

Configurar atualizações automáticas para o banco de dados de vulnerabilidades no FMC

Contents

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Configurar](#)

[Configurações](#)

[Verificar](#)

[Exibindo tarefas agendadas no calendário](#)

[Procedimento](#)

[Troubleshooting](#)

[Informações Relacionadas](#)

Introdução

Este documento descreve como configurar as Atualizações Automáticas para o Banco de Dados de Vulnerabilidade (VDB) no FMC.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Firepower Threat Defense (FTD)
- Firepower Management Center (FMC)
- Banco de dados de vulnerabilidade (VDB)

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

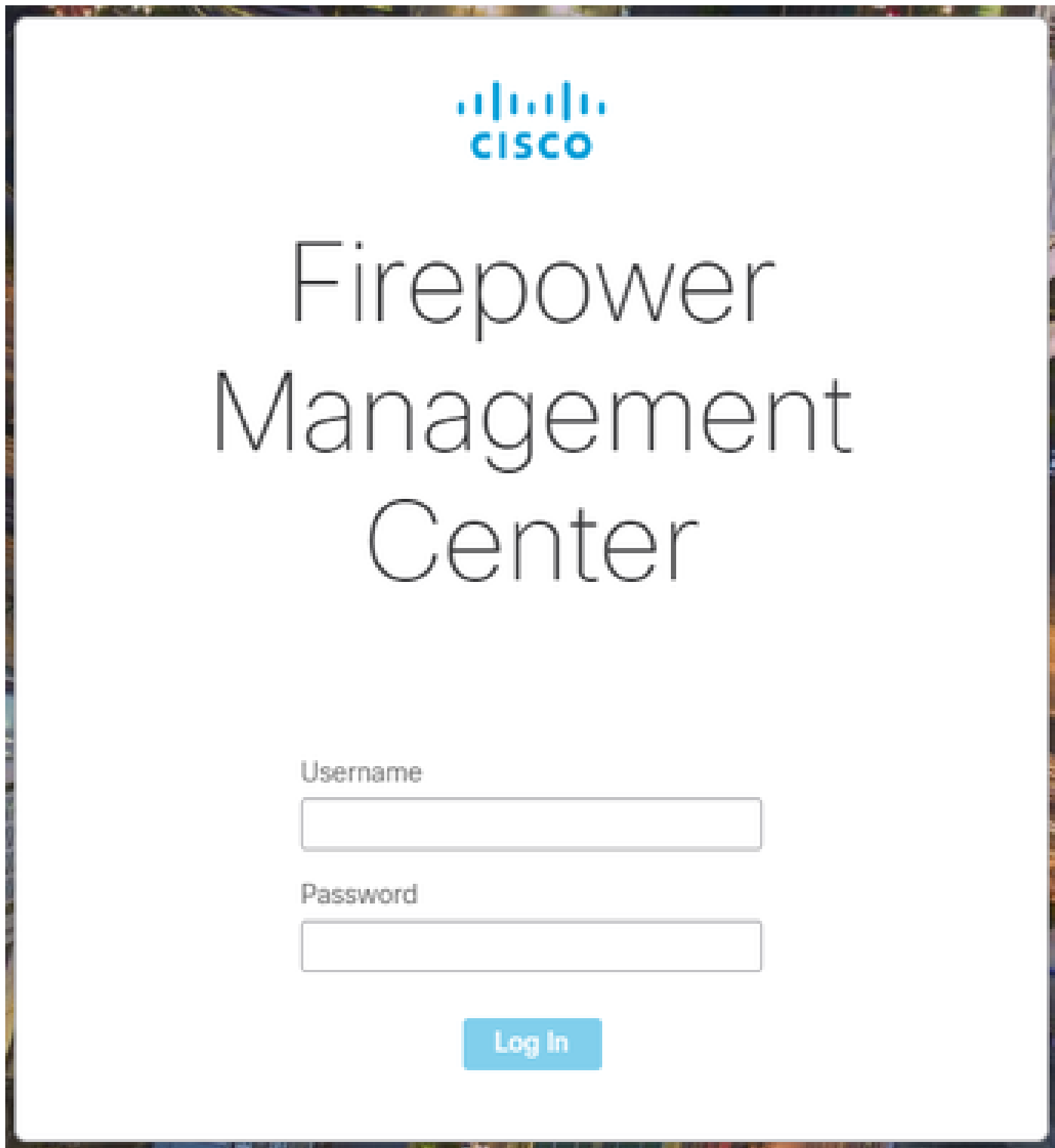
- FMC 7.0
- FTD 7.0

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Configurar

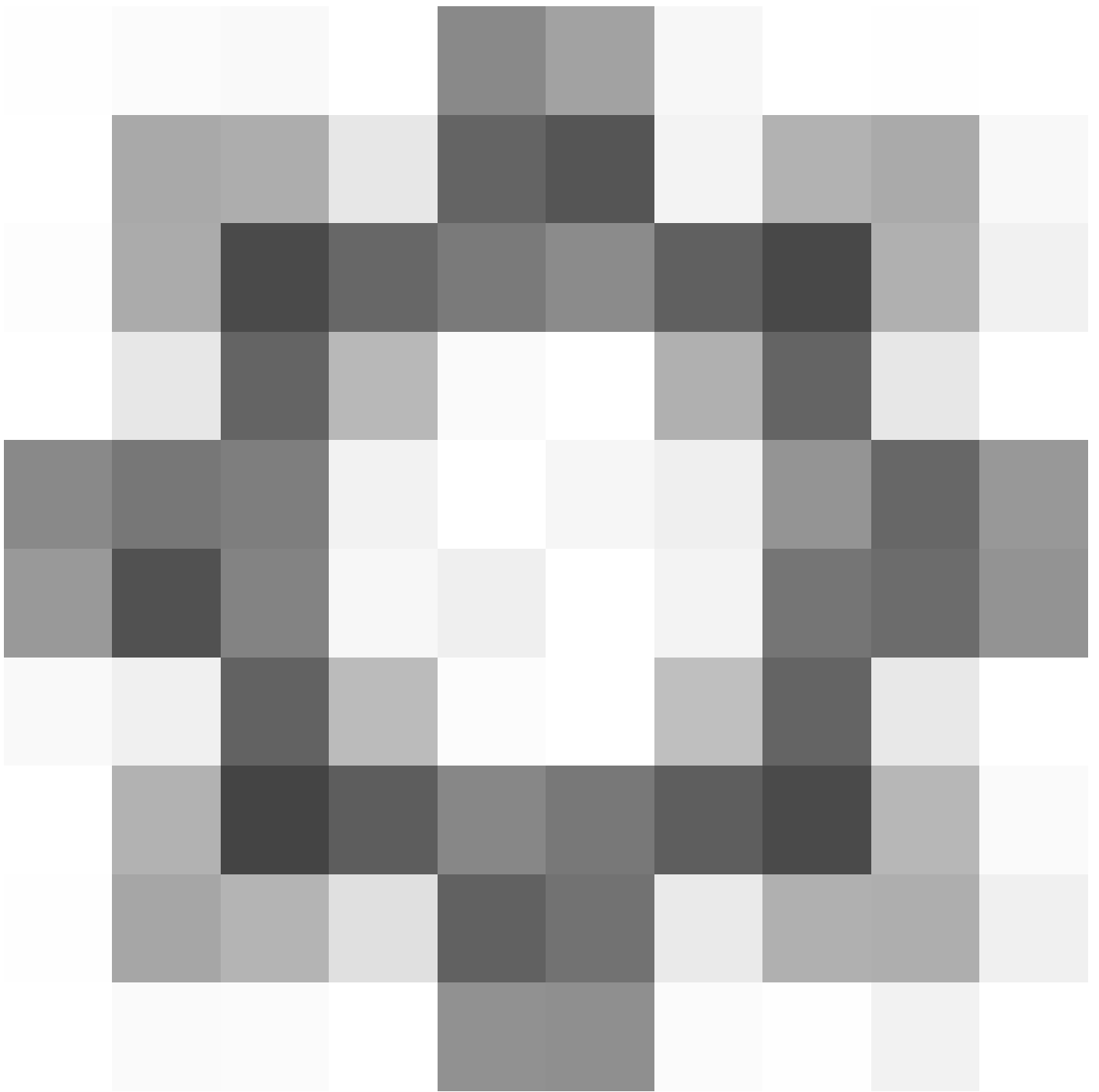
Configurações

1. Faça login no Firepower Management Center.

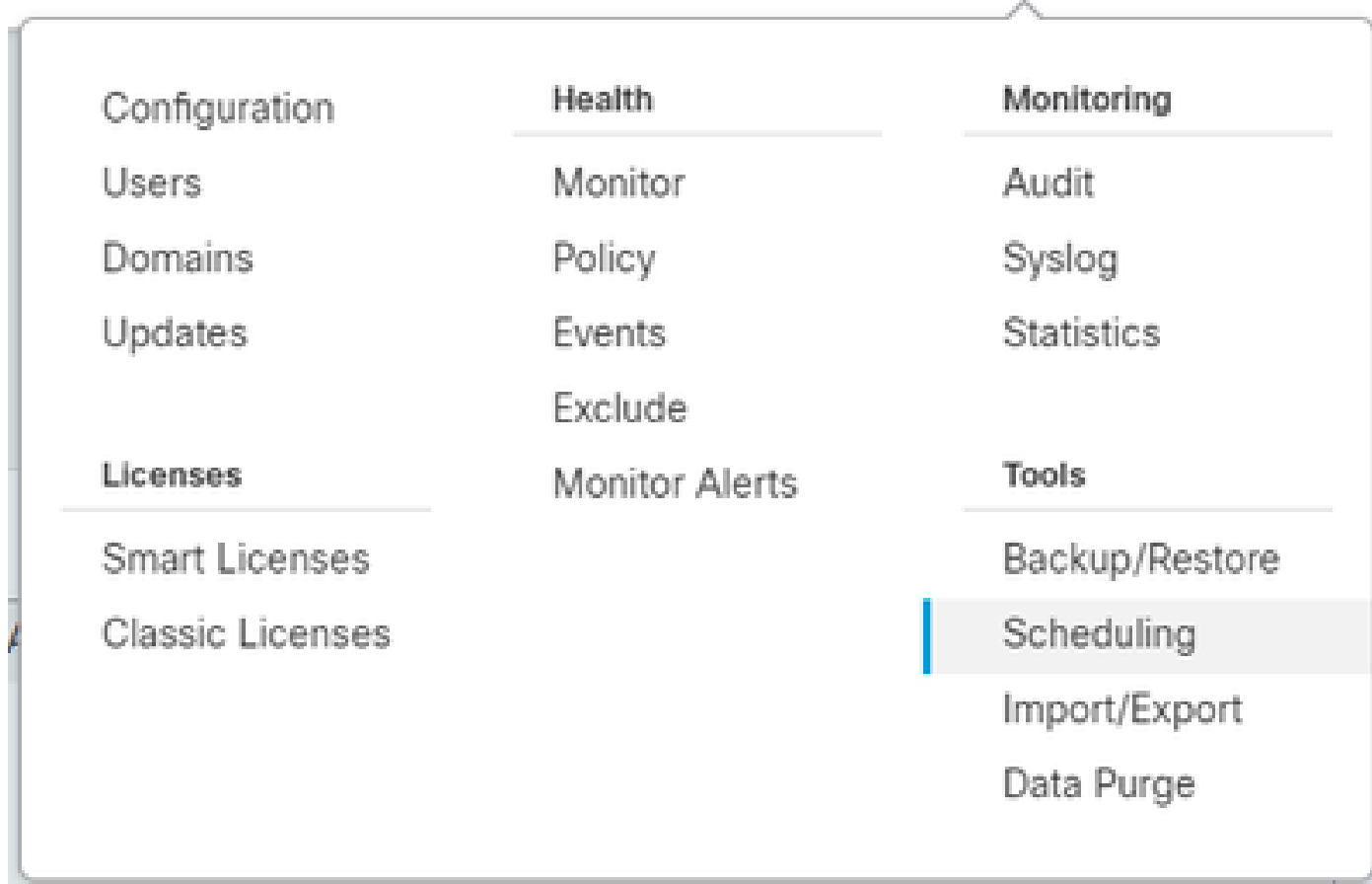


The screenshot shows the login interface for the Cisco Firepower Management Center. At the top center is the Cisco logo, consisting of a stylized bridge icon above the word "CISCO" in blue. Below the logo, the text "Firepower Management Center" is displayed in a large, grey, sans-serif font. Underneath the title, there are two input fields: the first is labeled "Username" and the second is labeled "Password". Both fields are empty and have a thin grey border. At the bottom center of the form is a blue button with the text "Log In" in white.

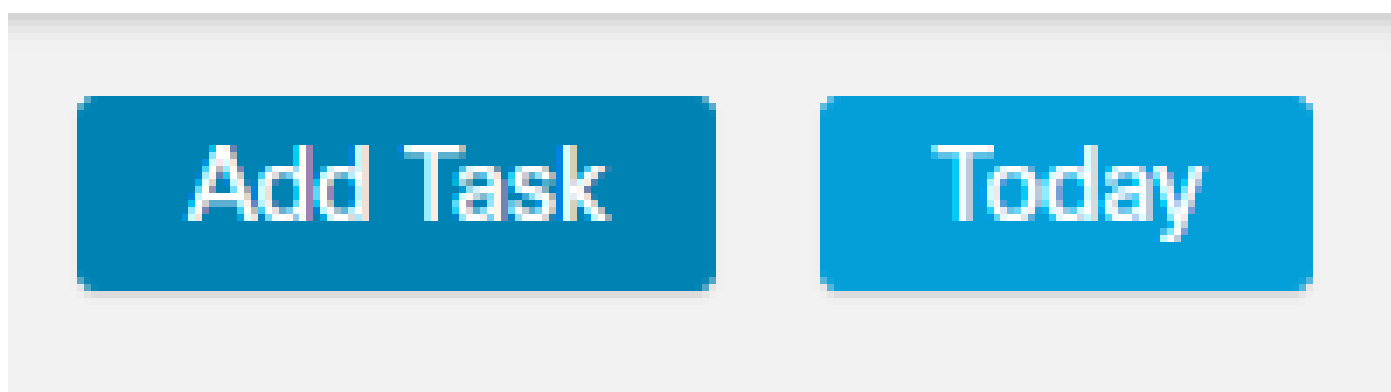
2. Navegue até Sistema(



)> Programação.



3. No canto superior direito da tela Agendamento, clique no botão Adicionar Tarefa.



4. Na tela Nova Tarefa, selecione Baixar Última Atualização no menu suspenso Tipo de Job e selecione as configurações de acordo com suas necessidades.

Na tarefa Agendar a ser executada, selecione Recorrente.

Na seção Atualizar itens, selecione Banco de dados de vulnerabilidade.

Em seguida, clique em Salvar.

New Task

Job Type

Schedule task to run Once Recurring

Start On

Repeat Every Hours Days Weeks Months

Run At

Repeat On Sunday Monday Tuesday Wednesday Thursday Friday Saturday

Job Name

Update Items Software Vulnerability Database

Comment

Email Status To Not available. You must set up your mail relay host.

5. Repita a Etapa 3 para voltar à tela Nova Tarefa e selecione Instalar Atualização Mais Recente no menu suspenso Tipo de Job e use as configurações para atender às suas necessidades e clique em Salvar.

New Task

Job Type

Schedule task to run Once Recurring

Start On

Repeat Every Hours Days Weeks Months

Run At

Repeat On Sunday Monday Tuesday Wednesday Thursday Friday Saturday

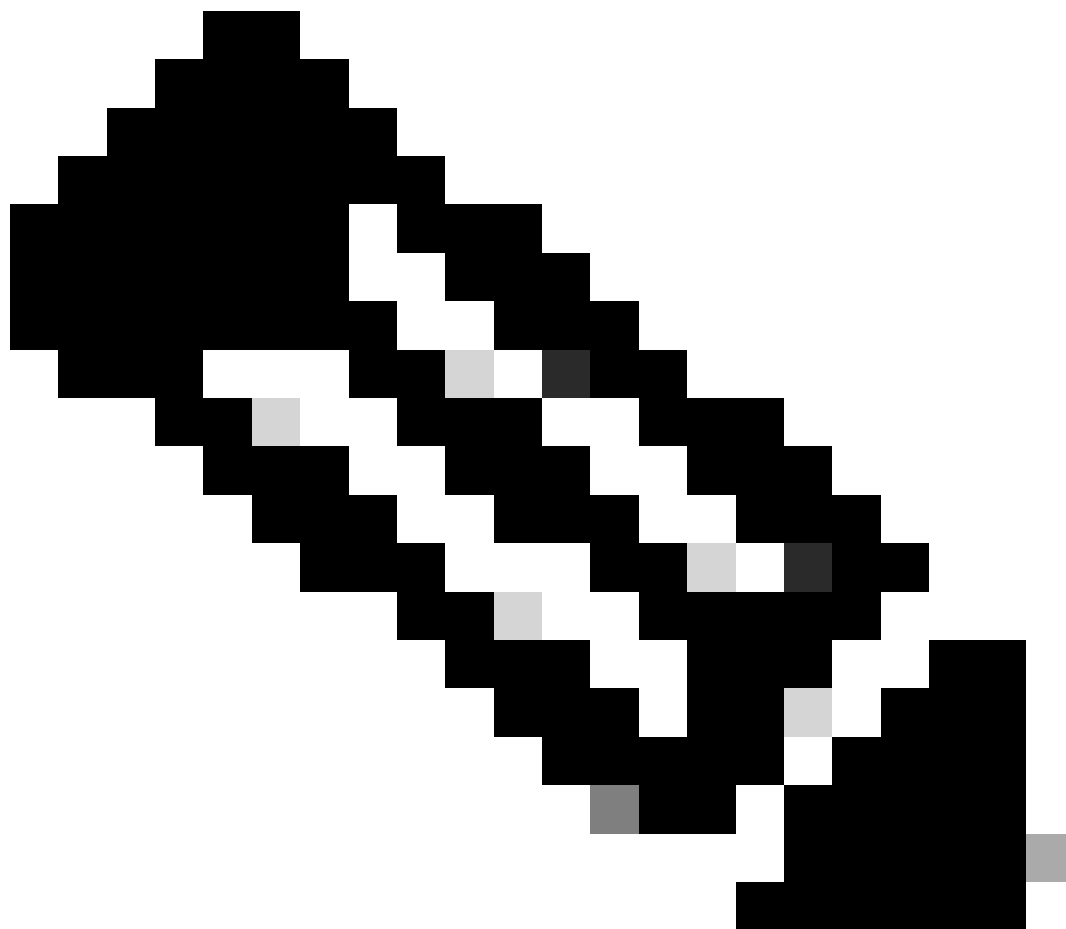
Job Name

Update Items Software Vulnerability Database

Device

Comment

Email Status To Not available. You must set up your mail relay host.



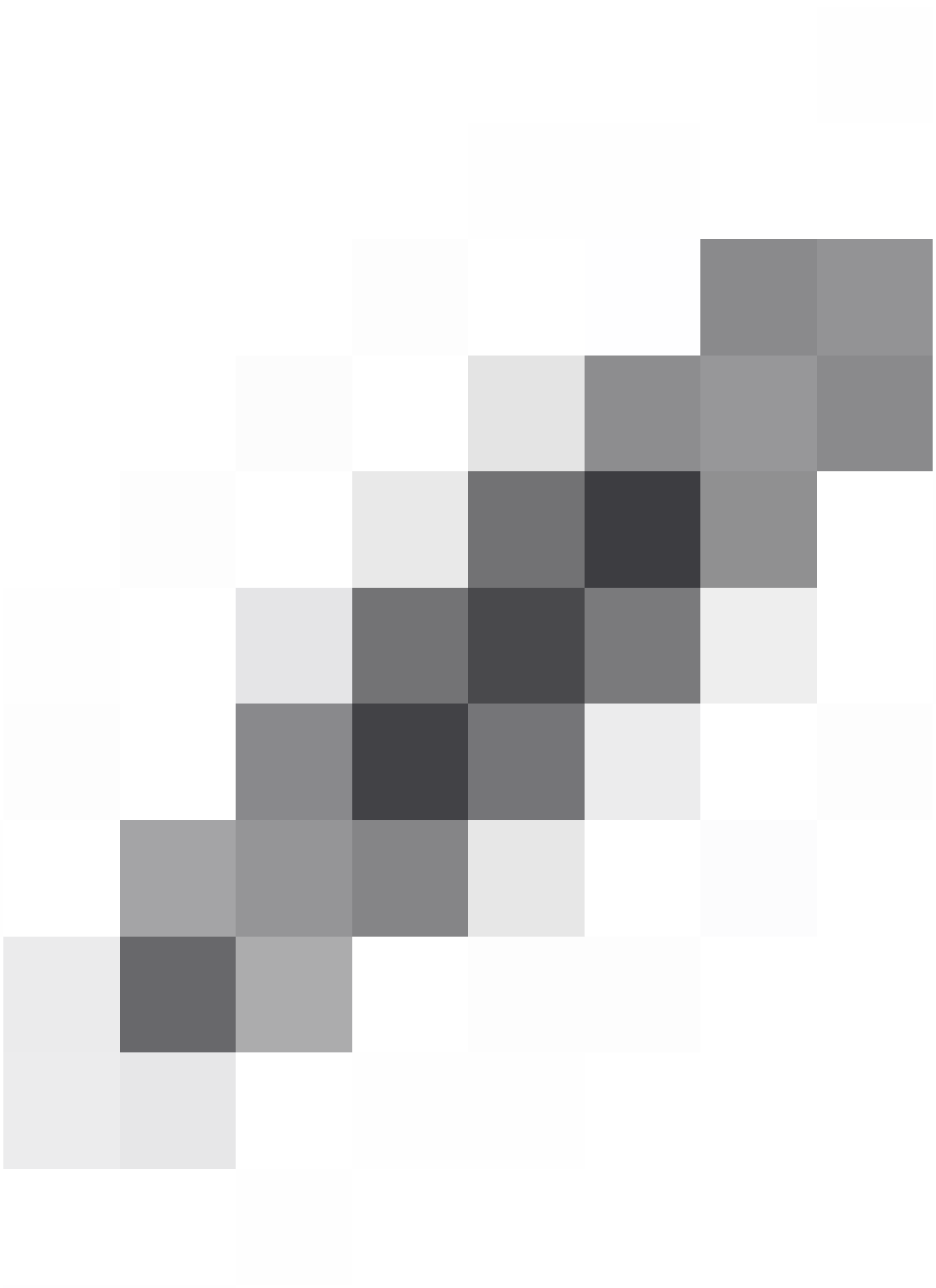
Observação: lembre-se de que, após a atualização do VDB, você também deve implantar alterações de configuração que possam interromper a inspeção e o fluxo do tráfego.

Warning

After you update the VDB, you must also deploy configuration changes, which might interrupt traffic inspection and flow.

OK

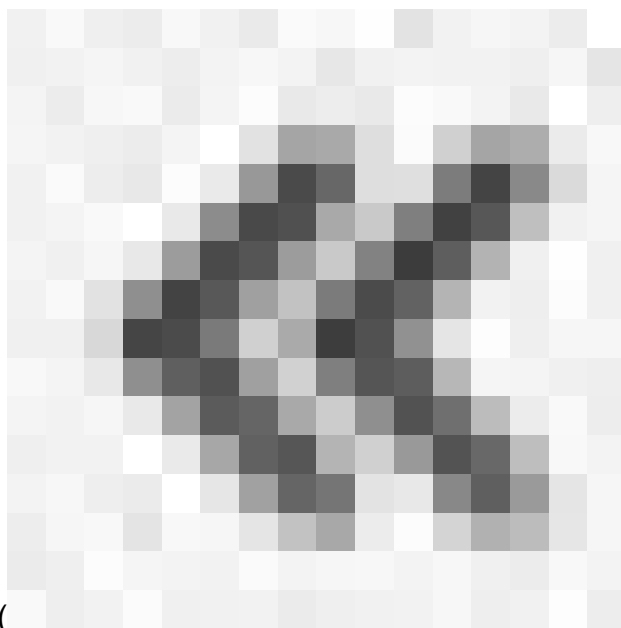
Você pode fazer um ajuste fino nas tarefas agendadas clicando na caneta de edição (



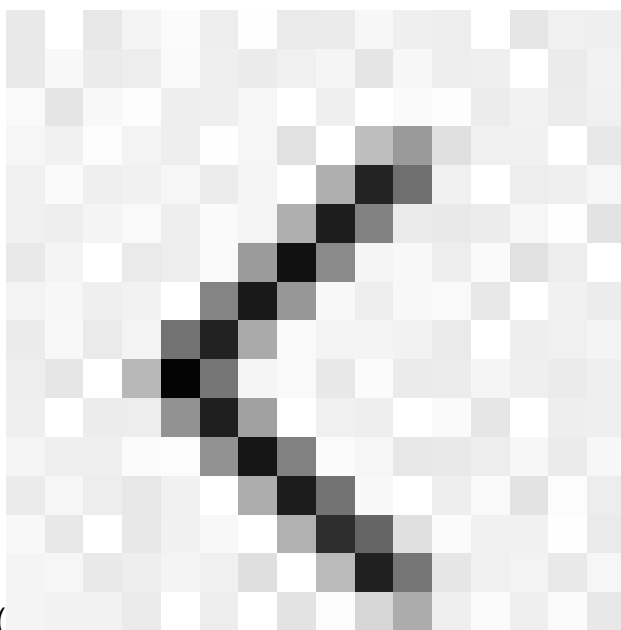
) ou excluí-las clicando na lixeira (



Passo 2 Você pode executar estas tarefas usando a exibição de calendário:



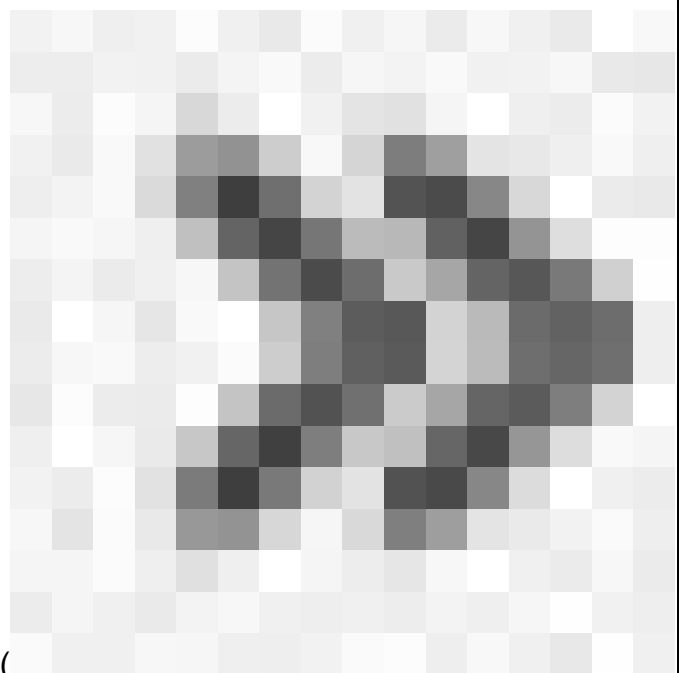
- Clique em Seta dupla para a esquerda() para voltar um ano.



- Clique em Seta única para a esquerda() para voltar um mês.
- Clique em Seta única para a direita(



)para avançar um mês.



- Clique em Seta dupla para a direita()para avançar um ano.

- Clique em Hoje para retornar ao mês e ano atuais.
- Clique em Adicionar Tarefas para agendar uma nova tarefa.
- Clique em uma data para exibir todas as tarefas agendadas para a data específica em uma tabela de lista de tarefas.
- Clique em uma tarefa específica em uma data para exibi-la em uma tabela de lista de tarefas.

Troubleshooting

Caso a atualização automática do VDB não esteja funcionando conforme esperado, você poderá reverter o VDB.

Etapas:

SSH para a CLI do dispositivo de gerenciamento (FMC, FDM ou SFR onbox).

Mude para o modo especialista e para a raiz e defina a variável de reversão:

```
<#root>
```

```
expert
```

```
sudo su  
export ROLLBACK_VDB=1
```

Verifique se o pacote VDB para o qual você pretende fazer downgrade está localizado no dispositivo em `/var/sf/updates` e instale-o:

```
<#root>
```

```
install_update.pl --detach /var/sf/updates/<name of desired VDB Package file>
```

Os logs de instalação normais do vdb podem ser encontrados no local aplicável em `/var/log/sf/vdb-*`

Quando a instalação do VDB for concluída, implante a política nos dispositivos.

No FMC, para verificar o status de instalação do VDB, o conteúdo do diretório pode ser revisado:

```
root@firepower:/var/log/sf/vdb-4.5.0-338# ls -la  
total 40
```

```
drwxr-xr-x 5 root root 4096 15 de maio de 2023 .
drwxr-xr-x 11 root root 4096 Apr 23 06:00 ..
-rw-r--r-- 1 raiz 3308 15 de maio 2023 flags.conf.complete
instalador de drwxr-xr-x 2 root root 4096 May 15 2023
drwxr-xr-x 2 root 4096 May 15 2023 post
drwxr-xr-x 2 root root 4096 May 15 2023 pre
-rw-r--r-- 1 raiz 1603 15 de maio de 2023 status.log
-rw-r--r-- 1 raiz 5703 15 de maio de 2023 vdb.log
-rw-r--r-- 1 raiz 5 maio 15 2023 vdb.pid
```

No FTD, para verificar o histórico de instalações do VDB, verifique o seguinte conteúdo do diretório:

```
root@firepower:/ngfw/var/cisco/deploy/pkg/var/cisco/packages# ls -al
72912 total
drwxr-xr-x 5 root root 130 Set 1 08:49 .
drwxr-xr-x 4 root root 34 Aug 16 14:40 ..
drwxr-xr-x 3 root root 18 Aug 16 14:40 export-7.2.4-169
-rw-r--r-- 1 raiz raiz 2371661 27 de julho 15:34 exportador-7.2.4-169.tgz
drwxr-xr-x 3 root 21 Aug 16 14:40 vdb-368
-rw-r--r-- 1 raiz 36374219 27 de julho 15:34 vdb-368.tgz
drwxr-xr-x 3 root root 21 Sep 1 08:49 vdb-369
-rw-r--r-- 1 raiz 35908455 Set 1 08:48 vdb-369.tgz
```

Informações Relacionadas

[Atualizar banco de dados de vulnerabilidade \(VDB\)](#)

[Agendamento de tarefas](#)

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.