Manual de Política de Segurança Cibernética

MU214004 Rev. C

30 de março de 2026

www.altus.com.br

Conforme o Código de Defesa do Consumidor vigente no Brasil, informamos, a seguir, aos clientes que utilizam nossos produtos, aspectos relacionados com a segurança de pessoas e instalações.

Os equipamentos de automação industrial fabricados pela Altus são robustos e confiáveis devido ao rígido controle de qualidade a que são submetidos. No entanto, equipamentos eletrônicos de controle industrial (controladores programáveis, comandos numéricos, etc.) podem causar danos às máquinas ou processos por eles controlados em caso de defeito em seus componentes e/ou de erros de programação ou instalação, podendo inclusive colocar em risco vidas humanas.

O usuário deve analisar as possíveis consequências destes defeitos e providenciar instalações adicionais externas de segurança que, em caso de necessidade, sirvam para preservar a segurança do sistema, principalmente nos casos da instalação inicial e de testes.

Os equipamentos fabricados pela Altus não trazem riscos ambientais diretos, não emitindo nenhum tipo de poluente durante sua utilização. No entanto, no que se refere ao descarte dos equipamentos, é importante salientar que quaisquer componentes eletrônicos incorporados em produtos contêm materiais nocivos à natureza quando descartados de forma inadequada. Recomenda-se, portanto, que quando da inutilização deste tipo de produto, o mesmo seja encaminhado para usinas de reciclagem que deem o devido tratamento para os resíduos.

É imprescindível a leitura completa dos manuais e/ou características técnicas do produto antes da instalação ou utilização do mesmo.

Os exemplos e figuras deste documento são apresentados apenas para fins ilustrativos. Devido às possíveis atualizações e melhorias que os produtos possam incorrer, a Altus não assume a responsabilidade pelo uso destes exemplos e figuras em aplicações reais. Os mesmos devem ser utilizados apenas para auxiliar na familiarização e treinamento do usuário com os produtos e suas características.

A Altus garante os seus equipamentos conforme descrito nas Condições Gerais de Fornecimento, anexada às propostas comerciais.

A Altus garante que seus equipamentos funcionam de acordo com as descrições contidas explicitamente em seus manuais e/ou características técnicas, não garantindo a satisfação de algum tipo particular de aplicação dos equipamentos.

A Altus desconsiderará qualquer outra garantia, direta ou implícita, principalmente quando se tratar de fornecimento de terceiros.

Os pedidos de informações adicionais sobre o fornecimento e/ou características dos equipamentos e serviços Altus devem ser feitos por escrito. A Altus não se responsabiliza por informações fornecidas sobre seus equipamentos sem registro formal.

Alguns produtos utilizam tecnologia EtherCAT (www.ethercat.org).

DIREITOS AUTORAIS

NOTIFICAÇÃO DE USO DE SOFTWARE ABERTO

Para obter o código fonte de componentes de software contidos neste produto que estejam sob licença GPL, LGPL, MPL, entre outras, favor entrar em contato através do e-mail opensource@altus.com.br. Adicionalmente ao código fonte, todos os termos da licença, condições de garantia e informações sobre direitos autorais podem ser disponibilizadas sob requisição.

Sumário

1. Introdução

A segurança cibernética desempenha um papel crucial no ambiente de automação industrial. Com o aumento alarmante de incidentes de segurança em fábricas, plantas e outras aplicações automatizadas, medidas efetivas para proteger esses sistemas tornaram-se imperativas. Este documento tem como propósito apresentar e justificar as medidas de cibersegurança implementadas nos produtos da Altus, notadamente o MasterTool, ambiente de desenvolvimento para controladores lógicos programáveis (CLPs), e as séries Nexto, Nexto Xpress e Hadron Xtorm.

Instituições governamentais, como a ICS-Cert e o Departamento Federal Alemão para Segurança da Informação (BSI), têm acompanhado de perto o aumento desses incidentes. Diante desse cenário, a elaboração de metodologias que assegurem a integridade e proteção dos sistemas tornou-se uma necessidade urgente. Um marco importante nesse sentido é a diretriz de padrão internacional IEC 62443, inicialmente publicada pelo comitê de segurança de sistemas de controle e automação industrial (ISA99) da Sociedade de Automação Industrial (ISA) e frequentemente referida como norma ISA/IEC 62443.

O escopo das medidas de cibersegurança abrange a proteção de vários aspectos, incluindo a disponibilidade das funcionalidades do controlador, a funcionalidade da aplicação, a confidencialidade do código fonte e da aplicação, a integridade das funções de aplicação, do sistema de desenvolvimento e dos componentes empregados, além da autenticidade do controlador e seus dados.

Neste contexto, este documento destaca as estratégias de cibersegurança adotadas pela Altus e seus produtos, visando proteger os clientes e suas operações industriais de ameaças cada vez mais sofisticadas e persistentes. O uso da norma ISA/IEC 62443 como referência sólida reflete o compromisso com a excelência na proteção do ambiente de automação industrial contra potenciais riscos cibernéticos.

Adicionalmente a adequação do produtos a norma ISA/IEC 62443, foi realizado um estudo envolvendo outro importante documento relacionado com cibersegurança, o módulo 5 do Manual de Procedimentos da Operação do ONS (Operador Nacional do Sistema). No capítulo 8, é possível encontrar a descrição de como cada requisito proposto se relaciona com os produtos Altus.

O conteúdo presente neste documento abrange as funcionalidades dos seguintes produtos: Mastertool IEC XE, NX3003, NX3004, NX3005, NX3008, NX3010, NX3020, NX3030, XP300, XP315, XP325, XP340, XP350, XP351, HX3040 e NL717.

2. Termos e Definições

2.1. Vulnerabilidades

Sistemas de automação podem sofrer ataques em diversos pontos de sua estrutura:

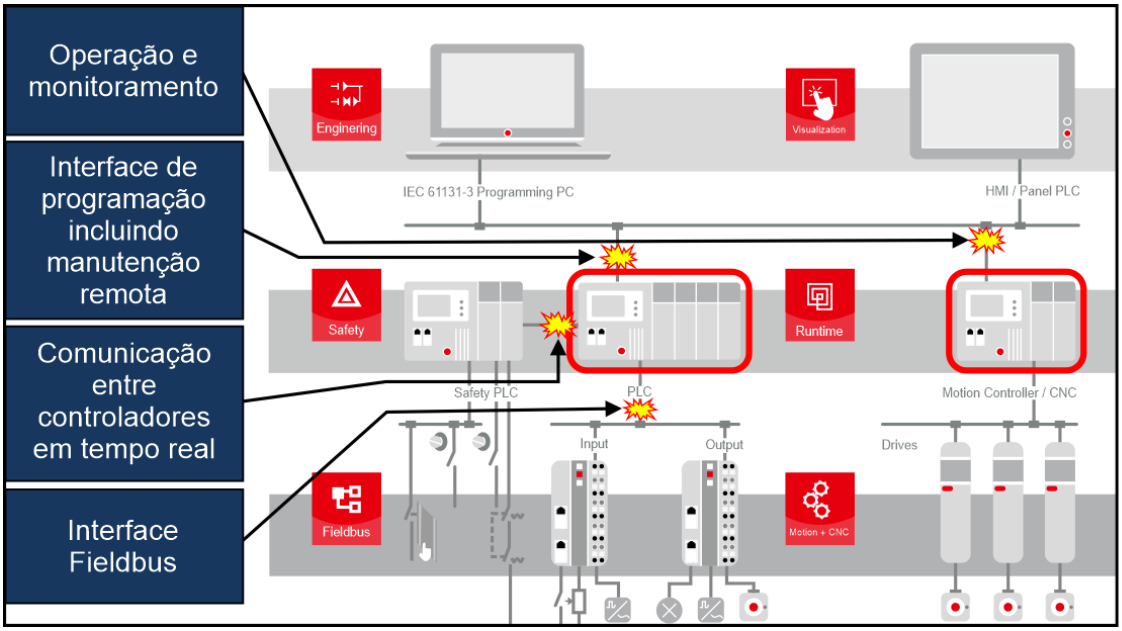


Figura 1: Possíveis vulnerabilidades de um típico sistema de automação.

2.2. Ameaça

Se refere a um conjunto de circunstâncias e sequência de eventos associados, com potencial para afetar negativamente as operações (incluindo missão, funções, imagem ou reputação), ativos, sistemas de controle ou indivíduos, através de acesso não autorizado, destruição, divulgação, modificação de dados e/ou negação de serviço. Em suma, é a possibilidade de ocorrência de eventos maliciosos ou indesejados que comprometam a integridade, confidencialidade ou disponibilidade dos recursos e informações em um ambiente de automação industrial.

2.3. Níveis de Proteção

Para atender a essa ampla abordagem, a norma ISA/IEC 62443 estabelece quatro principais níveis de proteção em escala crescente, cada um adaptado para enfrentar diferentes ameaças:

- Nível 1: Ameaças ocasionais e acidentais;
  Exemplos: Falha no disco rígido, erro operacional
- Nível 2: Ameaças intencionais por vias simples;
  Exemplo: Senha adivinhada com sucesso
- Nível 3: Ameaças intencionais por vias elaboradas;
  Exemplo: Uso de ferramental hacker
- Nível 4: Ameaças intencionais por vias elaboradas e recursos vastos.
  Exemplos: Desenvolvimento especializado, conhecimento da aplicação ou corrupção de funcionários

2.4. Controlador Programável

Um computador industrial usado na automação de sistema, que pode também ser chamado de CP ou apenas Controlador. Estes equipamentos podem ser alvos de ataques por suas características próprias e também dependem de uma programação projetada para a aplicação específica, que pode ser uma fonte de vulnerabilidades. Os controladores da Altus, tratados neste documento, são os pertencentes às linhas Nexto, Nexto Xpress ou Hadron Xtorm.

2.5. MasterTool

O MasterTool IEC XE é uma ferramenta completa para programação, depuração, configuração e simulação das aplicações do usuário. O software é baseado no conceito de ferramenta integrada, provendo flexibilidade e facilidade de uso permitindo aos usuários a programação em seis linguagens definidas pela norma IEC 61131-3: Texto Estruturado (ST), Sequenciamento Gráfico de Funções (SFC), Diagrama de Blocos Funcionais (FBD), Diagrama Ladder (LD) e Gráfico Contínuo de Funções (CFC).

2.6. Ambiente protegido

Todo sistema e equipamento precisa ser acessado durante sua instalação, operação e manutenção, porém o seu acesso não pode ser irrestrito para evitar falhas de operação e danos ao produto, intencional ou não. Para isso, é necessário que o sistema seja dividido em subsistemas para que cada subsistema tenha seu acesso controlado e apenas agentes autorizados os acessem, protegendo o ambiente.

3. Responsabilidades de diferentes agentes na segurança de sistemas industriais

Na configuração de aplicações de controle industrial, várias partes ativas e fornecedores estão envolvidos: os fornecedores de componentes de software e hardware, o integrador de sistemas ou construtor das aplicações de controle industrial e o operador. Como a segurança da tecnologia da informação é uma tarefa abrangente, todas as partes mencionadas devem realizar um esforço significativo para proteger a aplicação contra ataques.

- Fornecedor do Software:
  - analisar ativos e ameaças;
  - fornecer medidas de segurança aprovadas;
  - fornecer documentação técnica;
- Fornecedor de Componentes de Automação:
  - analisar ativos e ameaças;
  - implementar medidas de segurança de software e hardware;
  - fornecer documentação técnica;
- Integrador de Sistemas e Fabricante de Maquinário:
  - analisar ativos e ameaças;
  - implementar medidas de segurança de software e hardware;
  - implementar medidas de segurança de sistema;
  - fornecer documentação técnica;
- Operador/Gerente da Planta:
  - analisar ativos e ameaças;
  - implementar medidas de segurança de software, hardware e sistema;
  - testar, auditar e certificar sistema;
  - treinar funcionários;

4. Proteções gerais para Sistemas de Automação Industrial

Primeiramente, todas as medidas de segurança comumente conhecidas para computadores devem ser aplicadas em redes com equipamentos de automação industrial, tais como:

- Proteção contra vírus
- Senhas fortes que são regularmente alteradas
- Proteção de firewall
- Uso de túneis VPN para conexões entre redes
- Cautela ao lidar com dispositivos de armazenamento removíveis, como dispositivos de mídia USB

Além disso, é obrigatório ter um gerenciamento de usuários e permissões bem definido para o acesso aos controladores e suas redes interconectadas.

4.1. Uso em um ambiente protegido

Localizar o controlador em um ambiente protegido é absolutamente necessário para evitar acessos acidentais ou intencionais não autorizados ao controlador ou sua aplicação, que é executada para o funcionamento da máquina ou instalação.

Esse ambiente protegido pode ser, por exemplo, dentro de:

- Armários de controle elétrico trancados sem acesso de comunicação externa,
- Uma rede intranet com direitos de usuário bem definidos sem acesso externo, ou
- Uma rede com acesso à internet somente por meio de um firewall bem configurado via um túnel VPN.

Obviamente, o grau de proteção diminui ao longo desta lista.

Para criar um ambiente protegido como esse, várias regras devem ser seguidas:

- Manter a rede confiável o menor possível e independente de outras redes.
- Proteger a comunicação cruzada entre controladores e a comunicação entre controladores e dispositivos de campo por meio de protocolos de comunicação padrão (sistemas fieldbus) por medidas apropriadas.
- Bloquear essas redes e separá-las estritamente de acessos comuns.
- Usar sistemas de barramento de campo apenas em ambientes protegidos, pois eles não estão protegidos por medidas adicionais, como criptografia. O acesso físico ou de dados aberto aos sistemas de barramento de campo e seus componentes é um sério risco de segurança.

4.2. Usuários atentos à segurança

Usuários com conscientização sobre segurança desempenham um papel fundamental na proteção cibernética, visto que a maioria dos incidentes de segurança relatados ocorre sem intenção, devido a erros de manipulação ou de dispositivos. Portanto, tanto os fabricantes de máquinas e instalações quanto os operadores precisam estar cientes das possíveis ameaças e das medidas infraestruturais necessárias para evitá-las. Para alcançar esse objetivo, é recomendável aos usuários participar de treinamentos especiais ministrados por especialistas em segurança, seja dentro da empresa ou por profissionais externos. Esses treinamentos visam capacitar os usuários a adotarem práticas adequadas de segurança e a compreenderem como aplicar as medidas de proteção adequadas no desenvolvimento e operação dos controladores industriais.

5. Medidas de Segurança Presentes no MasterTool

Este capítulo informa sobre os recursos de segurança cibernética no programa MasterTool, informando sua importância e como encontrá-las nos manuais do produto. Abaixo dos títulos dos subcapítulos, são informados os requisitos de componente (RC) da norma IEC 62443-4-2:2019-02 à qual ela diz respeito.

5.1. Gerenciamento de Usuários

A configuração dos usuários e grupos (CR 1.3 da norma) é feita no diálogo *Projeto* na janela *Configurações do Projeto*. Na aba de *Usuários e Grupos*, pode ser cadastrado um usuário para cada pessoa que for trabalhar no projeto, e organizar estes usuários em grupos. Durante a criação dos usuários, as senhas não são avaliadas baseada em força, mas uma política de senhas fortes, se respeitada, atende ao requisito CR 1.7 da norma. Nesta tela, também é possível configurar o número máximo de tentativas de autenticação, atendendo ao requisito CR 1.11 da norma.

Informações mais detalhadas a respeito da utilização de cada ferramenta apresentada neste capítulo podem ser encontradas no Capítulo “Gerenciamento de Usuários e Direitos de Acesso” do Manual do Mastertool.

5.1.1. Gerenciamento de usuários nos níveis de projeto

RC 1.1, RE (1), 1.3, 1.4, 1.5, 1.7, 1.10, 1.11, 2.1, RE(1), RE(2), 2.5, 2.6 e 3.3 da norma IEC 62443-4-2

MasterTool oferece a capacidade de proteção de leitura/gravação de objetos individuais no projeto com uma administração de usuário. Essa proteção pode ser definida para comandos de menu, bem como para tipos de objeto específicos (por exemplo, criação de tarefas, POUs, métodos, GVLs etc.) ou objetos existentes no projeto (como configurações do projeto ou POUs ou tarefas dedicadas).

Através da administração de usuário, é possível limitar a gama de funcionalidades de uma forma mais profunda. Permitindo direito de acesso adaptados a necessidades de segurança específicas, protegendo assim a confidencialidade da propriedade intelectual, bem como a integridade do código do aplicativo.

O gerenciamento de usuários em um projeto somente é útil se combinado com o gerenciamento dos direitos de acesso. Em um novo projeto, basicamente todos os direitos de acesso não são definidos automaticamente, mas configurados para um valor padrão, ou seja, normalmente os direitos estão “garantidos”. Durante a execução do projeto, cada direito pode ser explicitamente garantido ou negado e configurado novamente para o padrão. O gerenciamento dos direitos de acesso é feito no diálogo *Permissões* ou - para os direitos de acesso aos objetos - no diálogo *Controle de Acesso* (que faz parte do diálogo *Propriedades do Objeto*).

Depois do acesso a alguma função ser restrito ao grupo *Everyone*, para acessá-lo é necessário realizar login em algum usuário com permissão de acesso. Durante o login, os caracteres da senha são ocultados por asteriscos.

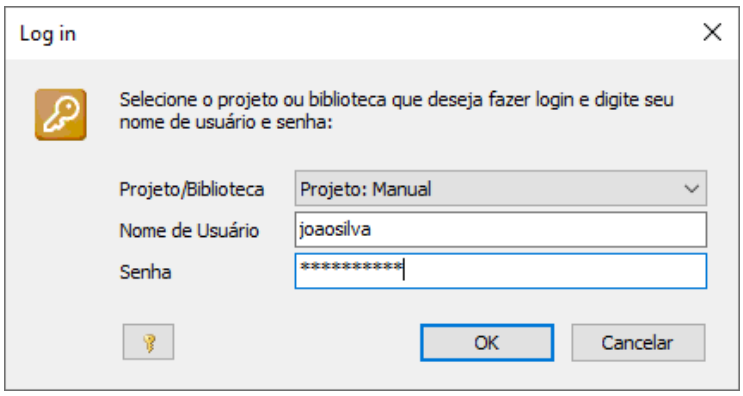


Figura 2: Tela de login.

Criando Usuários e Adicionando-os a Grupos

Em *Projeto* > *Configurações do Projeto* > *Usuários e Grupos* > *Usuários* > *Adicionar...* é possível adicionar um novo usuário ao projeto. Nesse mesmo menu, pode-se anexá-lo a um grupo, desta forma, todas as configurações do grupo serão aplicadas a este novo usuário. A partir dos grupos, pode-se definir as permissões daqueles usuários dentro do projeto. O usuário é unicamente identificado pelo seu *Nome de Login*.

A força das senhas utilizadas não é avaliada pelo software, mas ter e reforçar uma norma interna pode assegurar a segurança dos usuários para atender ao item 1.7 da norma.

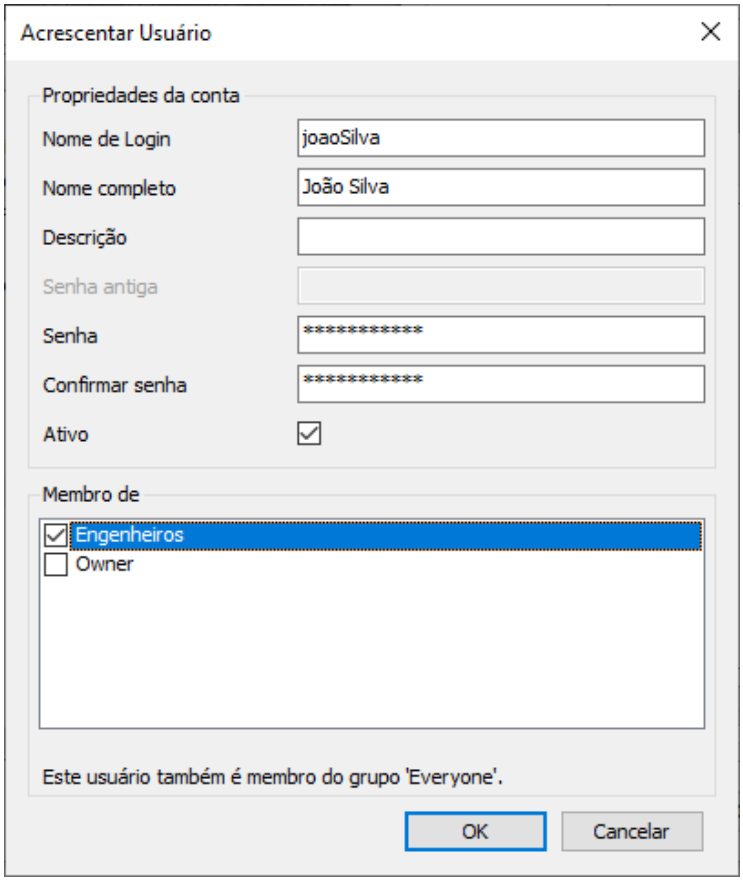


Figura 3: Criação de novo usuário.

A criação dos usuários, deve ser feita por um usuário do grupo *Owner*. No Mastertool, o projeto é iniciado com um usuário Owner que, por padrão, vem com senha vazia.

Gestão de usuários

É possível, através do Gerenciador de Usuários, definir o nível de acesso de usuário e fazer alterações, além de incluí-lo em grupos definidos pelo administrador. Para garantir nível de acesso a determinado usuário, deve-se adicioná-lo a um grupo que, por sua vez, terá diferentes níveis de acesso. Dessa forma, se o usuário tentar realizar uma operação no projeto que dependa de autorização, o Mastertool pedirá credenciais autorizadas para confirmar o acesso ou alteração.

No Mastertool, o usuário administrador é o Owner que, por padrão, vem com senha vazia. Dessa forma, para fazer login neste usuário deve-se acessar *Projeto* > *Gerenciamento de Usuário* > *Login do Usuário...* . Apenas usuários do grupo *Owner* podem adicionar ou editar as configurações de usuários e grupos, assim como editar as senhas de usuários.

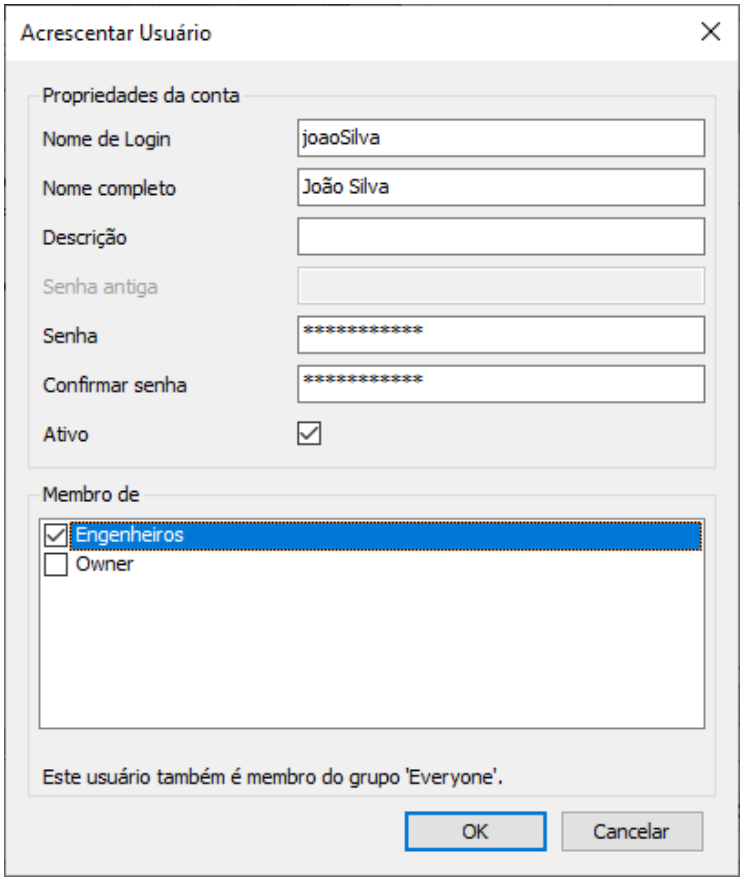


Figura 4: Criação de novo usuário.

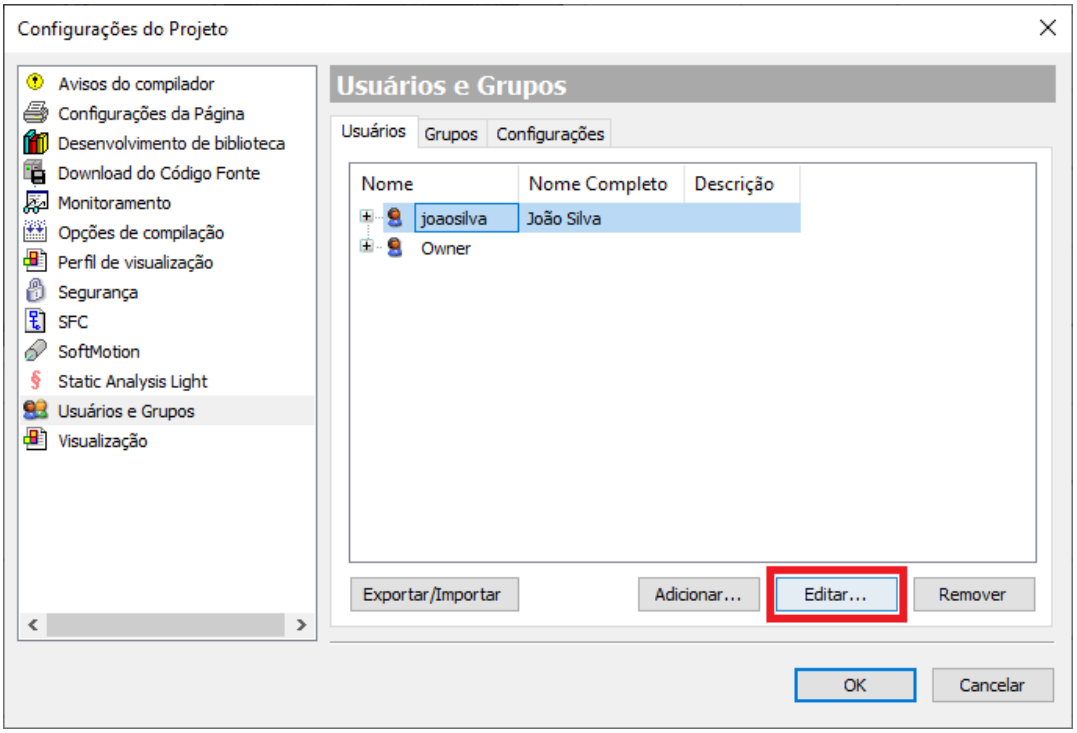


Figura 5: Botão de edição de usuário.

A ativação do usuário também ocorre na tela de edição, ao clicar na caixa de seleção *Ativo*. O usuário pode se encontrar desativado por configuração ou por ter excedido o limite de tentativas login. Esta configuração deve ser feita por um administrador do sistema.

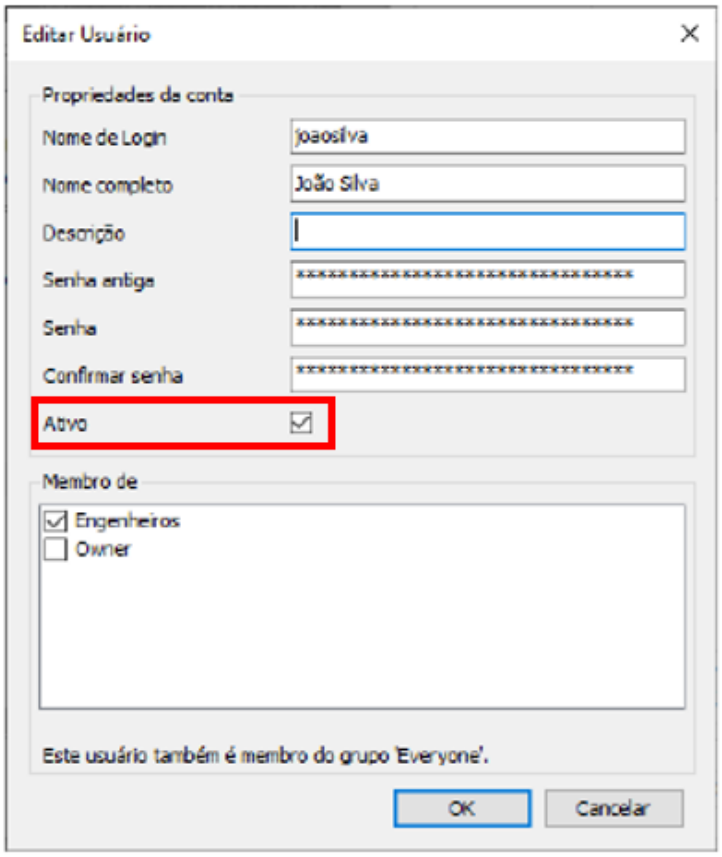


Figura 6: Edição de usuário.

Uma vez logado em Owner, crie um grupo em *Projeto* > *Configurações do Projeto* > *Usuários e Grupos* > *Grupos* > *Adicionar...*

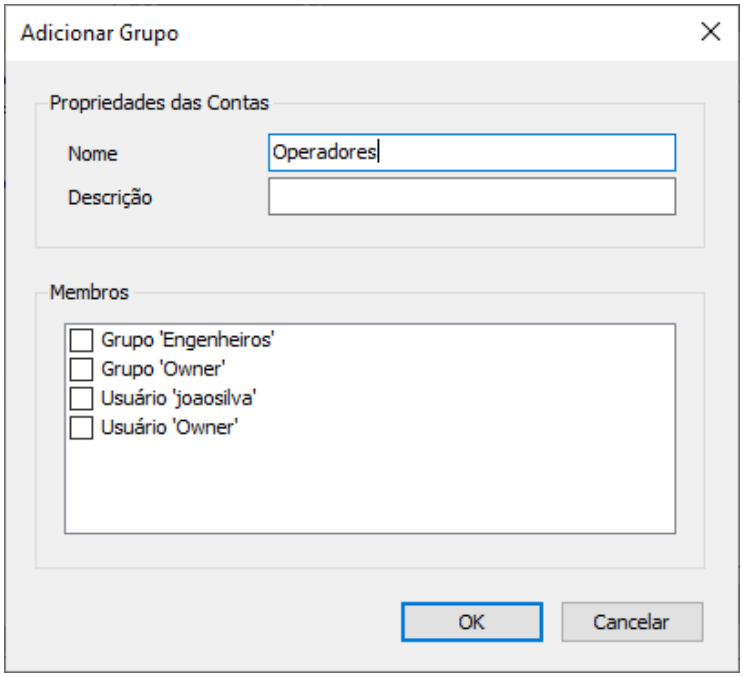


Figura 7: Adição de grupos.

Para verificar as permissões do projeto para determinado grupo de usuários, deve-se acessar *Projeto* > *Gerenciamento de Usuário* > *Permissões*. Neste menu é possível conceder e remover permissões a usuários. Dentro das pastas, estão contidos todos os comandos referentes a permissões do projeto. Ao clicar em cima de algum deles, uma aba é aberta na direita da tela, possibilitando permitir ou negar aquele comando aos grupos cadastrados no projeto.

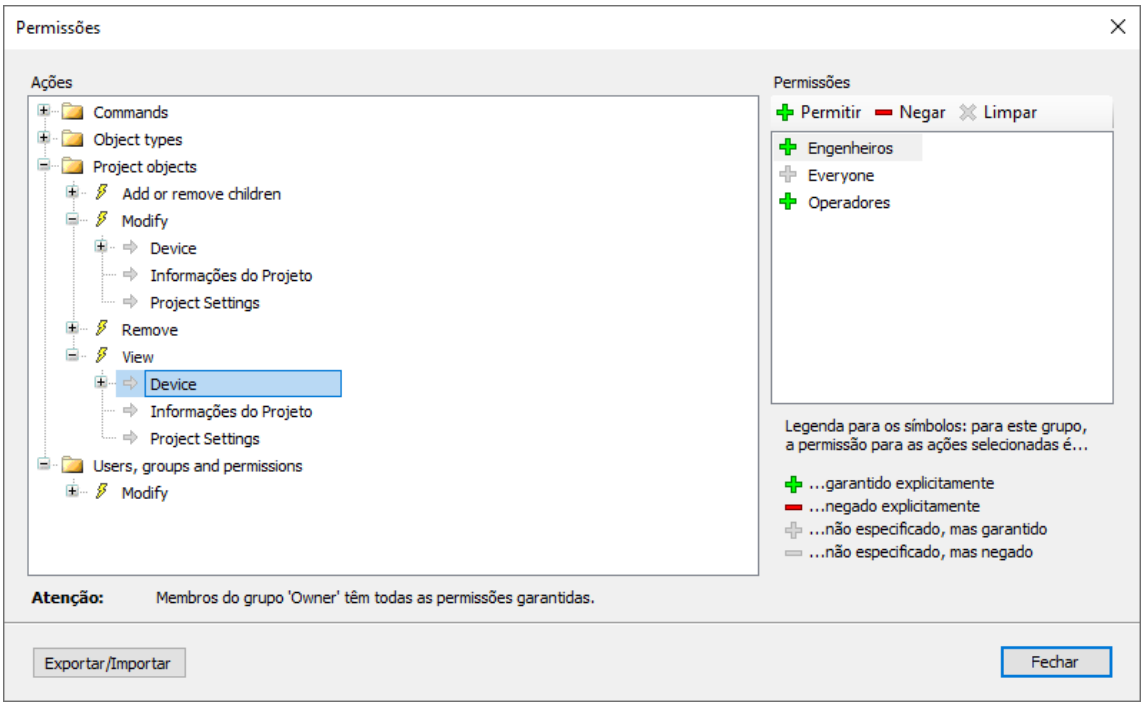


Figura 8: Tela de permissões por grupo.

Configurando opções de login

Para evitar ataques de força bruta por tentativas de logins, através do menu *Projeto* > *Configurações do projeto* > *Usuários e Grupos* > *Configurações* é possível configurar o número máximo de tentativas de autenticação. Caso esse limite seja ultrapassado, o usuário é desativado e permanecerá assim até algum administrador ativá-lo novamente. Na seção *Gestão de Usuário*, do capítulo 5.1.1 é indicado como ativar um usuário.

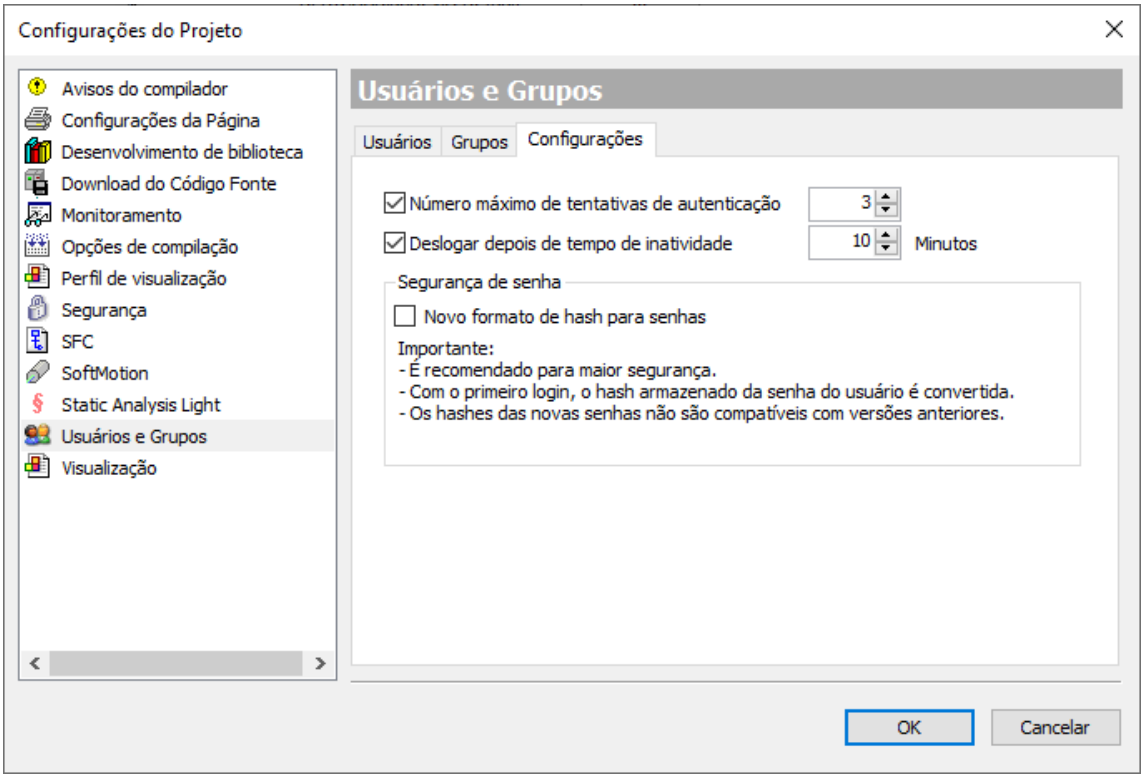


Figura 9: Tela de Configuração de Usuários e Grupos.

Na mesma tela é possível determinar um tempo máximo que o usuário pode ficar inativo logado no projeto até que tenha que realizar o login novamente. Esta configuração também vale para acessos remotos aos dispositivos.

Verificação da identificação e controle de uso ao tentar acesso com uma conta sem autorização

Para verificar que um usuário sem autorização não consegue acessar o projeto, pode-se acessar Projeto > *Gerenciamento de Usuário* > *Login do usuário* e inserir os dados de um usuário que não existe. A seguinte mensagem deve aparecer na tela.

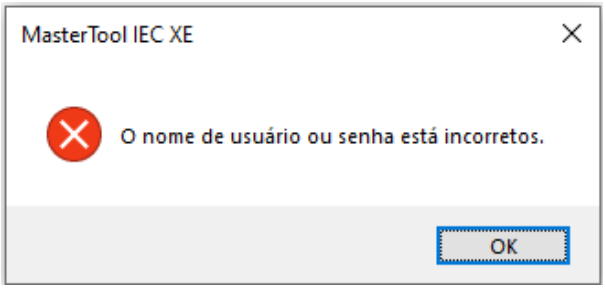


Figura 10: Mensagem de erro ao inserir credenciais inválidas.

5.1.2. Gerenciamento de Usuários da Visualização Integrada
RC 2.1 da norma IEC 62443-4-2

A visualização integrada do MasterTool permite uma operação direta do controlador e da aplicação. Recomenda-se fortemente separar a operação em diferentes partes ou telas de acordo com seu nível de influência funcional e de segurança. O MasterTool fornece a capacidade de proteger elementos de visualização individuais, bem como telas de visualização inteiras do projeto por meio de um gerenciamento de usuário de visualização especial.

Este gerenciamento de usuários permite a limitação do alcance de funcionalidade para determinados operadores. Modos de operação de segurança crítica, como a exportação de dados de produção, o processo de inicialização e parada da planta, e o acesso a funções de serviço dedicadas, pode ser restrito a operadores com permissões explicitamente atribuídas, garantindo sigilo da propriedade intelectual, bem como a disponibilidade e confiabilidade da máquina ou processo da planta.

5.2. Configuração do IP do CLP
RC 1.2 da norma IEC 62443-4-2

A funcionalidade *Easy Connection* permite fazer um scan em todos os PLCs conectados na mesma rede.

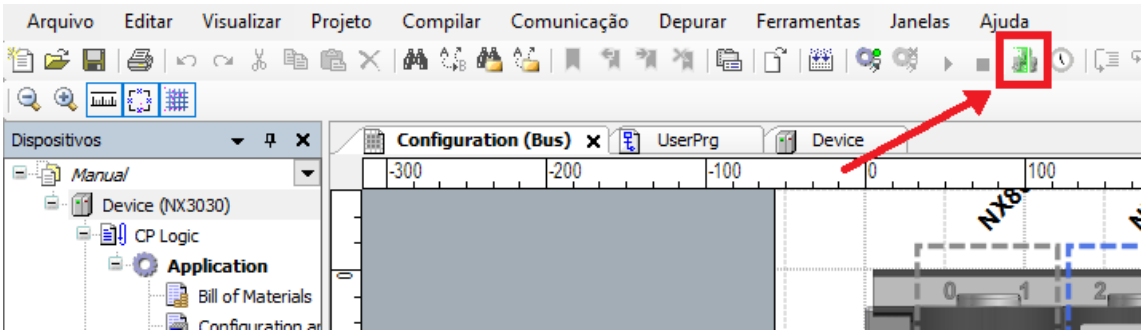


Figura 11: Botão do Easy Connection.

Após o scan, uma lista com os PLCs conectados irá aparecer. Por meio dela, é possível fazer a identificação da peça a partir do IP ou ao clicar em *Identificar dispositivo*. Ao utilizar o *Identificar dispositivo*, o LED DG do PLC começará a piscar rapidamente sendo possível garantir fisicamente qual é o PLC antes de realizar o login.

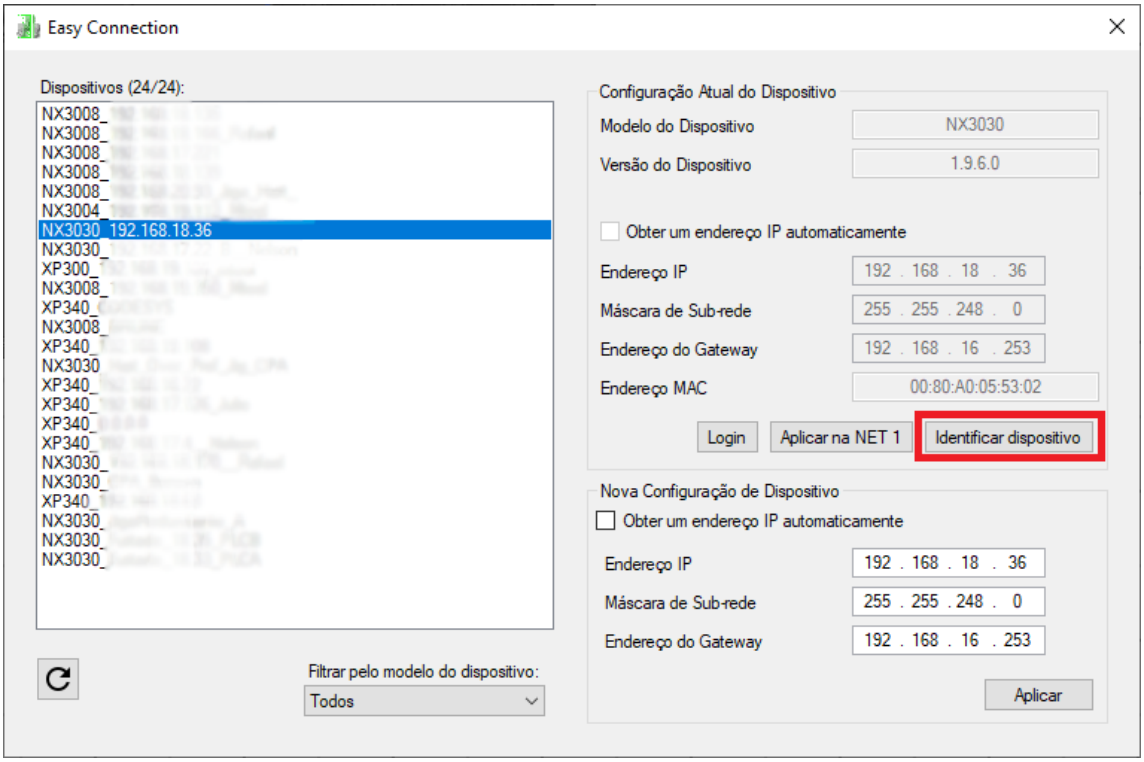


Figura 12: Easy Connection.

Para um controlador da série NX da Altus, outra forma de verificar o endereço de IP é por meio do botão na sua parte superior, que mostra diferentes informações de diagnóstico na tela, incluindo o endereço de IP.

Para alterar o IP do dispositivo, configure o novo endereço, subrede e gateway na interface *NET (1, 2 ou 3)*, e depois fazer o *Login* no dispositivo, com o IP atual que está sendo utilizado na comunicação com o computador ainda configurado nas propriedades do *Device*.

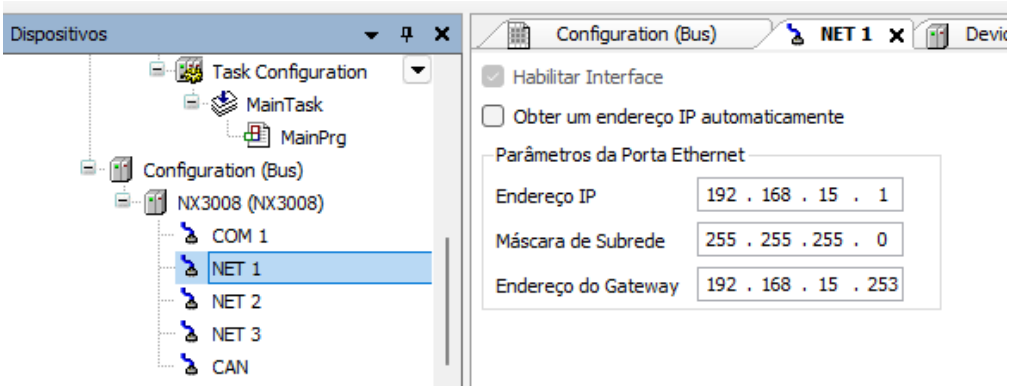


Figura 13: Alteração de configurações de rede pelo Mastertool.

Outra forma de editar as configurações de rede é pela interface Web do dispositivo, descrito na Seção 6.5.2.

5.3. Encriptação da Comunicação com WebVisu

RC 3.1 da norma IEC 62443-4-2

Para prevenir a interceptação da comunicação entre o controlador e o navegador web no computador, é possível utilizar uma conexão com encriptação HTTPS. Esta pode ser configurada com certificado auto-assinado ou com um gerado por uma

autoridade certificadora CA. Na tela de Device Security Settings, o uso de HTTPS pode ser configurado como obrigatório, ou permitir também conexões HTTP.

Esta funcionalidade está implementada no menu *Device* > *Configurações de comunicação* > *Dispositivo* > *Configurações de Segurança...*.

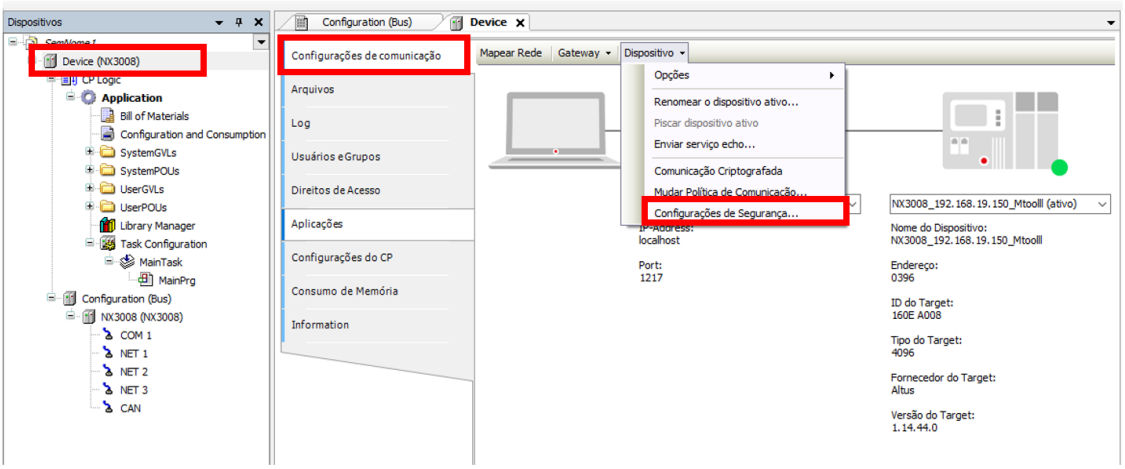


Figura 14: Configurações de Segurança

A opção *CommunicationMode* permite selecionar o protocolo de comunicação do Webvisu.

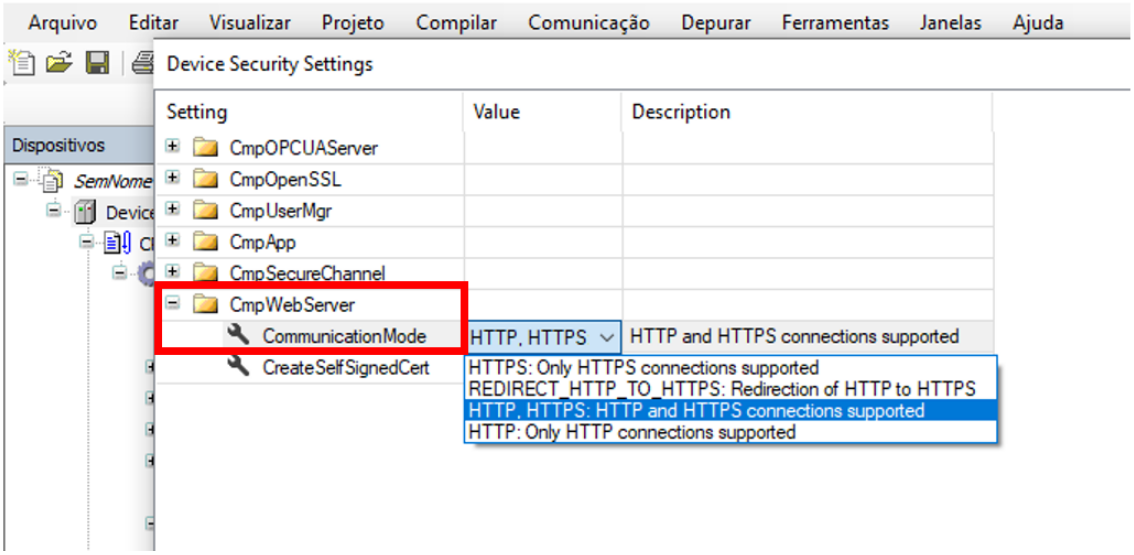


Figura 15: Protocolo de comunicação do Webvisu

5.4. Tela de Segurança

RC 1.8, 4.1, 4.3 da norma IEC 62443-4-2

A tela de segurança gerencia os certificados X.509, nos escopos de projeto e dispositivo, e os níveis de segurança do projeto. Ela pode ser acessada em *Visualizar* > *Tela de Segurança*.

Na aba "Usuário", é possível gerenciar o perfil e seus respectivos certificados para assinatura e decriptação de arquivos. Também é possível gerenciar o nível de segurança do projeto, forçando features como comunicação encriptada, encriptação de arquivos, assinatura de arquivos, assinatura de bibliotecas compiladas, entre outras.

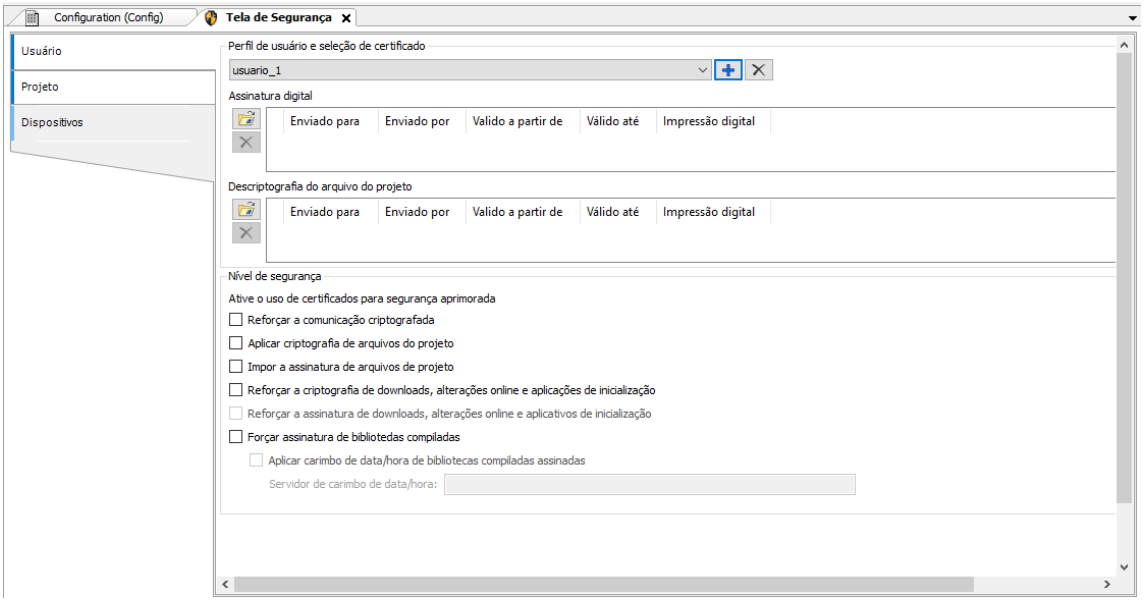


Figura 16: Aba de usuário da tela de segurança.

Na aba "Projeto", é possível selecionar o tipo de criptografia utilizada nos arquivos dos projetos, assim como os certificados dos usuários com acesso aos mesmos. Também é possível encriptar a aplicação de boot, assim como o download e as mudanças online. Na aba "Dispositivos", você pode configurar a encriptação da comunicação OPC UA utilizando o perfil Basic256SHA256, para uma conexão segura.

Funcionalidades como Assinatura de bibliotecas IEC Compiladas, Encriptação do código fonte da aplicação, e Métodos de proteção do projeto podem ser vistas em seus respectivos capítulos.

Para gerar um novo certificado veja o apêndice Gerenciamento de Certificados e Chaves TLS.

5.5. Assinatura de bibliotecas IEC Compiladas

RC 4.1 da norma IEC 62443-4-2

Uma biblioteca IEC pode ser assinada com um certificado X.509 se for salva como uma biblioteca compilada. Enquanto as bibliotecas compiladas garantem a proteção do código-fonte, a assinatura permite uma verificação da autenticidade da mesma.

O status das assinaturas das bibliotecas pode ser observado pelos ícones no *Gerenciar de Biblioteca* ou pelos Detalhes no menu de *Adicionar a biblioteca*.

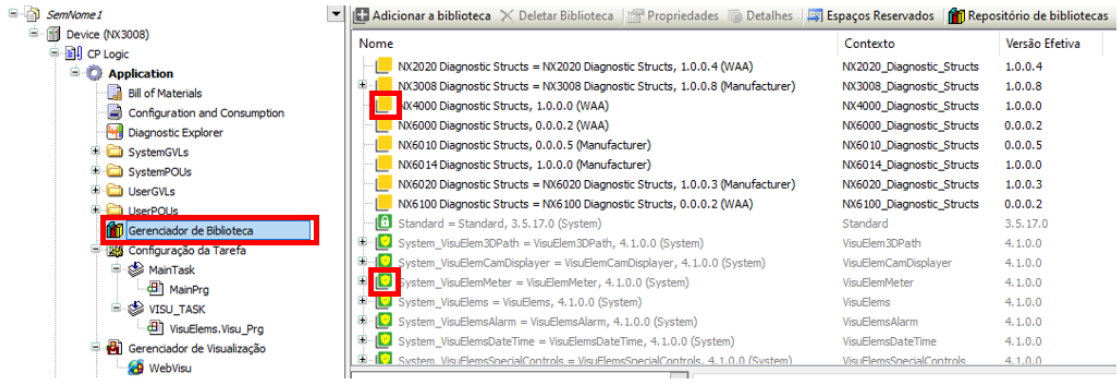


Figura 17: Bibliotecas assinadas e compiladas

O ícone em verde indica que aquela é uma biblioteca assinada por um certificado confiável. Caso o ícone seja amarela, significa que não é uma biblioteca assinada.

5.6. Encriptação do código fonte da aplicação

RC 4.1 da norma IEC 62443-4-2

O código-fonte da aplicação contém as informações detalhadas sobre o sistema abordado e, portanto, a propriedade intelectual de seu fabricante. Dessa forma, a proteção do código-fonte da aplicação é prioritário na presença de informações confidenciais.

O MasterTool permite para todo o projeto a criptografia por senhas ou chaves de segurança físicas tipo USB Dongle. Descrito na norma IEC 62443-4-2 em "Requisito de componente 4.3", a criptografia de senha é baseada nos métodos AES (Advanced Encryption Standard), já as soluções embasadas em chaves de seguranças são fornecidas pela empresa WIBU Systems. A utilização de senhas tem como principal vantagem dispensar um hardware adicional, porém, a utilização das chaves tornam o nível de proteção muito maior, uma vez que uma senha pode ser hackeada ou publicada.

Possibilita-se também o vínculo de várias chaves diferentes ao mesmo tempo a um projeto, limitando o acesso do código-fonte ao número de chaves e minimizando o risco à privação de acesso ao código, caso alguma chave seja destruída ou perdida. Para esse fim, recomenda-se a associação de uma chave a mais do que o que seria necessário.

O código-fonte também pode ser protegido usando certificados X.509. Nesse cenário, o código-fonte será criptografado simetricamente (algoritmo AES). A chave simétrica será então criptografada assimétricamente (algoritmo RSA) usando a chave pública de cada usuário que compartilha o código-fonte. Opcionalmente, o código-fonte também pode ser assinado digitalmente usando a chave privada associada ao certificado X.509 do usuário atual. A assinatura será salva lado a lado com o código-fonte em um arquivo com o extensão ".p7s" seguindo o formato PKCS #7 para assinaturas digitais.

Caso não seja possível utilizar criptografia, é estabelecido que o arquivo do projeto é salvo em um formato proprietário e sua integridade será verificada cada vez que o projeto é carregado, protegendo o sigilo da propriedade intelectual.

A seção 5.13 descreve com mais detalhes a configuração de criptografia no projeto.

5.7. Logs

RC 2.8, 2.9, RE(1), 2.11, RE(1), RE(2), 2.12, 3.3 da norma IEC 62443-4-2

Logs são fornecidos e podem identificar erros, falhas, advertências, informações do projeto e ações tomadas por usuários.

Para verificar os logs do dispositivo conectado, deve-se abrir o *Device* pela treeview do projeto. Em seguida, clicar em *Log*, no menu lateral da janela de *Device*.

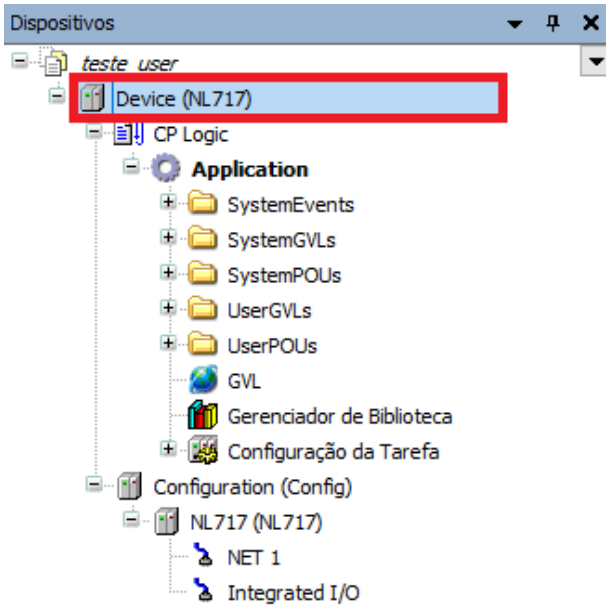


Figura 18: Treeview do projeto.

Através de cartões SDs, é possivel salvar os logs do sistema e caso haja preenchimento total, é notificado. Os logs do dispositivo são armazenados na memória interna. É possível exportar um arquivo contendo todos os registros, dessa forma, podendo ser salvo em qualquer outro lugar que o usuário desejar.

Para realizar a exportação, acessar os logs do dispositivo e clicar no ícone marcado na imagem abaixo.

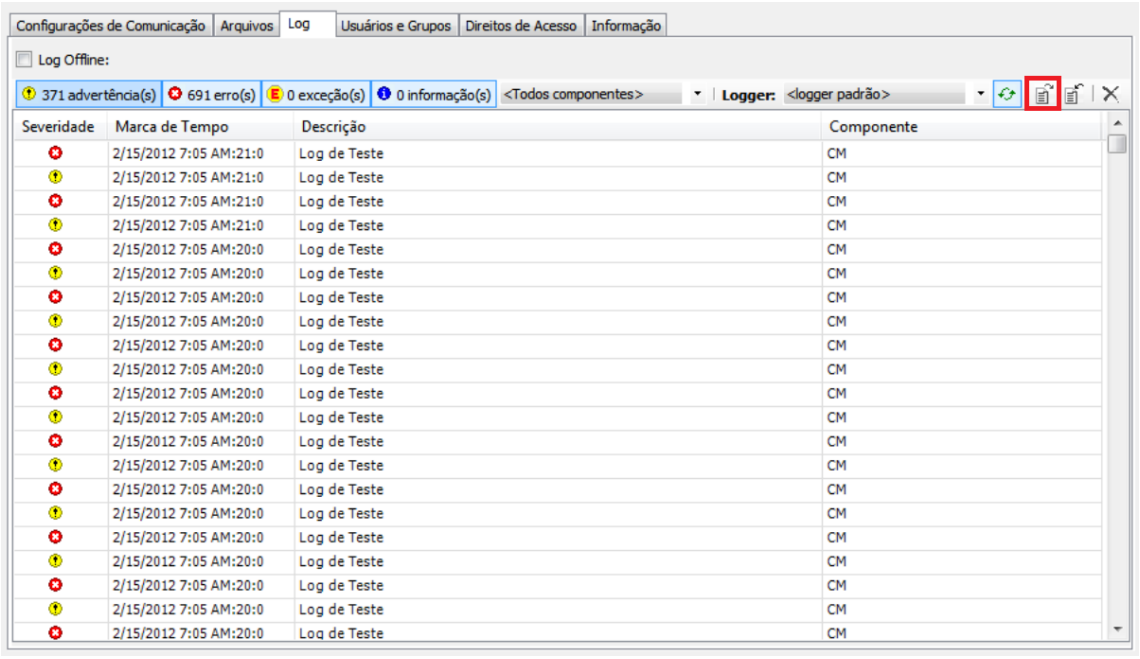


Figura 19: Tela de logs.

A assinatura de tempo do RTC do dispositivo é informada para cada log, e o RTC do dispositivo pode ser configurado pelo botão de *Configuração de Relógio*, ao lado do *Easy Connection*.

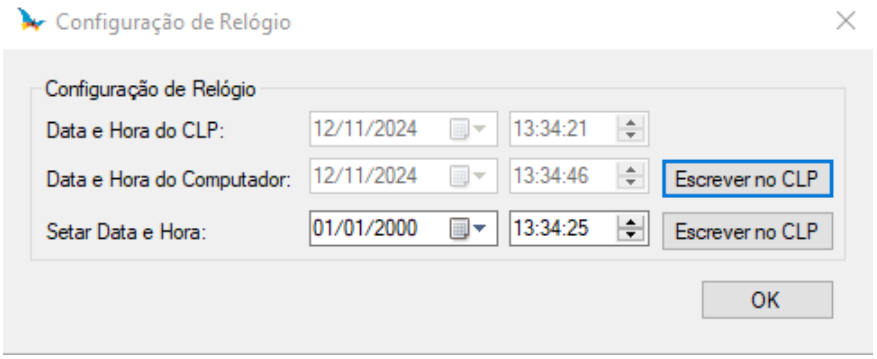


Figura 20: Configuração de relógio.

Os logs são salvos de forma circular, ou seja, uma vez que é atingido o limite de memória disponível, os registros mais antigos começam a ser sobrescritos.

Proteção das funções de configuração do RTC

A proteção das funções de configuração do RTC podem ser feitas através do gerenciamento de acesso a biblioteca de configuração do mesmo. É possível bloquear a mudança das configurações de RTC a partir do menu *Device*. Primeiramente, deve-se criar um grupo e adicionar a esse grupo, um usuário.

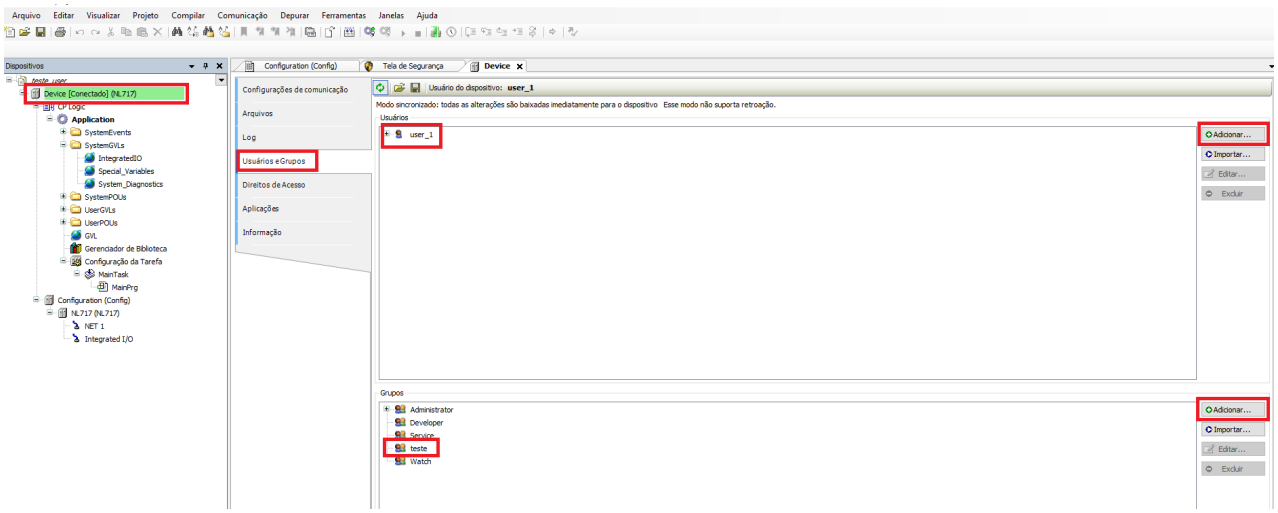


Figura 21: Adicionando um usuário ao dispositivo.

Na página *Direitos de acesso*, é onde se garante ou nega a execução de determinadas ações aos usuários cadastrados. Para bloquear mudança nas configurações do RTC, deve-se negar a modificação do parâmetro *Application* para o grupo desejado, como destacado na imagem.

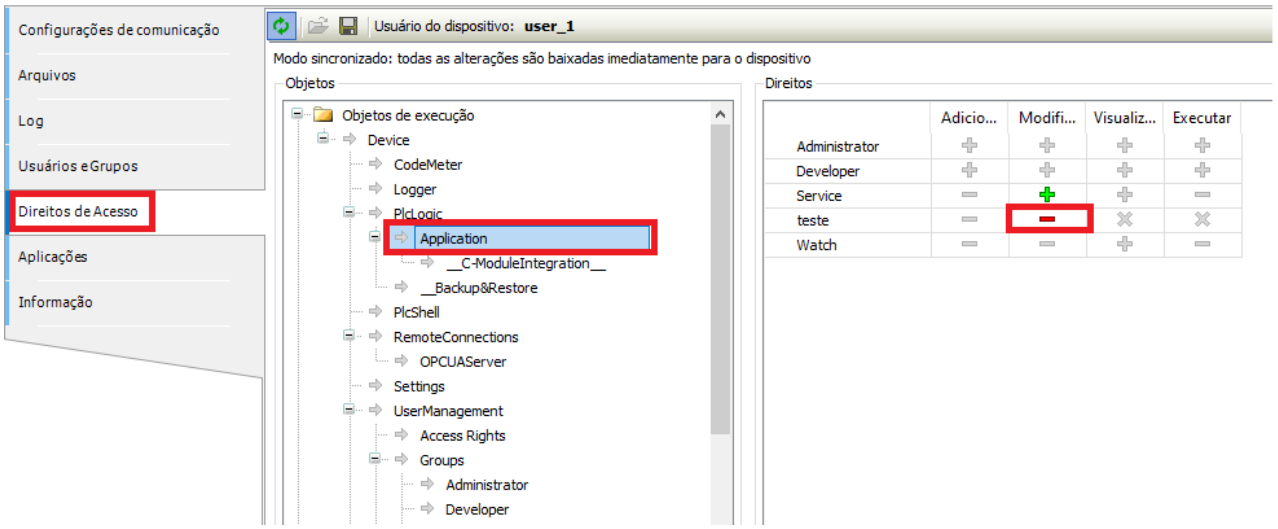


Figura 22: Configurando direitos de acesso no dispositivo.

Confirmação de que os logs do dispositivo continuam sendo salvos

Pode-se confirmar que os logs do dispositivo continuam ocorrendo ao acessar *Device* > *Log* e verificar a entrada de dados atualizados na lista. Uma forma de forçar ocorrências é realizar login no PLC, dessa forma ira ser apresentada a mensagem "*User logged in*" no topo da lista.

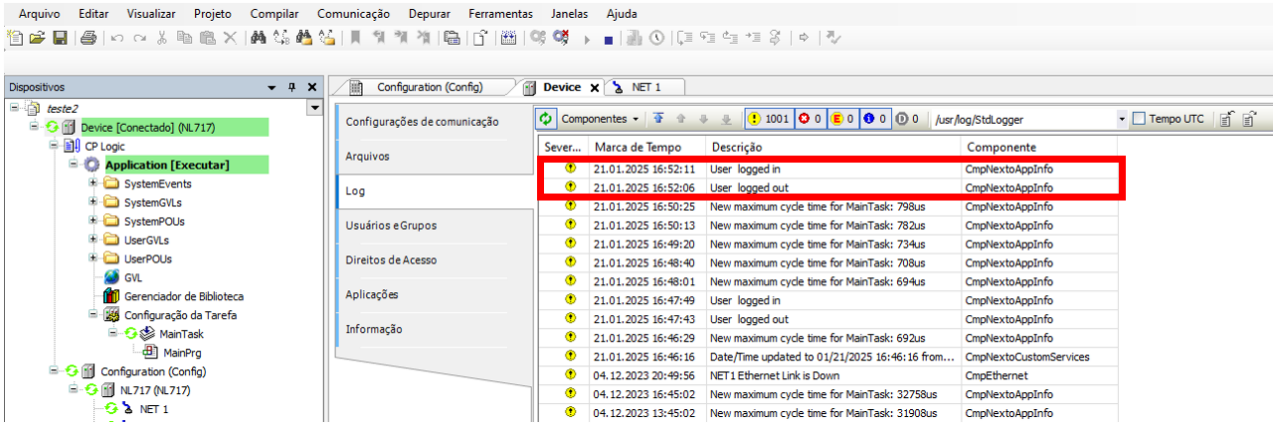


Figura 23: Demonstração dos logs sendo salvos.

5.8. Saídas Predeterminadas

RC 3.6 da norma IEC 62443-4-2

Dentro do Mastertool, é possível configurar o comportamento das saídas do componente após mau funcionamento ou falha. Isto é feito no menu *Device* > *Configurações do CP* na opção *Comportamento para saídas em STOP*.

- Manter os valores atuais: Os valores atuais são mantidos.
- Configurar todas as saídas para o padrão: Os valores padrão derivados do mapeamento de I/O são atribuídos.
- Executar programa: O gerenciamento dos valores de saída é regido por um programa incluído no projeto, que é executado no modo STOP. Insira o nome do programa no campo à direita.

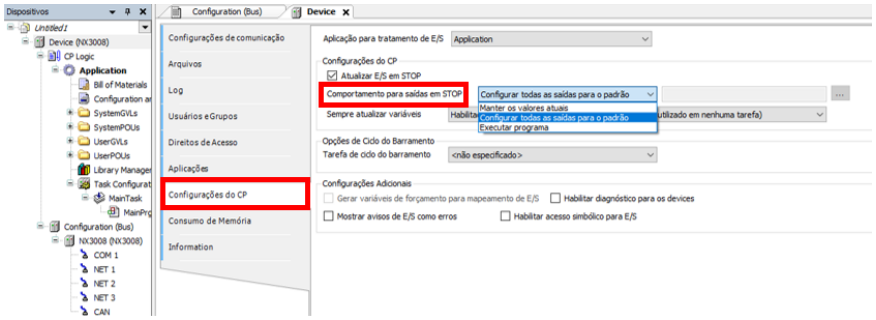


Figura 24: Configurações das saídas

5.9. Visualização de Erros

RC 3.7 da norma IEC 62443-4-2

Os erros ocorridos no sistema são apresentados de forma clara, objetiva e rápida, informando ao usuário as informações necessárias para sua correção ou diagnostico mais aprofundado. Além disso, não fornece dados tão detalhados a ponto de servirem de ajuda para ataques.

Existem dois lugares onde o sistema apresenta ao usuário os erros. Nos Logs (como apresenta a seção 5.7) e na janela de mensagens do Mastertool.

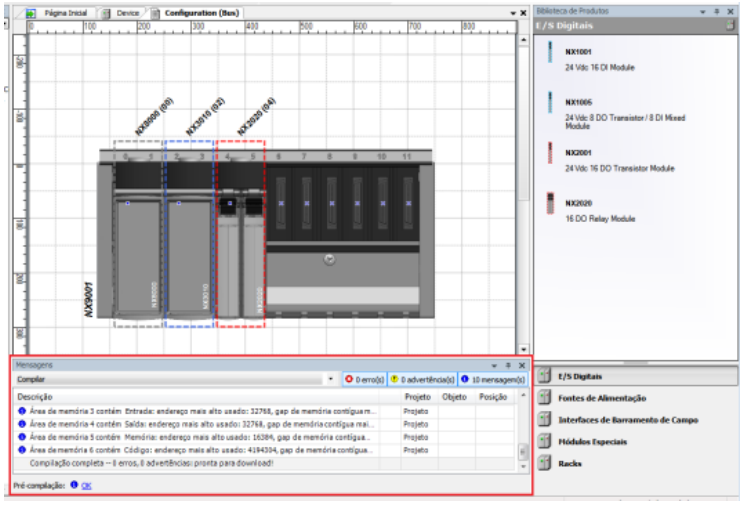


Figura 25: Janela de mensagens

Na janela de mensagens são exibidos os erros referentes ao desenvolvimento da aplicação, como erros de configuração ou sintaxe e má utilização de bibliotecas. Além disso, nesta aba também aparecem mensagens e advertências referentes ao projeto.

5.10. Backup do Sistema de Controle

RC 7.3 da norma IEC 62443-4-2

É possível realizar o download do código fonte dentro da memória interna da CPU para fins de backup.

Ao tentar fazer login no PLC após alguma modificação no projeto, será exibida uma caixa de seleção mudança online ou download das alterações e, após isso, é solicitado ao usuário se ele deseja fazer download do código fonte. Isso garante que o código fonte da aplicação seja armazenado em backup dentro do PLC.

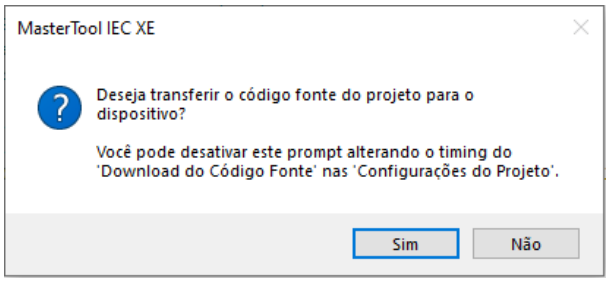


Figura 26: Opção de Download para o PLC.

Outra forma de manter uma cópia completa do código é através da extração do Arquivamento do Projeto. Isso irá gerar um arquivo que contém, além do código, todas as bibliotecas utilizadas para rodar a aplicação.

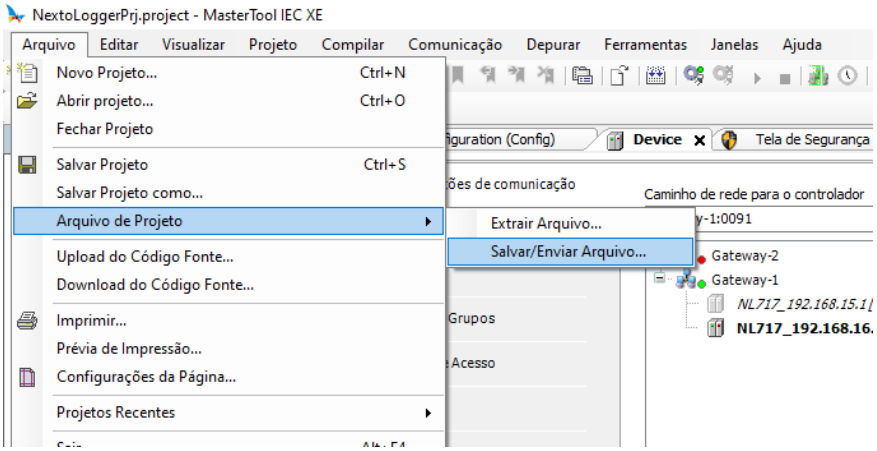


Figura 27: Arquivamento de PRojeto.

Para armazenar o firmware do PLC em backup, é necessário acessar https://www.altus.com.br/suporte/downloads/ e baixar o arquivo. Não é possível manter o firmware em backup na memória interna do PLC.

A atualização do firmware pode ser feita pela página web da peça. Para acessá-la, digitar o IP na barra de pesquisa do navegador. Em seguida, acessar *Gerenciamento da UCP*. Será necessário fazer login para executar essa ação (admin/admin). Deve-se carregar o arquivo baixado anteriormente. A atualização pode levar alguns minutos.

5.11. Inventário de componentes instalados

RC 7.8 da norma IEC 62443-4-2

É possivel verificar o inventário de componentes instalados no Mastertool ao acessar o menu Ajuda.

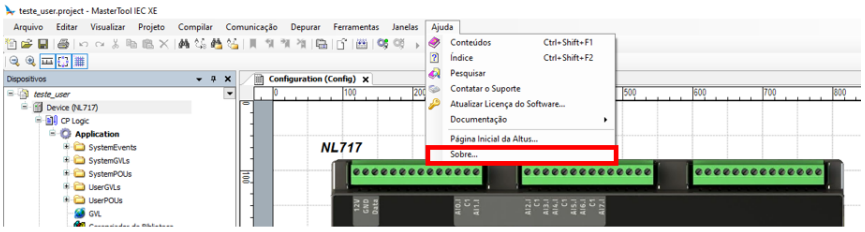


Figura 28: Inventário de Componentes instalados

Nesta página pode-se verificar todos os componentes instalados no Mastertool.

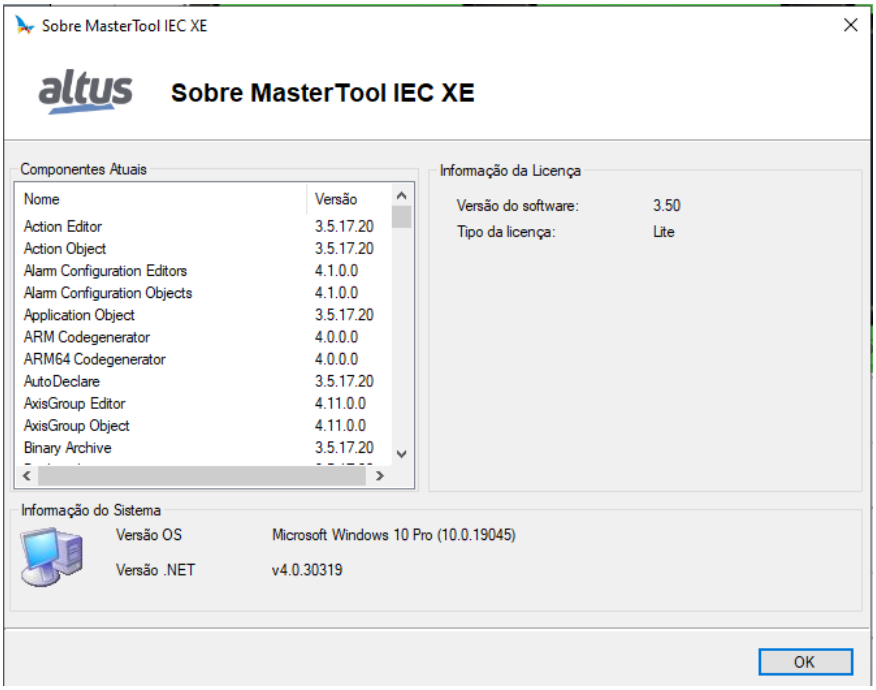


Figura 29: Componentes instalados

5.12. Proteção contra códigos maliciosos

RC 3.2 da norma IEC 62443-4-2

Por ser um sistema fechado, as formas de se carregar código malicioso são feitas através de carga de aplicativo ou atualização de firmware. A carga de aplicativo possui as proteções de usuário citadas anteriormente e, para atualização de firmware, o arquivo é encriptado e possui consistência de conteúdo.

5.13. Métodos de proteção do projeto

RC 4.3 da norma IEC 62443-4-2

É possível acessar as configurações de segurança do projeto no menu *Projeto* > *Configurações do projeto* > *Segurança*. Nesta tela, o usuário pode selecionar o método de segurança do projeto. O método padrão é *Verificação de integridade*, onde o arquivo é salvo em um formato proprietário e sua integridade é verificada a cada carregamento do projeto.

O método mais seguro é com utilização de criptografia, onde o usuário pode configurar uma senha usada para codificar o conteúdo do arquivo do projeto. Será necessário digitar a senha toda vez que o projeto for aberto. Também existe a possibilidade de configuração de encriptação a partir de certificados, sendo necessário que os certificados de todos os usuário que compartilham o projeto estejam salvos no armazenamento local.

Para realizar a importação e demais configurações dos certificados de proteção do projeto, veja Tela de Segurança.

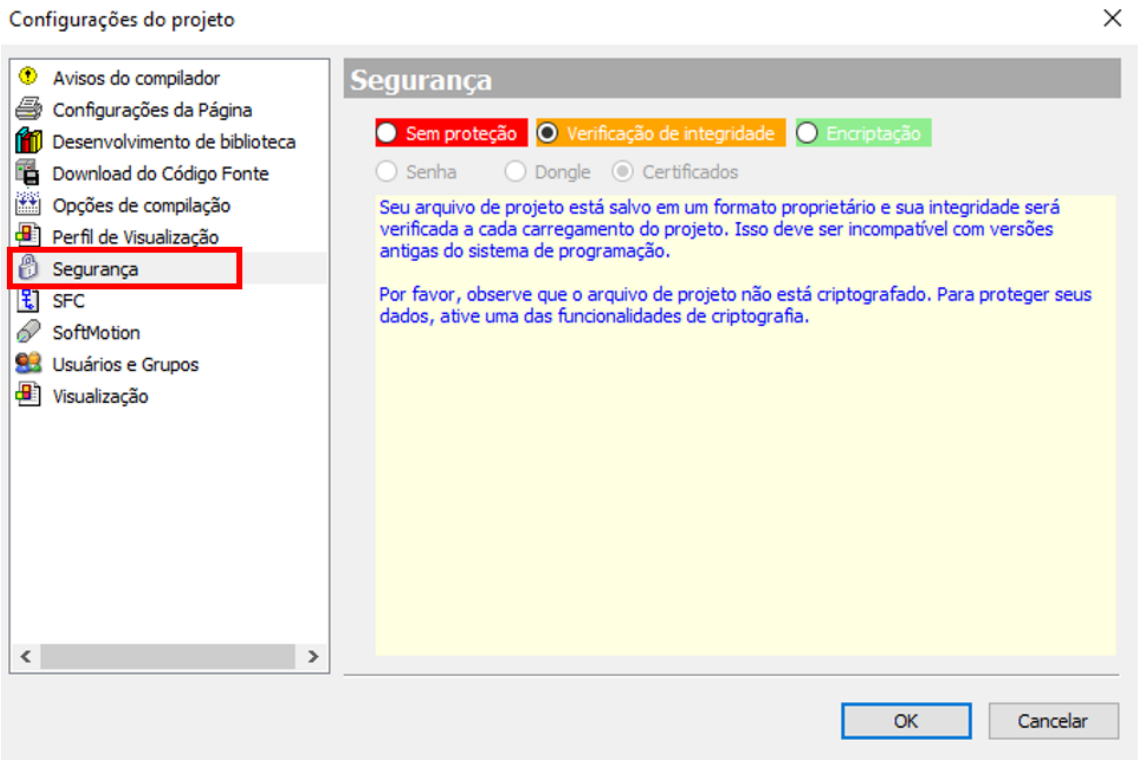


Figura 30: Menu de segurança.

6. Medidas de Segurança dos CLPs Altus

Os CLPs da Altus são equipados com diferentes dispositivos de segurança para evitar vulnerabilidades durante sua operação. Algumas medidas são presentes em apenas alguns modelos de controladores, então sempre cheque no manual específico do produto pelo recurso de segurança desejado. Abaixo dos títulos dos subcapítulos, é informado o requisito de componente (RC) ou o Requisito de Dispositivo Embarcado (EDR) da norma IEC 62443-4-2:2019-02 à qual ela diz respeito.

6.1. Gerenciamento de Usuários e Direitos de Acesso da UCP

RC 1.1, RE (1), 1.3, 1.4, 1.5, 1.7, 2.1, RE(1), RE(2) da norma IEC 62443-4-2

As UCPs Nexto possuem um sistema de gerenciamento de permissões de usuário, que bloqueia ou permite certas ações para cada grupo de usuários na UCP. Para editar estes direitos na UCP, o usuário necessita acessar um projeto no MasterTool IEC XE não sendo necessário estar logado na UCP. Deverá então clicar na Árvore de Dispositivos, localizada à esquerda do programa, dar dois cliques no item *Device* e, após, selecionar a UCP na aba *Configurações de Comunicação* que será aberta. Apenas as abas *Usuários e Grupos* e *Direitos de Acesso* se relacionam com este tópico. A figura abaixo ilustra os passos para acessar esta aba da CPU.

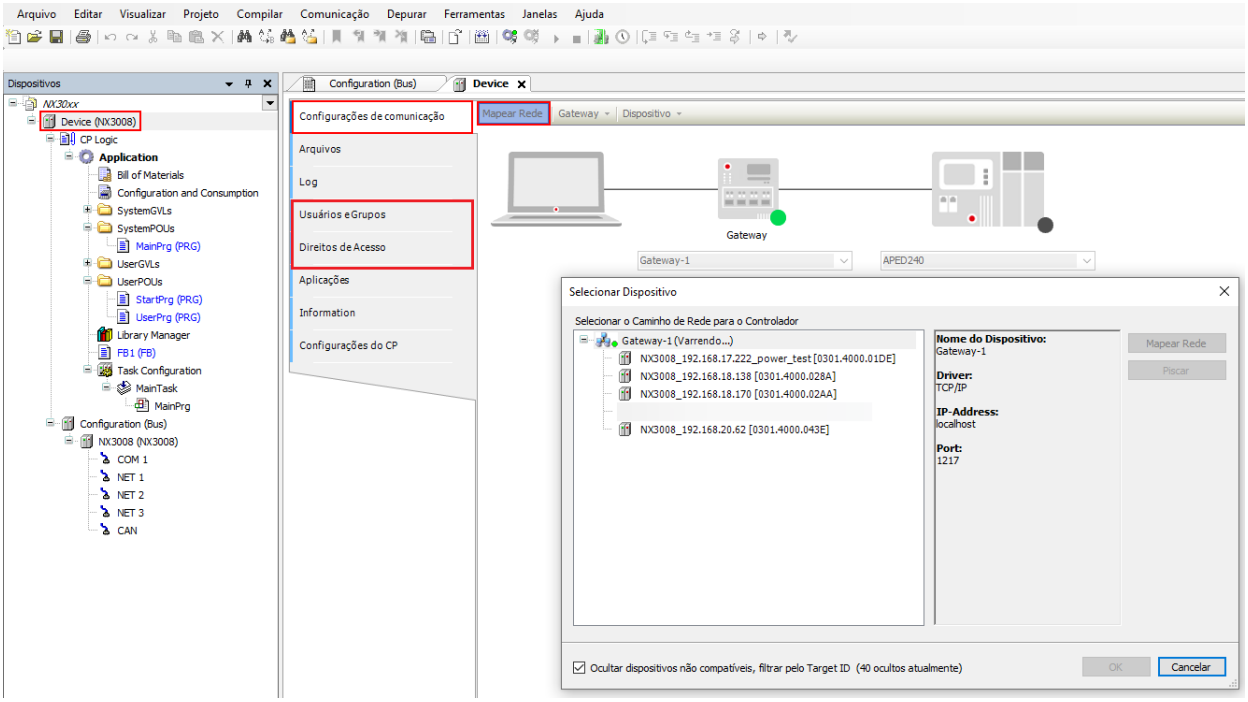


Figura 31: Acesso às Abas de Usuários, Grupos e Direitos de Acesso

ATENÇÃO

Caso o usuário esqueça a(s) senha(s) da(s) conta(s) com acesso à UCP, o único modo de recuperar este acesso será atualizando o firmware da mesma.

ATENÇÃO

Após executar o comando Logoff de um usuário da UCP, deve-se fechar a aba *Device* desse mesmo projeto para efetivamente encerrar os seus direitos de acesso.

6.1.1. Usuários e Grupos

O diálogo *Usuários e Grupos* é fornecido em uma guia do diálogo *Devices*. Ele permite configurar contas de usuários e grupos que, em conjunto com o gerenciamento dos direitos de acesso, controlam o acesso aos objetos no CP no modo online.

6.1.1.1. Comum

Para que algumas funções de um controlador possam ser executadas apenas por usuários autorizado, utiliza-se o *Gerenciamento de Usuário Online*. Esta opção fornece a possibilidade de definir contas de usuários, atribuir direitos de acesso para grupos e forçar a autenticação do usuário no login.

O gerenciamento de usuários específico do dispositivo pode ser predefinido pela descrição do dispositivo e também depende dessa descrição até que ponto as definições podem ser editadas nas caixas de diálogo de configuração no sistema de programação.

Da mesma forma que no gerenciamento de usuários do projeto, os usuários devem ser membros dos grupos e somente grupos de usuários podem obter determinados direitos de acesso.

6.1.1.2. Usando a Caixa de Diálogo de Configuração

Basicamente, o tratamento dos diálogos de gerenciamento de usuários online é similar ao do gerenciamento de usuários do projeto. Há a possibilidade de *importar* definições de contas de usuários a partir do gerenciamento de usuários do projeto.

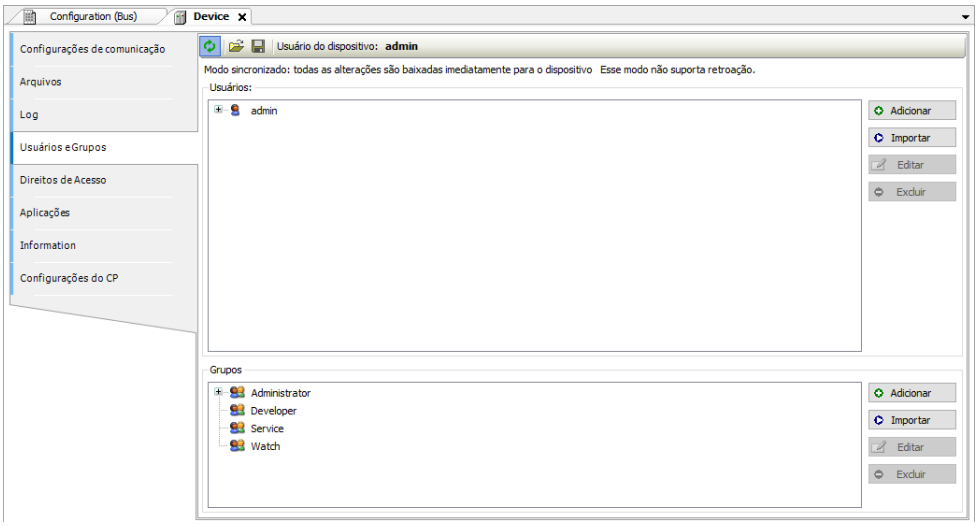


Figura 32: Caixa de Diálogo de Dispositivo, Usuários e Grupos

6.1.1.2.1. Usuários

Os seguintes botões estão disponíveis para configurar contas de usuários:

Adicionar: O diálogo *Adicionar usuário* abre onde você pode definir um nome de usuário e uma senha. A senha deve ser repetida no campo *Confirmar senha*.

ATENÇÃO

Ao abrir esse diálogo os campos *Senha* e *Confirmar Senha* estarão preenchidos com caracteres fictícios, o usuário deve substituir esses caracteres por uma senha válida.

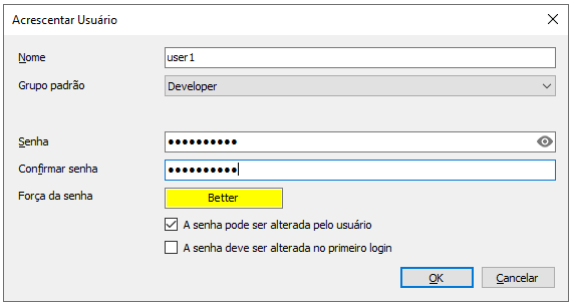


Figura 33: Adicionar Usuário (Caixa de Diálogo)

Importar: o diálogo *Importar Usuários* mostra todos os nomes de usuários atualmente definidos no gerenciamento de usuários do projeto. Selecione um ou mais itens e confirme com *OK*. No diálogo tecle *ENTER* a senha abrirá onde você deverá inserir a senha correspondente, conforme definido no gerenciamento de usuários do projeto, para importar a conta de usuário para o gerenciamento de usuários específico do dispositivo.

Editar: A conta de usuário atualmente selecionada pode ser modificada quanto ao nome de usuário e senha. Este diálogo *Editar Usuário* <nome do usuário> corresponde ao diálogo *Adicionar Usuário*.

Editar: a conta de usuário atualmente selecionada pode ser modificada quanto ao nome de usuário e senha. Este diálogo *Editar Usuário* <nome de usuário> corresponde ao diálogo *Adicionar Usuário*.

Excluir: A conta de usuário atualmente selecionada será excluída. *Excluir*: a conta de usuário atualmente selecionada será deletada.

6.1.1.2.2. Grupos

Adicionar: O diálogo *Adicionar Grupo* abre onde você pode definir um novo nome de grupo e selecionar entre os usuários atualmente definidos e aqueles que devem ser membros deste grupo.

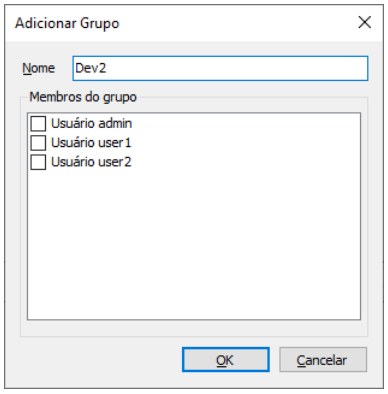


Figura 34: Adicionar Grupo (Caixa de Diálogo)

Importar: o diálogo *Importar Grupos* apresenta uma lista com os grupos atualmente definidos no gerenciamento de usuários do projeto. Selecione um ou mais itens e confirme com *OK* para integrá-los à lista de grupos do gerenciamento de usuários específico do dispositivo.

Editar: o grupo atualmente selecionado pode ser modificado no que se refere ao seu nome e usuários associados. Para tanto, usa-se o diálogo *Editar Grupo Service* <nome do grupo>, o qual corresponde ao diálogo *Adicionar Grupo*.

Excluir: o grupo atualmente selecionado será excluído.

6.1.1.3. Aplicando e Armazenando a Configuração Atual

 Ativa ou desativa a sincronização entre o editor e o sistema de gerenciamento de usuários do dispositivo.

Quando o botão não está ativado, o editor permanece em branco ou exibe uma configuração que você carregou do disco rígido.

Se você ativar a sincronização enquanto o editor contiver uma configuração de usuário que não foi sincronizada com o dispositivo, será solicitado a decidir como tratar o conteúdo do editor. Você tem as seguintes opções:

- **Carregar do dispositivo e substituir o conteúdo do editor**: Isto irá carregar a configuração do dispositivo para o editor, substituindo o conteúdo atual.
- **Baixar o conteúdo do editor para o dispositivo e substituir o gerenciamento de usuários lá**: Isto transferirá a configuração do editor para o dispositivo, aplicando-a e substituindo as configurações de gerenciamento de usuários existentes.

 salvar em Disco,  carregar do Disco: A configuração atual pode ser armazenada em um arquivo *.dum2 e recarregada a partir deste arquivo, o que é útil para configurar a mesma configuração de usuários em vários sistemas. O diálogo padrão para procurar arquivos no sistema será fornecido com esta finalidade. O filtro do arquivo é configurado automaticamente para *.*dum2*, o qual significa arquivos específicos de *Gerenciamento de usuários do dispositivo*.

Nota: Antes do CODESYS V3.5 SP16, o tipo de arquivo de gerenciamento de usuários do dispositivo (*.dum) era utilizado, o qual não exigia nenhuma criptografia.

As configurações atuais podem ser impressas ou documentadas através dos comandos *Imprimir...* (menu *Arquivo*) ou *Documento...* (menu *Projeto*).

6.1.1.4. Considerações sobre Usuários e Grupos Padrão

Nas versões 1.3.x.x ou inferiores do firmware existem os usuários e grupos: Everyone e Owner, conforme visto na tabela abaixo:

Usuários	Grupos
Todos	Todos
Proprietário	Proprietário

Tabela 1: Usuários e grupos nas versões 1.3.x.x

Já nas versões, ou superiores do firmware existem os usuários: Administrator e Everyone; e os grupos: Administrator, Developer, Everyone, Service e Watch. Como visto na tabela abaixo:

Usuários	Grupos
Administrador	Administrator
Todos	Developer
	Everyone
	Service
	Watch

Tabela 2: Usuários e grupos nas versões 1.4.x.x

6.1.1.4.1. Grupo Administrator

Este grupo possui todos os privilégios e não é possível removê-lo nas versões de firmware 1.4.x.x ou superiores. O grupo Developer faz parte deste grupo.

6.1.1.4.2. Grupo Developer

Grupo criado para definir direitos de acesso a usuários que são desenvolvedores de aplicações. O grupo Service faz parte deste grupo. Se não for utilizado, este grupo pode ser removido.

6.1.1.4.3. Grupo Everyone

Para versões de firmware 1.3.x.x ou inferiores: Este é o grupo padrão para realizar acessos em uma CPU enquanto não houver usuários e grupos definidos.

Para versões de firmware 1.4.x.x ou superiores: Este é o grupo padrão para realizar acessos em uma CPU enquanto não houver usuários e grupos definidos.

6.1.1.4.4. Grupo Service

Grupo criado para definir direitos de acesso a usuários que fornecem algum tipo de serviço no CP, por exemplo, equipes de manutenção. O grupo Watch faz parte deste grupo. Se não for utilizado, este grupo pode ser removido.

6.1.1.4.5. Grupo Watch

Grupo criado para definir direitos de acesso a usuários que apenas podem visualizar sem realizar nenhum tipo de modificação na aplicação, se não for utilizado este grupo pode ser excluído.

6.1.1.4.6. Usuário Administrator

O usuário Administrator está definido nos grupos Everyone e Administrator. A senha padrão do usuário Administrator é *Administrator* e pode ser modificada.

6.1.1.4.7. Usuário Everyone

Para versões de firmware 1.3.x.x ou inferiores: O usuário Everyone está definido no grupo Everyone. Este usuário não tem uma senha definida.

Para versões de firmware 1.4.x.x ou superiores: O usuário Everyone está definido nos grupos Everyone e Administrator. Este usuário não tem uma senha definida.

6.1.1.5. Usuários e Grupos de Projetos Antigos

Para manter esses dados de projetos antigos em um novo projeto após a atualização do firmware da CPU ou em uma nova CPU Nexto, é necessário executar o comando *Sincronização* () no projeto antigo com o firmware original, assim obtendo a configuração da CPU, e então executar o comando *Exportar para o disco*, salvando a configuração atual em um arquivo.

Na nova UCP Nexto ou na UCP atualizada, executar o comando *Importar do disco*, e selecionar o arquivo gerado anteriormente, execute o comando *Sincronização* de novo, enviando assim as configurações para a UCP.

ATENÇÃO

Caso o projeto antigo esteja com as versões 1.3.x.x ou inferiores do firmware deve-se, antes de salvar a configuração em um arquivo, um usuário e um grupo com o nome *Administrator* devem ser criados antes de salvar as configurações em um arquivo. Este procedimento garante que a configuração será carregada em projetos com versões 1.4.x.x ou superiores do firmware.

6.1.2. Direitos de Acesso

Este diálogo é fornecido em uma guia do diálogo *Device* (Editor do dispositivo). Ele faz parte do *Gerenciamento de Usuários Online* e é utilizado para conceder ou negar certas permissões aos grupos de usuários atualmente definidos, definindo assim os direitos de acesso do usuário a arquivos ou objetos (como uma aplicação) no CP em tempo de execução.

Observe que estas permissões somente podem ser atribuídas a grupos e não a usuários únicos. Por isto, um usuário deve estar definido como membro de um grupo. A configuração dos usuários e grupos é feita na guia *Usuários e Grupos* do editor do dispositivo.

A figura abaixo mostra os direitos de adicionar e remover filhos para o objeto Device para os grupos de usuários *Administrator*, *Developer*, *Service* e *Watch*.

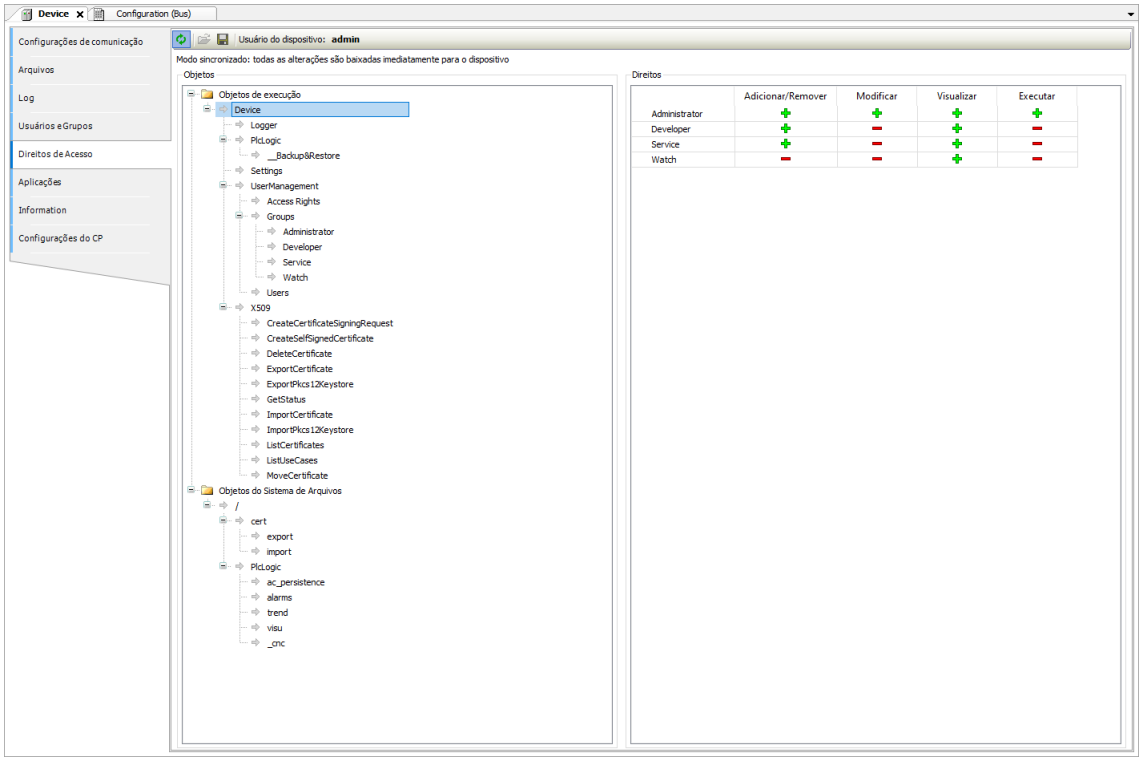


Figura 35: Direitos de Acesso ao Dispositivo

Veja a seguir como definir as permissões de acesso e como carregá-las para o dispositivo ou armazená-las em um arquivo recarregável.

6.1.2.1. Definindo os Direitos de Acesso

Para definir a permissão para executar uma ação em um ou vários objetos, selecione-os abaixo do tipo de ação desejada na janela *Objetos*, em seguida, selecione o grupo desejado no *Direitos de Acesso*, e clique no botão *Adicionar* ou *remover* (também na janela *Direitos de Acesso*).

Veja a seguir a descrição das janelas de diálogo específicas.

6.1.2.1.1. Objetos

Esta parte do diálogo lista as ações que podem ser realizadas durante a execução em arquivos no sistema de arquivos do CP e objetos de execução, como por exemplo, aplicações. A árvore é estruturada da seguinte forma:

- :
  - No nível superior, para fins de estruturação, encontram-se as *pastas* referentes aos objetos do sistema de arquivos e objetos de execução.
- :
  - Nesta pasta, existem nós para os quatro tipos de ações passíveis de execução nos objetos específicos. Estes nós servem apenas para fins estruturais:
  - Adicionar/remover secundários (adição ou remoção de objetos *secundários* para um objeto existente).
  - Executar (por exemplo, iniciar/parar aplicações, configuração de breakpoints, etc.)
  - Modificar (por exemplo, envio de aplicações, etc.)
  - Visualizar (monitoração)
- Objetos (ação *dispositivos*)

ATENÇÃO

Atribuindo uma definição de direito de acesso a um *objeto principal* na árvore de objetos, geralmente significa que o *objeto secundário* vai herdar esta definição enquanto não receber uma definição específica própria. Entretanto, dependendo do dispositivo, isto pode ser tratado diferentemente. De qualquer forma, as heranças não são visualizadas nos diálogos.

6.1.2.1.2. Direitos

Este campo mostra os grupos de usuários definidos e seus direitos. Ao selecionar um objeto na aba *Objetos*, você pode alterar seus direitos usando os seguintes botões:

- : as ações selecionadas no momento na janela *Objetos* são concedidas para o grupo.
- : as ações selecionadas no momento na janela *Objetos* são negadas para o grupo.
- : não há definição explícita de direito de acesso para as ações selecionadas no momento, na janela *Objetos*.

6.1.2.2. Aplicando e Armazenando a Configuração Atual

Ativa ou desativa a sincronização entre o editor e o sistema de gerenciamento de usuários do dispositivo.

Quando o botão não está ativado, o editor permanece em branco ou exibe uma configuração que você carregou do disco rígido.

Se você ativar a sincronização enquanto o editor contiver uma configuração de usuário que não foi sincronizada com o dispositivo, será solicitado a decidir como tratar o conteúdo do editor. Você tem as seguintes opções:

- **Carregar do dispositivo e substituir o conteúdo do editor**: Isto irá carregar a configuração do dispositivo para o editor, substituindo o conteúdo atual.
- **Baixar o conteúdo do editor para o dispositivo e substituir o gerenciamento de usuários lá**: Isto transferirá a configuração do editor para o dispositivo, aplicando-a e substituindo as configurações de gerenciamento de usuários existentes.

Salvar no disco, Carregar do disco: a configuração atual pode ser armazenada em um arquivo xml (*.drm) e recarregada a partir deste arquivo, o qual é útil para definir a mesma configuração de usuário em vários sistemas. O diálogo padrão para navegação no sistema de arquivos será fornecido para este propósito. O filtro do arquivo automaticamente é configurado para **.drm*, o qual quer dizer *direitos de acesso de dispositivo*.

As configurações atuais podem também ser documentadas em versões impressas via comando *Imprimir...* (menu *Arquivo*) ou *Documento...* (menu *Projeto*).

6.1.2.3. Direitos de Acesso de Projetos Antigos

Para manter os direitos de acesso de projetos antigos em novos projetos após a atualização de firmware da UCP ou em novas UCPs Nexto, é necessário no projeto antigo com o firmware original executar o comando *Sincronização* ( ) no projeto antigo com o firmware original, assim, obtendo a configuração da UCP, e após, o comando *Salvar em Disco*, salvando assim a configuração atual em um arquivo.

Na nova UCP Nexto ou na UCP atualizada, executar o comando *Carregar do Disco*, e selecionar o arquivo gerado anteriormente, executar o comando *Sincronização* de novo, assim, enviando a configuração para a CPU.

ATENÇÃO

Se o projeto antigo estiver com versões de firmware 1.3.x.x ou inferiores, um usuário e um grupo com o nome *Administrator* devem ser criados antes de salvar as configurações em um arquivo. Este procedimento garante que a configuração será carregada em projetos com versões de firmware 1.4.x.x ou superiores.

6.1.3. Acesso ao Sistema de Runtime com gerenciamento de permissões/Autenticações

RC 1.4 e 1.5 da norma IEC 62443-4-2

Existem diferentes fases de uma aplicação industrial: desde o início do desenvolvimento do código-fonte para seu comissionamento até a produção com a máquina ou planta e sua manutenção. Essas fases são normalmente operadas por diferentes técnicos com níveis de qualificação adequados.

Ao considerar esses níveis de qualificação, bem como as ameaças de um possível uso além da tarefa ou competência, faz sentido limitar o uso para determinados grupos de usuários.

O MasterTool suporta autenticação e gerenciamento de permissão para um usuário ou grupo de usuários administradores. Dependendo da política de segurança do sistema de runtime, o gerenciamento de usuários pode ser aplicado por padrão ou não. Caso não seja, todos são membros do grupo de administradores e têm direitos ilimitados no controlador até que o gerenciamento de usuários seja ativado. Ao utilizá-lo é necessário que sua primeira ativação seja durante o primeiro login, especificando um usuário administrador.

Assim que pelo menos um novo usuário é adicionado, todos os usuários devem se autenticar com seus nomes de usuário e senhas para cada conexão online com o controlador. As senhas são transferidas criptografadas (por padrão, usando criptografia assimétrica) e armazenadas codificadas como hashes de criptografía no sistema de runtime.

Esta medida reduz a ameaça de acesso acidental ou pretendido ao controlador em execução, o que poderia afetar a disponibilidade ou a integridade da aplicação compilada executada em o controlador.

O Login Seguro no controlador programável provê uma maneira de proteger a aplicação do usuário de qualquer acesso não autorizado. Habilitando esta característica, a UCP da Série Nexto irá solicitar uma senha de usuário antes de executar quaisquer comandos entre MasterTool IEC XE e a UCP, como parar e programar a aplicação ou forçar pontos de saída em um módulo.

6.2. Proteção contra ataques tipo flood

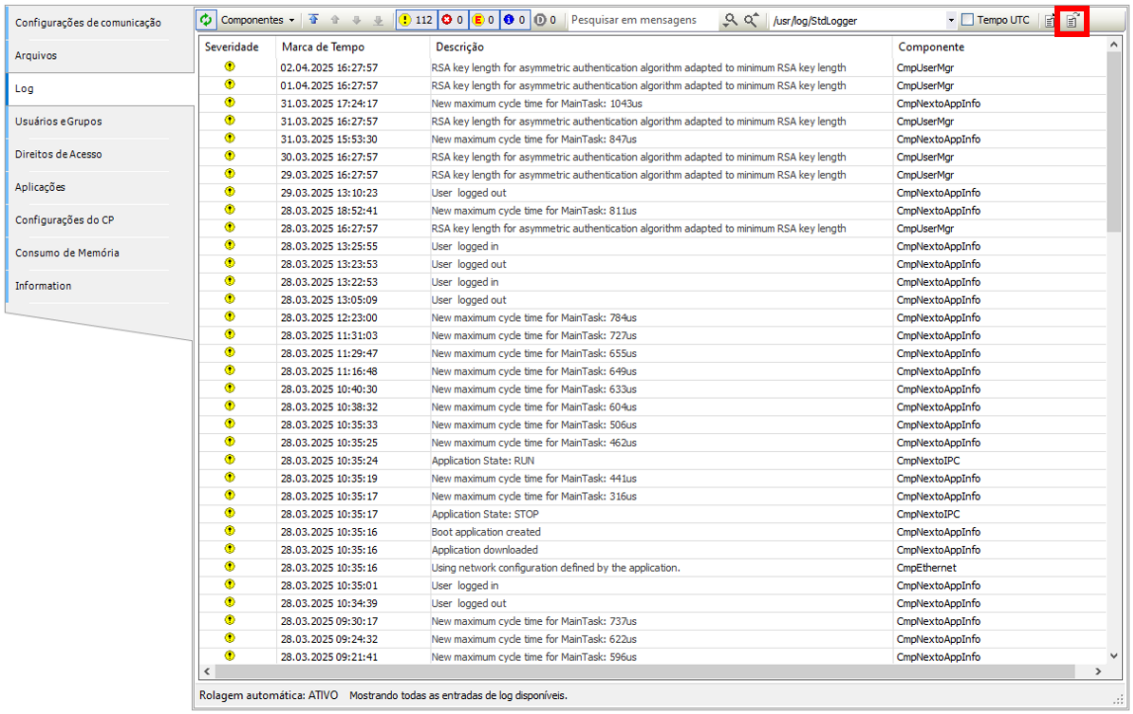
RC 7.1 da norma IEC 62443-4-2

Os controladores NX3035, NX3008, HX3040 e o módulo NX5000 são equipados com uma proteção contra ataques tipo flood. Esse recurso essencial de segurança é projetado para detectar e mitigar efetivamente ataques de inundação, nos quais uma grande quantidade de dados é enviada simultaneamente para sobrecarregar o sistema e causar indisponibilidade ou interrupção do serviço. Entretanto, sempre é recomendado o uso de regras de firewall para permitir tráfego apenas de endereços conhecidos, para aumentar esta proteção.

6.3. Armazenamento dos logs

RC 2.9, RE(1), CR 3.9 RE(1) da norma IEC 62443-4-2

Os logs do dispositivo são armazenados na memória interna. É possível exportar um arquivo contendo todos os registros, dessa forma, podendo ser salvo em qualquer outro lugar que o usuário desejar. Para realizar a exportação, deve-se acessar os logs do dispositivo e clicar no ícone marcado na imagem



Severidade	Marca de Tempo	Descrição	Componente
	02.04.2025 16:27:57	RSA key length for asymmetric authentication algorithm adapted to minimum RSA key length	CmpUserMgr
	01.04.2025 16:27:57	RSA key length for asymmetric authentication algorithm adapted to minimum RSA key length	CmpUserMgr
	31.03.2025 17:24:17	New maximum cycle time for MainTask: 1043us	CmpNextoAppInfo
	31.03.2025 16:27:57	RSA key length for asymmetric authentication algorithm adapted to minimum RSA key length	CmpUserMgr
	31.03.2025 15:53:30	New maximum cycle time for MainTask: 847us	CmpNextoAppInfo
	30.03.2025 16:27:57	RSA key length for asymmetric authentication algorithm adapted to minimum RSA key length	CmpUserMgr
	29.03.2025 16:27:57	RSA key length for asymmetric authentication algorithm adapted to minimum RSA key length	CmpUserMgr
	29.03.2025 13:10:23	User logged out	CmpNextoAppInfo
	28.03.2025 18:52:41	New maximum cycle time for MainTask: 811us	CmpNextoAppInfo
	28.03.2025 16:27:57	RSA key length for asymmetric authentication algorithm adapted to minimum RSA key length	CmpUserMgr
	28.03.2025 13:25:55	User logged in	CmpNextoAppInfo
	28.03.2025 13:23:53	User logged out	CmpNextoAppInfo
	28.03.2025 13:22:53	User logged in	CmpNextoAppInfo
	28.03.2025 13:05:09	User logged out	CmpNextoAppInfo
	28.03.2025 12:23:00	New maximum cycle time for MainTask: 784us	CmpNextoAppInfo
	28.03.2025 11:31:03	New maximum cycle time for MainTask: 727us	CmpNextoAppInfo
	28.03.2025 11:29:47	New maximum cycle time for MainTask: 655us	CmpNextoAppInfo
	28.03.2025 11:16:48	New maximum cycle time for MainTask: 649us	CmpNextoAppInfo
	28.03.2025 10:40:30	New maximum cycle time for MainTask: 633us	CmpNextoAppInfo
	28.03.2025 10:38:32	New maximum cycle time for MainTask: 604us	CmpNextoAppInfo
	28.03.2025 10:35:33	New maximum cycle time for MainTask: 506us	CmpNextoAppInfo
	28.03.2025 10:35:25	New maximum cycle time for MainTask: 462us	CmpNextoAppInfo
	28.03.2025 10:35:24	Application State: RUN	CmpNextoIPC
	28.03.2025 10:35:19	New maximum cycle time for MainTask: 441us	CmpNextoAppInfo
	28.03.2025 10:35:17	New maximum cycle time for MainTask: 316us	CmpNextoAppInfo
	28.03.2025 10:35:17	Application State: STOP	CmpNextoIPC
	28.03.2025 10:35:16	Boot application created	CmpNextoAppInfo
	28.03.2025 10:35:16	Application downloaded	CmpNextoAppInfo
	28.03.2025 10:35:16	Using network configuration defined by the application.	CmpEthernet
	28.03.2025 10:35:01	User logged in	CmpNextoAppInfo
	28.03.2025 10:34:39	User logged out	CmpNextoAppInfo
	28.03.2025 09:30:17	New maximum cycle time for MainTask: 737us	CmpNextoAppInfo
	28.03.2025 09:24:32	New maximum cycle time for MainTask: 622us	CmpNextoAppInfo
	28.03.2025 09:21:41	New maximum cycle time for MainTask: 596us	CmpNextoAppInfo

Figura 36: Exportar Logs

Os logs são salvos de forma circular, ou seja, uma vez que é atingido o limite de memória disponível, os registros mais antigos começam a ser sobrescritos.

6.4. SysLog

RC 2.9, RE(1) da norma IEC 62443-4-2

Syslog (System Logging Protocol) é um protocolo que permite que dispositivos enviem mensagens de log para um sistema centralizado de coleta e armazenamento de logs. Essas mensagens podem incluir informações sobre eventos do sistema, erros, avisos, e outras atividades relevantes para a administração e segurança do sistema.

A configuração da UCP como Client SysLog pode ser feita a partir da seção *Sistema* na aba *Gerenciamento* da página Web de Sistema da UCP. Conforme é mostrado na figura abaixo.

Figura 37: Configurações do SysLog

6.4.1. Configuração do SysLog

A configuração do SysLog é composta por apenas dois campos, o checkbox *"Habilitar Serviço"* por padrão é desabilitado, sendo necessário marcar-lo para ativar o serviço. No campo *"Endereço IP do Servidor"* é configurado o endereço IP do servidor SysLog que será utilizado.

Após a configuração do endereço IP do servidor e a habilitação do serviço, as configurações serão aplicadas clicando no botão *"Aplicar"*. É importante que o servidor Syslog esteja devidamente configurado para comunicar com o cliente via protocolo UDP, utilizando a porta 514.

Quando configurado, o SysLog enviará para o servidor todos os logs presentes nos *Logs de Sistema* do Mastertool, como detalhado na seção Logs. O serviço do SysLog apenas envia logs de prioridade *WARNING* ou superior, como indicado na classificação abaixo:

Categoria do Mastertool	Categoria do Syslog	Prioridade
Exception	Emergency	0
Error	Error	3
Warning	Warning	4

Tabela 3: Prioridade Das Mensagens Do SysLog

6.5. Funcionalidades página web

EDR 3.10 e RE(1) e RC 5.1 da norma IEC 62443-4-2

Os produtos oferecem uma página de configuração acessível através do navegador, basta digitar o endereço IP do equipamento na barra de pesquisa. Por lá, é possível configurar e monitorar diversas funcionalidades, a depender do produto.

6.5.1. Atualizar CLP

É possível fazer atualização de firmware dos PLC a partir da página web. Para acessá-la, digite o IP na barra de pesquisa do navegador. Em seguida, acesse *Gerenciamento da UCP*. Será necessário fazer login para executar essa ação (admin/admin por padrão).

Deve-se carregar o arquivo de firmware disponível em https://www.altus.com.br/suporte#suportedownload. A atualização pode levar alguns minutos.

Antes de efetivamente ser feita a gravação do firmware novo, são realizadas etapas de verificação de integridade do arquivo e da sessão. Primeiramente, é solicitado que o usuário realize login com senha no PLC, garantindo que apenas pessoas autorizadas tenham acesso. Após isso, o firmware passa por série de verificações em cima do binário passado, verificando modelo, CRC e quantidade de arquivos.

Após isso, os arquivos de firmware presentes no binário são descompactados e descriptografados, sendo também submetidos à verificação de CRC. Só depois disso são gravados.

6.5.2. Mudança do IP do CLP

Na página web do dispositivo, acesse o menu *Gerenciamento* e encontre a tela de *Configurações de rede*. Nesta tela, modifique os valores e salve as alterações.

Figura 38: Alteração de configurações de rede pela página web do dispositivo.

6.6. Cartão de Memória

RC 2.9, RE(1), CR 3.9 RE(1), da norma IEC 62443-4-2

Entre outras funcionalidades, este modelo de UCP da Série Nexto possibilita ao usuário a utilização de um cartão de memória, conforme as características do CLP utilizado.

Quando o cartão for inserido na UCP e estiver com sistema de arquivos diferente de FAT32, ela automaticamente identifica e pergunta ao usuário se ele deseja formatar. Em caso negativo, ele não poderá utilizar o cartão (o cartão não será montado e o visor não indicará a presença do cartão). Caso seja selecionada a opção de formatação, a UCP irá levar alguns minutos, dependendo do tempo de ciclo (execução) da aplicação rodando na UCP, para executar a operação. Assim que o cartão de memória for montado, a UCP irá ler informações gerais do mesmo, deixando o acesso ao cartão de memória mais lento nos primeiros minutos. Esse procedimento é feito quando o cartão é inserido, após a reinicialização da UCP ou através da página web do dispositvo.

ATENÇÃO

Recomenda-se realizar o procedimento de formatação do cartão de memória diretamente na UCP Nexto para evitar possíveis problemas de utilização, aumento do tempo de montagem ou até mesmo funcionamento incorreto.
Não é recomendado remover o cartão de memória ou desenergizar a UCP durante a formatação ou durante a transferência de arquivos, pois pode causar a perda de dados bem como danos irreversíveis ao cartão.

6.6.1. Memory Card Configuration

Foi desenvolvida uma página web para gerenciamento do cartão de memória. Dentre as funcionalidades oferecidas estão a formatação, opção para desmontar e remover o cartão e a possibilidade de habilitar e desabilitar a interface do cartão. Estas configurações foram desenvolvidas na seção "Cartão de Memória", na página web da UCP, dentro da aba de "Gerenciamento". Além das configurações, também são exibidas informações sobre o estado atual do dispositivo, espaço de armazenamento total e livre, ambos medidos em *kB*. A imagem abaixo apresenta a página inicial, com a interface habilita e sem nenhum dispositivo conectado.

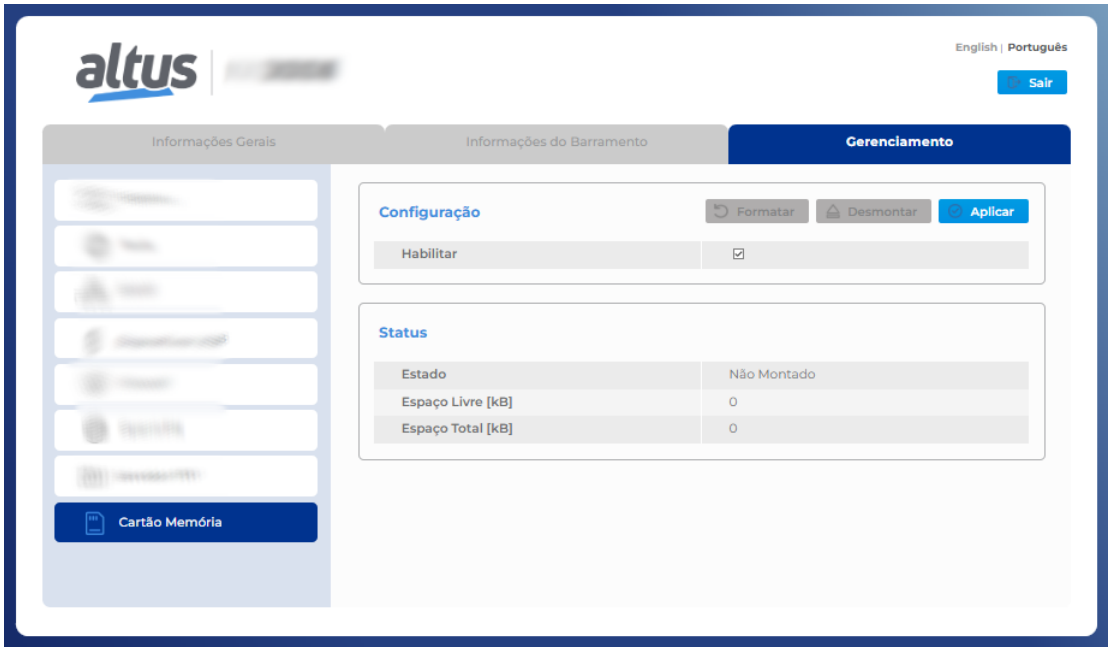


Figura 39: Cartão de Memória Página Inicial

Enquanto não há um cartão de memória inserido e montado na UCP, os botões *Formatar* e *Desmontar* ficam bloqueados para uso. A tabela de **Status** indica o Estado *Não Montado*. Ao inserir um cartão de memória na UCP, o botão *Formatar* é habilitado para uso. Depois que o cartão é montado o botão *Desmontar* também fica disponível para ser utilizado. Ao inserir um cartão de memória na CPU, pode levar alguns instantes para que o cartão seja montado e as informações sejam atualizadas na página da web. A imagem abaixo apresenta a página web quando há um cartão conectado e montado na UCP.

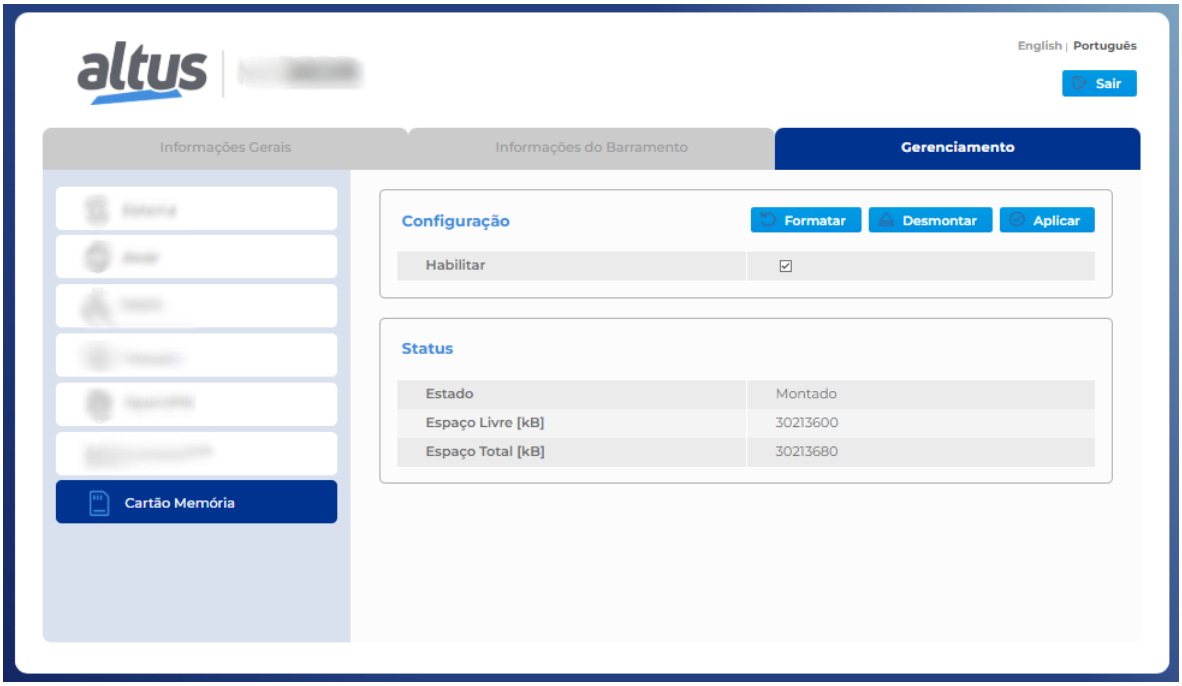


Figura 40: Cartão de Memória com Dispositivo Montado

6.6.1.1. Formatting the Memory Card

Para formatar o dispositivo, utilize o botão **Formatar**. Ao clicar, será exibida uma mensagem, estilo *pop-up*, solicitando a confirmação da operação. A imagem abaixo apresenta esta mensagem.

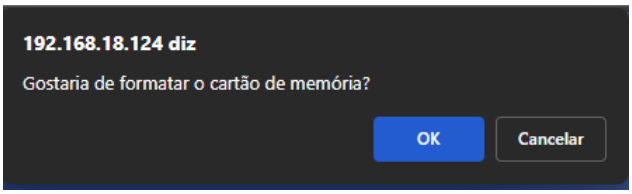


Figura 41: Mensagem Confirmação de Formatação

Ao confirmar no botão **OK**, a operação é iniciada, logo após, todas as configurações são bloqueadas. Os botões **Formatar**, **Desmontar** e **Aplicar** e também a caixa de seleção ficam indisponíveis durante a formatação. O processo de formatação é indicado na tabela de **Status**, com o valor do **Estado** alterado para *Formatando...*, como apresentado na figura abaixo.

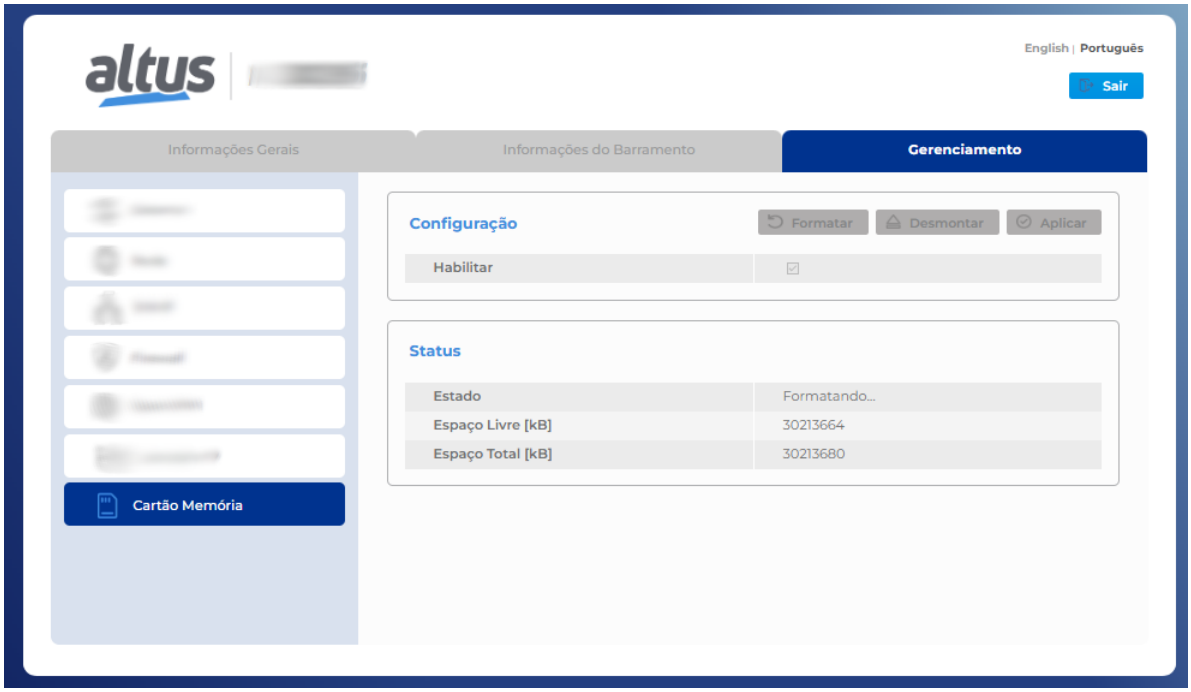


Figura 42: Cartão de Memória Formatando

Ao final do processo de formatação, é exibida uma mensagem indicando a finalização da operação no dispositivo. A figura a seguir apresenta esta mensagem.

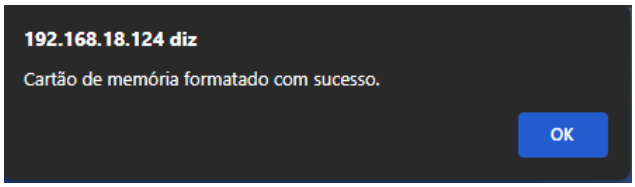


Figura 43: Mensagem de Formatação Concluída

Com a conclusão da operação, a página web retorna para o estado inicial, desbloqueando todos os botões e a caixa de seleção, da mesma forma que é apresentada na figura Cartão de Memória com Dispositivo Montado

6.6.1.2. Unmounting the Memory Card

Para desmontar e remover o dispositivo, utilize o botão **Desmontar**. Ao clicar, será exibida uma mensagem, estilo *pop-up*, solicitando a confirmação da operação. A imagem abaixo apresenta esta mensagem.

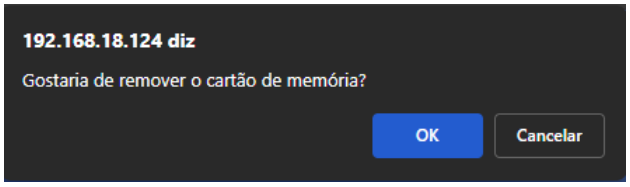


Figura 44: Mensagem Confirmação para Desmontar

Ao confirmar no botão **OK**, a operação é iniciada, logo após, todas as configurações são bloqueadas. Os botões **Formatar**, **Desmontar** e **Aplicar** e também a caixa de seleção ficam indisponíveis durante a desmontagem. O processo de desmontagem é indicado na tabela de **Status**, com o valor do **Estado** alterado para *Desmontando...*, como apresentado na figura abaixo.

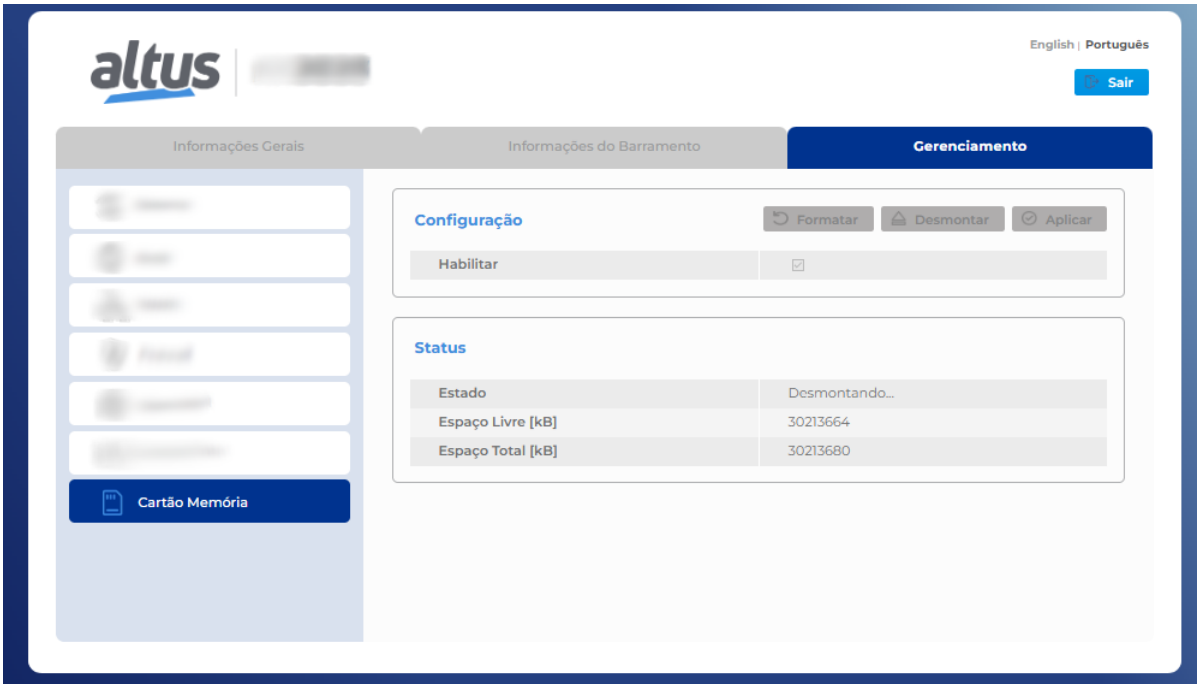


Figura 45: Cartão de Memória Desmontando

Ao final do processo de desmontagem, é exibida uma mensagem indicando a finalização da operação no dispositivo. A figura a seguir apresenta esta mensagem.

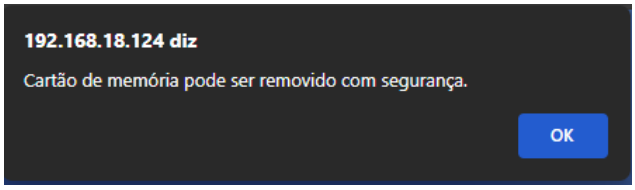


Figura 46: Mensagem de Desmontagem Concluída

Após a operação ser concluída com sucesso, os botões **Formatar** e **Aplicar** e também a caixa de seleção ficam disponíveis para uso. O botão **Desmontar** permanece bloqueado, pois o cartão já foi desmontado. A tabela de *Status* apresenta os dados para um cartão não montado, como pode ser visualizado na imagem abaixo:

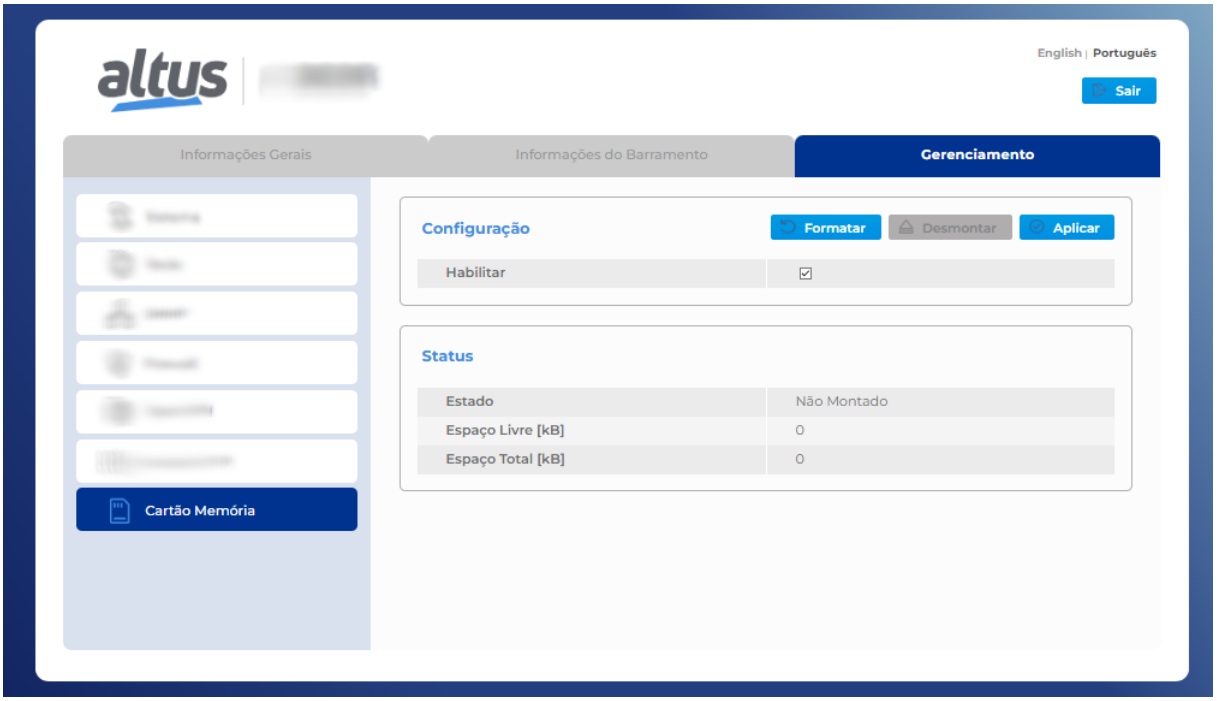


Figura 47: Cartão de Memória Não Montado

6.6.1.3. Memory Card Interface Management

Foi desenvolvida uma configuração na página web do cartão para habilitar e desabilitar a interface do cartão de memória, esta funcionalidade faz parte dos requisitos de segurança cibernética de nível um, de acordo com a IEC 62443. Para habilitar, marque a caixa de seleção *Habilitar* na tabela de **Configuração**. Então utilize o botão **Aplicar** para enviar a nova configuração. Para desabilitar, desmarque a caixa de seleção *Habilitar* e utilize o mesmo botão para aplicar a configuração. Ao clicar no botão **Aplicar** será exibida uma mensagem, do estilo *pop-up*, solicitando a confirmação da operação. A imagem abaixo mostra a mensagem.

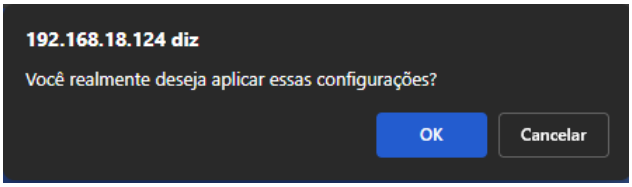


Figura 48: Mensagem Confirmação para Aplicar Configuração

Após confirmar no botão **OK**, a nova configuração é enviada para a UCP. Caso a interface tenha sido habilitada, as informações exibidas na página web dependem se há ou não um cartão de memória inserido para ser montado. Se não houver um dispositivo, a página apresentará as informações mostradas na figura Cartão de Memória Página Inicial. Quando há um dispositivo conectado as informações exibidas serão as apresentadas na figura Cartão de Memória com Dispositivo Montado, após o cartão ser defidamente montado.

Se a nova configuração desabilitar a interface, as informações apresentadas serão as da imagem abaixo.

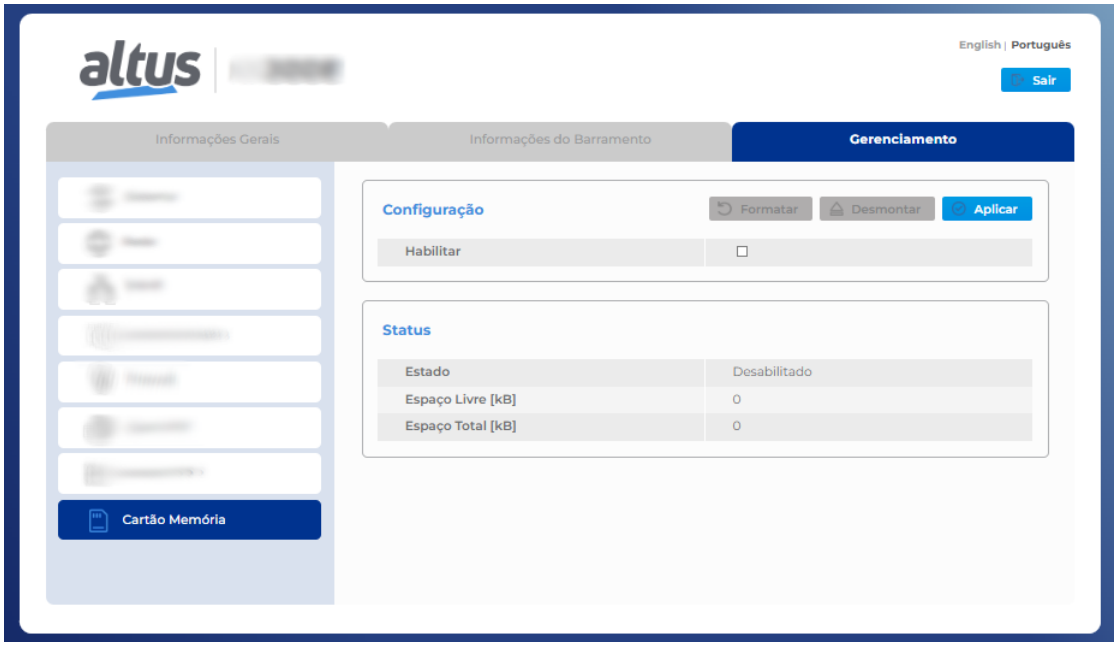


Figura 49: Cartão de Memória Interface Desabilitada

ATENÇÃO

No caso em que a desativação do cartão de memória estiver efetivada, a pasta MemoryCard não será montada.

6.6.1.4. Memory Card Interface Management by Application

Para facilitar o gerenciamento da interface do cartão de memória, foi desenvolvida uma função que pode ser chamada diretamente pelo código de aplicação do usuário. A função **SetMemCardState** foi implementada dentro da biblioteca **NextoStandard**. A imagem abaixo mostra a informações da biblioteca, apresentadas no *Library Manager*.

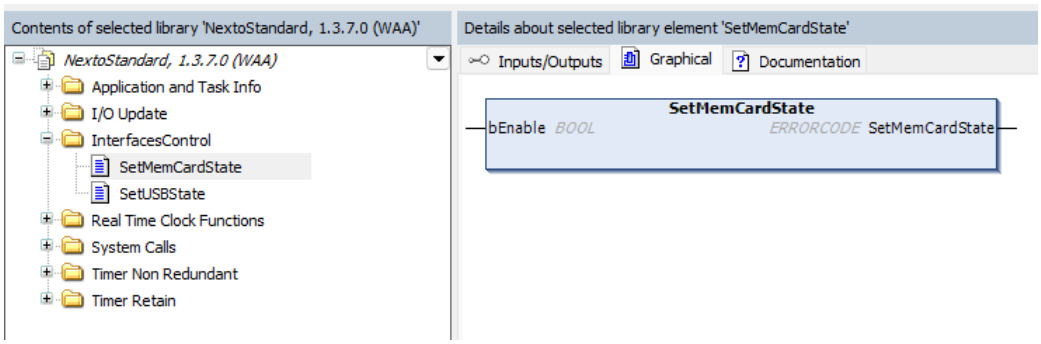


Figura 50: Informações de SetMemCardState no Library Manager

A função possui uma variável de entrada do tipo *bool*, **bEnable**, que recebe o valor para habilitar ou desabilitar a interface do cartão. A função possui três valores de retorno *NoError* em caso de sucesso, *SetMemCardStateFail* em caso de falha ou *ImportFunctionNotFound* caso a função não seja suportada. Segue abaixo um exemplo básico de declaração de variáveis e chamada da função.

```
PROGRAM UserPrg
VAR
  bSetMemoryCardInterfaceState : BOOL;
  stErrorCode : NextoStandard.ERRORCODE;
END_VAR
-------------------------------------------------------------------------
// Exemplo de chamada de função para configurar interface do cartão de memória
stErrorCode:= NextoStandard.SetMemCardState(bEnable :=
   bSetMemoryCardInterfaceState);
```

ATENÇÃO

A função executa o comando para definir o valor desejado para a interface do cartão de memória. Não é necessário, nem recomendado, que a função seja chamada ciclicamente.

6.7. Firewall

RDR 5.2 da norma IEC 62443-4-2

O Firewall foi desenvolvido para aumentar a segurança do dispositivo durante a sua utilização. A principal função do Firewall é realizar um filtro sobre os pacotes de dados que chegam e que saem do dispositivo. O filtro implementado utiliza informações de cada pacote de dados para decidir se aquele pacote é permitido ou não. Os principais parâmetros utilizados são as interfaces de entrada/saída, a porta, o protocolo da camada de transporte e os endereços de origem e destino.

6.7.1. Configuração

A configuração do Firewall é feita através de uma seção dedicada localizada na aba *Gerenciamento* da Página Web de Sistema do controlador, conforme mostrado abaixo:

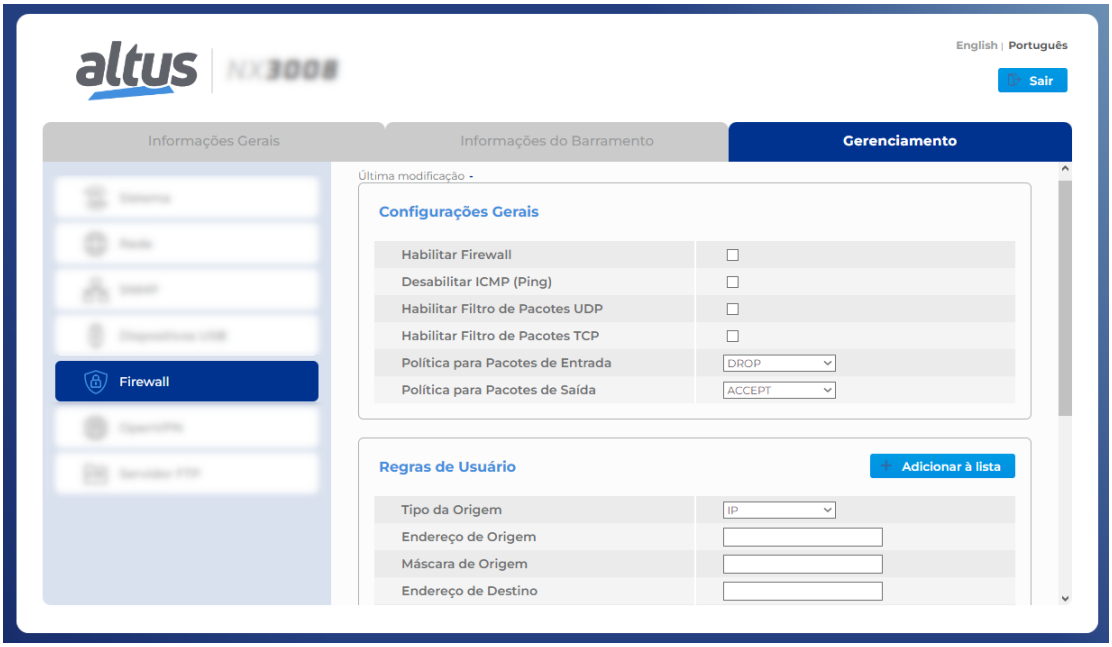


Figura 51: Tela de Configuração do Firewall

O Firewall trata-se de uma funcionalidade à parte ao Mastertool, isto é, não necessita de interação alguma com a ferramenta de programação. As configurações aplicadas na Página Web de Sistema passam a valer quando confirmadas através do botão *Aplicar* e, são salvas automaticamente no controlador. Contanto que a funcionalidade esteja habilitada, voltará a operar mesmo após a reinicialização do dispositivo.

As proximas seções descrevem as possíveis configurações para o Firewall, divididas de acordo com as tabelas da seção *Firewall*.

6.7.2. Configurações Gerais

A imagem abaixo exibe todas as configurações da tabela *Configurações Gerais*:

Figura 52: Tabela de Configurações Gerais do Firewall

Esta tabela expande de forma dinâmica ao selecionar as opções de habilitar filtros de pacotes UDP e TCP, revelando todos os itens possíveis de serem configurados. O primeiro item desta tabela, *Habilitar Firewall*, serve para habilitar e desabilitar esta funcionalidade. Quando o Firewall está habilitado, as configurações da seção, ao serem submetidas ao dispositivo, serão aplicadas nos arquivos de configurações e então, o Firewall passará a filtrar o que foi configurado. Caso o Firewall esteja desabilitado, a configuração que foi realizada é armazenada, porém as regras não são aplicadas no controlador.

O campo *Desabilitar ICMP (Ping)* habilita ou desabilita a proteção contra o protocolo ICMP. Quando selecionado, o controlador passa a não responder as requisições de *Ping*, uma vez que a proteção irá realizar o descarte de pacotes que utilizarem o protocolo ICMP. Já quando desativada, o funcionamento do dispositivo em relação a respostas de *Ping* mantém seu comportamento normal.

Os campos que habilitam o filtro de pacotes UDP e TCP, quando habilitado, realizam o filtro destes protocolos dentro dos limites configurados nos seus respectivos campos. A regra que realiza a filtragem dos pacotes possuí o seguinte funcionamento: para que um pacote seja aceito, é necessário que existam "créditos" disponíveis, um crédito é utilizado para aceitar um pacote de dado.

A configuração do campo *Estouro de Pacotes XXX* configura o valor inicial de pacotes, ou créditos, que serão aceitos. Dessa forma, é possível configurar um limite de estouro destes pacotes, onde caso haja um fluxo muito grande de pacotes, somente serão aceitos a quantidade configurada. O campo de *Pacotes XXX por Segundo*, configura quantos créditos aquela regra irá ganhar por segundo, ou seja, se for configurado o valor 5, a cada segundo a regra receberá cinco novos créditos, logo poderá aceitar mais cinco pacotes. A limitação para esse incremento no número de créditos é a própria configuração de *Estouro de Pacotes XXX*, o limite estabelecido aqui não é ultrapassado, mesmo com o incremento de pacotes a cada segundo. Estas configurações são aplicadas como um *estoque*, onde ao receber um pacote de dados, primeiro é verificado se há algum crédito disponível no estoque e então é tomada a decisão de aceitar ou não o pacote. Se o pacote é aceito neste filtro de quantidade, ele é direcionado para o filtro das demais regras de Firewall.

A configuração *Habilitar Filtro por IP*, faz com que a regra diferencie os endereços de origem de cada pacote e aplique os filtros de estouro e de pacotes por segundo de forma individual para cada endereço. Assim, retomando o exemplo anterior,

pode ser considerado que cada endereço de origem possuí o seu *estoque* de créditos e um endereço não pode utilizar os créditos que estão no *estoque* reservados para outro.

ATENÇÃO

Não é permitido a configuração de valores negativos para os campos de *Pacotes XXX por Segundo* e *Estouro de Pacotes XXX*. Caso sejam configurados valores negativos, ao aplicar as configurações será exibido uma mensagem de erro na tela indicando o campo que houve algum conflito. Caso o filtro seja habilitado, porém, os valores nestes campos sejam deixados em 0, o filtro não é aplicado.

As configurações desta tabela são aplicadas com o botão de *Aplicar* que aparece na figura 54.

Os campos para selecionar ambas as políticas, de entrada e de saída, possuem as opções de *Accept*, aceitar, e de *Drop*, descartar. As políticas possuem o seguinte funcionamento: se o Firewall estiver ativo, quando os pacotes de dados chegam, todas as regras que foram configuradas são verificadas, então será aplicada a politica configurada para estes pacotes, seja ela de *Accept* ou *Drop*. Assim, se for configurado uma politica de aceitação, *Accept*, todos os pacotes que não combinarem com nenhuma regra configurada, serão aceitos pelo Firewall e se configurado uma política de rejeição, *Drop*, os mesmos seriam todos descartados.

6.7.3. Regras de Usuário

A tabela *Regras de Usuário* foi criada para permitir um controle maior sobre as configurações de regras do Firewall. Com ela é possível configurar diferentes regras de forma dinâmica e com filtros mais precisos.

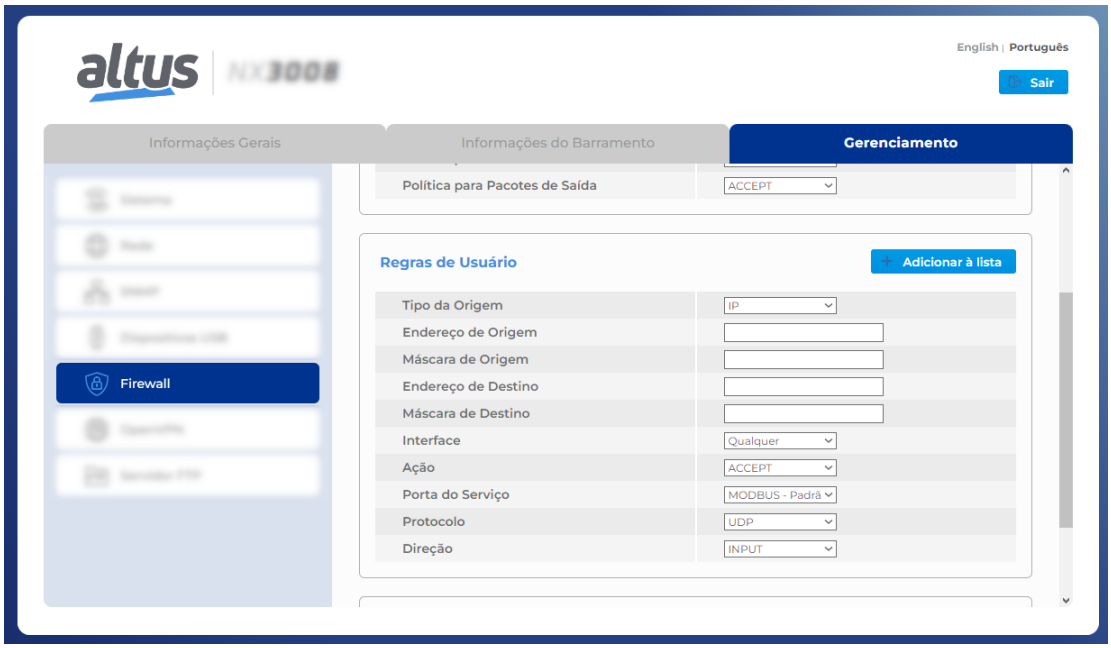


Figura 53: Tabela de Configuração de Regras de Usuário do Firewall

Esta tabela altera o seu formato de acordo com o *Tipo de Origem* selecionado, podendo ser IP ou MAC. Quando o tipo é *IP*, a tabela possuí os itens exibidos na figura acima, porém, quando é selecionado o tipo como *MAC* os campos de máscaras de origem e destinos desaparecem, assim como o campo de *Endereço do Destino*. O item *Endereço de Origem* passa a aceitar um endereço MAC como entrada em um formato de seis grupos de dois digitos hexadecimais separados por dois pontos, ex: "1A:2B:3C:4D:5E:6F". Além disso, uma regra com base em endereço *MAC* somente pode ser configurada como uma regra de entrada, ou seja, o campo *Direção* será forçado com o valor *INPUT*.

Com os campos de *Endereço de Origem* e *Endereço de Destino*, é possível informar os endereços que serão configurados para aquela regra específica e com o uso dos campos *Máscara de Origem* e *Máscara de Destino* é possível configurar uma faixa de rede para esta regra. A definição de um endereço e uma máscara resulta em um grupo de IP's que será atribuído a regra que está sendo configurada. Se for realizada somente a configuração do endereço, este único endereço será atribuído à regra, porém com diferentes configurações de máscara de rede é possível obter grupos de IP's de diversos tamanhos, que serão aplicados a regra.

A configuração de interface possibilita a seleção de cada interface física ou virtual disponível para o controlador, de forma individual. Além disso, existe a opção *Qualquer*. Com base na interface que for selecionada para determinada regra, somente os pacotes de dados que estiverem entrando ou saindo por ela, serão filtrados pelo Firewall. Se utilizado a opção *Qualquer*, a regra não possuíra filtro de interface, logo, a regra passa a valer para todas as disponíveis.

O campo *Ação* possuí três opções de configuração: *ACCEPT*, *DROP* e *REJECT*. A ação configura o que deve ser feito com o pacote cujas características conferem com a regra aplicada. Caso a ação escolhida seja *ACCEPT*, o pacote de dados que tiver suas características de acordo com a regra, será aceito. Caso seja *DROP*, o pacote será descartado e nenhuma resposta será enviada a quem enviou o pacote. Por último, caso seja configurado como *REJECT*, o pacote será rejeitado e será encaminhada uma resposta para quem enviou o pacote, informando que o *host* solicitado está inacessível.

O campo *Porta de Serviço* serve para indicar quais as portas serão configuradas nesta regra. Todas as portas de serviços que possuem um determinado protocolo ou comunicação *padrão* para o controlador, como por exemplo o protocolo MODBUS que tem a porta padrão 502, estão disponíveis com o nome do serviço e a porta utilizada ao lado. Assim, caso seja configurada a regra para o protocolo MODBUS, será aplicada a porta 502, caso seja configurada a regra para o serviço webvisu, será aplicada a porta 8080 e assim segue para os demais protocolos listados no campo de seleção. Este campo também possuí outras duas configurações, que são *Qualquer* e *Outra*. Quando é selecionada a opção *Qualquer*, a regra é aplicada para todas as portas de serviços, exceto a porta 80, então são criadas duas regras utilizando as seguintes faixas de portas: *1:79* e *81:65535*. Caso seja selecionada a opção *Outra*, será exibido uma caixa de texto na qual é possível configurar a porta que deseja, exceto a porta 80. Para configurar uma porta, basta escrever o seu número na caixa de texto, se desejar adicionar mais de uma única porta, é necessário utilizar o separador *"&"* e caso queira inserir uma faixa de portas, basta informar a porta inicial e final utilizando o separador *":"*.

Exemplo de configuração das portas 120, 144, e da faixa de 1300 a 1450 no mesmo campo: *120 & 144 & 1300:1450*.

Este campo não aceita valores fora da faixa 1:65535, a porta 80 ou repetições de portas.

A porta HTTP, 80, somente pode ser configurada através da seleção na lista de protocolos conhecidos e não pode ser aplicada a interface NET1. Sendo assim, caso o protocolo HTTP seja escolhido, os campos *NET1* e *Qualquer* do campo de Interface não serão possíveis de serem selecionados.

No campo de *Protocolo* é possível selecionar entre os protocolos *UDP*, *TCP* e *UDP|TCP*. Caso seja selecionado a opção *UDP|TCP*, serão criadas duas regras no Firewall, uma para cada protocolo de transporte.

No campo de *Direção* é possível selecionar entre *INPUT*, *OUTPUT* e *INPUT|OUTPUT*. Estas opções fazem com que a regra seja aplicada para os pacotes que estão chegando no dispositivo, opção de *INPUT*, ou que estão saindo do dispositivo, opção de *OUTPUT*. Caso seja configurado a opção conjunta, serão criadas duas regras, uma com cada opção de direção.

A figura abaixo demonstra como é feita a aplicação de uma regra:

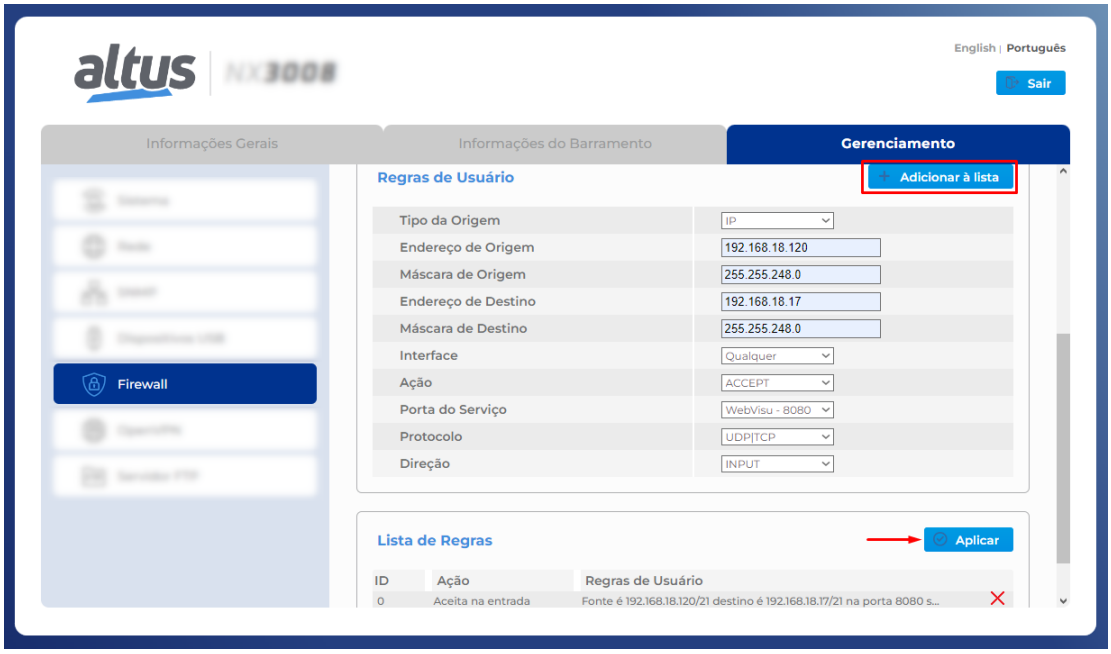


Figura 54: Tabela de Aplicação de Regras de Usuário do Firewall

Após preencher os campos conforme deseja configurar a regra de Firewall, deve-se clicar no botão *Adicionar à lista*. Ao fazer isso todas as configurações serão analisadas para conferir se há valores inválidos ou se há alguma regra duplicada. Não

é possível adicionar duas regras com os mesmos parâmetros de endereços, máscaras, interface, portas e direção. Caso algum conflito seja encontrado, será exibido uma mensagem indicando o campo que houve uma configuração inválida, ou ainda, o ID da regra presente na tabela cujas configurações ocasionaram o conflito com a nova regra configurada.

Após serem verificados todos os parâmetros, a regra será adicionada à lista abaixo da tabela de configuração. Esta lista se expande de forma automática, conforme são adicionadas ou excluídas regras. Caso queira excluir uma regra da lista, basta posicionar o mouse sobre a regra que deseja excluir. Ao fazer isto, será exibido um botão *X*, da cor vermelha, conforme mostrado na figura anterior. Ao clicar nele, a regra será excluída da tabela.

Ao adicionar novas regras, ou excluir uma existente na tabela das regras, deve-se clicar no botão de *Aplicar*, que aparece mais abaixo, para que a configuração seja aplicada no dispositivo.

ATENÇÃO

Durante a aplicação das regras de firewall pode haver uma momentânea instabilidade na comunicação Ethernet.

6.8. OpenVPN

RDR 5.3 da norma IEC 62443-4-2

VPN (Virtual Private Network) é uma sigla para Rede Virtual Privada, utilizada para navegar em redes não seguras, trafegando dados importantes ou, simplesmente, realizando o acesso à internet com um nível elevado de privacidade. A rede virtual da VPN pode ser compreendida como um túnel no qual as informações trafegam de forma segura, protegidas por certificados e chaves de segurança. O OpenVPN é um serviço do tipo *open source*, ou seja, gratuito para ser utilizado e distribuído, e com o seu código fonte aberto para que sejam realizadas modificações, caso sejam necessárias.

O principal objetivo da VPN é realizar uma comunicação de forma segura através de uma rede não segura. Para que isso seja possível, é utilizada a encriptação dos dados com base em certificados e chaves gerados utilizando o TLS, Transport Layer Security, um protocolo que realiza encriptações de 256 bits, uma das mais seguras.

Para realizar a configuração de um cliente ou servidor OpenVPN, foi criada a página OpenVPN, na aba *Gerenciamento* da página Web de Sistema da UCP. Conforme é mostrado na figura abaixo.

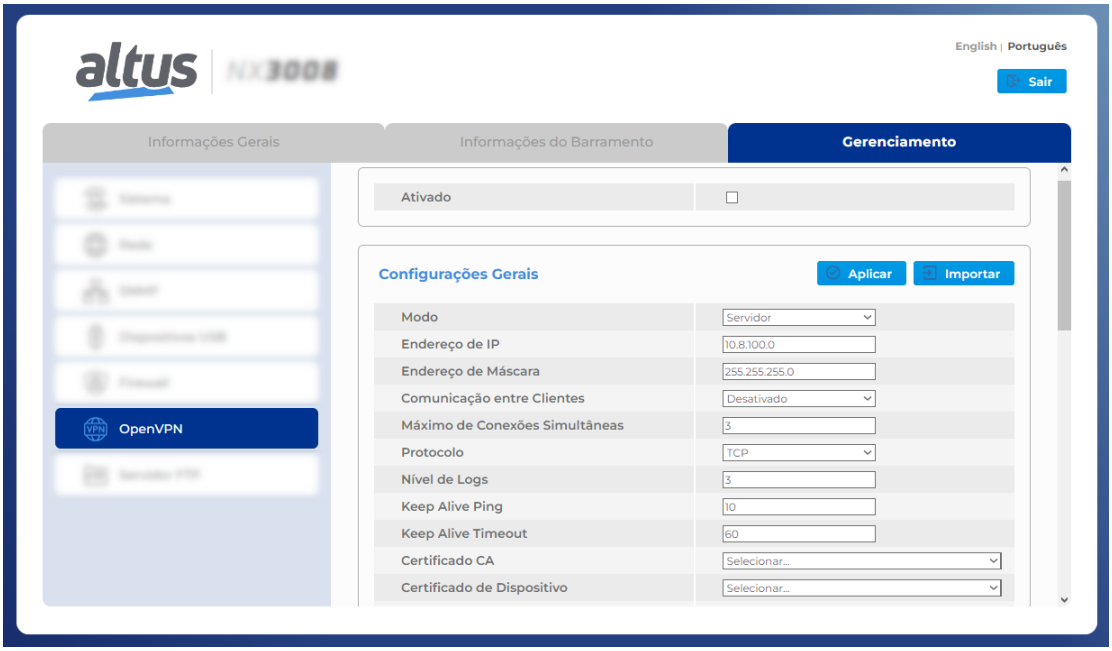


Figura 55: Tela de Configuração de OpenVPN

Por estar localizada dentro da aba *Gerenciamento*, o acesso a esta página é protegido por senha. As próximas seções descrevem as configurações e funcionalidades desta página.

6.8.1. Importação de Configurações

Para realizar a configuração da VPN de forma rápida e fácil no seu dispositivo, pode-se utilizar o botão *Importar* que aparece na figura 55 no canto superior direito da página. Ao clicar sobre este botão, é aberta uma janela, do explorador de arquivos, para que seja feita a seleção de um arquivo de configuração. Devem ser selecionados os arquivos com extensão *conf* ou *ovpn*. Ao selecionar um arquivo, o seu conteúdo será lido e os parâmetros de configuração que estiverem presentes preencherão os seus respectivos campos de configuração na página web.

Para que os parâmetros, do arquivo, sejam interpretados corretamente, eles devem seguir o padrão de sintaxe de arquivos de configuração do OpenVPN.

Caso existam arquivos de segurança, certificados ou chaves, escritos no arquivo de configuração, junto aos demais parâmetros, eles serão lidos e separados em arquivos distintos dentro do controlador para serem utilizados.

ATENÇÃO

Não devem ser utilizados espaços para separação das palavras no nome dos arquivos *".conf"*. Em vez disso, utilize *"_"* para separá-las.

6.8.2. Configuração do OpenVPN

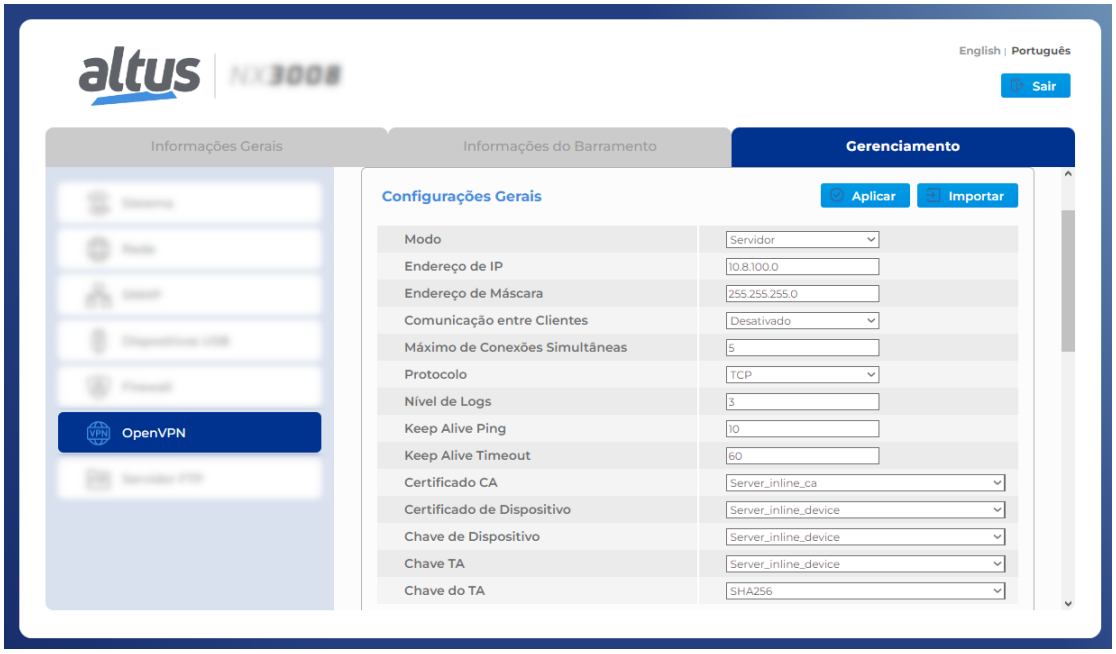


Figura 56: Tabela de Configurações de Servidor OpenVPN

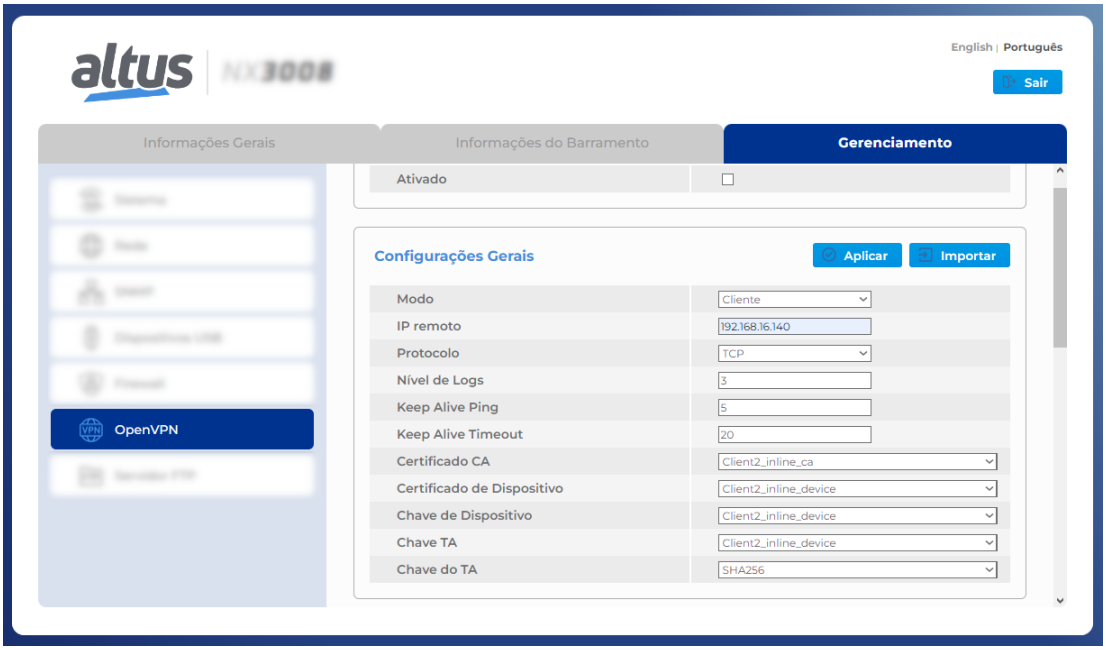


Figura 57: Tabela de Configurações de Cliente OpenVPN

Esta seção mostra como é realizada a configuração do OpenVPN. As configurações serão divididas em três partes: as comuns para ambos os modos de operação, as configurações exclusivas de um servidor e as configurações exclusivas de um cliente.

6.8.2.1. Configurações Comuns

Observando as figuras com as configurações de cliente, figura 57, e a de servidor, figura 56, é possível identificar que diversos parâmetros são os mesmos para ambas as configurações. São eles:

6.8.2.1.1. Modo

Com a configuração do *Modo* é possível selecionar entre duas opções, cliente ou servidor. Ao realizar a seleção de algum dos dois modos, a tabela de configurações se modifica de forma automática para permitir a configuração dos campos necessário para cada modo de operação.

6.8.2.1.2. Protocolo

Este campo configura qual será o protocolo de transporte a ser utilizado para a comunicação da VPN. É possível configurar entre UDP e TCP.

ATENÇÃO

A configuração do servidor e de todos os seus clientes deve ser a mesma. Com uma configuração divergente, o OpenVPN não é capaz de realizar a comunicação.

6.8.2.1.3. Nível de Logs

Este campo configura qual será o nível que o arquivo de logs receberá. A configuração varia de 0 até 5, sendo 0 o nível mais basico e 5 o nível mais avançado.

O nível 0 exibe logs somente sobre alguma falha crítica no OpenVPN e os níveis a partir de 4 são utilizados para depuração, pois há uma quantidade muito grande de informações sendo escritas no arquivo de logs. Para uma operação normal, recomenda-se a utilização do valor 3.

Este campo aceita somente números como entrada. Não é permitido utilizar letras e nem caracteres especiais.

6.8.2.1.4. *Keep Alive Ping*

Este campo configura qual o tempo, *em segundos*, em que o será encaminhada uma requisição de *Ping*. Esta requisição serve para verificar a conexão entre o servidor e os clientes.

Este parâmetro pode ser configurado tanto no servidor, quanto nos clientes do OpenVPN, porém, caso este parâmetro seja configurado no servidor, os clientes irão assumir o valor do servidor e não o valor configurado neles. Se o Servidor não possuir tal configuração, cada cliente assume a sua configuração normalmente. Caso deseje desabilitar o ping entre o servidor e os clientes, configure o valor 0.

Este campo aceita somente números como entrada. Não é permitido utilizar letras e nem caracteres especiais.

6.8.2.1.5. *Keep Alive Timeout*

Este campo configura o tempo, *em segundos*, em que ocorrerá o timeout da requisição de *Ping*. Após o término deste tempo, sem uma resposta do outro dispositivo VPN, ele será considerado desconectado.

Este parâmetro pode ser configurado tanto no servidor, quanto nos clientes do OpenVPN, porém, caso este parâmetro seja configurado no servidor, os clientes irão assumir metade do valor do servidor e não o valor configurado neles. Os clientes recebem metade do valor para garantir que eles estejam desconectados no caso de o servidor desconectar. Se o Servidor não possuir tal configuração, cada cliente assume a sua configuração normalmente. Caso deseje desabilitar esta funcionalidade, configure o valor 0.

Este campo aceita somente números como entrada. Não é permitido utilizar letras e nem caracteres especiais.

6.8.2.1.6. *Arquivos de Segurança*

Nos campos *Certificado CA*, *Certificado de Dispositivo*, *Chave de Dispositivo* e *Chave TA*, deve ser selecionado qual o arquivo de segurança, certificado ou chave, será utilizado para estabelecer a comunicação do OpenVPN. As opções de cada campo, *combobox*, são filtradas de acordo com o tipo de arquivo chave ou certificado, embora não exista diferenciação das chaves entre si e nem dos certificados entre si.

Para que seja possível selecionar algum arquivo é necessário que este tenha sido importado anteriormente.

Todos os arquivos de segurança são obrigatórios para que seja estabelecida a comunicação correta entre os clientes e o servidor VPN, exceto a *Chave TA*. Esta chave é opcional para realizar a comunicação, porém, caso ela seja utilizada no servidor, ela se torna de uso obrigatório para todos os clientes deste mesmo servidor.

Consulte a seção Gerenciamento de Certificados e Chaves TLS, para maiores informações sobre a geração de certificados e chaves de segurança com base no TLS.

6.8.2.1.7. *Chave do TA*

No campo *Chave do TA* é configurada qual será o tipo de criptografia aplicada para a *Chave TA*. Este campo se mantem oculto até que seja selecionado algum arquivo para a chave TLS, pois, ele somente é utilizado em conjunto com esta chave. O valor padrão deste parâmetro é *SHA1*, porém é possível selecionar entre os seguintes valores: *SHA256*, *SHA512* e *MD5*, além do padrão SHA1.

ATENÇÃO

É necessário que esta configuração seja igual entre os clientes e o servidor da mesma rede OpenVPN. Caso o valor deste campo seja diferente entre cliente e servidor, a conexão não será estabelecida.

6.8.2.2. Configurações Exclusivas do Servidor

As configurações exclusivas do servidor, observadas na figura 56, são descritas a seguir.

6.8.2.2.1. *Endereço de Rede*

A faixa de IP que será utilizada para atribuir os endereços do servidor e dos clientes da rede VPN é configurado pelo servidor através da configuração dos campos *Endereço de IP* e *Endereço de Máscara*. Todos os IP's que serão atribuídos para os clientes e ao servidor serão retirados da faixa especificada.

O endereço IP do servidor é sempre o endereço inicial da faixa configurada, para a atribuição de IP dos clientes, são utilizados os valores ainda disponíveis da faixa. Por exemplo, caso seja configurada uma rede com o endereço IP 10.8.12.4 e máscara

255.255.255.248, o servidor assumirá o IP 10.8.12.5 que é o primeiro endereço disponível da faixa configurada. Porém, caso seja configurada a máscara 255.255.255.0, o servidor assumirá o IP 10.8.12.1, que é o primeiro endereço disponível da faixa.

Os campos de endereço IP e máscara, somente aceitam as configurações que tenham a sintaxe de um endereço de IP e endereço de máscara, respectivamente. Caso seja configurado algo fora do padrão, será exibida uma mensagem de alerta, informando que houve algum erro.

6.8.2.2.2. Comunicação entre Clientes

Neste campo é possível habilitar ou desabilitar a comunicação entre os clientes da rede VPN. Quando a opção for selecionada como *Desativado*, somente é possível realizar a comunicação cliente-servidor diretamente. Se a opção for selecionada como *Ativado*, será permitida além da comunicação cliente-servidor, a comunicação entre os próprios clientes.

6.8.2.2.3. Máximos Clientes Conectados

Neste campo é possível configurar qual é o número máximo de clientes que podem se conectar com o servidor OpenVPN simultaneamente. Este campo aceita somente caracteres numéricos e o valor mínimo para ele é 1.

6.8.2.2.4. Redes Privadas

Ao selecionar o modo de operação do OpenPVN como servidor, será exibido uma tabela, normalmente oculta, que permite a configuração de redes privadas que podem estar abaixo do servidor e de cada cliente.

Figura 58: Tabela de Configurações de Redes Privadas OpenVPN

Para realizar a configuração de uma rede privada que está abaixo do servidor, basta selecionar o tipo da rede como *Servidor* e configurar os endereços de rede e máscara. A configuração de uma rede privada de um cliente necessita, além de configurar o tipo como *Cliente*, que seja informado o *Common Name* do cliente que possui a rede que está sendo configurada.

O Common Name de um cliente é configurado na geração do *Certificado de Dispositivo*. Este parâmetro é informado na criação do certificado e é único para cada cliente e cada servidor. A configuração destas redes privadas cria uma tabela de roteamento que será verificada ao receber ou enviar pacotes pela VPN.

A figura acima, mostra uma configuração de uma subrede *80* no servidor OpenVPN, logo, será configurada uma regra de roteamento que encaminhará os pacotes de dados, recebidos pela VPN, para a interface do dispositivo configurada nesta rede. Também é criada uma regra, interna do servidor, que caso um pacote de dado possua a subrede *70*, este pacote será roteado e encaminhado pelo túnel de VPN. O mesmo comportamento ocorre com o cliente *client2*, porém, com as sub redes trocadas, pois, abaixo deste cliente está a sub rede *70* e ele encaminhará para o túnel VPN os pacotes com a sub rede *80*.

Veja na figura a seguir um exemplo de arquitetura:

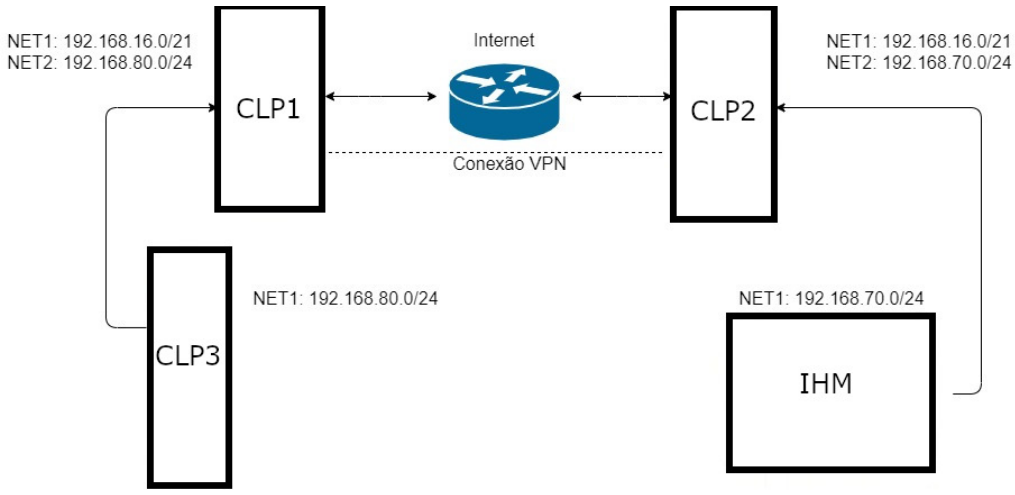


Figura 59: Exemplo de Arquitetura com Redes Privadas

Na Figura 59, o CLP1 da esquerda possui a rede privada 80 configurada na sua NET 2 e conectado a ele existe um CLP3 na mesma rede. O CLP2 da direita possui uma rede privada 70 configurada na NET 2 e conectado a ele existe uma IHM, na mesma rede. A arquitetura exemplo realiza a comunicação entre os dispositivos CLP3 e IHM pela VPN, através da configuração das suas respectivas redes privadas.

Após preencher os campos, mostrados na Figura 58, com a configuração desejada, deve-se clicar sobre o botão + azul que aparece na extrema direita dos campos de configuração, para que a regra seja adicionada à tabela. Caso deseje excluir alguma regra, arraste o mouse sobre a regra que deseja remover e, então, um *X* vermelho irá aparecer à direita, como é mostrado na Figura 58. Ao clicar sobre este *X*, a regra é removida da tabela.

Para que as configurações presentes na tabela sejam aplicadas no dispositivo é preciso clicar no botão *Aplicar* e confirmar a operação na janela de confirmação que irá surgir. Ao serem aplicadas as regras, será exibida uma mensagem indicando se houve êxito ou falha na operação.

6.8.2.3. Configurações Exclusivas de Cliente

Existe somente uma única configuração exclusiva de clientes OpenVPN na página, que pode ser visualizada na figura 57. Esta configuração é o *IP Remoto*.

6.8.2.3.1. IP Remoto

O campo de *IP Remoto*, configura qual é o endereço cujo o servidor VPN está esperando a comunicação dos clientes. Caso seja estabelecido um servidor OpenVPN em um computador, a configuração de IP remoto deve ser realizada conforme o endereço IP deste computador. Este campo também aceita *host names* como endereço remoto, portanto, é possível configurar um IP ou um host name neste parâmetro.

ATENÇÃO

Em função da necessidade de permitir parâmetros tão diferentes, IP's e host names, a única verificação existente neste campo é sobre a existência ou não de dados. Tenha atenção ao realizar a configuração.

6.8.2.4. Aplicação de Configurações

Para habilitar a funcionalidade, deve-se marcar o checkbox *Ativado*, exibido na figura 57. Caso deseje apenas aplicar as configurações realizadas e não habilitar o OpenVPN, desmarque este checkbox.

Após realizar todas as configurações desejadas, as configurações devem ser aplicadas no dispositivo, para isso utilize o botão *Aplicar*. Este botão é mostrado na figura 57, no canto inferior direito. Quando as configurações são aplicadas e a VPN

está habilitada, a seção *Firewall* irá realizar um *scroll* automático até a tabela de *status* do OpenVPN, exibida na seção Tabela de Status.

6.8.3. Arquivos de Segurança

Os arquivos de segurança são utilizados para estabelecer a comunicação do OpenVPN de forma segura, realizando o papel de criptografar e de descriptografar os pacotes de dados que trafegam pelo túnel da VPN. Na seção Gerenciamento de Certificados e Chaves TLS, é descrito como gerar chaves e certificados TLS. A figura a seguir mostra a seção responsável pelo gerenciamento dos arquivos de segurança:

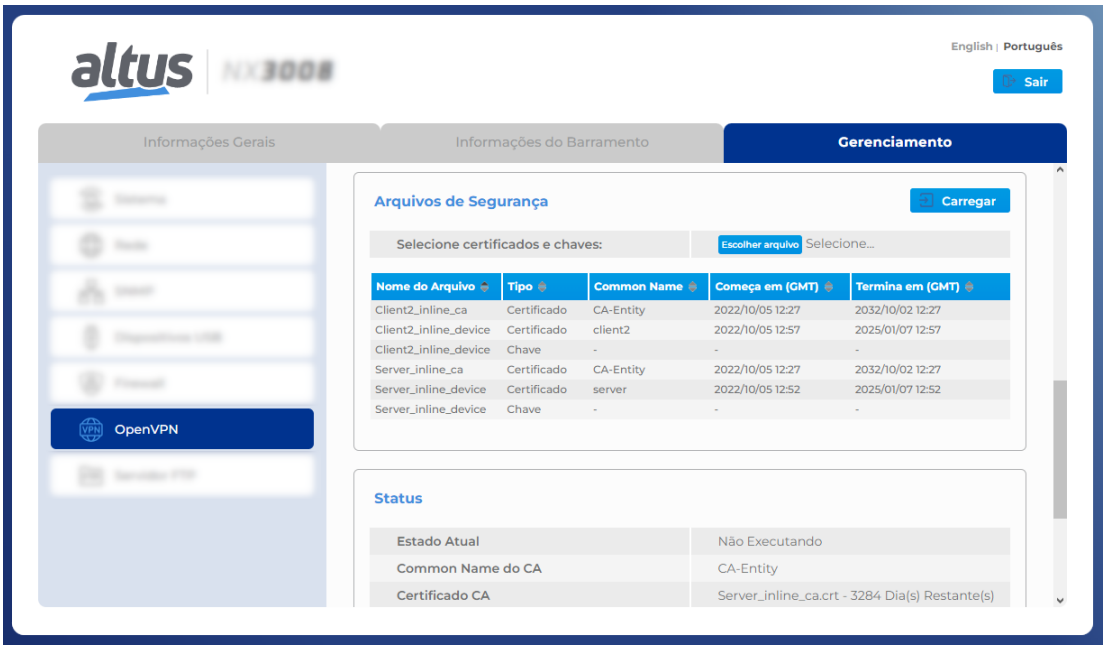


Figura 60: Tabela de Arquivos de Segurança OpenVPN

Nesta seção da Página Web de Sistema é possível realizar o gerenciamento dos arquivos de segurança. É possível realizar a importação de arquivos, monitorar a validade dos certificados, realizar o download dos arquivos carregados no dispositivo e excluir os arquivos que foram carregados.

Ao clicar no botão *Escolher arquivos*, é possível realizar importação de certificados e chaves, estes arquivos devem estar com as respectivas extensões *.crt* e *.key*. Este botão abre uma janela do explorador de arquivos e permite a seleção de um ficheiro, ou seja, múltiplos arquivos.

ATENÇÃO

Há um limite de importação de 12 arquivos para o controlador.

O controle dos arquivos é feito na tabela, que é mostrada na figura acima. Esta tabela adiciona novos itens, ou remove, conforme forem ocorrendo as operações de importar, ou de excluir arquivos. É possível identificar se o arquivo é uma chave ou um certificado através do segundo item da lista, o *Tipo*, que indica o que é aquele arquivo. Para os certificados, também são exibidos os seus *commons names* e as suas datas de validade, tanto de início, quanto de expiração.

É possível recuperar um arquivo que foi importado para a peça e, também, exclui-lo. Quando é arrastado o mouse sobre um arquivo da tabela, são exibidos dois botões, um para o download e outro para a exclusão.

6.8.4. Tabela de Status

Desenvolvida para permitir um monitoramento de dados, a tabela de status do OpenVPN se expande de forma automática, conforme é alterado alguma configuração e exibe diversos dados sobre a conexão, como o estado da VPN, o IP de VPN atribuído àquele dispositivo, os dados trafegados e os arquivos de segurança que estão sendo utilizados na comunicação.

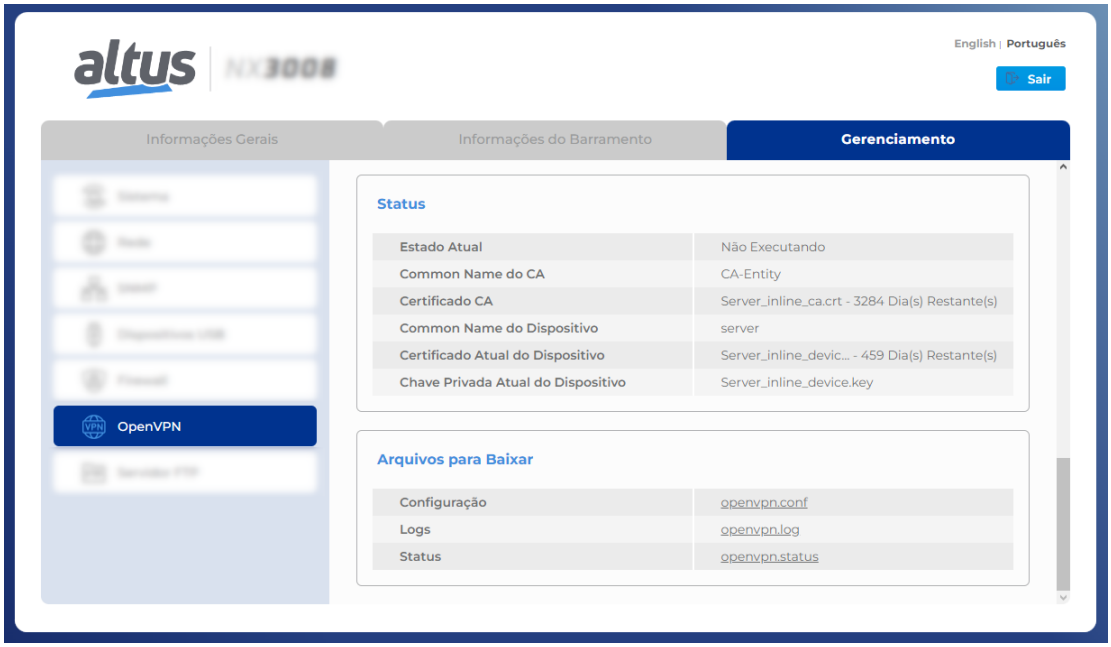


Figura 61: Tabela de Status OpenVPN com Funcionalidade Desativada

Quando a VPN está desativada, a tabela possui poucos parâmetros. O campo *Estado Atual* indica se a VPN está ativada ou não, e os demais campos exibem qual os certificados e chaves que estão configurados para a comunicação da VPN. Caso não tenha sido selecionado algum dos arquivos de segurança, no lugar do seu nome será exibido o caractere "-", indicando que não há um arquivo configurado.

Os campos de common name, tanto do CA quanto do dispositivo, exibem os commons names dados aos respectivos certificados, de autoridade certificadora e de dispositivo.

Ao lado do nome do arquivo, de cada certificado, é exibido o tempo restante, *em dias*, até a data da sua expiração.

Figura 62: Tabela de Status OpenVPN com Funcionalidade Ativada

Quando a funcionalidade é ativada e as configurações são aplicadas no dispositivo, a tabela tem as suas células dinamicamente modificadas para que as demais informações sejam exibidas. As informações sobre o estado da conexão do OpenVPN, podem ser consultadas nos dois primeiros tópicos da lista.

O item *Estado Atual* possuí os estados de *Não Executando*, *Iniciando serviço...* e *Executando*, que indicam, respectivamente, que a VPN esta desativada, que está iniciando, e que ela está ativada.

O item *Estado da Conexão* possuí os estados de *Não conectado*, *Conectando...* e *Conectado*.

As demais informações que podem ser obtidas nesta tabela são, o tempo total de conexão, o endereço IP do dispositivo e as quantidades de dados enviados e recebidos, em bytes. O status de quantos clientes estão atualmente conectados, somente é exibido quando a OpenVPN estiver operando como um servidor.

6.8.5. Arquivos para Baixar

É possível conferir as informações geradas pelo OpenVPN, através de arquivos de status e de log. A lista de arquivos para download somente é exibida quando há algum arquivo para ser baixado, caso não exista nenhum, a mensagem "Nenhum arquivo encontrado no controlador!"é exibida. Ao clicar sobre qualquer um dos links, será realizado o download do arquivo solicitado, através do navegador.

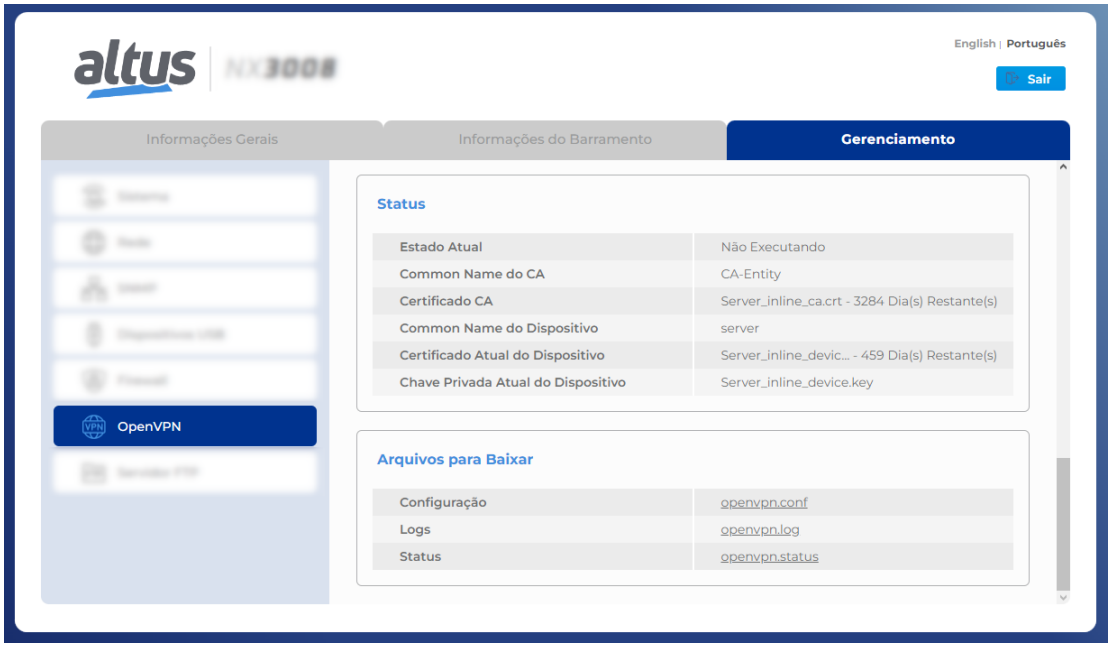


Figura 63: Seção de Downloads OpenVPN

6.8.6. Configuração de Arquiteturas

Nesta seção serão abordadas algumas possibilidades de configurações para o OpenVPN, como as arquiteturas Host-to-Host, Host-to-Site e Site-to-Site.

6.8.6.1. Host-to-Host

Figura 64: Exemplo de arquitetura Host-to-Host

Esta topologia permite a conexão entre dois hosts VPN. Ambos os hosts podem ser escolhidos para serem configurados como o servidor, logo, o outro deverá ser configurado como cliente, ou ainda, ambos os hosts podem ser configurados como clientes e haver um terceiro host que será o servidor da rede VPN.

A configuração deste tipo de arquitetura não exige nenhuma configuração específica, ou seja, não há restrição quanto às configurações disponíveis na seção *OpenVPN* da Página Web de Sistema.

6.8.6.2. Host-to-Site

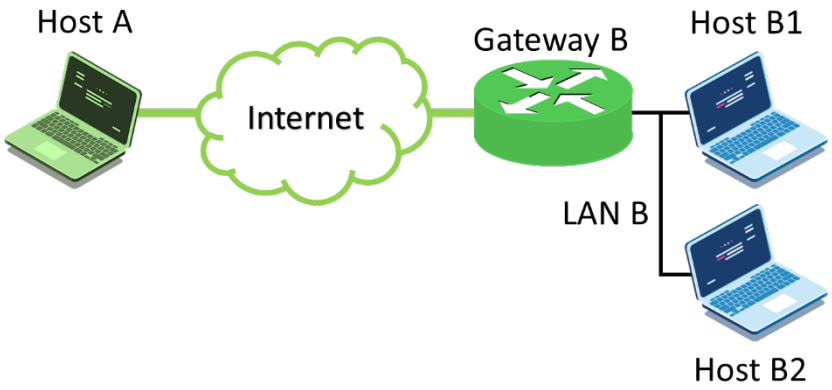


Figura 65: Exemplo de topologia Host-to-Site

Esta topologia permite a conexão entre dois hosts VPN, porém, um destes hosts atua também como um gateway para a rede VPN. Através deste gateway é realizado o roteamento para que seja estabelecida a comunicação entre os hosts A, B1, B2 e Gateway B. Neste cenário, tanto o Host A, quanto o Gateway B podem assumir o papel de servidor, sendo que, quando um é o servidor da rede, o outro será o cliente.

Os hosts, B1 e B2, que estão em uma rede privada Lan B, abaixo do Gateway B, não precisam ter suporte ao OpenVPN para conseguir se comunicar, pois, toda a comunicação é gerida pelo gateway da rede VPN.

Para que a comunicação entre todos os dispositivos da rede seja possível, é necessário criar regras de roteamento para o túnel da VPN. Consultar a seção Redes Privadas para verificar como criar regras de redes privadas.

Esta arquitetura de conexão VPN exige algumas configurações específicas. É necessário que o servidor tenha a sua configuração de topologia como subnet, sendo esta a configuração padrão do controlador, para que seja possível configurar as redes privadas abaixo do Gateway B, conforme observado na imagem acima.

Também é preciso informar o endereço da rede privada, Lan B, que estará realizando a comunicação através da VPN. Esta configuração é feita utilizando o comando *push "route IP_da_Lan_B Mascara_da_Lan_B"*, e é obrigatória independente se a rede privada está localizada a baixo do cliente ou do servidor do OpenVPN, porém, caso a rede privada esteja abaixo do cliente VPN, é necessário adicionar, além deste comando, a seguinte configuração: *route IP_da_Lan_B Mascara_da_Lan_B*. O comando *route* informa o servidor sobre qual é a rede privada que está conectada a rede da VPN e o comando utilizando o *push* faz com que os clientes daquele servidor VPN obtenham a mesma informação. Estas configurações são escritas no arquivo de configuração do servidor VPN.

6.8.6.3. Site-to-Site

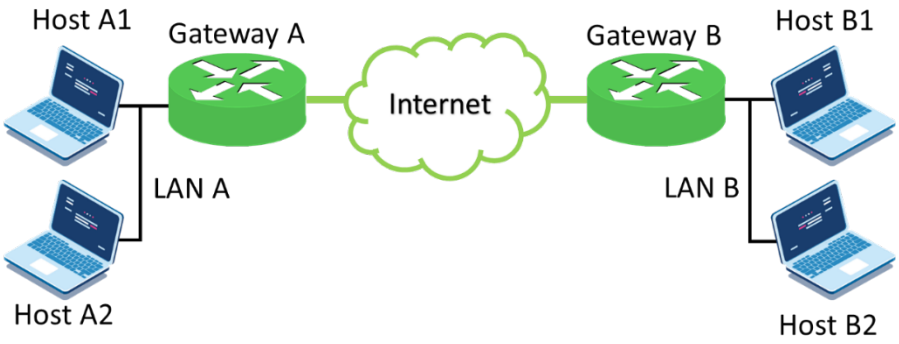


Figura 66: Exemplo de topologia Site-to-Site

Esta topologia permite a conexão entre dois hosts VPN, sendo que ambos atuam como gateways para a rede VPN. Através destes gateways é realizado o acesso para que seja estabelecida a comunicação entre os hosts A1, A2, B1, B2, Gateway A e Gateway B. Neste cenário, qualquer gateway pode assumir o papel de servidor, logo, o outro será o cliente.

Nenhum dos hosts que estão em uma rede privada, abaixo de um dos dois gateways, precisam ter suporte ao OpenVPN para conseguir se comunicar, pois, toda a comunicação é gerida pelos gateways da rede VPN.

Para que a comunicação entre todos os dispositivos da rede seja possível, é necessário criar regras de roteamento para o túnel da VPN. Consultar a seção Redes Privadas para verificar como criar regras de redes privadas.

As configurações para esta arquitetura precisam das mesmas configurações específicas descritas na seção Host-to-Site, com a diferença de que, nesta existem duas redes privadas e as duas devem seguir a configuração que foi demonstrada. Admitindo que o Gateway A é o servidor nesta conexão, deve ser adicionado os seguintes comandos ao arquivo de configuração: *push "route IP_da_Lan_A Mascara_da_Lan_A"*, *route IP_da_Lan_B Mascara_da_Lan_B* e *push "route IP_da_Lan_B Mascara_da_Lan_B"*. Caso o servidor seja o Gateway B, no arquivo de configuração seria adicionado: *push "route IP_da_Lan_B Mascara_da_Lan_B"*, *route IP_da_Lan_A Mascara_da_Lan_A* e *push "route IP_da_Lan_A Mascara_da_Lan_A"*.

6.9. Servidor OPC UA Seguro

RC 3.1 da norma IEC 62443-4-2

OPC UA é um protocolo de comunicação industrial para interoperabilidade desenvolvido pela OPC Foundation. O MasterTool é equipado com uma funcionalidade de servidor OPC UA para fornecer acesso ao controlador e sua aplicação. Várias medidas de segurança são fornecidas como: um servidor OPC UA operante com uma comunicação criptografada baseada em certificados X.509 e atuando com acesso a um conjunto de símbolos específico ao usuário, garantindo uma maior confidencialidade aos dados que são trocados com os clientes conectados.

6.9.1. Servidor OPC UA: Gerenciamento de usuários disponível

RC 2.1 da norma IEC 62443-4-2

Adicionando o objeto *Configuração de Símbolos* ao projeto para comunicação OPC, pode-se criar subconjuntos de todos os símbolos definidos (symbolSets). Na janela da *configuração de símbolos*, no menu *Configurações*, pode-se ativar os conjuntos de símbolos, como indicano na figura 67.

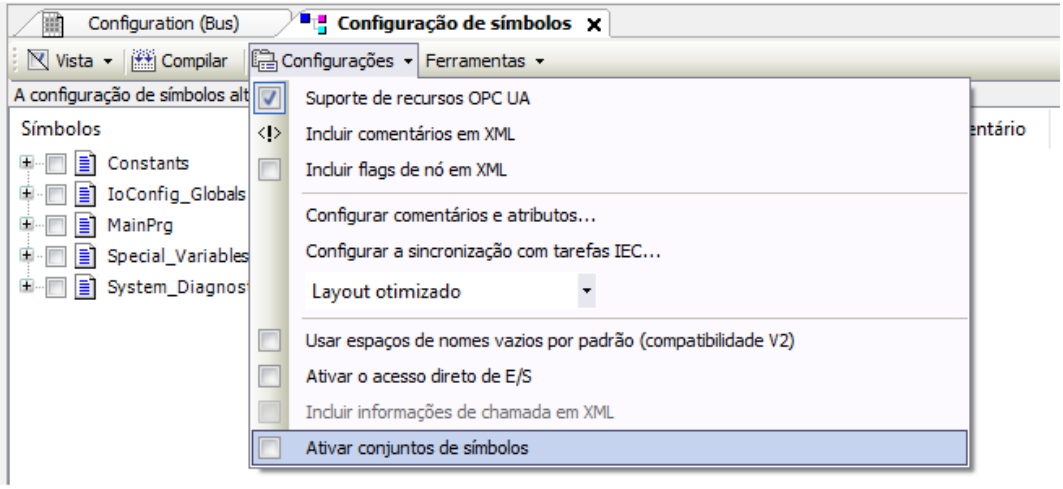


Figura 67: Ativando os conjuntos de símbolos.

Após ativado, um novo conjunto de símbolos pode ser criado pelo botão "+", mostrado na Figura 68.

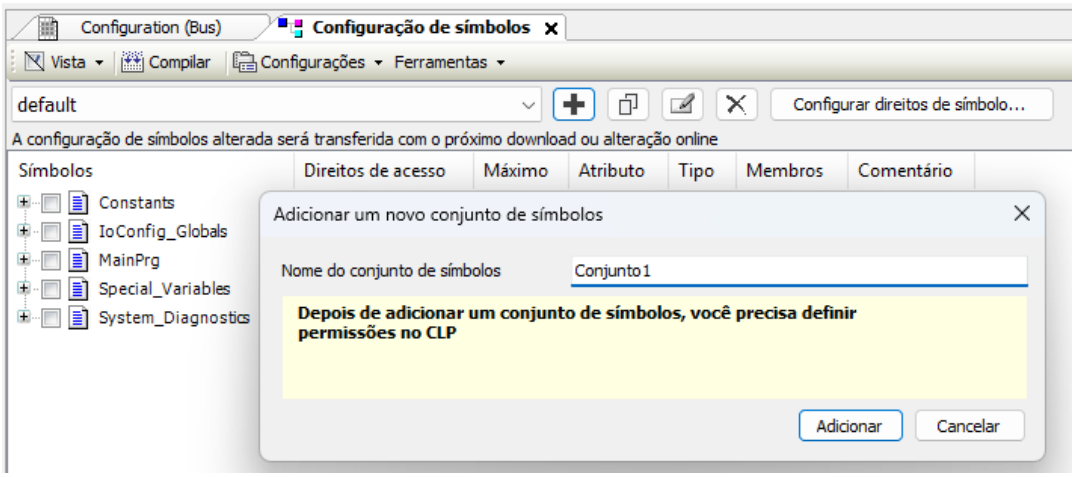


Figura 68: Criando um novo conjunto de símbolos.

Na lista de símbolos, podem ser selecionados os que deseja incluir no grupo. Com um gerenciamento de usuário ativado, esses conjuntos de símbolos podem ser atribuídos a usuários dedicados para visibilidade e determinação dos direitos de acesso de escrita/leitura, protegendo a confidencialidade dos dados que são trocados com os clientes conectados. Isso é realizado após a criação do subconjunto de símbolos, pelo botão *Configurar direitos de símbolo...*, nas abas *Usuário e Grupos* e *Direitos de Acesso*. Mais informações a respeito de Gerenciamento de usuários e direitos de acesso no capítulo 6.1

6.9.2. Servidor OPC UA: Suporte à comunicação baseada em certificados X.509 RC 3.1 da norma IEC 62443-4-2

Uma das funcionalidades do Servidor OPC UA é operar com uma comunicação criptografada baseada em certificados X.509. Os diferentes perfis de segurança são definidos pela Fundação OPC.

Dependendo do perfil, isso protege a integridade (apenas para perfis assinados) ou a integridade e confidencialidade (para perfis assinados e criptografados) dos dados trocados com os clientes conectados.

Essa medida protege a confidencialidade dos dados trocados com os clientes conectados.

Para verificar as configurações de certificados, deve-se acessar *Visualizar* > *Tela de Segurança* Se desejado, o usuário pode configurar criptografia para a comunicação OPC UA usando o perfil *Basic256SHA256*, para obter uma conexão segura (segurança cibernética).

Para configurar a criptografia num servidor OPC UA deve-se criar um certificado para o mesmo, executando os seguintes passos no programador Mastertool:

1. Definir um caminho ativo para comunicação com o controlador (não é necessário fazer login);
2. No menu *Visualizar*, selecionar *Tela de Segurança*;
3. Clicar na aba *Devices* no lado esquerdo desta tela;
4. Clicar no ícone  para executar um refresh;
5. Clicar no ícone *Device*, abaixo do qual se abrirão diversas pastas de certificados (*Own Certificates, Trusted Certificates, Untrusted Certificates, Quarantined Certificates*);
6. Clicar no ícone  para gerar um certificado e selecione os seguintes parâmetros:
   - *Key length* (bit): 3072
   - *Validity period* (days): 365 (pode ser modificado se desejado)
7. Aguarde enquanto o certificado é calculado e transferido para o controlador (isso pode levar alguns minutos);
8. Reinicialize (desligue e religue) o controlador.
9. No cliente OPC UA, execute os procedimentos necessários para se conectar ao servidor OPC UA e gerar um certificado com o perfil *Basic256Sha256* (ver manual do cliente OPC UA específico para detalhes);
10. De volta ao Mastertool, clique no ícone  da *Tela de Segurança* para executar um refresh;
11. Na *Tela de Segurança*, selecione a pasta "*Quarantined Certificates*"abaixo do *Device*. No painel direito deve-se observar um certificado solicitado pelo cliente OPC UA;
12. Arraste este certificado para a pasta "*Trusted Certificates*";
13. Prossiga as configurações no cliente OPC UA (ver manual do cliente OPC UA específico para detalhes).

Para remover a criptografia previamente configurada num controlador, deve-se seguir o seguinte procedimento:

1. Definir um caminho ativo para comunicação com o controlador (não é necessário fazer login);
2. No menu *Visualizar*, selecionar *Tela de Segurança*;
3. Clicar na aba *Devices* no lado esquerdo desta tela;
4. Clicar no ícone  para executar um refresh;
5. Clicar no *Device*, abaixo do qual se abrem diversas pastas de certificados (*Own Certificates, Trusted Certificates, Untrusted Certificates, Quarantined Certificates*);
6. Clicar na pasta "*Own Certificates*", e no painel direito selecionar o certificado (OPC UA Server);
7. Clicar no ícone  para remover este certificado do projeto e do controlador;
8. Reinicialize (desligue e religue) o controlador.

6.10. Gerenciamento de Recursos

RC 7.2 da norma IEC 62443-4-2

Para equipamentos com múltiplas interfaces de comunicação, é possível desativar algumas delas através do Mastertool, caso desejado. No entanto, é fundamental que pelo menos uma interface permaneça ativa para garantir a comunicação do usuário com o controlador.

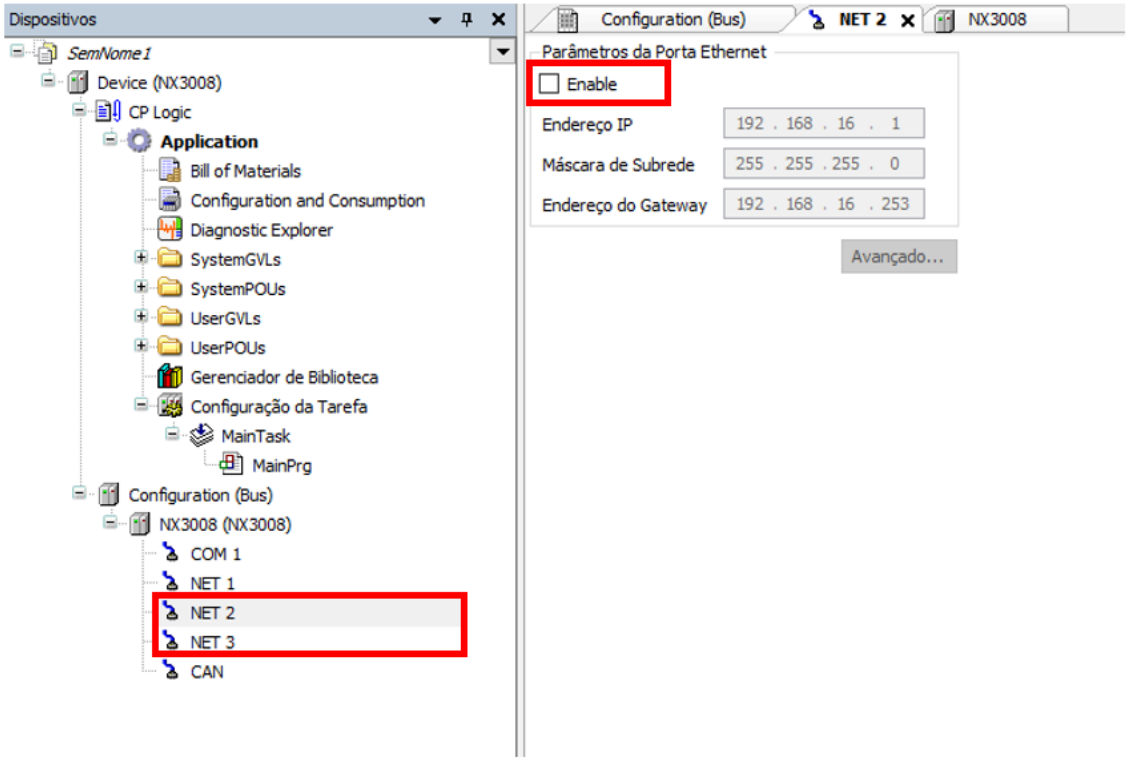


Figura 69: Desativando interfaces de rede

A tabela 4 indica as portas TCP reservadas dos equipamentos. Elas ficam abertas somente quando o protocolo correspondente estiver em uso, caso contrário se mantem fechadas.

6.11. Recuperação do sistema

RC 7.4 da norma IEC 62443-4-2

Os componentes apresentam a capacidade de recuperação para um estado conhecido após ocorrência de falhas a partir da realização de procedimentos que visam salvar dados e configurações. Isso deve ser feito pelo usuário em um momento que o sistema esteja em pleno funcionamento. Dessa forma, criando um backup completo do projeto.

6.11.1. Configurações de usuários

A exportação das permissões de usuário e direitos de acesso do projeto é feita a partir do menu *Projeto* > *Gerenciamento de Usuário* > *Permissões*. Ao clicar sobre *Exportar/Importar* e depois em *Exportar todas permissões...*, o Mastertool gerará um arquivo contendo as configurações.

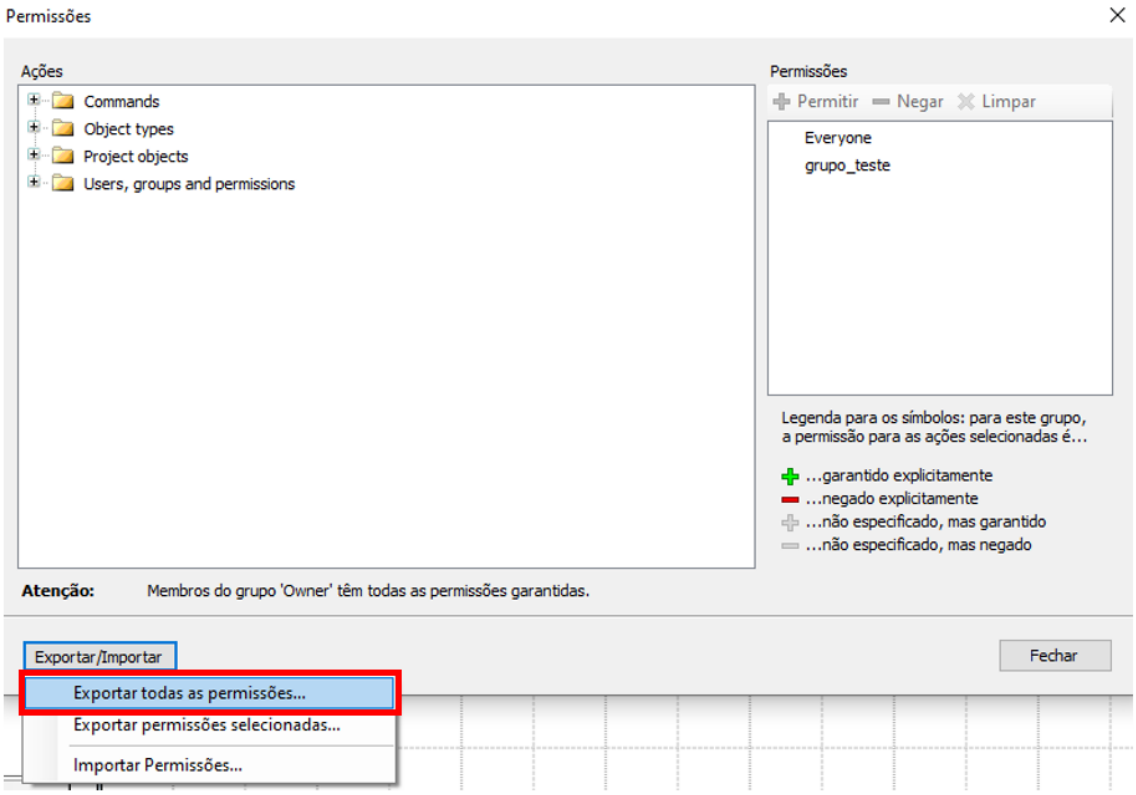


Figura 70: Exportando permissões do usuário

Para fazer a importação dessas permissões no projeto, deve-se acessar o mesmo menu, mas clicar em *Importar Permissões*.

6.11.2. Exportação de dados online

É possível exportar os valores das variáveis online a partir do menu *Comunicação* > *Exportar variáveis online*. Este comando criará um arquivo (salvo no mesmo diretório do projeto) contendo todos os valores das variáveis online.

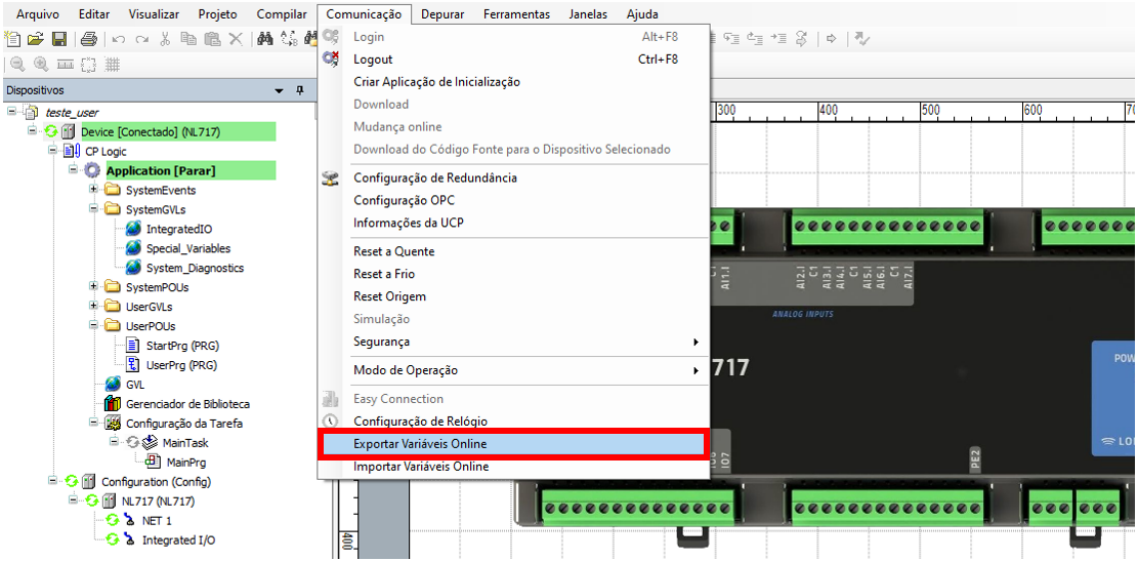


Figura 71: Exportando permissões do usuário

6.11.3. Exportação de dados de configuração

É possível realizar a exportação de algumas configuração a partir da página web do dispositivo. Ao clicar no botão *Exportar* disponível na página. Isso irá gerar um arquivo *.txt* que contem as configurações daquela funcionalidade. Isso pode ser armazenado em backup e, em caso de necessidade, importado novamente para o PLC.

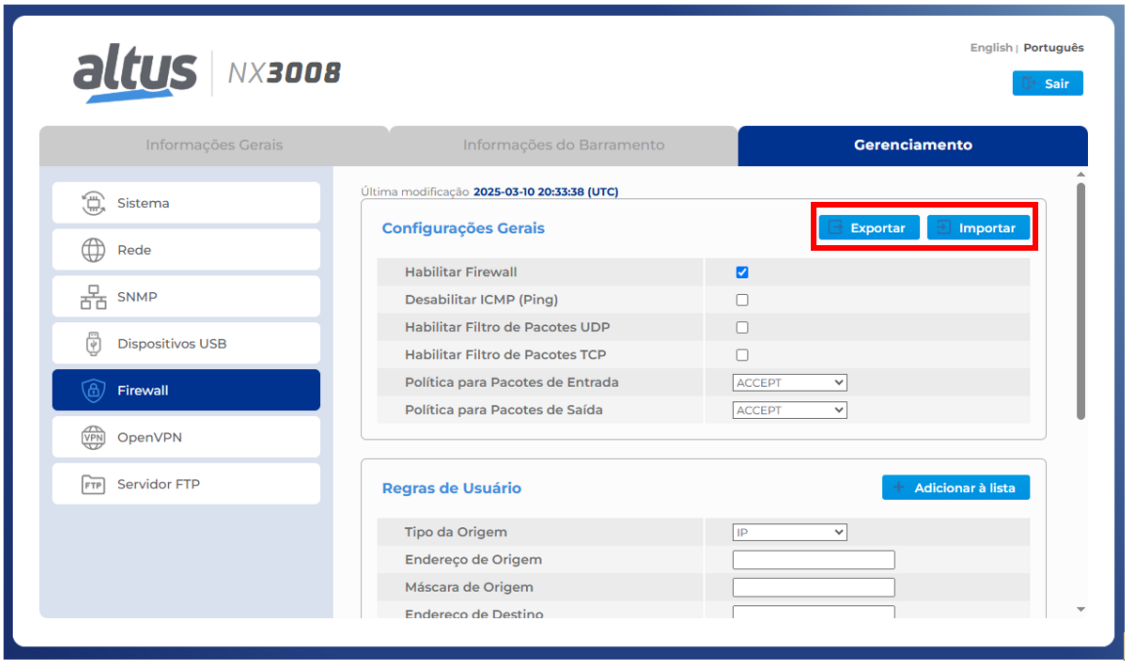


Figura 72: Exportando permissões do usuário

Também é possível realizar o mesmo procedimento para *Dispositivos USB*.

6.11.4. Exportar Firmware

Informações a respeito de backup do firmware do dispositivo estão contidas no capítulo 5.10.

6.12. Possíveis fontes de riscos

Conectar o dispositivo à internet sem a configuração adequada de Firewall e VPN apresenta grandes riscos. A porta Host USB presente nos controladores de algumas séries permite ampliar as funcionalidades do controlador utilizando diversos tipos de dongles USB, incluindo modems com chip SIM e adaptadores WiFi. Para dispositivos em bridge ou roteadores com acesso externo ativado (encaminhamento de porta), uma vez conectado à Internet, qualquer pessoa que conheça o endereço IP do modem poderá acessar o controlador remotamente. Portanto, por motivos de segurança, é extremamente importante e recomendado configurar os Direitos do Usuário no controlador para restringir as operações online do MasterTool IEC XE com login e senha. Por meio da página Web de gerenciamento, pode-se, inclusive, parar o controlador, o que é um risco para a segurança não apenas cibernética, mas também física dos funcionários e ativos.

6.13. Portas TCP/UDP Reservadas

As seguintes portas TCP/UDP das interfaces Ethernet, tanto locais quanto remotas, são tipicamente utilizadas por serviços da UCP (dependem da disponibilidade conforme manual do CP) e, portanto, são reservadas e não devem ser utilizadas pelo usuário.

Serviço	TCP	UDP
Página Web de Sistema	80	-
SNTP	-	123
SNMP	-	161
MODBUS TCP	502*	-
Mastertool	1217*	1740:1743
SQL Server	1433	-
MQTT	1883* / 8883*	-
EtherNet/IP	44818	2222
IEC 60870-5-104	2404*	-
IEC 61850	102*	-
DNP3	20000* / 20005*	-
OPC UA	4840	-
WEBVISU	8080	-
CODESYS ARTI	11740	-
PROFINET	-	34964
Portainer Docker	9000	-
SysLog	-	514
LibHART	1234	-

Tabela 4: Portas TCP/UDP reservadas

* Porta padrão, mas que pode ser alterada pelo usuário.

7. Atendimento da IEC 62443-4-2

A norma IEC 62443-4-2 determina requisitos de cibersegurança para componentes em sistemas de controle e automação industrial. Nela são abordados todos os componentes do sistema, como, por exemplo, aplicações de software, dispositivos de rede, dispositivos embarcados e servidores host.

Os componentes são compilados em quatro grupos, com contramedidas progressivas que buscam proteger a aplicação contra diferentes níveis de ataque. O primeiro grupo, chamado SL-1, busca proteger a aplicação contra erros acidentais, enquanto o quarto grupo, chamado SL-4, busca proteger a infraestrutura contra ataques direcionados e sofisticados.

Ao longo deste documento estão descritos apenas os que se aplicam a dispositivos embarcados (CR e EDR), que é o caso dos PLCs e demais produtos Altus.

Entretanto, na tabela abaixo, estão listados todos os requisitos da norma, incluindo os que não se aplicam ou não são atendidos. Aqueles que são atendidos estão com uma referencia à seção onde podem ser encontrados.

Requisito de Componente	**Nível de Proteção**	**Seção**
FR 1 - Controle de identificação e autenticação (IAC)		
CR 1.1 - Identificação e autenticação de usuários humanos	1	5.1.1, 6.1
RE (1) Identificação e autenticação únicos	2	5.1.1, 6.1
RE (2) Autenticação multifator para todas as interfaces	3	
CR 1.2 - Identificação e autenticação de processos de software e dispositivos	2	5.2
RE (1) Identificação e autenticação únicos	3	5.2
CR 1.3 - Gestão de contas	1	5.1.1, 6.1
CR 1.4 - Gestão de identificadores	1	5.1.1, 6.1, 6.1.3
CR 1.5 - Gestão de autenticadores	1	5.1.1, 6.1, 6.1.3
RE (1) Segurança de hardware para autenticadores	3	
NDR 1.6 - Gestão de acesso sem fio	1	N/A
RE (1) Identificação e autenticação únicos	2	N/A
CR 1.7 - Força da autenticação baseada em senha	1	5.1.1, 6.1
RE (1) Geração de senhas e restrições de tempo de vida para usuários humanos	3	
RE (2) Restrições de tempo de vida de senha para todos os usuários	4	
CR 1.8 - Certificados de infraestrutura de chave pública	2	5.4
CR 1.9 - Força da autenticação baseada em chave pública	2	
RE (1) Segurança de hardware para autenticação baseada em chave pública	3	
CR 1.10 - Feedback do autenticador	1	5.1.1
CR 1.11 - Tentativas de login malsucedidas	1	5.1.1
CR 1.12 - Notificação de uso do sistema	1	
NDR 1.13 - Acesso via redes não confiáveis	1	N/A
RE (1) Aprovação explícita de solicitação de acesso	3	N/A
CR 1.14 - Força da autenticação baseada em chave simétrica	2	
RE (1) Segurança de hardware para autenticação baseada em chave simétrica	3	
FR2 - Controle de uso (UC)		
CR 2.1 - Imposição de autorização	1	5.1.1, 5.1.2, 6.9.1, 6.1, 6.9.1
RE (1) Impor de autorização para todos os usuários	2	5.1.1, 5.1.2, 6.9.1, 6.1, 6.9.1
RE (2) Mapeamento de permissões para funções	2	5.1.1, 5.1.2, 6.9.1, 6.1, 6.9.1
RE (3) Sobrescrição do supervisor	3	
RE (4) Aprovação dupla	4	
CR 2.2 - Controle de uso sem fio	1	5.1.2, 6.9.1,6.9.1

Requisito de Componente	Nível de Proteção	Seção
CR 2.3 - Controle de uso para dispositivos portáteis e móveis	-	N/A
SAR 2.4 - Código móvel	1	N/A
RE (1) Verificação de autenticidade do código móvel	2	N/A
EDR 2.4 - Código móvel	1	N/A
RE (1) Verificação de autenticidade do código móvel	2	N/A
HDR 2.4 - Código móvel	1	N/A
RE (1) Verificação de autenticidade do código móvel	2	N/A
NDR 2.4 - Código móvel	1	N/A
RE (1) Verificação de autenticidade do código móvel	2	N/A
CR 2.5 - Bloqueio de sessão	1	5.1.1
CR 2.6 - Encerramento de sessão remota	1	5.1
CR 2.7 - Controle de sessões simultâneas	3	
CR 2.8 - Eventos auditáveis	1	5.7
CR 2.9 - Capacidade de armazenamento de auditoria	1	5.7, 6.3, 6.4
RE (1) Aviso quando o limite de capacidade de armazenamento de registros de auditoria for atingido	3	5.7, 6.3
CR 2.10 - Resposta a falhas no processamento de auditoria	1	5.7
CR 2.11 - Carimbos de tempo	1	5.7
RE (1) Sincronização de tempo	2	5.7
RE (2) Proteção da integridade da fonte de tempo	4	5.7
CR 2.12 - Não repúdio	1	5.7
RE (1) Não repúdio para todos os usuários	4	
EDR 2.13 - Uso de interfaces de teste e diagnóstico físico	2	
RE (1) Monitoramento ativo	3	
HDR 2.13 - Uso de interfaces de teste e diagnóstico físico	2	N/A
RE (1) Monitoramento ativo	3	N/A
NDR 2.13 - Uso de interfaces de teste e diagnóstico físico	2	N/A
RE (1) Monitoramento ativo	3	N/A
FR3 - Integridade do sistema (SI)		
CR 3.1 - Integridade da comunicação	1	5.3, 6.9, 6.9.2
RE (1) Autenticação de comunicação	2	
SAR 3.2 - Proteção contra código malicioso	1	N/A
EDR 3.2 - Proteção contra código malicioso	1	5.12
HDR 3.2 - Proteção contra código malicioso	1	N/A
RE (1) Relatório da versão da proteção de código	2	N/A
NDR 3.2 - Proteção contra código malicioso	1	N/A
CR 3.3 - Verificação da funcionalidade de segurança	1	5.1.1, 5.7
RE (1) Verificação da funcionalidade de segurança durante a operação normal	4	5.7
CR 3.4 - Integridade de software e informações	1	5.7
RE (1) Autenticidade de software e informações	2	
RE (2) Notificações automatizadas de violações de integridade	3	
CR 3.5 - Validação de entrada	1	5.7
CR 3.6 - Saída determinística	1	5.8
CR 3.7 - Tratamento de erros	1	5.9
CR 3.8 - Integridade da sessão	2	
CR 3.9 - Proteção das informações de auditoria	2	
RE (1) - registros de auditoria em mídia de escrita única	4	6.3
EDR 3.10 - Suporte para atualizações	1	6.5.1
RE (1) - Autenticidade e integridade das atualizações	2	6.5.1
HDR 3.10 - Suporte para atualizações	1	N/A
RE (1) - Autenticidade e integridade das atualizações	2	N/A
NDR 3.10 - Suporte para atualizações	1	N/A
RE (1) - Autenticidade e integridade das atualizações	2	N/A
EDR 3.11 - Resistência e detecção de adulteração física	2	
RE (1) Notificação de tentativa de adulteração	3	
HDR 3.11 - Resistência e detecção de adulteração física	2	N/A
RE (1) Notificação de tentativa de adulteração	3	N/A
NDR 3.11 - Resistência e detecção de adulteração física	2	N/A
RE (1) Notificação de tentativa de adulteração	3	N/A

Requisito de Componente	Nível de Proteção	Seção
EDR 3.12 - Provisionamento de raízes de confiança do fornecedor de produtos	2	
HDR 3.12 - Provisionamento de raízes de confiança do fornecedor de produtos	2	N/A
NDR 3.12 - Provisionamento de raízes de confiança do fornecedor de produtos	2	N/A
EDR 3.13 - Provisionamento de raízes de confiança do proprietário de ativos	2	
HDR 3.13 - Provisionamento de raízes de confiança do proprietário de ativos	2	N/A
NDR 3.13 - Provisionamento de raízes de confiança do proprietário de ativos	2	N/A
EDR 3.14 - Integridade do processo de inicialização	1	
RE (1) Autenticidade do processo de inicialização	2	
HDR 3.14 - Integridade do processo de inicialização	1	N/A
RE (1) Autenticidade do processo de inicialização	2	N/A
NDR 3.14 - Integridade do processo de inicialização	1	N/A
RE (1) Autenticidade do processo de inicialização	2	N/A
FR4 - Confidencialidade de dados (DC)		
CR 4.1 - Confidencialidade das informações	1	5.4, 5.5, 5.6
CR 4.2 - Persistência das informações	2	
RE (1) Apagar recursos de memória compartilhada	3	
RE (2) Verificação de apagamento	3	
CR 4.3 - Uso de criptografia	1	5.4, 5.13
FR5 - Fluxo de dados restrito (RDF)		
CR 5.1 - Segmentação de rede	1	6.8, 6.7
NDR 5.2 - Proteção de fronteira de zona	1	N/A
RE (1) Negar tudo, permitir por exceção	2	N/A
RE (2) Modo ilha	3	N/A
RE (3) Falha de fechamento	3	N/A
NDR 5.3 - Restrições de comunicação geral, pessoa a pessoa	1	N/A
FR6 - Resposta oportuna a eventos (TRE)		
CR 6.1 - Acessibilidade do registro de auditoria	1	5.7
RE (1) Acesso programático aos registros de auditoria	3	
CR 6.2 - Monitoramento contínuo	2	
FR7 - Disponibilidade de recursos (RA)		
CR 7.1 - Proteção contra negação de serviço	1	6.2
RE (1) Gerenciar carga de comunicação do componente	2	
CR 7.2 - Gestão de recursos	1	6.10
CR 7.3 - Backup do sistema de controle	1	5.10
RE (1) Verificação da integridade do backup	2	
CR 7.4 - Recuperação e reconstrução do sistema de controle	1	6.11
CR 7.5 - Energia de emergência	-	
CR 7.6 - Configurações de rede e segurança	1	6.5
RE (1) Relatórios legíveis por máquina das configurações atuais de segurança	3	
CR 7.7 - Funcionalidade mínima	1	6.10
CR 7.8 - Inventário de componentes do sistema de controle	2	5.11

Tabela 5: Tabela de atendimento da norma IEC 62443-4-2

7.1. Nível de Segurança 1

O Nível de Segurança 1 (SL-1) define os componentes básicos para prevenir o compartilhamento não autorizado de informações por interceptação (eavesdropping) ou exposição acidental.

Um dos requisitos deste nível que não é atendido é o CR 1.12, que determina que o sistema deve exibir uma notificação antes da autenticação do usuário e, além disso, permita que o administrador possa configurar a mensagem. Atualmente, os produtos exibem uma tela de confirmação de login mas que, no entanto, não é customizável como requer a norma.

Outro requisito que não é atendido é o EDR 3.14, onde a norma exige que o dispositivo realize uma verificação de integridade dos arquivos de firmware, software e configuração antes da inicialização. Esta ferramenta está atualmente em desenvolvimento, mas ainda não foi implementada.

O percentual de atendimento deste nível de segurança é de 94% (34 dos 36 requisitos).

7.2. Nível de Segurança 2

O nível de segurança 2 (SL-2) agrega as contramedidas do SL-1 e define componentes adicionais para prevenir o compartilhamento não autorizado de informações para uma entidade procurando ativamente com métodos simples, poucos recursos, habilidades genéricas e baixa motivação.

Para atingimento completo do nível 2 de segurança da norma, são propostos 22 requisitos, 7 são atendidos, totalizando 32% de atendimento.

Os requisitos não atendidos tratam, principalmente, de funcionalidades relacionadas com certificações de chaves públicas e integridade de arquivos internos do componentes, como firmware e configurações. De forma geral, para atendimento total deste nível de segurança, devem ser implementadas políticas mais avançadas de PKI, garantindo que os componentes realizem verificações mais robustas de certificados digitais. Isso inclui o uso de criptografia para validar a autenticidade e integridade dos certificados, aumentando a proteção contra ataques

Os requisitos não atendidos são:

1) CR 1.9
2) CR 1.14
3) EDR 2.13
4) CR 3.1 RE(1)
5) CR 3.4 RE(1)
6) CR 3.8
7) CR 3.9
8) EDR 3.11
9) EDR 3.12
10) EDR 3.13
11) EDR 3.14 RE(1)
12) CR 4.2
13) CR 6.2
14) CR 7.1 RE(1)
15) CR 7.3 RE(1)

7.3. Nível de Segurança 3

O nível de segurança 3 (SL-3) agrega as contramedidas do SL-1 e SL-2 e define componentes adicionais para prevenir o compartilhamento não autorizado de informações para uma entidade procurando ativamente com métodos sofisticados, recursos moderados, habilidades IACS (*Industrial Automation and Control Systems*) específicas e motivação moderada.

Para atingir o nível 3 de segurança da norma IEC62443-4-2, o componente deve satisfazer 16 requisitos. Por se tratarem de exigências mais robustas, apenas 2 destes são atendidos, totalizando 12,5%.

7.4. Nível de Segurança 4

O nível de segurança 4 (SL-4) agrega as contramedidas do SL-1, SL-2 e SL-3 e define componentes adicionais para prevenir o compartilhamento não autorizado de informações para uma entidade procurando ativamente com métodos sofisticados, recursos extensos, habilidades IACS específicas e alta motivação.

Dos 7 requisitos apresentados pela norma para este nível de segurança, 3 são atingidos atualmente, ou seja, 43%.

8. Adequação ao Manual de Procedimentos da Operação - ONS

Este capítulo demonstra a relação entre os produtos Altus e os requisitos do manual de "Rotina Operacional: Controles mínimos de segurança cibernética para o Ambiente Regulado Cibernético", do Operador Nacional do Sistema (ONS), a entidade responsável por controlar e coordenar a operação de geração e transmissão de energia elétrica no Brasil. Este documento se encontra no módulo 5 - Submódulo 5.13 do Manual de Procedimentos da Operação.

O objetivo deste manual é estabelecer os controles mínimos de segurança cibernética a serem implementados pelos agentes e pelo ONS no Ambiente Regulado Cibernético (ARCiber). A tabela a seguir apresenta as orientações propostas pelo ONS, acompanhadas de explicações sobre sua aplicação nos produtos Altus.

REQUISITO	COMENTÁRIO
4.1 Arquitetura tecnológica para o ambiente	
4.1.1 As redes devem ser segregadas em zonas de segurança, de acordo com a sua função. O agente deve definir uma arquitetura que segmente as redes minimamente em: a) Zona de Supervisão b) Zona DMZ Operativa c) Zona Corporativa	Considerando a separação em Zonas e Conduítes da ISA99 (IEC 62443) e o Purdue Reference Model, os dispositivos Altus serão instalados na Zona de Supervisão. Os dispositivos da Altus tem a capacidade de segregação necessária indicada nas especificações.
4.1.2 O ARCiber não deve ser diretamente acessível através da internet mesmo que protegido por um ou mais firewalls, bem como seus ativos.	Toda a rede pode ser acessada através de uma VPN única sem necessidade de características especificas do componente. Está no Roadmap da Altus implementar VPN para seus produtos no ano que vem. Mais informações a respeito de uso de VPN nos produtos Altus na seção 6.8.
4.1.3 O acesso ao ARCiber a partir de redes externas à organização (como, por exemplo, a internet) somente deve ser permitido para o desempenho de atividades autorizadas. Este acesso deve ser realizado por meio de Rede Privada Virtual (VPN), ou tecnologia similar, através de um gateway ou serviço que ofereça controles de segurança. a) Não devem ser visíveis nem ser acessíveis a partir da internet. b) Não devem ser capazes de se conectar com a internet.	
4.1.4 Soluções Antimalware devem ser implementadas no ARCiber e mantidas atualizadas. a) Soluções de application whitelisting podem ser implementadas como alternativa ou complemento às soluções Antimalware.	Não aplicável para os produtos.
4.2 Governança de segurança da informação	
4.2.1 Deve ser nomeado pelo menos um gestor e um suplente, responsáveis pela segurança cibernética do ARCiber e atuar como ponto de contato externo.	Estes requisitos se relacionam a processos, e, não necessariamente, tem ligação com funcionalidades dos produtos
4.2.2 Deve ser estabelecida política que defina papéis e responsabilidades em relação à segurança cibernética do ARCiber.	

REQUISITO	COMENTÁRIO
4.3 Inventário de ativos	
4.3.1 Todos os ativos, softwares e hardwares, conectados ao ARCiber devem ser inventariados minimamente a cada 24 meses e considerar minimamente: a) Tipo de dispositivo; b) Fabricante do equipamento; c) Função; d) Endereço IP ou MAC Address; e) Protocolo de aplicação e/ou porta de serviço; f) Versão do firmware e/ou sistema operacional;	Todas as informações são acessíveis via diagnósticos do equipamento.
4.3.2 O inventário dos ativos deve ser armazenado de forma segura, com políticas de armazenamento bem definidas, com acesso restrito às pessoas que necessitem das informações para o exercício de suas funções.	
4.3.3 Padrões de configuração segura (hardening) devem ser criados conforme política de segurança do agente para os sistemas operacionais, firmwares, banco de dados e demais versões de softwares existentes no ARCiber:	Conforme comentado o nosso produto é projetado não liberar portas, interfaces e protocolos não utilizados no sistema. Os recursos que podem ser e não são utilizados, são desabilitados. O sistema de arquivos do Sistema Operacional e do RTS (CoDeSys) também não são acessíveis ao usuário. A seção 6.10 apresenta mais informações a respeito do assunto.
4.4 Gestão de vulnerabilidades	
4.4.1 A política de segurança da organização deverá contemplar a gestão de pacotes de correção de segurança (patches) para todas as tecnologias conectadas ao ARCiber, contemplando no mínimo: a) Cronograma de implementação das correções; b) Mapeamento dos ativos inventariados para as atualizações disponibilizadas pelos fabricantes.	Os produtos Altus disponibilizam mecanismo de atualização de firmware (contendo todos os arquivos necessários ao sistema) que permite a correção de vulnerabilidades encontradas no equipamento. As atualizações estão disponíveis no site da Altus junto com histórico de revisões de produto (mais informações na seção 6.5.1). Está planejado a implementação de página de segurança da Altus onde as vulnerabilidades mapeadas serão publicadas.
4.4.2 Novos ativos somente deverão ser conectados ao ARCiber após a aplicação de todos os pacotes de correção de segurança disponíveis. a) Caso o novo equipamento esteja substituindo um equipamento existente que tenha apresentado defeito, a aplicação dos pacotes de correção de segurança poderá ser postergada, mas com prazo pré-definido.	A possibilidade de atualização dos equipamentos permite que os novos componentes sejam revisados e atualizados em bancada antes da instalação.
4.5 Gestão de Acessos	
4.5.1.1 Credenciais de acesso devem ser individuais e aprovadas pela alçada competente. Para os casos em que não seja possível implementar credenciais individuais, deve-se: a) Gerar e manter uma lista das pessoas autorizadas a usar as contas compartilhadas. b) Implementar os controles previstos em 4.5.1.6.	Informações a respeito de gerenciamento de usuários, login, senha estão contidos na seção 5.1

REQUISITO	COMENTÁRIO
4.5.1.2 Política de senhas que contemple: tamanho mínimo, complexidade, necessidade de ser diferente da senha padrão do fabricante, ações a serem tomadas caso um número máximo de tentativas de acesso malsucedidas seja atingido, e critérios para a gestão de mudanças (prazo, ocorrência de incidentes, etc). a) A política de senhas pode ser implementada por controles tecnológicos ou por procedimento. Caso as características de senha previstas na política não possam ser implementadas em determinados ativos devido à restrição tecnológica, deve-se implementar o nível máximo suportado pelo ativo.	Informações a respeito de gerenciamento de usuários, login, senha estão contidos na seção 5.1 e 6.1
4.5.1.3 Na construção dos perfis de acesso deve-se seguir o princípio de minimização (somente deve-se conceder o acesso mínimo necessário).	
4.5.1.4 Prazo máximo para cancelamento/remoção de credenciais de usuários desligados e de credenciais sem uso após um determinado tempo.	
4.5.1.5 Credenciais de acesso privilegiadas devem estar sujeitas a controles específicos, incluindo: a) Nível de aprovação adequado, com revisão periódica pelo gestor do ARCiber; b) Uso exclusivo durante a execução de tarefas administrativas; c) Monitoramento através de trilhas de auditoria; d) Utilização de múltiplos fatores de autenticação como, por exemplo, tokens OTP (one time password) ou reconhecimento biométrico.	O item D não é satisfeito devido a ausência de múltiplos fatores de autenticação nos produtos Altus.
4.5.1.6 As características especiais das credenciais de acesso padrão embarcadas (locais) nos sistemas operacionais e softwares devem ser consideradas na política de gestão de acessos e identidades: a) O acesso à senha de contas embarcadas deve ser restrito a um número limitado de pessoas; b) Cada ativo que possua credencial embarcada deve possuir uma senha distinta. Uma mesma senha não deve ser atribuída a mais de um ativo.	Não existe restrição quanto aos requisitos para a toda a gestão de acesso. A única funcionalidade exigida no nosso produto que ainda não temos é o MFA (multi-factor authentication), mas o mesmo está mapeado para ser implementado até o primeiro semestre de 2027. O usuário poderá optar pelo MFA. Caso opte, terá que entrar com senha e um token (senha temporária, como fazemos no internet banking), o Token será gerado a cada 1 minuto e aparece no menu do display da equipamento.
4.6 Monitoramento e resposta a incidentes	
4.6.1 Os ativos do ARCiber devem estar configurados para gerar logs de segurança apropriados para suportar investigações e a reconstrução de possíveis incidentes de segurança. Esses logs devem ser armazenados por prazo definido nas políticas de segurança cibernética da organização.	Os componentes geram logs para tal finalidade. Mais detalhes a respeito de geração de logs na seção 5.7

REQUISITO	COMENTÁRIO
4.6.2 Os dispositivos de segurança como Firewalls, IDS/IPS, Antimalware e subsistemas de autenticação devem estar configurados para gerar alertas caso identifiquem atividades suspeitas: a) As regras para geração de alertas devem ser revisadas periodicamente; b) Todos os alertas devem ser reportados imediatamente à equipe responsável definida na política de segurança do agente; c) Os alertas gerados devem ser analisados e respondidos no prazo definido pela política de segurança do agente.	Não existe restrição para utilização deste tipo de funcionalidade nos produtos Altus
4.6.3 Devem ser estabelecidos mecanismos para identificação e resposta a incidentes cibernéticos tempestivamente.	
4.6.4 Deve ser implementado um plano de resposta a incidentes cibernéticos, contemplando minimamente os seguintes requisitos: a) Identificação dos cenários de risco cibernéticos aplicáveis ao ARCiber e estratégias de tratamento para cada cenário; b) Classificação do impacto; c) Equipes envolvidas, com os seus respectivos papéis e responsabilidades antes, durante e depois da crise; d) Critérios para ativação do plano de resposta a incidentes cibernéticos.	
4.6.5 Testes de ativação dos planos de resposta a incidentes cibernéticos devem ser realizados periodicamente, em ciclos definidos na política de segurança cibernética da organização, cobrindo minimamente as listas de ativação (call tree) e revisão dos procedimentos descritos. Os exercícios deverão gerar documentos de lições aprendidas e as respectivas ações corretivas e de melhorias.	
4.6.6 Incidentes cibernéticos que afetem ativos do ARCiber devem ser informados ao ONS.	
5.1 Tratamento de Exceções	
5.1.1 Os casos em que requisitos não possam ser implementados devem ser tratados com uma exceção. Cada exceção gerada deve ser criada: a) Documentada detalhadamente, incluindo a data em que ela foi identificada, o motivo pelo qual ela precisa ser tratada como exceção, os itens desta RO que deixarão de ser atendidos e os impactos esperados; b) Aprovada pelo gestor responsável pela segurança cibernética do ARCiber;	Dentre os tópicos descritos nesse manual, o único requisito que não consegue ser atendido é o item 4.1.5.1-d) onde é exigido múltiplos fatores de autenticação.

REQUISITO	COMENTÁRIO
5.2 Adoção de Controles Complementares	
Cabe a cada organização adotar controles: a) complementares nos ativos que integram o ARCiber, conforme suas próprias políticas, diretrizes e avaliações de risco. b) de segurança cibernética nos ativos que não integram o ARCiber, conforme suas próprias políticas, diretrizes e avaliações de risco	Não existem restrições quanto esse tipo de controle nos produtos Altus

Tabela 6: Requisitos da Manual de Procedimentos da Operação - ONS

9. Componentes e Produtos CODESYS

O CVE (*Common Vulnerabilities and Exposures*) é uma ferramenta importante para rastrear vulnerabilidades em produtos utilizados em sistemas ao redor do mundo. Existe um banco de dados comum com todas as entradas de qualquer produto com uma vulnerabilidade conhecida. Este banco de dados pode ser acessado nos seguintes links:

https://www.cvedetails.com/

https://cve.mitre.org/

Atualmente, a Altus não possui um banco de dados próprio para registrar as vulnerabilidades conhecidas em seus produtos. Nesse caso, as vulnerabilidades conhecidas podem ser encontradas nos bancos de dados comuns por meio do uso de palavras-chave, como Altus, Hadron Xtorm, HX3040, entre outras. Muitos produtos Altus utilizam componentes e produtos CODESYS em seu desenvolvimento, e essas partes também possuem vulnerabilidades. Mais detalhes sobre essas vulnerabilidades, procedimentos de segurança e comunicados de segurança podem ser encontrados em:

https://www.codesys.com/ecosystem/security/latest-codesys-security-advisories/

No entanto, os produtos Altus não utilizam todos os produtos e componentes do CODESYS. Assim, para determinar se uma CVE relacionada ao CODESYS representa uma vulnerabilidade para os produtos Altus, é necessário saber quais componentes do CODESYS estão integrados nos produtos Altus.

A Tabela 7 mostra os componentes presentes na implementação de cada produto Altus. Todos os componentes utilizados são parte do CODESYS V3, portanto apenas vulnerabilidades referentes à esta versão devem ser consideradas.

Componente CODESYS	MasterTool	Nexto	Xpress	HX3040	NL717
CODESYS OPC DA Server SL	✓				
CODESYS Control for Linux ARM SL		✓ (Apenas NX3008)	✓		✓
CODESYS Control for Linux SL		✓ (Exceto NX3008)		✓	
CODESYS Scripting	✓				
CODESYS Visualization	✓				
CODESYS WebVisu	✓	✓ (Apenas NX3005 e NX 3008)	✓ (Apenas XP340)		
CODESYS Git	✓				
CODESYS PROFINET	✓	✓ (Exceto NX3003 e NX3004)	✓	✓	
CODESYS EtherNetIP	✓	✓ (Exceto NX3003 e NX3004)	✓		
Web Server (part of CODESYS runtime system)		✓	✓	✓	✓
CODESYS OPC UA Server		✓	✓	✓	✓
CODESYS SOFTMOTION CNC+ROBOTICS			✓ (Apenas XP351)		
CODESYS SOFTMOTION			✓ (Apenas XP350)		
Communication via Standard Ethernet		✓	✓	✓	✓
Package Manager	✓				
Alarm Configuration	✓	✓ (Apenas NX3005 e NX3008)	✓ (Apenas XP340)		
CODESYS Runtime Toolkit		✓	✓	✓	✓
CODESYS Development System or CODESYS Development System V3	✓				
CODESYS Control Runtime System Toolkit		✓	✓	✓	✓
CODESYS V3 Simulation Runtime (part of the CODESYS Development System)	✓				
CODESYS Gateway	✓				
Trace Manager	✓				

Tabela 7: Componentes CODESYS presentes nos produtos Altus

10. Considerações Finais

A segurança de sistemas de controle é um aspecto de extrema importância em um cenário onde a automação industrial está cada vez mais interconectada e digitalizada. Os incidentes de segurança têm aumentado significativamente, e isso exige que integradores e usuários estejam sempre vigilantes e proativos na observação e mitigação desses riscos.

Embora seja verdade que a segurança cibernética nunca pode ser garantida a 100%, é essencial compreender que a adoção de medidas de segurança e cuidados adequados pode elevar significativamente o nível de proteção para uma aplicação específica. A conscientização sobre as possíveis ameaças e a implementação de medidas preventivas podem criar uma barreira sólida contra ameaças potenciais.

Portanto, a colaboração entre fornecedores, integradores, operadores e usuários é fundamental para promover uma cultura de segurança robusta e eficiente. Ao investir em treinamento e capacitação, bem como na adoção de tecnologias de segurança adequadas, é possível mitigar riscos significativos e garantir a resiliência dos sistemas de controle em ambientes industriais.

Neste ambiente em constante evolução, é crucial reconhecer que a segurança é um esforço contínuo. Devemos permanecer atentos às últimas tendências e desenvolvimentos em segurança cibernética, atualizando e aprimorando regularmente nossas práticas e protocolos de segurança. Dessa forma, podemos enfrentar os desafios de segurança em um mundo cada vez mais digital, protegendo nossas operações e garantindo um ambiente de automação industrial mais seguro e confiável.

11. Apêndices

11.1. Gerenciamento de Certificados e Chaves TLS

Esta secção aborda a geração de arquivos de segurança, certificados e chaves, utilizando o TLS. Os certificados comentados a seguir são assinados por CA, este tipo de certificado considera uma entidade, denominada Autoridade Certificadora (CA), para gerar os certificados. Esta entidade pode ser um serviço de autoridade oficial ou um simples computador. Só é necessário restringir o acesso à CA para evitar qualquer quebra de segurança, uma vez que esta entidade pode gerar certificados para qualquer dispositivo. A imagem abaixo mostra como cada dispositivo interage com os arquivos.

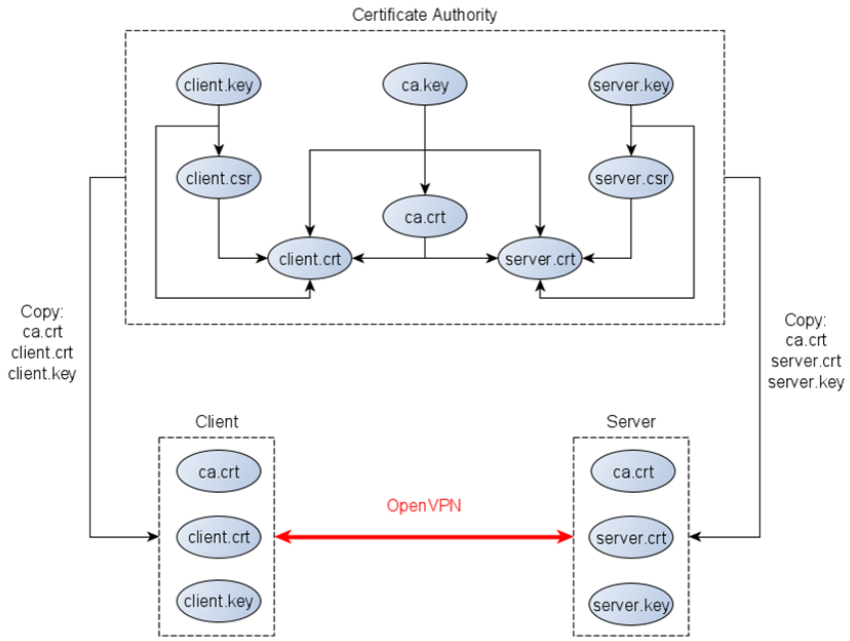


Figura 73: Fluxo de Geração de Certificados TLS

Em primeiro lugar, os arquivos gerados são chaves privadas. Cada dispositivo possui seu arquivo de chave, criado pela entidade CA ou pelo próprio dispositivo. O arquivo mais importante é a chave privada da CA *ca.key*, que não deve sair da entidade. A entidade CA gera seu certificado com base em sua chave privada *ca.crt*. Este certificado é um arquivo público usado pelos dispositivos para validar a conexão VPN. A geração de certificados do dispositivo requer primeiro um arquivo de solicitação (*.csr* ou *.req* dependendo da ferramenta) com base na chave privada do dispositivo. Este documento apresenta duas ferramentas diferentes para gerar os arquivos de certificado: Easy-RSA e OpenSSL.

Certifique-se de estar com a data e hora configuradas corretamente na entidade CA para que a geração dos certificados seja com base em um configuração atual.

11.1.1. Geração de Certificados por Easy-RSA

O projeto OpenVPN fornece essa ferramenta para ajudar com o certificado e as chaves. O Easy-RSA está disponível para Windows e Linux. Veja abaixo o passo a passo para gerar os arquivos em uma configuração do Windows:

1- Abra um prompt do Windows na pasta Easy-RSA e execute o seguinte comando para entrar no terminal da ferramenta:

```
.\EasyRSA-Start.bat
```

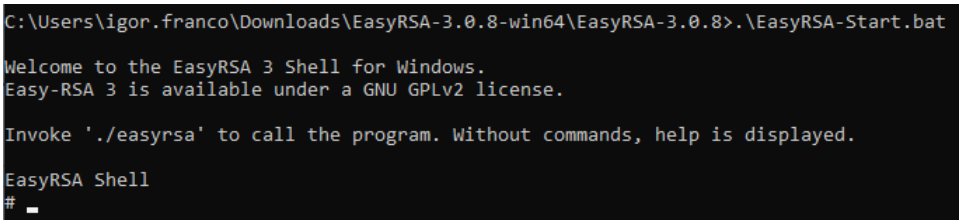


Figura 74: Geração de Certificado utilizando o Easy-RSA (passo 1)

2- Copie o arquivo *vars.example* e renomeie-o para *vars* na pasta de ferramentas.

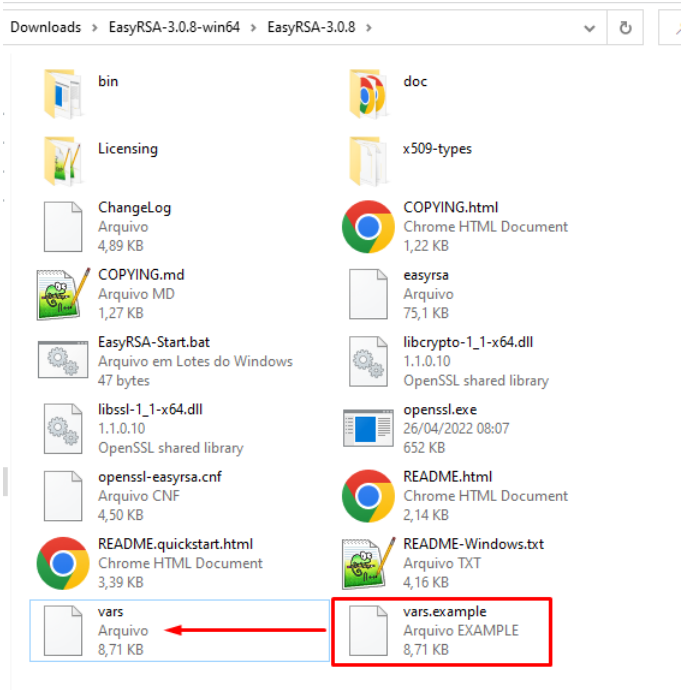


Figura 75: Geração de Certificado utilizando o Easy-RSA (passo 2)

3- Abra o arquivo *vars* com um editor de texto e altere as informações da Autoridade de Certificação.

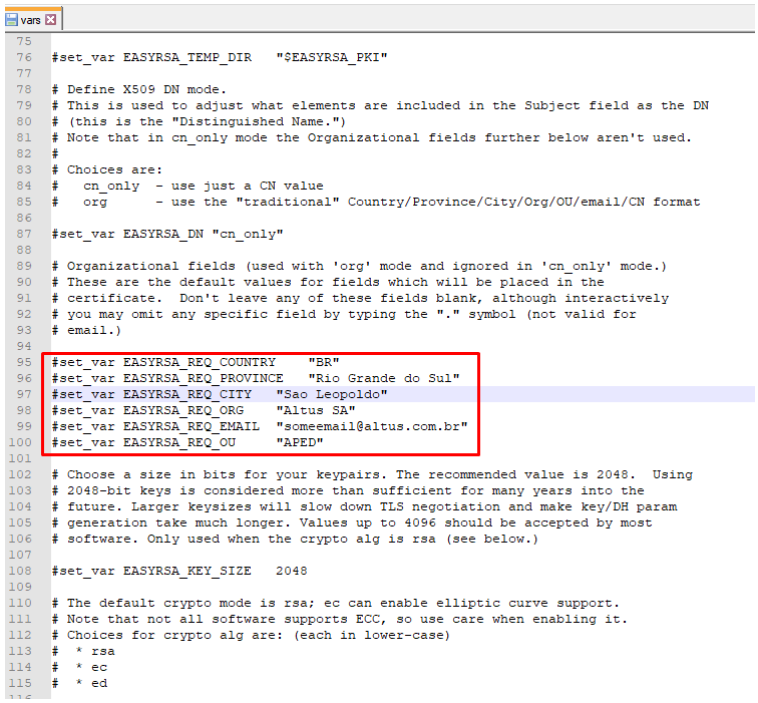


Figura 76: Geração de Certificado utilizando o Easy-RSA (passo 3)

4- Use o comando a seguir para preparar a configuração:

```
./easyrsa init-pki
```

Figura 77: Geração de Certificado utilizando o Easy-RSA (passo 4)

5- Em seguida, digite o seguinte para gerar o certificado CA.

```
./easyrsa build-ca nopass
```

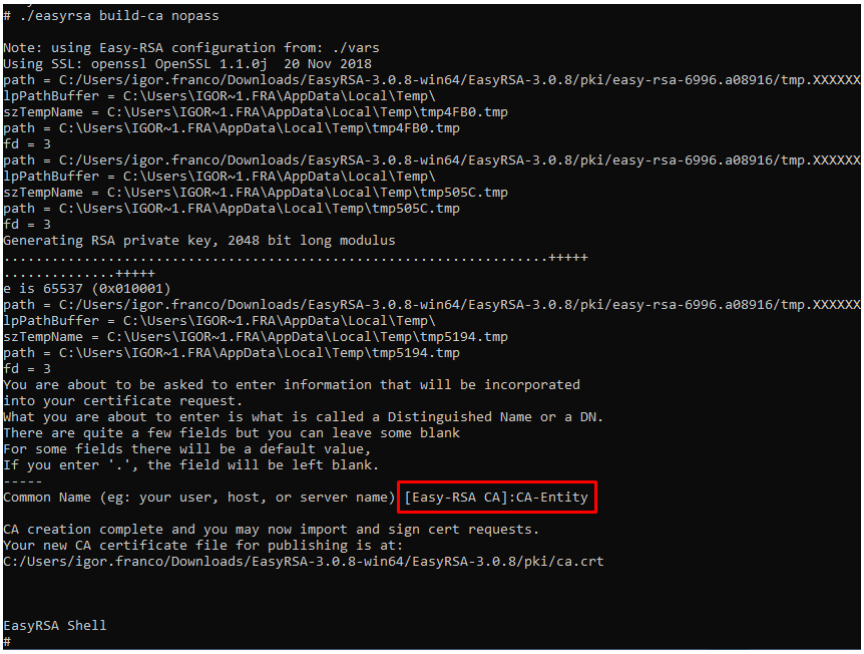


Figura 78: Geração de Certificado utilizando o Easy-RSA (passo 5)

6- Gere a chave do dispositivo e solicite arquivos usando o seguinte comando (altere o *DeviceName* com o nome comum desejado):

```
./easyrsa gen-req DeviceName nopass
```

Novamente, remova o argumento *nopass* para usar uma senha para o arquivo de certificado. Ao entrar com o Nome Comum como argumento, basta pressionar enter quando solicitado (quadrado vermelho).

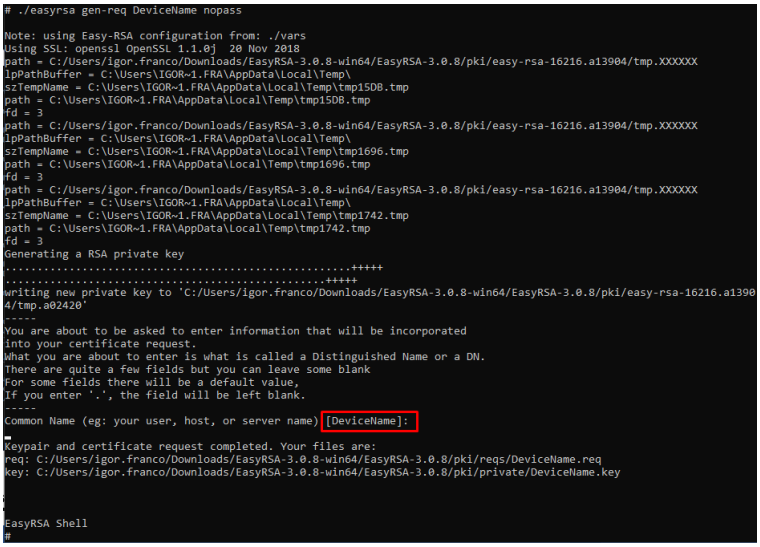


Figura 79: Geração de Certificado utilizando o Easy-RSA (passo 6)

7- Por fim, digite o seguinte comando para gerar o certificado do dispositivo (o *DeviceName* é o nome comum desejado e o *servidor* é o tipo; use *cliente* se estiver gerando para um cliente VPN).

```
./easyrsa sign-req server DeviceName
```

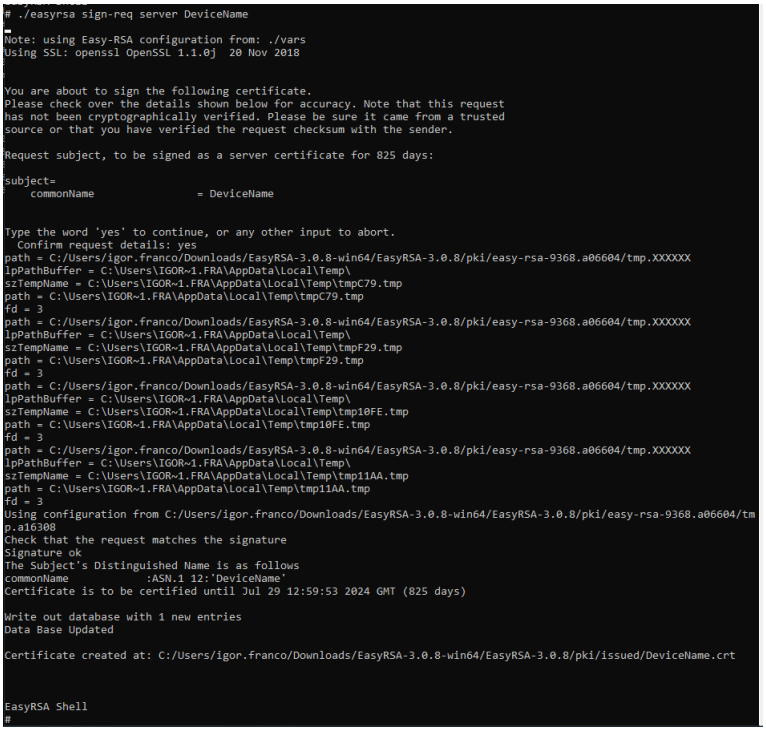


Figura 80: Geração de Certificado utilizando o Easy-RSA (passo 7)

8- Repita as etapas 6 e 7 para gerar mais certificados de dispositivo.

9- Encontre o *ca.crt* na pasta *pki*, as chaves privadas do dispositivo no caminho *pki/private* e os certificados do dispositivo no diretório *pki/issued*.

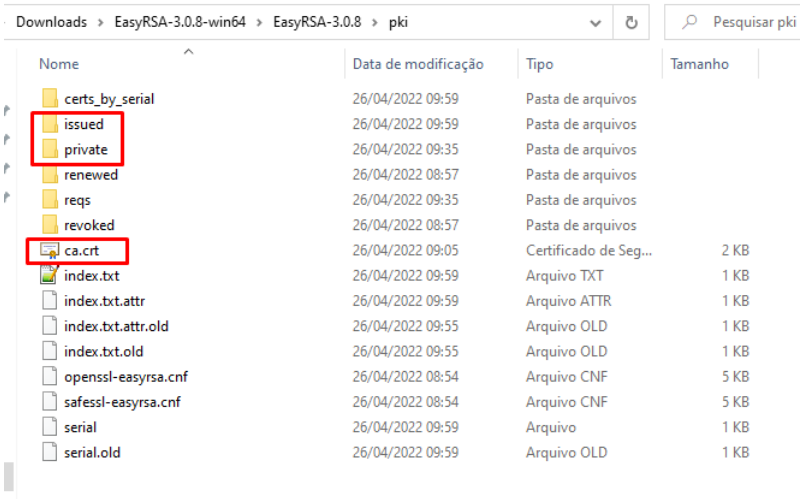


Figura 81: Geração de Certificado utilizando o Easy-RSA (passo 9)

11.1.2. Geração de Certificados por OpenSSL

O OpenSSL é um pacote de código aberto com ferramentas que ajudam a gerar muitos arquivos e recursos de segurança. Este pacote é nativo para a maioria das distribuições do Linux e está disponível para Windows. Apenas lembre-se de definir a pasta OpenSSL no PATH (variável de ambiente) para permitir o uso do comando de qualquer lugar através do prompt. Encontre abaixo o passo a passo utilizando este recurso (todos os arquivos podem ter qualquer nome conforme desejado, os passos consideram apenas um exemplo):

1- Abra um prompt na pasta do certificado (onde criará os arquivos).

2- Gere a chave privada da CA com o seguinte comando:

```
openssl genrsa -out ca.key 4096
```

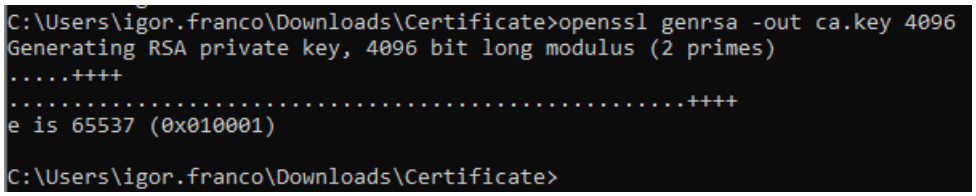


Figura 82: Geração de Certificado utilizando o OpenSSL (passo 2)

3- Em seguida, gere o certificado CA com base na chave privada, utilizando o comando a seguir.

```
openssl req -new -x509 -days 365 -key ca.key -out ca.crt
```

O parâmetro *-days* representa o tempo de expiração do certificado. Configure-o como desejar. Neste exemplo, o certificado é válido por um ano. Preencha os valores solicitados no prompt conforme necessário (pressione enter para usar o padrão, que está entre colchetes []). É obrigatório definir um Nome Comum para o trabalho do certificado.

Figura 83: Geração de Certificado utilizando o OpenSSL (passo 3)

4- Agora, gere a chave privada do dispositivo, semelhante à etapa 2, utilizando o seguinte comando:

```
openssl genrsa -out DeviceName.key 2048
```

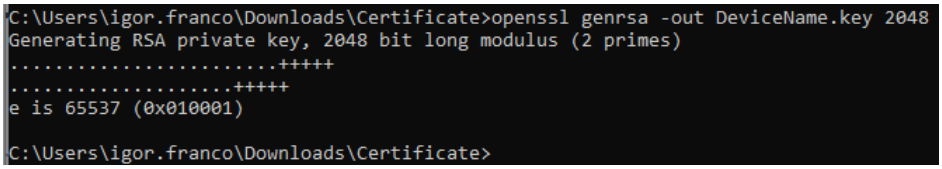


Figura 84: Geração de Certificado utilizando o OpenSSL (passo 4)

5- Depois disso, gere o arquivo de solicitação de certificado com base na chave privada, utilizando o comando a seguir:

```
openssl req -new -key DeviceName.key -out DeviceName.csr
```

Insira as informações desejadas e lembre-se de usar um nome comum diferente da CA.

Figura 85: Geração de Certificado utilizando o OpenSSL (passo 5)

6- Por fim, gere o certificado do dispositivo usando a chave privada da CA, o certificado da CA e o arquivo de solicitação de certificado do dispositivo, utilizando o comando que segue:

```
openssl x509 -req -days 365 -in DeviceName.csr -CA ca.crt -CAkey ca.key -set_serial 01 -out
```

Defina a data de expiração conforme desejado com o parâmetro *-days* e o número de série do certificado com o argumento *-set_serial*.

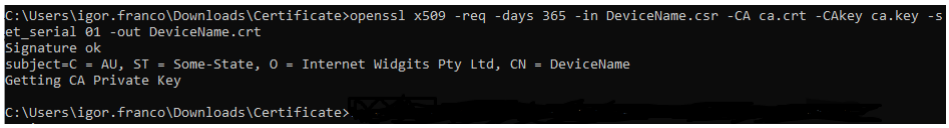


Figura 86: Geração de Certificado utilizando o OpenSSL (passo 6)

7- Repita as etapas 4 a 6 para qualquer novo dispositivo.

8- (Opcional) O OpenSSL oferece uma ferramenta para verificar se o certificado do dispositivo funciona com CA:

Utilize o seguinte comando:

```
openssl verify -purpose sslserver -CAfile ca.crt DeviceName.crt
```

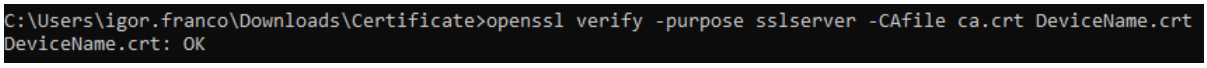


Figura 87: Geração de Certificado utilizando o OpenSSL (passo 8)

11.1.3. Geração de Chave TA pelo OpenVPN

O projeto OpenVPN fornece uma ferramenta para geração de uma chave TLS, comumente chamada de ta.key. Esta chave é uma camada de proteção extra nas portas UDP/TCP de comunicação do OpenVPN, sendo assim, a utilziação desta chave pode ser interpretada como um Firewall de HMAC para a comunicação VPN, fazendo com que seja necessário a existência do parâmetro dos dois lados da comunicação para que ela seja estabelecida.

A geração desta chave no Windows pode ser feita com o comando a seguir:

```
openvpn --genkey secret ta.key
```

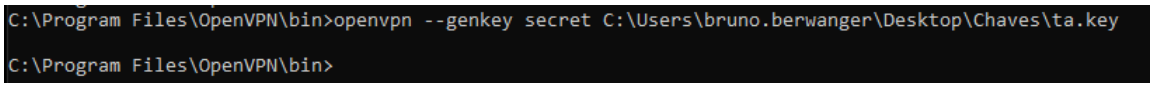


Figura 88: Exemplo de Geração de Chave TA no Windows

Para executar o comando foi utilizado o executável que é instalado juntamente ao pacote do OpenVPN. O diretório utilizado na imagem a cima é um exemplo e é opcional, pode ser utilizado somente o nome do arquivo desejado.

O comando pode ser utilizado para realizar a geração da chave pelo Linux, porém, há uma pequena alteração no comando em relação ao windows. Para gerar a chave no Linux utilize o seguinte comando: *openvpn –genkey –secret ta.key*. Para executa-lo, basta digitar o seguinte comando no terminal:

```
openvpn --genkey --secret ta.key
```

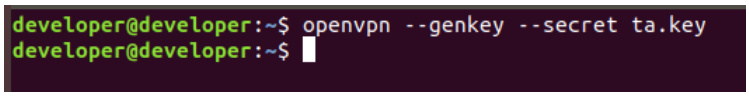


Figura 89: Exemplo de Geração de Chave TA no Linux

Este parâmetro não é obrigatório para a comunicação VPN, porém, caso o servidor esteja utilizando, todos os seus clientes devem também utilizar, sendo que a chave do servidor e dos clientes deve ser a mesma.