidade USB

Conclua estas etapas em um computador que esteja funcionando.

Nota: A formatação exclui todos os dados da unidade USB. Antes de continuar, faça backup de todos os arquivos importantes.

1. Insira a unidade USB no computador que está funcionando.
2. Abra o **Explorador de Arquivos**. Para abrir o Explorador de Arquivos, pressione a **tecla com o logotipo do Windows + E**.
3. Clique na unidade USB com o botão direito e selecione **Formatar**.
4. Defina estas configurações:
 - **Sistema de arquivos:** Selecione **FAT32**
 - **Rótulo do volume:** (Opcional) Digite **BIOS_RECOVERY**
 - **Formatação rápida:** Marque a caixa de seleção
5. Selecione **Iniciar**.
6. Na caixa de diálogo de advertência, selecione **OK**.
7. Após a conclusão da formatação, selecione **OK**.

Copiar o arquivo de recuperação na unidade USB

1. Abra o **Explorador de Arquivos**. Para abrir o Explorador de Arquivos, pressione a **tecla com o logotipo do Windows + E**.
2. Acesse a pasta onde você salvou **BIOS_IMG.rcv**.
3. Copiar o arquivo. Para copiar o arquivo, clique nele com o botão direito e selecione **Copiar** ou pressione **Ctrl + C**.
4. No Explorador de Arquivos, abra a unidade USB.
5. Cole o arquivo. Para colar o arquivo, clique na janela da unidade USB com o botão direito e selecione **Colar** ou pressione **Ctrl + V**.

Nota: O arquivo deve estar no diretório raiz da unidade USB, não dentro de uma pasta.
6. Faça a ejeção da unidade USB. No Explorador de Arquivos, clique na unidade USB com o botão direito e selecione **Ejetar**.

Etapa 3: Iniciar a recuperação do BIOS por unidade USB

Agora que você tem uma unidade de recuperação USB, use-a para recuperar o BIOS no computador afetado.

Localize o tipo de dispositivo abaixo e siga estas etapas:

Desktop ou all in one

1. Certifique-se de que nenhuma unidade USB esteja conectada
2. Ligue o computador
3. Pressione juntas as teclas **Ctrl + Esc** e as mantenha pressionadas
4. Solte-as quando vir a tela de recuperação.

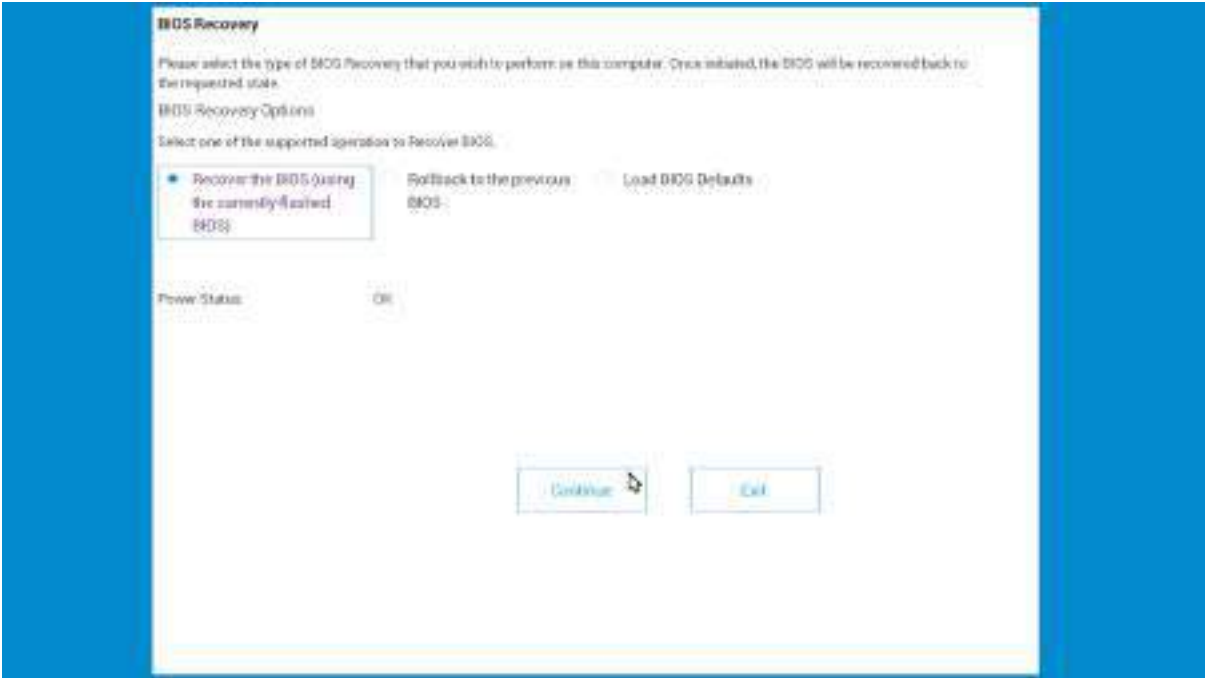
Se nada acontecer, tente novamente ou verifique se o computador oferece suporte à recuperação do BIOS.

Notebooks

1. Certifique-se de que nenhuma unidade USB esteja conectada
2. Certifique-se de que a bateria esteja carregada a pelo menos 25%
3. Desconecte o cabo de alimentação
4. Pressione juntas as teclas **Ctrl + Esc** e as mantenha pressionadas
5. Enquanto pressiona as teclas, conecte o cabo de alimentação
 - Para notebooks Alienware, pressione o botão liga/desliga uma vez.

6. Solte-o quando vir a tela de recuperação

Você precisará usar o teclado integrado do notebook. Teclados externos não funcionam.



Etapas 4: Concluir a recuperação

Agora que você vê o menu de recuperação:

- 1. Selecione **Recover BIOS** (também pode dizer "Recover the BIOS")
- 2. Selecione **Continue** ou pressione **Enter** para iniciar
- 3. Aguarde a recuperação do computador. O computador será reiniciado várias vezes, e esse é um comportamento normal.
- 4. Não desligue o computador

 **Nota:** Alguns sistemas podem mostrar a tela BIOS Setup. Se isso acontecer, pressione **Esc** para sair e inicializar normalmente.

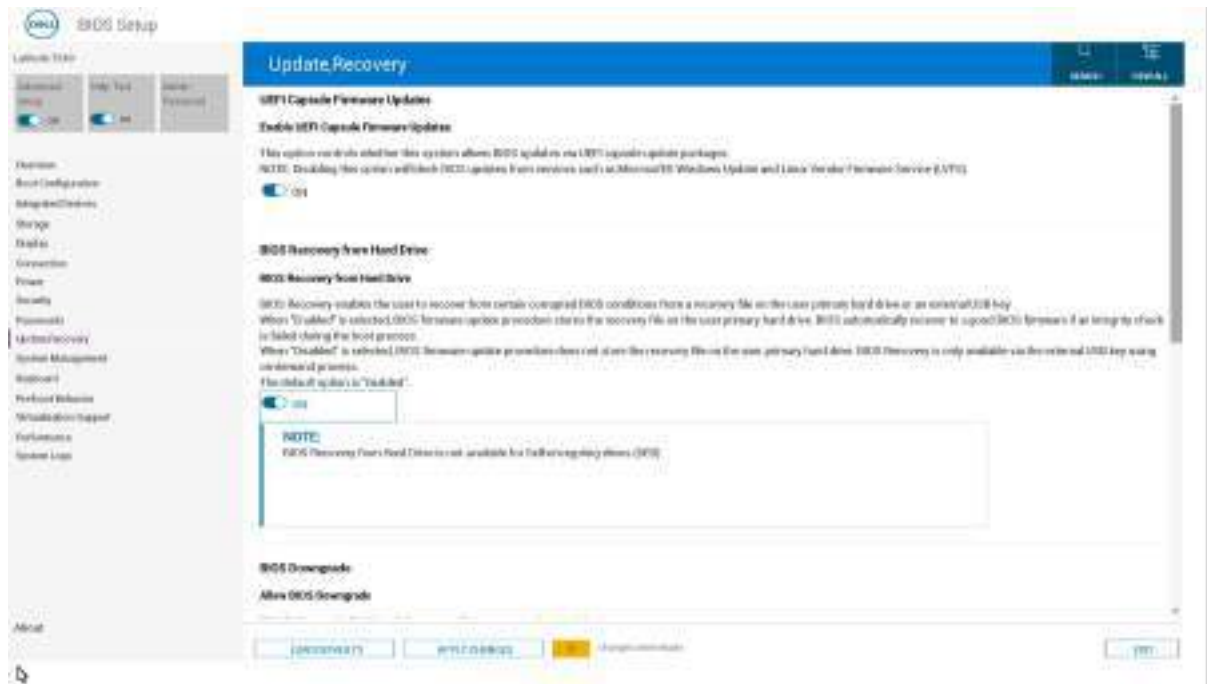
Verificar a compatibilidade do sistema

Verifique se o sistema oferece suporte à recuperação do BIOS seguindo estas etapas:

Se o computador inicializa

- 1. Reinicie o computador.
- 2. Durante a inicialização, pressione **F2** repetidamente até que a tela BIOS Setup abrir.
- 3. Procure a opção **BIOS Recovery from Hard Drive**.

Se você encontrar essa opção, isso significará que o sistema oferece suporte à recuperação do BIOS.



O computador provavelmente oferecerá suporte à recuperação do BIOS se atender a qualquer um destes critérios:

- Fabricado em dezembro de 2015 ou posteriormente
- Tem um processador Intel de 6^a geração (Skylake) ou mais recente

Se você usou a recuperação por USB porque o disco rígido não tinha o arquivo de recuperação, você pode restaurar o arquivo:

1. Certifique-se de que o computador agora liga normalmente e inicializa no Windows.
2. Faça download do BIOS mais recente na página [Drivers e downloads da Dell](#).
3. Execute a atualização do BIOS (o arquivo .exe que você baixou).
4. Aguarde a conclusão.

Problema: A tela de recuperação não aparece

1. **Pressione as teclas por mais tempo:** Tente manter pressionadas as teclas **Ctrl + Esc** por 30 segundos em vez de 15–20 segundos.
2. **Verifique o teclado (somente notebooks):** Verifique se você está usando o teclado integrado do notebook, não um teclado externo.

3. **Tente portas USB diferentes (somente recuperação por USB):** Conecte a unidade USB a uma porta diferente. Experimente as portas USB pretas (USB 2.0) antes das azuis (USB 3.0).
 4. **Verifique o arquivo da unidade USB (somente recuperação por USB):**
 - Certifique-se de que o arquivo tenha exatamente este nome: **BIOS_IMG.rcv**
 - Certifique-se de que ele esteja diretamente na unidade USB, não em uma pasta
 - Verifique se a unidade USB está formatada como FAT32
-

Problema: A mensagem "No recovery image found" é exibida

Isso significa que o arquivo de recuperação não está no disco rígido. Isso acontece quando:

- O disco rígido foi substituído
- O Windows foi reinstalado
- A unidade foi reformatada
- A unidade está criptografada (BitLocker)

Solução: Em vez disso, use o [Método 2 \(recuperação por USB\)](#).

Problema: O computador continua reiniciando, mas a recuperação não é concluída

Verifique se:

- O cabo de alimentação permaneceu conectado o tempo todo
- Você aguardou pelo menos 15 minutos
- Você não pressionou nenhuma tecla nem desligou o computador
- Para recuperação por USB: A unidade USB permaneceu conectada

Se ainda houver falha:

1. Tente criar uma nova unidade USB de recuperação.
2. Faça download do arquivo do BIOS novamente (ele pode estar corrompido).
3. Teste uma unidade USB diferente.

Se a recuperação ainda falhar depois de tentar essas etapas, talvez seja necessário substituir a placa-mãe. Entre em contato com o suporte técnico da Dell para obter as opções de reparo.

Problema: As luzes de LED continuam piscando

Padrões comuns de LED:

- **Três piscadas e, em seguida, seis piscadas (repetidamente):** BIOS corrompido. A recuperação deve corrigir isso.
- **Três piscadas e, em seguida, sete piscadas (repetidamente):** Falha de CPU/BIOS. Tente realizar a [recuperação do BIOS](#).
- **Outros padrões:** Pode ser falha de hardware, não corrupção do BIOS.

O que fazer:

1. Anote o padrão exato de piscadas.
 2. Tente realizar a recuperação do BIOS.
 3. Se as luzes continuarem piscando após a recuperação, procure o código de erro no [manual do usuário](#) do sistema.
-

As configurações do BIOS estão incorretas após a recuperação

Após a recuperação, as configurações do BIOS retornam aos valores padrão de fábrica. Talvez seja necessário alterar:

Ordem de inicialização:

1. Pressione **F2** durante a inicialização para acessar a tela BIOS Setup.

2. Selecione **Boot Sequence**.
3. Organize suas unidades na ordem desejada.
4. Salve e saia.

Outras configurações comuns:

- **Inicialização segura:** Ativar para Windows 11 ou 10, desativar para algumas versões do Linux
- **Virtualization:** Ativar se você usa VirtualBox, VMware ou Hyper-V
- **SATA Mode:** Manter como AHCI, a menos que você estivesse usando RAID antes

Restaurar a partição de recuperação do disco rígido

Se você usou a recuperação por USB porque o arquivo de recuperação do disco rígido estava ausente:

1. Certifique-se de que o computador inicializa no Windows normalmente.
2. Verifique se o BIOS está definido para o modo de inicialização **UEFI** (não Legacy).
3. Faça download da atualização mais recente do BIOS em [Drivers e downloads da Dell](#).
4. Execute o utilitário de atualização do BIOS (arquivo .exe).
5. Aguarde a conclusão da atualização.

A atualização do BIOS restaura automaticamente o arquivo de recuperação para o disco rígido, permitindo a recuperação por disco rígido em um uso futuro.

 **Nota:** Você poderá executar a atualização mesmo se já estiver usando a versão mais recente.

Perguntas frequentes

A recuperação do BIOS apagará meus dados ou a instalação do Windows?

Não. A recuperação do BIOS restaura apenas o firmware do BIOS. Todos os seus arquivos e programas e o Windows permanecem inalterados.

Devo tentar realizar primeiro a recuperação por disco rígido ou por USB?

Sempre tente realizar primeiro a recuperação por disco rígido. Ela é mais rápida, não requer preparação e funciona na maioria dos sistemas com discos rígidos originais. Somente crie uma unidade de recuperação USB se a recuperação por disco rígido falhar.

Preciso usar exatamente a mesma versão do BIOS que foi instalada anteriormente?

Não. Faça download da versão mais recente do BIOS disponível para seu modelo. O processo de recuperação funciona com qualquer versão.

A recuperação por disco rígido falhou. Como restauro o arquivo de recuperação para a próxima vez?

Após a recuperação bem-sucedida usando USB:

1. Certifique-se de que o BIOS esteja definido para o modo de inicialização UEFI.
2. Faça download do BIOS mais recente em [Drivers e downloads da Dell](#).
3. Execute o utilitário de atualização do BIOS.

A atualização restaura automaticamente o arquivo de recuperação no disco rígido. Você poderá executar a atualização mesmo se já estiver usando a versão mais recente.

Posso criar uma unidade de recuperação USB com antecedência como backup?

Sim. Você pode criar uma unidade de recuperação USB enquanto o computador está funcionando normalmente. Mantenha-a em um local seguro. Atualize o arquivo de recuperação quando atualizar o BIOS.

Preciso reinstalar o Windows após a recuperação do BIOS?

Não. O Windows e todos os programas de software permanecem inalterados. Após a conclusão da recuperação, o Windows inicializa normalmente. Talvez seja necessário redefinir algumas configurações do BIOS, como a ordem de inicialização.

Onde o arquivo de recuperação do BIOS é armazenado no disco rígido?

Em sistemas UEFI, o arquivo de recuperação está na Partição de sistema EFI (ESP), em: `\EFI\De11\BIOS\`

Essa partição fica oculta no Explorador de Arquivos do Windows e tem cerca de 100 MB a 500 MB.

Qual é a diferença entre BR2 e BR3?

Recuperação do BIOS 2 (BR2):

- Somente recuperação manual (usando `Ctrl + Esc`)
- Disponível em sistemas fabricados a partir de dezembro de 2015

Recuperação do BIOS 3 (BR3):

- Recuperação manual (usando `Ctrl + Esc`)
- Recuperação automática opcional na inicialização (deve estar ativada)
- Disponível em sistemas fabricados a partir de agosto de 2016

Para a maioria dos usuários, a diferença não importa. Ambas usam os mesmos procedimentos de recuperação.

O que é a configuração "Reset NVRAM" e devo desativá-la?

A NVRAM (Non-Volatile RAM, RAM Não Volátil) armazena as configurações do BIOS. Durante a recuperação:

- **Reset NVRAM ativada (padrão):** Todas as configurações do BIOS retornam aos valores padrão de fábrica
- **Reset NVRAM desativada:** Tenta manter as configurações atuais do BIOS

Recomendação:

- Primeira tentativa de recuperação: Desative Reset NVRAM para manter as configurações
- Se a recuperação falhar: Ative Reset NVRAM (a redefinição completa pode corrigir problemas subjacentes)

 **Nota:** Nem todos os sistemas mostram essa opção.

Por que a recuperação procura primeiro por unidades USB se a recuperação por disco rígido é recomendada?

Isso foi projetado para oferecer o máximo de flexibilidade:

- Quando uma unidade USB está conectada: O sistema usa USB (para sistemas sem arquivo de recuperação do disco rígido)
- Quando uma unidade USB não está conectada: O sistema usa o disco rígido (mais rápido, sem necessidade de preparação)

A ordem de procura garante que a recuperação funcione em todos os cenários. Você controla qual método é usado ao conectar ou não uma unidade USB.

Posso usar a mesma unidade de recuperação USB em vários computadores Dell?

Não. Cada unidade de recuperação USB é específica para um modelo de computador. O arquivo **BIOS_IMG.rcv** deve corresponder ao modelo exato do computador que você está recuperando. Você deve criar unidades de recuperação USB separadas para modelos diferentes.

E se o BitLocker estiver ativado?

A recuperação do BIOS pode acionar o modo de recuperação do BitLocker. Após a recuperação:

1. O BitLocker solicitará sua chave de recuperação de 48 dígitos
2. Digite a chave para desbloquear a unidade
3. Tudo funcionará normalmente depois disso

Nota: Localize a chave de recuperação do BitLocker ANTES de tentar realizar a recuperação. Verifique sua conta da Microsoft ou pergunte ao departamento de TI.

Posso usar um teclado USB externo para acionar a recuperação em um notebook?

Não. Os notebooks devem usar o teclado integrado para iniciar a recuperação do BIOS. Teclados USB e Bluetooth externos não funcionam para acionar a recuperação em notebooks. Desktops e all in ones podem usar teclados USB externos com fio.

Como formatar uma unidade USB maior que 32 GB?

O Windows não pode formatar unidades maiores que 32 GB para FAT32 usando a caixa de diálogo padrão de formatação. Em vez disso, use o PowerShell:

1. Clique com o botão direito em **Iniciar** e selecione **Windows PowerShell (Administrador)** ou **Terminal (Administrador)**.
2. Na caixa de diálogo Controle de Conta de Usuário, selecione **Sim**.
3. No prompt, digite este comando: `format /FS:FAT32 X:`
Substitua **X** pela letra da unidade USB. Para localizar a letra da unidade, confira o Explorador de Arquivos.

Exemplo: `format /FS:FAT32 D:`

4. Pressione **Enter**.
 5. Quando solicitado, pressione **Enter** novamente.
 6. Aguarde a conclusão da formatação. Isso pode levar vários minutos.
 7. Digite **exit** e pressione **Enter**.
-

Qual é a diferença entre "Recover BIOS" e "Load BIOS Defaults"?

Os dois termos têm o mesmo significado. Diferentes computadores Dell usam palavras diferentes para indicar a mesma opção de recuperação. Selecione a opção exibida para você.

Isso corrigirá problemas de hardware?

Não. A recuperação do BIOS corrige apenas o firmware corrompido do BIOS. Ela não corrige:

- RAM, disco rígido ou outro hardware com falha
- Danos na placa-mãe
- Telas ou teclados quebrados

Se a recuperação for concluída com sucesso, mas os problemas persistirem, provavelmente isso significará que você tem uma falha de hardware. Execute um [diagnóstico de hardware](#).

A bateria do meu notebook está descarregada. Ainda posso fazer a recuperação?

Sim, desde que o cabo de alimentação esteja conectado. No entanto, é mais seguro ter pelo menos 25% de carga da bateria caso a energia seja interrompida.

Mais informações

Perguntas frequentes

Confira aqui algumas perguntas frequentes sobre a recuperação do BIOS.

 **Nota:** Clique no título da seção que deseja abrir abaixo para visualizar o conteúdo.

[Mostrar tudo](#) | [Ocultar tudo](#)

Quais computadores e tablets Dell são compatíveis com a recuperação do BIOS? 

Como identificar se o meu computador Dell é compatível com a recuperação do BIOS? 

Como configurar a recuperação automática se ela estiver disponível? 

Onde está o arquivo de recuperação do BIOS? 

Como criar uma unidade USB externa para executar a recuperação do BIOS no meu computador ou tablet Dell? 

Como manter as configurações atuais do BIOS pela redefinição para os padrões de fábrica durante a recuperação do BIOS? 

Como recuperar o BIOS sem uma unidade USB externa? 

Como criar a partição EFI para recuperação do BIOS em uma unidade de disco rígido de substituição? 

Como recuperar o BIOS se o disco rígido estiver criptografado ou se a senha da unidade de disco rígido estiver ativada no BIOS? 

Como recuperar o BIOS se a unidade de disco rígido tiver sido substituída ou se a imagem de recuperação não estiver disponível na unidade de disco rígido? 

Estou ouvindo bipes ou os LEDs estão piscando em um padrão durante o processo de recuperação do BIOS, o que devo fazer? 

[Voltar ao início](#)

 O seu computador está fora da garantia? Para suporte fora da garantia, acesse o site [Dell.com/support](#) e digite a etiqueta de serviço Dell para visualizar nossas ofertas.

Produtos afetados

Alienware, Dell All-in-One, Dell Pro All-in-One, Dell Pro Max Micro, Dell Pro Max Slim, Dell Pro Max Tower, Dell Pro Micro, Dell Pro Slim, Dell Pro Tower, Dell Slim, Dell Tower, Inspiron, Legacy Desktop Models, OptiPlex, Vostro, XPS, G Series, Chromebook, G Series, Alienware, Dell Laptops, Dell Plus, Dell Pro, Dell Pro Max, Dell Pro Plus, Dell Pro Premium, Inspiron, Latitude, Dell Pro Rugged, Vostro, XPS, Legacy Laptop Models, Latitude Tablets, Venue, XPS Tablets, Fixed Workstations, Mobile Workstations, Dell Pro Max Micro XE FCM2250

Número do artigo: 000132453

Tipo de artigo: How To

Último modificado: 17 nov. 2025

Versão: 27

[Login](#) [Join SNIA](#)

Platinum Member Directory



[Check full member list](#)

AMD

 **BROADCOM**


CISCO

DELL
Technologies

HP
E

 **HUAWEI**

IBM

intel.

KIOXIA

micron


NetApp

SAMSUNG



Western Digital.

Not a member yet?

Complete our [member application](#)
today! Subscribe to [SNIA Monthly
Newsletter](#) .



SNIA: Experts on Data

SNIA develops and promotes architectures, standards, and education through vendor-neutral collaboration of experts on data technologies that lead the industry worldwide. Become a member today!

[Join SNIA](#)

Discover SNIA

[About](#)

[Technical Work](#)

[Education](#)

[Data Focus Areas](#)

[News & Events](#)

[Resources](#)

[Membership](#)

SNIA Blog

[SNIA: Experts on Data Blog](#)

SNIA Socials



[Site Map](#)

[Contact Us](#)

[Privacy Policy](#)

[Chat provider: LiveChat](#)

Copyright © 2026 SNIA

Suporte para OpenManage Essentials

Resumo: O OpenManage Essentials 2.5 é a versão final. O OpenManage Essentials não oferecerá suporte aos servidores PowerEdge atuais ou futuros e não serão adicionados novos aprimoramentos ao produto. Para fins de gerenciamento de seus dispositivos Dell EMC, a Dell EMC recomenda a migração para o OpenManage Enterprise.

Conteúdo do artigo

Sintomas

-  O OpenManage Essentials 2.5 é a versão final. O OpenManage Essentials não oferecerá suporte aos servidores PowerEdge atuais ou futuros e não serão adicionados novos aprimoramentos ao produto. Para fins de gerenciamento de seus dispositivos Dell EMC, a Dell EMC recomenda a migração para o [OpenManage Enterprise](#). A [ferramenta QuickMigrate](#) está disponível para ajudar a migrar do OpenManage Essentials para o OpenManage Enterprise.

[> Saiba mais sobre o OpenManage Enterprise](#)



O **OpenManage Essentials 2.5** é versão mais recente do Dell EMC OpenManage Essentials. O OpenManage Essentials oferece um ponto central de acesso, por meio de um console de gerenciamento de sistemas um-para-muitos, para monitorar e gerenciar sistemas, permitindo que um administrador tenha uma visão ampla de todo o ambiente empresarial.

O **OpenManage Essentials** pode aumentar o tempo de atividade do sistema, reduzir tarefas repetitivas e evitar interrupções nas operações comerciais essenciais. A ferramenta é fácil de instalar e possibilita o gerenciamento abrangente dos servidores modulares, em rack e em torre Dell PowerEdge. Além disso, o OME oferece monitoramento abrangente da integridade da infraestrutura, controle e suporte para servidores, armazenamento e rede da Dell EMC, bem como hardware de terceiros. Faça download da versão mais recente do OME, que está disponível para os clientes da Dell como um [download](#) gratuito.

Recursos e melhorias do OpenManage Essentials 2.5:

[Mostrar tudo](#) | [Ocultar tudo](#)

[> Recursos e melhorias do OpenManage Essentials 2.5](#)

[> Principais recursos do OpenManage Essentials](#)

[> Tour rápido pelo OpenManage Essentials](#)

[Fórum de discussão](#)

Downloads e documentação

O OpenManage Essentials v2.5 está disponível como um download gratuito no site de suporte da Dell. A função de inventário do console do OME integra-se com o Dell Repository Manager para automaticamente facilitar a [criação de repositórios personalizados](#) de novas atualizações para os sistemas.

Se você é um novo usuário do produto, consulte a documentação do produto ou use a ferramenta de solução de problemas ou a ferramenta de configuração de SNMP

- [Download do OpenManage Essentials 2.5](#)
- [Download da ferramenta de solução de problemas da Dell](#) (Esta ferramenta é usada para testar várias configurações e vários problemas de conectividade. A ferramenta de solução de problemas faz parte da instalação.)
- [Download da ferramenta de configuração de SNMP da Dell](#)
- [Documentação do OpenManage Essentials 2.5](#) (guia do usuário, matriz de suporte e notas da versão)
- [Perguntas frequentes sobre o OpenManage Essentials](#)

Whitepapers:

- Visão geral
 - [Como simplificar o gerenciamento do sistema com o Dell OpenManage em servidores Dell PowerEdge 13G](#)
- Instalação/configurações
 - [Como instalar o Dell EMC OpenManage Essentials \(OME\)](#)
 - [Como instalar várias instâncias de banco de dados do OME em um único banco de dados empresarial do Microsoft SQL Server](#)
 - [OpenManage Essentials: escalabilidade e desempenho](#)
- Descoberta e gerenciamento de dispositivos
 - [Descoberta e inventário de dispositivos Dell usando o OME](#)
 - [Como gerenciar o Dell PowerEdge VRTX com o OME](#)
 - [Descoberta da infraestrutura modular do Dell PowerEdge \(M1000e, FX2 e VRTX\) usando o OME](#)
 - [Dell EMC OpenManage Essentials: suporte a dispositivos](#)
 - [Detecção simplificada da infraestrutura modular Dell EMC PowerEdge \(MX7000\) no Dell EMC OpenManage Essentials](#)
- Implementação/configuração
 - [Provisionamento de hardware de servidor e implementação de sistema operacional usando o OME](#)
 - [Boot e implementação de configuração de rede usando o modelo de servidor com o OME](#)
 - [Gerenciamento da configuração do servidor usando o OME](#)
 - [Gerenciamento da infraestrutura modular usando o OME](#)
 - [Configuração de VLAN do IOA com o OME](#)
 - [Configuração de ações de alerta e definições de registro de alertas no OME](#)
 - [Configuração de ações de alerta usando o OME](#)
- Atualização de driver/firmware
 - [Como gerenciar a conformidade de driver e firmware usando várias linhas de base](#)
 - [Atualização de servidores Dell com o OME](#)
 - [Atualização de sistema sem agentes na banda com o OME](#)
- Interfaces
 - [REST API para interagir com o OpenManage Essentials](#)
 - [Vantagens da Interface de linha de comando \(CLI\) no OME](#)

Vídeos

- Instalação
 - [Como instalar o OpenManage Essentials 2.3](#) (mesmas etapas do OME v2.5)
 - [Atualização para o OpenManage Essentials mais recente](#)
- Configuração e integração:
 - [Suporte de várias linhas de base do catálogo no OpenManage Essentials](#)
 - [OpenManage Essentials e a integração com o Repository Manager](#)
- Descoberta e inventário
 - [Descoberta de dispositivos com base no tipo de dispositivo \(Assistente guiado e avançado de descoberta\)](#)
 - [Descoberta e monitoramento de dispositivos usando o protocolo SNMPv3](#)
 - [Como detectar e gerenciar o chassi do MX7000 usando o Dell EMC OpenManage Essentials](#)

Causa

Dell EMC

Resolução

Propriedades do artigo

Data da última publicação

01 Apr 2021

Versão

8

Tipo de artigo

Solution

in (<https://www.linkedin.com/company/trusted-computing-group/>)  (<https://twitter.com/TrustedComputin>)

 (<https://www.youtube.com/user/TCGadmin>)

中国 (<http://www.trustedcomputinggroup.org/work-groups/regional-forums/greater-china/>) 日本語 (<http://www.trustedcomputinggroup.org/work-groups/regional-forums/japan>)
Certification (<http://www.trustedcomputinggroup.org/membership/certification/>) Member Login (<https://members.trustedcomputinggroup.org/>)



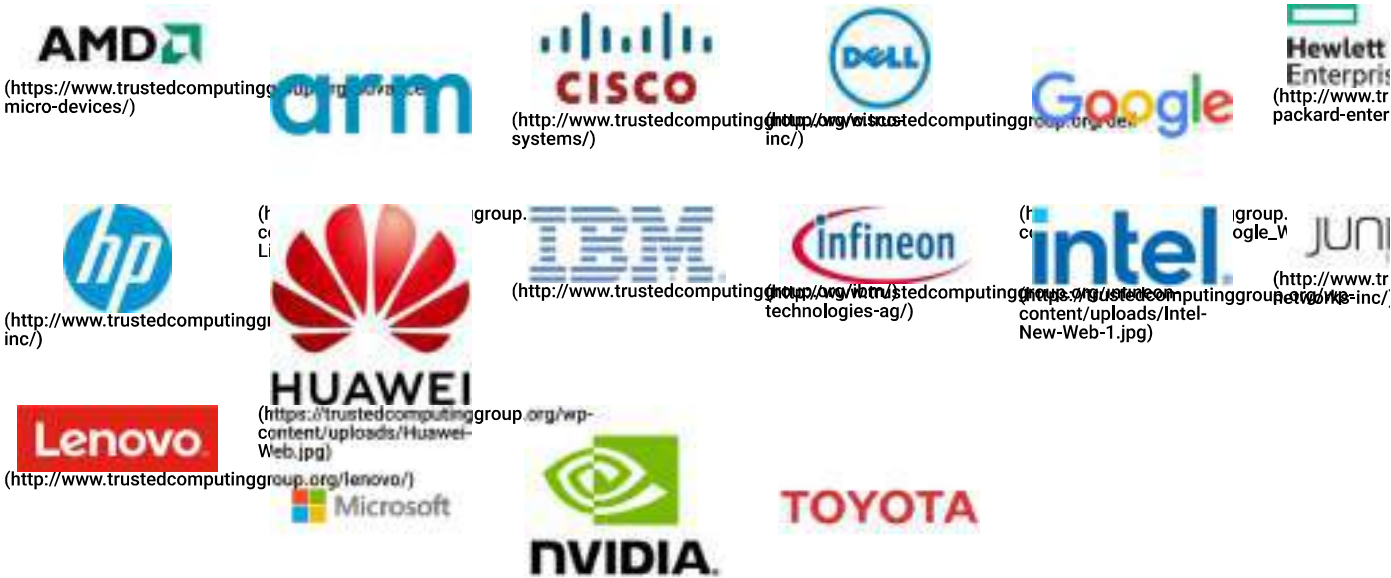
(<https://trustedcomputinggroup.org/>)

Home (<https://trustedcomputinggroup.org>) > Membership (<https://trustedcomputinggroup.org/membership/>) > Member Companies

Member Companies

To view the full member list, click [HERE](#)

Promoter



Contributor





Adopter/Associate



Full Member List

ITEMS PER PAGE

25



SEARCH TEXT

Enter a keyword to search

FILTER BY LEVEL

Any



1

2

3

4



Name ↓

Level

Absolute Software Corp

Adopter

[Privacy & Cookies Policy](#)

Name ↓	Level
Acer Inc.	Contributor
Advanced Micro Devices, Inc.	Promoter
Alibaba (China) Co., Ltd	Associate
AMI	Contributor
Ampere Computing LLC	Contributor
Ant Group Co., Ltd.	Contributor
ARM Ltd.	Promoter
Astera Labs, Inc.	Contributor
Beyond Identity	Contributor
Broadcom	Contributor
Canon Inc.	Contributor
Cisco Systems	Promoter
Compumax Computer S.A.S.	Adopter
Crypto Quantique LTD	Contributor
CS Services Co., Ltd	Adopter
Datang Gohighsec (Zhejiang) Information Technology Co., Ltd.	Adopter
Daten Tecnologia LTDA	Contributor
Dell, Inc.	Promoter
DesignFirst OU	Contributor
DRS Technologies	Adopter
Fagundez Distribuicao LTDA	Adopter
FUJIFILM Business Innovation Corp.	Contributor
Google Inc.	Promoter

Additional Resources

[CERTIFICATION \(HTTPS://TRUSTEDCOMPUTINGGROUP.ORG/109860/\)](https://trustedcomputinggroup.org/109860/)

[INDUSTRY & ACADEMIC PARTICIPATION \(HTTPS://TRUSTEDCOMPUTINGGROUP.ORG/MEMBERSHIP/INDUSTRY-PARTICIPATION/\)](https://trustedcomputinggroup.org/membership/industry-participation/)

[MEMBER COMPANIES \(HTTPS://TRUSTEDCOMPUTINGGROUP.ORG/MEMBERSHIP/MEMBER-COMPANIES/\)](https://trustedcomputinggroup.org/membership/member-companies/)

[TCG CERTIFICATION PROGRAMS](https://trustedcomputinggroup.org/membership/certification/) ➤ [\(HTTPS://TRUSTEDCOMPUTINGGROUP.ORG/MEMBERSHIP/CERTIFICATION/\)](https://trustedcomputinggroup.org/membership/certification/)

FAQ

[Industry Participation \(http://www.trustedcomputinggroup.org/industry-participation/\)](http://www.trustedcomputinggroup.org/industry-participation/)

[Resource Directory \(http://www.trustedcomputinggroup.org/resources/\)](http://www.trustedcomputinggroup.org/resources/)

[Certification \(http://www.trustedcomputinggroup.org/membership/certification/\)](http://www.trustedcomputinggroup.org/membership/certification/)

[Member Login \(https://members.trustedcomputinggroup.org/kiers/\)](https://members.trustedcomputinggroup.org/kiers/)

[Join Now \(http://www.trustedcomputinggroup.org/membership/\)](http://www.trustedcomputinggroup.org/membership/)

Newsletter Signup

Stay current with Trusted Computing Group (TCG) activities, including recent case studies, press releases, industry news and upcoming events via the TCG Newsletter!

First Name

Last Name

Email (required)

[Privacy & Cookies Policy](#)

Company/Organization		Sign up

Contact Us

Trusted Computing Group Administration Phone: +1.503.619.0562 (tel:+1.503.619.0562)
3855 SW 153rd Drive Fax: +1.503.644.6700 (tel:+1.503.644.6700)
Beaverton, Oregon 97003 Email: admin@trustedcomputinggroup.org (mailto:admin@trustedcomputinggroup.org)

© 2025 Trusted Computing Group. All Rights Reserved.

[Legal Notices \(https://trustedcomputinggroup.org/legal-notices/\)](https://trustedcomputinggroup.org/legal-notices/) [Privacy Policy \(https://trustedcomputinggroup.org/privacy-policy/\)](https://trustedcomputinggroup.org/privacy-policy/)
[in \(https://www.linkedin.com/company/trusted-computing-group/\)](https://www.linkedin.com/company/trusted-computing-group/) [🐦 \(https://twitter.com/TrustedComputin\)](https://twitter.com/TrustedComputin)
[You Tube \(https://www.youtube.com/user/TCGAdmin\)](https://www.youtube.com/user/TCGAdmin)

[About](#)[Membership](#)[Education](#)[Blog](#)[News](#)[Events](#)[Developers](#)[Public Support](#)

-Membership List



[Unified Extensible Firmware Interface Forum](#)

 [Home](#) » [Membership](#)

Membership List

The UEFI Forum community of members is represented by industry-leading OEMs, IHVs, chip manufactures, BIOS and firmware vendors and operating system vendors.

Promoters

[AMD](#)[HP, Inc.](#)[American Megatrends, Inc.](#)[Insyde Software](#)[Apple Inc.](#)[Intel](#)[ARM Limited](#)[Lenovo](#)[Dell](#)[Microsoft](#)[Hewlett Packard Enterprise](#)[Phoenix Technologies](#)

Contributors

[Absolute Software Corporation](#)[Alibaba \(China\) Co., Ltd.](#)[Ampere Computing LLC](#)[ASMedia Technology Inc.](#)[ASUSTeK COMPUTER INC.](#)[Beijing Bytedance Network Technology Ltd.](#)[Broadcom Corporation](#)[Canonical Limited](#)[Cisco](#)[Citrix Systems, Inc.](#)[Cumulus Networks Inc.](#)[Daten Tecnologia](#)[DisplayLink \(UK\) Ltd.](#)[Dynabook Inc](#)[EMC Corporation](#)[ExpressLuck Industrial Ltd.](#)[Facebook](#)[Microchip Technology](#)[Montage Technology](#)[Multilaser Industrial S/A](#)[Nanjing Byosoft Co., Ltd.](#)[NEC Corporation](#)[NUVIA Inc.](#)[NVIDIA](#)[NXP B.V.](#)[Oracle America, Inc.](#)[Positivo Tecnologia S.A.](#)[Pre-OS Security Inc.](#)[Qualcomm Inc.](#)[Realtek Semiconductor Corp.](#)[Red Hat, Inc.](#)[Seagate Technology LLC](#)[SIFIVE, INC.](#)[SUSE LLC](#)

<u>Google</u>	<u>Tachyum Inc</u>
<u>Huawei Technologies Co., Ltd</u>	<u>The Linux Foundation</u>
<u>IBM</u>	<u>The MITRE Corporation</u>
<u>ICC Intelligent Platforms GmbH</u>	<u>Ventana Micro Systems Inc.</u>
<u>INSPUR (Beijing) Electronic Information Industry Co., Ltd.</u>	<u>VMware, Inc.</u>
<u>Linaro Ltd.</u>	<u>Western Digital Technologies</u>
<u>Login Informatica Com. Repr. LTDA</u>	<u>Xilinx, Inc.</u>
<u>Loongson Technology Corporation Limited</u>	<u>ZD Technology (Beijing) Co., Ltd.</u>
<u>Marvell Asia Pte. Ltd.</u>	<u>Zoom Tecnologia Ltda.</u>
<u>Mellanox Technologies</u>	

Adopters

<u>3MD dba Hard Drives NW</u>	<u>JARI</u>
<u>3MDEB Embedded Systems Consulting</u>	<u>Jetway Information Security Industry Co., Ltd.</u>
<u>9elements GmbH</u>	<u>KingTrust Systems Ltd.</u>
<u>A.D. Nieman & Associates, LLC</u>	<u>Kioxia Corporation</u>
<u>AAEON Technology Inc.</u>	<u>Konsulko Group</u>
<u>ACAS Technologies, Inc.</u>	<u>Kontron Embedded Modules GmbH</u>
<u>Accusys, Inc.</u>	<u>Kraftway Corporation PLC</u>
<u>Acer Inc.</u>	<u>Kuhrman Technology Solutions LLC</u>
<u>Adaptec, Inc.</u>	<u>LCC Rubinteh</u>
<u>ads-tech GmbH</u>	<u>LCFC</u>
<u>Advantech Co., Ltd.</u>	<u>LG Electronics</u>
<u>AGN Group Suprimentos</u>	<u>Lockheed Martin Corporation</u>
<u>AGS Sundryne Technologies Pvt. Ltd.</u>	<u>Lontium Semiconductor Corporation</u>
<u>Airdesk Ltd.</u>	<u>LucidLogix</u>
<u>Alcor Micro Corp.</u>	<u>Matrox Graphics Inc.</u>
<u>Allion Labs, Inc.</u>	<u>MBDA UK Ltd.</u>
<u>ALTELL Ltd.</u>	<u>MBM Tecnologia e Industria de Informatica LTDA</u>
<u>AlterSciences</u>	<u>MediaTek Inc.</u>
<u>American Arium</u>	<u>MediCapture, Inc.</u>
<u>AMOI Electronics Co., Ltd.</u>	<u>Mensys B.V.</u>
<u>Anna University - College of Engineering</u>	<u>Mercury Computer Systems</u>
<u>Apricorn</u>	<u>Micro-Star Int'l Co., Ltd</u>
<u>Arca Noae, LLC</u>	<u>Micron Technology, Inc.</u>
<u>Arista Corp.</u>	<u>Microsemi Corporation</u>
<u>Arquimedes Automacao E Informatica LTDA.</u>	<u>Mitrastar Technology Corp.</u>
<u>ASSET InterTech, Inc.</u>	<u>MokaFive</u>
<u>AssurAware, Inc.</u>	<u>Mossbit Technologies</u>
<u>Atlona Inc.</u>	<u>Myricom, Inc.</u>
<u>ATTO Technology</u>	<u>National Instruments Corporation</u>
<u>AuthenTrend Technology Inc.</u>	<u>National Technical Systems</u>
<u>Authorizer Technologies, Inc.</u>	<u>Naval Postgraduate School</u>
<u>Aver Networks Corp.</u>	<u>NEC Personal Products Ltd.</u>
<u>Avery Design Systems</u>	<u>Neterion, Inc.</u>
<u>Avery Design Systmes</u>	<u>Netlist Inc.</u>
<u>Avid Technology, Inc.</u>	<u>Network 2000 Inc.</u>
<u>Axiom Electronics, LLC</u>	<u>NetXen Inc.</u>
<u>Axiomtek Co., Ltd.</u>	<u>Neusoft</u>
<u>Balance Software Corp.</u>	<u>New H3C Technologies Co., Ltd.</u>
<u>Battelle Memorial Institute, Pacific Northwest Division</u>	<u>Newport Enterprises Inc.</u>

[BCM Advanced Research](#)
[BedRock Systems, Inc.](#)
[Beijing AnHeng SecoTech Information Technology Co., Ltd.](#)
[BiTMICRO Networks Inc.](#)
[Booz Allen Hamilton](#)
[Brown's Operating System Services Limited](#)
[BSQUARE Corporation](#)
[CalDigit, Inc.](#)
[Calxeda, Inc.](#)
[Canon Inc.](#)
[Captec Ltd.](#)
[Centerm Information Co., Ltd.](#)
[CenterTools Software GmbH](#)
[Central South University](#)
[Check Point Software](#)
[Chelsio Communications, Inc.](#)
[China Greatwall Computer Shenzhen Co., Ltd.](#)
[CHUNGHSIN INDUSTRY GROUP](#)
[CircleSoft LLC](#)
[Circuitco](#)
[Cisc Systems](#)
[Computer Task Group](#)
[Concurrent Technologies Plc](#)
[congatec A.G.](#)
[conpal GmbH](#)
[coresystems GmbH](#)
[Courtyard Electronics Ltd.](#)
[Cray, Inc.](#)
[CrossInfo Architects](#)
[Cryptomill Technologies Ltd.](#)
[CSWL, Inc.](#)
[Dawning Information Industry_\(Beijing\)_Corp., Ltd. \(Sugon\)](#)
[Def-Logix, Inc.](#)
[Denali Software](#)
[DeviceVM, Inc.](#)
[Diablo Technologies, Inc.](#)
[Dialogue Technology Corp.](#)
[Diskeeper Corporation](#)
[Dot Hill](#)
[Eclypsium, Inc](#)
[Egis Technology Inc.](#)
[Elite Group Computer Systems Co., Ltd.](#)
[EliteBytes Limited](#)
[Eltan Comm B.V.](#)
[Embedded Now, Inc](#)
[Embedded Research Solutions](#)
[emBoot Inc.](#)
[Emerson Network Power, Embedded Computing](#)
[EMUTEX LTD.](#)
[Enmotus, Inc.](#)

[Nextiva](#)
[NTI Corporation](#)
[NVELO, Inc.](#)
[OpenMars Development LLC](#)
[Order N Development, LLC](#)
[Orion Technologies, LLC](#)
[OSBASE, LLC](#)
[Panasonic Corporation](#)
[Parallels IP Holdings GmbH](#)
[Pegatron Corporation](#)
[Peppercon AG](#)
[PGP Corporation](#)
[PixelNext Inc.](#)
[PLX Technology, Inc.](#)
[Portlock](#)
[PQURE Technology AB](#)
[Proformatique](#)
[Quanta Computer Inc.](#)
[Radisys Corporation](#)
[Red Flag Software Co., Ltd.](#)
[Renesas Electronics Corporation](#)
[RPA RusBITech](#)
[rubbersoft.com](#)
[Ruijie Networks](#)
[Sage-Microelectronics](#)
[Samsung Electronics Co., Ltd.](#)
[Sandia National Laboratories](#)
[SanDisk Corporation](#)
[Sanmina Corporation d/b/a Viking Technology](#)
[SDL Eletro Eletronica Ltda - EPP](#)
[SecurStar GmbH](#)
[SEMP TOSHIBA INFORMATICA LTDA](#)
[Sensics, Inc.](#)
[ServerEngines Corp.](#)
[Shanghai Advanced Research Institute](#)
[Shanghai IP3 Technology Co., Ltd.](#)
[Silicon Image, Inc.](#)
[Silicon Integrated Systems Corp.](#)
[SinoSun Technology, Ltd.](#)
[SoftIron, Inc.](#)
[softKVM LLC](#)
[Solarflare Communications Inc.](#)
[Sony Corporation](#)
[Spirent Communications](#)
[Sprezzatech](#)
[SSWW](#)
[STEC, Inc.](#)
[Stonewood Electronics Ltd.](#)
[Stream Labs](#)
[Super Future Equities, Inc.](#)

[EPEAK Studio Ltd.](#)
[Etegro Technologies](#)
[Eurosoft \(UK\) Ltd.](#)
[EVOC](#)
[Extreme Engineering Solutions, Inc.](#)
[F5 Networks, Inc.](#)
[Fastwel Group Co., Ltd.](#)
[Federal University of Ceara, Brazil](#)
[Fermilab](#)
[FernUniversität in Hagen](#)

[FirmTek, LLC](#)

[Flextronics Instituto de Tecnologia](#)
[focian Computer](#)
[Founder Technology Group Corp.](#)
[Framework Computer LLC](#)
[Freescale Semiconductor, Inc.](#)
[Fujitsu Ltd.](#)
[Gemalto SA](#)
[General Dynamics Canada](#)
[Genesi USA Inc.](#)
[Gigabyte United Inc.](#)
[GIT Japan Inc.](#)
[Glacier Peak Technology, LLC](#)
[Grain Media, Inc.](#)
[Greencroft Code](#)
[Guidance Software, Inc.](#)
[HighPoint Technologies, Inc.](#)
[Hitachi, Ltd.](#)
[Houter Brasil Eireli](#)
[HTC Corporation](#)
[Hunan New Cloudnet Technology Co., Ltd.](#)
[HXT Semitech](#)
[IATECAM](#)
[ICP Electronics, Inc.](#)
[InfoTeCS](#)
[Infrant Technologies, Inc.](#)
[Inphi Corp.](#)
[Institute of Physics, Academia Sinica](#)
[Integrated Device Technology Inc.](#)
[Intellico, LLC](#)
[Intelligency](#)
[Intelligraphics, Inc.](#)
[Inventec Corporation](#)
[Inventec Electronic \(Tianjin\) Co., Ltd.](#)
[IRCONA](#)
[ISP RAS](#)
[ITSC Library](#)
[Japan Digital Laboratory Co., Ltd.](#)

[Supermicro Computer, Inc.](#)
[SYBERA GmbH](#)
[Symantec Corporation](#)
[System Fabric Works](#)
[System Garden Ltd.](#)
[TCORP](#)
[Terascale, Inc.](#)
[Themis Computer, Inc.](#)
[TimeLab Corporation](#)
[Tokyo Electron Device Ltd.](#)
[Toshiba Samsung Storage Technology Korea Corporation](#)
[Trend Micro](#)
[Tsinghua Tongfang Co., Ltd.](#)
[Tuxera Inc.](#)
[TYA](#)
[Ubiquitous AI Corporation](#)
[ULINK Technology, Inc.](#)
[UNH InterOperability Laboratory](#)
[Unicompute Technology Co., Ltd](#)
[UniFabriX Ltd.](#)
[Unisys Corporation](#)
[University of California, Davis](#)
[UPEK, Inc.](#)
[US Technology Resources \(M\) SDN. BHD.](#)
[V&G Information System Co., Ltd.](#)
[VAIO Corporation](#)
[Validity Sensors](#)
[Venetex Corp](#)
[Vestel Dijital Yretim Sanayi A. S.](#)
[VIA Alliance Semiconductor Co., Ltd.](#)
[VIA Technologies, Inc.](#)
[VNPT Technology](#)
[VT Miltope](#)
[Wacom Technology](#)
[Wave Systems Corp.](#)
[WinMagic Inc.](#)
[Winsiders Seminars & Solutions, Inc.](#)
[WinSystems, Inc.](#)
[Wiwynn Corporation](#)
[Wuhan University](#)
[Wyse Technology](#)
[XGI Technology Inc.](#)
[Xi'an Saming Technology Co., Ltd.](#)
[Xi3 Corporation](#)
[Xitrix Computer Corporation](#)
[Xsense Connectivity Inc.](#)
[Zhejiang Dahua Technology Co., Ltd.](#)
[ZNYX Networks](#)

Individual Adopters

Alex Kunovszky	Karl O. Van Leuven IV
Barry Gian James	Kushal Koolwal
Benson Lin	Lee Fisher
Cheng-Lung Chang	Lucien Pullen
Connor Wood	Marvin Häuser
David Boyd	Michael Johnston
Dharmesh Tarapore	Michael Zimmermann
Don MacKellar	Patrick J. Kennedy
Ed Brundage	Paulo Henrique L. Amorim
Elika S. Kohen	Pete Batard
Gail B. Keown	Phooen Sonpooshi
George Fulk	Robert Jandacek
Gregory Havenga	Robert Johnston
Howard Peng	Rocky Wang
Ing-chao Lin	Roger Bertoldi
James Bottomley	Roger Thompson
Jason Christopher Stone	Seppe Sol
Jeong Kim	Shannon Lewis
John A. Newton	Shawn M. Pedersen
John M. Hare	VALETTE Teddy
Jonathan J. Willemin	Wang Qiang
Joseph LeGarreta	William J. Biessman
Juan Pablo Black Romero	Xie Tianming (Persmule)
Justin Loo	ZongQi Li
Justin Sligh	

* temporarily suspended

[Privacy Policy](#)[Member Login](#)[Site Map](#)[Contact Us](#)UEFI Forum © 2021

Find Us On...



Eldorado do Sul, 4 de agosto de 2026

À

A3 INFOTECH COMERCIO E PRESTAÇÃO DE SERVIÇOS E INFORMÁTICA LTDA

A/C Sr(a). Fabio Eduardo Maranesi

Ref.: Serviço Nacional de Aprendizagem Comercial – Administração Regional no Estado de São Paulo – Senac/SP – Pregão Eletrônico PEE 2026000049

ASSISTÊNCIAS TÉCNICAS

A **DELL COMPUTADORES DO BRASIL LTDA. (“Dell”)**, inscrita no CNPJ/MF sob o nº 72.381.189/0001-10, com sede na Av. Industrial Belgraf, 400, bairro Medianeira, Eldorado do Sul/RS, CEP 92.990-000, vem, através da presente, informar as suas assistências técnicas autorizadas:

Nome	UF	Cidade	Razão Social	CNPJ	Endereços	CEP	Gerente Logístico
Jaguareé	SP	São Paulo	Proxxi Tecnologia Ltda	47379565018990	AV. KENKITI SIMOMOTO, 448, JAGUARÉ	05347-010	Milton Ribeiro Correia - (14) 99757-8659

DELL COMPUTADORES DO BRASIL
LTDA:72381189000110

Digitally signed by DELL
COMPUTADORES DO BRASIL
LTDA:72381189000110
Date: 2026.08.04 15:19:39 -03'00'

Dell Computadores do Brasil Ltda.

Juliane Casagrande Rodrigues – Gerente de Vendas

***Esta declaração é válida pelo prazo de 90 (noventa) dias da sua emissão.**

DELL Computadores do Brasil Ltda.

Av. Industrial Belgraf, 400, Eldorado do Sul/RS. Geral: 51 3481 5500 Fax: 51 3481 5458

Eldorado do Sul, 4 de agosto de 2026

À

A3 INFOTECH COMERCIO E PRESTAÇÃO DE SERVIÇOS E INFORMÁTICA LTDA.

Ref.: Serviço Nacional de Aprendizagem Comercial – Administração Regional no Estado de São Paulo – Senac/SP – Pregão Eletrônico PEE 2026000049

DECLARAÇÃO

A **DELL COMPUTADORES DO BRASIL LTDA. ("Dell")**, inscrita no CNPJ sob o nº 72.381.189.0001-10, com sede na Av. Industrial Belgraf, 400, bairro Medianeira, Eldorado do Sul/RS, CEP 92.990-000, vem, por meio de seu representante legal, declarar que a empresa **A3 INFOTECH COMERCIO E PRESTAÇÃO DE SERVIÇOS E INFORMÁTICA LTDA.**, com sede na Rua Java, 34, sala 14, Jardim do Mar, São Bernardo do Campo/SP, CEP 09.750-650, inscrita no CNPJ sob o nº 31.385.684/0001-10, faz parte do Programa de Parceria DELL TECHNOLOGIES e é atualmente parceira da Dell, estando autorizada a comercializar os produtos e serviços Dell em todo o território brasileiro.

DELL COMPUTADORES
DO BRASIL
LTDA:72381189000110

Digitally signed by DELL
COMPUTADORES DO BRASIL
LTDA:72381189000110
Date: 2026.08.04 15:19:21 -03'00'

Dell Computadores do Brasil Ltda.

Juliane Casagrande Rodrigues – Gerente de Vendas

***Esta declaração é válida pelo prazo de 90 (noventa) dias da sua emissão.**

DELL Computadores do Brasil Ltda.

Av. Industrial Belgraf, 400, Eldorado do Sul/RS. Geral: 51 3481 5500 Fax: 51 3481 5458

Eldorado do Sul, 4 de agosto de 2026

À

A3 INFOTECH COMERCIO E PRESTAÇÃO DE SERVIÇOS E INFORMÁTICA LTDA

A/C Sr(a). Fabio Eduardo Maranesi

Ref.: Serviço Nacional de Aprendizagem Comercial – Administração Regional no Estado de São Paulo – Senac/SP – Pregão Eletrônico PEE 2026000049

DECLARAÇÃO

A **DELL COMPUTADORES DO BRASIL LTDA. (“Dell”)**, inscrita no CNPJ sob o nº 72.381.189.0001-10, com sede na Av. Industrial Belgraf, 400, bairro Medianeira, Eldorado do Sul/RS, CEP 92.990-000, com o objetivo de complementar as informações que não constam no Catálogo Técnico Oficial do(s) produto(s) abaixo ofertado(s), vem, através da presente, declarar o que segue:

Objeto: **PowerEdge R770 e PowerEdge R570**

- Os equipamentos e componentes ofertados são novos (sem uso, reforma ou recondicionamento), quando do fornecimento inicial do pedido; estão em linha de produção; são customizados em fábrica, não sofrendo qualquer adição de componentes após produção;
- A placa mãe é do mesmo fabricante dos equipamentos e desenvolvida especificamente para o modelo ofertado;
- A BIOS é do mesmo fabricante dos equipamentos ofertados, o qual é detentor dos direitos copyright;
- Os acessórios e cabos necessários para o funcionamento dos equipamentos serão fornecidos juntamente com eles.

DELL COMPUTADORES
DO BRASIL
LTDA:72381189000110

Digitally signed by DELL
COMPUTADORES DO BRASIL
LTDA:72381189000110
Date: 2026.08.04 15:19:57 -03'00'

Dell Computadores do Brasil Ltda.

Juliane Casagrande Rodrigues – Gerente de Vendas

***Esta declaração é válida pelo prazo de 90 (noventa) dias da sua emissão.**

DELL Computadores do Brasil Ltda.

Av. Industrial Belgraf, 400, Eldorado do Sul/RS. Geral: 51 3481 5500 Fax: 51 3481 5458