Microsoft Windows 10 IoT Enterprise para thin clients Dell Wyse

Guia do administrador

DELL EMC

Notas, avisos e advertências

NOTA: Uma NOTA indica informações importantes que ajudam você a usar melhor o seu produto.

CUIDADO: um AVISO indica possíveis danos ao hardware ou a possibilidade de perda de dados e informa como evitar o problema.

ATENÇÃO: uma ADVERTÊNCIA indica possíveis danos à propriedade, lesões corporais ou risco de morte.

2019 - 11

Rev. A09

Índice

1

Introdução

Thin clients Dell Wyse que executam o sistema operacional Windows 10 IoT Enterprise fornecem acesso a aplicativos, arquivos e recursos de rede. Os aplicativos e arquivos são disponibilizados em computadores que hospedam o Citrix Receiver, o Remote Desktop Connection e a sessão do VMware Horizon Client.

Outro software instalado localmente permite a administração remota dos thin clients e fornece funções de manutenção local. Mais suplementos estão disponíveis para suportar uma grande variedade de periféricos e recursos especiais para ambientes que precisam de uma interface de usuário segura que seja compatível com o Windows de 64 bits. Para obter mais informações, consulte www.microsoft.com.

NOTA:

- **O sistema operacional Windows 10 IoT é ativado quando você conecta o thin client à Internet. Se os servidores de ativação da Microsoft estiverem ocupados, você deve esperar até que o Windows 10 IoT seja ativado. Para verificar o status da ativação, acesse Iniciar > Configurações > Atualização e segurança > Ativação.**
- **Os recursos que são mencionados neste guia variam dependendo do modelo do thin client no seu local de trabalho. Para obter mais informações sobre os recursos aplicáveis ao seu thin client, consulte os respectivos Guias do usuário, em https://support.dell.com/manuals.**

Suporte técnico

Para acessar o portal de autoatendimento de recursos técnicos, os artigos da base de conhecimento, os downloads de software, o registro, as extensões de garantia/RMAs, os manuais de referência, as informações de contato e outros dados, visite https://support.dell.com.

Sobre este guia

Este guia é destinado aos administradores do thin client que executam o Windows 10 IoT Enterprise. Ele fornece informações e configurações detalhadas de sistema para ajudá-lo a projetar e gerenciar um ambiente do Windows 10 IoT Enterprise.

Thin clients suportados

Esta é a lista de thin clients que são executados no Windows 10 IoT Enterprise:

- Thin client Wyse 5470
- Thin client Wyse 5470 All-in-One
- Thin client Wyse 5070 com processador Celeron
- Thin client Wyse 5070 com processador Pentium
- Thin client estendido Wyse 5070 com processador Pentium
- Thin client Wyse 5060
- Thin client Wyse 7040
- Thin client móvel Latitude 3480
- Thin client móvel Latitude 5280

NOTA: O Thin client Wyse 7040 suporta o sistema operacional Windows 10 IoT Enterprise Threshold 1 e os thin clients restantes suportam o sistema operacional Windows 10 IoT Enterprise Redstone 1.

2

Primeiros passos

O aplicativo Quick Start é executado quando você inicializa em um thin client pela primeira vez. Essa ferramenta mostra recursos de software e hardware do thin client. Ela também fornece informações sobre os aplicativos de VDI, o software de gerenciamento e periféricos suportados.

Você também pode instalar o aplicativo Wyse Easy Setup usando o aplicativo Quick Start. O aplicativo Wyse Easy Setup permite que os administradores implantem configurações de maneira rápida e fácil em thin clients. Para obter mais informações, consulte Wyse Easy Setup.

Depois que você sair do aplicativo Quick Start, a área de trabalho do usuário é exibida por padrão. Você também pode abrir a ferramenta mais tarde.

É possível fazer login no thin client como usuário ou administrador. Um administrador pode configurar uma conta de usuário para fazer logon automática ou manualmente, digitando as credenciais de login.

Você pode usar o Wyse Management Suite para configurar, monitorar, gerenciar e otimizar seus thin clients de maneira centralizada. Para obter mais informações, consulte Como usar o Wyse Management Suite.

Para começar a usar o thin client, consulte:

- Logon automático e manual
- Antes de configurar thin clients
- Como usar o menu Iniciar
- Como usar a caixa de pesquisa
- Como usar a Central de Ações
- Como agrupar aplicativos nas áreas de trabalho
- Como conectar-se a uma impressora ou a um dispositivo externo
- Estado de energia

Log-in automático e manual

Quando um thin client é ligado ou reinicializado, você pode fazer login manual ou automaticamente com credenciais de administrador ou usuário, dependendo da configuração do administrador.

Para obter mais informações, consulte Como gerenciar usuários e grupos com contas de usuário.

NOTA:

- **Desative o Unified Write Filter (UWF) antes de alterar uma senha no thin client e depois ative o UWF após a alteração. Para obter mais informações, consulte Antes de configurar thin clients.**
- **Para alterar a senha, pressione CTRL+ALT+DEL e depois clique em <2>Alterar uma senha</2>. No entanto, esse recurso não se aplica a contas de Usuário.**

Quando você inicia o thin client, por padrão, ele faz automaticamente o log-in na área de trabalho do usuário.

Para fazer log-in com uma conta de usuário diferente, você deverá fazer log-out e clicar na conta de usuário preferencial na tela de log-in. Você pode usar as seguintes credenciais para fazer login em diferentes contas de usuário:

- **Administradores**: o nome de usuário padrão é **Administrador** e a senha padrão que diferencia maiúsculas de minúsculas é **DellCCCvdi**.
- **Usuários**: o nome de usuário padrão é **Usuário** e a senha padrão que diferencia maiúsculas de minúsculas é **DellCCCvdi**.
- **Usuário personalizado**: faça log-in no thin client digitando as credenciais de usuário que você definiu para a conta de usuário personalizada.

Antes de configurar thin clients

Antes de configurar thin clients, certifique-se de configurar o Unified Write Filter e o xData Cleanup Manager que protegem thin clients. O utilitário Unified Write Filter impede gravações indesejadas na memória flash e o xData Cleanup Manager evita que informações incorretas sobre limpeza sejam armazenadas no disco local.

No entanto, há casos em que o administrador de rede pode manter as configurações alteradas após sair e reiniciar o thin client.

Como usar a área de trabalho

As configurações definidas pelo administrador serão exibidas quando você fizer login no thin client pela primeira vez.

Se você fizer login como administrador, a **área de trabalho do administrador** será exibida. À direita da barra de tarefas, clique no ícone de **Notificações** para abrir a janela <3>Central de Ações</3>. Para obter mais informações sobre a Central de Ações, consulte Como usar a Central de Ações.

Além dos ícones padrão da área de trabalho, um conjunto estendido de recursos para configurar parâmetros de preferências do usuário e a administração do sistema está incluído no painel de controle do administrador. Para abrir o painel de controle, acesse **Iniciar** > **Painel de Controle**. Para obter mais informações, consulte Recursos administrativos.

Como usar o Menu Iniciar

O menu **Iniciar** ajuda você a acessar todos os programas, pastas e configurações no thin client. Ele contém uma lista de aplicativos que estão instalados no thin client.

NOTA: No menu Iniciar, você pode ver a lista de aplicativos usados com frequência em Mais usados.

Como usar a caixa de pesquisa

Use a caixa de pesquisa na barra de tarefas para procurar aplicativos, arquivos ou configurações. Digite o que você está pesquisando na caixa de pesquisa na barra de tarefas. Você também pode encontrar resultados para arquivos, aplicativos ou configurações do thin client. As sugestões e os resultados relacionados ao item pesquisado são mostrados na janela Início.

NOTA: Para pesquisar um determinado arquivo no thin client, aplique um dos seguintes filtros disponíveis no painel inferior da janela Início e, em seguida, procure o arquivo desejado:

- **Filtro de aplicativos**
- **Filtro de configurações**
- **Filtro de documentos**
- **Filtro de pastas**
- **Filtro de fotos**
- **Filtro de vídeos**
- **Filtro de músicas**

Como agrupar aplicativos nas áreas de trabalho

Crie áreas de trabalho virtuais para agrupar aplicativos no mesmo local. Na barra de tarefas, clique no ícone **Visão de tarefas** e, em seguida, na **Nova área de trabalho**, abra os aplicativos de que você precisa.

Para mover aplicativos entre áreas de trabalho virtuais, clique em **Visão de tarefas** e, em seguida, arraste o aplicativo que você deseja de uma área de trabalho para outra.

Como usar a Central de Ações

A Central de Ações coloca notificações importantes do Windows e seus aplicativos direito na barra de tarefas, junto com ações rápida, que o direcionam instantaneamente para as configurações e os aplicativos mais utilizados.

Para ver notificações e ações rápidas, clique no ícone da **Central de ações** na barra de tarefas. Você também pode pressionar a tecla com o logotipo do Windows + A.

- **Notificações resumidas**: quando uma notificação é exibida na área de trabalho ou quando você a visualiza na **Central de ações**, é possível expandi-la para ler mais informações ou tomar medidas sem que seja necessário abrir o aplicativo relacionado. Você também pode apagar a notificação, selecionando-a e arrastando-a para fora da tela para a direita, ou clicando no botão **Fechar**.
- **Ícones de Ação Rápida**: ícones de Rápida Ação permitem acessar **Todas as configurações** e os aplicativos que você provavelmente usa com frequência, do Bluetooth à VPN. Selecione a opção **Expandir** para visualizar as configurações e os aplicativos, como localização, período de silêncio, brilho, bluetooth, VPN, economia de bateria, projeto e conexão.

A seguir são apresentadas as opções de **Ação Rápida** na Central de Ações:

- **Modo Tablet**: o modo Tablet torna o Windows mais fácil e intuitivo de utilizar com toque em dispositivos como dispositivos 2 em 1, ou quando você não quer usar um teclado e um mouse. Para ativar o modo tablet, clique no ícone da **Central de Ações** na barra de tarefas e, em seguida, selecione **Modo Tablet**.
- **Conexão**: use essa opção para fazer a conexão com dispositivos Bluetooth e wireless.
- **Todas as configurações**: use essa opção para ajustar as configurações do Windows. Para obter mais informações, consulte Como usar o menu Iniciar.
- **Modo avião**: use essa opção para desativar as funções de transmissão wireless do dispositivo e ativar o **modo avião**.

Como conectar-se a uma impressora ou a um dispositivo externo

Você pode conectar impressoras USB ou impressoras com adaptador USB para paralelo ao dispositivo thin client usando uma porta USB. Siga as instruções de instalação via USB da impressora antes de fazer a conexão a uma porta USB.

Para conectar-se à impressora, adicione a impressora ao dispositivo thin client usando o assistente para **Adicionar impressora**. Para obter mais informações, consulte Como adicionar impressoras.

Se quiser se conectar a um dispositivo externo, adicione o dispositivo ao dispositivo thin client. Para obter mais informações, consulte Como adicionar dispositivos.

Como conectar-se a um monitor

Com base no modelo do thin client, você pode se conectar a um monitor externo usando as seguintes portas:

- Porta HDMI
- Porta VGA
- DisplayPort
- Porta DVI
- Porta DVI-D
- Porta tipo C

Para obter mais informações sobre como configurar dois monitores, consulte Como configurar dois monitores.

Estado de energia

Você pode alterar as opções do estado de energia do dispositivo thin client seguindo as etapas mencionadas aqui:

1. Na barra de tarefas, clique no botão do **menu Iniciar**.
2. Clique em **Ligar/Desligar** no menu Iniciar, e selecione qualquer uma destas opções:
   - **Suspensão** - Esse modo utiliza pouca energia e o dispositivo thin client é iniciado com mais rapidez.
   - **Desligar** - Recomendado para fechar todos os seus programas abertos e para desligar o sistema operacional.
   - **Reiniciar** - O dispositivo thin client é desligado e ligado instantaneamente.

   Para usar as opções de estado de energia, pressione as teclas ALT+F4 e, em seguida, selecione a opção preferida na lista suspensa.

   NOTA: Se o logon automático estiver ativado, o thin client fará imediatamente o logon na área de trabalho padrão do usuário.

3

Aplicativos acessíveis

Quando você faz login no thin client como administrador ou usuário, a área de trabalho do Windows exibe alguns recursos estendidos no menu **Iniciar**.

Você pode executar as seguintes tarefas:

- Navegar na Internet com o Internet Explorer
- Usar o Dell Thin Client Application
- Configurar os serviços de sessão do Citrix Receiver
- Configurar os serviços de sessão da Conexão de Área de Trabalho Remota
- Usar o VMware Horizon Client para conectar-se a uma área de trabalho virtual
- Usar o Ericom PowerTerm Terminal Emulation
- Usar o Ericom Connect-WebConnect Client
- Windows Media Player
- Wyse Easy Setup

NOTA: Aplicativo Indicador de Caps Lock do Teclado: o software do driver de teclado da Dell (KM632) fornece a indicação do status do Caps Lock na área de trabalho. Depois de fazer login no thin client, quando você pressionar a tecla `Caps Lock` para ativar o recurso Caps Lock, o símbolo de bloqueio será exibido na área de trabalho. Se você pressionar novamente a tecla Caps Lock para desativar o recurso Caps Lock, o símbolo de desbloqueio será exibido na área de trabalho.

Como navegar na Internet com o Internet Explorer

Para abrir o Internet Explorer, faça o seguinte:

- Vá para **Iniciar** > **Acessórios do Windows** > **Internet Explorer**.
- Clique duas vezes no ícone do **Internet Explorer** na área de trabalho.

NOTA:

- **Para limitar a gravação no disco, as configurações do Internet Explorer são definidas na fábrica. As configurações impedem o uso da quantidade limitada do espaço em disco disponível. É recomendável que essas configurações não sejam modificadas.**
- **As configurações de armazenamento em cache do Internet Explorer são definidas como 100 MB.**

Como usar o Dell Thin Client Application

Use o Dell Thin Client Application para ver as informações gerais sobre o dispositivo thin client, campos personalizados, disco de RAM, logon automático, atalhos do sistema e informações de suporte.

Para acessar a página Dell Thin Client Application, acesse **Iniciar** > **Dell Thin Client Application**. Você também pode acessar o **Dell Thin Client Application**, clicando no ícone **Dell Thin Client Application** na área de trabalho.

Na barra de navegação esquerda, clique nas seguintes guias:

- **Informações do cliente** - Mostra as informações sobre o dispositivo thin client.
- **QFE** - Mostra a lista de QFEs da Microsoft (anteriormente conhecidos como hot fixes), aplicáveis ao dispositivo thin client.
- **Produtos instalados** - Exibe a lista de aplicativos que estão instalados no dispositivo thin client.
- **Pacotes WDM/WMS** - Exibe a lista de pacotes de WDM e WMS que são aplicados ao thin client.
- **Direitos autorais/patentes** - Exibe informações sobre direitos autorais e patentes.

Depois de fazer login como administrador, você pode ver as guias **Campos personalizados**, **Disco de RAM**, **Logon automático**, **Atalhos do sistema** e **Sobre e suporte** na página do Dell Thin Client Application.

O logotipo Energy Star (um logotipo eletrônico) para a conformidade da Energy Star também é exibido na página do Dell Thin Client Application.

Na guia **Sobre e suporte**, você pode ver as informações relacionadas à versão do aplicativo, diretório de suporte, exportar dados de suporte e modo de exibição de HTML.

Para obter mais informações, consulte Recursos administrativos.

NOTA: As informações mostradas na caixa de diálogo variam de acordo com os diferentes dispositivos thin client e versões de software. Ao fazer login como usuário, apenas algumas guias como Informações do cliente, QFE, Produtos instalados, Pacotes de WDM/WMS, Direitos autorais/patentes e Sobre e suporte são exibidas.

Como configurar os serviços de sessão do Citrix Receiver

O Citrix Receiver é uma tecnologia de computação baseada no servidor que separa a lógica de um aplicativo da sua interface de usuário. O software cliente Citrix Receiver instalado no dispositivo thin client permite que você interaja com a GUI do aplicativo, enquanto todos os processos do aplicativo são executados no servidor.

Os serviços de sessão do Citrix Receiver estão disponíveis na rede usando o Windows Server 2008, Windows Server 2012 ou Windows Server 2016 com serviços de terminal e um dos seguintes programas instalados:

- Citrix Virtual Apps and Desktops 7.5
- Citrix Virtual Apps and Desktops 7.6
- Citrix Virtual Apps and Desktops 7.8
- Citrix Virtual Apps and Desktops 7.9
- Citrix Virtual Apps and Desktops 7.11
- Citrix Virtual Apps and Desktops 7.18

NOTA:

Se você usar um Windows Server 2008 R2, um Servidor de Licença de Acesso para Cliente de Serviços de Terminal (TSCAL) também deve estar acessível na rede. O servidor concede uma licença temporária, que expira após 120 dias. Depois que a licença temporária expirar, adquira e instale as TSCALs no servidor. Você não pode estabelecer uma conexão sem uma licença temporária ou permanente.

Para configurar uma sessão do Citrix Receiver, faça o seguinte:

1. Faça login como administrador.
2. Acesse o Citrix Server usando uma das seguintes opções:
   - No **menu Iniciar**, clique em **Citrix Receiver**.
   - Clique duas vezes no ícone do **Citrix Receiver** na área de trabalho.

   Depois de fazer logon no Citrix Server, a janela Adicionar conta é exibida.
3. Na janela Adicionar conta, digite o endereço IP do servidor.
4. Clique em **Avançar**.
   - Para conexões seguras, digite o `Nome de Domínio Totalmente Qualificado (FQDN)`.
   - Para conexões não seguras, digite o endereço IP.
5. Digite as credenciais do usuário e clique em **Fazer login**.
   Você pode adicionar uma conta fornecendo o endereço IP e visualizar os detalhes do Citrix Receiver.
6. Clique em **Sim** e em **Avançar**.
   A área de trabalho virtual do Citrix Receiver é exibida.
7. Na janela da área de trabalho virtual, acesse **Adicionar aplicativos (+)** > **Todos os aplicativos**.
   Você pode marcar ou desmarcar a caixa de seleção do aplicativo. Os aplicativos selecionados são exibidos na área de trabalho virtual.
8. Na área de trabalho virtual, clique em **Configurações** para atualizar, adicionar ou excluir a conta do servidor, e faça logoff.

Como configurar os serviços de sessão da conexão de área de trabalho remota

A conexão de área de trabalho remota é um protocolo de rede que fornece uma interface gráfica para se conectar a outro computador através de uma conexão de rede.

NOTA: Se você usar um Windows Server ou o Citrix XenApp 5.0 com o Windows Server, um Servidor de Licença de Acesso para Cliente de Serviços de Terminal (TSCAL) também deve estar acessível na rede. O servidor concede uma licença temporária, que expira após 120 dias. Depois que a licença temporária expirar, adquira e instale as TSCALs no servidor. Você não pode estabelecer uma conexão sem uma licença temporária ou permanente.

Para configurar uma conexão de área de trabalho remota:

1. Faça login como usuário ou administrador.
2. No menu **Iniciar**, clique em **Conexão de área de trabalho remota**, ou clique duas vezes no ícone de **Conexão de área de trabalho remota** na área de trabalho.
   A janela Conexão de Área de Trabalho Remota é exibida.
3. Na caixa **Computador**, digite o computador ou o nome de domínio.
4. Para opções avançadas de configuração, clique em **Mostrar Opções**.
   a. Na guia **Geral**, você pode digitar as credenciais de logon, editar ou abrir uma conexão de RDP existente, ou salvar um novo arquivo de conexão de RDP.
   b. Na guia **Vídeo**, gerencie o vídeo e a qualidade da cor de sua área de trabalho remota.
      - Mova o controle deslizante para aumentar ou diminuir o tamanho da sua área de trabalho remota. Para usar a tela inteira, mova o controle deslizante totalmente para a direita.
      - Selecione a qualidade da cor de sua preferência para a sua área de trabalho remota na lista suspensa.
      - Marque ou desmarque a caixa de seleção **Exibir a barra de conexão quando eu usar a tela inteira** para exibir ou ocultar a barra de conexão em modo de tela inteira.
   c. Na guia **Recursos Locais**, configure dispositivos de áudio, teclado ou dispositivos locais e recursos da área de trabalho remota.
      - Na seção Áudio remoto, clique em **Configurações** para ver opções avançadas de configurações de áudio.
      - Na seção **Teclado**, escolha quando e onde aplicar as combinações de teclado.
      - Na seção **Dispositivos e recursos locais**, selecione dispositivos e recursos que você quer usar em sua sessão remota. Clique em **Mais** para obter mais opções.
   d. Na guia **Experiência**, otimize o desempenho de sua sessão remota com base na qualidade da conexão.

      NOTA:

      Se o cache do Unified Write Filter estiver cheio, você pode desativar o Armazenamento de bitmaps em cache na guia Experiência, depois de clicar em Mostrar opções na janela.
   e. Na guia **Avançado**, selecione a ação a ser tomada quando a autenticação do servidor falhar e ajuste as configurações de conexão por meio do Gateway remoto.
5. Clique em **Conecta**r.
6. Para conectar-se à sessão remota, digite as credenciais de login na caixa de diálogo **Segurança**.

   A área de trabalho remota é exibida com a barra de conexão na parte superior se você selecionar a opção **Exibir a barra de conexão**.

Como usar o VMware Horizon Client para conectar-se à área de trabalho virtual

O VMware Horizon Client é um aplicativo de software instalado em nível local que se comunica entre o View Connection Server e o sistema operacional do thin client. Ele fornece acesso a áreas de trabalho virtuais hospedadas centralizadamente a partir de thin clients. Os serviços de sessão do VMware podem ser disponibilizados na rede depois de instalar o VMware Horizon 6. Ele fornece áreas de trabalho e aplicativos virtualizados ou hospedados por meio de uma única plataforma para usuários finais. Para conectar-se a uma área de trabalho virtual, use a janela VMware Horizon Client.

Para abrir e usar a janela VMware Horizon Client:

1. Faça login como usuário ou administrador.
2. Acesse a janela VMware Horizon Client usando uma das seguintes opções:
   - No **menu Iniciar**, clique em **VMware** > **VMware Horizon Client**.
   - Clique duas vezes no ícone **WMware Horizon Client** na área de trabalho.

   A janela VMware Horizon Client é exibida.
3. Na janela VMware Horizon Client, use as seguintes diretrizes:
   a) Para adicionar uma nova conexão de servidor, clique na opção **Novo servidor** ou clique duas vezes no ícone **Adicionar servidor** na janela VMware Horizon Client.

A caixa de diálogo **WMware Horizon Client** é exibida.

b) Na caixa de diálogo **VMware Horizon Client**, digite um nome de host ou um endereço IP de um VMware Horizon Connection Server na caixa de servidor de conexão.

c) Clique em **Conecta**r.

d) Na caixa de diálogo **Login**, digite o nome do usuário e a senha de login nas respectivas caixas.

e) Na lista suspensa **Domínio**, selecione o domínio onde está localizado o servidor.

f) Clique em **Fazer login**.

O VMware Horizon Client conecta-se à área de trabalho selecionada. Depois que a conexão é estabelecida, a lista de áreas de trabalho publicadas é exibida.

g) Clique com o botão direito no ícone da área de trabalho ou do aplicativo específico e, em seguida, clique em **Abrir** para se conectar a esse aplicativo ou a essa área de trabalho.

Para obter mais informações sobre o VMware Horizon Client, consulte o site www.vmware.com.

NOTA:

Modo de verificação de certificado - O modo de verificação de certificado determina como o cliente se comporta quando ele não consegue verificar se a conexão com o servidor é segura. A Dell recomenda que você não altere essa configuração, a menos que orientado pelo administrador do sistema.

Para acessar o modo de verificação de certificado, clique no ícone localizado no canto superior direito da janela e, em seguida, clique em Configurar SSL na lista suspensa. Na caixa de diálogo Configuração SSL do VMware Horizon Client, selecione uma das seguintes opções com base em suas necessidades:

- **Nunca se conectar a servidores não confiáveis**
- **Avisar antes de se conectar a servidores não confiáveis**
- **Não verificar o servidor, identificar certificados**

Como usar o Ericom Connect and WebConnect Client

O Ericom Connect and WebConnect Client fornece a você acesso remoto a áreas de trabalho e aplicativos do Windows a partir de qualquer telefone ou tablet compatível. Ele é dedicado ao acesso gerenciado do broker. As conexões do Ericom Connect and PowerTerm WebConnect usam o Gateway Seguro como o endereço. Você pode acessar o Ericom Connect-Web Connect Client como um aplicativo independente ou em uma rede.

Para acessar o Ericom Connect and WebConnect Client como um aplicativo independente:

1. Faça login como usuário ou administrador.
2. Acesse **Iniciar** > **Ericom Connect-WebConnect client** > **Ericom Connect-WebConnect client** ou clique duas vezes no ícone **Ericom Connect-WebConnect client** na área de trabalho.
   A janela de login Ericom AccessPad é exibida.
3. Na janela de login Ericom AccessPad, digite as credenciais e clique em **Login**.
   A janela <2>DELL – Zona de aplicativos Ericom</2> é mostrada.
   NOTA: Por padrão, a janela de login Ericom AccessPad é exibida. Para configurar a IU para o idioma de sua preferência, clique no ícone do globo no canto inferior direito da janela e selecione o idioma desejado na lista suspensa.
4. Na janela <6>DELL – Zona de aplicativos Ericom</6>, aplicativos publicados como **Blaze demo server**, **RDP demo server**, **Ericom server** e **Paint** serão exibidos.
   Clique duas vezes em qualquer um deles para acessá-los.

   Você também pode adicionar seus próprios aplicativos a partir do site do servidor.
5. Para criar um atalho na área de trabalho, clique em **Opções** > **Criar um atalho na área de trabalho** na janela DELL - Ericom Application Zone.
6. Para fazer logout, clique em **Arquivo** > **Logout** na janela DELL- Ericom Application Zone.

Para acessar o Ericom Connect-WebConnect client por meio do navegador da Web:

1. Clique duas vezes no ícone do **Internet Explorer**.

   A página da Web do Internet Explorer é exibida.

2. Digite o URL `http://serverIP/FQDNWebConnect6.0/AppPortal/Index.asp` para acessar o Ericom Power Term Emulation.

   A página do PowerTerm WebConnect Application Portal é exibida.
3. Na página PowerTerm WebConnect Application Portal, digite as credenciais e o nome de domínio.
4. Clique em **Fazer login**.
5. Depois de fazer login, áreas de trabalho e aplicativos publicados como, por exemplo, o **Blaze demo server**, **RDP demo server** e **Paint** serão exibidos.

   Clique duas vezes em qualquer um deles para acessá-los em uma nova página da Web.

   Você também pode adicionar seus próprios aplicativos a partir do site do servidor.
6. Clique em **Logout** no lado esquerdo da página PowerTerm WebConnect Application Portal para finalizar a sessão do Ericom Power Term WebConnect.

Como usar o Ericom PowerTerm Terminal Emulation

Para gerenciar suas conexões usando o Ericom PowerTerm Terminal Emulation, faça o seguinte:

1. Abra a janela TELNET : PowerTerm InterConnect para thin clients, usando uma das seguintes opções mencionadas:
   - Clique duas vezes no ícone **PowerTerm Terminal Emulation** na área de trabalho.
   - No **menu Iniciar**, clique em **Ericom PowerTerm Terminal Emulation** > **PowerTerm Terminal Emulation.**
2. Na caixa de diálogo **Conectar**, acesse **Tipo de sessão** > **TELNET** para configurar a conexão de sua escolha.

Windows Media Player

O Windows Media Player oferece uma interface intuitiva e fácil de usar para reproduzir arquivos de mídia digital. Ele organiza sua coletânea de mídia digital, e você pode gravar CDs com suas músicas favoritas, copiar músicas de CDs, sincronizar arquivos de mídia digital para um dispositivo portátil e fazer compras de conteúdo de mídia digital em lojas on-line. Para obter mais informações, consulte a documentação do Windows Media Player, em https://support.microsoft.com.

Wyse Easy Setup

O Wyse Easy Setup permite que os administradores implantem configurações de maneira rápida e fácil em thin clients.

O Wyse Easy Setup permite que você:

- Crie um cliente focado em um navegador dedicado ajustando as configurações do Internet Explorer.
- Configure várias conexões de broker como o Citrix, VMware e Remote Desktop Protocol (RDP).
- Configure um dispositivo para criar um aplicativo dedicado para obter uma linha específica de negócios.

Você pode criar um modo de quiosque para bloquear um dispositivo do Windows para evitar que os usuários acessem qualquer recurso ou função no dispositivo fora do modo de quiosque. Você também pode personalizar a interface do quiosque para habilitar ou desabilitar o acesso do usuário a configurações específicas.

Para obter mais informações, consulte o Guia do administrador do Wyse Easy Setup e as Notas da versão em https://downloads.dell.com/wyse.

Overlay Optimizer

O Overlay Optimizer é um componente de software que funciona com o Microsoft Unified Write Filter (UWF). O Overlay Optimizer oferece proteção contra gravação e estende o tempo de atividade dos dispositivos. O Overlay Optimizer funciona no sistema operacional Windows 10 IoT Enterprise.

O UWF protege o disco armazenando as alterações na sobreposição de RAM. Quando um aplicativo tenta gravar dados no disco, o filtro de gravação redireciona as operações de gravação para a sobreposição de RAM. O tamanho da sobreposição é pré-configurado e não pode aumentar dinamicamente. Quando a sobreposição ficar sem espaço por um período, o dispositivo será reiniciado.

O Overlay Optimizer monitora o espaço de sobreposição dos UWFs e o conteúdo. O Overlay Optimizer identifica um maior consumo de espaço de sobreposição no filtro de gravação e move o conteúdo não utilizado para a sobreposição de disco do Otimizador de sobreposição. Limpar a sobreposição UWF estende o tempo de atividade do dispositivo.

Para obter mais informações, consulte *Notas de versão do Overlay Optimizer* em https://downloads.dell.com/wyse/.

Dell Secure Client

O Dell Secure Client é um software de segurança para thin clients baseados em Windows. Este software aplica restrições às alterações feitas em arquivos, pastas e exclusões de registro.

Principais recursos do Dell Secure Client

Os itens a seguir são os principais recursos do Dell Secure Client:

- A lista de arquivos, pastas e exclusões de registro no filtro de gravação é exibida.
- O status do Dell Secure Client em relação ao Filtro de gravação unificado é exibido.
- O serviço Dell Secure Client atua como um mecanismo de política. Ele combina as políticas das pastas aninhadas e as atualiza no hive do registro.
- Você pode usar a interface de linha de comando do Dell Secure Client para atualizar o arquivo .csv com as políticas, quando o administrador fizer qualquer alteração usando a interface do usuário.
- O administrador pode usar o Dell Secure Client para adicionar, visualizar e remover políticas dos arquivos e registros excluídos no filtro de gravação.
- Você pode adicionar, remover, exibir ou modificar a política com base no nome de usuário, aplicativo e tempo de acesso para cada entrada na lista de exclusões de filtro de gravação.

  NOTA: O nome de usuário e o nome do aplicativo são obrigatórios.
- Você pode importar e exportar os dados de configuração da política no formato .csv ou .json.
- Você pode exportar a política como um arquivo .exe executável independente (SCE). O arquivo SCE encapsula a configuração da política no formato .json.
- É fornecido suporte multilíngue para a interface do usuário do administrador.
- A condição para manter as configurações do Dell Secure Client foi adicionada pelo usuário após você reiniciar o thin client.
- Você pode configurar as políticas somente depois de desativar o filtro de gravação.
- As políticas padrão são aplicadas a todos os usuários quando o Dell Secure Client está ativado.
- Você pode adicionar uma política a um usuário ou a um grupo usando a interface do usuário ou a interface de linha de comando do Dell Secure Client. Essa política é aplicada juntamente com a política padrão quando você faz login no respectivo usuário ou grupo.
- As políticas são salvas no formato .csv que é criptografado.

Acessando o Dell Secure Client

Você pode acessar o Dell Secure Client usando qualquer um dos seguintes métodos:

- Com uma conta de administrador:
  1. Faça login como administrador.
  2. Vá para **Iniciar** > **Dell** > **DellSecureClient**.
- Com uma conta de usuário:
  1. Faça login como usuário.
  2. Vá para **Iniciar** > **Dell** > **DellSecureClient**.

     A janela Controle de Conta de Usuário é exibida.
  3. Digite a senha do administrador e clique em **Sim**.

Configurando o Dell Secure Client

Você pode configurar o Dell Secure Client usando qualquer um dos seguintes métodos:

- Wyse Management Suite
- Interface do usuário do administrador local — GUI do Dell Secure Client

Configurando a política por meio da interface do usuário do Dell Secure Client

Você pode importar ou exportar uma configuração da interface do usuário do Dell Secure Client.

Importar uma configuração

1. Desative o filtro de gravação.
   O thin client é reiniciado.
2. Faça login como administrador.
3. Clique duas vezes no aplicativo Dell Secure Client.
   A interface do usuário do Dell Secure Client é exibida.
4. Clique em **Exportar/importar**.
5. Digite o caminho do arquivo de configuração.
6. Clique em **Importar**.
   A política de configuração é criptografada e salva como um arquivo .csv, em `C:\Arquivos de programas\Wyse\DellSecureClient\`.

Exportar uma configuração

1. Desative o filtro de gravação.
   O thin client é reiniciado.
2. Faça login como administrador.
3. Clique duas vezes no aplicativo Dell Secure Client.
   A interface do usuário do Dell Secure Client é exibida.
4. Clique em **Exportar/importar**.
5. Digite o caminho do arquivo de configuração.
6. Selecione as opções de formato de arquivo: csv (configurações do Dell Secure Client) ou .exe (pacote instalável).
7. Clique em **Exportar**.
   A política de configuração é descriptografada e exportada.

Formato CSV

O arquivo .csv de saída está no seguinte formato:

Tabela 1. formato .csv

Tipo de política	Arquivo/pasta	Aplicativos	Conta NT	Intervalo de tempo (opcional)
arquivo	`C:\Temp\Sample.txt`	`C:\Windows\System32\notepad.exe`	Usuário	0700-1900
pasta	`C:\Temp\`	`C:\Arquivos de programas\Windows NT\Accessories\Wordpad.exe`	Usuário	0700-1900
arquivo	`C:\Temp\Sample2.txt`	`C:\Windows\System32\notepad.exe`	Admin1	
pasta	`C:\Program Files\Windows Defender`	`C:\Windows\System32\mspaint.exe`	Sistema	
registro	`HKLM\SOFTWARE\WOW6432Node\3DMAX`	`C:\Arquivos de programas (x86)\AutoCAD\audtocadx86.exe`	Usuário	

Tipo de política	Arquivo/pasta	Aplicativos	Conta NT	Intervalo de tempo (opcional)
registro	HKLM\SOFTWARE\WOW6432Node\3DMAX	C:\Arquivos de programas (x86)\AutoCAD\audtocadx86.exe	Admin1	
registro	HKLM\SOFTWARE\WOW6432Node\Dell\CommandUpdate	C:\Arquivos de programas\Dell\Command Monitor\dataeng\bin\dsm_sa_datmgr64.exe	Sistema	
registro	HKLM\SOFTWARE\WOW6432Node\Dell\CommandUpdate	C:\Arquivos de programas\Dell\Command Monitor\dataeng\bin\dsm_sa_datmgr64.exe	Admin2	0900-1000

Formato JSON

O arquivo .json de saída está no seguinte formato:


```
{
  "deviceElements": null,
  "deviceElementsV2": null,
  "fullConfiguration": false,
  "shouldSendRemoteCommand": false,
  "isJailBroken": false,
  "compliantStatus": 0,
  "configCompliantStatus": 0,
  "passcodeCompliant": true,
  "encryptionCompliantStatus": 1,
  "computeJailbreak": true,
  "isCaValidationOn": false,
  "personInfoLean": null,
  "lastUpdatedAt": 1534142918777,
  "passcodeProfileDescription": null,
  "deviceQueryId": null,
  "deviceQueryStatus": null,
  "configurations": {
    "contentProvider": null,
    "description": null,
    "configSettings": [
      {
        "targetOS": null,
        "configName": "rcDellSecureClientSettings",
        "configItems": [
          {
            "itemKey": "rcDellSecureClientSettings",
            "itemValue": [
              [
                {
                  "itemKey": "policyType",
                  "itemValue": "file",
                  "itemValueExtra": null,
                  "valueType": "STRING"
                },
                {
                  "itemKey": "location",
                  "itemValue": " C:\\Program Files\\AutoCAD ",
                  "itemValueExtra": null,
                  "valueType": "STRING"
                },
```

```
                {
                  "itemKey": "application",
                  "itemValue": " C:\\Program Files\\AutoCAD\\audtocadx64.exe ",
                  "itemValueExtra": null,
                  "valueType": "STRING"
                },
                {
                  "itemKey": "user",
                  "itemValue": " User ",
                  "itemValueExtra": null,
                  "valueType": "STRING"
                },
                {
                  "itemKey": "duration",
                  "itemValue": "0700-1900",
                  "itemValueExtra": null,
                  "valueType": "STRING"
                }
              ],
              [
                {
                  "itemKey": "policyType",
                  "itemValue": "registry",
                  "itemValueExtra": null,
                  "valueType": "STRING"
                },
                {
                  "itemKey": "location",
                  "itemValue": "    HKEY_LOCAL_MACHINE\\SOFTWARE\\WOW6432Node\\3DMAX ",
                  "itemValueExtra": null,
                  "valueType": "STRING"
                },
                {
                  "itemKey": "application",
                  "itemValue": " C:\\Program Files (x86)\\AutoCAD\\audtocadx86.exe",
                  "itemValueExtra": null,
                  "valueType": "STRING"
                },
                {
                  "itemKey": "user",
                  "itemValue": "User ",
                  "itemValueExtra": null,
                  "valueType": "STRING"
                },
                {
                  "itemKey": "duration",
                  "itemValue": "0700-1900",
                  "itemValueExtra": null,
                  "valueType": "STRING"
                }
              ]
            ],
            "itemValueExtra": null,
            "valueType": "JSON"
          }
        ],
        "contentVersion": "2.3.0"
      }
    ]
  },
  "allowUnregistration": true,
  "businessRuleInfo": null,
  "currentBiosAdminPassword": null,
  "mqttUrl": "tcp://10.150.38.10:1883",
  "wmsUrl": "https://brl-hackthon-win12R2:443/ccm-web",
  "heartbeatIntervalInMins": 0,
  "checkInIntervalInHours": 0,
  "groupToken": null,
  "personalDeviceSettings": null,
  "wmsVersion": "4.3.0",
  "maxCheckinIntervalInHours": 0
}
```

Arquivo de extração automática

O arquivo de saída .exe de extração automática consiste no arquivo de configuração de política no formato .json. O arquivo .exe de extração automática invoca o valor `dscmgr` com comando de importação usando o arquivo de configuração como uma entrada.

O arquivo pode ser usado para importar a configuração para vários clients por meio da política avançada de aplicativos no Wyse Management Suite. O arquivo também retorna códigos de sucesso quando você importa uma política.

Implementando uma configuração

Você pode implementar uma configuração em vários thin clients usando os seguintes métodos:

- Interface do usuário do Dell Secure Client
- Wyse Management Suite

Opções de linha de comando

Tabela 2. Opções de linha de comando

Linha de comando	Descrição
`dscmgr /help or dscmgr ?`	Use esse comando para exibir o menu **Ajuda** do Dell Secure Client.
`dscmgr /init [Mode]`	Use esse comando para iniciar o Dell Secure Client no modo de hash do aplicativo ou de caminho do aplicativo. O modo de aplicativo é o padrão. Se você não digitar algum valor, o modo padrão será selecionado. [Modo] — Insira o modo para ativar ou bloquear o acesso. Você pode usar o hash binário do aplicativo ou o caminho do aplicativo. Esse parâmetro é opcional.
`dscmgr /getappauthenticationmode`	Esse comando exibe o modo de autenticação de aplicativo que foi usado.
`dscmgr /addpolicy <Caminho do arquivo, pasta ou chave de registro> <Nome do usuário local do Windows> <Nome do aplicativo> [Time Duration] [Policy Type]`	Use esse comando para adicionar uma política ao Dell Secure Client. Esse comando será ativado depois que você reiniciar o thin client. `Caminho do arquivo, pasta ou chave de registro` — As modificações no arquivo, na pasta ou na chave de registro são monitoradas pelo Dell Secure Client. O caminho inserido deve estar disponível na lista de exclusões do UWF. `Nome de usuário local do Windows` — Digite o nome de usuário do recurso para conceder acesso ao Dell Secure Client. `Nome do aplicativo` — Insira o nome do aplicativo pelo qual as modificações serão ativadas para o recurso. `Duração de tempo` — Insira o período durante o qual as modificações serão ativadas. Esse parâmetro é opcional. Se você não digitar algum valor, poderá modificar a política a qualquer momento. `Tipo de política` — Determina o tipo de política. O valor pode ser apenas um arquivo ou registro. Esse parâmetro é opcional. Por exemplo, o comando `dscmgr /addpolicy C:\Users\Administrator\Test.txt Administrator C:\Windows\System32\notepad.exe 0900-1100` permite que um administrador modifique `C:\Users\Administrator\Test.txt` entre as 9h00 e as 11h00 usando um bloco de notas. **NOTA: Para usar esse comando, o filtro de gravação deve estar desativado.**

Linha de comando	Descrição
`dscmgr /removepolicy <Caminho do arquivo, pasta ou chave de registro> <Nome do usuário local do Windows> <Nome do aplicativo> [Time Duration]`	Use esse comando para remover uma política do Dell Secure Client. Esse comando será ativado depois que você reiniciar o thin client. `Caminho do arquivo, pasta ou chave de registro` — As modificações no arquivo, na pasta ou na chave de registro são monitoradas pelo Dell Secure Client. O caminho inserido deve estar disponível na lista de exclusões do UWF. `Nome de usuário local do Windows` — Digite o nome de usuário do recurso para conceder acesso ao Dell Secure Client. `Nome do aplicativo` — Insira o nome do aplicativo pelo qual as modificações serão ativadas para o recurso. `Duração de tempo` — Insira o período durante o qual as modificações serão ativadas. Esse parâmetro é opcional. Se você não digitar algum valor, poderá modificar a política a qualquer momento. `Tipo de política` — Determina o tipo de política. O valor pode ser apenas um arquivo ou registro. Esse parâmetro é opcional. Por exemplo, o comando `dscmgr /removepolicy C:\Users\Administrator\Test.txt Administrator C:\Windows\System32\notepad.exe 0900-1100` remove o acesso a `C:\Users\Administrator\Test.txt` para um administrador entre as 9h00 e as 11h00 usando o bloco de notas. **NOTA: Para usar esse comando, o filtro de gravação deve estar desativado.**
`dscmgr /enabledsc`	Use esse comando para ativar o Dell Secure Client. Esse comando será ativado depois que você reiniciar o thin client. **NOTA: Para usar esse comando, o filtro de gravação deve estar desativado.**
`dscmgr /disabledsc`	Use esse comando para desativar o Dell Secure Client. Esse comando será ativado depois que você reiniciar o thin client. **NOTA: Para usar esse comando, o filtro de gravação deve estar desativado.**
`dscmgr /exportpolicy <Caminho do arquivo>`	Use esse comando para exportar as políticas do Dell Secure Client para um arquivo. `Caminho do arquivo` — Insira o caminho do arquivo para o qual as políticas devem ser exportadas. A extensão do arquivo deve ser .json ou .csv. Se o arquivo não estiver presente, um novo arquivo será criado. Se o arquivo já existir, o conteúdo do arquivo será atualizado. **NOTA: Para usar esse comando, o filtro de gravação deve estar desativado.**
`dscmgr /importpolicy <Caminho do arquivo>`	Use esse comando para importar as políticas de um arquivo para o Dell Secure Client. O arquivo deve conter um conjunto válido de políticas, conforme mencionado no comando `/addpolicy`. Esse comando será ativado depois que você reiniciar o thin client. `Caminho do arquivo` — Insira o caminho do arquivo no qual as políticas devem ser importadas. A extensão do arquivo deve ser .json ou .csv. **NOTA: Para usar esse comando, o filtro de gravação deve estar desativado.**

Linha de comando	Descrição
`dscmgr /exportinstallablepackage <Caminho da pasta>`	Use esse comando para exportar as políticas para o Dell Secure Client como um arquivo executável de extração automática. O arquivo pode ser usado para implementar as mesmas políticas em vários dispositivos. `Caminho da pasta` — Insira o caminho do arquivo para o qual as políticas devem ser exportadas. O arquivo `DefaultDSCPolicy.exe` é criado na pasta. **NOTA: Para usar esse comando, o filtro de gravação deve estar desativado.**
`dscmgr /getdscstate`	Use esse comando para visualizar o estado atual do Dell Secure Client. Se o Dell Secure Client estiver ativado, **1** será exibido. Se estiver desativado, **0** será exibido.

Gerar e visualizar arquivos de registro

Os arquivos de registro contêm um histórico de eventos do Dell Secure Client. Esta seção descreve as etapas para gerar e visualizar os arquivos de registro.

1. Acesse `C:\Arquivos de programas\Wyse\WyseLoggingLevel.ini`.
2. Atualize o parâmetro `[LoggingLevel] DSCSVC` para 4.
   Você pode visualizar os arquivos de registro de diferentes componentes do Dell Secure Client, em `C:\Wyse\WDA\DellSecureClient`.

Dicas e práticas recomendadas

Esta seção fornece informações sobre as práticas recomendadas e dicas que ajudam você a trabalhar de forma eficaz no Dell Secure Client.

- Antes de ativar e configurar o Dell Secure Client, certifique-se de que a sobreposição UWF esteja definida como RAM.
- É recomendável desativar o filtro de gravação antes de configurar a interface do usuário do Dell Secure Client.
- É recomendável não desativar o Dell Secure Client para proteger a lista de exclusões do filtro de gravação.
- As políticas são exibidas nas respectivas pastas, no campo **Exclusão de filtro de gravação**, na interface do usuário do Dell Secure Client.

Códigos de erro

Tabela 3. Códigos de erro

Código de erro	Descrição
localInvalidFileError	Selecione um caminho do arquivo válido para exportar a configuração do Dell Secure Client.
localExportFormatMsg	Selecione o formato de exportação.
cliPolicyExistsErrorMsg	A política já existe.
cliPolicyDoesntExist	A política não existe.
cliInvalidPolicy	Política inválida para a configuração.
cliIgnorePolicy	Ignorar a política.
cliInvalidFileExtension	A extensão de arquivo inválida foi inserida.
localEnterAppPath	Digitar caminho do aplicativo.
localEditSuccess	A edição foi um sucesso.
localFinishAddEditMsg	Completar a mensagem de adição ou edição.

Código de erro	Descrição
localExceptionInConfigMsg	Valor de exceção inválido na política do arquivo de configuração.
localWriteFilterEnabledWarning	Para modificar o estado e as políticas do Dell Secure Client, você precisa desativar o filtro de gravação.
localInvalidData	Dados inválidos inseridos no índice.
localAbortEditMsg	Anulando a edição.
cliErrorDSCSate	Erro ao consultar o estado do Dell Secure Client.
localCorruptFileErrorMsg	O arquivo de configuração pode estar corrompido. Se o arquivo estiver corrompido na próxima inicialização, as políticas padrão serão aplicadas.
cliPolicyLocationErrorMsg	Local da política não encontrado na lista de exclusão do UWF.
cliInvalidCommandErrorMsg	Comando inválido. Digite `dscmgr help` para obter a lista de comandos disponíveis no Dell Secure Client.
cliInvalidCommand	Comando inválido
cliErrorConfigFileRead	Erro ao ler o arquivo de configuração.
localAddPolicyErrorMsg	Campos obrigatórios não fornecidos. A política não pode ser adicionada.

4

Recursos administrativos

O **administrador** é um perfil de usuário padrão criado para o usuário que é membro do grupo de administradores.

Para fazer login como administrador, consulte Logon automático e manual. Ao fazer login no dispositivo thin client como administrador, você pode acessar certos recursos notáveis estendidos no Painel de Controle.

Para acessar o **Painel de Controle**, na barra de tarefas, clique em **Menu Iniciar** > **Painel de Controle**.

Você pode executar as seguintes funções como administrador:

- Como usar as ferramentas administrativas
- Como usar TPM e BitLocker
- Como usar campos personalizados
- Como configurar o tamanho do disco de RAM
- Como ativar o logon automático
- Como usar atalhos do sistema
- Como visualizar e configurar componentes do SCCM
- Como adicionar dispositivos
- Como adicionar impressoras
- Como configurar dois monitores.
- Como usar a caixa de diálogo de som.
- Como configurar a região e as preferências de idioma.
- Como gerenciar usuários e grupos com contas de usuário.
- Como usar o Windows Defender.
- Como usar o Windows Defender Advanced Threat Protection (ATP)
- Defesa contra ameaças
- Endpoint Security Suite Enterprise
- Como usar a ferramenta CAD.
- Como configurar o Wyse Device Agent.
- Como configurar o Citrix HDX RealTime Media Engine.

Como usar ferramentas administrativas

Para acessar a janela <6>Ferramentas administrativas</6>, clique em **Iniciar** > **Painel de controle** > **Ferramentas administrativas**.

Você pode usar a janela Ferramentas Administrativas para executar as seguintes tarefas:

- Como configurar os serviços de componentes
- Como gerenciar os serviços

Como configurar serviços de componentes

Para acessar e configurar os serviços de componentes, o visualizador de eventos e os serviços locais, use o console de **Serviços de componentes**.

Para obter mais informações, consulte *Ferramentas administrativas no Windows 10* em https://support.microsoft.com.

Como visualizar os eventos

Para visualizar mensagens de monitoramento e solução de problemas do Windows e de outros programas, use a janela Visualizador de Eventos.

No console Serviços de Componentes, clique no ícone do **Visualizador de Eventos** na árvore **Raiz do Console**. O resumo de todos os registros dos eventos que ocorreram no computador será exibido. Para obter mais informações, consulte o *Visualizador de eventos*em https://support.microsoft.com.

Como gerenciar os serviços

Para visualizar e gerenciar os serviços instalados no dispositivo thin client, use a janela Serviços. Para abrir a janela **Serviços**, acesse **Iniciar** > **Painel de Controle** > **Serviços de Ferramentas Administrativas**.

1. No console de **Serviços de Componentes**, clique no ícone de **Serviços** da árvore do console.
   A lista de serviços é exibida.
2. Clique com o botão direito em um serviço de sua escolha. Você pode executar as operações Iniciar, Parar, Pausar, Retomar e Reiniciar.

   Você pode selecionar o Tipo de inicialização na lista suspensa:

   - Automática (Atraso na Inicialização)
   - Automático
   - Manual
   - Desabilitado

   Para obter mais informações, consulte *Administração de serviços de componente,* em https://support.microsoft.com.

   NOTA: Verifique se o Filtro de Gravação está desativado quando gerenciar os serviços.

Como usar TPM e BitLocker

Trusted Platform Module (TPM) - Um TPM é um microchip que fornece funções básicas relacionadas à segurança, que envolvem principalmente chaves de criptografia.

Criptografia de Unidade de Disco BitLocker (BDE) - A BDE é um recurso de criptografia completa de disco que foi projetado para proteger os dados, fornecendo criptografia para volumes inteiros. Por padrão, ela usa o algoritmo de criptografia de AES no modo de Encadeamento de Blocos de Criptografia (CBC) com uma chave de 128 bits. Esse algoritmo é combinado com o difusor Elephant para a segurança extra específica da criptografia de disco.

O Windows 10 IoT Enterprise não suporta sysprep em um dispositivo criptografado do BitLocker. Devido a essa limitação, não é possível criptografar o dispositivo, executar um sysprep e obter a imagem. Para resolver esse problema, você precisa adicionar ou modificar o script relacionado ao TPM. O dispositivo não deve ser criptografado antes do sysprep (obtido). A criptografia do dispositivo é controlada pelo script de pós-push que usa o script `TPM_enable.ps1` localizado em `C:\Windows\setup\tools\`. Esse script deve ser incluído antes de ativar o UWF e após scripts sysprep. O PIN usado para criptografar o cliente deve ser passado para o script como um argumento.

Criptografar a memória flash usando TPM e BitLocker

Pré-requisitos

Se a memória flash tiver sido criptografada anteriormente, faça o seguinte para limpar o TPM:

1. Digite o modo do BIOS.
2. Na configuração do TPM, ajuste a opção **Alterar status do TPM** para **Limpo** e, em seguida, aplique as configurações.
3. Reinicialize o dispositivo e entre no modo do BIOS novamente.
4. Configure a opção **Alterar status do TPM** para **Permitir e ativar**.

Para criptografar a memória flash usando TPM e BitLocker, faça o seguinte:

1. Ative o TPM no menu do **BIOS**.
2. Modifique a parte relacionada ao TPM do script, com base na solução de imagem.
3. Remova a marca de comentário das linhas abaixo e atualize o pin para a criptografia de TPM no método de imagem Custom FICore em `C:\Windows\Setup\CustomSysprep\Modules\Post_CustomSysprep.psm1`

   - `#cd C:\windows\setup\Tools\TPM\`
   - `#.\TPM_enable.ps1 -pin 1234`
4. Remova a marca de comentário das linhas abaixo e atualize o pin para a criptografia de TPM no push do SCCM em `C:\Windows\Setup\ConfigMgrSysprep\Modules\Admin_ConfigMgrSysprep.psm1`

   - `#cd C:\windows\setup\Tools\TPM\`
   - `#.\TPM_enable.ps1 -pin 1234`
5. Remova a marca de comentário das linhas abaixo e atualize o pin para a criptografia de TPM no ambiente Non-Factory (WDM, WSI, solução de imagem USB) em `Post_CustomSysprep.psm1`

   - `#cd C:\windows\setup\Tools\TPM\`

- `#.\TPM_enable.ps1 -pin 1234`

Como configurar conexões Bluetooth

Você pode usar o dispositivo thin client com outros dispositivos Bluetooth, se ele tiver o recurso Bluetooth.

NOTA: Para manter as configurações, desative o Unified Write Filter (UWF) (Unified Write Filter - UWF) e configure o Application Launch Manager (Gerenciador de Inicialização do Aplicativo) e o xData Cleanup Manager (Gerenciador de Limpeza xData). Para obter mais informações, consulte Antes de configurar thin clients.

Para configurar conexões Bluetooth, consulte *Conectar um dispositivo Bluetooth* em https://support.microsoft.com.

Como ajustar configurações de rede wireless local

Para ajustar as configurações de rede wireless local, use a janela Configurar uma nova conexão ou rede, se o suporte wireless for permitido no dispositivo thin client.

Para definir as configurações de rede local wireless, consulte *Configurando uma rede wireless* em https://support.microsoft.com.

Como usar campos personalizados

Para inserir strings de configuração para que sejam usadas pelo Wyse Device Manager (WDM) e pelo Wyse Management Suite (WMS), use a caixa de diálogo **Campos personalizados**. As strings de configuração podem conter informações, como o local, usuário, administrador e assim por diante.

Para inserir as informações que podem ser usadas pelo servidor do WDM e do Wyse Management Suite, faça o seguinte:

1. Faça login como administrador.
2. Acesse **Iniciar** > **Dell Thin Client Application**.
   A janela Dell Thin Client Application é mostrada.
3. Na barra de navegação esquerda, clique em **Campos Personalizados**.
4. Digite as informações de campo personalizado nas caixas de campo personalizado e clique em **Aplicar**.

   As informações de campo personalizado são transferidas para o registro do Windows que é então disponibilizado para o servidor WDM/WMS.

   CUIDADO:

   Para salvar as informações permanentemente, desative/ative o Unified Write Filter (UWF). Para obter mais informações, consulte Antes de configurar thin clients.

   NOTA:

   Para obter mais detalhes sobre as informações do campo personalizado, consulte a documentação do WDM e do WMS no site www.dell.com/support.

Como configurar o tamanho do disco de RAM

O disco de RAM é um espaço de memória volátil usado para o armazenamento temporário de dados. Ele também pode ser usado para o armazenamento temporário de outros dados a critério do administrador. Para obter mais informações, consulte Como salvar arquivos e usar unidades locais

Os itens a seguir são armazenados no disco de RAM:

- Cache da página da Web do navegador
- Histórico do navegador
- Cookies do navegador
- Cache do navegador
- Arquivos temporários da Internet
- Spool de impressão
- Arquivos temporários de usuário/sistema

Para configurar o tamanho do disco de RAM, faça o seguinte:

1. Faça login como administrador.
2. Acesse **Iniciar** > **Aplicativo Dell Thin Client**.
   A janela Aplicativo Dell Thin Client é mostrada.
3. Na barra de navegação esquerda, clique em **Disco de RAM**.
4. No campo **Tamanho do disco de RAM**, digite ou selecione o tamanho do disco de RAM que você deseja configurar e, em seguida, clique em **Aplicar**.

   Se você alterar o tamanho do disco de RAM, deverá reiniciar o sistema para que as alterações sejam efetivadas.

   NOTA:

   Para salvar as informações permanentemente, desative o Unified Write Filter (UWF) (Unified Write Filter - UWF). Para obter mais informações, consulte Before Configuring your thin clients (Antes de configurar thin clients).

Como ativar o logon automático

O logon automático na área de trabalho do usuário é ativado por padrão no dispositivo thin client. Para ativar ou desativar o log-on automático e alterar o nome de usuário, senha e domínio padrão de um thin client, use o recurso de log-on automático.

Para ativar/desativar o log-on automático:

1. Faça login como administrador.
2. Acesse **Start (Iniciar)** > **Dell Thin Client Application**.
   A janela Dell Thin Client Application (Aplicativo Dell Thin Client) é mostrada.
3. Na barra de navegação esquerda, clique em **Auto Logon** (Logon automático).
4. Para iniciar com a página de log-on do administrador, digite `Admin` no campo **Default User Name** (Nome de usuário padrão).

   NOTA: Por padrão, a caixa de seleção Enable Auto Logon (Ativar o logon automático) é selecionada.
5. Se quiser iniciar com a janela Logon (Log-on) com as seleções de usuário e administrador padrão e outras contas, desmarque a caixa de seleção **Enable Auto Logon** (Ativar o log-on automático).

   CUIDADO: Para salvar as informações permanentemente, desative/ative o Unified Write Filter (UWF) (Filtro de Gravação Unificado - UWF). Para obter mais informações, consulte Before Configuring your thin clients (Antes de configurar thin clients).

   NOTA:

   Se o log-in automático estiver ativado e você fizer log-off da sua área de trabalho atual, a tela de bloqueio será exibida. Clique em qualquer lugar da tela de bloqueio para ver a janela Logon (Logon). Use essa janela para fazer log-in na conta de administrador ou usuário de sua preferência.

Atalhos do sistema

A página <3>Atalhos do sistema</3> permite acessar diretamente alguns aplicativos, diretórios, arquivos e pastas sem navegar pelo menu Iniciar ou pelo Painel de Controle.

1. Faça login como administrador.
2. Acesse **Iniciar** > **Dell Thin Client Application**.
   A janela Dell Thin Client Application é mostrada.
3. Na barra de navegação esquerda, clique em **Atalhos do sistema**.
   Os seguintes atalhos são mostrados na área **Atalhos do sistema**:
   - Ferramentas administrativas
   - Todos os itens do Painel de Controle
   - Diretório de Sistema
   - Arquivos de Programas
   - Pasta Temporária
   - Meus Documentos
   - Arquivos Recentes Acessados
   - Pasta do Dell Thin Client Application
   - Pasta de dados de aplicativo
4. Clique em qualquer um dos atalhos para acessar as respectivas pastas/arquivos/aplicativos.

Como visualizar e configurar componentes do SCCM

Para visualizar e configurar os componentes de SCCM que estão instalados no dispositivo thin client, use a caixa de diálogo Propriedades do Gerenciador de Configurações.

Para abrir a caixa de diálogo **Propriedades do Gerenciador de Configurações**:

1. Faça login como administrador.
2. Acesse **Iniciar** > **Painel de controle** > **Gerenciador de configurações**.
   A caixa de diálogo **Propriedades do Gerenciador de Configurações** é exibida.

Para obter mais informações sobre como usar a caixa de diálogo **Propriedades do Gerenciador de Configurações**, veja Como gerenciar thin clients Dell Wyse baseados no Windows usando o Guia do Administrador do System Center Configuration Manager no site support.dell.com/manuals.

System Center Configuration Manager Client LTSB 2016

O Microsoft System Center Configuration Manager (SCCM) ajuda a capacitar dispositivos e aplicativos que precisam ser produtivos, mantendo a conformidade e o controle empresariais. Ele faz isso por meio de uma infraestrutura unificada que fornece um único painel de vidro para gerenciar clientes físicos, virtuais e móveis.

Ele também fornece ferramentas e melhorias que facilitam o seu trabalho. Com o SP1, ele fornece integração com o Windows Intune para gerenciar PCs e dispositivos móveis, a partir da nuvem e do local, usando um único console administrativo. Para obter mais informações, consulte *Managing Windows-based Dell Wyse Thin Clients using System Center Configuration Manager Administrator's Guide* (Como gerenciar Thin Clients Dell Wyse baseados no Windows usando o Guia do System Center Configuration Manager Administrator) no site support.dell.com/manuals.

Dispositivos e impressoras

Para adicionar dispositivos e impressoras, use a janela Devices and Printers (Dispositivos e Impressoras).

CUIDADO: Para impedir a limpeza das configurações, ative/desative o Unified Write Filter - UWF (Filtro de Gravação Unificado - UWF) e configure o Application Launch Manager (Gerenciador de Inicialização do Aplicativo) e o xData Cleanup Manager (Gerenciador de Limpeza xData). Para obter mais informações, consulte Before Configuring your thin clients (Antes de configurar thin clients).

Para adicionar um dispositivo ou uma impressora ao thin client:

1. Faça login como administrador.
2. Acesse **Start** > **Control Panel** > **Devices and Printers** (Iniciar > Painel de controle > Dispositivos e impressoras).
   A janela Devices and Printers (Dispositivos e Impressoras) é exibida.

Como adicionar impressoras

Para adicionar uma impressora ao thin client:

1. Clique no ícone de **Devices and Printers** (Dispositivos e Impressoras) no Control Panel (Painel de Controle).
   A janela **Devices and Printers** (Dispositivos e Impressoras) é exibida.
2. Para abrir e usar o assistente **Add a Printer** (Adicionar uma impressora), clique em **Adicionar uma impressora** (Adicionar uma impressora).

   A sessão do assistente **Adicionar uma impressora** (Adicionar uma impressora) é iniciada.

   Um Dell Open Print Driver é instalado no thin client junto com outros drivers de impressão incorporados. Para imprimir textos e elementos gráficos inteiros em uma impressora local, instale o driver fornecido pelo fabricante de acordo com as instruções.

   É possível imprimir em impressoras de rede usando os aplicativos **Citrix Receiver**, **Remote Desktop Connection** ou **VMware Horizon Client** com os drivers de impressora nos servidores.

   Imprimir em uma impressora local usando os aplicativos **Citrix Receiver**, **Remote Desktop Connection** ou **VMware Horizon Client** com os drivers de impressora do servidor oferece toda a funcionalidade de textos e elementos gráficos da impressora. Instale o driver da impressora no servidor, e o driver apenas de texto no thin client usando o seguinte procedimento:

a) Clique em **Add a local printer** (Adicionar uma impressora local), e clique em **Next** (Avançar).
b) Clique em **Use an existing port** (Usar uma porta existente), selecione a porta na lista e, em seguida, clique em **Next** (Avançar).
c) Selecione o fabricante e o modelo da impressora e clique em **Next** (Avançar).
d) Digite um nome para a impressora e clique em **Next** (Avançar).
e) Selecione **Do not share this printer** (Não compartilhar esta impressora) e clique em **Next** (Avançar).
f) Selecione se deseja imprimir uma página de teste e clique em **Next** (Avançar).
g) Clique em **Finish** (Concluir) para concluir a instalação.

Uma página de teste será impressa após a instalação, se essa opção tiver sido selecionada.

Como adicionar dispositivos

Para adicionar um dispositivo ao thin client:

1. Clique no ícone de **Dispositivos e Impressoras** no Painel de Controle e abra a janela **Dispositivos e Impressoras**.
2. Para abrir e usar o assistente **Adicionar um dispositivo**, clique em **Adicionar um dispositivo**.
   A sessão do assistente **Adicionar um dispositivo** é iniciada. Você pode usar o assistente para adicionar um dispositivo de sua escolha ao thin client.

Como configurar vários monitores

Você pode usar a janela Resolução de tela para ajustar as configurações de dois monitores no dispositivo thin client compatível com dois monitores.

Para abrir a janela Resolução de tela:

1. Faça login como administrador.
2. Acesse **Iniciar** > **Painel de controle** > **Exibir** > **Alterar configurações de exibição**.
   A janela Resolução de tela é exibida. Para obter instruções detalhadas sobre como configurar a resolução de tela, acesse www.microsoft.com.

   Para mais informações sobre como configurar vários monitores, consulte *Como configurar vários monitores no Windows 10* em support.dell.com (em inglês).

Como gerenciar áudio e dispositivos de áudio

Para gerenciar o áudio e os dispositivos de áudio, use a caixa de diálogo **Som**.

Para gerenciar o áudio e os dispositivos de áudio, faça login como administrador e abra a caixa de diálogo **Som**.

Como usar a caixa de diálogo de som

Para gerenciar dispositivos de áudio, use a caixa de diálogo **Som**.

Para abrir a caixa de diálogo **Som**:

1. Acesse **Iniciar** > **Painel de controle** > **Som**.

   A caixa de diálogo **Som** é exibida.
2. Use as seguintes guias e ajuste as configurações relacionadas ao som:
   - **Reprodução** - Selecione um dispositivo de reprodução e modifique suas configurações.
   - **Gravação** - Selecione um dispositivo de gravação e modifique suas configurações.
   - **Sons** - Selecione um tema de som existente ou modificado para eventos no Windows ou em programas.
   - **Comunicações** - Clique em uma opção para ajustar o volume de diferentes sons quando você estiver usando o thin client para fazer ou receber chamadas telefônicas.
3. Clique em **Aplicar** e em **OK**.

NOTA:

- **É recomendável usar alto-falantes potentes.**
- **Você também pode ajustar o volume usando o ícone de Volume na área de notificação da barra de tarefas.**

Como configurar a região

Para selecionar os seus formatos regionais, inclusive os idiomas de exibição do Windows e do teclado, use a caixa de diálogo **Região**.

Para selecionar os seu formatos regionais, faça o seguinte:

1. Faça login como administrador.
2. Acesse **Iniciar** > **Painel de controle** > **Região**.
   A caixa de diálogo **Região** é exibida.
3. Na guia **Formatos**, selecione idioma, data e horário.

   Para personalizar os formatos, faça o seguinte:

   a) Clique em **Configurações adicionais**.
      A janela Personalizar Formato é exibida.
   b) Personalize as configurações e clique em **OK**.
4. Clique em **Aplicar** e depois clique em **OK**.
5. Na guia **Local**, selecione um local específico para mostrar as informações adicionais, como notícias e clima, por exemplo.
6. Na guia **Administrativo**, altere o idioma a ser exibido em programas incompatíveis com Unicode e copie as configurações.

Como gerenciar contas de usuário

Para gerenciar usuários e grupos, use a janela <2>Contas de usuário</2>.

Para abrir a janela Contas de usuário, faça o seguinte:

1. Faça login como administrador.
2. Acesse **Iniciar** > **Painel de controle** > **Contas de usuário**.

   Para obter mais informações sobre como usar a janela Contas de Usuário, consulte Como gerenciar usuários e grupos com contas de usuário.

Como usar o Windows Defender

Para verificar e proteger o computador contra spyware e malware, use a caixa de diálogo **Windows Defender**.

Para abrir a janela Windows Defender, faça o seguinte:

1. Faça login como administrador.
2. Acesse **Iniciar** > **Painel de controle** > **Windows Defender**.

   A janela Windows Defender é exibida. Na guia **Início**, selecione uma opção de verificação e clique em **Verificar agora**.

Para configurar e gerenciar o dispositivo thin client, você pode usar as configurações de software antimalware na guia **Configurações**.

O Windows Defender é um software antispyware que está incluído com o Windows e é executado automaticamente quando você liga o seu thin client. Usar o software antispyware ajuda você a proteger o dispositivo contra spyware e outros tipos de software potencialmente indesejados. O spyware pode ser instalado no dispositivo sem o seu conhecimento a qualquer momento que você se conectar à Internet, e pode infectar o computador quando você instala alguns programas usando um CD, DVD ou outra mídia removível. O spyware também pode ser programado para ser executado em momentos inesperados e não apenas na sua instalação.

NOTA: O Windows Defender faz uma atualização automática às 01:00 no segundo domingo de cada mês.

Windows Defender Advanced Threat Protection

O Windows Defender Advanced Threat Protection (ATP) é um novo serviço que ajuda as empresas a detectar, investigar e responder a ataques avançados em suas redes.

O Windows Defender ATP funciona com tecnologias de segurança existentes do Windows em pontos de extremidade, como o Windows Defender, AppLocker e Device Guard. Ele também trabalha lado a lado com soluções de segurança de terceiros e produtos antimalware. Para obter mais informações, consulte a documentação do *Proteção de ameaças avançada Windows Defender* no site *docs.microsoft.com*

Defesa contra ameaças

Dell Data Protection | O Threat Defense Agent (com tecnologia Cylance), detecta e bloqueia malwares antes de eles poderem afetar um computador. O Cylance usa uma abordagem matemática para a identificação de malware. Ele usa técnicas de aprendizagem por máquina, em vez de assinaturas reativas, sistemas baseados em confiança ou áreas restritas. O Dell Data Protection | Threat Defense analisa execuções em potencial de arquivos quanto à presença de malware no sistema operacional.

Endpoint Security Suite Enterprise

O elemento Advanced Threat Prevention do Dell Endpoint Security Suite Enterprise versão 10.1 é suportado. Este recurso é suportado apenas no thin client Wyse 5070, no thin client Wyse 5470 e no thin client Wyse 5470 All-in-One.

O Endpoint Security Suite Enterprise fornece segurança de dados para dados, sistemas e a reputação de empresas. O pacote oferece um cliente integrado que inclui prevenção avançada contra ameaças, criptografia de classe empresarial, tudo gerenciado de maneira centralizada por meio de um único console. Você pode facilmente impor e comprovar a conformidade para todos os pontos de extremidade usando relatórios consolidados de conformidade e notificações flexíveis de e-mail.

Ferramenta C-A-D

A ferramenta C-A-D permite que os administradores mapeiem a combinação de teclas Ctrl+Alt+Del de aplicativos de VDI para mostrar a tela de Ctrl+Alt+Del do aplicativo de VDI. Se a ferramenta CAD estiver ativada, você poderá usar a combinação de teclas Ctrl+Alt+Del para todos os aplicativos de VDI. Além disso, você pode usar a função das teclas Win+L e Ctrl+Alt+Delete na sessão remota, como sessões do Remote Desktop, Citrix e VMware.

A seguir são apresentadas as teclas mapeadas para diferentes aplicativos de VDI suportados pela ferramenta C-A-D:

- Citrix—Ctrl+F1
- RDP—Ctrl+Alt+End
- VMware — Ctrl+Alt+Insert

NOTA: A ferramenta C-A-D não funciona para Citrix Virtual Apps and Desktops (antigo Citrix XenDesktop) em uma sessão do Citrix, mas funciona apenas para Citrix Virtual Apps.

A ferramenta C-A-D está desativada por padrão...

Wyse Device Agent

O Wyse Device Agent (WDA) é um agente unificado para todas as soluções de gerenciamento de thin clients. Instalar o WDA em um thin client permite que ele seja gerenciado pelo Dell Wyse Device Manager (WDM) e pelo Dell Wyse Management Suite (WMS). Para obter mais informações, consulte as *Notas da versão do Dell Wyse Device Agent* no site support.dell.com/manuals.

NOTA: Você não pode gerenciar o thin client Wyse 5070, o thin client Wyse 5470 e o thin client Wyse 5470 All-in-One usando o Wyse Device Manager.

Citrix HDX RealTime Media Engine

O **Citrix HDX RealTime Optimization Pack** para o Microsoft Lync fornece uma solução altamente escalável para proporcionar conferência de vídeo e áudio em tempo real e a telefonia empresarial de VoIP por meio do Microsoft Lync nos ambientes XenDesktop e XenApp para usuários nos dispositivos Linux, Mac e Windows. O HDX RealTime Optimization Pack aplica sua infraestrutura existente do Microsoft Lync e opera em conjunto com outros pontos de extremidade do Microsoft Lync executados nativamente nos dispositivos.

Para obter mais informações, consulte a documentação do Citrix.

Como visualizar e exportar arquivos de manifesto de imagens do sistema operacional

O arquivo de manifesto é um documento xml que contém metadados sobre a imagem do sistema operacional. Os arquivos de manifesto atuais e de fábrica podem ser comparados para encontrar alterações no thin client. Os itens a seguir são os dois tipos de arquivos de manifesto baseados na fonte da coleta de dados:

Tabela 4. Arquivos de manifesto

Origem do manifesto	Produtos instalados	QFE	Drivers
Manifesto atual	Sim	Sim	Sim
Manifesto de fábrica	Sim	Sim	Sim

Os detalhes de produtos instalados, QFEs e drivers de arquivos de manifesto atuais e de fábrica podem ser comparados para encontrar a alteração no thin client em relação aos aplicativos instalados, QFEs e drivers, respectivamente.

NOTA: Produtos instalados são todos os aplicativos instalados no thin client.

Como visualizar e exportar informações de manifesto atual de imagens do sistema operacional

1. Faça login como administrador.
2. Acesse **Iniciar** > **Painel de controle** > **Dell Wyse Software Manifest Utilty**.
3. Clique em **Exportar dados de suporte**.
   Os dados são exportados para o caminho padrão `C:/Users/Public/Public Documents/Wyse`.

   NOTA:

   Você também pode exportar os dados para uma pasta personalizada, selecionando Caminho personalizado e acessando a pasta desejada.
4. Clique em **Diretório de suporte**.
   A pasta `DellTCASupportInfo` é exibida.

   O diretório de suporte contém os aplicativos, drivers e QFE de informações de manifesto atual do thin client.

Como visualizar informações de manifesto de fábrica de imagens do sistema operacional

1. Faça login como administrador.
2. Acesse `C:\Windows\Setup\Tools`.
   A pasta `BuildContent` contém o manifesto de fábrica do thin client.
3. Veja as informações do manifesto da imagem do sistema operacional.
   - Para visualizar as informações dos produtos instalados na fábrica no momento do envio, acesse **Apps (Aplicativos)** > **arquivo xml InstalledProducts**.
   - Para visualizar as informações dos QFEs instalados na fábrica no momento do envio, acesse **Qfe** > **arquivo xml QFE**.
   - Para visualizar as informações do manifesto dos drivers instalados atualmente, acesse **Drivers** > **arquivo xml Drivers**.

NOTA:

- **Os arquivos .xml InstalledProducts, QFE e Drivers gerados por meio do utilitário Dell Wyse Software Manifest (conjunto de informações do manifesto atual) e os arquivos .xml presentes na pasta `<drive C>\Windows\Setup\Tools\BuildContent` (conjunto de informações do manifesto de fábrica) podem ser comparados para encontrar as alterações com relação ao aplicativo instalado e QFEs.**
- **Você pode compartilhar os dados de suporte e os dados de conteúdo de compilação com a equipe de suporte durante a solução de problemas.**

Dock station Dell WD19

A dock station Dell WD19 é um dispositivo que conecta todos os seus dispositivos eletrônicos ao thin client usando uma interface de cabo USB Tipo C. Conectar o thin client à dock station permite acessar todos os periféricos (mouse, teclado, alto-falantes estéreo, disco rígido externo e monitores de tela grande) sem precisar conectar cada um ao computador.

O thin client Wyse 5470 é compatível com a Dell Dock Station WD19.

Para obter mais informações, consulte *o Guia do usuário da Dell Dock Station WD19* e as *Notas de versão do thin client Microsoft Windows 10 IoT Enterprise para Dell Wyse 5470* em support.dell.com/manuals.

5

Informações adicionais de configurações e utilitários para administradores

Esta seção fornece informações adicionais sobre utilitários e configurações disponíveis para administradores.

Utilitários iniciados automaticamente

Os seguintes utilitários são iniciados automaticamente após o sistema ser ligado, ou após o login no thin client:

- **Unified Write Filter** - Depois de ligar o sistema, o utilitário Unified Write Filter inicia automaticamente. O ícone na área de notificação da barra de tarefas indica o status ativo ou inativo do Unified Write Filter. Para obter mais informações, consulte Como usar o Unified Write Filter (UWF).

  NOTA: Embora os ícones e a funcionalidade do Dell Wyse Write Filter sejam compatíveis no momento, é recomendável que você use o UWF conforme descrito na documentação da Microsoft, disponível em www.microsoft.com, e acesse a documentação do Unified Write Filter.
- **Application Launch Manager** - O Application Launch Manager (ALM) versão 1.0 permite iniciar qualquer aplicativo com base em eventos pré-definidos como, por exemplo, inicialização de serviços, logoff de usuários ou desligamento do sistema na ausência de sessão. O aplicativo também permite que você configure logs em vários níveis, o que é essencial para facilitar a solução de problemas.
- **xData Cleanup Manager** - O xData Cleanup Manager (xDCM) versão 1.0 impede que informações estranhas sejam armazenadas no disco local. O xDCM pode ser usado para a limpeza automática de diretórios usados para o armazenamento temporário de informações em cache. A limpeza é acionada em casos de inicialização de serviços, logoff de usuários ou desligamento do sistema. Essa limpeza é invisível para o usuário e pode ser configurada completamente.
- **Servidor de VNC** - Depois que você fizer login no seu thin client, o utilitário Windows VNC Server é iniciado automaticamente. O VNC permite que uma área de trabalho de dispositivo thin client seja acessada remotamente para administração e suporte. Para obter mais informações, consulte Como usar o VNC rígido para criar a sombra de um thin client.

Utilitários afetados pelo logoff, pela reinicialização e pelo desligamento

Os seguintes utilitários são afetados pelo logoff, reiniciando e desligando o dispositivo thin client:

- **Unified Write Filter** - Depois de ligar o sistema, o utilitário Unified Write Filter inicia automaticamente. É recomendável usar o UWF conforme descrito na documentação da Microsoft. Para obter mais informações, consulte www.microsoft.com e vá para a documentação do Unified Write Filter.
- **Application Launch Manager** - O Application Launch Manager (ALM) versão 1.0 permite iniciar qualquer aplicativo com base em eventos pré-definidos como, por exemplo, inicialização de serviços, logoff de usuários ou desligamento do sistema na ausência de sessão. O aplicativo também permite que você configure logs em vários níveis, o que é essencial para facilitar a solução de problemas.
- **xData Cleanup Manager** - O xData Cleanup Manager (xDCM) versão 1.0 impede que informações estranhas sejam armazenadas no disco local. O xDCM pode ser usado para a limpeza automática de diretórios usados para o armazenamento temporário de informações

em cache. A limpeza é acionada em casos de inicialização de serviços, logoff de usuários ou desligamento do sistema. Essa limpeza é invisível para o usuário e pode ser configurada completamente.

- **Gerenciamento de energia**: um Monitor Saver desliga o sinal de vídeo para o monitor, permitindo que o monitor entre no modo de economia de energia após um período ocioso designado. Para acessar as configurações de energia, acesse **Iniciar** > **Painel de Controle** > **Opções de Energia**.
- **Wake-on-LAN:** esse recurso detecta todos os thin clients na sua LAN, e permite que você os ative, clicando em um botão. Por exemplo, para fazer atualizações de imagem e executar funções de administração remota em dispositivos que tenham sido desligados ou que estão em modo de espera. Para usar esse recurso, a alimentação do thin client deverá permanecer ligada.

Unified Write Filter

O Unified Write Filter (UWF) é um filtro de gravação baseado em setor que protege a mídia de armazenamento. O UWF redireciona as tentativas de gravação para uma sobreposição virtual, e intercepta as tentativas de gravação para o volume protegido. Isso melhora a estabilidade, a confiabilidade do dispositivo, reduzindo assim o desgaste na mídia gravação, como unidades de estado sólido. No UWF, uma sobreposição é um espaço de armazenamento virtual que salva as alterações efetuadas no volume protegido. Se o sistema de arquivos tentar modificar um setor protegido, o UWF copiará o setor do volume protegido para a sobreposição e, em seguida, a sobreposição será atualizada. Se um aplicativo tentar fazer a leitura a partir desse setor, o UWF retornará os dados da sobreposição, de modo que o sistema pareça ter gravado no volume, enquanto o volume permanece inalterado. Para obter mais informações, consulte a documentação do Unified Write Filter no site www.microsoft.com.

CUIDADO: Se você não deixar o Filtro de Gravação ativado (exceto para a manutenção regular, ou para instalações ou atualizações de aplicativos/drivers), isso esgotará prematuramente o armazenamento SSD/flash e invalidará a garantia.

Os itens a seguir são as pastas de arquivo padrão excluídas da filtragem pelo UWF:

- `C:\Users\Admin\AppData\LocalLow`
- `C:\Users\User\AppData\LocalLow`
- `C:\Program Files\Windows Defender`
- `C:\Program Files (x86)\Windows Defender`
- `C:\Windows\WindowsUpdate.log`
- `C:\Windows\Temp\MpCmdRun.log`
- `C:\Windows\system32\spp`
- `C:\ProgramData\Microsoft\Windows Defender`
- `C:\program files\Wyse\WDA\Config`
- `C:\Users\Public\Documents\Wyse`
- `C:\Wyse\WCM\ConfigMgmt`
- `C:\Wyse\WCM`
- `C:\Wyse\WDA`

Os itens a seguir são os registros padrão excluídos da filtragem pelo UWF:

- `HKLM\SYSTEM\CurrentControlSet\Control\WNT\DWCADTool`
- `HKLM\Software\Wyse\ConfigMgmt`
- `HKLM\SOFTWARE\Microsoft\Windows Defender`
- `HKLM\SYSTEM\CurrentControlSet\Control\WNT\UWFSvc`
- `HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\HomeGroup`
- `HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\NetworkList`
- `HKLM\SYSTEM\WPA`

CUIDADO: Siga o filtro de gravação adequado e as instruções de uso do Arquivo de página do Windows em todos os momentos. Essas instruções incluem certificar-se de que o filtro de gravação está habilitado durante o uso regular e é desativado somente temporariamente por um administrador quando necessário para upgrades de imagem, patches de segurança, alterações no registro e instalação de aplicativos. O filtro de gravação deve ser reativado assim que essas tarefas sejam concluídas. As instruções incluem nunca ativar o recurso Arquivo de página do Windows durante o uso regular do thin client. Qualquer operação de um thin client Dell Wyse Windows incorporado com o filtro de gravação desligado durante o uso regular e/ou com o Arquivo da página do Windows ativado desgastará prematuramente o seu armazenamento Flash/SSD, diminuirá o desempenho e diminuirá a vida útil do produto. A Dell não se responsabiliza por, não garantirá, não dará suporte, não reparará nem substituirá qualquer componente ou dispositivo thin client que não funcionar corretamente devido a uma falha em seguir estas instruções.

Como usar o Unified Write Filter

Para configurar dispositivos thin client usando UWF, faça o seguinte:

1. Faça login como administrador.
   Se o logon automático na área de trabalho do usuário estiver ativado, faça o logoff da área de trabalho do usuário e faça o login como um administrador.
2. Para desativar o Unified Write Filter, clique duas vezes no ícone **Desativar WF do Dell Wyse** na área de trabalho.
   Esse ícone desativa o filtro e inicializa o sistema.
3. Configure o dispositivo thin client conforme suas necessidades.
4. Depois de configurar o dispositivo thin client, para ativar o Unified Write Filter, clique duas vezes no ícone **Ativar WF do Dell Wyse** na área de trabalho.
   Esse ícone ativa o filtro e inicializa o sistema. Suas configurações no dispositivo thin client agora estão salvas e serão preservadas após a reinicialização do thin client.

Após a inicialização do sistema, o utilitário Unified Write Filter (UWF) é iniciado automaticamente.

Você pode adicionar arquivos ou pastas específicos em um volume protegido a uma lista de exclusão de arquivos para excluir esses arquivos e pastas da filtragem pelo UWF. Quando um arquivo ou uma pasta está na lista de exclusão para um volume, todas as gravações nesse arquivo ou nessa pasta ignoram a filtragem pelo UWF, e são realizadas diretamente no volume protegido e persistem após a reinicialização do dispositivo.

Você deve fazer login como administrador para adicionar ou remover exclusões de arquivos ou pastas durante o tempo de execução, e você precisa reiniciar o dispositivo para que novas exclusões sejam efetivadas.

Como executar opções de linha de comando do Unified Write Filter

Há várias linhas de comando que você pode usar para controlar o Unified Write Filter. Argumentos da linha de comando não podem ser combinados.

Use as diretrizes a seguir para a opção de linha de comando do Unified Write Filter. Você também pode usar os comandos se abrir a janela do Prompt de comando com privilégio elevado, digitando o comando na caixa **Executar**.

Tabela 5. Como executar opções de linha de comando do Unified Write Filter

Opções de linha de comando	Descrição
`uwfmgr`	Essa ferramenta de linha de comando configura e recupera configurações do Unified Write Filter (UWF). Se não houver nenhuma opção de linha de comando disponível, ela exibe a ajuda de comandos.
`uwfmgr filter enable`	Essa linha de comando ativa o Unified Write Filter após a próxima reinicialização do sistema. O ícone de status do Unified Write Filter fica verde quando o Unified Write Filter é ativado.
`uwfmgr filter disable`	Essa opção de linha de comando desativa o Unified Write Filter após a próxima reinicialização do sistema. O ícone de status do Unified Write Filter permanece vermelho enquanto estiver desativado.
`uwfmgr file commit C: <file_path>`	Essa linha de comando confirma alterações em um arquivo especificado para a sobreposição de um volume protegido do Unified Write Filter. É necessário ter permissões de administrador para usar esse comando. O parâmetro <file> precisa ser totalmente qualificado, incluindo o volume e o caminho. O arquivo `uwfmgr.exe` usa o volume especificado no parâmetro <file> para determinar qual volume contém a lista de exclusão de arquivos para o arquivo. Há um único espaço entre o nome do volume e file_path. Por exemplo, para confirmar um arquivo `C:\Program Files\temp.txt`, o

Opções de linha de comando	Descrição
	comando seria `uwfmgr commit C: \Program Files \temp.txt`.
`uwfmgr file add-exclusion C: <file_or_dir_path>`	Essa linha de comando adiciona o arquivo especificado na lista de exclusão de arquivos do volume protegido pelo Unified Write Filter. O Unified Write Filter começa a excluir o arquivo da filtragem após a próxima reinicialização do sistema. Por exemplo, para adicionar um diretório de registro `HKLM \SYSTEM\WPA`, o comando é `UWFmgr.exe registry add-exclusion HKLM\SYSTEM\WPA`.
`uwfmgr file remove-exclusion C: <file_or_dir_path>`	Essa linha de comando remove o arquivo especificado da lista de exclusão de arquivos do volume protegido pelo Unified Write Filter. O Unified Write Filter para de excluir o arquivo da filtragem após a próxima reinicialização do sistema.
`uwfmgr overlay get-config`	Essa linha de comando mostra os parâmetros de configurações para a sobreposição do Unified Write Filter. Exibe informações para a sessão atual e a próxima sessão.
`uwfmgr registry /?`	Essa linha de comando mostra os parâmetros de configurações para exclusões de chaves de registro.

NOTA: Se você abrir uma janela do Prompt de comando e digitar `uwfmgr ?` ou `uwfmgr help`, todos os comandos disponíveis serão exibidos. Para obter informações sobre um comando, use `uwfmgr help <command>`. Por exemplo, para obter informações sobre o comando, `volume`, digite o seguinte: `uwfmgr help volume`.

CUIDADO:

- **Os administradores devem usar a segurança do arquivo para evitar o uso indesejado desses comandos.**
- **Não tente fazer o alinhamento dos dados com o disco enquanto outra operação de alinhamento estiver em andamento.**

Como ativar e desativar o filtro de gravação usando os ícones da área de trabalho

O Unified Write Filter também pode ser ativado ou desativado por meio dos ícones para Ativar/Desativar o Filtro de Gravação na área de trabalho. O ícone na área de notificação da barra de tarefas indica o status ativo ou inativo do Unified Write Filter pelas cores verde e vermelha, respectivamente.

- **Ícone para Ativar o WF do Dell Wyse (verde)** - Clicar duas vezes nesse ícone ativa o Unified Write Filter. Esse utilitário tem o mesmo efeito de executar a linha de comando uwfmgr filter enable. No entanto, clicar duas vezes nesse ícone reinicia imediatamente o sistema e ativa o Unified Write Filter. O ícone de status do Unified Write Filter na área de notificação da barra de tarefas fica verde quando o Unified Write Filter é ativado.
- **Ícone para Desativar o WF do Dell Wyse (vermelho)** - Clicar duas vezes nesse ícone desativa o Unified Write Filter. Esse utilitário tem o mesmo efeito de executar a opção de linha de comando uwfmgr filter disable. No entanto, clicar duas vezes nesse ícone reinicia o sistema imediatamente. O ícone de status do Unified Write Filter na área de notificação da barra de tarefas permanece vermelho enquanto o Unified Write Filter estiver desativado.

Como configurar os controles do filtro de gravação

Para visualizar e gerenciar as configurações de controle do UWF, use a caixa de diálogo **Controle do Unified Write Filter**. Para abrir a caixa de diálogo, clique duas vezes no ícone do UWF na área de notificação da barra de tarefas do administrador.

Quando você ajusta as configurações de controle do UWF, alguns dos campos ficam indisponíveis. Você pode selecionar na lista de campos disponíveis durante a configuração.

A caixa de diálogo Controle do Unified Write Filter do Dell Wyse inclui o seguinte:

- **Status do UWF**
  - **Status atual** - Mostra o status do Unified Write Filter. O status pode ser Ativado ou Desativado.
  - **Comando de inicialização** - Mostra o status do Comando de inicialização. UWF_ENABLE significa que o UWF está ativado para a sessão seguinte; e UWF_DISABLE significa que o UWF está desativado para a sessão seguinte.
  - **RAM usada pelo UWF** - Mostra a quantidade de RAM alocada para o Unified Write Filter em Megabytes (MB) e Porcentagem. Se **Status atual** for desativado, a RAM alocada ao UWF é sempre zero (0).
  - **Quantidade de RAM usada para o cache do UWF** - Mostra a quantidade de RAM alocada para o cache do Unified Write Filter da sessão atual em Megabytes (MB).
  - <2>Aviso nº 1 (%)</2> - Mostra o valor percentual do cache do UWF no qual uma mensagem de aviso de Memória baixa é exibida para o usuário da sessão atual.
  - **Aviso nº 2 (%)** - Mostra o valor percentual do cache do UWF no qual uma mensagem de aviso de memória crítica é exibida para o usuário.
- **Configurações de cache do UWF**
  - **Quantidade de RAM a ser usada para o cache do UWF** - Mostra a quantidade de RAM que será usada como o cache do Unified Write Filter da próxima sessão em MB. Esse valor deve estar no intervalo de 256 MB a 2048 MB. Há uma verificação adicional para garantir que esse valor não exceda 50% do Total de RAM disponível.
- **Configurações de aviso do UWF**
  - **Aviso nº 1 (%)** - Mostra o valor percentual do cache do UWF no qual uma mensagem de aviso de Memória baixa é exibida para o usuário (Valor padrão = 80, Valor mínimo = 50, Valor máximo = 80).
  - **Aviso nº 2 (%)** - Mostra o valor percentual do cache do UWF no qual uma mensagem de aviso de memória crítica é exibida para o usuário. Quando o nível de memória cruzar o nível de aviso 2, o sistema reiniciará automaticamente. (Valor padrão = 90, Valor mínimo = 55, Valor máximo = 90)
- **Ativar UWF** - Permite que você ative o Unified Write Filter e solicita que você reinicie o dispositivo thin client. Para salvar as alterações, reinicie o thin client. Depois que o sistema é reiniciado para ativar o Unified Write Filter, o ícone de status do Unified Write Filter na área de notificação da área de trabalho fica verde.
- **Desativar UWF** - Permite que você desative o Unified Write Filter e solicita que você reinicie o dispositivo thin client. Para salvar as alterações, reinicie o thin client. Depois de desativar o Unified Write Filter, o ícone de status do Unified Write Filter na área de notificação da área de trabalho ficará vermelho e o Unified Write Filter permanecerá desativado depois que o sistema tiver sido reiniciado.
- **Padrões** - Permite redefinir a área de Configurações do cache do UWF e a área de Configurações de aviso do UWF como os valores padrão.
- **Área de Confirmação de arquivos**
  - **Caminho do arquivo** - Permite que você adicione, remova e confirme arquivos na mídia subjacente. O sistema não reiniciará o dispositivo thin client. As alterações são confirmadas imediatamente.

    NOTA: Exclua um caminho de arquivo da lista, se o arquivo não estiver confirmado.
- **Lista de exclusão da sessão atual**
  - **Caminho do Arquivo/Diretório** -

    Permite adicionar um arquivo ou diretório à lista de exclusão, ou removê-lo dessa lista, para a próxima sessão. Isso recupera a lista de arquivos ou diretórios que são gravados na sessão atual e o título do painel é mostrado como a Lista de exclusões da sessão atual. A Próxima sessão recupera a lista de arquivos ou diretórios que são gravados na próxima sessão e o título do painel é mostrado como a Lista de exclusões da próxima sessão. O sistema não reiniciará o thin client, e as alterações não serão confirmadas até que um administrador reinicie o dispositivo thin client manualmente.

Application Launch Manager

O Application Launch Manager (ALM) versão 1.0 permite iniciar um aplicativo com base em eventos pré-definidos como, por exemplo, inicialização de serviços, logon/logoff de usuários ou desligamento do sistema na conta do sistema. Você também pode configurar logs multinível que são essenciais para a solução de problemas usando o arquivo `DebugLog.xml`.

Você pode adicionar ou remover nós de configuração de aplicativo do arquivo de configuração de ALM usando a interface de linha de comando.

Ferramenta ALM CLI

Você pode usar a ferramenta ALM CLI para adicionar ou remover nós de configuração de aplicativo do arquivo de configuração de ALM `ApplicationLaunchConfig.xml`. Essa ferramenta está disponível no caminho de instalação do aplicativo ALM. Por padrão, a ferramenta está disponível em `%systemdrive%\Program Files\ALM`.

Configuração de nós usando ALM

Você pode usar as seguintes opções e parâmetros para configurar nós de aplicativo em `ApplicationLaunchConfig.xml`:

Tabela 6. Opções para configurar nós

Opção	Descrição
Adicionar aplicativo	Opção para adicionar um nó de aplicativo.
Remover aplicativo	Opção para excluir um nó de aplicativo.

Tabela 7. Parâmetros para configurar nós

Parâmetro	Valores
`Name:`<nome do aplicativo>	[Nome do aplicativo]
`Path:`<caminho do aplicativo>	[Caminho do aplicativo]
`Arguments:`<especificar as informações sobre configuração quando o aplicativo for iniciado>	[Argumento]

`Event:`<evento para executar o comando>	`USER_LOGOFF`
	`SVC_STARTUP`
	`ON_SHUTDOWN`
	`USER_LOGIN`

Exemplos para configurar nós usando xDCM

Tabela 8. Exemplos para configurar nós usando xDCM

Cenário	Comando
Adicionar um nó de aplicativo usado pelo serviço ClientServiceEngine para executar o arquivo `TestApp.exe` com um argumento `-t` quando você fizer logoff do sistema.	`ALM.exe -Add -Application -Name:ExampleApp -Path:C:\Windows\System32\TestApp.exe -Arguments:"-t" -Event: USER_LOGOFF`
Excluir um nó de aplicativo do aplicativo **ExampleApp**.	`ALM.exe -Remove -Application -Name: ExampleApp`

NOTA:

- **Você deve fornecer nomes exclusivos para adicionar uma nova entrada de aplicativo ao arquivo `ApplicationLaunchConfig.xml` usando `ALM.exe`.**
- **Somente três valores de eventos de execução `USER_LOGOFF`, `SVC_STARTUP` e `ON_SHUTDOWN`, são suportados no aplicativo ALM. Você só pode adicionar um desses valores para cada evento.**

xData Cleanup Manager

O xData Cleanup Manager (xDCM) versão 1.0 impede que informações estranhas sejam armazenadas no disco local. O xDCM pode ser usado para limpar automaticamente os diretórios usados para o armazenamento temporário de informações em cache. Uma limpeza é acionada em casos de inicialização de serviços, logoff de usuários ou desligamento do sistema.

Ela também permite que você configure logs multinível que são essenciais para a solução de problemas. Você pode limpar arquivos, pastas e ativar ou desativar xDCM usando a Interface de Programação de Aplicativos (API). Você também pode adicionar ou remover nós de configuração do arquivo de configuração do xDCM usando a interface de linha de comando.

NOTA:

- **Configurações existentes do arquivo `NetXclean.ini` são transferidas para o novo arquivo `xDataCleanupConfig.xml`.**
- **O conteúdo no xData Cleanup Manager é apagado por padrão.**

Ferramenta xDCM CLI

Você pode usar a ferramenta xDCM CLI para adicionar ou remover nós de configuração do arquivo de configuração xDCM `XdataCleanupConfig.xml`. Essa ferramenta está disponível no caminho de instalação do aplicativo xDCM. Por padrão, a ferramenta está disponível em `%systemdrive%\Program Files\XDCM`.

Configuração de nós usando xDCM

Você pode usar as seguintes opções e parâmetros para configurar nós de aplicativo em `XdataCleanupConfig.xml`:

Tabela 9. Opções para configurar nós

Opção	Descrição
Adicionar	Opção para adicionar um nó de limpeza da pasta.
Remover	Opção para excluir um nó de limpeza da pasta.

Tabela 10. Parâmetros para configurar nós

Parâmetro	Valores

`CleanupType:`<tipo do nó de limpeza>	`Pasta`
	`Arquivo`
	`Registro`

`Name:`<nome do nó de limpeza>	[Nome da pasta/arquivo/registro]
`Path:`<caminho do nó de limpeza>	[Caminho da pasta/arquivo/registro]
`PathExclusions:`<caminhos que serão excluídos da exclusão (Path1,Path2)/NULL>	[Caminho/NULO]

`Event:`<evento para executar o comando>	`USER_LOGOFF`
	`SVC_STARTUP`
	`ON_SHUTDOWN`

`CleanType:`<tipo de limpeza>	`DIR_DELETE` `DIR_EMPTY`
`CleanFrom:`<tipo de memória>	`Disco` `Sobreposição`

Exemplos para configurar nós usando xDCM

Tabela 11. Exemplos para configurar nós usando xDCM

Cenário	Comando
A adição de um nó de limpeza de pasta em `XdataCleanupConfig.xml` sob o elemento **DiskCleanup**.	`XDCM.exe -Add -CleanupType:Folder -Name:Notepad -Path:C:\Windows\Security -PathExclusions:"C:\Windows\Security\database, C:\Windows\logs" -Event: USER_LOGOFF -CleanType:DIR_EMPTY -CleanFrom:Disk`
Apagar um nó de limpeza de arquivo sob o elemento **OverlayCleanup Notepad** no arquivo `XdataCleanupConfig.xml`.	`XDCM.exe -Remove -CleanupType:File -Name:Notepad -CleanFrom:Overlay`

NOTA:

- **Se você se desconectar do thin client quando o UWF estiver desativado, o nó de limpeza de pasta é usado pelo serviço ClientServiceEngine para limpar o conteúdo dentro do diretório `C:\Windows\Security`. Além disso, quando o conteúdo desse diretório é excluído, o conteúdo das pastas `C:\Windows\Security\database` e `C:\Windows\logs` é excluído à medida que é adicionado nos caminhos excluídos.**
- **Você deve fornecer nomes exclusivos para adicionar uma nova entrada de aplicativo ao arquivo `XdataCleanupConfig.xml` usando `XDCM.exe`.**
- **Quando você estiver executando o comando para adicionar uma entrada, o caminho da pasta é comparado com as entradas existentes. Se o caminho já estiver disponível, apenas os caminhos de exclusão são adicionados à entrada da pasta existente.**

Como capturar arquivos de log

Você pode configurar o arquivo `DebugLog.xml` para coletar diferentes tipos de logs para um aplicativo. Você pode modificar os níveis do log para obter o tipo específico de logs. Os arquivos de log são criados em `C:\Windows\Logs\<Application name>\Logs`.

NOTA: Por padrão, nenhum log é criado para um aplicativo.

Configuração do arquivo XML DebugLog

Você pode usar o aplicativo de console Editor de Configuração de Depuração (DCE) para configurar o arquivo XML de configuração de depuração. Essa ferramenta pode ser usada para confirmar, excluir ou modificar o arquivo de configuração de depuração.

Para confirmar, excluir ou modificar o arquivo de configuração de depuração, digite os seguintes comandos no Editor de Configuração de Depuração:

- Para confirmar o arquivo e obter os arquivos de log: `DebugConfigEditor.exe -CommitLog -Path "DebugLog.xml"`. Esse comando confirma o arquivo presente no caminho que é mencionado no arquivo `Debug.xml`.
- Para excluir o conjunto de logs de uma pasta mencionada no arquivo `Debug.xml`: `DebugConfigEditor.exe -ExcludeLog -Path "DebugLog.xml"`.
- Para configurar o arquivo `Debug.xml` para coletar diferentes tipos de logs: `DebugConfigEditor.exe -UpdateConfig -Path "DebugLog.xml" -LogPath "Path of Log File" -LogFileName "Name of log File" -LogLevel "logLevel"`.

  A tabela a seguir descreve os diferentes valores de LogLevel que podem ser usados:

Tabela 12. Valores de LogLevel

Valor	Descrição
0	Logs não são capturados.
1	Logs de erros são capturados.
2	Logs de avisos são capturados.
3	Logs de erros e avisos são capturados.
4	Logs de informações são capturados.
7	Todos os logs são capturados.

Como salvar arquivos e usar unidades locais

Thin clients usam um sistema operacional incorporado com uma quantidade fixa de espaço em disco. A Dell recomenda que você salve os arquivos que deseja manter em um servidor em vez de salvá-los em um thin client.

CUIDADO: Tenha cuidado com configurações de aplicativos que fazem gravações na unidade C, que ocupam o espaço em disco. Por padrão, esses aplicativos gravam arquivos de cache na unidade C no sistema local. Se tiver de gravar em uma unidade local, altere as configurações do aplicativo para usar a unidade Z. Os parâmetros de configuração padrão que são mencionados em Como gerenciar usuários e grupos com contas de usuário minimizam a gravação na unidade C para aplicativos instalados de fábrica.

unidade Z

A Unidade Z é a memória volátil integrada (Disco de RAM Dell Wyse) do thin client. É recomendável que você não utilize essa unidade para salvar os dados que deseja manter.

Para obter informações sobre como usar a unidade Z com perfis móveis, consulte Como participar de domínios.

unidade C

A Unidade C é a memória flash não volátil integrada. A Dell recomenda que você evite gravar na unidade C. Isso reduz o espaço livre em disco. Se o espaço livre em disco na unidade C for reduzido para menos de 500 MB, o thin client ficará instável.

NOTA: A Dell recomenda que 500 MB de espaço em disco sejam deixados sem uso. Se o espaço livre em disco for reduzido para 500 MB, a imagem do thin client será danificada irreparavelmente e será necessário que você entre em contato com um centro de serviço autorizado para reparar o thin client.

A ativação do Unified Write Filter protege o disco contra danos e apresenta uma mensagem de erro se o cache for sobrescrito. No entanto, se essa mensagem aparecer, você não poderá alinhar arquivos do cache do Unified Write Filter e qualquer alteração na configuração do thin client ainda armazenada em cache será perdida. Itens gravados no cache do Unified Write Filter ou diretamente no disco, se o Unified Write Filter estiver desativado durante as operações normais, incluem:

- Favoritos
- Conexões criadas
- Excluir/editar conexões

Como mapear unidades de rede

Os administradores podem mapear unidades de rede. Para mapear a unidade de rede e manter os mapeamentos depois que o dispositivo thin client for reiniciado, consulte *Mapear uma unidade de rede* em https://support.microsoft.com.

Como participar de domínios

Você pode participar de domínios incluindo o dispositivo thin client em um domínio ou usando perfis móveis.

Para ingressar em um domínio, consulte

1. Faça login como administrador.
2. Acesse **Iniciar** > **Painel de controle** > **Sistema**.
   A janela Sistema é exibida.
3. Na seção **Nome do computador, domínio e configurações de grupo de trabalho**, clique em **Alterar configurações**.
   A caixa de diálogo **Propriedades do sistema** é exibida.
4. Clique na opção **Alterar** para alterar o domínio ou o grupo de trabalho.
   a) Clique em **Domínio**.
      A caixa de diálogo **Alterações de Nome/Domínio do Computador** é exibida.
   b) Insira o domínio de sua escolha.
   c) Clique em **OK**.
5. Para adicionar um dispositivo thin client a um domínio, clique em **ID de rede**.
   O assistente **Ingressar em um Domínio ou Grupo de Trabalho** é exibida. Na primeira página do assistente, selecione a opção que descreve a sua rede.
   - Rede Comercial - Clique nessa opção se o seu thin client for membro da rede empresarial e se você usá-lo para se conectar a outros clientes no local de trabalho.
     a. Clique em **Avançar**.
     b. Selecione a opção de acordo com a disponibilidade da rede da sua empresa em um domínio.
        Se você selecionar a opção **Rede com um domínio**, é preciso digitar as seguintes informações:
        - Nome de usuário
        - Senha
        - Nome do domínio

        Se você selecionar a opção **Rede sem um domínio**, pode inserir o **Grupo de trabalho** e, em seguida, clicar em **Avançar**.

        NOTA: Você pode clicar em Avançar, mesmo que não saiba o nome do grupo de trabalho.
     c. Para aplicar as alterações, é preciso reiniciar o computador. Clique em **Concluir**.

NOTA: Antes de reiniciar o computador, salve todos os arquivos abertos e feche todos os programas.

- Rede doméstica - Clique nessa opção se o seu thin client for um cliente doméstico e se ele não for membro de uma rede comercial. Para aplicar as alterações, é preciso reiniciar o computador. Clique em **Concluir**.

CUIDADO: Tome cuidado ao adicionar o dispositivo thin client a um domínio, pois o perfil baixado no login pode exceder o cache ou a memória flash.

Ao adicionar o dispositivo thin client a um domínio, o Unified Write Filter deve ser desativado para que as informações do domínio possam ser armazenadas permanentemente nesse dispositivo. O Unified Write Filter deve permanecer desativado durante a próxima reinicialização, pois as informações são gravadas no thin client na reinicialização depois de participar do domínio. Esse UWF é importante ao participar de um domínio do Active Directory. Para ver mais detalhes sobre a desativação e a ativação do Unified Write Filter, consulte Antes de configurar o seu thin client.

Para que as alterações no domínio sejam permanentes, faça o seguinte:

a) Desative o Unified Write Filter.
b) Participe de um domínio.
c) Reinicie o thin client.
d) Ative o Unified Write Filter.

NOTA:

Se você usar o ícone de Ativação do Filtro de Gravação para ativar o Filtro de Gravação, o thin client é reiniciado automaticamente.

Como usar perfis móveis

Você pode participar de domínios gravando perfis móveis na unidade C. Os perfis devem ter tamanho limitado, e não são mantidos quando o dispositivo thin client é reiniciado. Para fazer download corretamente e conseguir o bom funcionamento, é preciso que haja espaço suficiente em disco disponível para os perfis móveis. Às vezes, pode ser necessário remover componentes de software para liberar espaço para perfis móveis.

Como usar os utilitários Net e Tracert

Os utilitários Net e Tracert estão disponíveis para uso administrativo. Por exemplo, determinar a rota que os pacotes percorreram através de uma rede IP.

Para obter mais informações sobre esses utilitários, acesse www.microsoft.com.

Como gerenciar usuários e grupos com contas de usuário

Para criar e gerenciar contas de usuário e grupos, e configurar propriedades avançadas do perfil do usuário, use a janela Contas de Usuário. Por padrão, um novo usuário só é membro do grupo **Usuários** e não está bloqueado. Como administrador, você pode selecionar os atributos e as configurações do perfil para os usuários.

Esta seção fornece diretrizes de início rápido sobre:

- Como criar contas de usuário
- Como editar contas de usuário
- Como configurar perfis de usuário

NOTA: Para obter informações detalhadas sobre como usar a janela Contas de usuário, clique no ícone de ajuda e nos links de exemplos fornecidos em todos os assistentes. Por exemplo, você pode usar a janela Ajuda e Suporte do Windows para procurar itens como os perfis de usuário e grupos de usuários. Obtenha links para instruções detalhadas sobre como criar e gerenciar esses itens.

Como criar contas de usuário

Apenas administradores podem criar novas contas de usuário local ou remotamente por meio de VNC. No entanto, devido a limitações de espaço em disco ou flash local, o número de usuários adicionais no dispositivo thin client deve ser mantido ao mínimo.

CUIDADO: Para salvar as informações permanentemente, desative o Unified Write Filter (UWF).

1. Faça login como administrador.
2. Acesse **Iniciar** > **Painel de controle** > **Contas de usuário**.
3. Na janela **Contas de usuário**, clique em **Gerenciar outra conta**.
   A janela **Gerenciar contas** é exibida.
4. Clique em **Adicionar novo usuário** nas configurações do PC.
   O assistente **Configurações do PC** é iniciado. Use esse assistente para criar uma conta de usuário.
5. Depois de criar os usuários e administradores padrão, esses usuários aparecerão na janela **Gerenciar Contas**. Conclua a **Etapa 3**.

Como editar contas de usuário

Abra a janela **Contas de usuário** conforme descrito em Como gerenciar contas de usuário.

Para editar as configurações padrão de uma conta de usuário ou de administrador padrão:

1. Na janela **Conta de usuário**, clique em **Gerenciar outra conta**.
   A janela **Gerenciar contas** é exibida.
2. Para alterar, conforme o necessário, selecione **Usuário**.
   A janela **Alterar uma conta** é exibida. Agora faça as alterações desejadas usando os links fornecidos.

Como configurar perfis de usuário

Abra a janela **Contas de usuário** conforme descrito em Como gerenciar contas de usuário.

CUIDADO:

- **Por padrão, todas as configurações de aplicativos são definidas para o armazenamento em cache na unidade C. A Dell recomenda que você faça o armazenamento em cache na unidade Z do disco de RAM, conforme pré-definido nos perfis da conta, a fim de evitar que o cache do Unified Write Filter seja excedido.**
- **É recomendável que outros aplicativos disponíveis para usuários novos e antigos sejam configurados para impedir a gravação no sistema de arquivos local devido ao tamanho limitado do espaço em disco. É recomendável tomar cuidado ao alterar parâmetros de configuração de aplicativos instalados de fábrica.**

Para configurar os perfis padrão de administrador e de usuário armazenados no thin client:

1. Na janela Conta de usuário, clique em **Configurar propriedades de perfil de usuário avançado**.

   A caixa de diálogo **Perfis de usuário** é exibida.
2. Use os botões de comando, como **Alterar tipo**, **Excluir** e **Copiar para**, conforme descrito na documentação da Microsoft fornecida durante os assistentes.

Como alterar o nome do computador de um thin client

Os administradores podem alterar o nome do computador de um thin client. As informações de nome do computador e a Licença de Acesso para Cliente de Serviços de Terminal (TSCAL) são preservadas, independentemente do estado do Unified Write Filter (ativado ou desativado). Isso mantém as informações de identidade de um computador específico e facilita o gerenciamento de imagens do thin client.

Para alterar o nome do computador de um dispositivo thin client, consulte

1. Faça login como administrador.
2. Acesse **Iniciar** > **Painel de controle** > **Sistema**.
   A janela Sistema é exibida.
3. Na seção **Nome do computador, domínio e configurações de grupo de trabalho**, clique em **Alterar configurações**.
   A caixa de diálogo **Propriedades do sistema** é exibida.
4. Clique na guia **Alterar** para renomear o nome do computador.
5. Na janela <4>Nome do computador</4>, digite o nome do dispositivo thin client no campo **Nome do computador** e clique em **OK**.
6. Na caixa de diálogo Confirmação, clique em **OK** para reiniciar e aplicar as alterações.
7. Clique em **Fechar** e, em seguida, em **Reiniciar agora** para aplicar as alterações.

6

Administração do sistema

Para manter o ambiente do dispositivo thin client, você poderá executar tarefas de administração de sistema local e remoto. As tarefas incluem:

- Accessing thin client BIOS settings
- Unified Extensible Firmware Interface (UEFI) e boot seguro
- Como usar o Wyse Management Suite
- Portas e slots
- Como usar TightVNC (servidor e visualizador) para sombrear um thin client

Accessing thin client BIOS settings

Para acessar as configurações do BIOS thin client, faça o seguinte:

1. Na inicialização do sistema, pressione F2 quando você vir o logotipo da Dell.
   A tela Configuração do BIOS é exibida.
2. Altere as configurações do BIOS, conforme o necessário.
3. Salva as alterações e sai.

Unified Extensible Firmware Interface e boot seguro

A Unified Extensible Firmware Interface (UEFI) é uma interface de firmware padrão projetada para melhorar a interoperabilidade do software e solucionar as limitações do BIOS. A UEFI é projetada para substituir o Sistema Básico de Entrada/Saída (BIOS).

O Boot Seguro é um recurso em clientes baseados em UEFI que ajuda a aumentar a segurança de um cliente, impedindo que software não autorizado seja executado em um cliente durante a sequência de inicialização. Ele verifica se cada software tem uma assinatura válida, incluindo o sistema operacional (SO) que está sendo carregado durante a inicialização.

O dispositivo thin client é fornecido com a UEFI e o Boot Seguro ativados. Graças a esse recurso, só é possível fazer a inicialização a partir de chaves USB se você entrar no BIOS, desativar o Boot Seguro, alterar o modo de boot para Legacy e ativar a opção **Inicializar a partir do USB**.

Como inicializar a partir de uma chave USB DOS

A seguinte tabela fornece as diretrizes para inicializar a partir de uma chave USB DOS nos dispositivos thin client suportados:

Tabela 13. Como inicializar a partir de uma chave USB DOS

Thin clients	Diretrizes para inicializar o thin client
• Thin client Wyse 5020 com Win10 IoT (D90Q10) • Thin client Wyse 7020 com Win10 IoT (Z90Q10) • Thin client Wyse 7020 com gráficos acelerados com Win10 IoT (Z90QQ10) • Thin client Wyse 5060	Para inicializar o thin client a partir de uma chave USB DOS, faça o seguinte: 1. Na inicialização do sistema, pressione `Excluir` quando você vir o logotipo do Wyse. A tela Configuração do BIOS é exibida. 2. Defina o **Boot Seguro** como **Desativado**. 3. Defina o **Modo de inicialização** como **Legado**. 4. Defina **Inicializar a partir do USB** como **Ativado**. 5. Salva as alterações e sai.

Thin clients	Diretrizes para inicializar o thin client
	6. No menu pop-up, selecione sua chave USB e inicialize como **Normal**.

Como inicializar a partir de uma chave USB UEFI

A seguinte tabela fornece as diretrizes para inicializar a partir de uma chave USB UEFI nos dispositivos thin client suportados:

Tabela 14. Como inicializar a partir de uma chave USB UEFI

Thin clients suportados	Diretrizes para inicializar o thin client
• Thin client Wyse 5020 com Win10 IoT (D90Q10) • Thin client Wyse 7020 com Win10 IoT (Z90Q10) • Thin client Wyse 7020 com gráficos acelerados com Win10 IoT (Z90QQ10)	Para inicializar o thin client a partir de uma chave USB UEFI, faça o seguinte: 1. Na inicialização do sistema, pressione `Excluir` quando você vir o logotipo do Wyse. A tela Configuração do BIOS é exibida. 2. Defina o **Boot Seguro** como **Desativado**. 3. Defina **Inicializar a partir do USB** como **Ativado**. 4. Salva as alterações e sai. 5. No menu pop-up, selecione sua chave USB e inicialize como **Normal**.
• Thin client Wyse 5470 • Thin client Wyse 5470 All-in-One • Thin client Wyse 5060 • Thin client Wyse 7040 • Thin client móvel Latitude 3480 • Thin client móvel Latitude 5280	Para inicializar o thin client a partir de uma chave USB UEFI, faça o seguinte: 1. Na inicialização do sistema, pressione `F2` quando você vir o logotipo da Dell. A tela Configuração do BIOS é exibida. 2. Defina o **Boot Seguro** como **Desativado**. 3. Clique em **Configuração do Sistema** > **Configuração de USB** e selecione a caixa de seleção **Habilitar suporte à inicialização via USB**. 4. Salva as alterações e sai. 5. Na inicialização do sistema, pressione `F12` e selecione a chave USB no menu de inicialização. **NOTA: Você pode inicializar os dispositivos de 64 bits com Windows 10 IoT Enterprise (WIE10) se o boot seguro estiver definido como Desativado. No entanto, para fins de segurança, isso não é recomendado.**

Como criar uma chave USB UEFI inicializável

Para criar uma chave USB UEFI inicializável, faça o seguinte:

1. Obtenha um shell UEFI executável.
2. Salve o arquivo como `bootx64.efi` no seu cliente.
3. Formate a chave USB com `FAT32`.
4. Na chave USB, crie o diretório `\efi\boot`.
5. Copie o arquivo `bootx64.efi` para o diretório `\efi\boot` na chave USB.
   A chave USB UEFI inicializável é criada.

Como usar o Dell Wyse Management Suite

O Wyse Management Suite é a solução de gerenciamento da próxima geração que permite configurar, monitorar, gerenciar e otimizar de maneira centralizada seus thin clients Dell Wyse. O novo Suite facilita a implementação e o gerenciamento de thin clients com alta funcionalidade e desempenho, e facilidade de uso. Ele também oferece opções avançadas de recursos como a implementação na nuvem versus local, gerenciamento em qualquer lugar utilizando um aplicativo móvel, segurança avançada, como a configuração do BIOS e o bloqueio de portas. Recursos adicionais incluem detecção e registro de dispositivo, gerenciamento de ativos e inventários, gerenciamento de configurações, implantação de sistemas operacionais e aplicativos, comandos em tempo real, monitoramento, alertas, elaboração de relatórios e solução de problemas em pontos de extremidade.

Para obter mais informações sobre o Dell Wyse Management Suite, acesse dell.com/support/manuals.

NOTA: Para registrar os dispositivos que executam o sistema operacional Windows 10 IoT Enterprise no Wyse Management Suite, consulte *Como registrar thin clients padrão incorporados do Windows no Wyse Management Suite usando o Wyse Device Agent,* em dell.com/support/manuals.

Portas e slots

O dispositivo thin client tem muitas portas e slots. Para obter informações sobre as portas e os slots no dispositivo thin client em seu local de trabalho, consulte o respectivo Guia de Início Rápido no site dell.com/support.

Para fornecer os serviços através das portas, instale o software ou driver adequado para o dispositivo thin client.

NOTA:

- **Você pode instalar outros serviços e suplementos que estão disponíveis no site da Dell gratuitamente ou pagando uma taxa de licenciamento.**
- **Você pode configurar o dispositivo thin client para usar periféricos compatíveis com Bluetooth. Para obter mais informações, consulte Como configurar conexões Bluetooth.**

TightVNC – servidor e visualizador

Para configurar ou reiniciar um dispositivo thin client a partir de um local remoto, use TightVNC (servidor e visualizador). O TightVNC foi criado principalmente para fins de suporte e solução de problemas.

Instale o TightVNC em nível local no dispositivo thin client. Após a instalação, ele permite que o thin client seja sombreado, operado e monitorado a partir de um dispositivo remoto.

O TightVNC Server é iniciado automaticamente como um serviço mediante a reinicialização do dispositivo thin client. A inicialização do TightVNC Server também pode ser controlada usando a janela Serviços neste procedimento.

Para abrir a janela **TightVNC Server**:

1. Faça login como um Administrador.
2. Clique em **Menu Iniciar** > **TightVNC** > **TightVNC Server**.

NOTA:

- **O TightVNC Viewer está disponível a partir do site do TightVNC.**
- **O TightVNC está incluído no software WDM como um componente.**
- **O TightVNC Viewer deve ser instalado em um sombreamento ou máquina remota antes do uso.**
- **Se quiser salvar permanentemente o estado do serviço, alinhe os arquivos do Unified Write Filter durante a sessão do sistema atual.**

TightVNC – pré-requisitos

Antes da instalação do TightVNC Server em uma máquina remota, para acessar um dispositivo thin client, você precisa saber o seguinte:

- O endereço IP ou o nome DNS válido do dispositivo thin client para sombrear, operar ou monitorar.
- A senha principal do dispositivo thin client para sombrear, operar ou monitorar.

NOTA:

- **Para obter o endereço IP do dispositivo thin client, mova o ponteiro sobre o ícone do TightVNC na barra de tarefas.**
- **Para configurar o TightVNC Server, a senha padrão é `DELL`.**

Como usar o TightVNC para criar a sombra de um thin client

O TightVNC Server é iniciado automaticamente como um serviço mediante a inicialização do thin client. O serviço do TightVNC Server também pode ser interrompido e iniciado usando a janela Serviços.

1. Faça login como administrador.
2. Clique em **Iniciar** > **Painel de Controle** > **Ferramentas Administrativas** > **Serviços** e, em seguida, selecione **TightVNC Server**.
3. Você também pode usar os recursos do TightVNC Server em **Iniciar** > **TightVNC**.

   Para sombrear um thin client a partir de uma máquina remota:

   a) Em uma máquina remota na qual o TightVNC Viewer está instalado, abra a caixa de diálogo **Nova conexão do TightVNC**.
   b) Digite o endereço IP ou o nome DNS válido do thin client que será sombreado, operado ou monitorado.
   c) Clique em **OK**.
   A caixa de diálogo **Autenticação de VNC** é mostrada.
   d) Digite a **Senha** do thin client que será sombreado; ela é a Senha principal do thin client que será sombreado.
   e) Clique em **OK**.

   O thin client que será sombreado, operado ou monitorado será exibido para o administrador em uma janela separada no computador remoto. Use o mouse e o teclado no computador remoto para operar o thin client como você faria se estivesse operando-o localmente.

Como configurar as propriedades do servidor do TightVNC no thin client

1. Para abrir a caixa de diálogo **Configuração do TightVNC Server (off-line)**, clique em **Iniciar** > **TightVNC** > **TightVNC Server - Configuração Off-line**.
   A caixa de diálogo **Configuração do TightVNC Server (off-line)** é exibida.
2. Na guia **Servidor**, defina a **Senha principal**. Use essa senha enquanto sombreia o thin client. A senha principal padrão é `Wyse`.
3. Na guia **Servidor**, marque as seguintes caixas de seleção:
   - Aceitar conexões de entrada
   - Requerer autenticação de VNC
   - Ativar transferências de arquivo
   - Ocultar papel de parede da área de trabalho
   - Mostrar ícone na área de notificação
   - Servir Java Viewer para clientes da Web
   - Usar um driver espelho se disponível
   - Segurar janelas transparentes
4. Manter as seguintes caixas de seleção em branco:
   - Bloquear eventos de entrada remota
   - Bloquear entrada remota em atividade local
   - Sem entrada local durante sessões de cliente
5. Na caixa **Porta do servidor principal**, selecione ou digite 5900.
6. Na caixa **porta de acesso à Web**, selecione ou digite 5800.
7. Na caixa **Ciclo de pesquisa de tela**, selecione ou digite 1000.
8. Clique em **OK**.

   NOTA: Para fins de segurança, é recomendável que a senha principal seja alterada logo após o recebimento do thin client, e ela deve ser usada exclusivamente pelo administrador.

7

Arquitetura de rede e ambiente de servidor

Esta seção contém informações sobre a arquitetura de rede e o ambiente de servidor empresarial necessários para fornecer serviços de rede e sessão para o thin client. Ela inclui:

- Como configurar seus serviços de rede
- Como usar o Dynamic Host Configuration Protocol (DHCP)
- Opções do DHCP
- Como usar o Sistema de Nomes de Domínio (DNS)
- Sobre o Citrix Studio
- Sobre os serviços do VMware Horizon View Manager

Como configurar seus serviços de rede

Os serviços de rede fornecidos para thin clients podem incluir DHCP, serviços de arquivos FTP e DNS. Você pode configurar, projetar e gerenciar seus serviços de rede, dependendo da disponibilidade em seu ambiente.

Você pode configurar serviços de rede usando:

- Protocolo DHCP
- Sistema de Nomes de Domínio (DNS)

Como usar o Dynamic Host Configuration Protocol

Um thin client é configurado inicialmente para obter seu endereço IP e configurações de rede de um servidor de Protocolo de Configuração de Host Dinâmico (DHCP). Um servidor DHCP fornece o endereço IP ou o nome DNS do servidor FTP e a localização do caminho-raiz do FTP do software no formulário `Microsoft.msi` para acessar as configurações do endereço IP e da rede por meio do processo de atualização do DHCP.

O DHCP é recomendado para configurar e atualizar thin clients, pois ele economiza tempo e esforços necessários para realizar esses processos em nível local em vários thin clients. Se um servidor DHCP não estiver disponível, endereços IP fixos poderão ser atribuídos e deverão ser inseridos em nível local para cada dispositivo.

Um servidor DHCP também pode fornecer o endereço IP do servidor WMS.

Opções de DHCP

As opções de DHCP listadas na tabela a seguir são aceitas pelos thin clients.

Tabela 15. Opções de DHCP

Opção	Descrição	Observações
1	Máscara de sub-rede	Obrigatório
3	Roteador	Opcional, mas recomendado. Não é necessário, a menos que o thin client precise interagir com servidores em uma sub-rede diferente.
6	Servidor de Nomes de Domínio (DNS)	Opcional, mas recomendado
12	Nome do host	Opcionais
15	Nome do domínio	Opcional, mas recomendado
43	Informações específicas de classe de fornecedor	Opcionais

Opção	Descrição	Observações
50	IP solicitado	Obrigatório
51	Período de lease	Obrigatório
52	Sobrecarga opcional	Opcionais
53	Tipo de mensagem de DHCP	Obrigatório
54	Endereço IP do servidor DHCP	Recomendado
55	Lista de solicitações de parâmetro	Enviado por thin client
57	Tamanho máximo da mensagem de DHCP	Opcional (sempre enviado pelo thin client)
58	Tempo T1 (renovar)	Obrigatório
59	Tempo T2 (revincular)	Obrigatório
61	Identificador de cliente	Sempre enviado
155	Endereço IP ou nome do servidor remoto	Opcionais
156	Nome de usuário de login usado para uma conexão	Opcionais
157	Nome de domínio usado para uma conexão	Opcionais
158	Senha de login usada para uma conexão	Opcionais
159	Linha de comando para uma conexão	Opcionais
160	Diretório de trabalho para uma conexão	Opcionais
163	Lista de endereços IP do servidor de interceptação SNMP	Opcionais
164	Comunidade SNMP Set	Opcionais
165	Aplicativos publicados de inicialização da Conexão de Área de Trabalho Remota	Opcionais
168	Nome do servidor da porta virtual	Opcionais
165	Etiqueta de opção do URL do servidor Wyse Management Suite	Opcionais
166	Etiqueta de opção de URL do servidor MQTT	Opcionais
167	Etiqueta de opção do URL do servidor de validação de CA do Wyse Management Suite	Opcionais
199	Etiqueta de opção do URL do servidor de token de grupo do Wyse Management Suite	Opcionais

NOTA: Para obter mais informações sobre como configurar um servidor DHCP, consulte www.microsoft.com.

Como usar o Sistema de Nomes de Domínio

Dispositivos thin client aceitam nomes de DNS válidos registrados em um servidor DNS disponível para a intranet corporativa. O dispositivo thin client envia uma consulta para o servidor DNS na rede para converter o nome no endereço IP correspondente. O DNS permite que hosts sejam acessados pelos seus nomes de DNS registrados em vez do seu endereço IP.

Cada servidor DNS do Windows no Windows Server 2000 e posterior inclui um DNS Dinâmico (DDNS) e cada servidor é registrado de maneira dinâmica com o servidor DNS. Para informações sobre a entrada DHCP do domínio DNS e informações da localização do servidor, consulte Como usar o Dynamic Host Configuration Protocol (DHCP).

Sobre o Citrix Studio

O Citrix Studio é um programa de software que permite que você configure e gerencie áreas de trabalho e aplicativos personalizados. Ele fornece uma experiência de computação do usuário final fácil em todos os dispositivos e redes, além de fornecer desempenho ideal, melhor segurança e melhor personalização.

NOTA: Para obter mais informações sobre como instalar e configurar o Citrix Studio, acesse o site do Citrix.

O Citrix Studio consiste em vários assistentes que permitem que você execute as seguintes tarefas:

- Publicar aplicativos virtuais
- Criar grupos de sistemas operacionais de desktop ou servidor
- Atribuir aplicativos e desktops a usuários
- Conceder acesso do usuário a recursos
- Atribuir e transferir permissões
- Obter e monitorar licenças do Citrix
- Configurar o StoreFront

Todos os Aplicativos de Área de Trabalho Virtual (VDA) disponíveis são mostrados no Studio. Na lista de VDA, selecione o aplicativo que você gostaria de publicar. As informações mostradas no Studio são recebidas a partir do Serviço de Agente no Controlador.

Sobre o VMware Horizon View Manager

O VMware View é um gerenciador de área de trabalho virtual de classe empresarial que conecta de maneira segura usuários autorizados a áreas de trabalho virtuais centralizadas. Ele fornece uma solução completa de ponto a ponto que melhora o controle e a gerenciabilidade, além de fornecer uma experiência de área de trabalho familiar. O software cliente conecta usuários de maneira segura a áreas de trabalho virtuais centralizadas, sistemas físicos de back-end ou servidores de terminal.

NOTA: Para obter mais informações sobre como instalar e configurar o View Manager, acesse o site do VMware.

O VMware View inclui os seguintes componentes principais:

- **View Connection Server**: um serviço de software que atua como um intermediário para conexões de clientes por meio da autenticação e do direcionamento subsequente de solicitações recebidas de usuários de uma área de trabalho remota para a devida área de trabalho virtual, área de trabalho física ou servidor de terminal.
- **View Agent**: um serviço de software que é instalado em todas as máquinas virtuais convidadas, sistemas físicos ou servidores de terminal. O View Manager gerencia esse software. O agente fornece recursos como o monitoramento do Remote Desktop Connection, a impressão virtual, suporte USB remoto e logon único.
- **View Client**: é um aplicativo de software instalado em nível local que se comunica com o View Connection Server para permitir que os usuários se conectem às suas áreas de trabalho usando o Microsoft Remote Desktop Connection.
- **View Portal**: um componente semelhante ao View Client, mas que fornece uma interface de usuário View por meio de um navegador da Web. Ele é suportado em vários sistemas operacionais e navegadores.
- **View Administrator**: esse componente oferece administração do View por meio de um navegador da Web. Administradores do View usam-no para fazer o seguinte:
  - Gerenciar parâmetros de configuração.
  - Gerenciar áreas de trabalho virtuais e direitos de áreas de trabalho de usuários e grupos do Windows.

  O View Administrator também oferece uma interface para monitorar eventos de log e é instalado com o View Connection Server.
- **View Composer**: para permitir que o View Manager implante rapidamente várias áreas de trabalho com clone vinculado a partir de uma única imagem de base centralizada, o serviço do software **View Composer** é instalado no servidor do Virtual Center.

8

Como instalar um firmware usando a USB Imaging Tool

A instalação do firmware é o processo de instalação do firmware do Windows 10 IoT Enterprise em seu thin client.

Use a Dell Wyse USB Imaging Tool versão 3.2.0 para instalar a imagem do Windows 10 IoT Enterprise em seu thin client. Para obter informações sobre as instruções de instalação, consulte o *Guia do usuário do Dell Wyse USB Imaging Tool versão 3.2.0* em https://downloads.dell.com/wyse/.

9

Perguntas frequentes

Como instalar o Skype for Business

Para instalar o Skype for Business em seus thin clients, faça o seguinte:

1. Faça login como administrador.
2. Desative o Unified Write Filter.
3. Faça o download do Skype for Business autônomo (64 bits), em https://support.microsoft.com.
4. Clique duas vezes no arquivo .exe e, em seguida, clique em **Executar**.
5. Depois de concluída a instalação, clique em **Fechar**.
6. Abra o Skype for Business.
7. Na tela do contrato de licença, clique em **Aceitar**.
8. Ative o Unified Write Filter.

   Para obter mais informações, consulte *Instalar o Skype for Business* em https://support.office.com.

Como configurar um leitor de smart card

Para configurar um leitor de smart card, faça o seguinte:

1. <1></1>Faça login como administrador.
2. Desative o Unified Write Filter.
3. Faça o download do seu aplicativo de smart card preferido.
4. Extraia o arquivo para sua unidade local.
5. Conecte o leitor de smart card ao smart card, e clique em **Configuração**.
6. Depois que a instalação estiver concluída, instale o certificado do servidor se você quiser estabelecer uma conexão para a configuração do Citrix ou do VMware.
7. Ative o Unified Write Filter.
8. Conecte-se à sua sessão de VDI preferida como o Citrix, VMware ou RDP.

Como usar o redirecionamento USB

O Redirecionamento USB permite que você conecte um dispositivo externo a uma porta USB em seu thin client e acesse o dispositivo usando um aplicativo ou área de trabalho remota.

Você pode configurar o Redirecionamento USB em um ambiente Citrix Virtual Apps and Desktops (antigo Citrix XenDesktop). Para obter mais informações, consulte *Guia de Configuração do Redirecionamento USB Genérico do Citrix* no site support.citrix.com.

Você também pode configurar opções para usar e gerenciar dispositivos USB em uma sessão de área de trabalho virtual de exibição. Para obter mais informações, consulte *Redirecionamento de dispositivo USB, configuração e uso em desktops virtuais de exibição* no site www.vmware.com

Como capturar e enviar uma imagem de sistema operacional Windows 10 IoT Enterprise

Você pode capturar e enviar uma imagem do sistema operacional Windows 10 IoT Enterprise usando qualquer um dos seguintes métodos:

- Wyse Management Suite
- Microsoft System Center Configuration Manager (SCCM)
- USB Imaging Tool

Para obter informações sobre o Wyse Management Suite e o SCCM, consulte os respectivos guias, em https://support.dell.com/manuals.

Para obter informações sobre o USB Imaging Tool, consulte o *Guia do usuário do Dell Wyse USB Imaging Tool,* em https://downloads.dell.com/wyse.

10

Solução de problemas

Problemas de personalização de teclado

Para personalizar um idioma de teclado que não seja suportado por padrão, faça o seguinte:

1. Acesse `C:\Windows\system32\oobe`.
2. Exclua o arquivo `oobe.xml` e os subdiretórios relacionados.
3. Personalize o arquivo sysprep.xml manualmente e configure o teclado, locais, e assim por diante, para o respectivo idioma.
4. Implante o arquivo .xml manualmente, ou usando o SCCM ou Custom Sysprep.

Todas as preferências de teclado, local, fuso horário, países, e assim por diante, são aplicadas.

Como resolver problemas de memória

Para solucionar problemas de erro de **falta de memória** em thin clients Dell Wyse com Windows, use uma das seguintes ferramentas para identificar e ajustar os requisitos de memória:

- Gerenciador de Tarefas do Windows
- Unified Write Filter
- Explorador de arquivos

NOTA: O nome da caixa de diálogo de erro ajuda a identificar a origem do problema de memória.

Como usar o Gerenciador de Tarefas do Windows

1. Faça login como administrador.
2. Pressione Ctrl+Alt+Delete.
3. Clique em **Gerenciador de tarefas**.

   A janela do **Gerenciador de Tarefas** é exibida.
4. Clique em **Mais detalhes**.
5. Clique na guia **Performance**, e analise os recursos de memória do seu sistema.
6. Feche os programas que estão usando mais memória.

Como usar o Unified Write Filter

1. Faça login como administrador.
2. Clique duas vezes no ícone UWF na bandeja do sistema.
3. Configure a opção **Quantidade de memória RAM a ser usada para o cache do FBWF (MB)**.

Como usar o Explorador de arquivos

Você pode usar o Explorador de arquivos para verificar o tamanho da sua unidade Z: (RAMDisk). Você deve atualizar a aplicação para ver os valores atualizados.

Problemas de BSOD ou erro de tela azul

Um erro de tela azul ou BSOD com o código de erro `CRITICAL PROCESS DIED` é observado no thin client Wyse 5070 com discos de estado sólido Apacer com Windows 10 IoT Enterprise versão 10.03.06.10.18.00. Para resolver esse problema, você precisa desativar o link do modo de gerenciamento de energia para dispositivos de armazenamento que estão conectados ao this client usando uma interface AHCI.

NOTA: Este problema é resolvido em imagens criadas com o Windows 10 IoT Enterprise com versões posteriores a versão 10.03.06.10.18.00, e, portanto, você não precisa aplicar a entrada de registro manualmente.

Para desativar o link do modo de gerenciamento de energia usando um arquivo de registro, faça o seguinte:

1. Faça login como administrador.
2. Desative o Unified Write Filter.

   O sistema será reiniciado.
3. Faça login como administrador novamente.
4. Abra o bloco de notas e digite a seguinte sintaxe:

```
Windows Registry Editor Version 5.00
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\storahci\Parameters\Device]
"SingleIO"=hex(7):2a,00,00,00
"NoLPM"=hex(7):2a,00,00,00
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Power\PowerSettings
\0012ee47-9041-4b5d-9b77-535fba8b1442\0b2d69d7-a2a1-449c-9680-
f91c70521c60\DefaultPowerSchemeValues\381b4222-f694-41f0-9685-ff5bb260df2e]
"ACSettingIndex"=dword:00000000
"DCSettingIndex"=dword:00000000
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Power\PowerSettings
\0012ee47-9041-4b5d-9b77-535fba8b1442\0b2d69d7-a2a1-449c-9680-
f91c70521c60\DefaultPowerSchemeValues\8c5e7fda-e8bf-4a96-9a85-a6e23a8c635c]
"ACSettingIndex"=dword:00000000
"DCSettingIndex"=dword:00000000
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Power\PowerSettings
\0012ee47-9041-4b5d-9b77-535fba8b1442\0b2d69d7-a2a1-449c-9680-
f91c70521c60\DefaultPowerSchemeValues\a1841308-3541-4fab-bc81-f71556f20b4a]
"ACSettingIndex"=dword:00000000
"DCSettingIndex"=dword:00000000
```

5. Salve o arquivo como um arquivo `.reg`.
6. Clique em **Iniciar**.
7. Digite `cmd` no campo de pesquisa.
8. Clique com o botão direito em **Prompt de comando**.
9. Clique em **Executar como administrador**.

   A janela Controle de Conta de Usuário é exibida.
10. Clique em **Sim**.

    A janela do prompt de comando elevado é exibida.
11. Execute o comando `reg import <file path of the registry file>`.
12. Ative o Unified Write Filter.