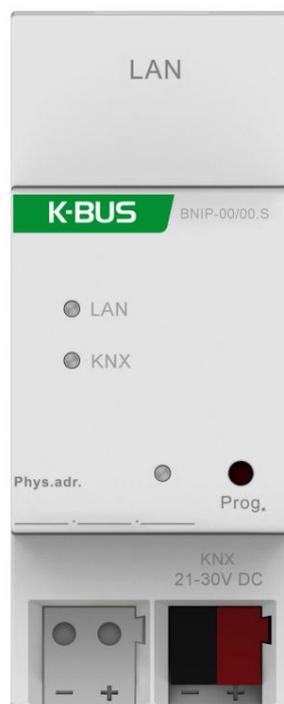


Manual do usuário

Interface IP K-BUS•R com Secure_V1.1

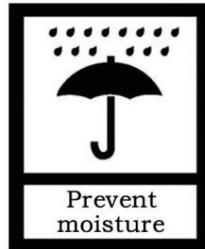
BNIP-00/00.S



Sistema de controle residencial e predial KNX/EIB

atenções

1. Por favor, mantenha os dispositivos longe do campo magnético forte, alta temperatura, ambiente úmido;



2. Por favor, não deixe cair o dispositivo no chão ou o faça ficar duro impacto;



3. Por favor, não use pano úmido ou reagente volátil para limpar o dispositivo;



4. Não desmonte os dispositivos.

Conteúdo

Resumo do capítulo 1	4
Capítulo 2 Dados técnicos	5
Capítulo 3 Dimensão e Diagrama de Conexão	6
3.1. Diagrama de dimensões	6
3.2. Diagrama de conexão	6
Capítulo 4 Descrição da configuração de parâmetros no ETS	7
4.1. Janela de parâmetros "Geral"	7
4.2. Uso dos servidores de tunelamento integrados	10
4.3. KNX Secure	12
4.4. Descarregando o dispositivo	18
4.5. Leia as informações do dispositivo	19
Capítulo 5 Configuração de fábrica	19
Capítulo 6 Configuração da Web	20

Capítulo 1 Resumo

A Interface IP com Secure é projetada para um sistema de controle predial inteligente, que é usado para facilitando a comunicação entre a rede Ethernet e o sistema KNX. O telegrama KNX pode ser enviados ou recebidos de outros dispositivos através da rede.

O dispositivo suporta o protocolo KNX Secure (KNXnet/IP Security).

O dispositivo serve de interface entre instalações KNX e redes IP, podendo configurar, parametrizar e comissionar a instalação KNX, bem como o monitoramento do grupo via LAN usando o Software ETS.

A conexão de barramento é realizada usando terminais de conexão de barramento KNX.

O dispositivo adota uma interface Ethernet RJ45 para se conectar à rede LAN. A interface de rede pode ser operado com uma velocidade de transmissão de 10/100Mbit/s Auto Sensing.

O endereço IP do dispositivo pode ser fixo ou pode ser recebido de um servidor DHCP. Se você precisar permaneça o endereço IP estático ou aqui nenhum servidor DHCP na rede, você pode atribuir um endereço IP fixo para o dispositivo via ETS.

Ele pode suportar o telegrama UDP/TCP e o número da porta 3671, e suportar até 5 clientes IP KNX conexões, consulte o capítulo 3.3.

É capaz de usar o Engineering Tool Software ETS (ETS5 ou posterior) com um arquivo .knxprod para alocar o endereço físico e defina o parâmetro.

É um dispositivo de instalação modular. Pode ser instalado no quadro de distribuição em montagem de 35mm trilhos de acordo com EN 60 715.

Este manual fornece informações técnicas detalhadas sobre a função, bem como a montagem e programação do dispositivo para usuários e explica como usar o dispositivo de interface pelo aplicativo exemplos.

Nota: O dispositivo não suporta a própria programação usando uma conexão de encapsulamento IP, mas ele pode ser programado por meio de uma conexão de transmissão (Realtek PCIe GBE Family Controller).

O dispositivo também não suporta monitoramento de barramento.

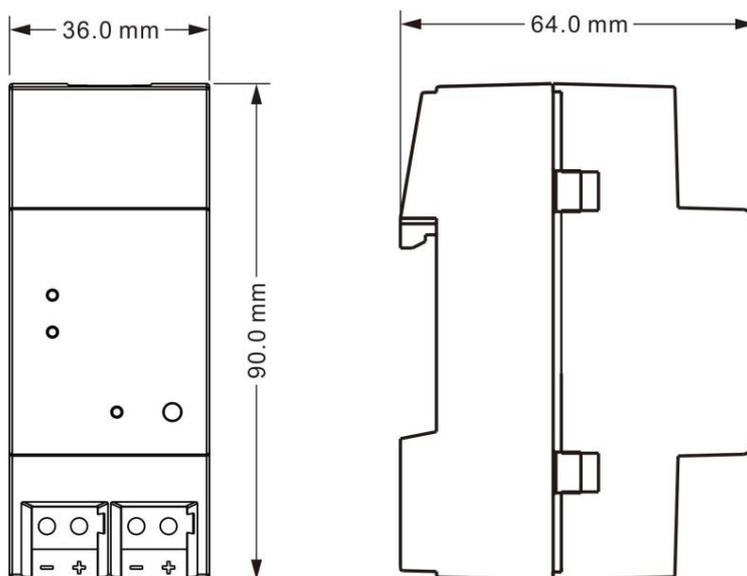
Capítulo 2 Dados Técnicos

Fonte de energia	Tensão de operação	21-30V DC, através do barramento KNX
	Consumo atual	<19,5 mA, 24 V; <15,5mA, 30V
	Consumo de energia	<470mW
Conexões	KNX	Através do terminal de conexão de barramento (vermelho/preto)
	E	Soquete RJ45 para 10/100Base-T, IEEE 802.3 rede, detecção automática
Operacional e mostrar	LED de programação e botão	Para atribuição do endereço físico
	LAN LED ON	Indicador de conexão de rede
	LAN LED piscando	Tráfego de telegrama entre o dispositivo e a rede
	LED KNX LIGADO	Indicador de conexão de barramento KNX
	LED KNX piscando	Tráfego de telegramas entre o dispositivo e o bus KNX
Temperatura	Operação	-5 °C ... + 45 °C
	Armazenar	-25 °C ... + 55 °C
	Transporte	- 25 °C ... + 70 °C
Ambiente	Umidade	<93%, exceto condensação
Projeto	Dispositivo de instalação modular, em trilho de montagem de 35 mm	
Dimensões	36 mm x 90 mm x 64 mm	
Peso	0,1KG	
Carcaça, cor	Carcaça de plástico, bege	

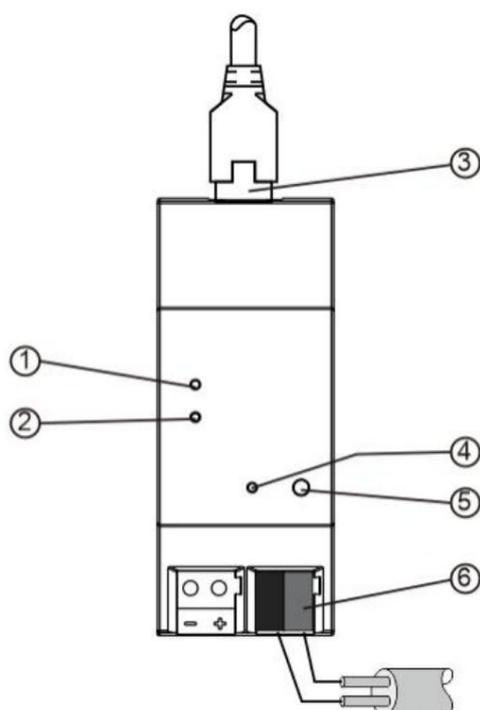
Programa de aplicação	Máx. número de objetos de comunicação	máx. número de endereço do grupo	máx. número de associações
Interface IP com Secure 0		0	0

Capítulo 3 Dimensão e Diagrama de Conexão

3.1. Diagrama de dimensões



3.2. Diagrama de conexão



① LAN LED ON, indica que a rede está conectada normalmente

LAN LED piscando, indica que o tráfego de telegrama entre dispositivo e rede

② KNX LED ON, indicam que o barramento KNX está conectado normalmente

LED KNX piscando, indica que o tráfego de telegrama entre Barramento e dispositivo KNX

③ conexão LAN

④ LED de programação, LED vermelho aceso para atribuição de endereço físico

⑤ Botão de programação, para entrar ou sair do físico modo de programação de endereço

Redefinir o dispositivo para a configuração de fábrica: pressione o botão de programação e segure por 4 segundos solte, repita a operação por 4 vezes e o intervalo entre cada operação é inferior a 3 segundos

⑥ Terminal de ligação bus KNX

Capítulo 4 Descrição da configuração de parâmetros no ETS

4.1. Janela de parâmetros “Geral”

A janela de parâmetros “General” é mostrada na fig. 4.1.1. As informações do dispositivo, incluindo o nome da empresa, nome do projeto, o servidor DNS pode ser definido aqui.

--- IP Interface with Secure > General

General

Company Name

Project Name

DNS server

IP Settings

Configuration in ETS windows -> Properties <-

Device name: Device --> Properties --> Settings --> Name

IP addresses: Device --> Properties --> IP

Fig 4.1.1 Janela de parâmetros "Geral"

Parâmetro "Nome da empresa (30 caracteres)"

Este parâmetro é usado para definir o nome da empresa à qual o dispositivo pertence. Máximo de 30 caracteres pode ser entrada.

Parâmetro "Nome do projeto (30 caracteres)"

Este parâmetro é usado para definir o nome do projeto ao qual o dispositivo pertence. Máximo de 30 caracteres podem ser entrada.

Parâmetro "servidor DNS"

Este parâmetro é usado para definir o endereço do servidor DNS.

Parâmetro "Configurações de IP..."

Configuração nas janelas ETS-->Propriedades

Configure os parâmetros IP do dispositivo IP na janela de propriedades do ETS.

Nome do dispositivo: Dispositivo-->Propriedades-->Configurações-->Nome

O nome do dispositivo pode ser inserido na janela Propriedades de configurações. O nome do dispositivo carregado em o dispositivo pode ser alterado no campo Nome, conforme Figura 4.1.2 abaixo.

O nome do dispositivo é usado para identificação do dispositivo na LAN. Por exemplo, a instalação a localização pode ser identificada pelos nomes atribuídos aos dispositivos, por exemplo, interface IP, hall, etc.

Nota: Somente os primeiros 30 caracteres do nome do dispositivo são carregados no dispositivo; o resto é truncado.

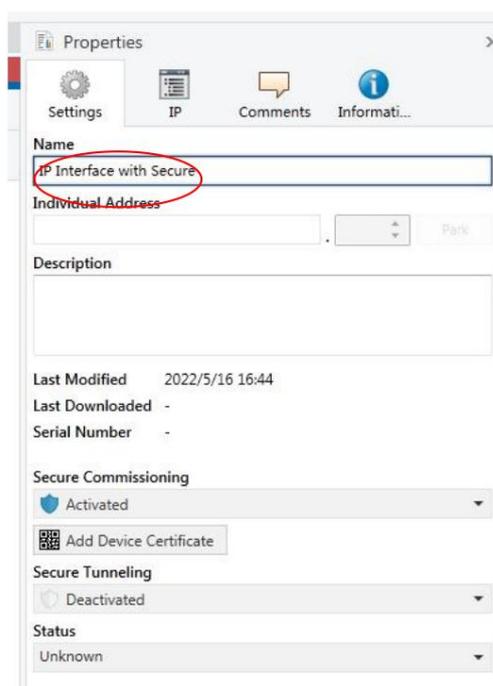


Fig. 4.1.2 Configurações

Endereços IP: Dispositivo-->Propriedades-->IP

O endereço IP pode ser definido na janela IP Properties, conforme Figura 4.1.3 abaixo.

As seguintes opções estão disponíveis para configurar o endereço IP:

Opções:

Obter um endereço IP automaticamente

Use um endereço IP estático

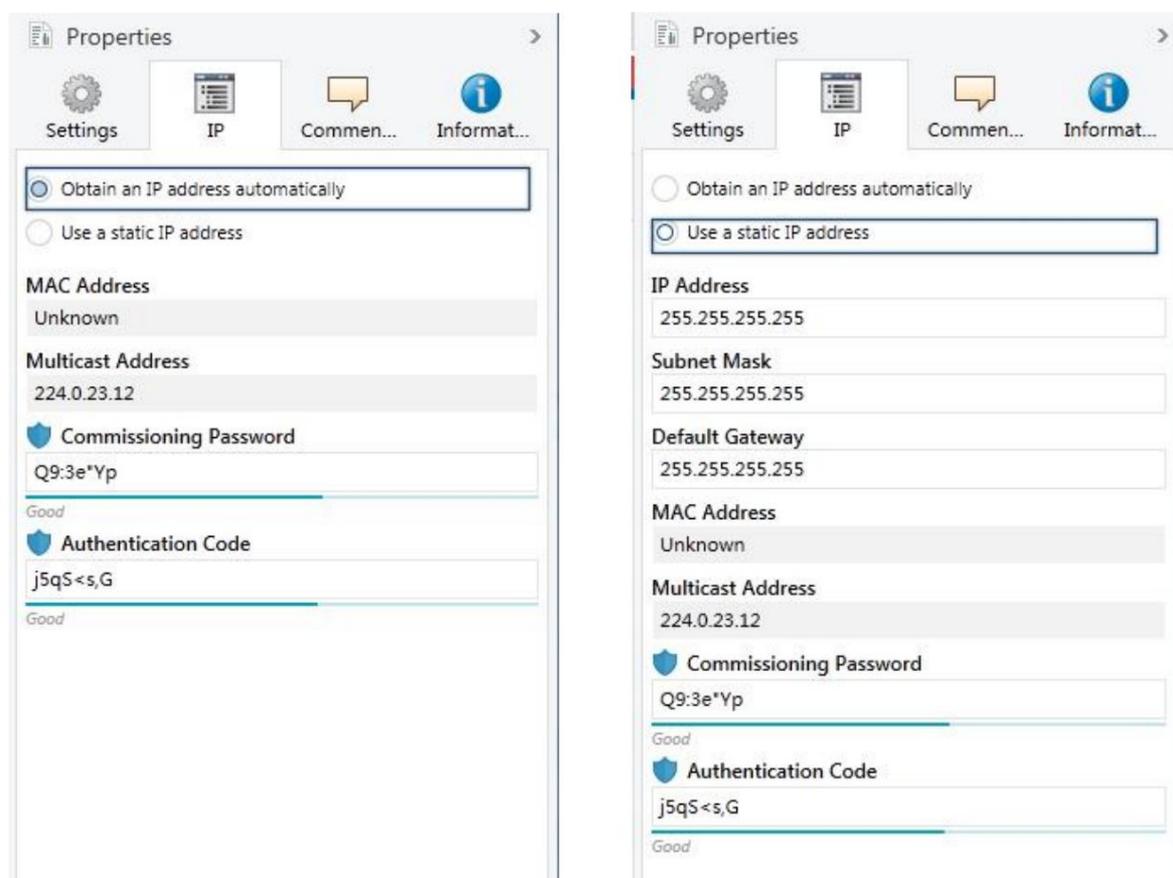


Fig. 4.1.3 PI

Obter um endereço IP automaticamente: Na configuração padrão, a interface IP com segurança espera que o atribuição de um endereço IP por um servidor DHCP (protocolo de configuração de host dinâmico). este servidor responde a uma solicitação atribuindo um endereço IP gratuito ao dispositivo. Se um servidor DHCP não estiver disponível em a rede, o dispositivo ficará inacessível.

Use um endereço IP estático Se nenhum servidor DHCP estiver instalado na rede ou se o endereço IP permanecer o mesmo, ele pode ser atribuído como estático. Ao atribuir endereços IP estáticos, certifique-se de que cada dispositivo recebe um endereço IP diferente e também configura a máscara de sub-rede correspondente e padrão

Porta de entrada.

O endereço MAC é lido do dispositivo após um download

O endereço multicast é exibido apenas aqui, 224.0.23.12, não pode ser alterado.

A senha de ativação e o código de autenticação só são visíveis quando o KNX Secure está ativados e são necessários para conexões de túnel IP.

4.2. Uso dos servidores de tunelamento integrados

A Interface IP com Secure oferece 5 endereços físicos adicionais, que podem ser usados para um conexão de tunelamento, mostrado na fig. 4.2.1. Esses chamados servidores de tunelamento podem ser usados com o ETS como uma interface de programação ou com outro cliente de exibição visual, com smartphone, com tablet, com ferramenta de barramento etc.

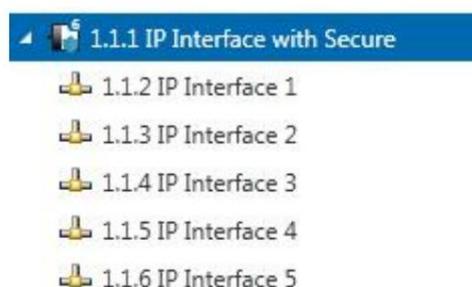


Fig.4.2.1 Tunelamento

O endereço físico de cada conexão de encapsulamento pode ser alterado na janela de propriedades de configuração, e seus endereços físicos devem caber na topologia.

No ETS, os primeiros cinco endereços livres na linha são atribuídos automaticamente após o dispositivo ter sido inserido em uma linha. Esta é uma propriedade do ETS e não pode ser alterada.

Os endereços estarão disponíveis no dispositivo após o primeiro download.

Se isso não for desejado, a configuração pode ser alterada manualmente na janela Propriedades ativando o Park, mostrado na fig. 4.2.2. Este túnel receberá o endereço 15.15.255 após o download. Se a opção Park for selecionado para todos os servidores de encapsulamento, todos os servidores de encapsulamento receberão o endereço 15.15.255. (15.15.255 é o endereço padrão para dispositivos sem endereço físico atribuído)

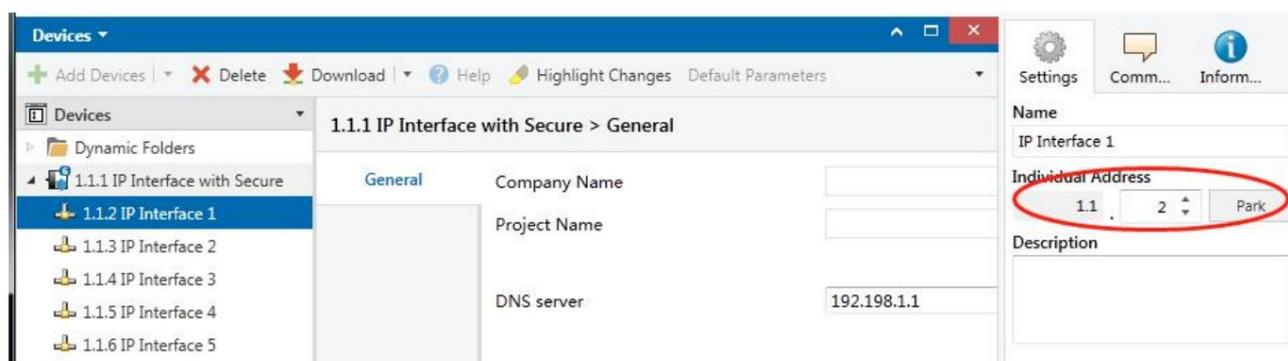


Fig.4.2.2 Configuração - Estacionar

Além disso, os servidores de tunelamento também podem ser criptografados com KNX Secure. Primeiro ative o Secure Comissionamento e, em seguida, ative o Secure Tunneling, conforme mostrado na Figura 4.2.3. Depois de ativar o Secure

Tunneling, a senha para cada conexão Tunneling pode ser definida no ETS, conforme mostrado na Figura 4.2.4, e os usuários podem alterar essa senha conforme necessário.

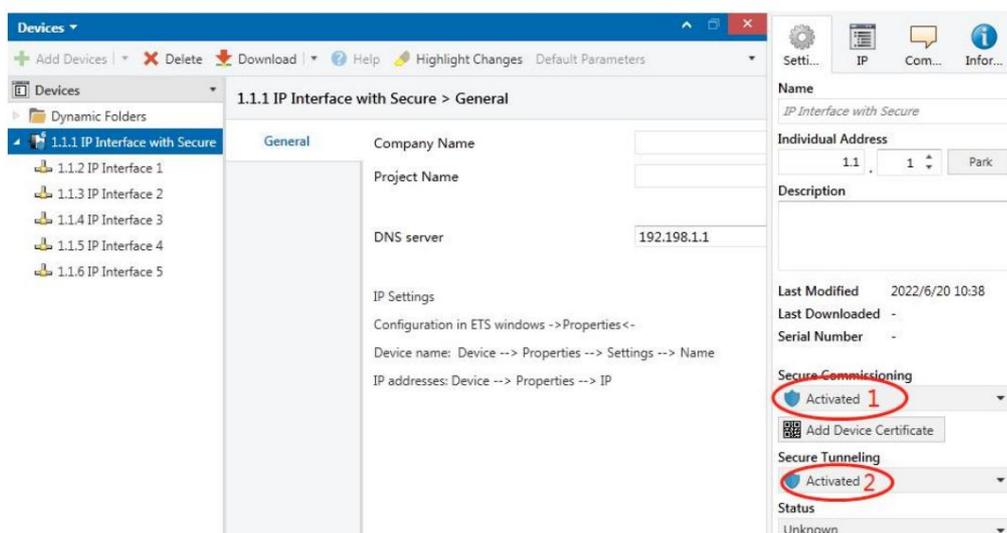


Fig.4.2.3 Configuração - Seguro ativado

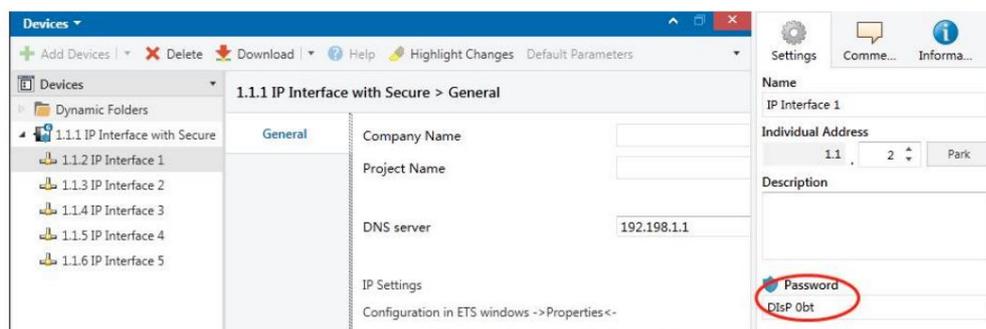


Fig.4.2.4 Configuração - senha de encapsulamento

Se uma senha de projeto não for atribuída ao projeto, o ETS solicitará a atribuição de uma senha de projeto quando ativar o Comissionamento Seguro, conforme mostrado na Figura 4.2.5 abaixo. Em outras palavras, você deve definir um senha do projeto para o projeto, caso contrário, o Comissionamento Seguro não pode ser ativado.



Fig.4.2.5 Definir senha do projeto

4.3. KNX Secure

A Interface IP com Secure é um dispositivo KNX de acordo com o padrão KNX Secure. Em outras palavras, o dispositivo pode ser executado em modo seguro e a conexão de encapsulamento é criptografada.

Portanto, as seguintes informações devem ser levadas em consideração durante o comissionamento do dispositivo:

• É essencial atribuir uma senha de projeto assim que um dispositivo KNX Secure for importado para um projeto. Isso protegerá o projeto contra acesso não autorizado.

A senha deve ser mantida em local seguro – o acesso ao projeto não é possível sem ela

(nem mesmo a Associação KNX ou o fabricante do dispositivo poderão acessá-lo)!

Sem a senha do projeto, a chave de comissionamento não poderá ser importada.

• Uma chave de comissionamento é necessária ao comissionar um dispositivo KNX Secure (primeiro download). Esta chave (FDSK = Chave de configuração padrão de fábrica) está incluída em um adesivo na lateral do dispositivo e devem ser importados para o ETS antes do primeiro download.

• No primeiro download do dispositivo, uma janela aparece no ETS para solicitar que o usuário insira a chave, conforme mostrado na Figura 4.3.1 abaixo. O certificado também pode ser lido no dispositivo usando um QR digitalizador (recomendado).



Fig.4.3.1 Janela Adicionar certificado de dispositivo

• Alternativamente, os certificados de todos os dispositivos seguros podem ser previamente inseridos no ETS. Esse é feito na guia "Segurança" na página de visão geral do projeto, conforme mostrado na Figura 4.3.2 abaixo.

Os certificados também podem ser adicionados ao dispositivo selecionado no projeto, conforme Figura 4.3.3.

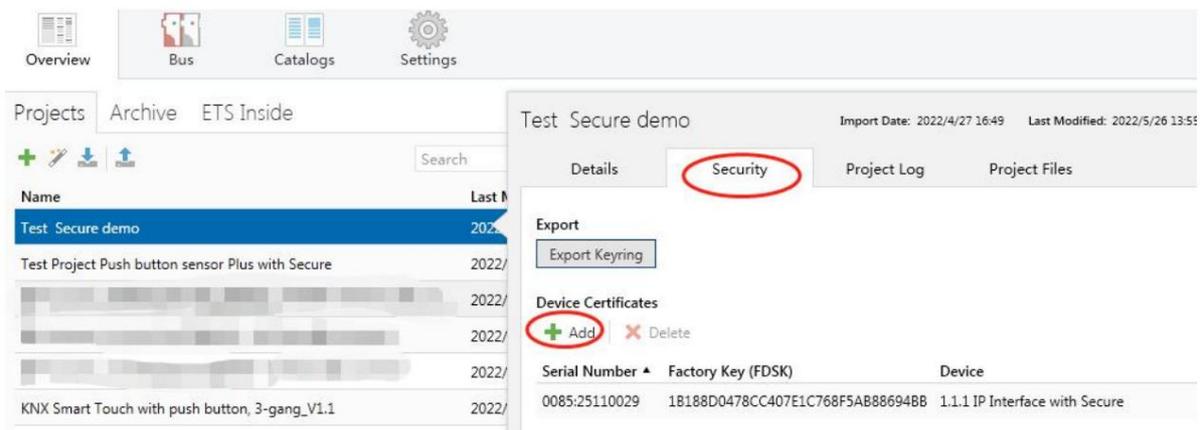


Fig. 4.3.2 Adicionar certificado de dispositivo na visão geral

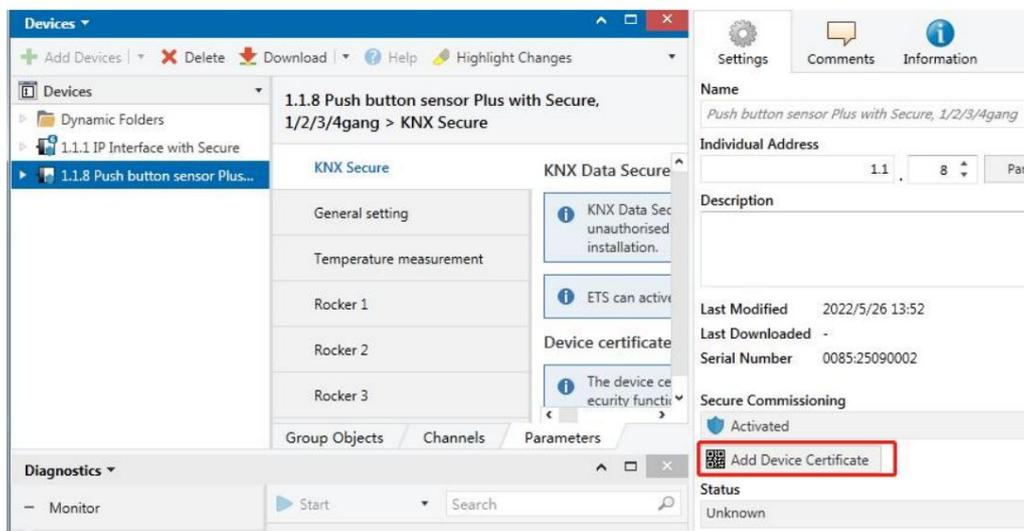


Fig. 4.3.3 Adicionar certificado de dispositivo no projeto

Dois adesivos FDSK são aplicados no dispositivo. Um deles pode ser usado para o projeto documentação, e o outro pode permanecer no dispositivo.

Sem o FDSK, não será mais possível operar o dispositivo no modo KNX Secure

após uma reinicialização.

O FDSK é necessário apenas para o comissionamento inicial. Depois de inserir o FDSK inicial, o ETS atribuir uma nova chave, conforme mostrado na Figura 4.3.4 abaixo.

O FDSK será necessário novamente apenas se o dispositivo tiver sido redefinido para as configurações de fábrica (por exemplo, se o dispositivo deve ser usado em um projeto ETS diferente).



Fig. 4.3.4 Janela Adicionar certificado de dispositivo

Exemplo:

Se este aplicativo do projeto precisar ser testado em outro dispositivo, ele não é mais o original dispositivo. Quando o aplicativo for baixado para um novo dispositivo, o seguinte prompt aparecerá à esquerda da figura 4.3.5, clique em sim, a janela Add Device Certificate aparecerá, então digite o FDSK inicial do novo dispositivo e você precisa redefinir o dispositivo para as configurações de fábrica (não é necessário se o dispositivo ainda estiver padrão de fábrica; Se tiver sido usado, será necessário redefinir, caso contrário, a seguinte mensagem de erro será aparecerem à direita da figura 4.3.5) e, em seguida, o dispositivo pode ser baixado com sucesso novamente.

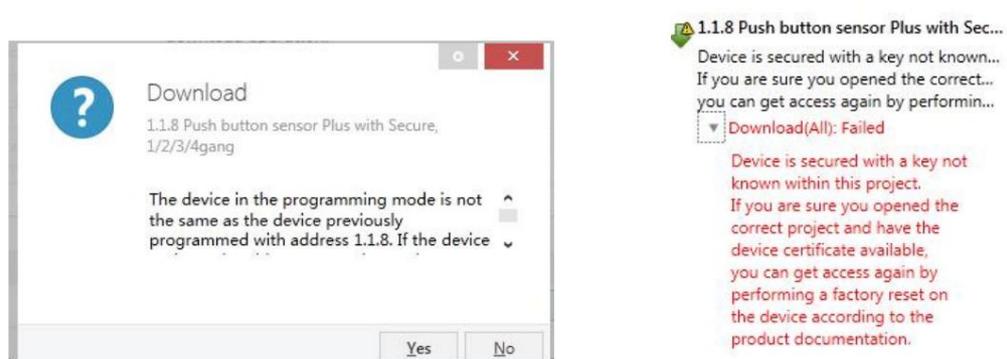


Fig. 4.3.5 Exemplo

Se o dispositivo for substituído no mesmo projeto ou se o dispositivo for substituído em um projeto diferente, o processamento é semelhante: **Redefina o dispositivo para as configurações de fábrica e reatribua o FDSK.**

Depois que o dispositivo for baixado com sucesso, o rótulo Adicionar certificado de dispositivo ficará cinza, indicando que a chave para este dispositivo foi atribuída com sucesso, conforme mostrado na Figura 4.3.6 abaixo.



Fig. 4.3.6

O ETS gera e gerencia as chaves:

Chaves e senhas podem ser exportadas conforme necessário para o uso de chaves de segurança fora do projetos ETS associados, por exemplo, se um cliente quiser acessar um dos túneis. Conforme mostrado na Figura 4.3.7 abaixo, a extensão do arquivo é .knxkeys.

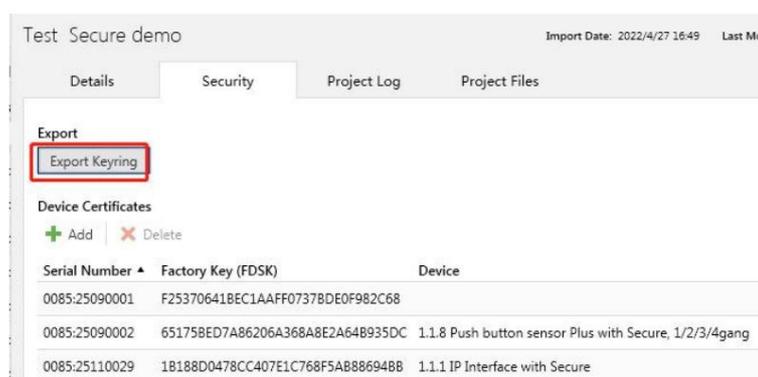


Fig. 4.3.7

ETS com exemplo de conexão IP:

Todo o processo é mostrado na Figura 4.3.8 abaixo. Selecione o dispositivo de interface IP, selecione um dos Tunelamento (como endereço físico 1.1.2), clique em "Test", a senha de comissionamento e a janela de entrada do código de autenticação aparecerá (a senha e o código de autenticação podem ser visualizados em a janela de propriedades do dispositivo no projeto), insira a senha e o código de autenticação. Após clicar em "OK", a palavra Ok aparecerá ao lado do botão "Testar" e, em seguida, clique em "Selecionar" para conectar.

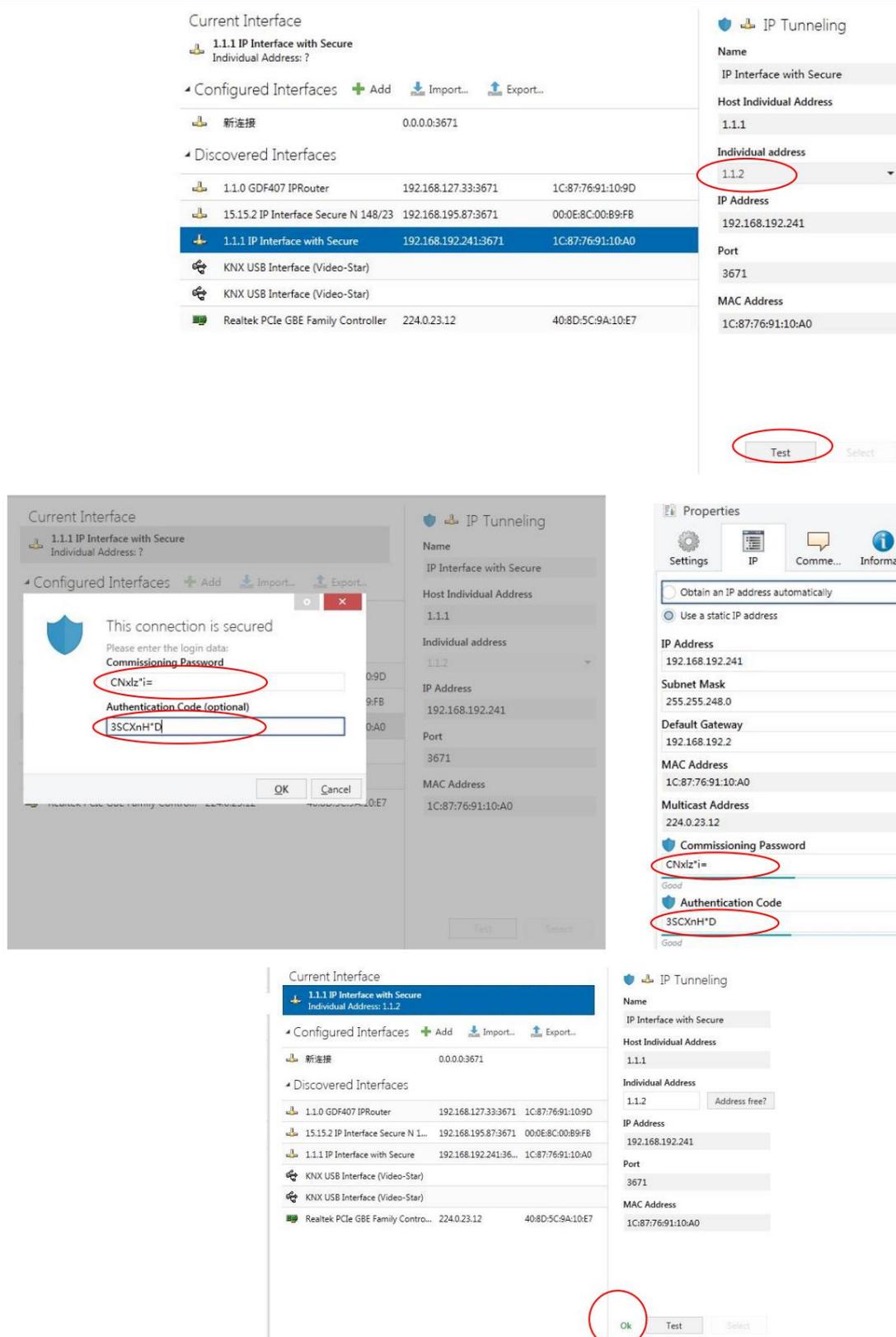


Fig. 4.3.8 Conexão de túnel IP

Na Figura 4.3.8, se o Secure Tunneling não estiver ativado, a senha de comissionamento e o código de autenticação não é necessário quando o dispositivo está conectado como uma interface; se túnel seguro

estiver ativado, o ETS solicitará que você insira a senha de comissionamento e o código de autenticação quando conectando.

A Interface IP pode ser redefinida para as configurações de fábrica, se necessário, consulte o capítulo 5, Configuração de fábrica

Nota: Qualquer interface USB usada para programar um dispositivo KNX Secure deve suportar “long quadros”. Caso contrário, o ETS reportará uma informação de falha de download, conforme mostrado abaixo.



Fig. 4.3.9

4.4. Descarregando o dispositivo

O dispositivo pode ser redefinido para as configurações de fábrica. Este é um dispositivo seguro, portanto, as informações a seguir deve ser observado:

Quando o dispositivo é operado no modo KNX Secure, ele pode ser redefinido através do ETS somente se o ETS usar o projeto com o qual o dispositivo foi parametrizado ou se a chave de comissionamento está disponível no projeto.

O dispositivo pode ser descarregado clicando com o botão direito do mouse no ETS.

Descarregando o aplicativo:

• O endereço IP e a configuração IP serão mantidos

• As senhas dos servidores de encapsulamento serão excluídas. Não será necessário entrar no senha de comissionamento e código de autenticação ao conectar (se houver o pop-up janela, está vazia)

• A chave atribuída pelo ETS será mantida. Em outras palavras, o FDSK não será necessário para reprogramando

• O endereço físico será mantido

Descarregando o endereço físico e o aplicativo

• O dispositivo será redefinido para o estado de fábrica

• O FDSK será necessário para o recomissionamento, a menos que ainda esteja disponível no projeto ETS do processo de comissionamento original

4.5. Ler informações do dispositivo

A leitura das informações do dispositivo só pode ser feita no projeto do dispositivo, selecionando o

dispositivo-->clique com o botão direito do mouse-->informações-->informações do dispositivo, conforme mostrado na fig.4.5 abaixo.



Fig. 4.5 Leia as informações do dispositivo

Capítulo 5 Configuração de fábrica

A Interface IP é entregue com as seguintes configurações padrão de fábrica:

Endereço físico	15.15.254
Endereços de tunelamento	15.15.241
	15.15.242
	15.15.243
	15.15.244
	15.15.245
configuração de IP	
endereço de IP	192.168.2.200
máscara de sub-rede	255.255.255.0
Gateway padrão	192.168.2.1

A redefinição para as configurações de fábrica também pode ser realizada diretamente no dispositivo. A operação específica como segue:

Pressione o botão de programação e segure por 4 segundos e solte, repita a operação por 4 vezes, e o intervalo entre cada operação é inferior a 3 segundos, depois disso, a LAN, KNX e os indicadores LED de programação estão todos desligados e, em seguida, a LAN e o KNX voltam ao normal instruções e o dispositivo entra na reinicialização e, após a conclusão da reinicialização, pode ser restaurado para as configurações de fábrica.

Para obter mais informações sobre o FDSK (chave de configuração padrão de fábrica). Consulte o capítulo 4.3, KNX Secure.

Capítulo 6 Configuração da Web

A configuração da Web é normalmente usada para modificar endereços IP e nomes de dispositivos e atualizar dispositivos. **Nota: Se a segurança KNX estiver habilitada, a configuração de rede não pode ser modificada via web configuração.**

Insira o endereço IP do dispositivo no navegador da Web para entrar na interface de configuração da Web do a Interface IP, conforme mostrado na Fig.6.1 abaixo.

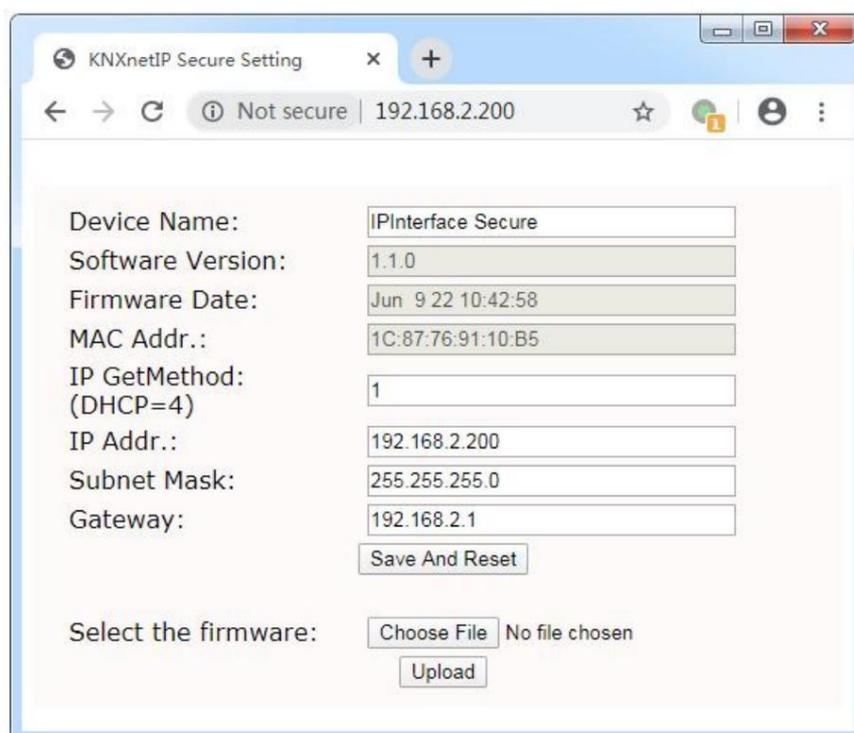


Fig.6.1 Janela de configuração da interface IP da web

• **Nome do dispositivo:** Exibe ou define o nome do dispositivo.

• **Versão do Software:** Exibe a versão do firmware (software).

• **Data do Firmware:** Exibe a data do firmware do dispositivo.

• **Endereço MAC:** Exibe o endereço MAC.

• **IP GetMethod:** O método para obter o endereço IP. Quando o valor é definido como 1, representa o IP fixo endereço. O endereço IP personalizado, a máscara de sub-rede e o gateway padrão podem ser inseridos abaixo. Quando o valor é definido como 4, o endereço IP é atribuído automaticamente através do servidor DHCP.

• **IP Addr.:** Exibe ou define o endereço IP.

• **Máscara de sub-rede:** Exibe ou define a máscara de sub-rede.

• **Gateway:** exibe ou define o gateway.

Nota: Ao usar uma configuração de endereço IP fixo, certifique-se de que cada dispositivo receba um IP diferente endereço e configurar uma máscara de sub-rede apropriada e gateway padrão, caso contrário, a web a interface de configuração não pode ser aberta mesmo se o endereço IP for inserido.

• **Salvar e redefinir:** Clique neste botão para salvar e redefinir após a conclusão das alterações de configuração. Neste momento, a página saltará para a janela conforme mostrado na Fig.6.2, indicando que o dispositivo está reiniciando. Depois de reiniciar, o página retornará automaticamente à janela de configuração.

Se o endereço IP for alterado, você precisará inserir o novo endereço IP para entrar na interface de configuração novamente.

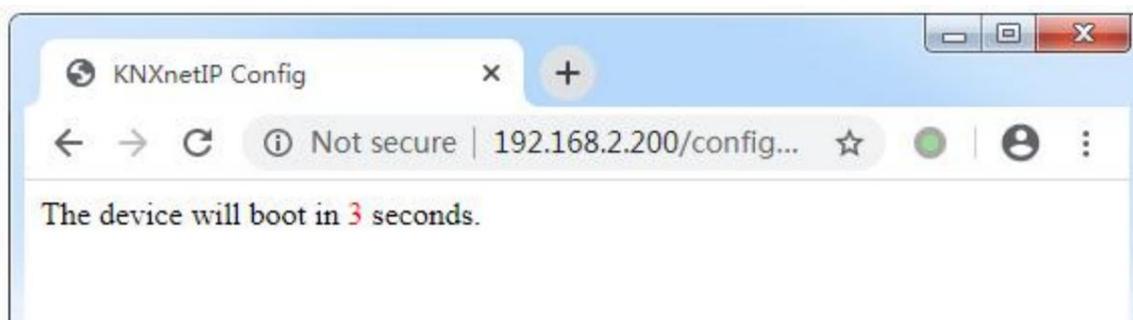


Fig. 6.2

• **Selecione o firmware:** É usado para atualizar o firmware do dispositivo. Clique no botão [Escolher arquivo] para escolha o firmware (.bin) do dispositivo atualizado e clique no botão [Upload] para atualizar o dispositivo. Figura 6.3 mostra a atualização do firmware com sucesso.

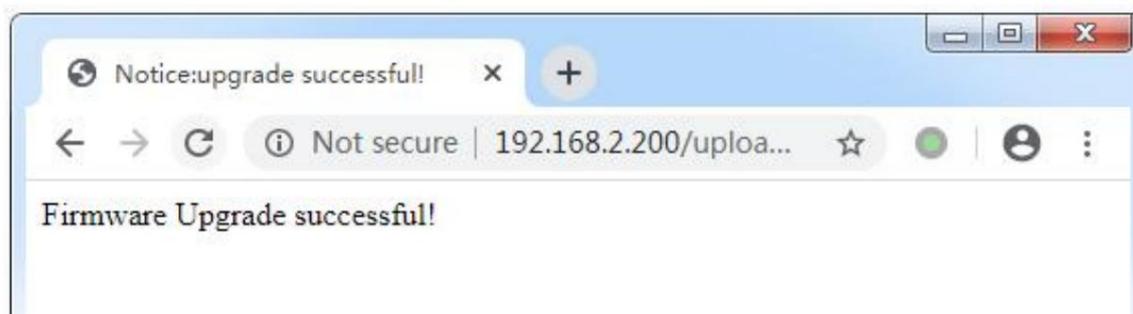


Fig. 6.3

Observação: Se o usuário não souber ou esquecer o endereço IP, redefina o endereço IP do dispositivo para o endereço padrão de 192.168.2.200 por meio da restauração da configuração de fábrica (consulte o Capítulo 5 para obter detalhes) e, em seguida, digite este endereço IP no navegador para entrar na janela de configuração web do dispositivo e alterar o IP configurações e depois salve.