 Confidencialida	Tipo de Documento:	Procedimento
	Área de Aplicação:	Segurança da Informação
	Título do Documento:	Procedimento de Hardening para EndPoint

Sumário

1.	OBJETIVO.....	1
2.	ÂMBITO DE APLICAÇÃO	1
3.	DEFINIÇÕES.....	1
4.	DOCUMENTOS DE REFERÊNCIA	3
5.	RESPONSABILIDADES.....	3
6.	REGRAS BÁSICAS.....	3
7.	CONTROLE DE REGISTROS.....	19
8.	ANEXOS.....	19
9.	REGISTRO DE ALTERAÇÕES.....	19

1. OBJETIVO

Garantir a proteção dos servidores em redes e a proteção da infraestrutura do **Grupo CPFL Energia**.

2. ÂMBITO DE APLICAÇÃO

2.1. Empresa

Todas as empresas com participação direta do **Grupo CPFL Energia** e sistemas considerados críticos e para SOX.


2.2. Área

Todas as áreas do **Grupo CPFL Energia**.

3. DEFINIÇÕES


- **CONFIDENCIALIDADE:** É a garantia de que a informação é acessada somente por usuários com o devido direito. Está diretamente vinculada a proteção da privacidade dos usuários e suas informações.
- **INTEGRIDADE:** É a garantia de que a informação no momento que é acessada está em sua completeza, totalidade, plenitude, sem qualquer alteração em seu conteúdo, quando foi armazenada.

N.Documento:	Categoria:	Versão:	Aprovado por:	Data Publicação:	Página:
18933	Instrução	1.0	Emerson Cardoso	08/09/2021	1 de 19

 Confidencialida	Tipo de Documento:	Procedimento
	Área de Aplicação:	Segurança da Informação
	Título do Documento:	Procedimento de Hardening para EndPoint

- **DISPONIBILIDADE:** É a garantia de que a informação está disponível para o usuário (que tem tal direito de acesso) e para o sistema de informação no momento que o usuário necessita consumi-la.
- **SEGURANÇA DA INFORMAÇÃO:** Proteção da informação contra ameaças para garantir a continuidade das atividades finalísticas e meio da instituição, minimizar os riscos e maximizar a eficiência e a efetividade das ações realizadas no **Grupo CPFL Energia**.
- **INCIDENTE DE SEGURANÇA DA INFORMAÇÃO:** Qualquer evento que possa comprometer a Segurança da Informação do **Grupo CPFL Energia**.
- **RISCOS:** Combinação da probabilidade de um evento e suas possíveis consequências.
- **HARDENING:** É uma técnica de blindagem de sistemas que envolve um processo de mapeamento das ameaças, mitigação dos riscos e execução das atividades corretivas com foco na infraestrutura. Seu objetivo principal é tornar o sistema preparado para enfrentar tentativas de ataque.
- **ACESSO:** É o nível de permissão onde se pode realizar uma operação sobre algum recurso computacional.
- **AUTORIZAÇÃO:** Trata-se do que o usuário autenticado pode fazer.
- **CONTROLE:** Forma de gerenciar o risco, incluindo políticas, procedimentos, diretrizes, práticas ou estruturas organizacionais, que podem ser de natureza administrativa, técnica, de gestão ou legal.
- **DISPOSITIVO:** Equipamento e/ou acessório utilizado para acessar, transmitir, compartilhar, visualizar, editar, fazendo-se uso do meio eletrônico para tal.
- **SERVIDOR:** São computadores e outros dispositivos interligados que compartilham informações ou recursos do **Grupo CPFL Energia**.
- **REDE CORPORATIVA:** São computadores e outros dispositivos interligados que compartilham informações ou recursos do **Grupo CPFL Energia**.
- **USUÁRIO:** Qualquer pessoa (colaboradores, visitantes, estagiários, empregados, temporários, prestadores de serviços etc.) que possua ou não ligação com o **Grupo CPFL Energia** e que necessite de Credenciais de Acesso para acessar um sistema ou recurso computacional da organização.

N.Documento:	Categoria:	Versão:	Aprovado por:	Data Publicação:	Página:
18933	Instrução	1.0	Emerson Cardoso	08/09/2021	2 de 19

 Confidencialidade	Tipo de Documento:	Procedimento
	Área de Aplicação:	Segurança da Informação
	Título do Documento:	Procedimento de Hardening para EndPoint

- **CITRIX:** A tecnologia do software de espaço de trabalho da Citrix cria uma forma simples, segura e mais eficiente de trabalhar, em qualquer lugar e em qualquer organização.

4. DOCUMENTOS DE REFERÊNCIA

- ABNT/ISO 27001-2013;
- ABNT/ISO 27002-2013;
- Política de Segurança da Informação do **Grupo CPFL Energia**;
- Norma de Classificação da Informação do **Grupo CPFL Energia**;
- Código de Ética e de Conduta Empresarial do **Grupo CPFL Energia**;
- Esta Norma é complementada pela Política, e demais Normas e Procedimentos do **Grupo CPFL Energia**.

5. RESPONSABILIDADES

• Diretoria de Tecnologia da Informação

Propor mecanismos e processos para restringir o acesso e monitorar o cumprimento das regras contidas neste documento, além disso implementar os controles tecnológicos e processos para manter controle e monitoração de toda a rede do **Grupo CPFL Energia**.

• Departamento de Segurança da Informação


- ✓ Prover e manter o sistema de guarda, criação e alteração das credenciais dos usuários;
- ✓ Bloquear ou desabilitar as credenciais após tentativas de troca de senhas sem sucesso, notificando o usuário e o setor responsável pelo Tratamento de Incidentes de Segurança da Informação;
- ✓ Reportar as irregularidades/incidentes detectados;
- ✓ Liberar o acesso de acordo com as normas previstas;
- ✓ Implementar sistemas de monitoramento nas estações de trabalho, servidores, correio eletrônico, conexões com a Internet, dispositivos móveis ou wireless e outros componentes da rede - a informação gerada por esses sistemas poderá ser utilizada para identificar usuários e respectivos acessos efetuados, bem como o material que foi manipulado;
- ✓ Instalar sistemas de proteção, prevenção e detecção, para garantir a segurança das informações e dos perímetros de acesso.

6. REGRAS BÁSICAS

Para configurações gerais no sistema, os métodos de proteção introduzidos são os mesmos usados para servidores usuais baseados em SO Windows.

Público-alvo

N.Documento:	Categoria:	Versão:	Aprovado por:	Data Publicação:	Página:
18933	Instrução	1.0	Emerson Cardoso	08/09/2021	3 de 19

 Confidencialida	Tipo de Documento:	Procedimento
	Área de Aplicação:	Segurança da Informação
	Título do Documento:	Procedimento de Hardening para EndPoint

Todos os funcionários e Prestadores de Serviço do **Grupo CPFL Energia**, que façam uso de dispositivos que não são de propriedade do Grupo, e que tenham acesso a informações e/ou sistemas do Grupo.

6.1 Microsoft Windows Defender

O Microsoft Defender Antivírus é um componente importante da sua proteção da próxima geração no Microsoft Defender para Ponto de Extremidade. Essa proteção reúne o aprendizado de máquina, análise de big data, pesquisa aprofundada de resistência a ameaças e a infraestrutura de nuvem da Microsoft para proteger dispositivos (ou pontos de extremidade) em sua organização. O Microsoft Defender Antivírus está integrado ao Windows, e funciona com o Microsoft Defender para Ponto de Extremidade para fornecer proteção ao seu dispositivo e na nuvem.

6.1.1 Compatibilidade com outros produtos antivírus

Se estiver usando, em seu dispositivo, um produto antivírus/antimalware que não seja da Microsoft, você poderá executar o Microsoft Defender Antivírus no modo passivo junto com a solução de antivírus que não seja da Microsoft. Depende do sistema operacional utilizado e se seu dispositivo está integrado ao Defender para Ponto de extremidade.

6.1.2 Comparando o modo ativo, modo passivo e modo desabilitado

6.1.2.1 Modo ativo

No modo ativo, o Microsoft Defender Antivírus é usado como o principal aplicativo antivírus no dispositivo. Os arquivos são verificados, as ameaças são corrigidas e as ameaças detectadas são listadas nos relatórios de segurança da sua organização e no seu aplicativo de Segurança do Windows.


6.1.2.2 Modo passivo

No modo passivo, o Microsoft Defender Antivírus não é usado como o principal aplicativo antivírus no dispositivo. Os arquivos são verificados e as ameaças detectadas são relatadas, mas as ameaças não são corrigidas pelo Microsoft Defender Antivírus.

6.1.2.2 Desativado ou desinstalado

Quando desabilitado ou desinstalado, o Microsoft Defender Antivírus não é utilizado. Os arquivos não são verificados e as ameaças não são corrigidas. Em geral, não recomendamos desativar ou desinstalar o Microsoft Defender Antivírus.

N.Documento:	Categoria:	Versão:	Aprovado por:	Data Publicação:	Página:
18933	Instrução	1.0	Emerson Cardoso	08/09/2021	4 de 19

 Confidencialida	Tipo de Documento:	Procedimento
	Área de Aplicação:	Segurança da Informação
	Título do Documento:	Procedimento de Hardening para EndPoint


6.1.3 Verifique o estado do Microsoft Defender Antivírus no seu dispositivo

Use o aplicativo de Segurança do Windows para verificar o status do Microsoft Defender Antivírus

1. Em seu dispositivo Windows, selecione o menu Iniciar e comece a digitar Security. Em seguida, abra o aplicativo de Segurança do Windows nos resultados.
2. Select **Proteção contra vírus e ameaças**.
3. Em **Configurações de proteção contra vírus e ameaças**, escolha **Gerenciar configurações**.

Você verá o nome de sua solução de antivírus/antimalware na página de configurações.

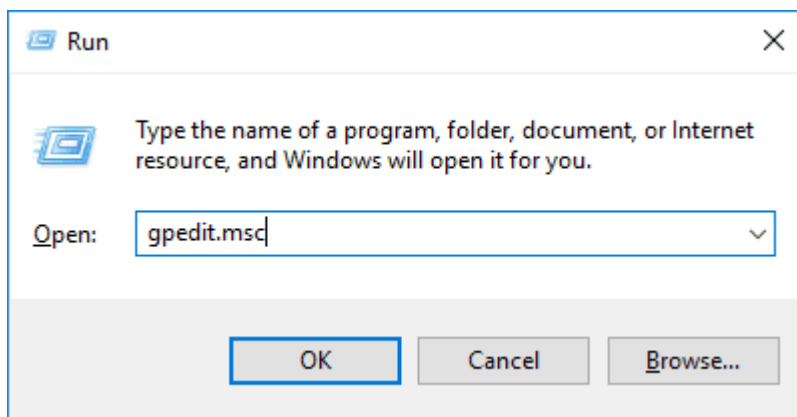
N.Documento:	Categoria:	Versão:	Aprovado por:	Data Publicação:	Página:
18933	Instrução	1.0	Emerson Cardoso	08/09/2021	5 de 19

 Confidencialida	Tipo de Documento:	Procedimento
	Área de Aplicação:	Segurança da Informação
	Título do Documento:	Procedimento de Hardening para EndPoint

6.1.4 Aumentando os níveis de proteção

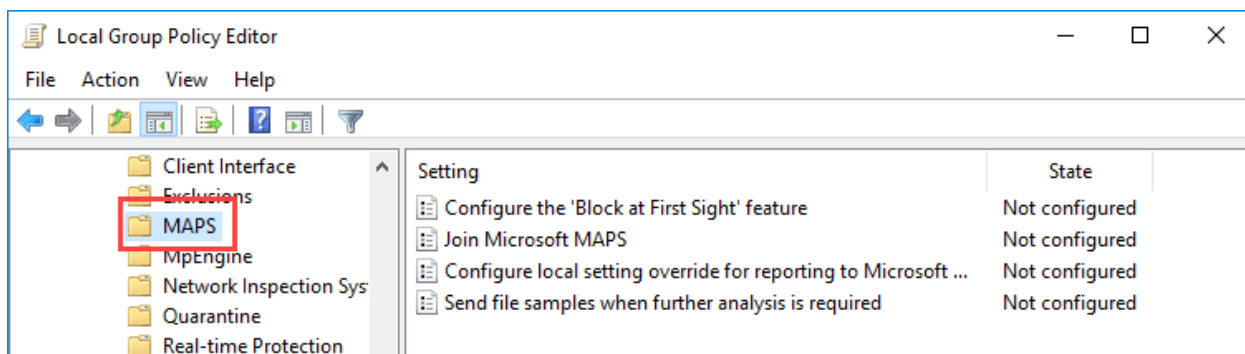
Use o editor de política de grupo

O Editor de Diretiva de Grupo oferece uma maneira fácil e direta de aprimorar o Windows Defender. Para abrir o editor de política de grupo, pressione **Win + R**, Tipo **gpedit.msc** E pressione **Enter**.



No "Editor de política de grupo", vá para:


Computer Configuration -> Administrative Templates -> Windows Components -> Windows Defender Antivirus -> MAPS.



No painel direito, você verá quatro políticas diferentes. Configure-o conforme mostrado abaixo, de acordo com a ordem em que foram apresentados.

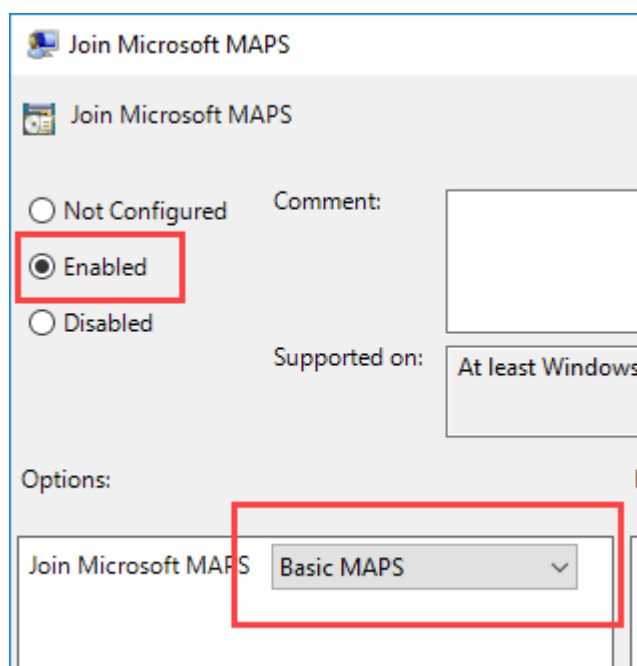
Junte-se ao Microsoft MAPS: A primeira coisa que você precisa fazer é ingressar no programa Microsoft (Programa de Proteção Avançada da Microsoft). O MAPS é uma

N.Documento:	Categoria:	Versão:	Aprovado por:	Data Publicação:	Página:
18933	Instrução	1.0	Emerson Cardoso	08/09/2021	6 de 19

 Confidencialida	Tipo de Documento:	Procedimento
	Área de Aplicação:	Segurança da Informação
	Título do Documento:	Procedimento de Hardening para EndPoint


comunidade online que visa detectar rapidamente ameaças menos conhecidas e pode até mesmo impedir novas ameaças maliciosas.

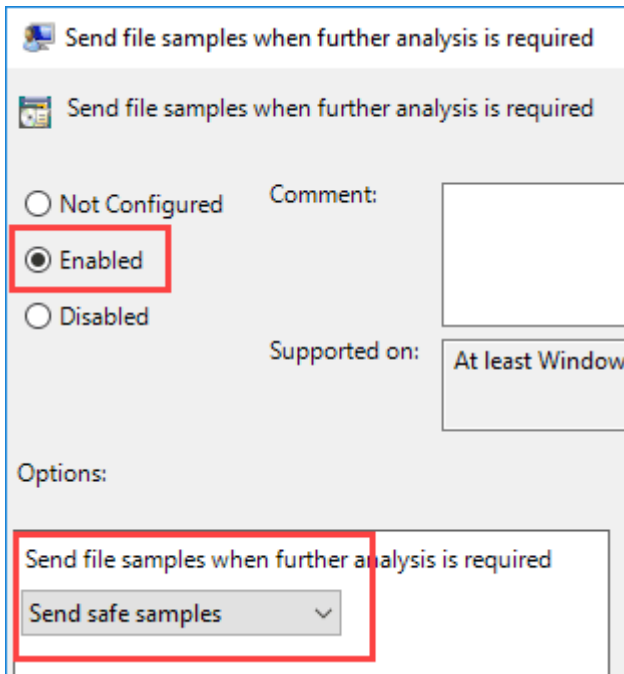
Clique duas vezes nesta política e selecione o botão de opção "**Talvez**, Selecione um **MAPS básico**" Ou" **MAPS avançado**. No menu suspenso e clique no botão "**ESTÁ BEM**" Para salvar as alterações. Você pode encontrar a diferença entre as opções Básicas e Avançadas na seção Ajuda que aparece no painel direito.



Envie amostras de arquivos quando uma análise adicional for necessária: Para que o MAPS funcione corretamente, você precisa fornecer amostras de arquivos para que possam ser verificados e verificados com os dados fornecidos pela comunidade online. Abra a política e selecione a opção "**Talvez**". Na seção de opções, você pode escolher entre três opções: **enviar amostras seguras**, **enviar todas as amostras**, E as **sempre alerta**.

Se você selecionar a quarta opção, **Nunca envie** "Esta primeira política e cena não funcionarão". Selecione uma das três opções discutidas acima e clique no botão "**ESTÁ BEM**" Para salvar as alterações. No meu caso, escolho a opção "**Envie amostras com segurança**" No menu suspenso.

 Confidencialida	Tipo de Documento:	Procedimento
	Área de Aplicação:	Segurança da Informação
	Título do Documento:	Procedimento de Hardening para EndPoint



Send file samples when further analysis is required

Send file samples when further analysis is required

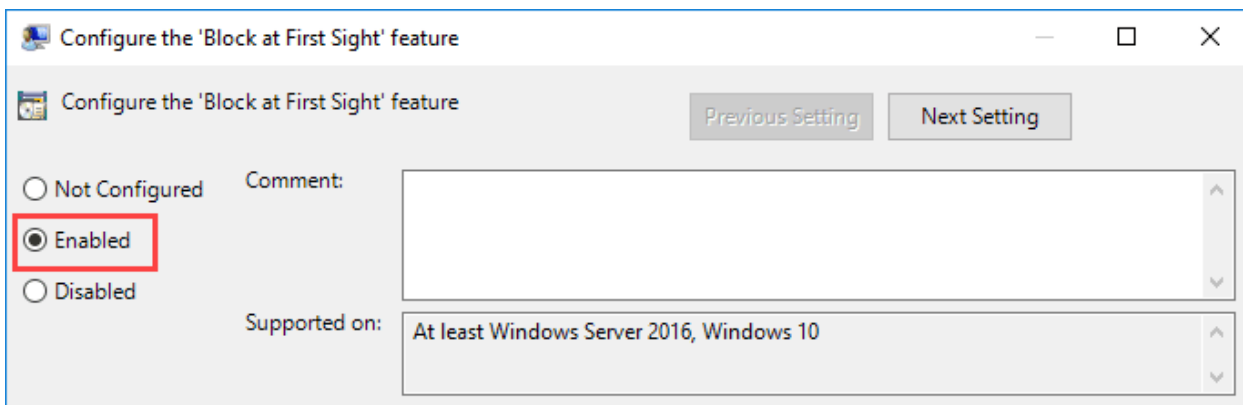
☐ Not Configured Comment:
☒ **Enabled**
☐ Disabled

Supported on:

Options:

Send file samples when further analysis is required

Configure o recurso "Block at First Sight": Esse recurso permite o monitoramento do MAPS em tempo real e gerência apenas conteúdo específico após a digitalização com o MAPS. Para habilitar este recurso, abra a política e selecione **"Talvez"** E clique no botão **"ESTÁ BEM"** Para salvar as alterações.



Configure the 'Block at First Sight' feature

Configure the 'Block at First Sight' feature


Previous Setting Next Setting

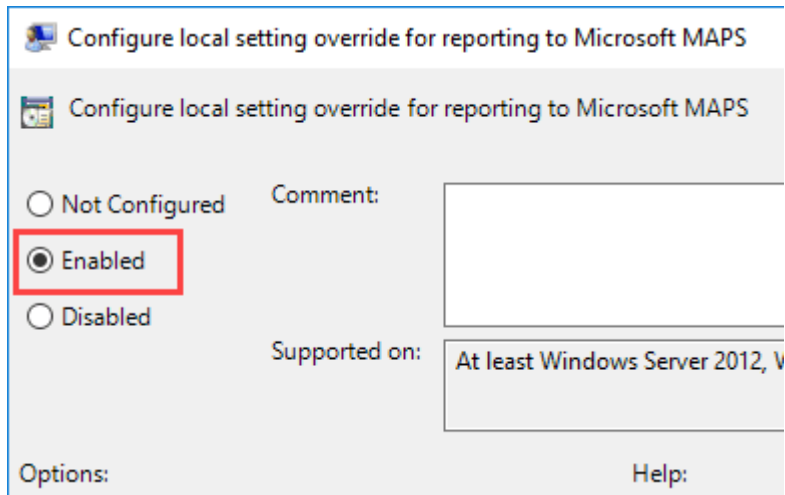
☐ Not Configured Comment:
☒ **Enabled**
☐ Disabled

Supported on:

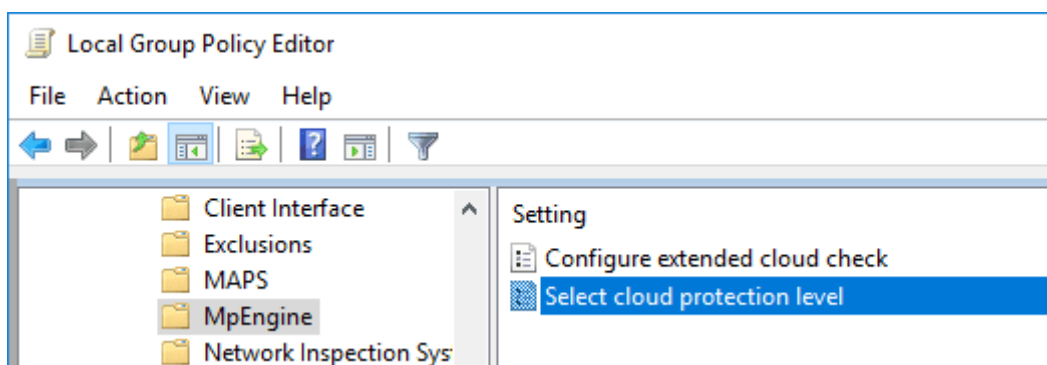
Defina a substituição das configurações locais para relatar ao Microsoft MAPS: Essa configuração garante que a prioridade local terá precedência sobre a política de grupo. Para habilitar este recurso, abra a política e selecione o botão de opção **"Talvez"** E clique no botão **"ESTÁ BEM"** Para salvar as alterações.

N.Documento:	Categoria:	Versão:	Aprovado por:	Data Publicação:	Página:
18933	Instrução	1.0	Emerson Cardoso	08/09/2021	8 de 19

 Confidencialida	Tipo de Documento:	Procedimento
	Área de Aplicação:	Segurança da Informação
	Título do Documento:	Procedimento de Hardening para EndPoint

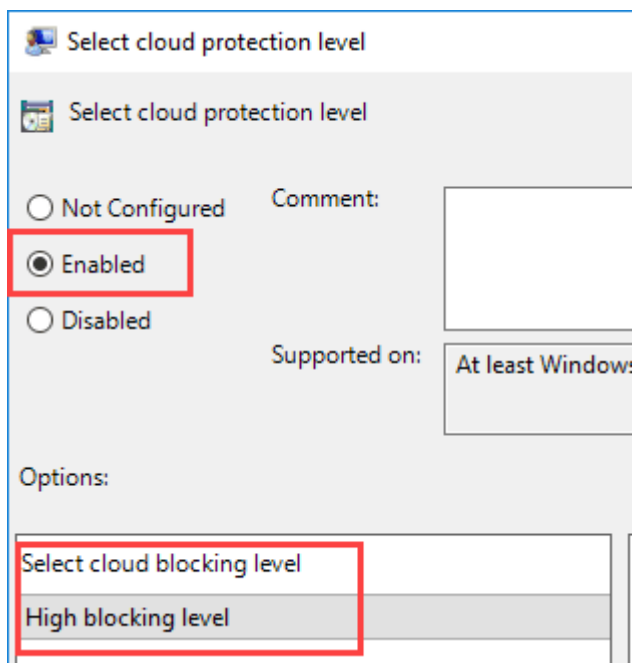


Para tornar as coisas um pouco mais seguras, você pode ajustar as configurações do Cloud Protection. No painel esquerdo, selecione a pasta "**MpEngine**". No painel direito, clique duas vezes na política. **Selecione o nível de proteção na nuvem.** "




Na janela Configurações de política, selecione o botão de opção "**Talvez**", Em seguida, selecione a opção "**Alto nível de bloqueio**" No menu suspenso da seção "**Opções.**" Clique "**ESTÁ BEM**" Para salvar as alterações.

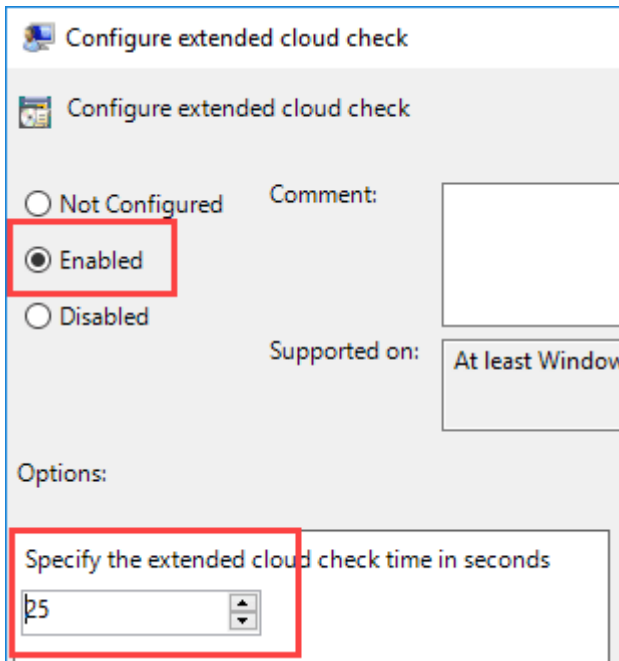
N.Documento:	Categoria:	Versão:	Aprovado por:	Data Publicação:	Página:
18933	Instrução	1.0	Emerson Cardoso	08/09/2021	9 de 19



De modo geral, o Windows Defender bloqueia qualquer arquivo suspeito e verifica-o na nuvem. Por padrão, o tempo limite é definido como dez segundos. Se desejar, você pode estender o limite de tempo para até sessenta segundos.

Para fazer isso, abra a política “**Configurar verificação de nuvem estendida**”, Selecione o botão de opção “**Talvez**” Em seguida, insira o número de segundos na seção Opções. Você pode estender o tempo para cinquenta segundos. Mesmo se você inserir mais de cinquenta segundos, o tempo progressivo total da varredura na nuvem será de sessenta segundos, junto com o padrão de dez segundos.

 Confidencialidade	Tipo de Documento:	Procedimento
	Área de Aplicação:	Segurança da Informação
	Título do Documento:	Procedimento de Hardening para EndPoint



Configure extended cloud check

☐ Not Configured Comment:
☒ Enabled
☐ Disabled


Supported on:

Options:

Specify the extended cloud check time in seconds

É isso, uma vez que você tenha que reiniciar seu sistema.
Use o Editor de registro do Windows

Se você for um usuário do Windows comum, não terá acesso ao "Editor de Política de Grupo", mas poderá usar o "Registro do Windows" para obter o mesmo resultado. Onde você precisava gerar várias chaves e alguns valores, mas eu fiz o trabalho para você. Tudo que você precisa fazer é mesclar esses valores com o registro do Windows. Você deve baixar o arquivo zip daqui e extraí-lo em seu desktop.

 Confidencialida	Tipo de Documento:	Procedimento
	Área de Aplicação:	Segurança da Informação
	Título do Documento:	Procedimento de Hardening para EndPoint

Você deve ter dois arquivos: **MPEngine Key.reg** E a **"Spynet Key.reg**. Seu conteúdo é o seguinte.

MPEngine Key.reg:

Windows Registry Editor Version 5.00

[HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows Defender\MpEngine]

"MpBafsExtendedTimeout"=dword:00000019

"MpCloudBlockLevel"=dword:00000002

- Spynet Key.reg:

Windows Registry Editor Version 5.00

[HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows Defender\Spynet]

"DisableBlockAtFirstSeen"=dword:00000000


"SpynetReporting"=dword:00000002

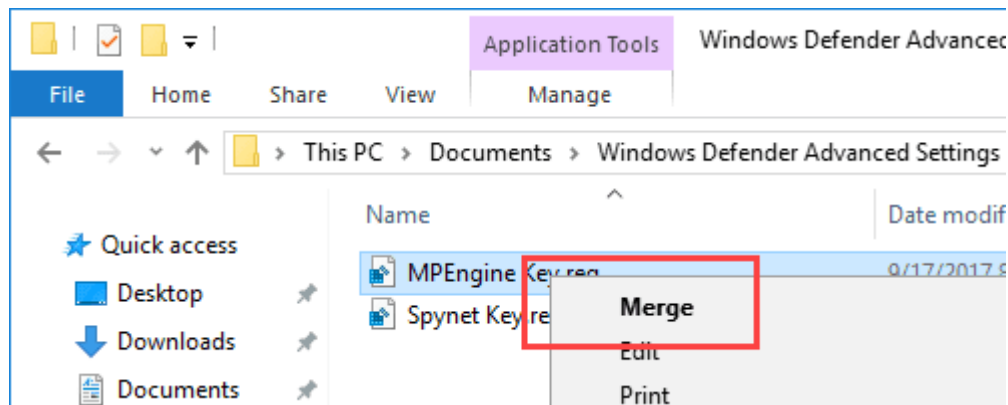
"LocalSettingOverrideSpynetReporting"=dword:00000001

"SubmitSamplesConsent"=dword:00000001

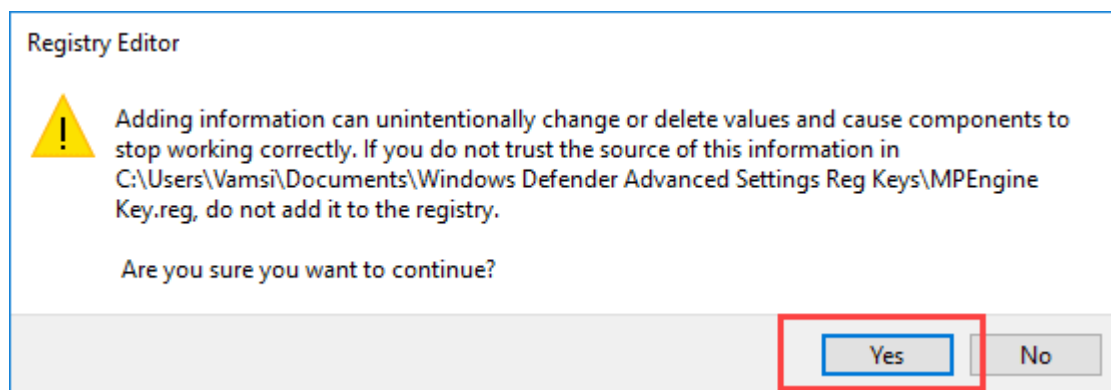
Clique com o botão direito no arquivo **reg** E selecione a opção **"Unir"**.

N.Documento:	Categoria:	Versão:	Aprovado por:	Data Publicação:	Página:
18933	Instrução	1.0	Emerson Cardoso	08/09/2021	12 de 19

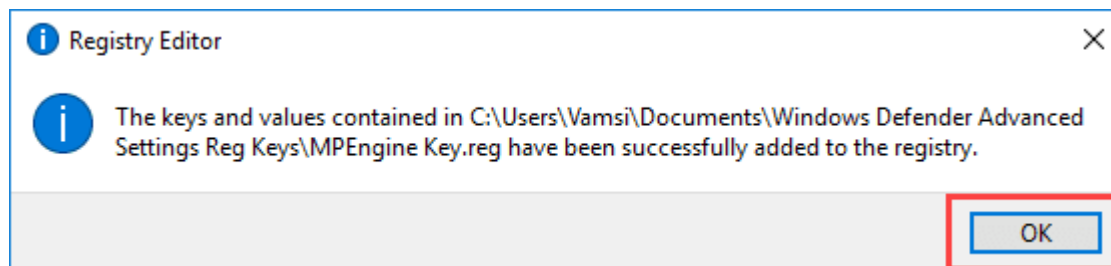
 Confidencialida	Tipo de Documento:	Procedimento
	Área de Aplicação:	Segurança da Informação
	Título do Documento:	Procedimento de Hardening para EndPoint




Você receberá uma mensagem de aviso. Clique no botão **"Sim"** seguir.



O procedimento acima irá mesclar o **reg** Especificado com seu registro. Faça o mesmo para o segundo arquivo de log.



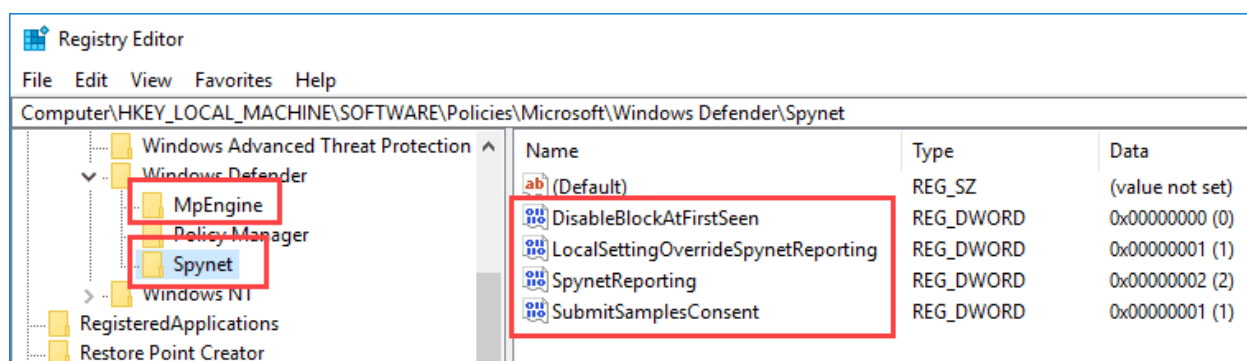
N.Documento:	Categoria:	Versão:	Aprovado por:	Data Publicação:	Página:
18933	Instrução	1.0	Emerson Cardoso	08/09/2021	13 de 19


 Confidencialidade	Tipo de Documento:	Procedimento
	Área de Aplicação:	Segurança da Informação
	Título do Documento:	Procedimento de Hardening para EndPoint

Assim que a adição estiver concluída, você deve reiniciar o dispositivo. Se quiser ver quais valores e chaves foram adicionados ao Registro do Windows, abra o Editor do Registro e vá para o seguinte local:

HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows Defender

Aqui você pode ver os switches Spynet (MAPS) e MpEngine recém-criados. Ao selecionar as chaves, você pode ver os valores associados a essa chave.




 Confidencialida	Tipo de Documento:	Procedimento
	Área de Aplicação:	Segurança da Informação
	Título do Documento:	Procedimento de Hardening para EndPoint

6.1.5 Boas Práticas para o Microsoft Defender ATP

6.1.5.1 Ativar proteção contra adulteração

- ✓ Por quê? A primeira etapa em muitos ataques APT é usar um 'Dropper' para desabilitar o antivírus ou outras configurações de segurança por meio do registro, PowerShell, GPO, etc.
- ✓ Este é um recurso do Microsoft Defender que não requer o Windows 10 E5, mas se você tiver o E5, poderá aproveitar o Intune para evitar que o usuário desative esse recurso. A vantagem de exigir o Intune é que ele abstrai a capacidade de desabilitar antivírus para uma pilha de gerenciamento separada. Caso contrário, o invasor pode usar vários métodos para desativar o AV. Este recurso avançado requer Windows 10 ou superior.
- ✓ [Atualização de fevereiro de 2021] Este recurso agora pode ser habilitado globalmente nas configurações de recursos avançados do Defender for Endpoint. Agora, a única vez que você precisa usar o Endpoint Manager / Intune para controlar a proteção contra adulteração é se precisar de um controle mais granular por dispositivo / grupo.
- ✓ Usando perfis de dispositivo Intune:
- ✓ Crie um perfil que inclua as seguintes configurações:
- ✓ Plataforma: Windows 10 e posterior
- ✓ ProfileType: proteção de endpoint
- ✓ **Configurações> Central de Segurança do Windows Defender> Proteção contra adulteração**

N.Documento:	Categoria:	Versão:	Aprovado por:	Data Publicação:	Página:
18933	Instrução	1.0	Emerson Cardoso	08/09/2021	15 de 19

 Confidencialidade	Tipo de Documento:	Procedimento
	Área de Aplicação:	Segurança da Informação
	Título do Documento:	Procedimento de Hardening para EndPoint


6.1.5.2 Habilitar regras de redução da superfície de ataque (ASR)

- ✓ As regras ASR são um recurso do Windows 10 E3 e do Windows 10 E5. A versão E5 adiciona duas regras exclusivas que não estão disponíveis na versão E3.
- ✓ As regras ASR podem ser habilitadas sem o MDATP, mas o benefício de usar o MDATP é o relatório centralizado, caso contrário, as auditorias seriam descentralizadas no visualizador de eventos local.
- ✓ ASR Rules são marcadas como parte do “Microsoft Defender Exploit Guard”, que é uma série de recursos de segurança do Windows 10, incluindo Acesso Controlado a Pasta, Proteção Exploit e Proteção de Rede.
- ✓ Algumas das regras ASR exigem que a proteção fornecida pela nuvem seja ativada.
- ✓ A regra ASR "Executáveis que não atendem a critérios de prevalência, idade ou lista confiável" examina .exe, .dll, .scr para determinar se eles estão em uma lista de permissões mantida pela MSFT e não há como adicionar exclusões, portanto, recomendamos definir esta regra para o modo de auditoria.
- ✓ No Intune, navegue até Configuração **do dispositivo - Perfis > Nome do perfil > Endpoint Protection > Microsoft Defender Exploit Guard > Redução da superfície de ataque**.

6.1.5.3 Habilite “Bloquear no primeiro site”

- ✓ Esta é uma série de itens de configuração que enviam um novo executável ou script para a nuvem. Bloquear à primeira vista usa apenas o back-end de proteção em nuvem para arquivos executáveis e arquivos executáveis não portáteis que são baixados da Internet ou originados da zona da Internet.
- ✓ Você pode configurar isso usando Intune, SCCM ou Política de Grupo.
- ✓ No Intune, navegue até Configuração **do dispositivo - Perfis > Nome do perfil > Restrições do dispositivo > Antivírus do Windows Defender**.
 - Proteção fornecida pela nuvem: Ativar
 - Nível de bloqueio de arquivo: alto
 - Extensão de tempo para verificação de arquivos pela nuvem: 50
 - Avisar os usuários antes do envio da amostra: Envie todos os dados sem avisar
 - Enviar amostras de consentimento: Enviar todas as amostras automaticamente.

N.Documento:	Categoria:	Versão:	Aprovado por:	Data Publicação:	Página:
18933	Instrução	1.0	Emerson Cardoso	08/09/2021	16 de 19

 Confidencialidade	Tipo de Documento:	Procedimento
	Área de Aplicação:	Segurança da Informação
	Título do Documento:	Procedimento de Hardening para EndPoint

6.1.5.4 Ativar o compartilhamento de amostra MDATP para todos os arquivos

- ✓ **No Intune, navegue até Configuração** do dispositivo - Perfis> **Nome do perfil** > Microsoft Defender ATP (Windows 10)> Compartilhamento de amostra para todos os arquivos> Ativar
- ✓ **No Intune, navegue até Configuração** do dispositivo - Perfis> **Nome do perfil** > Microsoft Defender ATP (Windows 10)> Acelerar frequência de relatórios de telemetria> Ativar

6.1.5.5 Habilitar investigação e correção automáticas MDATP

- ✓ Crie um Grupo de Funções em Configurações de MDATP> Permissões> Funções (selecione um grupo)
- ✓ Crie um grupo de máquinas MDATP, defina-o para todas as máquinas e atribua-o como Completo - Corrija ameaças automaticamente
- ✓ Habilite a investigação automatizada em Configurações de MDATP> Recursos avançados
- ✓ Habilite * todas * as Configurações do MDATP> Recursos avançados (ou tantos quantos você estiver licenciado, por exemplo: Azure ATP, Intune, MCAS, etc).


6.1.5.6 Bloquear cancelamento manual do Intune

- ✓ No Intune, navegue até Configuração **do dispositivo - Perfis> Nome do perfil** > **Restrições do dispositivo> Geral> Cancelamento manual do registro> Bloquear**
- ✓ No Intune, navegue até Configuração **do dispositivo - Perfis> Nome do perfil** > **Restrições do dispositivo> Geral> Acesso direto à memória> Ativado**

6.1.5.7 Habilitar proteção de rede

- ✓ A proteção de rede expande o escopo do Windows Defender SmartScreen para bloquear todo o tráfego HTTP (s) de saída que tenta se conectar a fontes de baixa reputação (com base no domínio ou nome do host).
- ✓ A Proteção de Rede é marcada como parte do “Microsoft Defender Exploit Guard”, que é uma série de recursos de segurança do Windows 10, incluindo Acesso Controlado a Pasta, Proteção de Exploit e regras ASR.
- ✓ A proteção de rede pode ser habilitada sem MDATP, mas o benefício de usar MDATP é o relatório centralizado, caso contrário, as auditorias seriam descentralizadas no visualizador de eventos local.

N.Documento:	Categoria:	Versão:	Aprovado por:	Data Publicação:	Página:
18933	Instrução	1.0	Emerson Cardoso	08/09/2021	17 de 19

 Confidencialida	Tipo de Documento:	Procedimento
	Área de Aplicação:	Segurança da Informação
	Título do Documento:	Procedimento de Hardening para EndPoint

- ✓ No Intune, navegue até Configuração **do dispositivo - Perfis> Nome do perfil > Proteção de endpoint> Microsoft Defender Exploit Guard> Filtragem de rede> Proteção de rede.**

6.1.5.8 Habilitar SmartScreen

- ✓ Já integrado ao Microsoft Edge (e Chromium-Edge)
- ✓ “Proteção do navegador do Windows Defender” está disponível como um suplemento para o Chrome


6.1.5.9 Ative o modo de bloco EDR.

- Originalmente, presumia-se que esse recurso só era aplicável quando o Defender estava no modo passivo atrás de outro cliente AV. Embora esse seja o caso de uso principal para o modo Bloco EDR, a documentação da Microsoft recomenda habilitar esse recurso mesmo quando o Defender está no modo Ativo.
- “Recomendamos manter o EDR no modo de bloqueio, quer o Microsoft Defender Antivirus esteja sendo executado no modo passivo ou no modo ativo. O EDR no modo de bloqueio fornece outra camada de defesa com o Microsoft Defender para Endpoint. Ele permite que o Defender for Endpoint execute ações com base nas detecções de EDR comportamentais pós-violação”.

6.1.5.10 Bloquear macros (config.office.com)

- ✓ Desative a notificação da barra de confiança para suplementos de aplicativos não assinados e bloqueie-os
- ✓ Desative todas as notificações da Barra de confiança para problemas de segurança
- ✓ Configurações de notificação de macro VBA: Habilite com "Desativar sem notificação"
- ✓ Desativar VBA para aplicativos do Office
- ✓ Bloqueia a execução de macros em arquivos do Office da Internet
 - Para evitar problemas com usuários que precisam de macros válidas / confiáveis, você pode habilitar duas configurações adicionais:
 - Permitir locais confiáveis na rede
 - Bloqueie as permissões NTFS e / ou de compartilhamento para permitir que apenas usuários autorizados (administradores?) Adicionem macros a este caminho (peça a cada departamento para fornecer macros para revisão)

N.Documento:	Categoria:	Versão:	Aprovado por:	Data Publicação:	Página:
18933	Instrução	1.0	Emerson Cardoso	08/09/2021	18 de 19

 Confidencialida	Tipo de Documento:	Procedimento
	Área de Aplicação:	Segurança da Informação
	Título do Documento:	Procedimento de Hardening para EndPoint

- Local confiável nº 1 (a nº 20)
- É aqui que você pode especificar o caminho de rede de onde as macros autorizadas podem ser executadas

7 CONTROLE DE REGISTROS

Identificação	Armazenamento e Preservação	Proteção (acesso)	Recuperação e uso	Retenção	Disposição
Norma de SI	Eletrônico (GED)	Restrição de acesso	Por tema ou título	Até a próxima atualização do documento	Substituição

8 ANEXOS

Listas mencionadas nos itens 6.2 e 6.3;

9 REGISTRO DE ALTERAÇÕES

9.1 Colaboradores

Empresa	Área	Nome
NAVA	Segurança da Informação	Mateus Rocha

9.2 Alterações

Versão Anterior	Data da Versão Anterior	Alterações em relação à Versão Anterior
Não Aplicável	Não Aplicável	Documento em versão inicial