

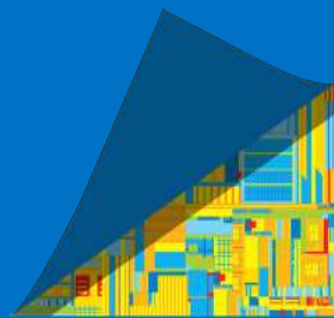


# Intel vPro

## Marcio Paulino

[marcio.paulino@intel.com](mailto:marcio.paulino@intel.com)

Novembro 2018



# O que é o vPro?

- Tecnologia integrada ao hardware que permite gerenciar computadores mesmo se ele estiver desligado, com sistema operacional inoperante, ou com falha no HD.



[https://software.intel.com/sites/manageability/AMT\\_Implementation\\_and\\_Reference\\_Guide/default.htm](https://software.intel.com/sites/manageability/AMT_Implementation_and_Reference_Guide/default.htm)

# Desde 2006...

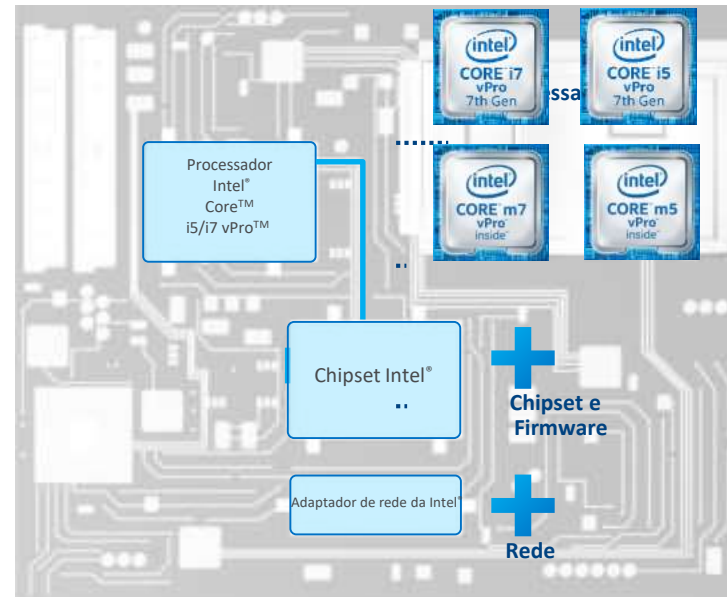
- AMT 1.0 lançado em 2006
- AMT 11 é a versão do vPro na família Core i5/i7 sexta-geração
- A cada nova geração do AMT novos recursos são inseridos



# Plataforma vPro

É composta por:

- Processador Core i5/Core i7
- Core m5/m7
- Chipset versão Q?x....
- Adaptador de rede Centrino
- ME Firmware

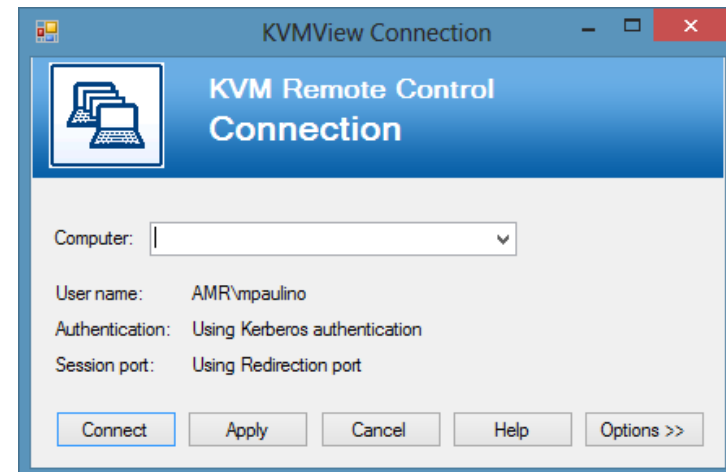


# vPro - Principais Recursos

# KVM

## Permite capturar

- Tela, teclado e mouse
- Não requer agente de software
- Funciona mesmo com a máquina desligada
- Suporte a 3 monitores



# Redirecionamento de Boot - IDEr

- Redireciona o boot para um arquivo ISO
- Usado para remoção de virus e reinstalação do Sistema Operacional



# Inventário de Hardware

- Acesso ao inventário de hardware diretamente no chip
- Leitura mesmo com a máquina desligada

## System Information

### Platform

Computer model	HP EliteBook Revolve 810 G1
Manufacturer	Hewlett-Packard
Version	A1029F1103
Serial number	2CE3410CYL
System ID	03638e56-2fc5-11e3-9673-ce39e79cb403

### Baseboard

Manufacturer	Hewlett-Packard
Product name	18F8
Version	KBC Version 51.25
Serial number	PDMQR1A2F5H1FE
Asset tag	Unknown
Replaceable?	Yes

### BIOS

Vendor	Hewlett-Packard	
Version	68IOD Ver. F.48	
Release date	02/10/2014	
Supported functions	PCI	PC card
	Upgradeable	Shadowing is allowed
	Boot from CD	Selectable boot
	EDD spec	Print Screen service
	8042 keyboard services	Serial services
	Printer services	



# Acesso Remoto a BIOS

- Acesso a BIOS remotamente via IP
- Permite alterar parâmetros remotamente



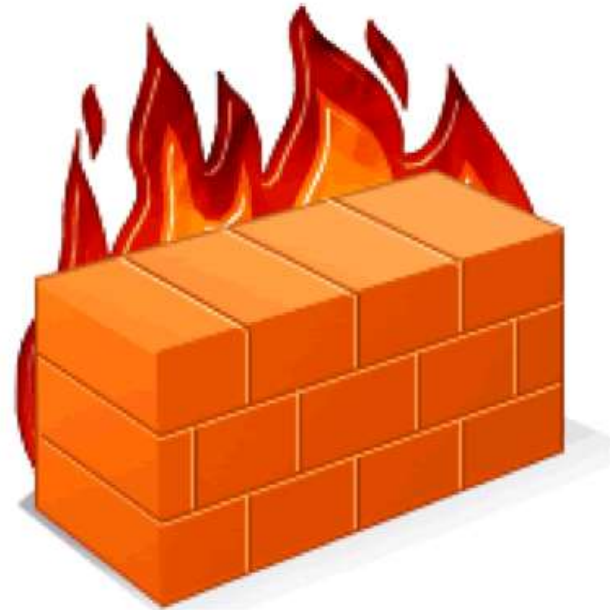
# Power On e OFF Remoto

- Power on e off remoto via IP
- Não confinado ao domínio de VLAN



# System Defense

- Firewall embarcado no chipset baseado em hardware
- Protegido do Sistema Operacional



# Presença de Agente

- Monitora aplicações ativas no Sistema operacional
- Ativa o System Defense com base nos aplicativos locais



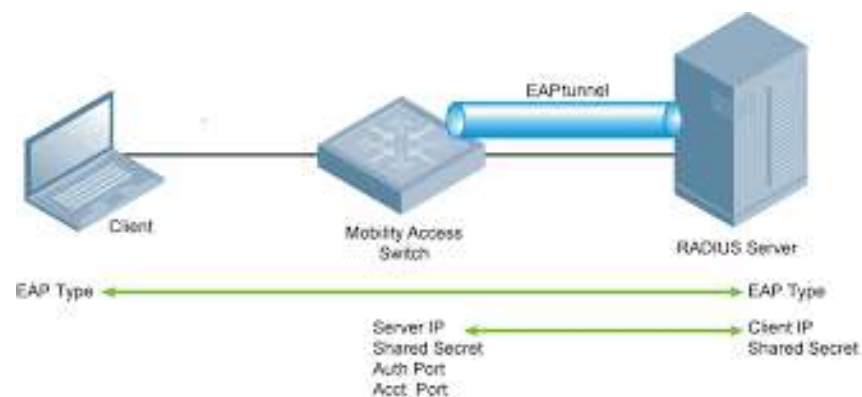
# PC Alarm Clock

- Power on com hora marcada
- Sem necessidade de conexão a rede



# vPro e 802.1x

- Suplicante no chip
- Acesso ao vPro mesmo com a máquina desligada
- Ethernet e Wifi



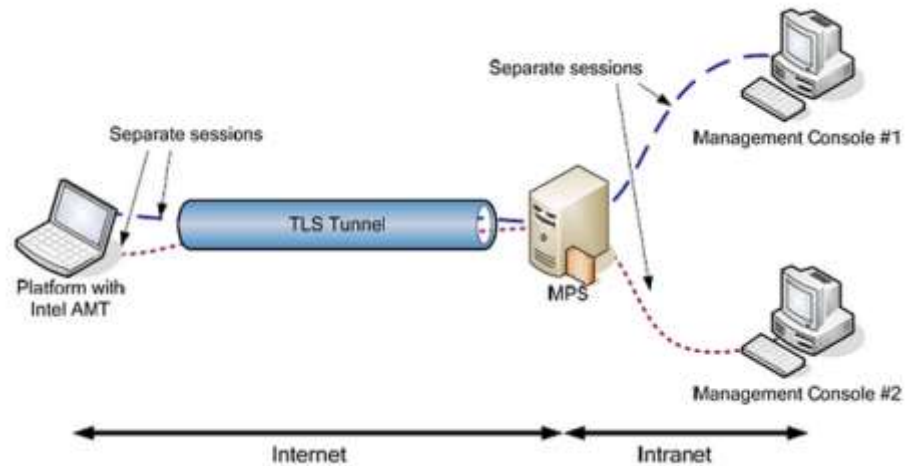
# PC Alarm Clock

- Power on com hora marcada
- Sem necessidade de conexão a rede



# Fast Call for Help

- Habilita o vPro na internet
- Permite reparo via internet (BIOS, IDE-r e KVM)



<https://software.intel.com/en-us/articles/fast-call-for-help-overview/>



# Intel IPT with OTP

- Fornece o segundo fator de autenticação
- Token hardware presente no processador

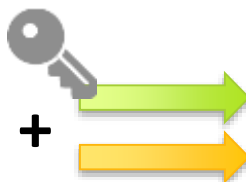


# IPT com PKI

- Reduz os custos da VPN reduzindo senhas

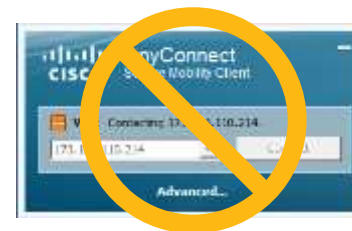


Primeiro fator: Senha do Windows\* ou disco rígido



Intel® IPT com PKI: Chaves de firmware embarcadas

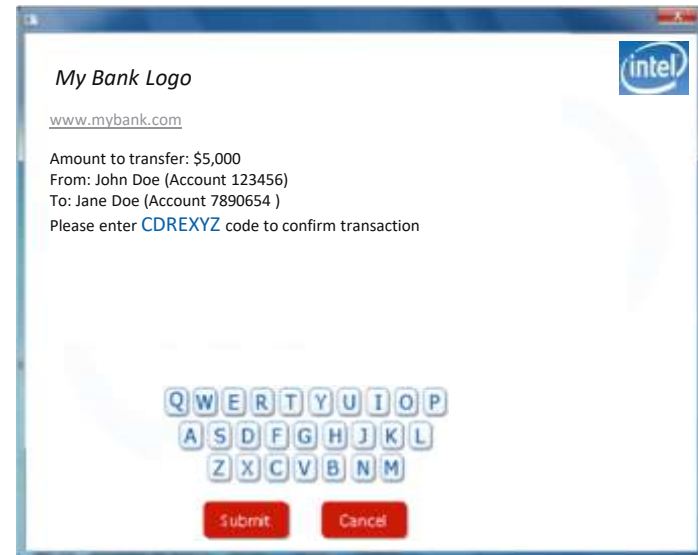
=



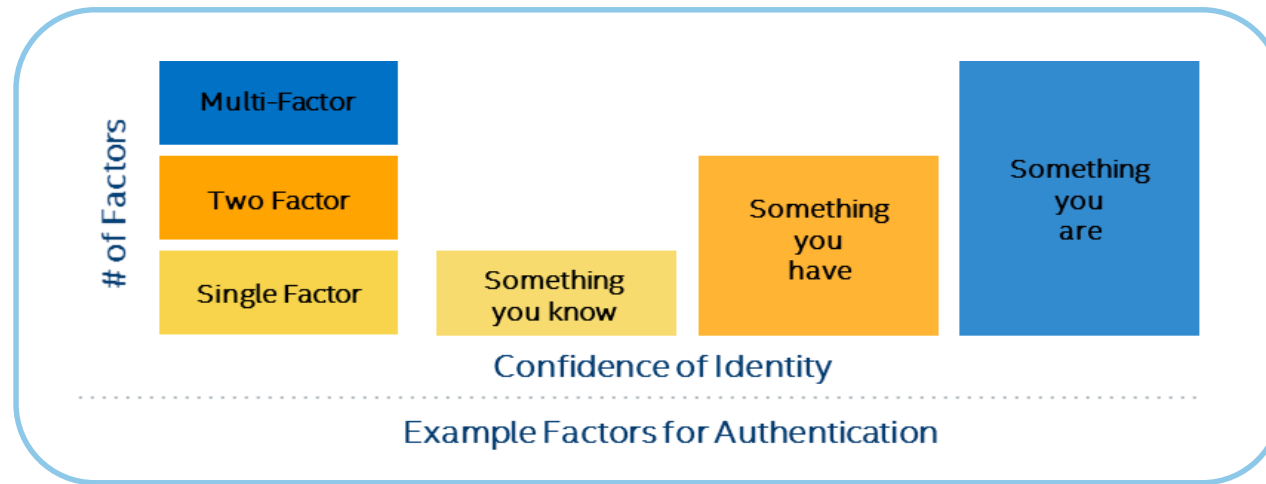
Não há mais necessidade de senha de VPN

# Intel PTD

- Protege o teclado virtual
- O atacante (hacker) não consegue ver a tela do teclado virtual



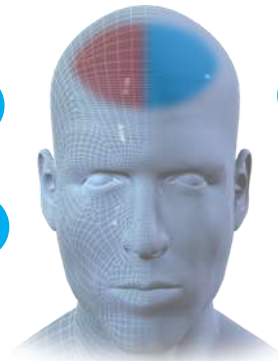
# Multi-Fatores de Autenticação



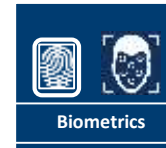
Something  
you Know



Something  
you Have



Something  
you Are



Somewhere  
you Are



# Intel SSD Pro 7x00p, 6000p e 5450s

- Digital Fence
- Remote Erase
- Criptografia acelerada em hardware <2s.



Intel Confidential

# Intel Unite: Colaboração



## Intel Unite:

- Wireless display (na sala ou remoto)
- Share ponto a ponto
- Split de tela
- Anotações temporárias
- Transferencia de arquivos
- Administração remota
- Suporte a plugin
- Criptografia

# Provisionamento

# Provisionamento

## Client Mode

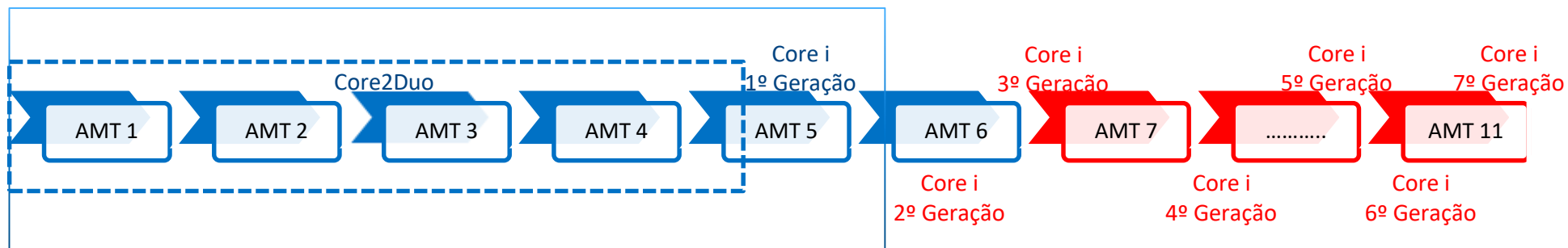
- Ativação rápida e fácil
- Compatível com as versões AMT 7, 8, 9 e 11
- Ethernet ou Wifi

## Admin Mode

- Presente em todas as versões do vPro, AMT 1.0 até 11
- Requer infra-estrutura
- Ethernet only



# Modos Suportados



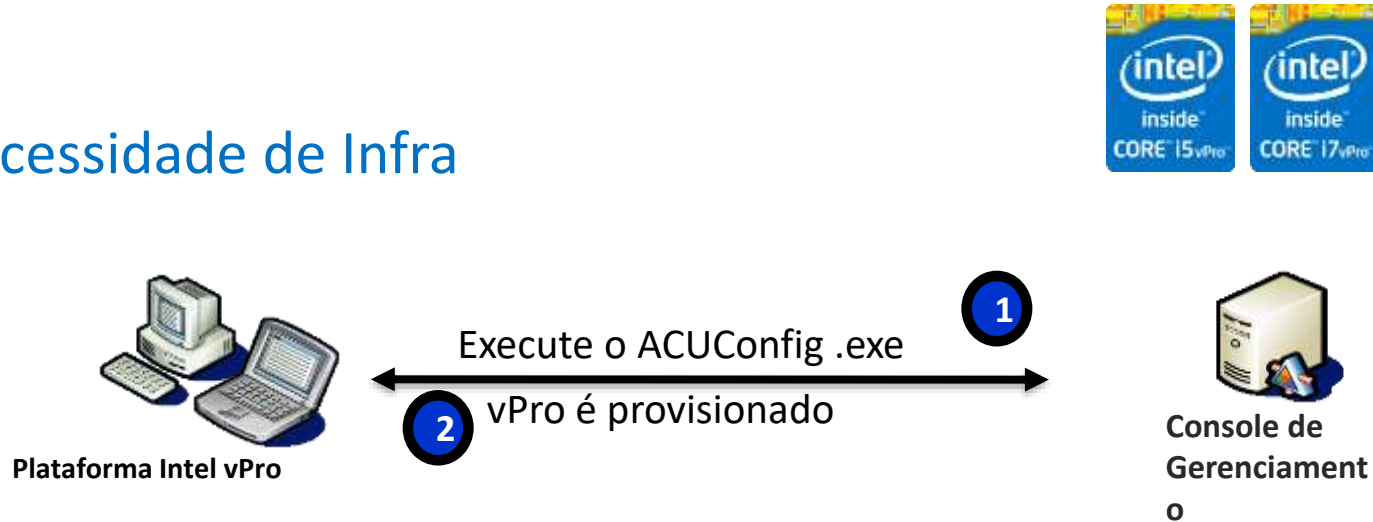
Admin Mode



Client Mode

# Client Mode

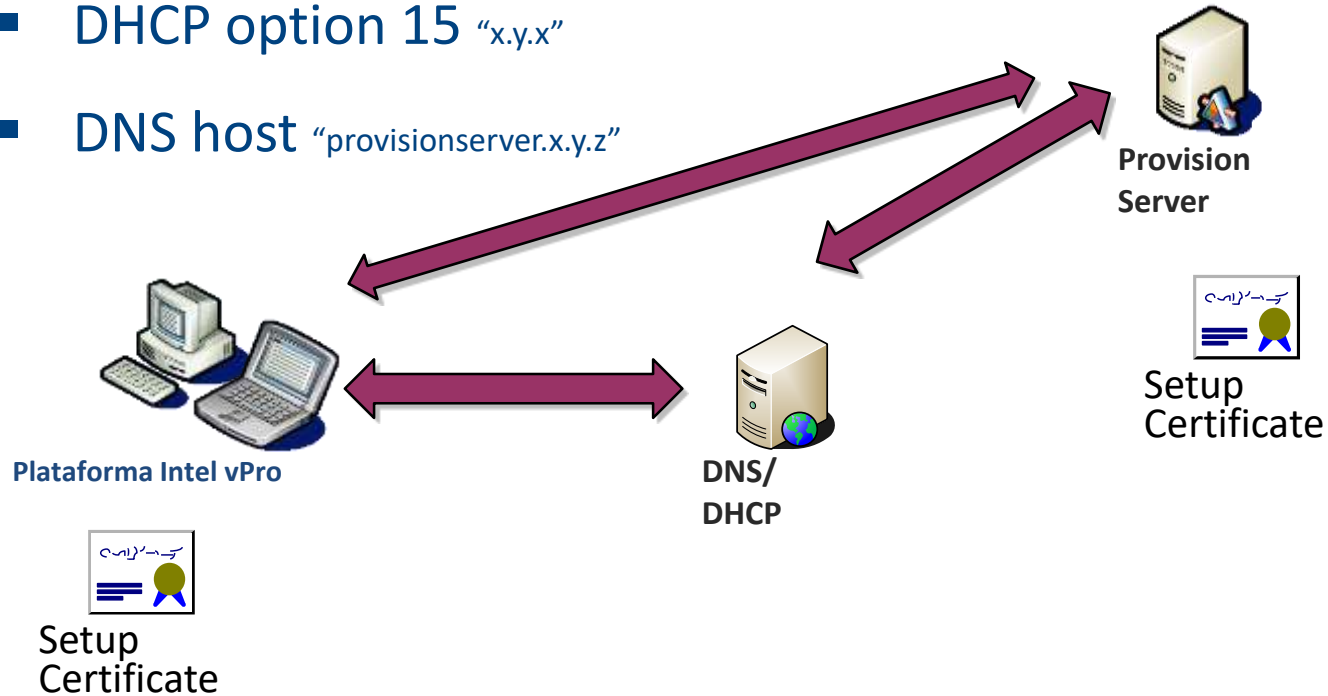
Sem necessidade de Infra



O provisionamento é executado localmente

# Admin Mode

- DHCP option 15 "x.y.x"
- DNS host "provisionserver.x.y.z"

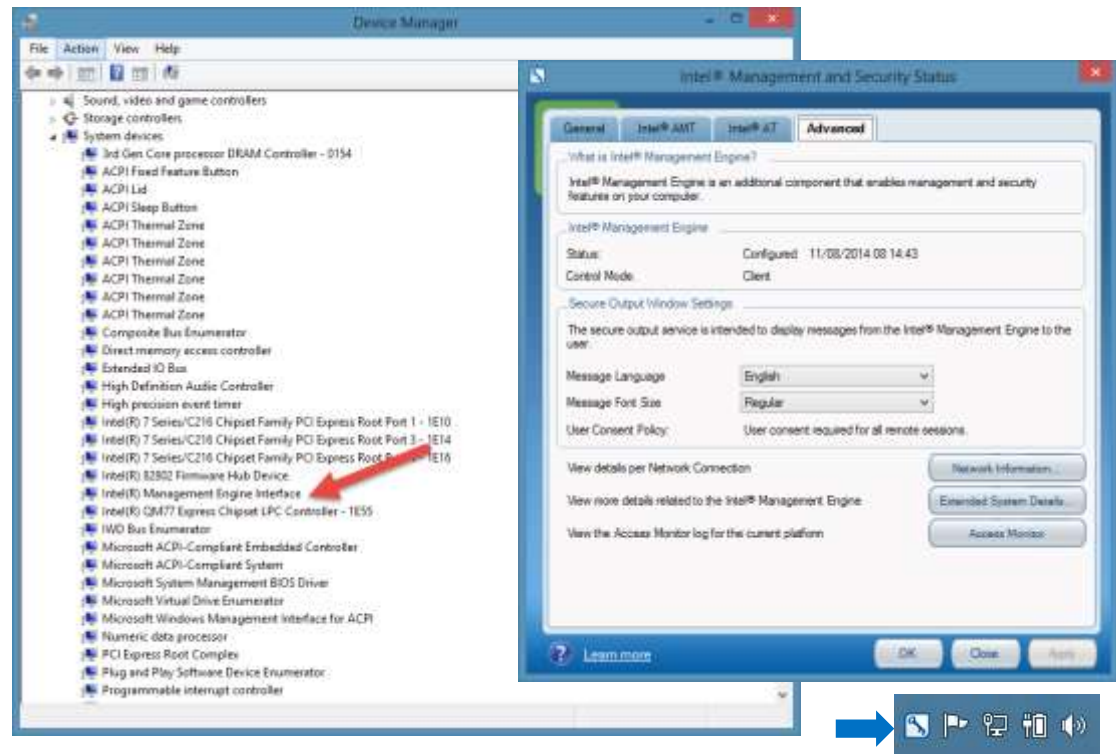


Ativação é executada pela rede



# Pré-Requisito para Provisionamento

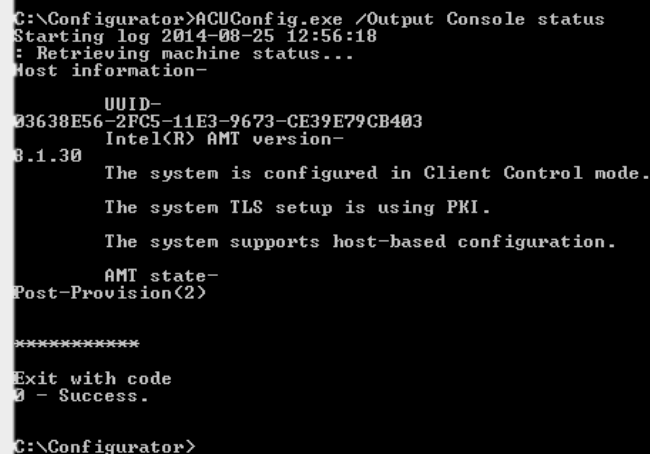
- ME driver instalado
- Faz ponte entre o SO e o AMT
- Cada versão do AMT tem o seu driver
- Não é possível instalar um driver genérico



# Executar o Provisionamento

- Através do executável acuconfig.exe junto com o arquivo xml exportado do Intel SCS
- Client mode
- Admin mode
- Direitos de administrador

Acuconfig.exe /Output Console Status



```
C:\Configurator>ACUConfig.exe /Output Console status
Starting log 2014-08-25 12:56:18
: Retrieving machine status...
Host information-

      UUID-
03638E56-2FC5-11E3-9673-CE39E79CB403
      Intel(R) AMT version-
8.1.30
      The system is configured in Client Control mode.
      The system TLS setup is using PKI.
      The system supports host-based configuration.

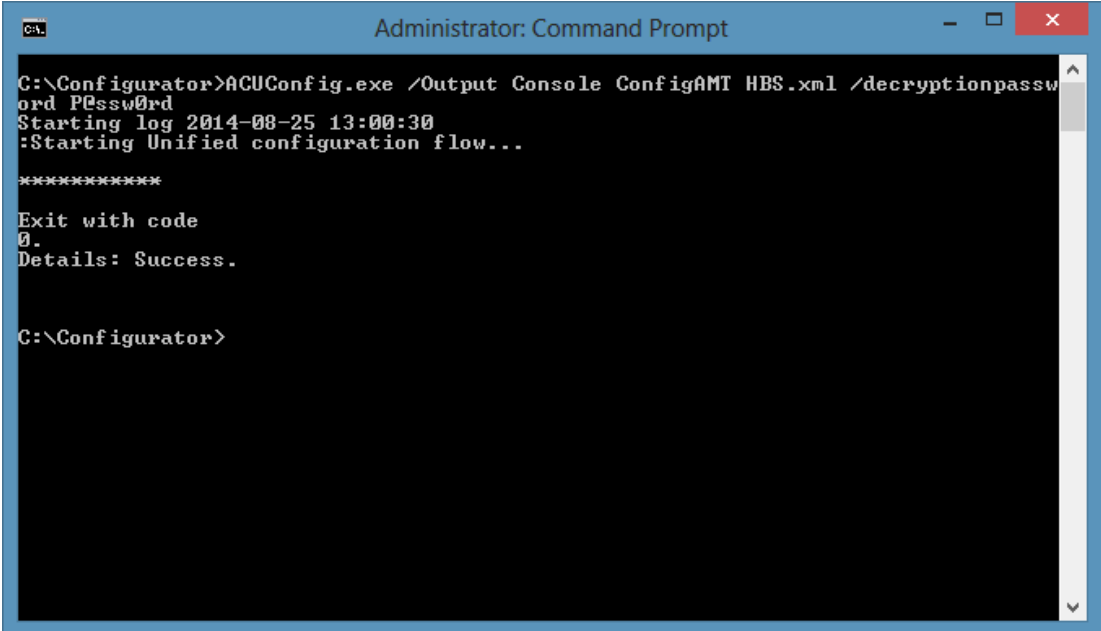
      AMT state-
Post-Provision(2)

*****
Exit with code
0 - Success.

C:\Configurator>
```

# Provisionamento em Client Mode

- `Acuconfig.exe /Output Console ConfigAMT profile1.xml /decryptionpassword`



```
C:\>Administrator: Command Prompt

C:\Configurator>ACUConfig.exe /Output Console ConfigAMT HBS.xml /decryptionpassword P@ssw0rd
Starting log 2014-08-25 13:00:30
:Starting Unified configuration flow...

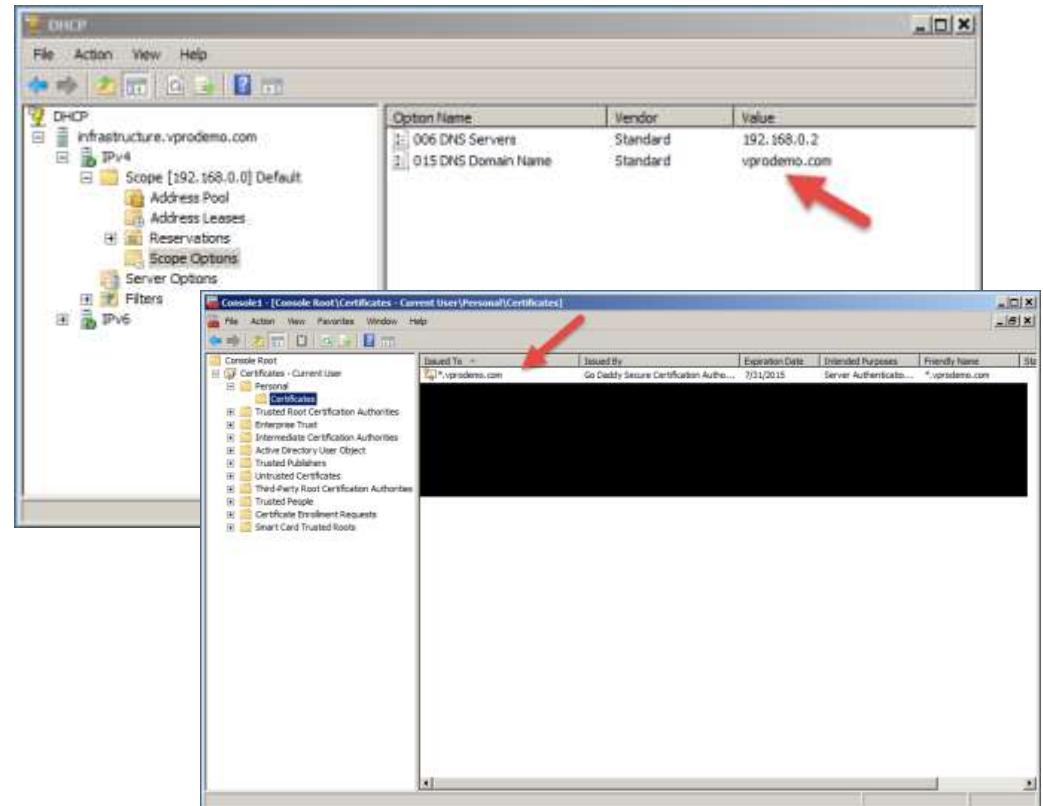
*****
Exit with code
0.
Details: Success.

C:\Configurator>
```

`Acuconfig.exe /Output Console ConfigAMT profile1.xml /decryptionpassword P@ssw0rd`

# Provisionamento em Admin Mode

- DHCP e DNS
- Opção 15 no escopo do DHCP configurada com o nome de domínio
- Certificado de provisionamento instalado no Intel SCS



Acuconfig.exe /Output Console ConfigViaRCSOnly 192.168.1.10 Profile1 /WMIUser vprodemo\administrator /WMIUserpassword P@ssw0rd

# Verificando o Certificado

- Use o aplicativo ZTC para identificar os certificados instalados no vPro



ZTC.zip

ZTCLocalagent.exe -discovery

```
Administrator: Command Prompt

Friendly Name = Go Daddy Class 2 CA
Default = true
Active = true
Hash Algorithm = SHA1

Certificate Hash:
27 96 BA E6 3F
18 01 E2 77 26
1B A0 D7 77 70
02 8F 20 EE E4

Certificate hash entry:

Friendly Name = Comodo AAA CA
Default = true
Active = true
Hash Algorithm = SHA1

Certificate Hash:
D1 EB 23 A4 6D
17 D6 8F D9 25
64 C2 F1 F1 60
17 64 D8 E3 49

Certificate hash entry:

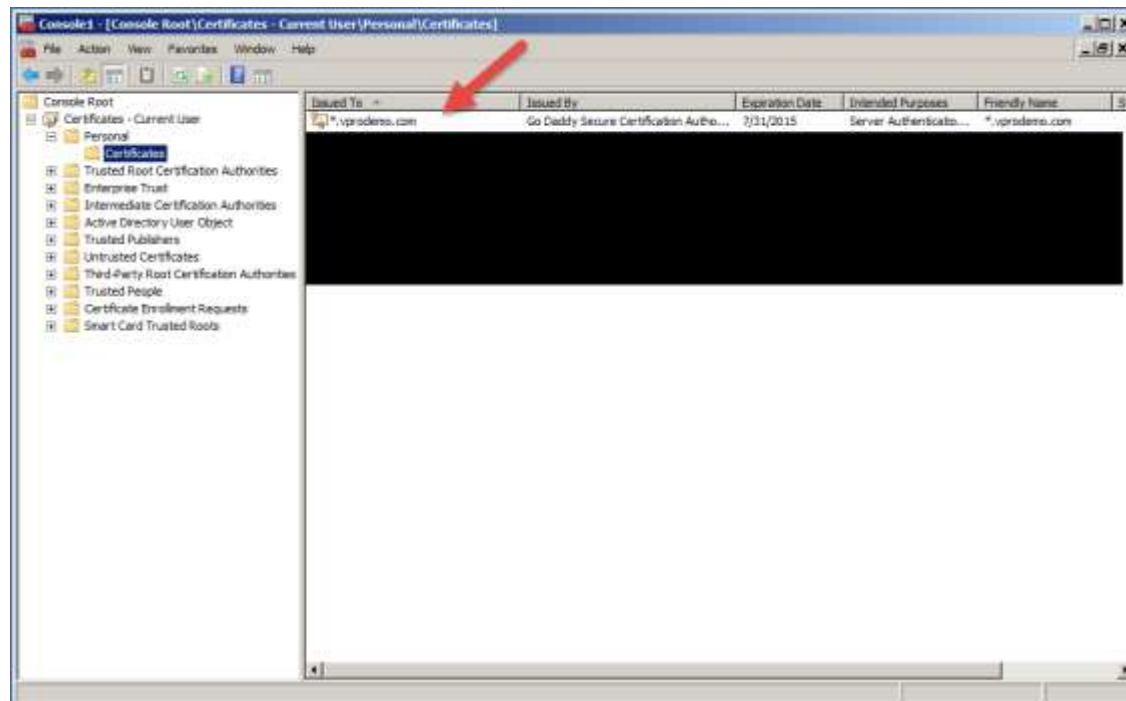
Friendly Name = Starfield Class 2 CA
Default = true
Active = true
Hash Algorithm = SHA1

Certificate Hash:
AD 7E 1C 28 B0
64 EF 8F 60 03
40 20 14 C3 D0
E3 37 0E B5 8A
```



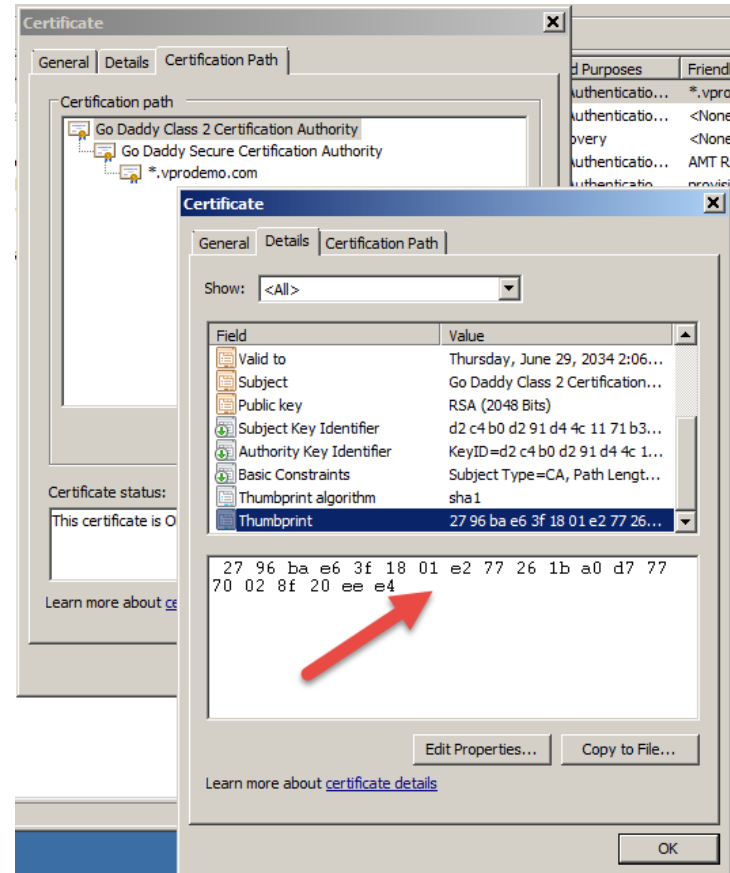
# Verificando o Certificado

- O certificado deverá ser instalado na area de usuário que instalou o Intel SCS



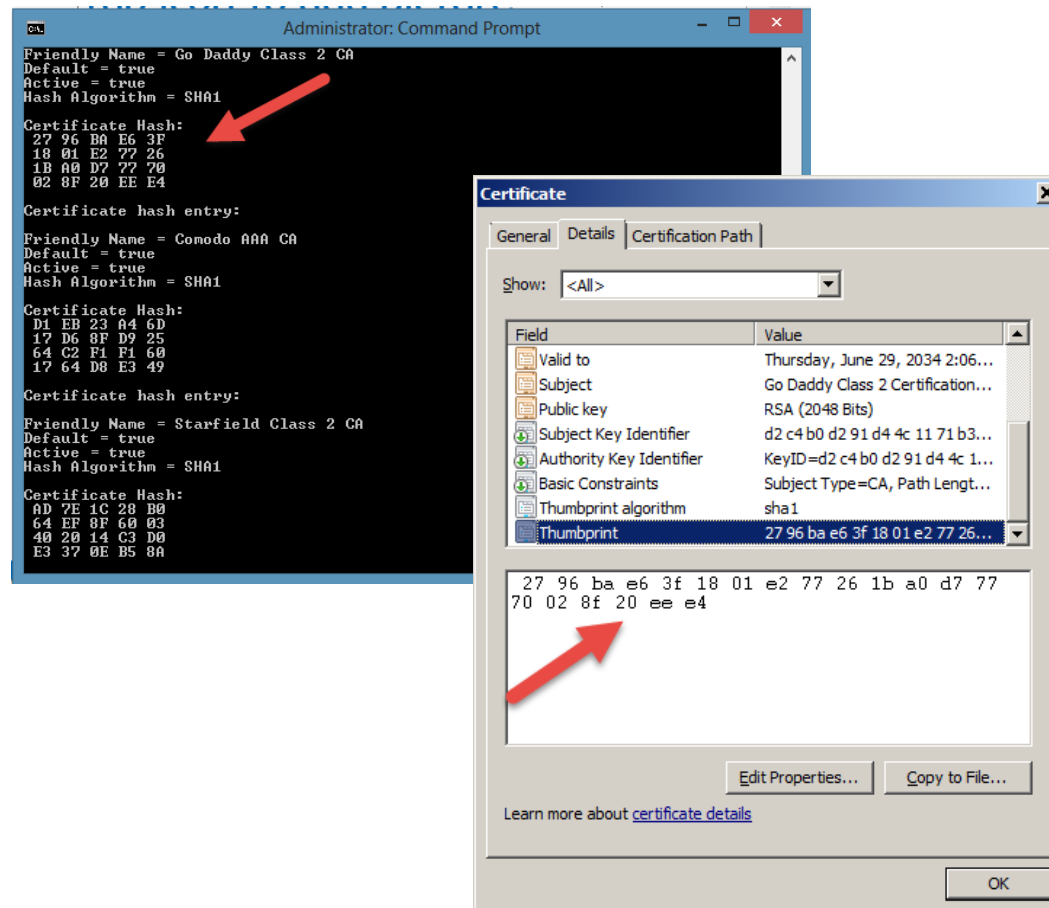
# Verificando o Certificado

- Click duas vezes no certificado vprodemo.com
- Escolha Certification Path
- Detalhes
- Thumbprint



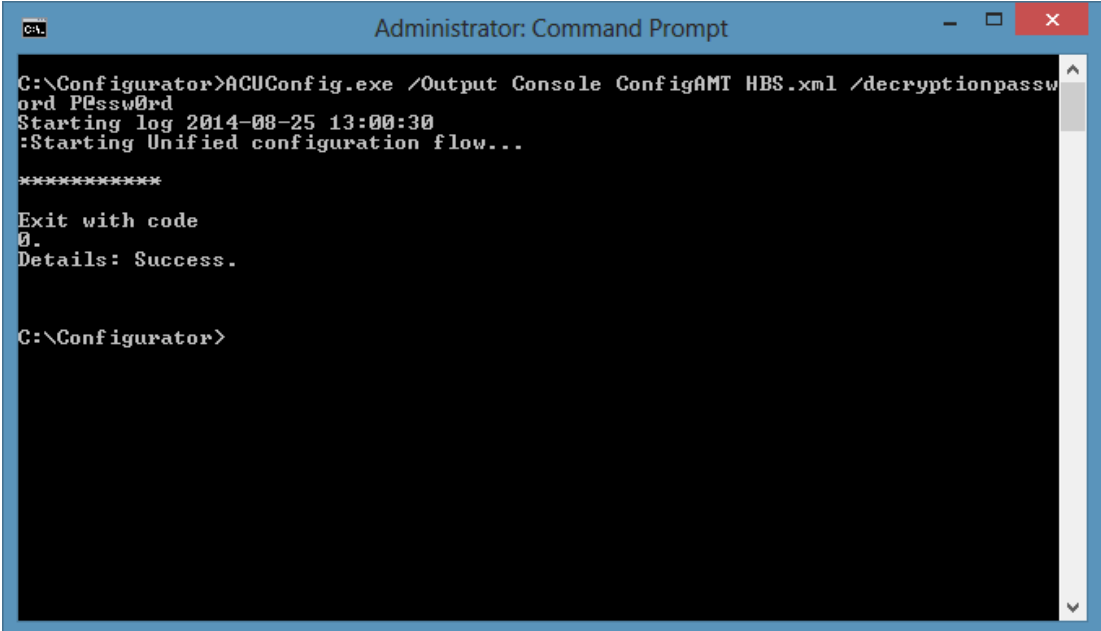
# Verificando o Certificado

- Comparar o certificado publico do ME com certificado vPro
- Tem que apresentar o mesmo valor



# Provisionamento em Admin Mode

- `Acuconfig.exe /Output Console ConfigViaRCSOnly profile1.xml /WMIUser vprodemo\administrator /WMIUserpassword P@ssw0rd`



```
C:\Configurator>ACUConfig.exe /Output Console ConfigAMT HBS.xml /decryptionpassword P@ssw0rd
Starting log 2014-08-25 13:00:30
:Starting Unified configuration flow...

*****
Exit with code
0.
Details: Success.

C:\Configurator>
```

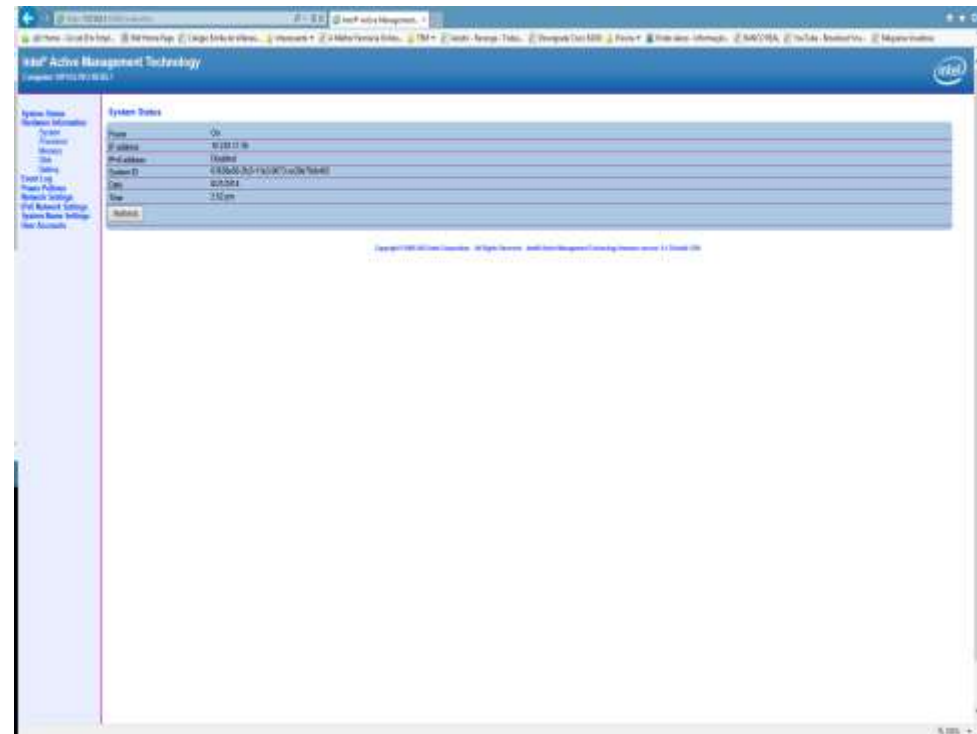
`Acuconfig.exe /Output Console ConfigViaRCSOnly profile1 /WMIUser vprodemo\Administrator /WMIUserPassword P@ssw0rd`

# Acessando a Plataforma vPro

# Acesso Web

- Verificar o status da máquina
- Acesso ao inventário de hardware
- Power on/off remote
- Informações de rede

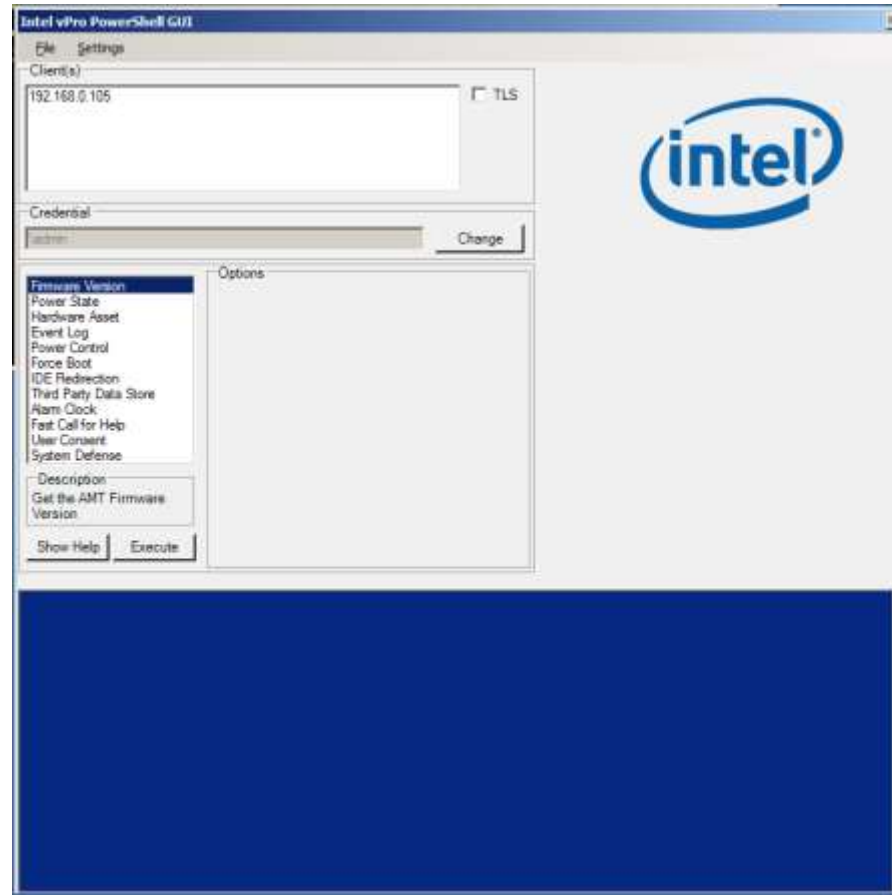
<http://nomedamáquina:16992>



# PowerShell

- Versão do AMT
- Power State
- Inventário de Hardware
- Power Control
- Alarm Clock
- User Consent
- System Defense

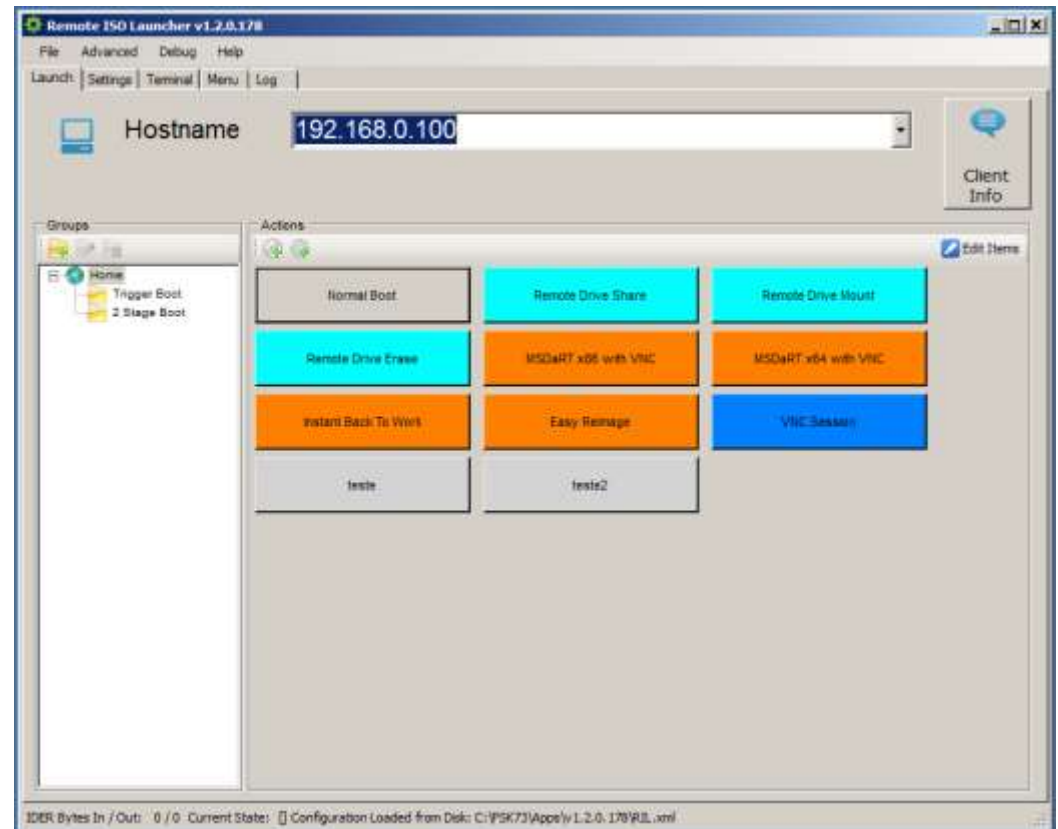
[https://downloadcenter.intel.com/Detail\\_Desc.aspx?DwnldID=22504](https://downloadcenter.intel.com/Detail_Desc.aspx?DwnldID=22504)



# Remote ISO Launcher

- Lançado de ISO
- Interface fácil e simples
- Altamente customizável

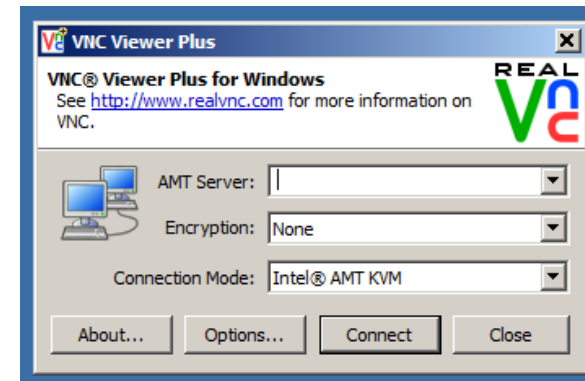
[https://downloadcenter.intel.com/Detail\\_Desc.aspx?DwnldID=20961](https://downloadcenter.intel.com/Detail_Desc.aspx?DwnldID=20961)





# Real VNC Plus

- Controle remote
- Teclado, video e mouse
- Power on/off
- BIOS
- IDE-r



<http://www.realvnc.com/products/viewerplus/>

# Intel vPro Platform Solution Manager

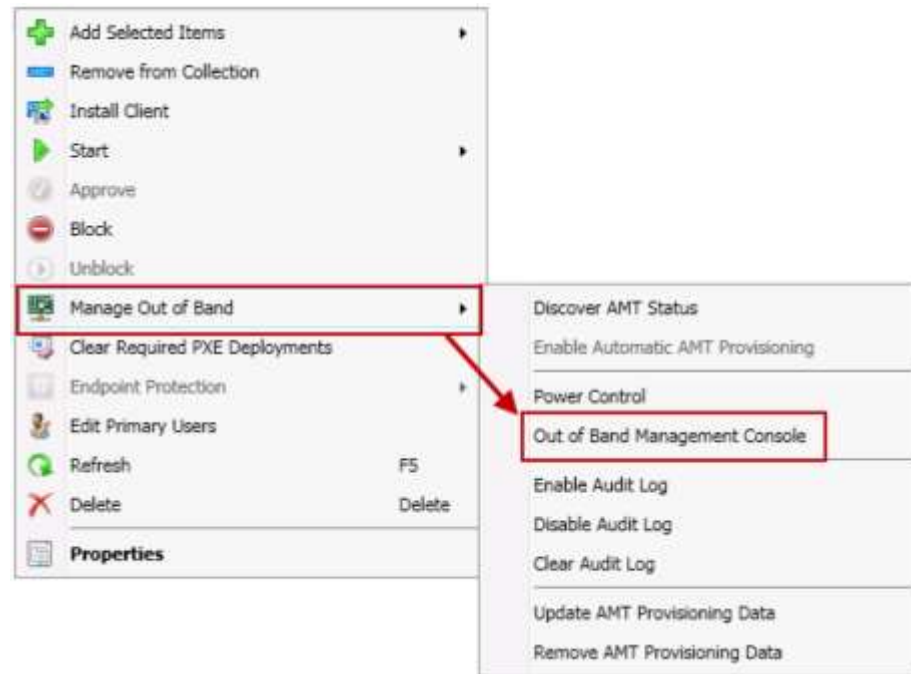
- Ferramenta de demonstração das funcionalidades vPro
- Livre download



<https://software.intel.com/en-us/blogs/2013/04/19/introducing-the-intel-vpro-platform-solution-manager>

# Intel SCS Add-on 2.1for SCCM

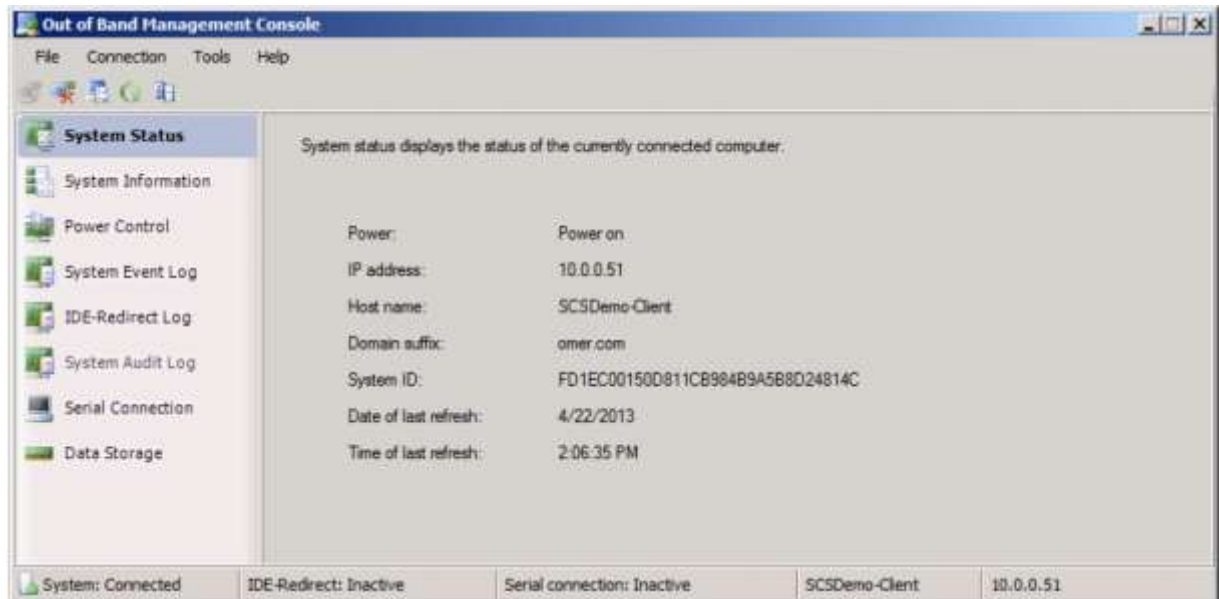
- Habilita o SCCM para trabalhar com vPro
- Requer conexão SSL
- CA Server



[https://downloadcenter.intel.com/Detail\\_Desc.aspx?DwnldID=24010](https://downloadcenter.intel.com/Detail_Desc.aspx?DwnldID=24010)

# Intel SCS Add-on 2.1for SCCM

- System Status
- Power Control
- IDE-Redirect
- Serial Over Lan



# Intel® AMT Features

Value-added features requested by, and designed for, IT administrators



Features	DASH profiles DMTF's standards for remote management	Intel® Standard Manageability Remote manageability features available on desktop platforms	Intel AMT Full suite of remote device management capabilities available on desktop and mobile platforms
Hardware inventory	✓	✓	✓
Software inventory	✓	✓	✓
User account management	✓	✓	✓
Boot control	✓	✓	✓
Web Services Management (WS-Man) specification	✓	✓	✓
Power state management	✓	✓	✓
Redirection	✓	✓	✓
Alarm clock		✓	✓
Agent presence		✓	✓
Access monitor		✓	✓
Remote configuration		✓	✓
System defense filters		✓	✓
Out-of-band KVM remote control	*		✓
Wireless Intel AMT			✓
Fast Call for Help (CIRA)			✓
Intel® Remote Secure Erase with Intel® SSD Pro			✓

\*Note: DASH KVM profile DSP1076 does not include full Out-of-Band KVM remote control features

# Intel® 300 Series Chipsets Business

- Supports 8<sup>th</sup> Gen Intel® Core™ (Coffee Lake-S) processors
- Support for integrated Intel® Wireless-AC
  - Wi-Fi 802.11ac R2 & Bluetooth\* 5
- Integrated USB 3.1 Gen 2 (10 Gb/s)
- Support for next generation Intel® Optane™ Memory
- Support for Intel® Smart Sound Technology with quad-core audio DSP
- Three independent display support
- Intel® Rapid Storage Technology 16
- Intel® Platform Trust Technology (w/o Intel® TXT)
- Intel® Boot Guard
- Intel® Rapid Storage Technology for CPU-attached Intel PCIe Storage<sup>1</sup>
- Integrated Gigabit Ethernet MAC
  - Supports Intel® Ethernet Connection I219 (Jacksonville LAN PHY)

Key Feature Differentiation	Q370	B360
Intel® ME 12 Firmware SKU	Corporate	Consumer/ Corporate
Processor PCI Express* 3.0 Configuration Support	1x16 or 2x8 or 1x8+2x4	1x16
Independent Display Ports / Pipes Support	3/3	3/3
Memory Channels / DIMMs per Channel	2/2	2/2
Integrated Intel® Wireless-AC Support	Yes	Yes
Intel® Smart Sound Technology <sup>3</sup>	Yes	Yes
Intel® SIPP Eligible <sup>4</sup>	Yes	No
Intel® vPro™ Technology Eligible <sup>4</sup>	Yes	No
Intel® Active Management Technology <sup>4</sup>	Yes	No
Intel® Standard Manageability	Yes	No
Intel® Optane™ Memory Support	Yes	Yes
Integrated SDXC (SDA 3.0) Support	Yes	Yes
Maximum High Speed I/O Lanes	30	24
Total USB Ports (Maximum USB 3.1) <sup>2</sup>	14 (10)	12 (6)
Maximum USB 3.1 Ports: Gen 2 (10 Gb/s) / Gen 1 (5 Gb/s) <sup>2</sup>	6 / 10	4 / 6
Maximum SATA 3.0 Ports (6 Gb/s) <sup>2</sup>	6	6
Maximum PCI Express* 3.0 lanes <sup>2</sup>	24	12
Intel® Rapid Storage Technology	Yes	Yes
Maximum Intel® RST for PCIe Storage Ports (x2 M.2 or x4 M.2) <sup>2</sup>	3	1
Intel® RST PCIe RAID 0, 1, 5 <sup>1</sup>	Yes	No
Intel® RST SATA RAID 0, 1, 5, 10 <sup>1</sup>	Yes	No
Intel® Rapid Storage Technology for CPU-attached Intel PCIe Storage <sup>1</sup>	Yes	No

1. Some features and capabilities require SSDs and/or multiple HDDs
2. Maximum lanes/port counts available may vary depending on platform implementation.
3. Certain features may not be present in all SKUs.
4. Intel SIPP, Intel vPro™, & Intel AMT support requires select Coffee Lake-S processors and select Intel® 300 series chipsets

Intel Confidential - NDA Platform Roadmap. All dates and plans are subject to change without notice.

# Intel® 200 Series Chipsets - Business

- Supports 7<sup>th</sup> Gen Intel® Core™ (Kaby Lake-S) & 6<sup>th</sup> Gen Intel® Core™ (Skylake-S) processors LGA 1151
- Support for Intel® Optane™ memory
- Intel® Rapid Storage Technology 15
- Three independent displays
- Intel® Platform Trust Technology (w/o Intel® TXT)
- Intel® Boot Guard
- Intel® Smart Sound Technology
- Integrated Gigabit Ethernet MAC
  - Supports Intel® Ethernet Connection I219 (Jacksonville LAN PHY)

Some features are not available on all corporate chipset skus.

1. Intel SIPP, Intel vPro™, & Intel AMT support requires select Kaby Lake-S processors and select Intel® 200 series chipsets
2. Some features and capabilities require SSDs and/or multiple HDDs
3. Maximum lanes/port counts available may vary depending on platform implementation

Key Feature Differentiation	Q270	Q250	B250
Intel® ME 11 Firmware SKU	Corporate	Corporate	Corporate / Consumer
Processor PCI Express* 3.0 Configuration Support	1x16 or 2x8 or 1x8+2x4	1x16	1x16
Intel® SIPP Eligible	Yes <sup>1</sup>	Yes <sup>1</sup>	No
Intel® vPro™ Technology	Yes <sup>1</sup>	No	No
Intel® Active Management Technology	Yes <sup>1</sup>	No	No
Intel® Standard Manageability	Yes	Yes	No
Intel® Optane™ Memory Support	Yes	Yes	Yes
Intel® Rapid Storage Technology	Yes	Yes	Yes
Intel® RST PCIe RAID 0, 1, 5 <sup>2</sup>	Yes	No	No
Intel® RST SATA RAID 0, 1, 5, 10 <sup>2</sup>	Yes	No	No
Intel® Smart Response Technology <sup>2</sup>	Yes	No	No
I/O Port Flexibility	Yes	Yes	Yes
Maximum High Speed I/O Lanes	30	27	25
Total USB Ports (Maximum USB3) <sup>3</sup>	14 (10)	14 (8)	12 (6)
Maximum SATA 3.0 Ports (6 Gb/s) <sup>3</sup>	6	6	6
Maximum PCI Express* 3.0 lanes <sup>3</sup>	24	14	12
Maximum Intel® RST for PCIe Storage Ports (x4 M.2 or x2 SATA Express) <sup>3</sup>	3	1	1

Intel Confidential - NDA Platform Roadmap. All dates and plans are subject to change without notice.

# vPro

## Integração com AD



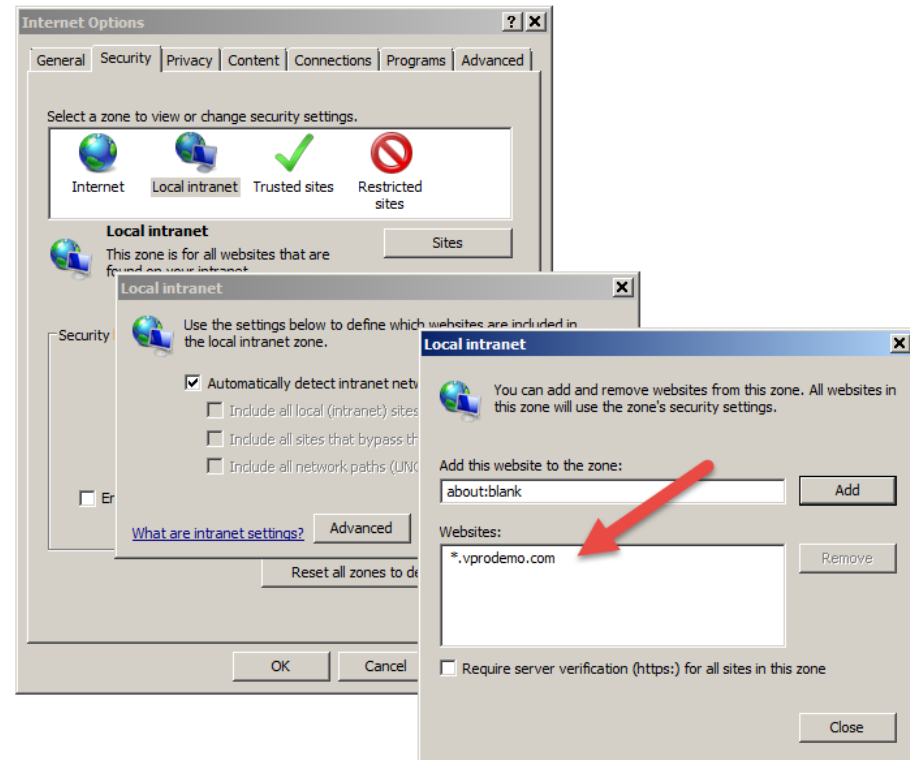
# Integração com AD

- Criar chave no registro
- Configurações no Browser

[https://downloadcenter.intel.com/Detail\\_Desc.aspx?DwnldID=24010](https://downloadcenter.intel.com/Detail_Desc.aspx?DwnldID=24010)

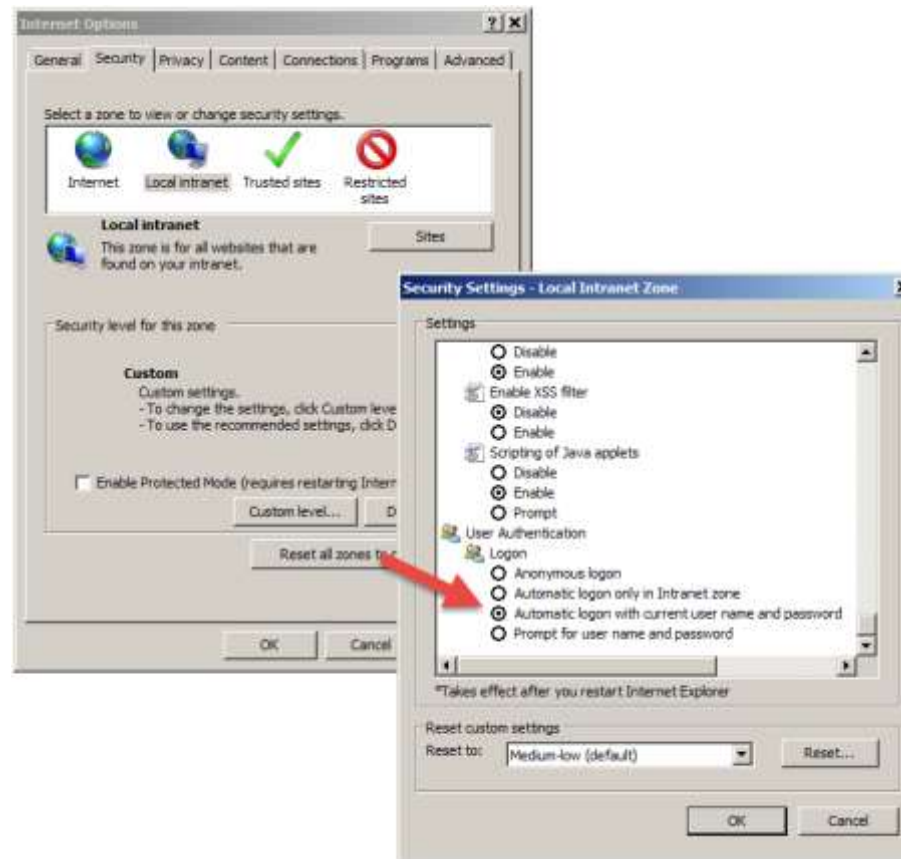
# Configurações Browser

Adicione em Security, Local Intranet, Advanced o domínio interno



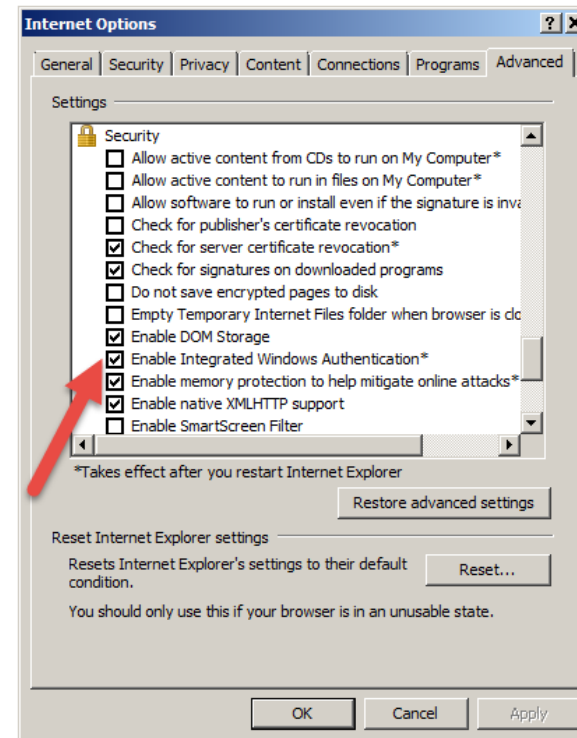
# Configurações Browser

Adicione em Security, Local Intranet, Custom Level



# Configurações Browser

Em Advanced, habilite  
Integrated Windows  
Authentication



# Chave no Registro (criar em 32 e 64)

## Para computadores de 32 bits

Clique em **Iniciar**, clique em **Executar**, digite **regedit** e clique em **OK**.

No painel esquerdo, localize e, em seguida, clique na seguinte subchave do registro:

**HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Main\FeatureControl**

No menu **Editar**, aponte para **novoe**, em seguida, clique em **chave**.

Digite **FEATURE\_INCLUDE\_PORT\_IN\_SPN\_KB908209** e pressione ENTER.

No menu **Editar**, aponte para **novoe**, em seguida, clique em **Valor DWORD**.

Digite **iexplore.exe** e pressione ENTER.

No menu **Editar**, clique em **Modificar**.

Digite **1** na caixa **dados do valor** e, em seguida, clique em **OK**.

Saia do Editor do registro.

## Para computadores de 64 bits

Clique em **Iniciar**, clique em **Executar**, digite **regedit** e clique em **OK**.

No painel esquerdo, localize e, em seguida, clique na seguinte subchave do registro:

**HKEY\_LOCAL\_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Internet Explorer\Main\FeatureControl**

No menu **Editar**, aponte para **novoe**, em seguida, clique em **chave**.

Digite **FEATURE\_INCLUDE\_PORT\_IN\_SPN\_KB908209** e pressione ENTER.

No menu **Editar**, aponte para **novoe**, em seguida, clique em **Valor DWORD**.

Digite **iexplore.exe** e pressione ENTER.

No menu **Editar**, clique em **Modificar**.

Digite **1** na caixa **dados do valor** e, em seguida, clique em **OK**.

Saia do Editor do registro.

Obrigado