



# Markvision Enterprise

---

Guia do usuário

## Nota de edição

Janeiro de 2012

**O parágrafo a seguir não se aplica a países onde as cláusulas descritas não são compatíveis com a lei local:** A LEXMARK INTERNATIONAL, INC. FORNECE ESTA PUBLICAÇÃO "NO ESTADO EM QUE SE ENCONTRA", SEM QUALQUER TIPO DE GARANTIA, EXPRESSA OU TÁCITA, INCLUINDO, ENTRE OUTRAS, GARANTIAS IMPLÍCITAS DE COMERCIALIZIDADE OU ADEQUAÇÃO A UM DETERMINADO PROPÓSITO. Alguns estados não permitem a contestação de garantias expressas ou implícitas em certas transações. Conseqüentemente, é possível que esta declaração não se aplique ao seu caso.

É possível que esta publicação contenha imprecisões técnicas ou erros tipográficos. Serão feitas alterações periódicas às informações aqui contidas; essas alterações serão incorporadas em edições futuras. Alguns aperfeiçoamentos ou alterações nos produtos ou programas descritos poderão ser feitos a qualquer momento.

As referências feitas nesta publicação a produtos, programas ou serviços não implicam que o fabricante pretenda torná-los disponíveis em todos os países nos quais opera. Qualquer referência a um produto, programa ou serviço não tem a intenção de afirmar ou sugerir que apenas aquele produto, programa ou serviço possa ser usado. Qualquer produto, programa ou serviço funcionalmente equivalente que não infrinja qualquer direito de propriedade intelectual existente poderá ser usado no seu lugar. A avaliação e verificação da operação em conjunto com outros produtos, programas ou serviços, exceto aqueles expressamente designados pelo fabricante, são de responsabilidade do usuário.

Para obter suporte técnico da Lexmark, acesse [support.lexmark.com](http://support.lexmark.com).

Para obter informações sobre suprimentos e downloads, acesse [www.lexmark.com](http://www.lexmark.com).

Caso você não tenha acesso à Internet, entre em contato com a Lexmark pelo correio:

Lexmark International, Inc.  
Bldg 004-2/CSC  
740 New Circle Road NW  
Lexington, KY 40550  
USA

© 2012 Lexmark International, Inc.

**Todos os direitos reservados.**

### Marcas registradas

Lexmark, Lexmark com desenho de losango e MarkVision são marcas registradas da Lexmark International, Inc. nos Estados Unidos e/ou em outros países.

Todas as outras marcas registradas pertencem a seus respectivos proprietários.

### GOVERNMENT END USERS

The Software Program and any related documentation are "Commercial Items," as that term is defined in 48 C.F.R. 2.101, "Computer Software" and "Commercial Computer Software Documentation," as such terms are used in 48 C.F.R. 12.212 or 48 C.F.R. 227.7202, as applicable. Consistent with 48 C.F.R. 12.212 or 48 C.F.R. 227.7202-1 through 227.7207-4, as applicable, the Commercial Computer Software and Commercial Software Documentation are licensed to the U.S. Government end users (a) only as Commercial Items and (b) with only those rights as are granted to all other end users pursuant to the terms and conditions herein.

### Avisos de licenciamento

Todos os avisos de licenciamento associados a este produto podem ser vistos no diretório raiz do CD do software de instalação.

# Conteúdo

- Nota de edição.....2**
- Visão geral.....7**
  - O que é Markvision Enterprise?.....7
- Preparação inicial.....8**
  - Instruções de suporte.....8
    - Requisitos de sistema .....8
    - Servidores do banco de dados suportados.....8
  - Instalação do Markvision.....8
  - Atualização para a versão mais recente do Markvision.....9
  - Backup e restauração do banco de dados Firebird.....9
  - Acesso ao Markvision.....10
  - Migração do MarkVision Professional para o Markvision Enterprise.....11
  - Uso do Markvision.....12
  - Para entender a tela Início.....14
  - Compreensão das portas e protocolos.....15
- Gerenciamento de ativos.....18**
  - Localização de dispositivos.....18
    - Criando um perfil de localização.....18
    - Edição ou exclusão de um perfil de localização .....19
    - Importando dispositivos de um arquivo .....20
  - Gerenciamento de dispositivos.....21
    - Configuração do estado do ciclo de vida útil do dispositivo .....21
    - Auditoria de um dispositivo .....21
    - Exibição de propriedades do dispositivo .....22
- Localização e organização de dispositivos no sistema.....24**
  - Pesquisa por dispositivos no sistema.....24
  - Trabalho com marcadores.....27
    - Criação de marcadores .....27
    - Acesso a marcadores .....27
    - Exclusão de marcadores .....27
  - Uso de categorias e palavras-chave.....27
    - Adição, edição ou exclusão de categorias .....28
    - Adição, edição ou exclusão de palavras-chave .....28

Atribuição de palavras-chave a um dispositivo ..... 28  
 Remoção de uma palavra-chave atribuída de um dispositivo ..... 29

**Gerenciamento de políticas.....30**

Criação de uma política.....30  
     Criação de uma nova política..... 30  
     Criação de uma política de um dispositivo ..... 31  
 Entendimento da política de segurança.....32  
     Compreensão dos dispositivos protegidos ..... 32  
     Compreensão das definições de políticas de segurança ..... 33  
     Criação de uma política de segurança ..... 34  
     Alteração das credenciais de comunicação de um dispositivo restrito ..... 39  
 Edição ou exclusão de uma política.....40  
 Atribuição de uma política.....40  
 Verificação da conformidade com uma política.....41  
 Aplicação de uma política.....41  
 Remoção de uma política.....41

**Gerenciamento da Central de serviços.....42**

Trabalho com políticas.....42  
     Verificação da conformidade do dispositivo com as políticas ..... 42  
     Aplicação de políticas ..... 42  
 Trabalho com um dispositivo.....42  
     Verificação do status de um dispositivo ..... 42  
     Exibição de um dispositivo, remotamente ..... 43  
     Exibição da página da Web incorporada..... 43

**Gerenciamento de eventos de dispositivo.....44**

Criação de um destino.....44  
 Edição ou exclusão de um destino.....44  
 Criação de um evento.....45  
 Edição ou exclusão de um evento.....45  
 Atribuição de um evento a um dispositivo.....45  
 Remoção de um evento de um dispositivo.....46  
 Exibição de detalhes de eventos.....46

**Execução de outras tarefas administrativas.....47**

Download de arquivos genéricos.....47  
 Configurando as definições de e-mail.....47  
 Configuração das definições do sistema.....48

Adição, edição ou exclusão de um usuário no sistema.....	48
Ativação da autenticação do servidor LDAP.....	49
Geração de relatórios.....	54
Tarefas de programação.....	55
Exibição do log do sistema.....	56
<b>Perguntas freqüentes.....</b>	<b>57</b>
<b>Solução de problemas.....</b>	<b>58</b>
O usuário esqueceu a senha.....	58
O aplicativo não consegue localizar um dispositivo de rede.....	58
Verifique as conexões da impressora .....	58
Certifique-se de que o servidor de impressão interno esteja instalado adequadamente e ativado.....	58
Verifique se o nome do dispositivo no aplicativo é o mesmo que o nome definido no servidor de impressão.....	59
Verifique se o servidor de impressão está se comunicando na rede. ....	59
As informações sobre o dispositivo estão incorretas.....	59
<b>Apêndice.....</b>	<b>60</b>
<b>Glossário de termos de segurança.....</b>	<b>61</b>
<b>Índice.....</b>	<b>62</b>



## Visão geral

### O que é Markvision Enterprise?

O *Markvision™Enterprise* (MVE) é um utilitário de gerenciamento de dispositivos ativado para a Web e desenvolvido para profissionais de TI. O MVE funciona como um aplicativo cliente-servidor. O servidor localiza e se comunica com dispositivos na rede e fornece as informações sobre eles ao cliente. O cliente exibe as informações e fornece uma interface de usuário para o gerenciamento desses dispositivos. Cada servidor do Markvision pode gerenciar milhares de dispositivos de uma vez.

Os recursos de segurança incorporados impedem o acesso não autorizado ao aplicativo e somente usuários autorizados podem usar o cliente para acessar opções de gerenciamento.

O Markvision permite que você monitore e gerencie toda a sua frota de impressoras, que é composta de impressoras e servidores de impressão. Na *Biblioteca de infra-estrutura de tecnologia da informação* (ITIL), impressoras e servidores de impressão também são conhecidos como *Itens de configuração* (CIs). Neste documento, CIs, impressoras ou servidores de impressão às vezes são chamados de dispositivos.

# Preparação inicial

## Instruções de suporte

Para obter uma lista completa dos sistemas operacionais e navegadores da Web suportados, consulte as *Notas de versão*.

## Requisitos de sistema

### RAM

- Necessário: 1 GB
- Recomendado: 2 GB+

### Velocidade do processador

- Necessário: 1 físico de 2 GHz ou superior (Hyper-Threaded/Dual Core)
- Recomendado: 1+ físico de 3 GHz (Hyper-Threaded/Dual Core+)

### Espaço na unidade de disco rígido do computador

- Pelo menos 60 GB de espaço de armazenamento disponível

### Resolução da tela

- Pelo menos 1024 x 768 pixels (somente para MVE clientes)

## Servidores do banco de dados suportados

- Firebird
- Microsoft SQL Server 2008
- Microsoft SQL Server 2005

### Notas:

- O aplicativo suporta somente as versões de 32 bits e vem com um banco de dados Firebird pré-configurado.
- O servidor de banco de dados onde o MVE for instalado deve ter somente uma *placa de interface de rede* (NIC).

## Instalação do Markvision

Com o Markvision, você pode usar Firebird ou o Microsoft SQL Server como o banco de dados back-end.

Se estiver usando o Microsoft SQL Server, então faça o seguinte antes de instalar o Markvision:

- Ative a autenticação do modo misto e a Execução automática.
- Defina as Bibliotecas de rede para usar uma porta estática e soquetes TCP/IP.
- Crie uma conta de usuário que o Markvision usará para criar o esquema do banco de dados e todas as conexões do banco de dados.

- Crie os seguintes bancos de dados:
  - ESTRUTURA
  - MONITOR
  - QUARTZO

**Nota:** Certifique-se de que a conta de usuário que você criou é a proprietária desses bancos de dados ou possui os privilégios apropriados para criar um esquema e executar operações de *Linguagem de manipulação de dados* (DML).

- 1 Descompacte os arquivos instalados para um caminho que *não* contenha nenhum espaço.
- 2 Inicie o **setup.exe** e siga as instruções exibidas na tela do computador.

## Atualização para a versão mais recente do Markvision

A atualização foi desenvolvida para funcionar somente de uma versão imediatamente precedente.

- 1 Backup do banco de dados.

**Notas:**


- Se estiver usando um banco de dados Firebird, consulte “Backup do banco de dados Firebird” na página 9 para obter mais informações.
- Se você estiver usando o MS SQL Server, entre em contato com o administrador do MS SQL.

- 2 Descompacte os arquivos de instalação em um local temporário e verifique se o caminho *não* contém espaços.
- 3 Inicie o **setup.exe** e siga as instruções exibidas na tela do computador.

## Backup e restauração do banco de dados Firebird

### Backup do banco de dados Firebird

**Nota:** Se você estiver usando o MS SQL Server como banco de dados, entre em contato com o administrador do MS SQL.

- 1 Encerre o serviço do MarkVision Enterprise.
  - a Clique em  ou clique em **Iniciar > Definições**.
  - b Selecione **Painel de Controle** e, se necessário, clique em **Sistema & segurança**.
  - c Clique duas vezes em **Ferramentas administrativas**.
  - d Se necessário, clique duas vezes em **Serviços de componente**.
  - e Clique duas vezes em **Serviços**.
  - f No painel **Serviços**, selecione **Markvision Enterprise** e clique em **Parar**.
- 2 Localize a pasta onde o Markvision Enterprise foi instalado e navegue até `firebird\data`.  
Por exemplo: `C:\Arquivos de Programas\Lexmark\Markvision Enterprise\firebird\data`

- 3 Copie os bancos de dados a seguir em um repositório seguro.
  - FRAMEWORK.FDB
  - MONITOR.FDB
  - QUARTZ.FDB
- 4 Reinicie o serviço do MarkVision Enterprise.
  - a Repita as etapas 1a a 1e.
  - b No painel Serviços, selecione **Markvision Enterprise** e clique em **Reiniciar**.

## Restauração do banco de dados Firebird

- 1 Verifique se concluiu o processo de backup do banco de dados Firebird.
- 2 Encerre o serviço do MarkVision Enterprise.

Para obter mais informações, consulte etapa 1 de “Backup do banco de dados Firebird” na página 9.
- 3 Localize a pasta onde o Markvision Enterprise foi instalado e navegue até firebird\data.

Por exemplo: **C:\Arquivos de Programas\Lexmark\Markvision Enterprise\firebird\data**
- 4 Substitua os bancos de dados a seguir pelos bancos de dados salvos quando você concluiu o processo de backup.
  - FRAMEWORK.FDB
  - MONITOR.FDB
  - QUARTZ.FDB
- 5 Reinicie o serviço do MarkVision Enterprise.

Para obter mais informações, consulte etapa 4 de “Backup do banco de dados Firebird” na página 9.

## Acesso ao Markvision

- 1 Abra o navegador da Internet e digite **http://MVE\_SERVER:9788/mve/** no campo URL.

**Nota:** Substitua **MVE\_SERVER** pelo nome do host ou endereço IP da máquina que hospeda o Markvision.
- 2 No campo Usuário, digite **admin**.
- 3 No campo Senha, digite **Administrator1** e clique em **Login**.

**Nota:** Para alterar a senha, clique em **Alterar senha** no canto superior direito da tela Bem-vindo.

Se o Markvision ficar ocioso por mais de 30 minutos, ele será desconectado automaticamente. Será necessário fazer o login novamente para acessar o MarkVision:

# Migração do MarkVision Professional para o Markvision Enterprise

**Nota:** O Markvision Enterprise (MVE) suporta somente migração de dados do MarkVision Professional (MVP) v11.2.1.

## Exportação de dados do MVP

### Uso da página da Web do servidor MVP

1 Abra um navegador da Web e digite `http://MVP_SERVER:9180/~MvServer` no campo URL.

**Nota:** Substitua `MVP_SERVER` pelo endereço IP ou nome do host do Servidor MVP.

2 Na página Servidor da Web do MarkVision, clique em **Dir de dados**.

3 Insira o seu nome de usuário e senha caso solicitado.

4 Na página Diretório de dados de carregamento, clique em  para carregar seus dados do MVP como um arquivo zip.

5 Salve o arquivo zip.

### Uso do sistema de arquivos

1 No sistema executando o Servidor MVP, navegue para o local onde o Servidor MVP está instalado.

2 Compacte a pasta Dados em um arquivo zip.

## Importação de dados para o MVE

1 Faça o login para Markvision Enterprise.

2 Na caixa de diálogo “Importar dados do MarkVision Professional”, clique em **Sim** e, em seguida, clique em **Procurar**.

#### Notas:

- Se você clicar em **Sim**, a caixa de diálogo não aparecerá na próxima vez que fizer login para o MVE.
- Se você clicar em **Não** e não quiser ver a caixa de diálogo novamente, selecione **Não mostrar esta mensagem novamente**.

3 Navegue para o local onde seu arquivo zip está armazenado e clique em **Abrir**.

4 Na área “Dados a serem importados”, selecione o tipo de dados que deseja importar.

Dados	Detalhes
<b>Usuários</b>	<ul style="list-style-type: none"> <li>• No MarkVision Professional, os usuários recebem privilégios para funções individuais.</li> <li>• No Markvision Enterprise, os usuários são atribuídos a papéis associados a diferentes funções.</li> <li>• Todos os usuários importados do MVP são atribuídos automaticamente a todas as funções exceto <b>ROLE_ADMIN</b>.</li> <li>• Se uma senha de usuário do MVP não atender aos critérios de senha do MVE, então a seqüência <b>Administrator1</b> é anexada à senha atual do usuário.</li> </ul>

Dados	Detalhes
<b>Dispositivos</b>	<ul style="list-style-type: none"> <li>• O MVE importa somente informações básicas do dispositivo do MVP, incluindo nome do modelo, número de série, endereço MAC e endereço IP.</li> <li>• Se já existir uma impressora no MVE, então aquela impressora será ignorada durante a importação.</li> <li>• Durante a importação, o MVE desconsidera as impressoras conectadas aos Adaptadores de rede externos (ENAs), já que o MVE atualmente não suporta ENAs.</li> <li>• Os dispositivos importados são definidos automaticamente para o estado do ciclo de vida útil <b>Gerenciado (Normal)</b>.</li> <li>• O MVP gerencia impressoras e servidores de impressão. O MVE gerencia apenas impressoras. Portanto, duas entradas no MVP tornam-se uma única entrada no MVE.</li> </ul>
<b>Perfis de localização</b>	<ul style="list-style-type: none"> <li>• Quando os perfis do MVP são importados para o sistema do MVE, somente os seguintes detalhes são importados: <ul style="list-style-type: none"> <li>– Nome da comunidade SNMP</li> <li>– Tentativas</li> <li>– Timeout</li> <li>– Excluir endereço</li> <li>– Incluir endereço</li> </ul> </li> <li>• No MVP, cada entrada para Incluir/Excluir contém uma definição de Nome da comunidade de Leitura/Gravação SNMP. Um perfil que contenha várias entradas para Incluir/Excluir pode conter também diversas definições de Nome da comunidade de Leitura/Gravação. No MVE, a definição de Nome da comunidade de Leitura/Gravação pertence ao próprio perfil. Cada perfil pode conter apenas uma definição de Nome da comunidade de Leitura/Gravação. Portanto, um perfil de localização no MVP (contendo várias definições únicas de Nome da comunidade de Leitura/Gravação) é separado em diversos perfis de localização quando importado para o MVE (cada um contendo uma definição de Nome da comunidade de Leitura/Gravação). O número de perfis no MVE é igual ao número de definições únicas de Nome da comunidade de Leitura/Gravação no perfil MVP original.</li> <li>• Para Tempo limite, o MVE converte o Tempo limite do MVP em milissegundos ao multiplicar o valor do MVP (em segundos) por 1.000.</li> <li>• A opção Gerenciar automaticamente é definida como <b>Falso</b> durante a importação.</li> </ul>

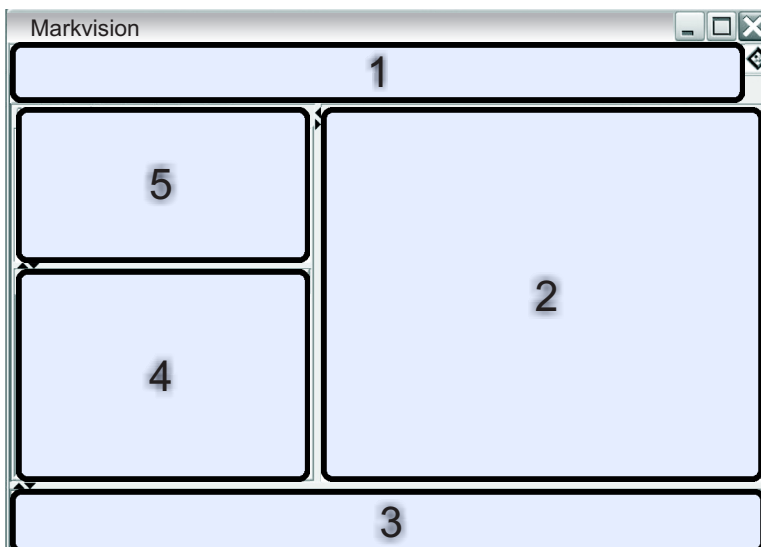
5 Clique em **Importar**.

## Uso do Markvision

Os recursos e funções do Markvision são divididos em quatro áreas de serviço. Isso fornece maior facilidade de uso ao garantir que a visualização da interface seja preenchida somente com as funções e os recursos necessários para a tarefa disponível. Cada área de serviço é acessível por meio de uma guia na tela inicial e corresponde a um estágio do ciclo de vida útil do serviço na Biblioteca de infra-estrutura de tecnologia da informação (ITIL) versão 3. A disciplina de ITIL é reconhecida de forma global por sua compilação de práticas recomendadas por gerenciar recursos de TI em uma organização.

Use essa guia	Para
<b>Ativos</b>	<p>Localize, identifique, catalogue, organize e controle os ativos físicos (impressoras e dispositivos multifuncionais) que compõe sua frota de impressoras. Aqui, você pode reunir e manter informações sobre os modelos da frota, os recursos, as opções instaladas e o ciclo de vida útil.</p> <p>Na ITIL, isso se encaixa na área de Transição do serviço.</p> <p>Se uma de suas responsabilidades inclui o gerenciamento de ativos de TI, vá para “Gerenciamento de ativos” na página 18.</p>
<b>Políticas</b>	<p>Defina e gerencie a configuração de software da frota de impressoras. Aqui, você pode atribuir uma política definida que especifique as definições de configuração particulares para cada modelo. É possível monitorar se a frota de impressoras está em conformidade com as políticas e aplicar essas políticas quando necessário.</p> <p>Na ITIL, isso se encaixa na área de Transição do serviço.</p> <p>Se uma de suas responsabilidades inclui a administração e a manutenção de ferramentas de gerenciamento da configuração, vá para “Gerenciamento de políticas” na página 30.</p>
<b>Serviço de help desk</b>	<p>Interaja diretamente com um único dispositivo na frota de impressoras. Aqui, você pode gerenciar o dispositivo de forma remota, verificar a conformidade com a política e aplicar políticas, além de personalizar as definições de configuração por meio do servidor da Web Incorporado do dispositivo.</p> <p>Na ITIL, isso se encaixa na área de Operação do serviço.</p> <p>Se uma de suas responsabilidades inclui o gerenciamento ou a administração do serviço de suporte à TI do cliente, vá para “Gerenciamento da Central de serviços” na página 42.</p>
<b>Gerente de eventos</b>	<p>Crie um evento automatizado quando um dispositivo enviar um alerta para a rede. É possível escolher enviar um e-mail ou executar outras ações com script para notificar as pessoas identificadas.</p> <p>Na ITIL, isso se encaixa na área de Operação do serviço.</p> <p>Se uma de suas responsabilidades inclui gerenciamento de problemas ou averiguação de incidentes, vá para “Gerenciamento de eventos de dispositivo” na página 44.</p>

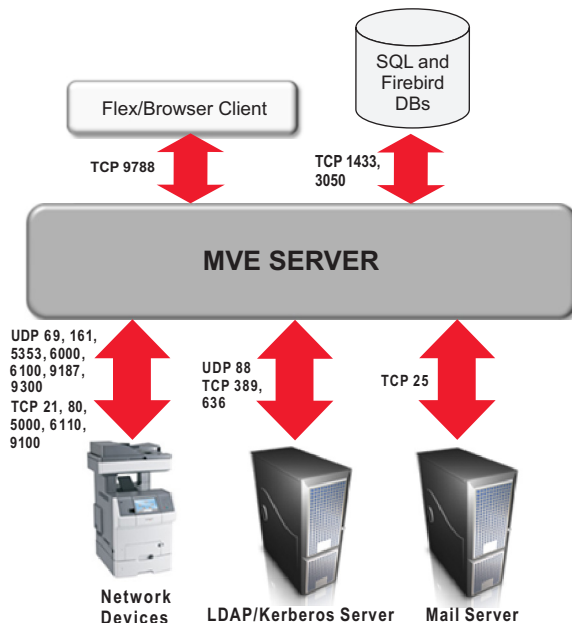
## Para entender a tela Início



Use essa área	Para	
1	Cabeçalho	Acesse as quatro guias da área de serviço e execute outras tarefas administrativas.
2	Resultados da pesquisa	Visualize a lista completa em páginas dos dispositivos que correspondem à pesquisa ou ao marcador atualmente selecionado.
3	Informações da tarefa	Visualize o status da atividade mais recente.
4	Resumo de resultados da pesquisa	Visualize um resumo categorizado da pesquisa ou do marcador atualmente selecionado.
5	Marcadores e Pesquisa avançada	Gerencie e selecione marcadores e refine consultas de pesquisa.

## Compreensão das portas e protocolos

O Markvision usa diferentes portas e protocolos para os vários tipos de comunicação de rede, conforme mostrado no diagrama a seguir.



**Nota:** As portas são bidirecionais e devem estar abertas ou ativadas para o Markvision funcionar corretamente. Certifique-se de que todas as portas do dispositivo estejam definidas como **Seguro e não-seguro** ou **Ativado**, dependendo do dispositivo.

## Comunicação entre servidor e dispositivo

Abaixo, as portas e os protocolos usados durante a comunicação entre o Servidor do Markvision e os dispositivos da rede.

Protocolo	Servidor do Markvision	Dispositivo	Usado para
<b>NPAP</b> <i>Network Printer Alliance Protocol</i>	Porta efêmera <i>User Datagram Protocol</i> (UDP)	UDP 9300	Comunicação com impressoras de rede da Lexmark
<b>XMLNT</b> <i>XML Network Transport</i> (Armazenamento de objeto)	Portas efêmeras UDP e <i>Transmission Control Protocol</i> (TCP)	UDP 6000 TCP 5000	Comunicação com impressoras de rede da Lexmark
<b>LST</b> <i>Lexmark Secure Transport</i>	UDP 6100 Porta TCP efêmera (saudação)	UDP 6100 TCP 6110 (saudação)	Comunicação criptografada com impressoras de rede da Lexmark
<b>mDNS</b> <i>Multicast Domain Name System</i>	Porta UDP efêmera	UDP 5353	Encontrar certas impressoras de rede da Lexmark e determinar recursos de segurança de dispositivos
<b>SNMP</b> <i>Simple Network Management Protocol</i>	Porta UDP efêmera	UDP 161	Encontrar impressoras de rede de terceiros e da Lexmark e para a comunicação entre elas

Protocolo	Servidor do Markvision	Dispositivo	Usado para
<b>FTP</b> <i>File Transfer Protocol</i>	Porta TCP efêmera	TCP 21	Downloads de arquivos genéricos
<b>TFTP</b> <i>Trivial File Transfer Protocol</i>	Porta UDP efêmera	UDP 69	Atualizações de firmware e downloads de arquivos genéricos
<b>HTTP</b> <i>Hypertext Transfer Protocol</i>	Porta TCP efêmera	TCP 80	Downloads de arquivos genéricos
<b>Porta de impressão bruta</b>	Porta TCP efêmera	TCP 9100	Downloads de arquivos genéricos

## Comunicação entre dispositivo e servidor

Esta é a porta e o protocolo usados durante a comunicação entre os dispositivos de rede e o Servidor do Markvision.

Protocolo	Dispositivo	Servidor do Markvision	Usado para
<b>NPAP</b>	UDP 9300	UDP 9187	Recepção e geração alertas

## Comunicação entre servidor e banco de dados

Estas são as portas usadas durante comunicação entre o Servidor do Markvision e os bancos de dados.

Servidor do Markvision	Banco de dados	Usado para
Porta TCP efêmera	TCP 1433 (SQL Server) Esta é a porta padrão que pode ser usada pelo usuário.	Comunicação com um banco de dados do SQL Server
Porta TCP efêmera	TCP 3050	Comunicação com um banco de dados Firebird

## Comunicação entre servidor e cliente

Estes são a porta e o protocolo usados durante a comunicação entre o cliente Flex/Browser e o Servidor do Markvision.

Protocolo	Cliente Flex/Browser	Servidor do Markvision
<b>AMF</b> <i>Formato de mensagem ActionScript</i>	Porta TCP	TCP 9788

## Mensagens e alertas

Estes são a porta e o protocolo usados durante a comunicação entre o Servidor do Markvision e o servidor de e-mails.

Protocolo	Servidor do Markvision	Servidor SMTP	Usado para
<b>SMTP</b> <i>Simple Mail Transfer Protocol</i>	Porta TCP efêmera	TCP 25 Esta é a porta padrão que pode ser usada pelo usuário.	Fornecimento da funcionalidade de e-mail usada para receber alertas de dispositivos

## Comunicação entre o Servidor do Markvision e o servidor LDAP

Estes são a porta e os protocolos usados durante a comunicação envolvendo grupos de usuário e a funcionalidade de autenticação.

Protocolo	Servidor do Markvision	Servidor LDAP	Usado para
<b>LDAP</b> <i>Lightweight Directory Access Protocol</i>	Porta TCP efêmera	TCP 389 ou a porta para a qual o servidor LDAP foi configurada para ser ouvida	Autenticação de usuário de Markvision Enterprise usando um servidor LDAP
<b>LDAPS</b> <i>Secure Lightweight Directory Access Protocol</i>	Porta TCP efêmera	<i>Transport Layer Security (TLS)</i> ou a porta para a qual o servidor LDAP foi configurada para ser ouvida Isso é para conexões criptografadas TLS.	Autenticação de usuários do Markvision Enterprise usando um servidor LDAP por meio de um canal seguro que usa TLS
<b>Kerberos</b>	Porta UDP efêmera	UDP 88 Esta é a porta Kerberos Authentication Service padrão.	Autenticação Kerberos

# Gerenciamento de ativos

## Localização de dispositivos

O aplicativo permite que você pesquise a rede em busca de dispositivos. Quando os dispositivos são encontrados, as informações de identificação são armazenadas no sistema. Use marcadores ou pesquisas para visualizar os dispositivos dos Resultados da pesquisa.

Os dispositivos encontrados são, por padrão, definidos como **Novo** e não são gerenciados pelo sistema. Antes de executar qualquer ação em um dispositivo, defina-o como **Gerenciado**. Para obter mais informações, consulte “Gerenciamento de dispositivos” na página 21.

Veja abaixo as duas maneiras de adicionar dispositivos ao sistema:


- **Uso de um perfil de localização** — encontre dispositivos na rede usando parâmetros personalizados.
- **Importação de dispositivos a partir de um arquivo** — Use um arquivo de *valores separados por vírgula* (CSV) para importar arquivos.

**Nota:** Você pode usar somente uma das duas maneiras: Realizando ambos procedimentos para adicionar dispositivos nos resultados do sistema em dispositivos duplicados.

Depois de adicionar um dispositivo no sistema, realize uma auditoria do dispositivo imediatamente. A realização da auditoria oferece informações adicionais sobre o dispositivo, que são necessárias para concluir algumas tarefas com sucesso. Para obter mais informações sobre como fazer a auditoria de um dispositivo, consulte “Auditoria de um dispositivo” na página 21.

**Nota:** Nota: Isto se aplica *somente* aos dispositivos sem restrições. No caso dos dispositivos restritos, primeiro atribua a política de segurança e depois aplique-a nos dispositivos restritos antes de realizar uma auditoria. Caso contrário, isto resultará em uma falha de auditoria e definirá o estado dos dispositivos restritos como **(Gerenciado) Ausente**. Para obter mais informações sobre os dispositivos restritos, consulte “Compreensão dos dispositivos protegidos” na página 32.


## Criando um perfil de localização

- 1 Se necessário, na guia Ativos, clique em **Perfis de localização** para mostrar a seção Perfis de localização.
- 2 Clique em **+** e digite o nome do novo perfil de localização.
- 3 Na guia Endereços, selecione **Incluir** ou **Excluir**.
- 4 Para importar uma lista de termos de um arquivo a ser incluído ou excluído, faça o seguinte:
  - a Clique em .
  - b Navegue até a pasta onde o arquivo está salvo.
  - c Selecione o arquivo e clique em **Abrir**.

**Nota:** O arquivo pode conter qualquer um dos padrões que podem ser inseridos no campo de texto acima de Endereço/Intervalo. Para visualizar os exemplos de um padrão válido, passe o mouse sobre o campo de texto.

- 5 Ao lado de **+**, digite o endereço IP, o nome de host DNS totalmente qualificado, as subredes com caracteres curinga ou intervalos de endereços desejados e, depois, clique em **+**.

**Notas:**

- Só é possível digitar uma entrada de cada vez. Para visualizar exemplos de uma entrada válida, passe o mouse sobre o campo de texto acima de Endereço/Intervalo.
- Ao digitar intervalos de endereço, *não* use caracteres curinga.
- Para excluir uma entrada, selecione-a e, em seguida, clique em .

**6** Clique na guia **SNMP** e, depois, selecione **Versão 1.2c** ou **Versão 3**.

**Nota:** Se não tiver certeza de qual versão o SNMP está usando, entre em contato com o responsável pelo suporte do sistema.

**7** Se você tiver selecionado **Versão 1.2c** em etapa 6, na área Nomes de comunidade, defina o perfil de privacidade. Se você tiver selecionado **Versão 3**, na área Segurança, defina o perfil de segurança.

**Nota:** Caso não saiba como configurar o perfil de segurança SNMP Versão 3, entre em contato com o responsável pelo suporte do sistema.

**8** Clique na guia **Geral** e, na área Desempenho, faça o seguinte:

- No campo Tempo limite, especifique o tempo (em milissegundos) a ser aguardado pela resposta dos dispositivos.
- No campo Novas tentativas, especifique o número de novas tentativas antes que o sistema pare de tentar se comunicar com um dispositivo.


**9** Especifique se deseja incluir os dispositivos seguros na localização.**Notas:**

- Se não tiver um dispositivo seguro, *não* selecione essa opção. Caso contrário, o desempenho será prejudicado, o que resultará em um tempo muito maior de localização de dispositivos.
- Quando um dispositivo estiver seguro, uma ou ambas as condições se aplicarão: (a) as portas de comunicação são desativadas e (b) a autenticação é obrigatória para obter informações do dispositivo.


**10** Selecione se o perfil de localização deverá gerenciar automaticamente os dispositivos localizados.

**Nota:** Se você selecionar essa opção, todos os dispositivos localizados serão definidos automaticamente para o estado do ciclo de vida **Gerenciado**.

**11** Clique em **Salvar >Fechar**.**Notas:**

- Clicar em  executa o perfil de localização e *não* o salva.
- Um novo perfil de localização reúne informações suficientes para identificar um dispositivo de forma confiável. Para reunir informações completas de um dispositivo, defina o estado do dispositivo para **Gerenciado** e execute uma auditoria do dispositivo.
- Para garantir que as informações do dispositivo estejam atuais, é possível programar uma localização para ocorrer regularmente. Para obter mais informações, consulte “Tarefas de programação” na página 55.

## Edição ou exclusão de um perfil de localização

**1** Se necessário, clique em **Perfis de localização** na guia Ativos para mostrar a seção de perfis de localização.**2** Selecione um perfil e clique em  para editar ou  para excluir o perfil de localização.**3** Siga as instruções na tela do computador.

## Importando dispositivos de um arquivo

Use um arquivo de valores separados por vírgula (CSV) para importar dispositivos.

**Nota:** Durante a preparação para uma implementação, a Markvision permite que você adicione dispositivos ao sistema mesmo *antes* de eles estarem disponíveis na rede.

**1** Na guia Assets, clique em **Importar** e, depois, em **Procurar**.

**2** Navegue até a pasta onde o arquivo CSV está armazenado.

**Nota:** Verifique se cada linha do arquivo CSV representa um único dispositivo.

**3** Selecione o arquivo CSV e clique em **Abrir**.

**4** Na seção Colunas possíveis, selecione as colunas que correspondem aos valores no arquivo CSV.

**5** Se estiver usando o protocolo SNMP V3 para se comunicar com o dispositivo, você *deverá* selecionar as seguintes colunas:

- **SNMP V3 Read/Write User**
- **SNMP V3 Read/Write Password**
- **SNMP V3 Minimum Authentication Level**
- **SNMP V3 Authentication Hash**
- **SNMP V3 Privacy Algorithm**

**Nota:** No arquivo CSV selecionado na etapa 3, verifique se os seguintes parâmetros contêm um dos valores especificados abaixo deles:

- Nível de Autenticação Mínimo
  - **NO\_AUTHENTICATION\_NO\_PRIVACY**
  - **AUTHENTICATION\_NO\_PRIVACY**
  - **AUTHENTICATION\_PRIVACY**
- Autenticação de hash
  - **MD5**
  - **SHA1**
- Algoritmo de privacidade
  - **DES**
  - **AES\_128**
  - **AES\_192**
  - **AES\_256**

**Nota:** Se seu arquivo CSV não contiver os valores exatos especificados, o MVE não reconhecerá o dispositivo.

**6** Clique em **Adicionar** para mover as colunas selecionadas na seção Colunas do arquivo CSV.

- Se quiser que o sistema ignore uma coluna no arquivo CSV, selecione **Ignorar**. Repita esse procedimento para cada coluna no arquivo CSV que não esteja listada na seção Colunas possíveis.
- Para alterar a ordem das colunas que você selecionou de acordo com o arquivo CSV, selecione uma coluna na seção Colunas do arquivo CSV e, em seguida, use as setas para mover os cabeçalhos para cima ou para baixo.

**7** Indique se a primeira linha no seu arquivo CSV contém um cabeçalho.

- 8 Indique se os dispositivos importados devem ser automaticamente definidos para o estado de ciclo de vida **Gerenciado**.
- 9 Clique em **OK**.

## Gerenciamento de dispositivos

Um dispositivo pode ser atribuído a três diferentes estados do ciclo de vida útil:

- **Gerenciado** – Isso inclui o dispositivo em todas as atividades que podem ser executadas no sistema.
  - **Gerenciado (Normal)** – O dispositivo está em seu estado constante.
  - **Gerenciado (Alterado)** – Essas são alterações na propriedade física do dispositivo desde a última auditoria. A próxima vez que o sistema se comunicar com o dispositivo e não houver mais alterações em suas propriedades físicas, o dispositivo irá reverter para o estado Gerenciado (Normal).
  - **Gerenciado (Ausente)** – O sistema não pode se comunicar com sucesso com o dispositivo. A próxima vez que o sistema for capaz de se comunicar com sucesso com o dispositivo e não houver alterações em suas propriedades físicas, o dispositivo irá reverter para o estado Gerenciado (Encontrado).
  - **Gerenciado (Encontrado)** – O dispositivo está ausente anteriormente, mas é capaz de se comunicar com sucesso com o sistema em sua tentativa mais recente. A próxima vez que o sistema for capaz de se comunicar com sucesso com o dispositivo e não houver alterações em suas propriedades físicas, o dispositivo irá reverter para o estado Gerenciado (Normal).
- **Não gerenciado** – Isso exclui o dispositivo de todas as atividades executadas no sistema.
- **Desativado** – O dispositivo está anteriormente no estado Gerenciado, mas agora foi removido da rede. O sistema retém as informações do dispositivo, mas não espera ver o dispositivo na rede novamente. Se o dispositivo aparecer novamente na rede, então o sistema define seu estado como Novo.

## Configuração do estado do ciclo de vida útil do dispositivo

Antes que qualquer ação possa ser executada em um dispositivo, verifique se o dispositivo está definido para **Gerenciado**.

- 1 Na guia Ativos, selecione **Novas impressoras** do menu suspenso Marcadores e pesquisas.
- 2 Marque a caixa de seleção ao lado do endereço IP do dispositivo.  
**Nota:** Você pode selecionar vários ou todos os dispositivos.
- 3 No menu suspenso “Definir estado como”, selecione **Gerenciado** e clique em **Sim**.

## Auditoria de um dispositivo

Uma auditoria reúne informações de qualquer dispositivo atualmente Gerenciado na rede e armazena as informações do dispositivo no sistema. Para certificar-se de que as informações em seu sistema sejam atuais, execute uma auditoria regularmente.

- 1 Na área Resultados da pesquisa, marque a caixa de seleção ao lado do endereço IP de um dispositivo.

**Notas:**

- Caso não saiba o endereço IP do dispositivo, localize o dispositivo na coluna Nome do sistema ou Nome do host.

- Para fazer a auditoria de vários dispositivos, marque as caixas de seleção ao lado dos endereços IP dos dispositivos.
- Para fazer a auditoria de todos os dispositivos, marque a caixa de seleção ao lado do "endereço IP".

## 2 Clique em **Auditoria**.

O status da auditoria é exibido na área de Informações da tarefa.

## 3 Quando a auditoria estiver concluída, clique em na área do Cabeçalho.

Os resultados da auditoria mais recente são exibidos na caixa de diálogo Registro.

Depois de realizada a auditoria dos dispositivos, as seguintes instâncias pode pedir que o sistema defina um dispositivo para um estado **Gerenciado (Alterado)**:

- Existem alterações em qualquer um desses valores de identificação ou recursos do dispositivo:
  - Etiqueta de propriedade
  - Nome do host
  - Nome do contato
  - Localização do contato
  - Endereço IP
  - Tamanho da memória
  - Nome da opção copiadora
  - Duplex
- Existem adições ou remoções de qualquer uma dessas opções de hardware do dispositivo:
  - Suprimentos
  - Opções de entrada
  - Opções de saída
  - Ports
- Existem adições ou remoções de qualquer uma dessas funções ou aplicativos do dispositivo:
  - Fontes
  - Aplicativos eSF

**Nota:** Uma auditoria pode ser programada para que ocorra em um momento predeterminado ou regularmente. Para obter mais informações, consulte "Tarefas de programação" na página 55.

## Exibição de propriedades do dispositivo

Para ver a lista completa de informações sobre o dispositivo, certifique-se de que já executou uma auditoria do dispositivo.

**1** Na guia Ativos, selecione **Impressoras gerenciadas** no menu suspenso Marcadores e pesquisas.

**2** Na seção Todas as impressoras, selecione o endereço IP do dispositivo.

**Nota:** Caso não saiba o endereço IP do dispositivo, localize o dispositivo na coluna Nome do sistema.

**3** Na caixa de diálogo Propriedades do ativo:

Clique em	Para visualizar
<b>Identificação</b>	As informações de identificação da rede do dispositivo.
<b>Datas</b>	A lista de eventos do dispositivo. Isso inclui a data adicionada ao sistema, a data de localização e a data de auditoria mais recente.
<b>Firmware</b>	Os níveis de código de firmware do dispositivo.
<b>Recursos</b>	Os recursos do dispositivo.
<b>Ports</b>	As portas disponíveis no dispositivo.
<b>Suprimentos</b>	Os detalhes e níveis de suprimentos do dispositivo.
<b>Cartuchos de fontes</b>	Informações sobre todos os cartuchos de fontes instalados.
<b>Opções</b>	Informações sobre as opções do dispositivo, como o disco rígido do dispositivo e seu espaço livre restante.
<b>Opções de entrada</b>	Configurações para as bandejas de papel disponíveis e outras entradas de dispositivo.
<b>Opções de saída</b>	Configurações para as bandejas de saída de papel disponíveis.
<b>Aplicativos eSF</b>	Informações sobre os aplicativos <i>Estrutura de Soluções Incorporadas</i> (eSF) instalados no dispositivo, como número da versão e status.
<b>Estatísticas do dispositivo</b>	Valores específicos para cada uma das propriedades de dispositivos.
<b>Detalhes da alteração</b>	Informações sobre as alterações no dispositivo. <b>Nota:</b> Isso se aplica <i>somente</i> aos dispositivos que são definidos no estado <b>Gerenciado (Alterado)</b> .

# Localização e organização de dispositivos no sistema

## Pesquisa por dispositivos no sistema

### Uso de marcadores padrão

Marcadores indicam uma pesquisa salva. Ao selecionar um marcador, os dispositivos que são mostrados correspondem aos critérios da pesquisa.

Os marcadores padrão são baseados no estado do ciclo de vida do dispositivo.

- 1 No menu suspenso Marcadores e pesquisas, selecione um marcador:

Selecione	Para
<b>Impressoras gerenciadas</b>	Pesquise dispositivos ativos no sistema. <b>Nota:</b> Dispositivos que aparecem ao selecionar esse marcador podem estar em qualquer um dos seguintes estados: <ul style="list-style-type: none"> <li>• Gerenciado (Normal)</li> <li>• Gerenciado (Alterado)</li> <li>• Gerenciado (Ausente)</li> <li>• Gerenciado (Encontrado)</li> </ul>
<b>Impressoras gerenciadas (Normais)</b>	Pesquise dispositivos ativos no sistema com propriedades de dispositivos permanecendo as mesmas desde a última auditoria.
<b>Impressoras gerenciadas (Alteradas)</b>	Pesquise dispositivos ativos no sistema com propriedades de dispositivos que mudaram desde a última auditoria.
<b>Impressoras gerenciadas (Ausentes)</b>	Pesquise dispositivos com os quais o sistema não conseguiu estabelecer comunicação.
<b>Impressoras gerenciadas (Encontradas)</b>	Pesquise dispositivos que são relatados como ausentes de consultas de pesquisa anteriores, mas que agora foram encontrados.
<b>Novas impressoras</b>	Pesquise dispositivos que foram recentemente adicionados ao sistema.
<b>Impressoras não gerenciadas</b>	Pesquise dispositivos que foram marcados para exclusão das atividades executadas no sistema.
<b>Impressoras desativadas</b>	Pesquise dispositivos que não estão mais ativos no sistema.

- 2 Na área de Resumo de resultados da pesquisa, selecione um critério para refinar os resultados de sua pesquisa com marcador rápida e facilmente.

### Uso da pesquisa avançada

O recurso Pesquisa avançada permite que você execute pesquisas complexas rapidamente baseadas em um ou em vários parâmetros.

- 1 No menu suspenso Marcadores e pesquisas, selecione **Pesquisa avançada**.
- 2 Selecione se todos ou pelo menos um critério devem ser atendidos.

### 3 Para adicionar um critério de pesquisa, clique em **+**.

Para agrupar critérios de pesquisa, clique em **[+]** e, em seguida, clique em **+** para adicionar um critério individual.

**Nota:** Se você agrupar os critérios de pesquisa, então o sistema trata todos os critérios definidos que são agrupados em um critério.

### 4 No menu suspenso Parâmetro, selecione um parâmetro:

Selecione	Para
<b>Etiqueta de ativo</b>	Pesquise dispositivos que possuem uma etiqueta do ativo atribuída.
<b>Recurso Cor</b>	Pesquise dispositivos por sua capacidade de imprimir em cores.
<b>Localização do contato</b>	Pesquise dispositivos que possuem uma localização especificada.
<b>Nome do contato</b>	Pesquise dispositivos que possuem um nome do contato especificado.
<b>Recurso Copiar</b>	Pesquise dispositivos por sua capacidade de copiar arquivos.
<b>Recurso Frente e verso</b>	Pesquise dispositivos por sua capacidade de executar impressão frente e verso.
<b>Recurso eSF</b>	Pesquise dispositivos por sua capacidade de gerenciar um aplicativo Estrutura de Soluções Incorporadas (eSF).
<b>Aplicativo eSF (Nome)</b>	Pesquise dispositivos por seu nome específico do aplicativo eSF atualmente instalado.
<b>Aplicativo eSF (Estado)</b>	Pesquise dispositivos pelo estado atual de seu aplicativo eSF instalado.
<b>Aplicativo eSF (Versão)</b>	Pesquise dispositivos pela versão de seu aplicativo eSF instalado.
<b>Versão do firmware</b>	Pesquise dispositivos por sua versão do firmware.
<b>Firmware:AIO</b>	Pesquise dispositivos pelo valor AIO de seu firmware.
<b>cartão de firmware</b>	Pesquise dispositivos pela versão de base de seu firmware.
<b>Firmware:Mecanismo</b>	Pesquise dispositivos pelo mecanismo de seu firmware.
<b>Firmware:Fax</b>	Pesquise dispositivos pelo valor de fax de seu firmware.
<b>Firmware:Fonte</b>	Pesquise dispositivos pelo valor da fonte de seu firmware.
<b>Firmware:Kernel</b>	Pesquise dispositivos pelo valor de kernel de seu firmware.
<b>Firmware:Carregador</b>	Pesquise dispositivos pelo valor do carregador de seu firmware.
<b>Firmware:Rede</b>	Pesquise dispositivos pelo valor de rede de seu firmware.
<b>Firmware:Driver da rede</b>	Pesquise dispositivos pelo valor de driver de rede de seu firmware.
<b>Firmware:Painel</b>	Pesquise dispositivos pela versão do painel de seu firmware.
<b>Firmware:Scanner</b>	Pesquise dispositivos pela versão do scanner de seu firmware.
<b>Nome do host</b>	Pesquise dispositivos por seus nomes do host.
<b>Endereço IP</b>	<p>Pesquise dispositivos por seus endereços IP.</p> <p><b>Nota:</b> Você pode usar um asterisco (*) como curinga nos últimos três octetos do endereço IP para achar todos os endereços IP correspondentes. Se um asterisco é usado como um octeto, os outros octetos têm de conter asteriscos também.</p> <ul style="list-style-type: none"> <li>Exemplos válidos são 157 . 184 . 32 . *, 157 . 184 . * . * e 157 . * . * . *</li> <li>Um exemplo inválido é 157 . 184 . * . 10.</li> </ul>
<b>Palavra-chave</b>	Pesquise dispositivos por suas palavras-chave atribuídas, se houver.
<b>Total de páginas já impressas</b>	Pesquise dispositivos por seus valores de total de páginas já impressas.

Selecione	Para
<b>Endereço MAC</b>	Pesquise dispositivos por seus endereços MAC.
<b>Contador de manutenção</b>	Pesquise dispositivos pelo valor de rede de seu contador de manutenção.
<b>Fabricante:</b>	Pesquise dispositivos pelo nome de seu fabricante.
<b>Recurso MFP</b>	Pesquise dispositivos por sua capacidade de ser uma impressora multifuncional (MFP).
<b>Tecnologia de marcação</b>	Pesquise dispositivos pelo valor da tecnologia de marcação que suportam.
<b>Model</b>	Pesquise dispositivos por seus nomes de modelo.
<b>Status da impressora</b>	Pesquise dispositivos por seu status atual (por exemplo: <b>Pronto, Atolamento de papel, Bandeja 1 ausente</b> ).
<b>Recurso Perfil</b>	Pesquise dispositivos por sua capacidade de perfil suportada.
<b>Recurso Receber fax</b>	Pesquise dispositivos por sua capacidade de receber fax.
<b>Recurso Digitalizar para e-mail</b>	Pesquise dispositivos por sua capacidade de executar uma tarefa Digitalizar para e-mail.
<b>Recurso Digitalizar para fax</b>	Pesquise dispositivos por sua capacidade de executar uma tarefa Digitalizar para fax.
<b>Recurso Digitalizar para rede</b>	Pesquise dispositivos por sua capacidade de executar uma tarefa Digitalizar para rede.
<b>Número de série</b>	Pesquise dispositivos por seu número de série.
<b>Estado</b>	Pesquise dispositivos por seu estado atual no banco de dados.
<b>Status dos suprimentos</b>	Pesquise dispositivos pelo status atual de seus suprimentos.
<b>Nome de sistema</b>	Pesquise dispositivos por seus nomes de sistema.

5 No menu suspenso Operação, selecione um operador:

Selecione	Para
<b>Contém</b>	Pesquise dispositivos com um parâmetro que contenha um valor específico.
<b>Não contém</b>	Pesquise dispositivos com um parâmetro que não contenha um valor específico.
<b>Diferente de</b>	Pesquise dispositivos com um parâmetro que não seja equivalente a um valor exato.
<b>Termina com</b>	Pesquise dispositivos com um parâmetro que termine com um valor específico.
<b>Igual a</b>	Pesquise dispositivos com um parâmetro que seja equivalente a um valor exato.
<b>Inicia com</b>	Pesquise dispositivos com um parâmetro que inicie com um valor específico.

6 No campo ou menu suspenso Valor, insira o valor do parâmetro.

**Nota:** Se desejar excluir o critério, clique em **X**.

7 Clique em **OK** para começar a pesquisa.

Os dispositivos localizados aparecem na área de Resultados da pesquisa.


8 Na área de Resumo de resultados da pesquisa, selecione um critério para refinar os resultados de sua pesquisa com marcador rápida e facilmente.

## Trabalho com marcadores

Marcadores indicam uma pesquisa salva.

Quando um dispositivo entra no sistema e atende aos critérios especificados para um marcador, o dispositivo é incluído nos resultados de pesquisa sempre que o marcador for selecionado.

### Criação de marcadores

- 1 No menu suspenso Marcadores e pesquisas, selecione o marcador que representa o grupo de dispositivos a partir dos quais você gostaria de começar sua pesquisa.  
Para refinar a pesquisa, clique em **Pesquisa avançada**.
- 2 Se necessário, em Resumo de resultados da pesquisa, clique nas subcategorias disponíveis para refinar mais a pesquisa.
- 3 Quando o dispositivo ou grupo de dispositivos que você deseja aparecer na janela de pesquisa, clique em  .
- 4 Insira um nome para o marcador e clique em **OK**.

### Acesso a marcadores

- 1 No menu suspenso Marcadores e pesquisas, selecione o marcador que você deseja exibir.
- 2 Se necessário, em Resumo de resultados da pesquisa, clique nas subcategorias disponíveis para refinar mais a pesquisa.

### Exclusão de marcadores

- 1 No menu suspenso Marcadores e pesquisas, selecione **Gerenciar marcadores**.
- 2 Selecione o(s) marcador(es) que deseja excluir e clique em **—**.
- 3 Clique em **Sim** e em **Fechar**.

## Uso de categorias e palavras-chave


Palavras-chave permitem que você atribua marcas personalizadas aos dispositivos, fornecendo flexibilidade adicional ao localizar e organizar dispositivos no sistema. Agrupe palavras-chave em categorias e então atribua várias palavras-chave de diversas categorias a um dispositivo.

Antes que você possa criar uma palavra-chave, primeiro crie uma categoria para a qual a palavra-chave pertença.

Por exemplo, você pode criar uma categoria chamada **Localização** e então criar palavras-chave nessa categoria. Exemplos de palavras-chave na categoria Localização podem ser **Prédio 1**, **Prédio 2** ou algo mais específico para as necessidades de seus negócios.

Após criar as categorias e palavras-chave, você pode atribuir as palavras-chave a vários dispositivos. Você poderá procurar dispositivos com base em palavras-chave atribuídas a eles e então marcar os resultados de sua pesquisa para uso futuro.


## Adição, edição ou exclusão de categorias

- 1 Se necessário, clique em **Palavras-chave** na guia Ativos para exibir a seção Palavras-chave.
- 2 No painel Categoria, clique em **+** para adicionar,  para editar ou **—** para excluir uma categoria.

**Nota:** Excluir uma categoria também exclui suas palavras-chave e as remove dos dispositivos para os quais as palavras-chave são atribuídas.

- 3 Siga as instruções na tela do computador.

## Adição, edição ou exclusão de palavras-chave

- 1 Se necessário, clique em **Palavras-chave** na guia Ativos para exibir a seção Palavras-chave.
- 2 No painel Palavras-chave, execute um dos seguintes procedimentos:
  - Para adicionar uma palavra-chave:
    - a No painel Categoria, selecione uma categoria onde a palavra-chave pertença.
    - b No painel Palavra-chave, clique em **+**.
    - c Digite o nome da nova palavra-chave e pressione **Enter**.
  - Para editar uma palavra-chave:
    - a Selecione uma palavra-chave existente e clique em .
    - b Edite o nome e, em seguida, pressione **Enter**.
  - Para excluir uma palavra-chave:
    - a Selecione uma palavra-chave existente e clique em **—**.
    - b Clique em **Sim**.

**Nota:** Excluir uma palavra-chave a remove dos dispositivos para os quais ela é atribuída.

## Atribuição de palavras-chave a um dispositivo

- 1 Se necessário, clique em **Palavras-chave** na guia Ativos para exibir a seção Palavras-chave e selecione uma palavra-chave.

**Nota:** Para selecionar várias palavras-chave, use **Shift + clique** ou **Ctrl + clique**.

- 2 Marque a caixa de seleção ao lado do endereço IP do dispositivo onde você deseja atribuir à palavra-chave.

**Nota:** Você pode selecionar vários ou todos os dispositivos.


- 3 Clique em .

- 4 Na área de Informações da tarefa, verifique se a tarefa está concluída.

- 5 Para verificar se a palavra-chave foi atribuída com sucesso ao dispositivo, veja as propriedades do dispositivo ao selecionar o endereço IP do dispositivo.

Na seção Propriedade da identificação, o novo valor da palavra-chave para o dispositivo aparece.

## Remoção de uma palavra-chave atribuída de um dispositivo

- 1** Na guia Ativos, marque a caixa de seleção ao lado do endereço IP do dispositivo do qual deseja remover uma palavra-chave.
- 2** Se necessário, clique em **Palavras-chave** para exibir a seção Palavras-chave.
- 3** Selecione uma palavra-chave e clique em .
- 4** Selecione a palavra-chave que deseja remover e clique em **OK**.  
**Nota:** Para selecionar várias palavras-chave, use **Shift + clique** ou **Ctrl + clique**.
- 5** Na área de Informações da tarefa, verifique se a tarefa está concluída.
- 6** Para verificar se a palavra-chave foi removida com sucesso do dispositivo, faça o seguinte:
  - a** Selecione o endereço IP do dispositivo.
  - b** Na seção Propriedade da identificação, certifique-se de que a palavra-chave não aparece mais.

# Gerenciamento de políticas

Uma política é um conjunto de informações de configuração que podem ser atribuídas a um dispositivo ou a um grupo de dispositivos do mesmo modelo. Verifique se as informações de configuração para um dispositivo ou um grupo de dispositivos correspondem à política específica executando uma verificação de conformidade. Se a verificação de conformidade indicar que o dispositivo não está em conformidade com a política, então você poderá escolher aplicar a política no dispositivo ou no grupo de dispositivos.

Crie políticas por um tipo funcional predefinido:

- Cópia
- Email/FTP
- Fax
- Unidade flash
- Firmware
- Geral
- Rede
- Papel
- Imprimir
- Segurança

**Nota:** Para obter mais informações sobre a política de segurança, consulte “Entendimento da política de segurança” na página 32.

Cada tipo de política contém configurações exclusivas que garantem que configurações conflitantes não ocorram ao atribuir vários tipos de políticas a um dispositivo.

## Criação de uma política

### Criação de uma nova política

**1** Se necessário, na guia Políticas, clique em **Políticas do dispositivo** para exibir a seção Políticas do dispositivo.

**2** Clique em **+** e digite o nome da nova política.

**Nota:** Certifique-se de que o nome da política para cada modelo do dispositivo seja único e ainda não exista no banco de dados.

**3** Na lista Modelos suportados, selecione um dispositivo.

**4** Do menu suspenso Tipo, selecione um tipo de política e clique em **OK**.

**5** Na caixa de diálogo Nova política, marque a caixa de seleção **Nome da configuração**.

Todas as configurações são selecionadas automaticamente, permitindo que você personalize cada configuração.


**6** Desmarque a caixa de seleção ao lado de uma configuração para *excluí-la* ao executar uma verificação de conformidade com a política ou tarefa de aplicação de política.

**7** Selecione um valor para cada configuração que você deseja incluir ao executar uma verificação de conformidade com a política ou tarefa de aplicação de política.

**8** Clique em **Salvar**.

## Criação de uma política de um dispositivo

**1** Na guia Políticas, marque a caixa de seleção ao lado do endereço IP do dispositivo.


**2** Clique em **Políticas do dispositivo** para exibir a seção Políticas do dispositivo e clique em .

**3** No campo Nome, digite o nome da nova política.

**4** Selecione o tipo de política e clique em **OK**.

**Nota:** Você pode selecionar também vários ou todos os tipos de política.

**5** Se necessário, edite as configurações da política criada recentemente.

**a** Na seção Políticas do dispositivo, selecione o nome da política criada recentemente e clique em .

**b** Selecione um valor para cada configuração que você deseja incluir ao executar uma verificação de conformidade com a política ou tarefa de aplicação de política.

**c** Desmarque a caixa de seleção ao lado de uma configuração para *excluí-la* ao executar uma verificação de conformidade com a política ou tarefa de aplicação de política.

**d** Clique em **Salvar**.

**6** Certifique-se de que as configurações na política criada recentemente contenham valores válidos.

Se a política aparecer em texto em vermelho e seu nome começar com um ponto de exclamação, então ela não poderá ser atribuída a um dispositivo. Isso significa que uma ou mais configurações na política contêm um valor inválido e, portanto, não podem ser aplicadas em um dispositivo em seu estado atual.

Para tornar uma política atribuível a um dispositivo, faça o seguinte:

**a** Selecione a política e clique em .

**b** Insira um valor válido para as configurações e clique em **Salvar**.

**c** Se uma mensagem de aviso aparecer, então anote as configurações com valores inválidos.

**d** Clique em **Não** e insira um valor válido para cada uma das configurações especificadas.

**e** Clique em **Salvar**.

**f** Se necessário, repita de etapa c a etapa e até que a mensagem de aviso não apareça mais.

## Entendimento da política de segurança

O Markvision pode definir a configuração de dispositivos Lexmark ativados por segurança, incluindo as definições de segurança das várias funções de dispositivo, assim como o modo como a comunicação remota é realizada.

Ao usar a política de segurança, certifique-se de usar *somente* o Markvision para gerenciar as definições de segurança nos dispositivos. Se você estiver usando algum outro sistema junto com o Markvision, isto pode resultar em um comportamento inesperado.

A política de segurança pode ser atribuída somente a um subconjunto específico de dispositivos. Para ver a lista completa de dispositivos suportados, consulte “Impressoras Lexmark que suportam a política de segurança” na página 60.

## Compreensão dos dispositivos protegidos

Podem existir várias configurações para um dispositivo protegido. Porém, atualmente o Markvision suporta apenas dispositivos que são *completamente sem restrições* ou *completamente restritos*.

### Configurações para dispositivos completamente sem restrições e completamente restritos

		Completamente sem restrições	Completamente restrito
Definições do dispositivo	Controle de acesso da função de gerenciamento remoto (RM FAC) ou senha avançada  <b>Nota:</b> Para obter uma lista de dispositivos que suportam RM FAC, consulte “Impressoras Lexmark que suportam a política de segurança” na página 60.	Sem segurança ou sem senha	RM FAC é definido usando um modelo de segurança ou uma senha é configurada
	Portas significativas	As seguintes portas ficam abertas: <ul style="list-style-type: none"> <li>• UDP 161 (SNMP)</li> <li>• UDP 9300/9301/9302 (NPAP)</li> </ul>	Encerrado
	Portas relacionadas à segurança	As seguintes portas ficam abertas: <ul style="list-style-type: none"> <li>• UDP 5353 (mDNS)</li> <li>• TCP 6110</li> <li>• TCP/UDP 6100 (LST)</li> </ul>	As seguintes portas ficam abertas: <ul style="list-style-type: none"> <li>• UDP 5353 (mDNS)</li> <li>• TCP 6110</li> <li>• TCP/UDP 6100 (LST)</li> </ul>

		Completamente sem restrições	Completamente restrito
Definições do MarkVision	Perfil de localização	Verifique se a opção <b>Incluir impressoras seguras na localização</b> foi desmarcada.	Verifique se a opção <b>Incluir impressoras seguras na localização</b> foi selecionada.
	Os canais de segurança são usados para comunicação entre o Markvision e os dispositivos de rede?	Não <b>Notas:</b> <ul style="list-style-type: none"> <li>Este tipo de configuração é recomendada, a não ser que você esteja particularmente preocupado com a segurança de sua comunicação de rede.</li> <li>Uma exceção a isso é se existem determinadas definições que podem ser lidas/gravadas <i>somente</i> por meio de canais seguros.</li> </ul>	Sim
	Como determino a configuração de segurança dos dispositivos em minha rede?	Na grade de dados do Markvision, um ícone de cadeado <i>aberto</i> é exibido ao lado do endereço IP de um dispositivo completamente sem restrições.	Na grade de dados principal do Markvision, um ícone de cadeado <i>fechado</i> é exibido ao lado do endereço IP de um dispositivo completamente restrito. <b>Nota:</b> Se o Markvision não conhecer as credenciais de comunicação do dispositivo, o ícone de cadeado fechado terá uma barra vermelha em cima. Isto significa que o Markvision não pode se comunicar naquele momento, além desta localização mínima, com o dispositivo.
	Como procuro dispositivos que têm este tipo de configuração?	<ol style="list-style-type: none"> <li>Na área "Marcadores e Pesquisa avançada", selecione <b>Todas as impressoras</b>.</li> <li>Na área de Resumo de resultados da pesquisa, role para baixo até a categoria Comunicações e selecione <b>Não seguro</b>.</li> </ol>	<ol style="list-style-type: none"> <li>Na área "Marcadores e Pesquisa avançada", selecione <b>Todas as impressoras</b>.</li> <li>Na área de Resumo de resultados da pesquisa, role para baixo até a categoria Comunicações e selecione <b>Seguro</b>.</li> </ol>

**Notas:**

- Se o dispositivo ou perfil de localização não aderir a um desses cenários, provavelmente existirá um comportamento inesperado ou indefinido.
- Verifique se o dispositivo está no estado correto e o perfil de localização está configurado corretamente *antes* de localizar o dispositivo. A mudança em um ou outro após a execução do perfil de localização provavelmente resultará em um comportamento inesperado ou indefinido.

**Compreensão das definições de políticas de segurança**

Use a política de segurança para personalizar as definições de segurança de um dispositivo de rede.

Para que o Markvision realize funções de gerenciamento remoto com eficiência em um dispositivo de rede, certifique-se de que a política de segurança segue os seguintes parâmetros:

- Na seção Definições gerais da política de segurança, as configurações de acesso de porta a seguir são definidas como **Ativado** ou **Seguro e não-seguro**:
  - Acesso à porta: mDNS (UDP 5353)
  - Acesso à porta: TCP/UDP (6110/6100)
- Na seção Controles de acesso (se disponível para o modelo do dispositivo), as configurações Alterações na configuração do adaptador da rede NPA e Atualizações de firmware são definidas para **Sem segurança**.
- As seções a seguir (se disponíveis para o modelo do dispositivo) são somente leitura e não podem ser editadas:
  - Controles de acesso
  - Modelos de segurança
    - Nota:** Os Building blocks sob a coluna Configuração da autenticação podem precisar das credenciais fornecidas.
  - Definições variadas

**Nota:** As seções Controles de acesso, Modelos de segurança e Definições variadas não estão disponíveis para todos os modelos de dispositivos. Para obter mais informações, consulte “Impressoras Lexmark que suportam a política de segurança” na página 60.

## Utilização de building blocks de um aplicativo eSF

Se você quiser usar o building block de um aplicativo Estrutura de Soluções Incorporadas (eSF) para a política de segurança, certifique-se de que o aplicativo eSF foi instalado manualmente em todos os dispositivos afetados. A instalação do aplicativo *não* é aplicada quando o Markvision aplica uma política de segurança.

**Nota:** Apenas as definições internas disponíveis para todos os aplicativos eSF serão clonadas, terão a conformidade verificada ou serão aplicadas pela política de segurança.

## Criação de uma política de segurança

Para criar uma política de segurança, primeiro faça o clone de uma política existente de um dispositivo principal pré-configurado.

## Clonagem de uma política de segurança para dispositivos restritos

### Etapa 1. Configuração de um dispositivo como restrito usando o Servidor da Web incorporado.

Após configurar um dispositivo como restrito, use esse dispositivo como o dispositivo principal que será usado para a criação de um clone para uma política de segurança.

- 1 Se o modelo de dispositivo suportar o controle de acesso de Gerenciamento remoto, defina o controle de acesso para um modelo de segurança existente. Se o dispositivo não suportar o controle de acesso de Gerenciamento remoto, configure uma senha avançada. Execute um dos seguintes procedimentos:

**Nota:** Para obter uma lista de dispositivos que suportam o controle de acesso de Gerenciamento remoto, consulte “Impressoras Lexmark que suportam a política de segurança” na página 60.

### Configurando o controle de acesso de Gerenciamento remoto

- a No Markvision, clique em **Central de serviços**.
- b Localize o dispositivo que deseja configurar e, em seguida, selecione o seu endereço IP.

- c Clique em **Página da Web incorporada >Definições >Segurança >Configuração de segurança**.
- d Na seção Definição avançada de segurança, clique em **Controles de acesso**.
- e Role para Gerenciamento remoto e, no menu suspenso, selecione um modelo de segurança.

**Nota:** O modelo de segurança deve especificar somente a autenticação.

- f Clique em **Enviar**.

### Configurando uma senha avançada

- a No Markvision, clique em **Central de serviços**.
- b Localize o dispositivo que deseja configurar e, em seguida, selecione o seu endereço IP.
- c Clique em **Página da Web incorporada >Configuração >Segurança**.
- d Clique em **Criar/Alterar senha** ou **Criar senha**.
- e Se necessário, clique em **Criar senha avançada** e digite uma senha.
- f Confirme a senha digitando-a novamente no próximo campo e clique em **Enviar**.

- 2 Verifique se as portas significativas estão fechadas e se as portas de segurança estão abertas.

**Nota:** Se aplicável, selecione **Modo de segurança** e pule para a etapa 3.


- a No Embedded Web Server, clique em **Definições** ou **Configuração** e clique em **Segurança >Acesso à porta TCP/IP**.
- b Localize as seguintes portas significativas e, se necessário, desmarque as caixas de seleção ao lado delas ou selecione **Desativado** nos menus suspensos.
  - **UDP 161 (SNMP)**
  - **UDP 9300/9301/9302 (NPAP)**
- c Localize as portas de segurança a seguir e verifique se as caixas de seleção ao lado delas estão selecionadas ou se **Seguro e não-seguro** está selecionado nos menus suspensos.
  - **UDP 5353 (mDNS)**
  - **TCP 6110**
  - **TCP/UDP 6100 (LST)**
- d Clique em **Enviar**.

- 3 Configure outras definições de segurança.

- a No Embedded Web Server, clique em **Definições** ou **Configuração** e clique em **Segurança**.
- b Faça outras alterações nas definições de segurança, de acordo com a necessidade.
- c Depois que fizer outras alterações, clique em **Definições** ou **Configuração** e, em seguida, clique em **Segurança >Exibir resumo de segurança** (se disponível no modelo de dispositivo).
- d Verifique se suas alterações são refletidas na página de resumo.


**Nota:** Se estiver usando uma senha avançada em vez do controle de acesso de Gerenciamento remoto, não será necessário usar o Embedded Web Server para restringir o dispositivo principal. É possível usar o Markvision para criar uma política de segurança de qualquer dispositivo e, em seguida, configurar a Senha avançada e as definições de porta na seção Definições gerais da política.

**Etapa 2. Verifique se o Markvision reconhece o seu dispositivo principal restrito.**

- 1 Crie um perfil de localização. Para obter mais informações sobre a criação de um perfil de localização, consulte “Criando um perfil de localização” na página 18.
- 2 Na caixa de diálogo Perfil de localização – Adicionar, verifique se a opção “Incluir impressoras seguras na localização” está selecionada.
- 3 Para executar o perfil de localização, clique em .

**Nota:** Neste ponto, o dispositivo está "parcialmente descoberto". Isto significa que o Markvision descobriu o dispositivo com informações limitadas, mas não conseguirá realizar funções adicionais com conformidade com a política, aplicação de política e auditoria. Para adquirir as suas informações completas, você precisa fornecer as credenciais de comunicação do dispositivo.


**Etapa 3. Início do processo de clonagem.**

- 1 No Markvision, clique em **Políticas**.
- 2 Localize o seu dispositivo principal restrito e marque a caixa de seleção ao lado do endereço IP.
- 3 Se necessário, clique em **Políticas de dispositivo** e, em seguida, clique em .
- 4 No campo Nome, digite o nome da nova política de segurança.
- 5 Verifique se Tipo de política de segurança foi selecionado.
- 6 Informe as credenciais necessárias para fazer a autenticação com o dispositivo e clique em **OK**.

**Nota:** Use as credenciais do modelo de segurança definidas no Controle de acesso de gerenciamento remoto ou use a senha avançada que você configurou.

- 7 Deixe que o processo de clonagem seja concluído.

Se a política for exibida no texto em vermelho, significa que estão faltando credenciais e, portanto, não pode ser atribuída a um dispositivo em seu estado atual. Para tornar a política atribuível a um dispositivo, informe as credenciais corretas para o dispositivo.

- 8 Edite as definições da nova política de segurança e verifique se as definições na política contêm valores válidos.
  - a Na seção Políticas do dispositivo, selecione o nome da política e clique em .
  - b Selecione um valor para cada definição que quiser incluir ao executar uma verificação de conformidade com a política ou tarefa de aplicação de política.
  - c Desmarque a caixa de seleção ao lado de uma definição para *excluí-la* ao executar uma verificação de conformidade com a política ou tarefa de aplicação de política.
  - d Digite a senha de segurança e clique em **Salvar**.

**Nota:** Para obter mais informações sobre definições válidas para uma política de segurança, consulte “Compreensão das definições de políticas de segurança” na página 33.

- 9 Atribua a política de segurança a dispositivos sem restrições que sejam do mesmo modelo do dispositivo principal restrito.

Para obter mais informações sobre a atribuição de uma política a vários dispositivos, consulte “Atribuição de uma política” na página 40.

**10** Aplique a política de segurança nos dispositivos selecionados.

Para obter mais informações sobre a aplicação de uma política, consulte “Aplicação de uma política” na página 41.

**11** Localize os dispositivos novamente.

Os dispositivos agora estão restritos. Além disso, o Markvision agora conhece as credenciais de comunicação do dispositivo e pode usar essas credenciais para executar tarefas nas áreas de serviço Ativos e Políticas.

## Clonagem de uma política de segurança para dispositivos sem restrições

### Etapa 1. Configuração de um dispositivo sem restrições usando o Servidor da Web incorporado.

Após configurar um dispositivo como sem restrições, use esse dispositivo como o dispositivo principal que será usado para a criação de um clone para uma política de segurança.

- 1 Se o modelo de dispositivo suportar o controle de acesso de Gerenciamento remoto, defina o controle de acesso para **Sem segurança**. Se o dispositivo não suportar o controle de acesso de Gerenciamento remoto, remova a senha avançada. Execute um dos seguintes procedimentos:

**Nota:** Para obter uma lista de dispositivos que suportam o controle de acesso de Gerenciamento remoto, consulte “Impressoras Lexmark que suportam a política de segurança” na página 60.

#### Configurando o controle de acesso de Gerenciamento remoto

- a No Markvision, clique em **Central de serviços**.
- b Localize o dispositivo que deseja configurar e, em seguida, selecione o seu endereço IP.
- c Clique em **Página da Web incorporada >Definições >Segurança >Configuração de segurança**.
- d Na seção Definição avançada de segurança, clique em **Controles de acesso**.
- e Role para **Gerenciamento remoto** e, no menu suspenso, selecione **Sem segurança**.
- f Clique em **Enviar**.

#### Removendo a senha avançada

- a No Markvision, clique em **Central de serviços**.
- b Localize o dispositivo que deseja configurar e, em seguida, selecione o seu endereço IP.
- c Clique em **Página da Web incorporada >Configuração >Segurança**.
- d Clique em **Criar/Alterar senha** ou **Criar senha**.
- e Se necessário, clique em **Criar senha avançada**.
- f Limpe os campos de Senha e, em seguida, clique em **Enviar**.

- 2 Verifique se as portas significativas e as portas de segurança estão abertas.

- a No Embedded Web Server, clique em **Definições** ou **Configuração** e clique em **Segurança >Acesso à porta TCP/IP**.
- b Localize as portas a seguir e verifique se elas estão selecionadas ou definidas como **Seguro e não-seguro**.

Portas significativas

- **UDP 161 (SNMP)**
- **UDP 9300/9301/9302 (NPAP)**

Portas de segurança

- **UDP 5353 (mDNS)**
- **TCP 6110**
- **TCP/UDP 6100 (LST)**


c Clique em **Enviar**.

**3** Configure outras definições de segurança.


- a No Embedded Web Server, clique em **Definições** ou **Configuração** e clique em **Segurança**.
- b Faça outras alterações nas definições de segurança, de acordo com a necessidade.
- c Depois que fizer outras alterações, clique em **Definições** ou **Configuração** e, em seguida, clique em **Segurança >Exibir resumo de segurança** (se disponível no modelo de dispositivo).
- d Verifique se suas alterações são refletidas na página de resumo.

**Nota:** Se estiver usando uma senha avançada em vez do controle de acesso de Gerenciamento remoto, não será necessário usar o Embedded Web Server para deixar o dispositivo principal sem restrições. É possível usar o Markvision para criar uma política de segurança de qualquer dispositivo e, em seguida, configurar a Senha avançada e as definições de porta na seção Definições gerais da política.

**Etapa 2. Verifique se o Markvision reconhece o seu dispositivo principal sem restrições.**

- 1** Crie um perfil de localização. Para obter mais informações sobre a criação de um perfil de localização, consulte "Criando um perfil de localização" na página 18.
- 2** Na caixa de diálogo "Perfil de localização – Adicionar", verifique se a caixa de seleção **Incluir impressoras seguras na localização** foi desmarcada.
- 3** Para executar o perfil de localização, clique em .

**Etapa 3. Início do processo de clonagem.**


- 1** No Markvision, clique em **Políticas**.
- 2** Localize o seu dispositivo sem restrições e marque a caixa de seleção ao lado do endereço IP.
- 3** Se necessário, clique em **Políticas de dispositivo** e, em seguida, clique em .
- 4** No campo Nome, digite o nome da nova política de segurança.
- 5** Verifique se Tipo de política de segurança foi selecionado.
- 6** Informe as credenciais necessárias para fazer a autenticação com o dispositivo e clique em **OK**.

**Nota:** Use as credenciais do modelo de segurança definidas no Controle de acesso de gerenciamento remoto ou use a senha avançada que você configurou.

**7** Deixe que o processo de clonagem seja concluído.

Se a política for exibida no texto em vermelho, significa que estão faltando credenciais e, portanto, não pode ser atribuída a um dispositivo em seu estado atual. Para tornar a política atribuível a um dispositivo, informe as credenciais corretas para o dispositivo.

**8** Edite as definições da nova política de segurança e verifique se as definições na política contêm valores válidos.

- a Na seção Políticas do dispositivo, selecione o nome da política e clique em .
- b Selecione um valor para cada definição que quiser incluir ao executar uma verificação de conformidade com a política ou tarefa de aplicação de política.

- c Desmarque a caixa de seleção ao lado de uma definição para *excluí-la* ao executar uma verificação de conformidade com a política ou tarefa de aplicação de política.
- d Clique em **Salvar**.

**Nota:** Para obter mais informações sobre definições válidas para uma política de segurança, consulte “Compreensão das definições de políticas de segurança” na página 33.

- 9 Atribua a política de segurança a dispositivos sem restrições que sejam do mesmo modelo do dispositivo principal sem restrições.

**Notas:**

- Para obter mais informações sobre a atribuição de uma política a vários dispositivos, consulte “Atribuição de uma política” na página 40.
- Se um dos dispositivos selecionados estiver restrito, ele ficará sem restrições depois da aplicação da política.

- 10 Aplique a política de segurança nos dispositivos selecionados.

Para obter mais informações sobre a aplicação de uma política, consulte “Aplicação de uma política” na página 41.

- 11 Localize os dispositivos novamente.

Os dispositivos agora estão sem restrições e podem ser usados por todas as áreas de serviço.

## Alteração das credenciais de comunicação de um dispositivo restrito

*Credenciais de comunicação* são necessárias para autenticação com um dispositivo de rede através do Lexmark Secure Transport (LST). As credenciais de comunicação podem ser uma combinação de qualquer um dos seguintes itens abaixo: nome de usuário, domínio, senha e *número de identificação pessoal* (PIN).


**Nota:** Alguns modelos de dispositivo suportam somente senhas. Para obter mais informações, consulte “Impressoras Lexmark que suportam a política de segurança” na página 60.

Existem dois tipos de building blocks de credenciais de comunicação:

- **Autoridade final** — O building block é a autoridade final quando se trata de autenticação ou autorização de credencial. Alguns exemplos de senhas ou PINs.
- **Autoridade de passagem** — O building block passa as credenciais junto com uma autoridade externa para autenticação ou autorização. Alguns exemplos de uma autoridade externa são o Lightweight Directory Access Protocol (LDAP) e Kerberos.


### Alteração das credenciais de um bulding block de autoridade final

**Nota:** As opções de política de segurança Controles de acesso e Modelos de segurança não estão disponíveis para todos os modelos de dispositivos. Para obter mais informações, consulte “Impressoras Lexmark que suportam a política de segurança” na página 60.



- 1 Se necessário, na guia Políticas, clique em **Políticas do dispositivo** para exibir a seção Políticas do dispositivo.
- 2 Selecione a política de segurança restrita desejada e clique em  **>Controles de acesso**.
- 3 Localize o **Gerenciamento remoto** e anote o seu valor.
- 4 Clique em **Modelos de segurança**.
- 5 Na coluna Configuração da autenticação, selecione o building block ao lado do valor anotado na etapa 3.

- 6 No campo Senha, digite a nova senha.
- 7 Confirme a senha digitando-a novamente no próximo campo e clique em **Salvar**.
- 8 Aplique a política de segurança restrita em seus dispositivos atribuídos.  
Quando a tarefa de aplicação for concluída com sucesso, as credenciais de comunicação com o dispositivo serão atualizadas.

### Alteração das credenciais de um bulding block de autoridade de passagem

- 1 Na autoridade externa que você estiver usando, faça as alterações nas credenciais.
- 2 Na página do MarkVision na Web, clique em **Políticas >Políticas do dispositivo** para exibir a seção Políticas do dispositivo.
- 3 Selecione a política de segurança restrita desejada e clique em  **>Credenciais do dispositivo**.
- 4 Na seção Credenciais do dispositivo, atualize os valores atuais pelos novos valores informados na autoridade externa.
- 5 Clique em **Salvar**.
- 6 Aplique a política de segurança restrita em seus dispositivos atribuídos.  
Quando a tarefa de aplicação for concluída com sucesso, o Markvision poderá se comunicar com os dispositivos novamente.

## Edição ou exclusão de uma política

- 1 Se necessário, clique em **Políticas do dispositivo** na guia Políticas para exibir a seção Políticas do dispositivo.
- 2 Selecione uma política e execute um dos seguintes procedimentos:
  - Para editar a política, cliquem em  .
    - a No campo Nome da política, digite o novo nome da política, se aplicável.
    - b Selecione um valor para cada configuração que desejar incluir ao executar uma verificação de conformidade com a política ou tarefa de aplicação de política.
    - c Desmarque a caixa de seleção ao lado de uma configuração para *excluí-la* ao executar uma verificação de conformidade com a política ou tarefa de aplicação de política.
    - d Clique em **Salvar**.
  - Para excluir a política, clique em  e, em seguida, clique em **Sim**.

## Atribuição de uma política


- 1 Se necessário, clique em **Políticas do dispositivo** na guia Políticas para exibir a seção Políticas do dispositivo.
- 2 Selecione uma política.

### Notas:

- Para selecionar várias políticas, use **Shift + clique** ou **Ctrl + clique**.
- Você pode atribuir vários tipos de políticas a um dispositivo ao mesmo tempo, mas pode usar apenas uma política para cada tipo de política.

3 Marque a caixa de seleção ao lado do endereço IP do dispositivo para o qual deseja atribuir a política.

**Nota:** Você pode selecionar também vários ou todos os dispositivos.

4 Clique em .

Na coluna Tipo de política, um ponto de interrogação aparece ao lado do dispositivo que você selecionou.

O ponto de interrogação indica que o dispositivo ainda não está verificado para estar em conformidade com a política atribuída.

## Verificação da conformidade com uma política


1 Na guia Políticas, marque a caixa de seleção ao lado do endereço IP do dispositivo.

**Nota:** Você pode selecionar também vários ou todos os dispositivos.

2 Clique em **Conformidade**.

3 Na caixa de diálogo Políticas de verificação de conformidade, selecione um tipo de política e clique em **OK**.

4 Na coluna Tipo de política, verifique se uma marca de verificação aparece ao lado do dispositivo que você selecionou.

5 Se aparecer um ponto de interrogação ou X, então clique em  para visualizar os detalhes específicos.

**Nota:** Uma verificação da conformidade com uma política pode ser programada para que ocorra em um momento predeterminado ou regularmente. Para obter mais informações, consulte “Tarefas de programação” na página 55.


## Aplicação de uma política

1 Na guia Políticas, marque a caixa de seleção ao lado do endereço IP do dispositivo.

**Nota:** Você pode selecionar também vários ou todos os dispositivos.

2 Clique em **Aplicar**.


3 Na caixa de diálogo Aplicar políticas, selecione um tipo de política e clique em **OK**.

4 Clique em  para verificar se a política foi aplicada.

**Nota:** Uma tarefa de aplicação da política pode ser programada para que ocorra em um momento predeterminado ou regularmente. Para obter mais informações, consulte “Tarefas de programação” na página 55.

## Remoção de uma política

1 Na guia Políticas, marque a caixa de seleção ao lado do endereço IP do dispositivo.

2 Se necessário, clique em **Políticas do dispositivo** para exibir a seção Políticas do dispositivo e clique em .

3 Na caixa de diálogo Remover política, selecione uma política e clique em **OK**.


**Nota:** Você pode selecionar também várias políticas.

# Gerenciamento da Central de serviços


## Trabalho com políticas

Antes de tentar solucionar um problema em um dispositivo, primeiro verifique se o dispositivo está em conformidade com suas políticas atribuídas.

### Verificação da conformidade do dispositivo com as políticas

- 1 Na guia Central de serviços, marque a caixa de seleção ao lado do endereço IP do dispositivo.  
**Nota:** Você pode selecionar também vários ou todos os dispositivos.
- 2 Clique em **Conformidade**.
- 3 Na caixa de diálogo Políticas de verificação de conformidade, selecione um tipo de política e clique em **OK**.
- 4 Aguarde a conclusão da tarefa na área de informações da tarefa.
- 5 Clique em  para ver os resultados da verificação de conformidade.




### Aplicação de políticas

- 1 Na guia Central de serviços, marque a caixa de seleção ao lado do endereço IP do dispositivo.  
**Nota:** Você pode selecionar também vários ou todos os dispositivos.
- 2 Clique em **Aplicar**.
- 3 Na caixa de diálogo Aplicar políticas, selecione um tipo de política e clique em **OK**.
- 4 Aguarde a conclusão da tarefa na área de informações da tarefa.
- 5 Clique em  para verificar se a política foi aplicada.

## Trabalho com um dispositivo

### Verificação do status de um dispositivo

- 1 Localize um dispositivo usando Marcadores ou Pesquisa avançada.  
**Nota:** Você pode usar as categorias na área de Resumo de resultados de pesquisa para restringir a lista de dispositivos encontrados.
- 2 Marque a caixa de seleção ao lado do endereço IP do dispositivo e clique em **Coletar status atual**.
- 3 Nas colunas Status da impressora e Status dos suprimentos, observe o ícone ao lado do dispositivo.

Ícone	status
	<b>OK</b> – O dispositivo está pronto e os suprimentos são suficientes.
	<b>Aviso</b> – O dispositivo está funcionando, mas os suprimentos podem estar baixos ou podem requerer atenção em um momento posterior.
	<b>Erro</b> – O dispositivo ou os suprimentos precisam de atenção imediata.

4 Clique em **Trabalhar com dispositivo** para ver os detalhes sobre o status do dispositivo.

## Exibição de um dispositivo, remotamente

**Nota:** Esse recurso está disponível somente para dispositivos que suportam a visualização remota.

1 Na guia Central de serviços, marque a caixa de seleção ao lado do endereço IP do dispositivo.

2 Clique em **Trabalhar com dispositivo**.

Uma caixa de diálogo aparece, exibindo os detalhes e uma imagem do dispositivo.

3 Clique em **Painel do operador remoto > Clique aqui para continuar**.

Aparece outra caixa de diálogo, mostrando remotamente uma exibição dinâmica do painel de controle do dispositivo em seu estado atual.

4 No lado inferior esquerdo, consulte a chave do teclado equivalente para cada um dos comandos do botão do dispositivo.

**Nota:** A localização da chave do teclado equivalente pode ser diferente dependendo do modelo do dispositivo.

## Exibição da página da Web incorporada

**Nota:** Esse recurso está disponível somente para dispositivos que suportam visualização remota de sua página da Web incorporada.

1 Na guia Central de serviços, marque a caixa de seleção ao lado do endereço IP do dispositivo.

2 Clique em **Trabalhar com dispositivo**.

Uma caixa de diálogo aparece, mostrando os detalhes e uma imagem do dispositivo.

3 Clique em **Página da Web incorporada**.

**Nota:** Na parte inferior da caixa de diálogo, você pode selecionar também o idioma que deseja usar.

## Gerenciamento de eventos de dispositivo

O Gerenciador de eventos permite que você monitore e gerencie sua frota de impressoras de forma pró-ativa. Defina um destino para notificar você ou outros usuários especificados sobre a ocorrência de um determinado incidente. Crie um evento automatizado quando um dispositivo enviar um alerta para a rede.

### Criação de um destino


Destino é uma ação predefinida que executa um comando definido caso ocorra um evento especificado em um grupo de dispositivos. O destino pode ser uma notificação por e-mail ou um prompt de linha de comando usado quando é necessária uma ação personalizada.



- 1 Se necessário, clique em **Destinos** na guia Gerenciador de eventos para mostrar a seção de destinos.
- 2 Clique em **+** e insira um nome exclusivo para o destino.
- 3 Execute um dos seguintes procedimentos:
  - Selecione **Comando** e clique em **Avançar**.
    - a Insira o nome de um comando executável na caixa Caminho do comando.
    - b Adicione palavras-chave aos parâmetros de comando selecionando uma palavra-chave na lista Espaços reservados. Clique em **▶**.
  - Selecione **E-mail** e clique em **Avançar**.
    - a Verifique na caixa de diálogo Configuração do sistema se você definiu corretamente as configurações de e-mail. Para obter mais informações, consulte “Configurando as definições de e-mail” na página 47.
    - b Insira os valores nos campos apropriados:
      - **De** — Insira o endereço de e-mail do remetente.
      - **Para** — Insira o endereço de e-mail do destinatário.
      - **CC** — Insira os endereços de e-mail dos outros destinatários que receberão uma cópia da mensagem.
      - **Assunto** — Insira um título para o assunto caso deseje que a mensagem de e-mail contenha um assunto.
      - **Corpo** — Insira a mensagem de e-mail.

**Nota:** Na coluna Espaços reservados, você pode usar os *espaços reservados* disponíveis como parte do título do assunto ou como o título do assunto inteiro. Você também pode usar os espaços reservados como parte de uma mensagem de e-mail. Os espaços reservados são elementos variáveis que, quando usados, são substituídos pelo valor real.

- 4 Clique em **Concluir**.

### Edição ou exclusão de um destino


- 1 Se necessário, clique em **Destinos** na guia Gerenciador de eventos para mostrar os destinos ativos.
- 2 Selecione um destino e:
  - Para editar o destino, clique em  .
    - a Se necessário, edite o nome do destino e clique em **Avançar**.
    - b Se necessário, edite o nome do comando executável na caixa Caminho do comando.

- c Para excluir uma palavra-chave da caixa Parâmetros de comando, clique duas vezes na palavra-chave e pressione **Excluir**.
- d Para adicionar mais palavras-chave aos parâmetros de comando, selecione uma palavra-chave na lista Espaços reservados e clique em .
- Para excluir o destino, clique em  e **Sim**.

**Aviso—Dano Potencial:** Quando um destino é excluído, os eventos associados a ele também são excluídos.

3 Clique em **Concluir**.



## Criação de um evento

- 1 Se necessário, clique em **Eventos** na guia Gerenciador de eventos para mostrar a seção de eventos.
- 2 Clique em  e insira um nome exclusivo para o evento e sua descrição.
- 3 Na seção Alertas, selecione um alerta e clique em **Avançar**.


**Nota:** Você pode selecionar vários ou todos os alertas.

- 4 Selecione um destino e:
  - Para acionar o evento quando o alerta está ativo, selecione **Apenas quando ativo**.
  - Para acionar o evento quando o alerta está ativo e limpo, selecione **Quando ativo e limpo**.
- 5 Clique em **Concluir**.


## Edição ou exclusão de um evento

- 1 Se necessário, clique em **Eventos** na guia Gerenciador de eventos para mostrar os eventos ativos.
- 2 Selecione um destino e:
  - Para editar o evento, clique em 
    - a Se necessário, edite o nome e a descrição do evento.
    - b Na seção Alertas, adicione outros alertas selecionando-os ou remova um alerta desmarcando a caixa de seleção ao lado dele.
    - c Clique em **Avançar**.
    - d Na seção Destinos, adicione outros destinos selecionando-os ou remova um destino desmarcando a caixa de seleção ao lado dele.
    - e Selecione um destino de acionamento e clique em **Concluir**.
  - Para excluir o evento, clique em  e **Sim**.

## Atribuição de um evento a um dispositivo

- 1 Na guia Gerenciador de eventos, marque a caixa de seleção ao lado do endereço IP do dispositivo.
- 2 Se necessário, clique em **Eventos** para mostrar os eventos ativos.
- 3 Selecione um evento e clique em .

## Remoção de um evento de um dispositivo

- 1 Na guia Gerenciador de eventos, marque a caixa de seleção ao lado do endereço IP do dispositivo.
- 2 Se necessário, clique em **Eventos** para mostrar os eventos ativos.
- 3 Selecione um evento e clique em .


## Exibição de detalhes de eventos

- 1 Na guia Gerenciador de eventos, localize um dispositivo usando Marcadores ou pesquisa Avançada.  
**Nota:** Você pode usar as categorias na área de Resumo de resultados de pesquisa para restringir a lista de dispositivos encontrados.
- 2 Na área Resultados da pesquisa, marque a caixa de seleção ao lado do endereço IP de um dispositivo.  
**Nota:** Caso não saiba o endereço IP do dispositivo, localize o dispositivo na coluna Nome do sistema.
- 3 Clique em **Propriedades**.  
Uma caixa de diálogo aparece, mostrando as condições ativas atuais e os detalhes de eventos atribuídos ao dispositivo.

# Execução de outras tarefas administrativas

## Download de arquivos genéricos

O aplicativo permite que você carregue arquivos diversos do Servidor do Markvision para um ou mais dispositivos em uma rede. Isso permite a distribuição instantânea de vários tipos de arquivos, incluindo *arquivos de configuração universal* (UCF) para os dispositivos que o aplicativo gerencia.


- 1 Na área do cabeçalho, clique em .
- 2 No menu suspenso Incluir impressoras, selecione um grupo de dispositivos ou um marcador disponível.
- 3 Clique em **Procurar** e navegue até a pasta onde o arquivo está salvo.
- 4 Selecione o arquivo que você deseja carregar e clique em **Abrir**.
- 5 No menu suspenso Destino, selecione um dos seguintes:
  - **Configuração (HTTP)** – Isso carrega um UCF da impressora.
  - **Configuração (FTP)** – Isso carrega um UCF da rede.
  - **Atualização de firmware** – Isso carrega uma atualização de firmware para os dispositivos.
  - **Imprimir (FTP)** – Isso carrega um arquivo imprimível em uma rede FTP.
  - **Imprimir (soquete bruto)** – Isso carrega um arquivo imprimível do computador.
- 6 Clique em **Download**.

### Notas:

- As tarefas do Download genérico de arquivo não estarão disponíveis quando a opção Bloqueio da impressora estiver habilitada.
- Uma tarefa do Download genérico de arquivo pode ser programada para que ocorra em um momento predeterminado ou regularmente. Para obter mais informações, consulte “Tarefas de programação” na página 55.


## Configurando as definições de e-mail

**Nota:** Você precisa configurar as definições de SMTP (Simple Mail Transfer Protocol) para que o Markvision possa enviar notificações de e-mail para mensagens de erro e alertas.


- 1 Na área do Cabeçalho, clique em  > guia **E-mail**.
- 2 Insira os valores nos campos apropriados:
  - **Servidor de e-mail SMTP** – Insira as informações do servidor de e-mail.
  - **Porta** – Insira o número da porta do servidor de e-mail SMTP.
  - **De** – Insira o endereço de e-mail do remetente.

- 3 Se um usuário precisar efetuar login antes de enviar o e-mail, marque a caixa de seleção **Login necessário**.
  - a Insira as informações de login e a senha.
  - b Confirme a senha digitando-a novamente.
- 4 Clique em **Aplicar** > **Fechar**.

## Configuração das definições do sistema



- 1 Na área do Cabeçalho, clique em  > guia **Geral**.
- 2 Na seção Origem do nome de host, selecione a origem para o sistema onde obter o nome do host para um dispositivo e clique em **Aplicar**.
- 3 Na seção Gerenciador de eventos, defina o intervalo que o sistema deve esperar antes de registrar novamente os dispositivos para alertas e clique em **Aplicar**.

## Adição, edição ou exclusão de um usuário no sistema

- 1 Na área do Cabeçalho, clique em  > guia **Usuário**.
- 2 Execute um dos seguintes procedimentos:
  - Para adicionar um usuário, clique em **+**.
    - a Insira os detalhes necessários.
    - b Na seção Funções, selecione a função do novo usuário e clique em **OK**.

Um usuário pode ser atribuído a uma ou várias funções:

- **Admin** – O usuário pode acessar e executar tarefas em todas as guias. Somente usuários atribuídos a essa função possuem privilégios administrativos, como adição de mais usuários ao sistema ou configuração de definições do sistema.
- **Ativos** – O usuário pode somente acessar e executar tarefas encontradas na guia Ativos.
- **Gerenciador de eventos** – O usuário pode somente acessar e executar tarefas encontradas na guia Gerenciador de eventos.
- **Políticas** – O usuário pode somente acessar e executar tarefas encontradas na guia Políticas.
- **Central de serviços** – O usuário pode somente acessar e executar tarefas encontradas na guia Central de serviços.

- Selecione um usuário existente e clique em  para editar ou  para excluir.

- 3 Siga as instruções na tela do computador.

**Nota:** Três falhas consecutivas nas tentativas de login desativam a conta do usuário; e ela pode ser reativada somente por um Administrador. Entretanto, se o usuário for o único no sistema com a função Admin, então a conta é suspensa temporariamente por cerca de cinco minutos apenas.

## Ativação da autenticação do servidor LDAP


O Lightweight Directory Access Protocol (LDAP) é um protocolo extensível baseado em padrões que pode ser usado em múltiplas plataformas e que é executado diretamente no topo do TCP/IP, sendo usado para acessar bancos de dados especializados chamados *diretórios*.

Os administradores do Markvision podem usar o servidor LDAP da empresa para autenticar IDs e senhas de usuários. Assim, os usuários não precisam manter um ID de login e uma senha separados somente para o Markvision.

O Markvision primeiro tenta a autenticação em relação às credenciais do usuário válidas presentes no sistema. Se o Markvision não conseguir autenticar o usuário em sua primeira tentativa, então tenta a autenticação em relação aos usuários registrados no servidor LDAP. Porém, se um usuário tiver o mesmo nome de usuário no servidor interno Markvision e no servidor externo de diretório LDAP, o Markvision usará as credenciais armazenadas em seu servidor interno. Isto significa que o usuário precisa usar a senha do Markvision e *não* a senha do LDAP.

Como um pré-requisito, o servidor LDAP deve conter grupos de usuários que correspondam às funções definidas em “Adição, edição ou exclusão de um usuário no sistema” na página 48.

### Etapa 1. Configure as definições de autenticação

1 Na área do Cabeçalho, clique na guia do  >LDAP.

2 Na seção Informações de autenticação, digite os valores nos campos apropriados.

- **Servidor** – Digite o endereço IP ou o nome de host do servidor do diretório LDAP onde será realizada a autenticação.

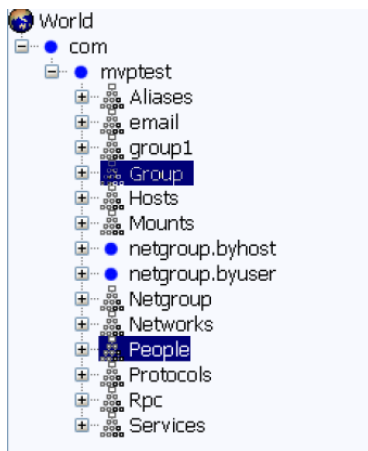
Se quiser usar comunicação criptografada entre o servidor MVE e o servidor do diretório LDAP, faça o seguinte:

- a Use o *nome de domínio totalmente qualificado* (FQDN) do host do servidor.
- b Acesse o arquivo do host da rede e, em seguida, crie uma entrada para mapear o nome de host do servidor para o seu endereço IP.

#### Notas:

- Em um sistema operacional UNIX/Linux, o arquivo do host da rede geralmente é encontrado em `/etc/hosts`.
  - Em um sistema operacional Windows, o arquivo do host da rede geralmente é encontrado em `%SystemRoot%\system32\drivers\etc`.
  - O *Protocolo TLS* requer que o nome do host do servidor corresponda ao host “Emitido para” especificado no certificado TLS.
- **Porta**—Insira o número da porta que será usado pelo computador local para se comunicar com o servidor da comunidade LDAP.  
O número da porta padrão é 389.

- **DN raiz** – Digite o nome diferenciado base do nó raiz. Na hierarquia do servidor da comunidade LDAP, esse deve ser o ancestral direto do nó de usuário e do nó de grupo. Nesta ilustração, você digitaria `dc=mvptest, dc=com` no campo DN raiz.

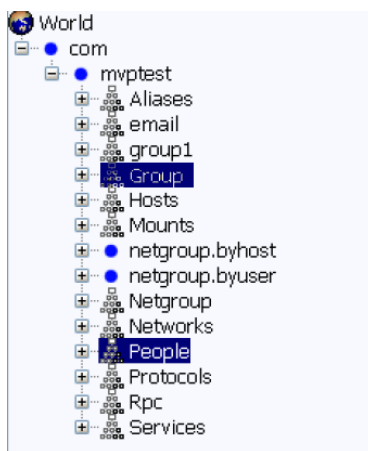


**Nota:** Quando especificar o DN raiz, certifique-se de que apenas `dc` e `o` sejam parte da expressão DN raiz. Se `ou` ou `cn` ficarem como o ancestral comum do nó do usuário e do nó de grupo, use `ou` ou `cn` nas expressões Base de pesquisa do usuário e Base de pesquisa do grupo.

- 3 Se você quiser que o Markvision pesquise por *usuários* aninhados no servidor da comunidade LDAP, selecione **Ativar pesquisa do usuário aninhada**.

Para refinar ainda mais a pesquisa, digite os valores nos campos apropriados.

- **Base de pesquisa do usuário** — digite o nó no servidor de comunidade LDAP onde está o objeto do usuário. Este também é o nó sob o DN raiz onde todos os Nós de usuários são listados. Nesta ilustração, você digitaria `ou=people` no campo Base de pesquisa do usuário.

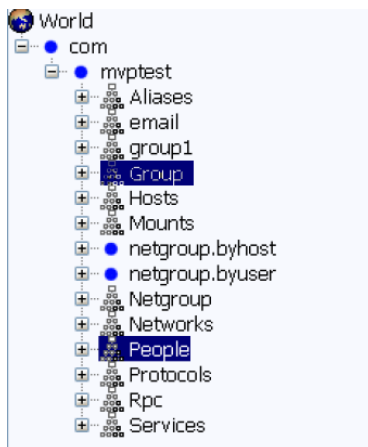


Se os usuários estiverem em níveis variados de hierarquia de pastas no servidor da comunidade LDAP, faça o seguinte:

- a Calcule qualquer hierarquia ascendente comum de todos os possíveis locais do nó do usuário.
- b Inclua a configuração no campo Base de pesquisa do usuário.

**Nota:** Como alternativa, você também pode selecionar **Ativar pesquisa do usuário aninhada** e deixar o campo Base de pesquisa do usuário em branco. Isso informa ao Markvision a pesquisar em toda a árvore LDAP iniciando no DN raiz e de base para os usuários.

- **Filtro de pesquisa do usuário** — digite o parâmetro para localizar um objeto de usuário no servidor da comunidade LDAP. Nesta ilustração, você digitaria `(uid={0})` no campo Filtro de pesquisa do usuário.



A função Filtro de pesquisa do usuário pode acomodar várias condições e expressões complexas, como ilustrado na tabela a seguir.

Para o usuário conectar-se usando o	Digite isto no campo Filtro de pesquisa do usuário
Nome comum	<code>(CN={0})</code>
Nome de login	<code>(sAMAccountName={0})</code>
Número de telefone	<code>(telephoneNumber={0})</code>
Nome de login ou Nome comum	<code>(   (sAMAccountName={0}) (CN={0}) )</code>

**Notas:**

- Essas expressões se aplicam *somente* ao servidor LDAP Windows Active Directory.
- Para Filtro de pesquisa do usuário, o único padrão é `{0}`, que significa que MVE pesquisará pelo nome de login do usuário do MVE.

**4** Se você quiser que o Markvision pesquise por *grupos* no servidor da comunidade LDAP, selecione **Ativar pesquisa do grupo aninhada**.

Para refinar ainda mais a pesquisa, digite os valores nos campos apropriados.

- **Base de pesquisa de grupo** – Insira o nó do servidor da comunidade LDAP onde existam os grupos de usuários correspondentes às funções do Markvision. Este também é o nó sob o DN raiz onde todos os nós (função) de grupo são listados.

Nesta ilustração, você digitaria **ou=group** no campo Base de pesquisa de grupo.

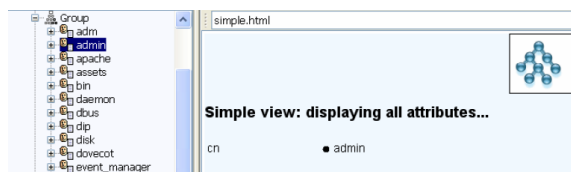


**Nota:** A Base de pesquisa consiste em vários atributos separados por vírgulas, como cn (nome comum), ou (unidade organizacional), o (organização), c (país) e dc (domínio).

- **Filtro da pesquisa de grupo** – Insira o parâmetro para localizar um usuário em um grupo que corresponda a uma função no Markvision.

**Nota:** Você pode usar os padrões **{0}** e **{1}**, dependendo da configuração do esquema do seu servidor da comunidade LDAP de back-end. Se você usar **{0}**, o MVE pesquisará pelo DN (Nome diferenciado) do usuário LDAP. O DN do usuário é recuperado internamente durante o processo de autenticação do usuário. Se você usar **{1}**, o MVE pesquisará pelo nome de login do usuário MVE.

- **Atributo de função de grupo** — Insira o atributo que contém o nome completo do grupo (função). Nesta ilustração, você digitaria **cn** no campo Atributo de função de grupo.



**Nota:** A seleção de **Ativar pesquisa do usuário aninhada** e **Ativar pesquisa do grupo aninhada** especifica a profundidade do servidor da comunidade LDAP. Por padrão, a Pesquisa do usuário LDAP e Pesquisa do grupo LDAP ocorre no máximo em um nível abaixo da Base de pesquisa do usuário e Base de pesquisa do grupo especificados, respectivamente. Sendo assim, a Pesquisa aninhada (subárvore) é usada para indicar a pesquisa de todas as entradas em todos os níveis aninhados e incluindo a Base de pesquisa do usuário e a Base de pesquisa do grupo especificadas.

## Etapa 2. Configure as definições de encadernação

Esta seção determina o protocolo utilizado pelo servidor MVE para se comunicar com o servidor externo de Diretório LDAP.

### 1 Clique em **Informações de ligação**.

#### Notas:

- Se não houve uma configuração LDAP armazenada no Markvision, por padrão, Ligação anônima do LDAP é selecionada automaticamente. Isto significa que o servidor MVE não produz sua identidade ou credencial

para o servidor LDAP para usar o recurso de consulta do servidor LDAP. A sessão de consulta LDAP de acompanhamento será somente comunicação não criptografada.

- O LDAP do Windows Active Directory *não* suporta a opção de associação anônima.

**2** Se quiser que o servidor MVE produza sua identidade para que o servidor LDAP consiga usar o recurso de consulta do servidor LDAP, configure a opção Associação simples.

**a** Selecione **Associação simples**.

**b** No campo DN de ligação, digite o nome diferenciado de ligação.

**c** Digite a senha de ligação e confirme a senha digitando-a novamente.

**Notas:**

- A senha de associação é dependente das configurações do usuário de associação no servidor do diretório LDAP. Se o usuário de associação for definido como **Não vazio** no LDAP, uma senha de associação será necessária. Se o usuário de associação for definido como **Não vazio** no LDAP, uma senha de associação *não* será necessária. Para obter informações sobre as configurações do usuário de associação, entre em contato com o Administrador do LDAP.
- A opção Associação simples usa comunicação não criptografada entre MVE e LDAP.

**3** Se quiser usar comunicação criptografada entre o servidor MVE e o servidor do diretório LDAP, selecione **Protocolo TLS (Transport Layer Security)** ou **Kerberos V5 (Windows Active Directory)**.

Se você selecionar **TLS**, significa que o servidor MVE terá que se autenticar completamente para o servidor do diretório LDAP usando a identidade (DN de associação) e as credenciais (Senha de associação) do servidor MVE.

**a** No campo DN de associação, digite o nome diferenciado de associação.

**b** Digite a senha de ligação e confirme a senha digitando-a novamente.

**Nota:** A senha de associação é necessária.

Para certificados autoassinados, a impressão digital de TLS deve ser disponibilizada para o armazenamento de chave da *Java Virtual Machine (JVM)* em todo o sistema denominado **cacerts**. Esse armazenamento de chave existe na pasta [mve.home]/jre/lib/security, onde [mve.home] é a pasta de instalação do Markvision.

Se você selecionou **Kerberos V5 (Windows Active Directory)**, faça o seguinte:

**a** No campo Nome de usuário KDC, digite o nome do Key Distribution Center (KDC).

**b** Digite a senha KDC e confirme a senha digitando-a novamente.

**c** Clique em **Procurar** e navegue até a pasta onde o arquivo *krb5.conf* está armazenado.

**Notas:**

- Para obter mais informações sobre o arquivo de configuração Kerberos, consulte a documentação que acompanha o protocolo de segurança Kerberos.
- O protocolo de segurança kerberos é suportado *somente* no Windows Active Directory que tem endosso de suporte GSS-API.

**d** Selecione o arquivo e clique em **Abrir**.

### Etapa 3. Configure as definições de mapeamento de função

**1** Clique em **Mapeamento de função**.

**2** Digite os valores nos campos apropriados.

- **Admin** — digite a função existente em LDAP que terá direitos administrativos em MVE.
- **Ativos** — digite a função existente que gerenciará o módulo Ativos em MVE.

- **Políticas** — digite a função existente em LDAP que gerenciará o módulo Políticas em MVE.
- **Serviço de help desk** — digite a função existente em LDAP que gerenciará o módulo Serviço de help desk em MVE.
- **Gerenciador de eventos**— digite a função existente em LDAP que gerenciará o módulo Gerenciador de eventos em MVE.

**Notas:**

- MVE mapeará automaticamente o Grupo (função) LDAP para a função MVE correspondente.
- Você pode atribuir um Grupo LDAP para multiplicar as Funções MVE, além de digitar mais de um Grupo LDAP em um campo de Função MVE.
- Ao digitar vários Grupos LDAP nos campos de função, use o caractere de barra vertical ( | ) para separar os grupos LDAP. Por exemplo, se quiser incluir os grupos **admin** e **assets** na função Admin, digite **admin | assets** no campo Admin.

**3** Se você escolher *não* usar algumas das funções MVE, deixe os campos correspondentes em branco.

**Nota:** Isto se aplica a todas as outras funções, *exceto* a função de Admin.

**4** Para validar sua configuração, clique em **Testar**.


**5** Digite o nome de usuário LDAP e a senha e, depois, clique em **Testar login**.

A caixa de diálogo Testar resultados da configuração LDAP é exibida. Se houver erros, faça o seguinte:

- Verifique as informações da caixa de diálogo para determinar a causa dos erros.
- Atualize as entradas feitas nas guias Informações de autenticação, Informações de ligação e Mapeamento de função.
- Repita a etapa 4 a etapa 5 até que não haja mais erros na caixa de diálogo Testar resultados da configuração LDAP.

**6** Clique em **Aplicar >Fechar**.

## Geração de relatórios


- 1 Na área do Cabeçalho, clique em .
- 2 No menu suspenso Incluir impressoras, selecione um grupo de dispositivos baseado em suas pesquisas que receberam marcadores anteriormente.
- 3 No menu suspenso Tipo de relatório, selecione o tipo de dados que deseja visualizar.

Selecione	Para visualizar
<b>Estado do ciclo de vida útil – Resumo</b>	Um relatório resumido dos estados do ciclo de vida útil dos dispositivos.
<b>Fabricante da impressora – Resumo</b>	Um relatório resumido dos fabricantes do dispositivo.
<b>Modelo da impressora – Resumo</b>	Um relatório resumido dos nomes e números dos modelos do dispositivo.
<b>Recursos da impressora</b>	Uma planilha listando os recursos do dispositivo.
<b>Recursos da impressora – Resumo</b>	Um relatório resumido dos recursos do dispositivo.
<b>Estado do ciclo de vida útil</b>	Uma planilha listando o estado do ciclo de vida útil dos dispositivos.
<b>Total de páginas já impressas</b>	Uma planilha listando o total de páginas já impressas dos dispositivos.


Selecione	Para visualizar
<b>Contagem de manutenção</b>	Uma planilha listando a contagem de manutenção dos dispositivos.
<b>Versões de firmware</b>	Uma planilha listando as versões de firmware dos dispositivos.
<b>Soluções eSF</b>	Uma planilha listando as diferentes soluções Estrutura de servidor incorporada (eSF) instaladas nos dispositivos.
<b>Estatísticas:Trabalhos por Folhas impressas</b>	Uma planilha listando o número de trabalhos de impressão executados pelos dispositivos.
<b>Estatísticas:Trabalhos por Contagem de lados de mídia</b>	Uma planilha listando o número de contagens de transporte para trabalhos de impressão, fax e cópia executados pelos dispositivos.
<b>Estatísticas:Trabalhos por Uso de digitalização</b>	Uma planilha listando o número de trabalhos de digitalização executados pelos dispositivos.
<b>Estatísticas:Trabalhos por Uso do fax</b>	Uma planilha listando o número de trabalhos de fax executados pelos dispositivos.
<b>Estatísticas:Trabalhos por Informações sobre suprimentos</b>	Uma planilha listando os detalhes importantes para cada um dos itens de suprimento nos dispositivos.

- 4 No menu suspenso Formato de relatório, selecione **PDF** ou **CSV**.
- 5 Se você selecionar PDF, então no campo Título poderá escolher personalizar o título do relatório.
- 6 Se aplicável, selecione um grupo do menu suspenso Grupo.
- 7 Clique em **Gerar**.

## Tarefas de programação

- 1 Na área do cabeçalho, clique em .
- 2 No menu suspenso Adicionar, faça o seguinte:
  - Selecione **Auditoria** e, em seguida, selecione um grupo de dispositivos.
  - Selecione **Localização** e, em seguida, selecione um perfil de localização.
  - Selecione **Conformidade** e, em seguida, selecione um grupo de dispositivos e um tipo de política.
  - Selecione **Aplicação** e, em seguida, selecione um grupo de dispositivos e um tipo de política.
  - Selecione **Download genérico de arquivo** e, em seguida, selecione um grupo, arquivo e destino de dispositivo. Somente usuários com a função Admin podem usar esta opção.
- 3 Clique em **Avançar**.
- 4 No campo Nome, digite o nome do novo evento programado.
- 5 Selecione suas definições e clique em **Concluir**.

## Exibição do log do sistema

- 1 Na área do cabeçalho, clique em .
- Por padrão, a última atividade no banco de dados é listada primeiro.
- 2 Se desejar visualizar as atividades por categoria, então faça o seguinte:
  - a Clique em **Filtro**.
  - b Na seção Período, selecione as datas de início e término.
  - c No campo ID(s), insira os números de ID da tarefa.  
**Nota:** Esse é um campo opcional.
  - d Na seção Nome da tarefa, desmarque a caixa de seleção ao lado da tarefa que não deseja incluir no arquivo de log.
  - e Na seção Categorias, desmarque a caixa de seleção ao lado da categoria que não deseja incluir no arquivo de log.
  - f Clique em **OK**.
- 3 Clique em **Preparar para exportar > Finalizar a exportação**.
- 4 No menu suspenso “Salvar em”, navegue até a pasta onde deseja salvar o arquivo de log.
- 5 No campo “Nome do arquivo”, digite o nome do arquivo e clique em **Salvar**.
- 6 Navegue até a pasta onde o arquivo de log está salvo e, em seguida, abra o arquivo para visualizar o log do sistema.

## Perguntas freqüentes

### Que dispositivos são compatíveis com o aplicativo?

Para obter uma lista completa dos dispositivos compatíveis, consulte as Notas de versão.

### Como altero minha senha?

Na área do cabeçalho, clique em **Alterar senha** e siga as instruções na tela do computador.

### Por que não posso escolher vários dispositivos na lista Modelos compatíveis da caixa de diálogo Criar política?

Comandos e definições de configuração variam dependendo do modelo. Um comando de definição que funciona em um modelo pode não funcionar em outro. As políticas são limitadas a um modelo por vez para impedir a criação de políticas que não funcionem corretamente.

A melhor maneira de impedir a criação de políticas ineficazes é criar uma política e, em seguida, atribuir a política recém-criada a vários dispositivos.

### Outros usuários podem acessar meus marcadores?

Sim. Marcadores são globais e, por isso, podem ser visualizados e gerenciados por qualquer usuário.

### Onde posso encontrar os arquivos de registro?

Navegue até este diretório para localizar os seguintes arquivos de registro do instalador: %TEMP%\

- *mve-\*.log*
- *\*.isf*

Navegue para este diretório para localizar os arquivos de registro do aplicativo:



<INSTALL\_DIR>\tomcat\logs, onde <INSTALL\_DIR> é a pasta de instalação do Markvision.

Os arquivos neste diretório com o formato *\*.log* são os arquivos de registro do aplicativo.

## Solução de problemas

### O usuário esqueceu a senha

Para redefinir a senha do usuário, você precisa ter privilégios de administrador.

- 1 Na área do Cabeçalho, clique em .
- 2 Na guia Usuário, selecione um usuário e clique em .
- 3 Altere a senha.
- 4 Clique em **OK** e em **Fechar**.
- 5 Peça para o usuário efetuar login novamente.

### O aplicativo não consegue localizar um dispositivo de rede

#### VERIFIQUE AS CONEXÕES DA IMPRESSORA

- Verifique se o cabo de alimentação está conectado na impressora e em uma tomada elétrica devidamente aterrada.
- Certifique-se de que a impressora esteja ligada.
- Certifique-se de que outros equipamentos elétricos que sejam conectados à tomada funcionem.
- Verifique se o cabo da LAN está conectado ao servidor de impressão e à LAN.
- Verifique se o cabo da LAN está funcionando adequadamente.
- Reinicie a impressora e o servidor de impressão.

#### CERTIFIQUE-SE DE QUE O SERVIDOR DE IMPRESSÃO INTERNO ESTEJA INSTALADO

##### ADEQUADAMENTE E ATIVADO.

- Imprima uma página de configuração da impressora. O servidor de impressão deve ser exibido na lista de anexos da página de configuração.
- Verifique se o TCP/IP está ativado no servidor de impressão. O protocolo deve estar ativo para que o servidor de impressão e o aplicativo funcionem. No painel de controle da impressora, verifique se o protocolo está ativo.
- Consulte a documentação de seu servidor de impressão.

## **VERIFIQUE SE O NOME DO DISPOSITIVO NO APLICATIVO É O MESMO QUE O NOME DEFINIDO NO SERVIDOR DE IMPRESSÃO.**

- 1 Verifique o nome do dispositivo definido no aplicativo.

Na área de Resultados da pesquisa, localize o endereço IP da impressora.

O nome do dispositivo aparece ao lado do endereço IP. Esse é o nome do dispositivo do aplicativo e *não* o nome do dispositivo do servidor de impressão.

- 2 Verifique o nome do dispositivo definido no servidor de impressão. Para obter mais informações, consulte a documentação do servidor de impressão.

## **VERIFIQUE SE O SERVIDOR DE IMPRESSÃO ESTÁ SE COMUNICANDO NA REDE.**

- 1 Execute o comando ping no servidor de impressão.
- 2 Se o ping funcionar, verifique o endereço IP, a máscara de rede e o gateway do servidor de impressão para certificar-se de que estão corretos.
- 3 Desligue a impressora e execute o comando ping novamente para verificar se há endereços IP duplicados. Se o comando ping não funcionar, então imprima uma página de configuração e verifique se o IP está ativado.
- 4 Se o TCP/IP estiver ativado, verifique se o endereço IP, a máscara de rede e o gateway estão corretos.
- 5 Verifique se as unidades bridge e os roteadores estão funcionando e configurados corretamente.
- 6 Verifique se todas as conexões físicas entre o servidor de impressão, a impressora e a rede estão funcionando.

## **As informações sobre o dispositivo estão incorretas**

Se o aplicativo exibir informações sobre o dispositivo que pareçam incorretas, execute uma auditoria no dispositivo.

## Apêndice

### Impressoras Lexmark que suportam a política de segurança

Lexmark C520*	Lexmark E460	Lexmark T640*	Lexmark W840*	Lexmark X463	Lexmark X790
Lexmark C522*	Lexmark E462	Lexmark T642*	Lexmark W850	Lexmark X464	Lexmark X850*
Lexmark C524*		Lexmark T644*		Lexmark X466	Lexmark X852*
Lexmark C530*		Lexmark T650		Lexmark X548	Lexmark X854*
Lexmark C532*		Lexmark T652		Lexmark X642*	Lexmark X860
Lexmark C534*		Lexmark T654		Lexmark X650	Lexmark X862
Lexmark C734				Lexmark X651	Lexmark X864
Lexmark C736				Lexmark X652	Lexmark X925
Lexmark C770*				Lexmark X654	Lexmark X940*
Lexmark C772*				Lexmark X656	Lexmark X945*
Lexmark C780*				Lexmark X658	Lexmark X950
Lexmark C782*				Lexmark X734	Lexmark X952
Lexmark C792				Lexmark X736	Lexmark X954
Lexmark C920*				Lexmark X738	
Lexmark C925					
Lexmark C930*					
Lexmark C935*					
Lexmark C950					
Lexmark Pro5500 Series*					
Lexmark Pro710 Series*					
Lexmark Pro910 Series*					
Lexmark Pro4000 Series*					

\* Indica dispositivos que não suportam o seguinte:

- As seções Controles de acesso, Modelos de segurança e Definições variadas das definições de política de segurança
- O controle de acesso de gerenciamento remoto do Embedded Web Server
- O nome de usuário, domínio e credenciais de comunicação PIN

## Glossário de termos de segurança

<b>Agrupar</b>	Um grupo de usuários compartilhando características comuns.
<b>Autenticação</b>	Um método para identificar com segurança um usuário.
<b>Autorização</b>	Um método para especificar quais funções estão disponíveis a um usuário, por exemplo, o que é permitido ao usuário fazer.
<b>Building Blocks</b>	Ferramentas de autenticação e autorização usadas no Servidor da Web Incorporado. Elas incluem: senha, PIN, Contas internas, LDAP, LDAP + GSSAPI, Kerberos 5 e NTLM.
<b>Controles de acesso</b>	Configurações que controlam se menus, funções e definições de um dispositivo individual estão disponíveis e para quem. Também conhecido como Funções de controles de acesso em alguns dispositivos.
<b>Modelo de segurança</b>	Um perfil criado e armazenado no Embedded Web Server, usado em conjunto com os Controles de acesso para gerenciar funções do dispositivo.

# Índice

## A

- adição de um usuário 48
- alteração de senhas 57
- aplicação de políticas 42
- aplicação de uma política 41
- aprendendo sobre a tela Bem-vindo 14
- Área de Informações da tarefa 14
- Área de Marcadores e Pesquisas avançadas 14
- Área de Resultados da pesquisa 14
- Área de Resumo de resultados da pesquisa 14
- Área do cabeçalho 14
- arquivos
  - fazendo download 47
- arquivos de registro
  - localizando 57
- arquivos de registro do aplicativo
  - localizando 57
- arquivos de registro do instalador
  - localizando 57
- ativação da autenticação do servidor LDAP 49
- atribuição de palavras-chave a um dispositivo 28
- atribuição de uma política 40
- atribuição de um evento a um dispositivo 45
- atualização para a versão mais recente do Markvision 9
- auditoria de um dispositivo 21
- avisos 2

## B

- backup do banco de dados Firebird 9
- banco de dados Firebird
  - backup 9
  - restaurando 10
- building blocks
  - uso de um aplicativo eSF 33

## C

- categorias
  - adicionando 28
  - editando 28

- excluindo 28
  - usando 27
- compreensão das portas 15
- compreensão dos dispositivos protegidos 32
- compreensão dos protocolos 15
- configuração das definições do sistema 48
- configurações do sistema
  - configurando 48
- configurando as definições de e-mail 47
- credenciais de comunicação
  - alterando 39
- criação de marcadores 27
- criação de uma nova política 30
- criação de uma política de um dispositivo 31
- criação de um evento 45
- criação de um perfil de localização 18

## D

- destino
  - criando 44
  - editando 44
  - excluindo 44
- dispositivo
  - atribuição de palavras-chave 28
  - atribuição de um evento 45
  - auditoria 21
  - exibição de detalhes do evento 46
  - exibição de propriedades 22
  - exibição remota 43
  - importação de um arquivo 20
  - remoção de uma palavra-chave atribuída 29
  - remoção de um evento 46
  - verificando o status 42
- dispositivo, alertas
  - recebendo 48
- dispositivo, nome do host
  - obtenção 48
- dispositivo restrito
  - mudança das credenciais de comunicação 39
- dispositivos
  - localização 18

- pesquisa 24
- dispositivos, protegidos
  - compreendendo 32
- dispositivos restritos
  - clonagem de uma política de segurança 34
- dispositivos sem restrições
  - clonagem de uma política de segurança 37
- dispositivos suportados 57
- download de arquivos genéricos 47

## E

- edição de uma política 40
- edição de um destino 44
- edição de um evento 45
- edição de um perfil de localização 19
- edição de um usuário 48
- e-mail
  - configurando definições 47
- espaços reservados 44
- esquecimento de senha do usuário 58
- estado do ciclo de vida útil do dispositivo
  - definindo 21
  - Desativado 21
  - Gerenciado 21
  - Gerenciado (Alterado) 21
  - Gerenciado (Ausente) 21
  - Gerenciado (Encontrado) 21
  - Gerenciado (Normal) 21
  - Não gerenciado 21
- evento
  - criando 45
  - editando 45
  - excluindo 45
  - exibição de detalhes 46
  - remoção de um dispositivo 46
- exclusão de marcadores 27
- exclusão de uma política 40
- exclusão de um destino 44
- exclusão de um evento 45
- exclusão de um perfil de localização 19
- exclusão de um usuário 48

- exibição da página da Web incorporada 43
- exibição de detalhes do evento 46
- exibição de propriedades do dispositivo 22
- exibição do registro do sistema 56
- exibição remota de um dispositivo 43

## G

- geração de relatórios 54
- guia ativos
  - usando 12
- guia central de serviços
  - usando 12
- guia Geral
  - usando 48
- guia gerenciador de eventos
  - usando 12
- guia políticas
  - usando 12

## I

- importação de dispositivos de um arquivo 20
- informações do dispositivo incorretas 59

## L

- lista de modelos suportados 57
- localização de dispositivos 18

## M

- marcadores
  - acessando 27
  - criando 27
  - excluindo 27
- marcadores padrão, uso de 24
- Markvision
  - acessando 10
  - instalando 8
  - usando 12
- Markvision Enterprise
  - atualização para a versão mais recente 9
  - definição 7
- MarkVision Professional
  - migração para o Markvision Enterprise 11

- migração do MarkVision Professional para o Markvision Enterprise 11
- MVE
  - migração para 11
- MVP
  - importação para o Markvision Enterprise 11
  - migração para o Markvision Enterprise 11

## N

- não foi possível descobrir um dispositivo de rede 58
- nomes do sistema
  - verificando 58

## P

- página da Web incorporada
  - exibindo 43
- palavras-chave
  - adicionando 28
  - atribuição a um dispositivo 28
  - editando 28
  - excluindo 28
  - remoção de um dispositivo 29
  - usando 27
- perfil de localização
  - criando 18
  - editando 19
  - excluindo 19
- pesquisa avançada, uso de 24
- pesquisa por dispositivos 24
- política
  - aplicação 41
  - atribuindo 40
  - criação de um dispositivo 31
  - criando 30
  - editando 40
  - excluindo 40
  - removendo 41
  - tipos 30
  - verificação da conformidade 41
- política de segurança
  - clonagem para dispositivos irrestritos 37
  - clonagem para dispositivos restritos 34
- impressoras Lexmark suportadas 60
- personalizando definições 33

- políticas
  - aplicação 42
  - gerenciando 30
  - verificação da conformidade do dispositivo 42
- portas
  - compreendendo 15
- preparação inicial
  - tela Bem-vindo 14
- programação de tarefas 55
- propriedades, dispositivo
  - exibindo 22
- protocolos
  - compreendendo 15

## R

- RAM do computador 8
- recebimento de alertas de dispositivos 48
- redefinição de senha do usuário 58
- registro do sistema
  - exibindo 56
- relatórios
  - gerando 54
- remoção de uma palavra-chave atribuída de um dispositivo 29
- remoção de uma política 41
- remoção de um evento de um dispositivo 46
- requisitos do sistema
  - espaço no disco rígido do computador 8
  - RAM 8
  - resolução da tela 8
  - velocidade do processador 8
- restauração do banco de dados Firebird 10

## S

- senha, usuário
  - redefinindo 58
- servidores do banco de dados suportados 8
- servidores do banco de dados suportados 8
- servidor LDAP
  - ativação da autenticação 49
- solução de problemas
  - informações do dispositivo incorretas 59

não foi possível descobrir um  
dispositivo de rede 58  
redefinição de senha do  
usuário 58  
Status da impressora 42  
status do dispositivo  
verificando 42  
Status dos suprimentos 42

## T

tarefas  
programação 55  
tela Bem-vindo  
compreendendo 14

## U

uso de categorias 27  
uso de palavras-chave 27  
usuário  
adicionando 48  
editando 48  
excluindo 48

## V

velocidade do processador 8  
verificação da conformidade com  
uma política 41  
verificação da conformidade do  
dispositivo com as políticas 42  
verificação do status do  
dispositivo 42  
visão geral 7