	serviço	
SERVERACCOUNTPWD	Senha de usuário para o serviço	Valor da sequência de caracteres.
DBTYPE	Tipo de banco de dados	▪ MySQL – Um banco de dados MySQL ou MariaDB será usado. ▪ MSSQL – Um banco de dados do Microsoft SQL Server (SQL Express) será usado.
MYSQLSERVERNAME	Nome completo do servidor MySQL ou MariaDB	Valor da sequência de caracteres.
MYSQLSERVERPORT	Número de uma porta para conexão ao MySQL Server ou MariaDB	Valor numérico.
MYSQLDBNAME	Nome do banco de dados do MySQL Server ou MariaDB	Valor da sequência de caracteres.
MYSQLACCOUNTNAME	Nome do usuário para a conexão ao banco de dados do MySQL Server ou MariaDB	Valor da sequência de caracteres.
MYSQLACCOUNTPWD	Senha do usuário para a conexão ao banco de dados do MySQL Server ou MariaDB	Valor da sequência de caracteres.
MSSQLCONNECTIONTYPE	Tipo de uso do banco de dados MSSQL	▪ InstallMSSEE – Instalar a partir de um pacote. ChooseExisting – Usar o servidor instalado.
MSSQLSERVERNAME	Nome completo da instância do SQL Server	Valor da sequência de caracteres.
MSSQLDBNAME	Nome do banco de dados do SQL Server	Valor da sequência de caracteres.
MSSQLAUTHTYPE	Método de autenticação para a conexão ao SQL Server	▪ Windows. ▪ SQLServer.
MSSQLACCOUNTNAME	Nome do usuário para a conexão ao SQL Server no modo SQLServer	Valor da sequência de caracteres.
MSSQLACCOUNTPWD	Senha do usuário para a conexão ao SQL Server no modo SQLServer	Valor da sequência de caracteres.
CREATE_SHARE_TYPE	Método para especificar a pasta compartilhada	▪ Create – Criar uma nova pasta compartilhada. Neste caso, as seguintes propriedades devem ser definidas:

		▪ SHARELOCALPATH – Caminho a uma pasta local. ▪ SHAREFOLDERNAME – Nome da rede de uma pasta. ▪ Null – A propriedade EXISTSHAREFOLDERNAME deve ser especificada.
EXISTSHAREFOLDERNAME	Caminho completo para uma pasta compartilhada existente	Valor da sequência de caracteres.
SERVERPORT	O número da porta usado para conectar ao Servidor de Administração	Valor numérico.
SERVERSSLPORT	Número de uma porta para estabelecer a conexão SSL ao Servidor de Administração	Valor numérico.
SERVERADDRESS	Administration Server address	Valor da sequência de caracteres.
SERVERCERT2048BITS	Tamanho da chave para o certificado do Servidor de Administração (bits)	▪ 1 – O tamanho da chave para o certificado do Servidor de Administração é de 2048 bits. ▪ 0 – O tamanho da chave para o certificado do Servidor de Administração é de 1024 bits. ▪ Se nenhum valor for especificado – O tamanho da chave para o certificado do Servidor de Administração é de 1024 bits.
MOBILESERVERADDRESS	Endereço do Servidor de Administração para a conexão de dispositivos móveis; ignorado se o componente MobileSupport não foi selecionado	Valor da sequência de caracteres.

Parâmetros de instalação do Agente de Rede

A tabela abaixo descreve as propriedades MSI que você pode configurar ao instalar o Agente de Rede. Todos os parâmetros são opcionais, exceto para o EULA e SERVERADDRESS.

Parâmetros da instalação do Agente de Rede no modo silencioso

Propriedade de MSI	Descrição	Valores disponíveis
EULA	Aceitação dos termos do Contrato de Licença	▪ 1 – Eu li, entendo e aceito por completo os termos do Contrato de Licença do

		▪ 0 – Eu não aceito os termos do Contrato de Licença (a instalação não é executada). Nenhum valor – Eu não aceito os termos do Contrato de Licença (a instalação não é executada).
DONT_USE_ANSWER_FILE	Ler as configurações de instalação a partir do arquivo de resposta	▪ 1 – Não usar. ▪ Outro valor ou sem valor – Leitura.
INSTALLDIR	Caminho para a pasta de instalação do Agente de Rede	Valor da sequência de caracteres.
SERVERADDRESS	Endereço do Servidor de Administração (necessário)	Valor da sequência de caracteres.
SERVERPORT	Número de uma porta para conexão ao Servidor de Administração	Valor numérico.
SERVERSSLPORT	Número da porta para a conexão criptografada ao Servidor de Administração usando protocolo SSL	Valor numérico.
USESSL	Decida se deseja usar uma conexão SSL	1 – Usar. ▪ Outro valor ou sem valor – Não usar.
OPENUDPPORT	Decida se deseja abrir uma porta UDP	▪ 1 – Abrir. Outro valor ou sem valor – Não abrir.
UDPPORT	Número da porta UDP	Valor numérico.
USEPROXY	Decida se deseja usar um servidor proxy	▪ 1 – Usar. ▪ Outro valor ou sem valor – Não usar.
PROXYLOCATION (PROXYADDRESS:PROXYPORT)	Endereços de proxy e número de uma porta para conexão ao servidor de proxy	Valor da sequência de caracteres.
PROXYLOGIN	Conta para a conexão ao servidor proxy	Valor da sequência de caracteres.
PROXYPASSWORD	Senha da conta para conexão ao servidor proxy (Não especifique nenhum detalhe de contas privilegiadas nos parâmetros dos	Valor da sequência de caracteres.

GATEWAYMODE	Modo de uso do gateway de conexão	0 – Não usar gateway de conexão. 1 – Usar este Agente de Rede como gateway de conexão. ▪ 2 – Conectar-se ao Servidor de Administração usando o gateway de conexão.
GATEWAYADDRESS	Endereço gateway-conexão	Valor da sequência de caracteres.
CERTSELECTION	Método para receber um certificado	▪ GetOnFirstConnection – Receber um certificado a partir do Servidor de Administração. GetExistent – Selecionar um certificado existente; se esta opção estiver selecionada, a propriedade CERTFILE deve ser especificada.
CERTFILE	Caminho para o arquivo do certificado	Valor da sequência de caracteres.
VMVDI	Ativar o modo dinâmico para a Virtual Desktop Infrastructure (VDI)	▪ 1 – Ativar. ▪ 0 - Não ativar. Sem valor – Não ativar.
LAUNCHPROGRAM	Decida se deseja iniciar o serviço Agente de Rede após a instalação	▪ 1 – Iniciar. ▪ Outro valor ou sem valor – Não iniciar.
NAGENTTAGS	Tag para o Agente de Rede (tem prioridade sobre a tag fornecida no arquivo de resposta)	Valor da sequência de caracteres.

Infraestrutura virtual

O Kaspersky Security Center é compatível com o uso de máquinas virtuais. Você pode instalar o Agente de Rede e do aplicativo de segurança em cada máquina virtual, assim como a proteção de máquinas virtuais em nível de hipervisor. No primeiro caso, você pode usar o aplicativo de segurança padrão ou o Kaspersky Security for Virtualization Light Agent para proteger suas máquinas virtuais. No segundo caso, você pode usar o Kaspersky Security for Virtualization Agentless.

Kaspersky Security Center suporta reversões de máquinas virtuais ao estado anterior

Dicas sobre como reduzir a carga em máquinas virtuais

Ao instalar o Agente de Rede em uma máquina virtual, você é aconselhado a considerar a desativação de alguns recursos do Kaspersky Security Center que parecem ser de um pouco uso para máquinas virtuais.

Ao instalar o Agente de Rede em uma máquina virtual ou em um modelo destinado para a geração de máquinas virtuais, recomendamos executar as seguintes ações:

Se estiver executando uma instalação remota, na janela Propriedades do pacote de instalação do Agente de Rede na seção **Avançado**, selecione a opção **Otimizar as configurações para VDI**.

- Se você estiver executando uma instalação interativa por meio de um assistente, na janela assistente, selecione a opção **Otimizar as configurações do Agente de Rede para a infraestrutura virtual**.

Selecionar essas opções alterará as configurações do Agente de Rede para que os seguintes recursos permaneçam desativados por padrão (antes da política ser aplicada):

- Recuperar informações sobre o software instalado
- Recuperar informações sobre o hardware
- Recuperar informações sobre as vulnerabilidades detectadas
- Recuperar informações sobre as atualizações necessárias

Normalmente, aqueles recursos não são necessários em máquinas virtuais porque elas usam o software uniforme e o hardware virtual.

A desativação dos recursos é irreversível. Se algum dos recursos desativados for necessário, você pode ativá-lo através da política do Agente de Rede ou através das configurações locais do Agente de Rede. As configurações locais do Agente de Rede estão disponíveis através do menu de contexto do dispositivo relevante no Console de Administração.

Suporte de máquinas virtuais dinâmicas

O Kaspersky Security Center Cloud Console é compatível com as máquinas virtuais dinâmicas. Se uma infraestrutura virtual tiver sido implementada na rede da organização, as máquinas virtuais dinâmicas (temporárias) podem ser usadas em determinados casos. As VMs dinâmicas são criadas sob nomes únicos com base em um modelo que foi preparado pelo administrador. O usuário trabalha em uma VM durante algum tempo, então, depois ser desligada, esta máquina virtual será removida da infraestrutura virtual. Se o Kaspersky Security Center tiver sido implementado na rede da organização, uma máquina virtual com o Agente de Rede instalado será adicionada ao banco de dados do Servidor de Administração. Depois que você desliga uma máquina virtual, a entrada correspondente também deve ser removida do banco de dados do Servidor de Administração.

Para tornar funcional o recurso de remoção automática de entradas em máquinas virtuais, ao instalar o Agente de Rede em um modelo para máquinas virtuais dinâmicas, selecione a opção **Ativar modo dinâmico para VDI**:

- Para a instalação remota - na janela de propriedades do pacote de instalação do Agente de Rede (seção Avançado)

Para a instalação interativa – No Assistente de instalação de Agente de Rede

Evite selecionar a opção **Ativar modo dinâmico para VDI** ao instalar o Agente de Rede em dispositivos físicos.

Se desejar que os eventos das máquinas virtuais dinâmicas sejam armazenados no Servidor de Administração durante algum tempo após essas máquinas virtuais serem removidas, então, na janela Propriedades do Servidor de Administração, na seção **Repositório de eventos**, selecione a opção **Armazenar eventos após a exclusão dos dispositivos** e especifique o período máximo de armazenamento para eventos (em dias).

Suporte para copiar máquinas virtuais

Copiar uma máquina virtual com o Agente de Rede instalado ou criar um a partir de um modelo com o Agente de Rede instalado, é idêntico a implementação de Agentes de Rede ao capturar e copiar uma imagem do disco rígido. Deste modo, no caso geral, ao copiar máquinas virtuais, você tem de executar as mesmas ações feitas ao implementar o Agente de Rede copiando uma imagem do disco.

No entanto, as duas caixas descritas abaixo apresentam o Agente de Rede que detecta a cópia automaticamente. Devido aos motivos acima, você não tem que executar as operações sofisticadas descritas sob "Implementar ao capturar e copiar o disco rígido de um dispositivo":

A opção **Ativar modo dinâmico para VDI** foi selecionada durante a instalação do Agente de Rede. Após cada reinicialização do sistema operacional, esta máquina virtual será reconhecida como um novo dispositivo, independentemente de ter sido copiada ou não.

- Um dos seguintes hypervisors está em uso: VMware™, HyperV®, ou Xen®: o Agente de Rede detecta a cópia da máquina virtual através das IDs alteradas do hardware virtual.

A análise das modificações no hardware virtual não é absolutamente confiável. Antes de aplicar este método amplamente, você deve testá-lo em um pequeno conjunto de máquinas virtuais da versão do hypervisor atualmente usado na sua organização.

O suporte do sistema de arquivos reverte para dispositivos com o Agente de Rede

O Kaspersky Security Center é um aplicativo distribuído. Reverter o sistema de arquivos a um estado anterior em um dispositivo com o Agente de Rede instalado conduzirá a dessincronização e ao funcionamento impróprio do Kaspersky Security Center.

O sistema de arquivos (ou uma parte dele) pode ser revertido nos seguintes casos:

- Ao copiar uma imagem do disco rígido.

  Ao restaurar um estado da máquina virtual por meio da infraestrutura virtual.

- Ao restaurar os dados de uma cópia backup ou de um ponto de recuperação.

Os cenários sob os quais o software de terceiros nos dispositivos com o Agente de Rede instalado que afetam a pasta %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\ somente são cenários críticos para o Kaspersky Security Center. Portanto, você sempre deve excluir esta pasta do procedimento de recuperação, se ssível.

Como as regras do local de trabalho de algumas organizações compreendem a possibilidade para a reversão do sistema de arquivos em dispositivos, o suporte para a reversão do sistema de arquivos em dispositivos com o Agente de Rede instalado foi adicionado ao Kaspersky Security Center, a partir da versão 10 Maintenance Release 1 (Servidor de Administração e os Agentes de Rede devem ser da versão 10 Maintenance Release 1 ou posterior). Quando detectado, estes dispositivos são automaticamente reconectados ao Servidor de Administração com a total limpeza dos dados e a total sincronização.

Por padrão, o suporte da reversão de detecção do sistema de arquivos está ativado no Kaspersky Security Center 14.2.

Tanto quanto possível, evite reverter a pasta %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\ nos dispositivos com o Agente de Rede instalado, porque a ressincronização completa dos dados requer uma grande quantidade de recursos.

A reversão do estado de sistema não é absolutamente permitida em um dispositivo com o Servidor de Administração instalado. A reversão do banco de dados também não é usada pelo Servidor de Administração.

Você pode restaurar um estado do Servidor de Administração a partir de uma cópia backup somente com o utilitário klbackup padrão.

Sobre a configuração de perfis de conexão para usuários ausentes

Os usuários ausentes de laptops (aqui também referidos como "dispositivos") podem precisar alterar o método da conexão a um Servidor de Administração ou alternar entre Servidores de Administração dependendo da localização atual do dispositivo na rede corporativa.

Os perfis de conexão têm suporte somente para dispositivos que executam Windows e macOS.

Usar endereços diferentes de um Servidor de Administração único

Os dispositivos com o Agente de Rede instalado podem conectar-se ao Servidor de Administração da intranet da organização ou a partir da Internet. Esta situação pode necessitar que o Agente de Rede use endereços diferentes para a conexão ao Servidor de Administração: o endereço do Servidor de Administração externo para a conexão com a Internet e o endereço do Servidor de Administração interno para a conexão da rede interna.

Para fazer isto, você deve adicionar um perfil (para a conexão ao Servidor de Administração a partir da Internet) à política do Agente de Rede. Adicione o perfil nas propriedades da política (Seção **Conectividade**, subsecção **Perfis de conexão**). Na janela de criação do perfil, você deve desativar a opção **Usar somente para receber atualizações** e selecionar a opção **Sincronizar as configurações de conexão com as configurações do Servidor de Administração especificadas nesse perfil**. Se você usa um gateway de conexão para acessar o Servidor de Administração (por exemplo, em uma configuração do Kaspersky Security Center que está descrita em No acesso à Internet: Agente de Rede como um gateway de conexão em DMZ), deverá especificar o endereço do gateway de conexão no campo correspondente do perfil de conexão.

Alternar entre Servidores de Administração dependendo da rede atual

Se a organização tiver múltiplos escritórios com diferentes Servidores de Administração e alguns dispositivos com o Agente de Rede instalado se moverem entre eles, você precisa do Agente de Rede para conectar-se ao Servidor de Administração da rede local no escritório onde o dispositivo está atualmente localizado.

Neste caso, você deve criar um perfil para a conexão ao Servidor de Administração nas propriedades da política do Agente de Rede de cada um dos escritórios, exceto para o escritório doméstico onde o Servidor de Administração mestre original esteja localizado. Você deve especificar os endereços dos Servidores de Administração em perfis de conexão e ativar ou desativar a opção **Usar somente para receber atualizações**:

- Selecione a opção se você precisar que o Agente de Rede seja sincronizado com o Servidor de Administração mestre, usando o Servidor local somente para baixar as atualizações.

  Desative a opção se for necessário que o Agente de Rede seja gerenciado completamente pelo Servidor de Administração local.

Após isso, você deve definir as condições da troca para os perfis recém criados: ao menos uma condição de cada um dos escritórios, exceto para o escritório doméstico. Cada propósito de condição consiste na detecção de itens que são específicos para o ambiente de rede de um escritório. Se uma condição for verdadeira, o perfil correspondente é ativado. Se nenhuma das condições for verdadeira, o Agente de Rede alterna para o Servidor de Administração mestre.

Implementar o recurso de Gerenciamento de dispositivos móveis

Esta seção providencia informação da implementação inicial da função Gerenciamento de dispositivos móveis.

Conectar dispositivos KES ao Servidor de Administração

Dependendo do método usado para a conexão de dispositivos ao Servidor de Administração, dois esquemas de implementação são possíveis para o Kaspersky Device Management for iOS para dispositivo KES:

Esquema de implementação com conexão direta dos dispositivos ao Servidor de Administração

- Esquema de implementação envolvendo um firewall corporativo que dá suporte à delegação de restrição Kerberos

Conexão direta de dispositivos ao Servidor de Administração

Os dispositivos KES podem conectar-se diretamente à porta 13292 do Servidor de Administração.

Dependendo do método usado para a autenticação, duas opções são possíveis para a conexão de dispositivos KES ao Servidor de Administração:

- Conectar dispositivos com um certificado do usuário
- Conectar dispositivos sem um certificado do usuário

Conectar um dispositivo com um certificado do usuário

Ao conectar um dispositivo com um certificado do usuário, aquele dispositivo é associado com a conta de usuário à qual o certificado correspondente foi atribuído através das ferramentas do Servidor de Administração.

Neste caso, a autenticação SSL de duas vias (autenticação mútua) será usada. Tanto o Servidor de Administração quanto o dispositivo serão autenticados com certificados.

Conectar um dispositivo sem um certificado do usuário

Ao conectar um dispositivo sem um certificado do usuário, aquele dispositivo não se associa com nenhuma das contas de usuário no Servidor de Administração. No entanto, quando o dispositivo recebe qualquer certificado, ele é associado ao usuário ao qual o certificado correspondente foi atribuído através das ferramentas do Servidor de Administração.

Ao conectar aquele dispositivo ao Servidor de Administração, a autenticação SSL bilateral será aplicada, o que significa que somente o Servidor de Administração será autenticado com o certificado. Após o dispositivo recuperar o certificado do usuário, o tipo de autenticação mudará para a autenticação SSL bilateral (autenticação bilateral SSL, autenticação mútua).

Esquema para conectar dispositivos KES ao servidor envolvendo a delegação de restrição Kerberos (KCD)

O esquema para conectar dispositivos KES ao Servidor de Administração envolvendo a delegação restringida Kerberos (KCD) fornece o seguinte:

Integração com um firewall corporativo compatível com a KCD.

- Uso do Kerberos Constrained Delegation (aqui referido como KCD) para a autenticação de dispositivos móveis.
- Integração com a Infraestrutura de chaves públicas (aqui referida como PKI) para aplicar certificados de usuário.

Ao usar este esquema de conexão, observe o seguinte:

O tipo de conexão dos dispositivos KES com o firewall corporativo deve ser "autenticação SSL bilateral", ou seja, um dispositivo deve conectar-se ao firewall corporativo por meio de seu certificado do usuário proprietário. Para fazer isto, você deve integrar o certificado do usuário no pacote de instalação de Kaspersky Endpoint Security for Android que foi instalado no dispositivo. Este pacote KES deve ser criado pelo Servidor de Administração especificamente para este dispositivo (usuário).

Você deve especificar o certificado especial (personalizado) em vez do certificado de servidor padrão para o protocolo móvel:

1. Na janela de propriedades do Servidor de Administração, na seção **Configurações**, marque a caixa de seleção **Abrir a porta para dispositivos móveis** e selecione **Adicionar certificado** na lista suspensa.
2. Na janela que é aberta, especifique o mesmo certificado que foi definido no firewall corporativo quando o ponto do acesso ao protocolo móvel foi publicado no Servidor de Administração.

- Os certificados de usuário de dispositivos KES devem ser emitidos por Certificate Authority (CA) do domínio. Tenha em mente que se o domínio incluir CAs de múltiplas raízes, os certificados do usuário devem ser emitidos pela CA, que foi definida na publicação no firewall corporativo.
  Você pode assegurar-se de que o certificado do usuário esteja em conformidade com requisito acima descrito, usando um dos seguintes métodos:
  - Especifique o certificado do usuário especial no Assistente de novo pacote e no Assistente de instalação de certificados.

- Integre o Servidor de Administração com o PKI do domínio e defina a configuração correspondente nas regras de emissão de certificados:

  1. Na árvore do console, expanda a pasta **Gerenciamento de Dispositivos Móveis** e selecione a subpasta **Certificados**.
  2. No espaço de trabalho da pasta **Certificados**, clique no botão **Configurar as regras de emissão de certificados** para abrir a janela **Regras de emissão do certificado**.
  3. Na seção **Integração com PKI**, configure a integração com a infraestrutura de chaves públicas.
  4. Na seção **Emissão de certificados móveis**, especifique a origem dos certificados.

Abaixo encontra-se um exemplo da Kerberos Constrained Delegation (KCD) com as seguintes suposições:

- O ponto do acesso ao protocolo móvel no Servidor de Administração é definido na porta 13292.
- O nome do dispositivo com o firewall corporativo é firewall.mydom.local.
- O nome do dispositivo com o Servidor de Administração é ksc.mydom.local.
- O nome da publicação externa do ponto de acesso ao protocolo móvel é kes4mob.mydom.global.

Conta de domínio para o Servidor de Administração

Você deve criar uma conta de domínio (por exemplo, KSCMobileSrvcUsr) sob a qual o serviço Servidor de Administração será executado. Você pode especificar uma conta do serviço Servidor de Administração ao instalar o Servidor de Administração ou através do utilitário klsrvswch. O utilitário klsrvswch está localizado na pasta de instalação do Servidor de Administração. O caminho de instalação padrão: <Disco>:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center.

Uma conta de domínio deve ser especificada pelos seguintes motivos:

- O recurso para o gerenciamento de dispositivos KES é uma parte integral do Servidor de Administração.
- Para assegurar um funcionamento apropriado do Kerberos Constrained Delegation (KCD), o lado recebedor (ou seja, o Servidor de Administração) deve ser executado sob uma conta de domínio.

Nome do serviço principal para http/kes4mob.mydom.local

No domínio, sob a conta KSCMobileSrvcUsr, adicione um SPN para publicar o serviço de protocolo móvel na porta 13292 do dispositivo com o Servidor de Administração. Para o dispositivo kes4mob.mydom.local com o Servidor de Administração, isto aparecerá como segue:

```
setspn -a http/kes4mob.mydom.local:13292 mydom\KSCMobileSrvcUsr
```

Configurar as propriedades de domínio do dispositivo com o firewall corporativo (firewall.mydom.local)

Para delegar o tráfego, você deve confiar o dispositivo com o firewall corporativo (firewall.mydom.local) ao serviço definido pelo SPN (http/kes4mob.mydom.local:13292).

Para confiar o dispositivo com firewall corporativo ao serviço definido pelo SPN (http/kes4mob.mydom.local:13292), o administrador deve executar as seguintes ações:

1. No snap-in Microsoft Management Console nomeado "Usuários e Computadores do Active Directory", selecione o dispositivo com o firewall corporativo instalado (firewall.mydom.local).
2. Nas propriedades do dispositivo, na guia **Delegação**, defina **Confiar neste computador somente para a delegação ao serviço especificado** alterne para **Usar qualquer protocolo de autenticação**.
3. Na lista **Serviços aos quais esta conta pode apresentar credenciais delegadas**, adicione o SPN http/kes4mob.mydom.local:13292.

Certificado especial (personalizado) para a publicação (kes4mob.mydom.global)

Para publicar o protocolo móvel do Servidor de Administração, você deve emitir um certificado especial (personalizado) para o FQDN kes4mob.mydom.global e especificá-lo em vez do certificado de servidor padrão nas configurações do protocolo móvel do Servidor de Administração no Console de Administração. Para fazer isso, na janela de propriedades do Servidor de Administração, na seção **Configurações**, selecione a caixa de seleção **Abrir a porta para dispositivos móveis** e, a seguir, selecione **Adicionar certificado** na lista suspensa.

Observe que o contêiner de certificado do servidor (arquivo com a extensão p12 ou pfx) também deve conter uma cadeia de certificados raiz (chaves públicas).

Configurar a publicação no firewall corporativo

No firewall corporativo, para o tráfego que vai de um dispositivo móvel até a porta 13292 do kes4mob.mydom.global, é necessário configurar a KCD no SPN (http/kes4mob.mydom.global:13292), usando o certificado emitido para o FQDN (kes4mob.mydom.global). Observe que publicar e ponto de acesso publicado (porta 13292 do Servidor de Administração) deve compartilhar o mesmo certificado de servidor.

Usar o Google Firebase Cloud Messaging

Para assegurar respostas em tempo dos dispositivos KES no Android aos comandos do administrador, você tem de ativar o uso do Google™ Firebase Cloud Messaging (aqui referido como FCM) nas propriedades do Servidor de Administração.

Para ativar o uso do FCM:

1. No console de administração, selecione o nó **Gerenciamento de Dispositivos Móveis** e a pasta **Dispositivos móveis**.
2. No menu de contexto da pasta **Dispositivos móveis**, selecione **Propriedades**.
3. Nas propriedades da pasta, selecione a seção **Configurações do Google Firebase Cloud Messaging**.
4. Nos campos **ID do Remetente** e **Chave do servidor**, especifique as configurações do FCM: SENDER_ID e Chave API.

O serviço FCM é executado nas seguintes faixas de endereços:

- Do dispositivo KES, o acesso é necessário às portas 443 (HTTPS), 5228 (HTTPS), 5229 (HTTPS) e 5230 (HTTPS) dos seguintes endereços:

- google.com

  fcm.googleapis.com

- android.apis.google.com

  Todos dos endereços IP listados no ASN da Google de 15169

- No Servidor de Administração, o acesso é necessário à porta 443 (HTTPS) dos seguintes endereços:
  - fcm.googleapis.com
  - Todos dos endereços IP listados no ASN da Google de 15169

Se as configurações do servidor proxy (**Avançado** / **Configurações de conexão à Internet**) tiverem sido especificadas nas propriedades do Servidor de Administração no Console de Administração, elas serão usadas para a interação com o FCM.

Configuração FCM: recuperando SENDER_ID e Chave API

Para configurar o FCM, o administrador deve executar as seguintes ações:

1. Registrar-se no portal do Google.
2. Siga para o portal Desenvolvedores.
3. Crie um novo projeto ao clicar no botão **Criar projeto**, especifique o nome do projeto e especifique a ID.
4. Esperar que o projeto seja criado.

   Na primeira página do projeto, na parte superior da página, o campo **Número do projeto** mostra o SENDER_ID relevante.
5. Siga para a seção **APIs e autenticação/APIs**, e ative o **Google Firebase Cloud Messaging for Android**.
6. Siga para a seção **APIs e autenticações/credenciais**, e clique no botão **Criara nova chave**.
7. Clique no botão **Chave do servidor**.
8. Para impor restrições (se alguma), clique no botão **Criar**.
9. Recupere a Chave API a partir das propriedades da chave recentemente criada (campo **Chave do servidor**).

Integração com a infraestrutura de chaves públicas

A integração com a infraestrutura de chaves públicas (aqui referido como PKI) é principalmente destinada para simplificar a emissão de certificados de usuário de domínio pelo Servidor de Administração.

O administrador pode atribuir um certificado de domínio para um usuário no Console de Administração. Isto pode ser feito usando um dos seguintes métodos:

- Atribuir ao usuário um certificado especial (personalizado) de um arquivo no Assistente de instalação de certificados

- Execute a integração com PKI e atribua o PKI a atuar como a fonte de certificados de um tipo específico de certificados ou para todos os tipos de certificados.

As configurações de integração com a PKI estão disponíveis na área de trabalho da pasta **Gerenciamento de Dispositivos Móveis** / **Certificados** ao clicar no link **Integrar com infraestrutura de chave pública**.

Princípio geral de integração com PKI para a emissão de certificados de usuário de domínio

No Console de Administração, clique no link **Integrar com infraestrutura de chave pública** no espaço de trabalho da pasta **Gerenciamento de Dispositivos Móveis** / **Certificados** que será usada pelo Servidor de Administração para emitir os certificados do usuário do domínio através do CA do domínio CA (aqui referido como a conta sob a qual a integração com PKI é executada).

Observe o seguinte:

- As configurações da integração com PKI fornecem-lhe a possibilidade de especificar o modelo padrão para todos os tipos de certificados. Observe que as regras de emissão de certificados (disponível no espaço de trabalho da pasta **Gerenciamento de Dispositivos Móveis**/**Certificados** clicando no botão **Configurar as regras de emissão de certificados**) permitem especificar um modelo individual para cada tipo de certificado.

  Um certificado de Enrollment Agent (EA) especial deve ser instalado no dispositivo com o Servidor de Administração, no repositório de certificados da conta sob a qual a integração com PKI é executada. O certificado Enrollment Agent (EA) é emitido pelo administrador da CA do domínio (Autoridade de Certificado).

A conta sob a qual a integração com PKI é executada deve atender os seguintes critérios:

- É um usuário do domínio.

  É um administrador local do dispositivo com o Servidor de Administração a partir do qual a integração com PKI é iniciada.

- Tem o direito de fazer *Login como serviço*.

- O dispositivo com o Servidor de Administração instalado deve ser executado ao menos uma vez sob desta conta para criar um perfil de usuário permanente.

Servidor Web do Kaspersky Security Center

O Servidor Web do Kaspersky Security Center (aqui referido como Servidor Web) é um componente do Kaspersky Security Center. O Servidor da Web foi projetado para publicar pacotes de instalação independentes, pacotes de instalação independentes para dispositivos móveis e arquivos da pasta compartilhada.

Os pacotes de instalação que foram criados são publicados no Servidor da Web automaticamente e então removidos após o primeiro download. O administrador pode enviar o novo link ao usuário de qualquer forma prática: por exemplo, por e-mail.

Ao clicar no link, o usuário poderá baixar as informações necessárias para um dispositivo móvel.

Configurações do servidor da Web

Se um ajuste fino do Servidor da Web for necessário, suas propriedades lhe permitem alterar as portas para HTTP (8060) e HTTPS (8061). Além de alterar as portas, você pode substituir o certificado do servidor por HTTPS e alterar o FQDN o servidor da Web para HTTP.

Outro trabalho de rotina

Esta seção fornece recomendações no trabalho de rotina com o Kaspersky Security Center.

Monitorando as luzes de tráfego e os eventos registrados no Console de Administração

O Console de Administração permite avaliar rapidamente o status atual do Kaspersky Security Center e dos dispositivos gerenciados ao verificar os sinais luminosos. Os sinais luminosos são mostrados no espaço do nó do **Servidor de Administração**, na guia **Monitoramento**. A guia fornece seis painéis de informações com luzes de tráfego e eventos registrados. O sinal luminoso é uma barra vertical colorida no lado esquerdo de um painel. Cada painel com um sinal luminoso corresponde a um escopo funcional específico do Kaspersky Security Center (veja a tabela abaixo).

Escopos cobertos por sinais luminosos no Console de Administração

Nome do painel	Escopo do sinal luminoso
Implementação	Instalar Agente de Rede e aplicativos de segurança em dispositivos em uma rede da organização
Esquema do gerenciamento	Estrutura de grupos de administração. Verificação da rede. Regras de migração de dispositivos
Configurações de proteção	Funcionalidade do aplicativo de segurança: status de proteção, verificação de malwares
Atualizar	Atualizações e patches
Monitoramento	Status de proteção
Servidor de Administração	Recursos e propriedades do Servidor de Administração

Cada sinal luminoso pode ser para qualquer de uma destas quatro cores (veja a tabela abaixo). A cor de um sinal luminoso depende do status atual do Kaspersky Security Center e dos eventos que foram registrados.

Códigos em cores de sinais luminosos

Status	Cor do sinal luminoso	Significação da cor do sinal luminoso
Informativo	Verde	Intervenção do administrador não é necessária.
Advertência	Amarelo	Intervenção do administrador é necessária.
Crítico	Vermelho	Problemas sérios foram encontrados. A intervenção do administrador é necessária para solucioná-los.
Informativo	Azul-claro	Os eventos foram registrados e que são não relacionados com ameaças potenciais ou reais à segurança de dispositivos gerenciados.

A meta do administrador é manter verdes os sinais luminosos em todos dos painéis de informações da guia **nitoramento**.

Os painéis de informações também mostram eventos registrados que afetam as luzes de tráfego e o status do Kaspersky Security Center (consulte a tabela abaixo).

Nome, descrição e cores das luzes de tráfego de eventos registrados

Cor do sinal luminoso	Nome de exibição do tipo de evento	Tipo de evento	
Vermelho	**A licença expirou em %1 dispositivo(s)**	IDS_AK_STATUS_LIC_EXPAIRED	Eve tipo qua con exp Uma o Ka Sec veri lice nos Qua lice con exp Kas Sec forr ape fun bás Para usa Kas Sec é ne ren lice con
Vermelho	**O aplicativo de segurança não está em execução em: %1 dispositivos**	IDS_AK_STATUS_AV_NOT_RUNNING	Eve tipo qua apli seg inst disp esta exe Ver con Kas Enc Sec em disp
Vermelho	**A proteção está desativada em: %1 dispositivos**	IDS_AK_STATUS_RTP_NOT_RUNNING	Eve tipo qua

			seg disp des mai o in esp Ver stat pro tem disp con tod con da p nec está
Vermelho	**Foi detectada uma vulnerabilidade de software nos dispositivos**	IDS_AK_STATUS_VULNERABILITIES_FOUND	Eve tipo qua *Enc* *vuln* *e at* *nec* det vuln con grav esp apli inst disp

			Ver de a disp sub **Atu** **Sof** upo na p **Ger** **de a** Ess con lista atu para da M para de s out forn recu pelo Adr para pos dist os c Apo as in sob atu disp inst disp
Vermelho	**Eventos críticos registrados no Servidor de Administração**	IDS_AK_STATUS_EVENTS_OCCURED	Eve tipo qua crít Ser Adr são Ver de e arm Ser Adr a se os e crít
Vermelho	**Foram registrados erros em eventos no Servidor de Administração**	IDS_AK_STATUS_ERROR_EVENTS_OCCURED	Eve tipo qua ines regi lado de Adr

			Ver de arm Ser Adr a se os e um.
Vermelho	**Conexão perdida para %1 dispositivos**	IDS_AK_STATUS_ADM_LOST_CONTROL1	Eve tipo qua con Ser Adr o di per Visu de des e te rec
Vermelho	**%1 dispositivos(s) não conectado(s) ao Servidor de Administração há muito tempo**	IDS_AK_STATUS_ADM_NOT_CONNECTED1	Eve tipo qua disp se Ser Adr den inte tem esp pois disp des Ver con disp liga Age esta exe
Vermelho	**%1 dispositivo(s) com status diferente de OK**	IDS_AK_STATUS_HOST_NOT_OK	Eve tipo qua *OK* disp con Ser Adr muc *Crí*

			É p solu pro usa utili diag rem Kas Sec
Vermelho	**Bancos de dados desatualizados em: %1 dispositivo(s)**	IDS_AK_STATUS_UPD_HOSTS_NOT_UPDATED	Eve tipo qua ban dad anti fora atu disp den inte tem esp Siga inst atu ban dad Kas
Vermelho	**Dispositivos nos quais a verificação de atualizações do Windows Update não é executada há muito tempo: %1**	IDS_AK_STATUS_WUA_DATA_OBSOLETE	Eve tipo qua *Exe* *sinc* *do* *Upd* exe den inte tem esp Siga inst sinc atu Win Upd Ser Adr
Vermelho	**%1 plug-in(s) do Kaspersky Security Center deve(m) ser instalado(s)**	IDS_AK_STATUS_PLUGINS_REQUIRED2	Eve tipo qua nec inst adic apli Kas

			Baix os p gere nec para Kas part da V Sup da K
Vermelho	**As ameaças ativas são detectadas em %1 dispositivo(s)**	IDS_AK_STATUS_NONCURED_FOUND	Eve tipo qua ame são em gere Visu info sob ame det siga rec
Vermelho	**A tarefa %1 foi concluída com um erro**	IDS_AK_STATUS_TASK_FAILED	Eve tipo qua exe uma con um Ver pro tare seg rec tare
Vermelho	**Muitos vírus foram detectados em: %1 dispositivo(s)**	IDS_AK_STATUS_TOO_MANY_THREATS	Eve tipo qua são em gere Visu info sob det siga rec
Vermelho	**Ataque de vírus**	IDS_AK_STATUS_VIRUS_OUTBREAK	Eve tipo qua núm obje mal

			dive disp gere exc den curt de t Visu info sob ame det siga rec
Vermelho	**Os bancos de dados no repositório não foram atualizados há muito tempo**	IDS_AK_STATUS_UPD_SERVER_NOT_UPTODATE	Eve tipo qua ban dad anti são no em Ver fre atu ban dad anti seg os b dad anti
Amarelo	**Os bancos de dados no repositório não foram atualizados há muito tempo**	IDS_AK_STATUS_UPD_SERVER_NOT_UPTODATE	Eve tipo qua ban dad anti são no por dia, de Ver fre atu ban dad anti seg os b dad anti
Amarelo	**O conflito de nomes NetBIOS**	IDS_AK_STATUS_ADM_NAME_CONFLICT	Eve tipo

	foi detectado nos dispositivos		disp os r nom Net Ren disp
Amarelo	**No(s) dispositivo(s) %s, a criptografia de dados mudou para o status especificado nos critérios de detecção de status do dispositivo**	IDS_AK_STATUS_ENCRYPTION_FAULTS_FOUND	Eve tipo qua crip dac disp gere
Amarelo	**A licença %1 expira em %2 dias**	IDS_AK_STATUS_LIC_EXPAIRING	Eve tipo qua no exp núm esp Para usa Kas Sec é ne ren lice con
Amarelo	**Dispositivos não atribuídos que tiveram o Agente de Rede instalado: %1**	IDS_AK_STATUS_NAGENTS_IN_UNASSIGNED	Eve tipo qua disp des red Mov disp con de grup disp gere
Amarelo	**Os Agentes de Rede em %1 dispositivo(s) não podem ser executados até que sejam reiniciados. Na última vez, este status era %2**	IDS_AK_STATUS_NAGENTS_NOT_RUNNING_UNTIL_REBOOT	Eve tipo qua Age não exe disp Rein disp
Amar		IDS_AK_STATUS_NEW_ARS_FILE_APPEARED	

	detectados **devem ser enviados para a** **Kaspersky para análise adicional**		tipo qua arq pro infe víru det mo Qua Env arq Kas aná
Amarelo	**Dispositivo(s) gerenciado(s):** **%1.. O aplicativo de segurança** **está instalado** **em: %2 dispositivo(s)**	IDS_AK_STATUS_NO_AV	Eve tipo qua Kas Enc Sec est em disp ger Inst Kas Enc Sec tod disp ger
Amarelo	**A tarefa de instalação %1** **foi concluída com êxito em** **%2** **dispositivo(s); a reinicialização é** **necessária em %3** **dispositivo(s)**	IDS_AK_STATUS_RI_NEED_REBOOT	Eve tipo qua Kas Enc Sec de em ger Rei disp apó inst Kas Enc Sec
Amarelo	**A verificação de** **malware não foi executada por** **um longo tempo em: %1** **dispositivo(s)**	IDS_AK_STATUS_SCAN_LATE	Eve tipo qua nec exe veri mal disp ger

			Exe veri víru
Amarelo	**Dispositivo(s) com vulnerabilidades de software detectadas: %1**	IDS_AK_STATUS_VULNERABLE_HOSTS_FOUND	Eve tipo qua vulr são em disp gere Visu infc sob vulr det cor
Verde	**Dispositivo(s) gerenciado(s): %3.. Dispositivo(s) não atribuído(s) detectado(s): %1**	IDS_AK_STATUS_ADM_OK1	Eve tipo qua disp det grup adn
Verde	**O aplicativo de segurança é instalado em todos os dispositivos gerenciados**	IDS_AK_STATUS_DEPLOYMENT_OK	Eve tipo qua Kas Enc Sec inst tod disp gere
Verde	**O Kaspersky Security Center está funcionando corretamente**	IDS_AK_STATUS_GENERAL_OK	Eve tipo qua Kas Sec esta fun cor
Verde	**O aplicativo de proteção em tempo real não está instalado**	IDS_AK_STATUS_RTP_NA	Eve tipo qua apli anti esta nos gere
Verde	**A proteção está ativada**	IDS_AK_STATUS_RTP_OK	Eve tipo qua pro tem

			disp gere
Verde	**O aplicativo de segurança não está instalado**	IDS_AK_STATUS_SCAN_NA	Eve tipo qua apli anti esta nos gere
Verde	**A verificação de malware está sendo executada conforme o agendamento**	IDS_AK_STATUS_SCAN_OK	Eve tipo qua de *de* sen exe con age
Verde	**O repositório de atualizações foi atualizado pela última vez: %1**	IDS_AK_STATUS_UPD_OK	Eve tipo qua rep atu atu
Azul-claro	**Os bancos de dados no repositório não foram atualizados há muito tempo**	IDS_AK_STATUS_UPD_SERVER_NOT_UPTODATE	Eve tipo qua ban dad anti atu dur
Azul-claro	**A Declaração da Kaspersky Security Network aceita está obsoleta**	IDS_AK_STATUS_ACCEPTED_KSN_AGREEMENT_OBSOLETE	Eve tipo qua Dec Kas Sec Net des
Azul-claro	**As atualizações de software da Kaspersky não foram aprovadas**	IDS_AK_STATUS_APPLICABLE_KL_PATCHES_NOT_APPROVED	Eve tipo qua adm ainc apr pat apli os a Kas gere
Azul-claro	**As atualizações do aplicativo Kaspersky**	IDS_AK_STATUS_APPLICABLE_KL_PATCHES_REVOKED	Eve tipo qua

	foram revogadas		adn ainc recu pat revo
Azul-claro	**O Contrato de Licença de Usuário Final do software móvel da Kaspersky não foi aceito**	IDS_AK_STATUS_KL_MOBILE_EULAS_NOT_ACCEPTED	Eve tipo qua adn ainc ace Cor Lice Usu para móv Kas
Azul-claro	**O Contrato de Licença de Usuário Final para atualizações de software da Kaspersky não foi aceito**	IDS_AK_STATUS_KL_PATCHES_EULAS_NOT_ACCEPTED	Eve tipo qua adn ainc ace Cor Lice Usu para atu sof Kas
Azul-claro	**A Declaração da Kaspersky Security Network para atualizações de software da Kaspersky não foi aceita**	IDS_AK_STATUS_KL_PATCHES_KSN_AGREEMENTS_NOT_ACCEPTED	Eve tipo qua adn ainc ace Dec Kas Sec Net atu sof Kas
Azul-claro	**O usuário deve aceitar o Contrato de Licença para instalar as atualizações**	IDS_AK_STATUS_NEED_ACCEPT_EULA	Eve tipo qua atu está disp inst o ac ainc ace Cor Lice
Azul-claro	**Novas versões**	IDS_AK_STATUS_NEW_DISTRIBUTIVES_AVAILABLE	Eve

	da Kaspersky estão disponíveis		qua ver apli Kas disp inst disp ger
Azul-claro	**As atualizações estão disponíveis para os componentes do Kaspersky Security Center**	IDS_AK_STATUS_NEW_KSC_VERSIONS_AVAILABLE	Eve tipo qua atu est disp os con do Sec
Azul-claro	**As atualizações estão disponíveis para os aplicativos da Kaspersky**	IDS_AK_STATUS_NEW_VERSIONS_AVAILABLE	Eve tipo qua atu est disp os a Kas
Azul-claro	**A tarefa de instalação do aplicativo %1 foi concluída com êxito em %2 dispositivo(s), mas falhou em %3 dispositivo(s)**	IDS_AK_STATUS_RI_FAILED	Eve tipo qua *Inst apli* ape o sc algu disp poc esp
Azul-claro	**Execução da tarefa de implementação - %1 (%2%%)**	IDS_AK_STATUS_RI_RUNNING	Eve tipo qua de imp est exe disp ger
Azul-claro	**A verificação completa nunca foi executada em %1 dispositivo(s)**	IDS_AK_STATUS_SCAN_NOT_SCANNED	Eve tipo qua veri con foi núm esp disp
Azul-		IDS_AK_STATUS_UPD_SRV_UPDATE_IN_PROGRESS	

claro	**tarefa de download da atualização (progresso: %1 %%)**		tipo qua tare baix atu est exe disp ger

Acesso remoto aos dispositivos gerenciados

Esta seção fornece informações sobre o acesso remoto aos dispositivos gerenciados.

Uso da opção "Não desconectar do Servidor de Administração" para fornecer conectividade contínua entre um dispositivo gerenciado e o Servidor de Administração

Caso os servidores push não sejam usados, o Kaspersky Security Center não fornece conectividade contínua entre dispositivos gerenciados e o Servidor de Administração. Os Agentes de Rede em dispositivos gerenciados periodicamente estabelecem conexões e sincronizam com o Servidor de Administração. O intervalo entre as sessões de sincronização é definido em uma política do agente de rede. Caso seja necessária uma sincronização antecipada, o Servidor de Administração (ou um ponto de distribuição, se estiver em uso) enviará um pacote de rede assinado por uma rede IPv4 ou IPv6 para a porta UDP do agente de rede. Por padrão, o número de porta é 15000. Caso nenhuma conexão via UDP seja possível entre o Servidor de Administração e um dispositivo gerenciado por qualquer motivo, a sincronização será executada na próxima conexão regular entre o agente de rede e o Servidor de Administração dentro do intervalo de sincronização.

Algumas operações não podem ser executadas sem uma conexão antecipada entre o agente de rede e o Servidor de Administração, como executar e interromper tarefas locais, receber estatísticas de um aplicativo gerenciado ou criar um túnel. Para resolver esse problema, caso os servidores push não estejam sendo usados, será possível usar a opção **Não desconectar do Servidor de Administração** para se certificar de que haja conectividade contínua entre um dispositivo gerenciado e o Servidor de Administração.

Para fornecer conexão contínua entre um dispositivo gerenciado e o Servidor de Administração:

1. Execute uma das seguintes ações:

   - Caso o dispositivo gerenciado acesse o Servidor de Administração diretamente (ou seja, não por meio de um ponto de distribuição):

     a. Na árvore do console, selecione a pasta **Dispositivos gerenciados**.

     b. Na área de trabalho da pasta, selecione o dispositivo gerenciado com o qual deseja fornecer conectividade contínua.

     c. No menu de contexto do dispositivo, selecione **Propriedades**.

     A janela de propriedades do dispositivo selecionado é aberta.

   - Caso o dispositivo gerenciado acesse o Servidor de Administração por meio de um ponto de distribuição e

a. Na árvore do console, selecione o nó do **Servidor de Administração**.

b. No menu de contexto do nó selecione **Propriedades**.

c. Na janela de propriedades do Servidor de Administração que é exibida, selecione a seção **Pontos de distribuição**.

d. Na lista, selecione o ponto de distribuição necessário e clique em **Propriedades**.

A janela de propriedades do ponto de distribuição é aberta.

2. Na seção **Geral** da janela exibida, selecione a opção **Não desconectar do Servidor de Administração**.

A conectividade contínua é estabelecida entre o dispositivo gerenciado e o Servidor de Administração.

O número total máximo de dispositivos com a opção **Não desconectar do Servidor de Administração** selecionada é 300.

Sobre verificar o tempo de conexão entre um dispositivo e o Servidor de Administração

Para desligar um dispositivo, o Agente de Rede notifica o Servidor de Administração sobre este evento. No Console de Administração, esse dispositivo é exibido como desligado. No entanto, o Agente de Rede não pode notificar o Servidor de Administração sobre todos tais eventos. O Servidor de Administração, portanto, periodicamente analisa o atributo **Conectado ao Servidor de Administração** (o valor deste atributo é exibido no Console de Administração, nas propriedades do dispositivo, na seção **Geral**) para cada dispositivo e compara-o com o intervalo de sincronização a partir das configurações atuais do Agente de Rede. Se um dispositivo não tiver respondido ao longo de mais de três intervalos de sincronização sucessivos, aquele dispositivo é marcado como desligado.

Sobre a sincronização forçada

Embora o Kaspersky Security Center automaticamente sincronize o status, configurações, tarefas e políticas para dispositivos gerenciados, em alguns casos o administrador precisa saber exatamente se a sincronização já foi executada para um dispositivo especificado no presente momento.

No menu de contexto dos dispositivos gerenciados no Console de Administração, o item de menu **Todas as tarefas** contém o comando **Forçar a sincronização**. Quando o Kaspersky Security Center 14.2 executa este comando, o Servidor de Administração tenta se conectar ao dispositivo. Se esta tentativa for bem sucedida, a sincronização forçada será executada. Caso contrário, a sincronização será forçada somente após a próxima conexão entre o Agente de Rede e o Servidor de Administração.

Sobre tunelamento

O Kaspersky Security Center permite o tunelamento de conexões de TCP, do Console de Administração via Servidor de Administração, e então via Agente de Rede a uma porta especificada em um dispositivo gerenciado. O tunelamento é projetado para conectar um aplicativo cliente em um dispositivo com o Console de Administração instalado à uma porta TCP em um dispositivo gerenciado – se nenhuma conexão direta for possível entre o Console de Administração e o dispositivo alvo.

Por exemplo, o tunelamento é usado para conexões a uma área de trabalho remota, para conectar-se a uma sessão existente e para criar uma nova sessão remota.

O tunelamento também pode ser ativado usando ferramentas externas. Por exemplo, o administrador pode executar o utilitário putty, o cliente VNC e outras ferramentas desta forma.