



CONFIGURAÇÃO DE SERVIDOR NTP

Sincronização de horário do
servidor facial Hikvision

Versão 1
Março de 2024



Sumário

1. INTRODUÇÃO	4
2. REQUISITOS.....	4
3. CONFIGURANDO O SERVIÇO NTP NO SERVIDOR KEYACCESS	4
3.1 DONWLOAD E INSTALAÇÃO.....	5
3.2 CONFIGURANDO O FIREWALL DO WINDOWS.....	6
4. CONFIGURANDO OS SERVIDORES FACIAIS HIKVISON.....	13



1. INTRODUÇÃO

Este guia tem como propósito detalhar os procedimentos necessários para configurar o servidor KeyAccess com o serviço NTP, permitir o tráfego na porta de comunicação no Firewall do sistema operacional Microsoft Windows e ajustar os servidores faciais da marca Hikvision para sincronização com o horário atualizado.

2. REQUISITOS

- O servidor KeyAccess requer conexão à internet.
- A empresa responsável pela integração e manutenção do sistema deve configurar o serviço NTP no servidor KeyAccess.
- É necessário habilitar a porta de comunicação 123, utilizando o protocolo UDP, no firewall do Windows.
- Por último, configurar a atualização do horário nos servidores faciais, apontando para o IP do servidor KeyAccess, definindo a porta 123 como padrão e especificando o intervalo de tempo para a atualização automática da data e hora.

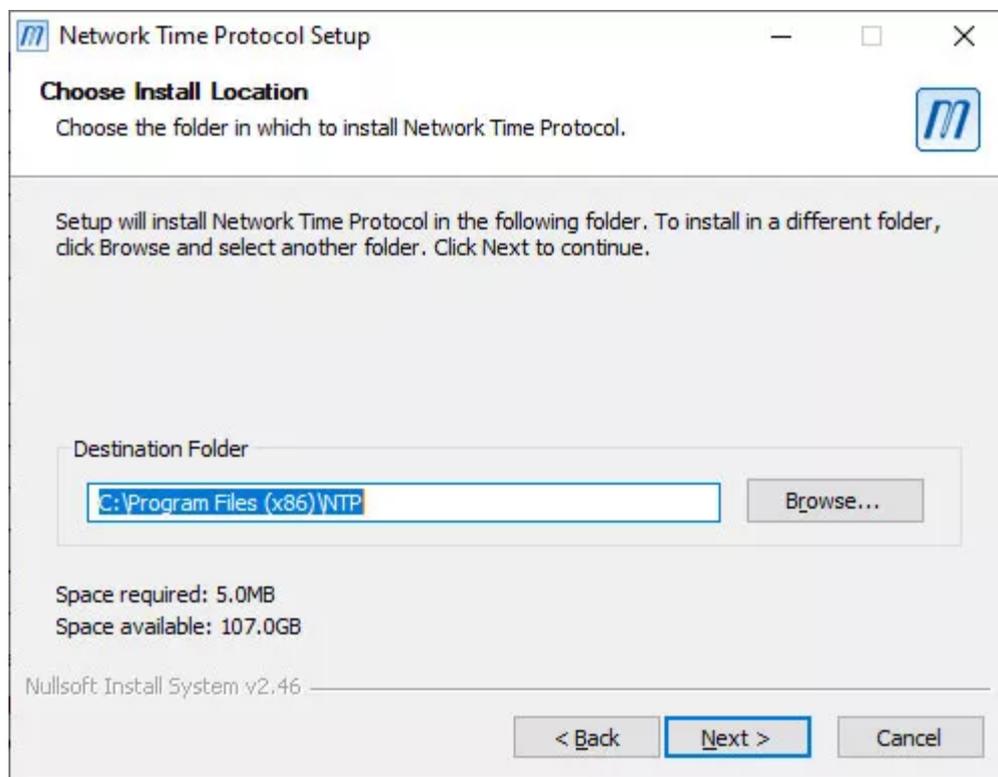
3. CONFIGURANDO O SERVIÇO NTP NO SERVIDOR KEYACCESS

As instruções para configurar o servidor NTP no servidor KeyAccess estão disponíveis em um vídeo na plataforma YouTube, acessível através do seguinte link: https://youtu.be/6edjml_yEdw.



3.1 Download e instalação

Faça o download do sistema de sincronização de horário da NTP.BR através do seguinte link: <http://www.meinberg.de/english/sw/ntp.htm>. Para sistemas Windows (a partir do Windows XP) com suporte a IPv6, baixe o instalador ntp-4.2.8p15a-win32-setup.exe. Após o download, execute o software, aceite os termos de uso e selecione o local de instalação do programa.



Clique em "Next" para continuar com a instalação. Certifique-se de selecionar e instalar todos os componentes fornecidos durante o processo.

Clique em "Next" para avançar com a instalação. Na tela seguinte, selecione "Create initial configuration file with the following settings" e preencha o campo "You can specify up to 9 NTP servers..." com os nomes dos servidores NTP separados por vírgulas.

a.st1.ntp.br,b.st1.ntp.br,c.st1.ntp.br,d.st1.ntp.br,gps.ntp.br,a.ntp.br,b.ntp.br,c.ntp.br



Os servidores separados por ordem são:

a.st1.ntp.br

b.st1.ntp.br

c.st1.ntp.br

d.st1.ntp.br

gps.ntp.br

a.ntp.br

b.ntp.br

c.ntp.br

Selecione "Next" para prosseguir a instalação. Será perguntado se você deseja rever o arquivo de configuração para adicionar outras configurações. Selecione "Não".

Em seguida, clique em "Next" para continuar. Mantenha os valores de padrão nas configurações de serviço e clique em "Next".

Será pedido para criar um usuário. Preencha com os dados que desejar.

Clique em "Next" para prosseguir. Espere o serviço ser iniciado e clique em "Finish" para terminar a instalação.

3.2 Configurando o firewall do Windows

Depois de instalar e configurar a aplicação, será preciso ativar a porta 123, utilizando o protocolo UDP, no firewall do sistema operacional Microsoft Windows.

Acesse o Painel de Controle do Windows.

Selecione a opção "Sistema e Segurança".



> Painel de Controle

Ajuste as configurações do computador Exibir por: Categoria ▾

- Sistema e Segurança**
 - Verificar o status do computador
 - Salvar cópias de backup dos arquivos com Histórico de Arquivos
 - Backup e Restauração (Windows 7)
- Rede e Internet**
 - Exibir o status e as tarefas da rede
- Hardware e Sons**
 - Exibir impressoras e dispositivos
 - Adicionar dispositivo
 - Ajustar as configurações de mobilidade comumente usadas
- Programas**
 - Desinstalar um programa
- Contas de Usuário**
 - Alterar o tipo de conta
- Aparência e Personalização**
- Relógio e Região**
 - Alterar formatos de data, hora ou número
- Facilidade de Acesso**
 - Permitir que o Windows sugira configurações
 - Otimizar exibição visual

Em seguida, clique sobre Windows Defender Firewall e selecione o item configurações avançadas.

Windows Defender Firewall

< > ▾ ↑ > Painel de Controle > Sistema e Segurança > Windows Defender Firewall

Início do Painel de Controle

- Permitir um aplicativo ou recurso através do Windows Defender Firewall
- Alterar configurações de notificação
- Ativar ou Desativar o Windows Defender Firewall
- Restaurar padrões
- Configurações avançadas
- Solucionar problemas com a rede

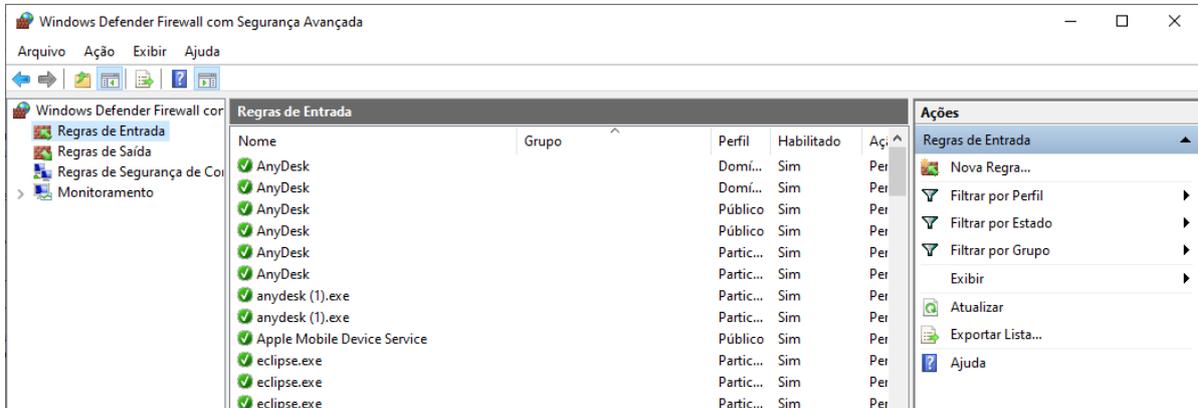
Ajude a proteger o PC com o Windows Defender Firewall

O Windows Defender Firewall ajuda a impedir que hackers ou softwares mal-intencionados obtenham acesso ao PC através da Internet ou de uma rede.

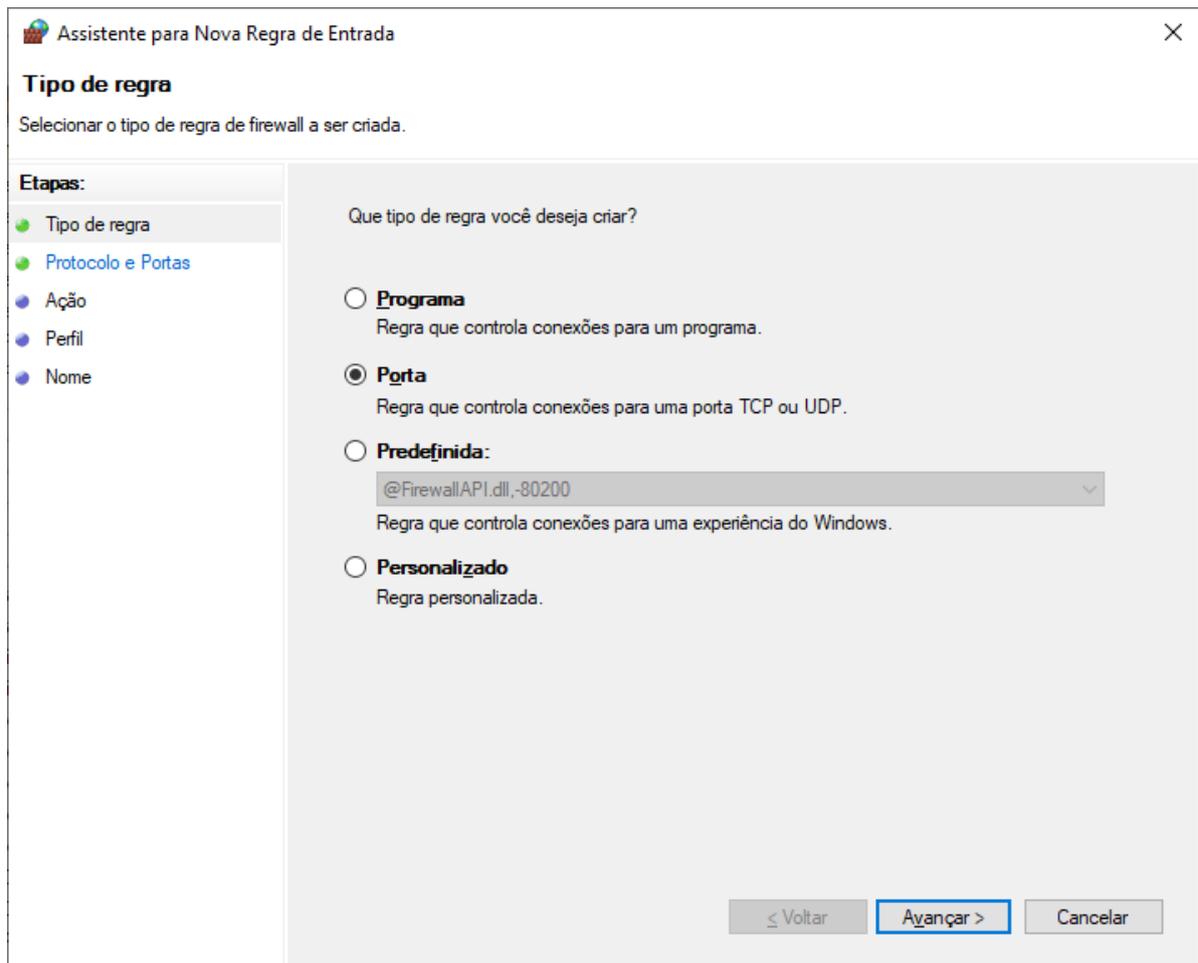
	Redes privadas	Não conectado ▾
	Redes públicas ou convidadas	Conectado ▲
Redes em locais públicos como aeroportos ou cafés		
Estado do Windows Defender Firewall:	Ativado	
Conexões de entrada:	Bloquear todas as conexões com aplicativos que não estejam na lista de aplicativos permitidos	
Redes públicas ativas:	MM-Connect-5G OpenVPN TAP-Windows6	
Estado da notificação:	Notificar-me quando o Windows Defender Firewall bloquear um aplicativo novo	



Clique em regras de entrada e nova regra.



Escolha porta como tipo de regra e clique em avançar.





Em protocolo e portas, selecione a opção UDP. No campo portas locais específicas, preencha o valor 123. Clique sobre avançar.

Assistente para Nova Regra de Entrada [X]

Protocolo e Portas

Especifique os protocolos e as portas a que a regra se aplica.

Etapas:

- Tipo de regra
- Protocolo e Portas**
- Ação
- Perfil
- Nome

Essa regra se aplica a TCP ou a UDP?

TCP

UDP

Essa regra se aplica a todas as portas locais ou a portas locais específicas?

Todas as portas locais

Portas locais específicas:

Exemplo: 80, 443, 5000-5010



Em ação, clique sobre permitir a conexão e em avançar.

Assistente para Nova Regra de Entrada [X]

Ação

Especifique a ação executada quando uma conexão atender às condições especificadas na regra.

Etapas:

- Tipo de regra
- Protocolo e Portas
- **Ação**
- Perfil
- Nome

Que ação deve ser tomada quando uma conexão corresponde às condições especificadas?

- Permitir a conexão**
Isso inclui conexões protegidas com IPsec bem como as sem essa proteção.
- Permitir a conexão, se for segura**
Isso inclui conexões que foram autenticadas usando IPsec. As conexões serão protegidas por meio de uso das configurações nas regras e propriedades IPsec no nó Regra de Segurança de Conexão.
[Personalizar...](#)
- Bloquear a conexão**

[< Voltar] [**Avançar >**] [Cancelar]



Mantenha as regras marcadas e acione o comando avançar.

Assistente para Nova Regra de Entrada

Perfil

Especificar os perfis aos quais essa regra se aplica.

Etapas:

- Tipo de regra
- Protocolo e Portas
- Ação
- Perfil**
- Nome

Quando esta regra se aplica?

- Domínio**
Aplica-se quando um computador está conectado ao seu domínio corporativo.
- Particular**
Aplica-se quando um computador está conectado a um local de rede privada, como residência ou local de trabalho.
- Público**
Aplica-se quando um computador está conectado a um local de rede pública.

≤ Voltar **Avançar >** Cancelar

No campo nome, preencha as informações:

KeyAccess - NTP - Atualização de servidores faciais

Na descrição, entre com os dados:

Permite que os servidores faciais atualizem suas configurações de data e hora com base nas informações do servidor KeyAccess.



Para finalizar, clique sobre concluir.

Assistente para Nova Regra de Entrada

Nome
Especificar o nome e a descrição desta regra.

Etapas:

- Tipo de regra
- Protocolo e Portas
- Ação
- Perfil
- Nome**

Nome:
KeyAccess - NTP - Atualiação de servidores faciais

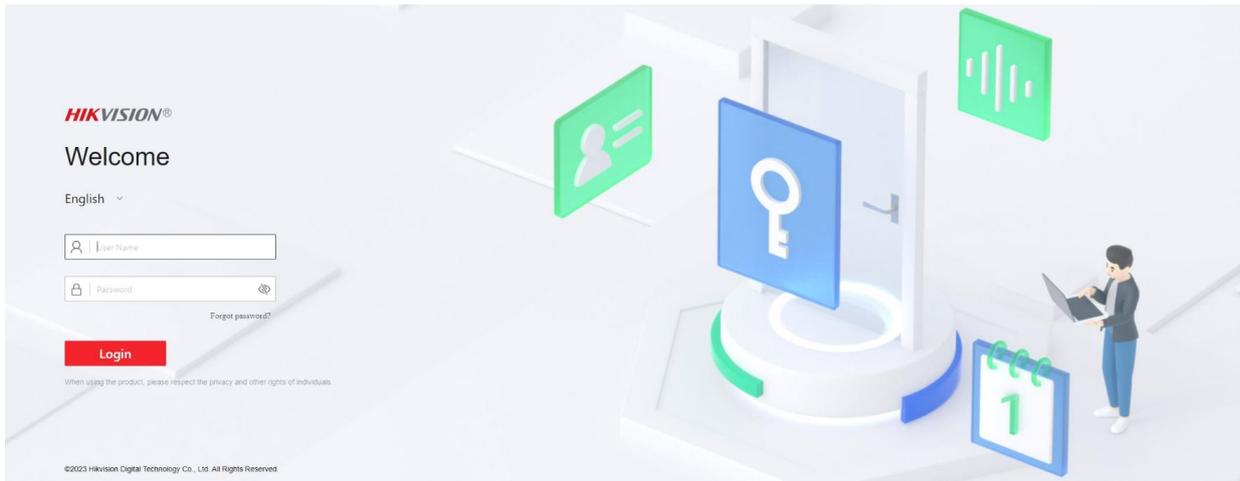
Descrição (opcional):
Permite que os servidores faciais atualizem suas configurações de data e hora com base nas informações do servidor KeyAccess.

≤ Voltar Concluir Cancelar



4. CONFIGURANDO OS SERVIDORES FACIAIS HIKVISION

No navegador, digite o IP do PAD leitor facial (servidor), preencha os campos user name e password e clique sobre o comando login.



No menu lateral clique sobre configuration. Em seguida, selecione a opção System Settings.

Na aba Time Settings entre com as informações:

- Time Zone: (GMT -03:00) Georgetown, Brasília
- Time Synchronization mode: NTP
- Server IP Address: [insira o IP do servidor KeyAccess]
- NTP Port: 123
- Interval: 5 min



HIKVISION®

System ^

- Overview
- System Settings**
- User Management
- Network v
- Video/Audio
- Image
- Event v
- Access Control
- Intercom
- Card Settings
- Platform Attendance
- Security
- Smart
- Preference

Basic Information **Time Settings**

Device Time 2024-03-13 10:21:32

Time Zone (GMT-03:00) Georgetown, Brasilia v

Time Synchronization mode NTP Manual

*Server IP Address 192.168. [REDACTED]

*NTP Port 123

*Interval 5 min ^ v

DST

DST

Save