

Manual de Segurança Cibernética

MT / cMTx

Interface Homem-Máquina (IHM)



Manual de Segurança Cibernética

MT / cMTx

Documento: 10014443612

Idioma: Português

Revisão: 00

Data de publicação: 03/2026

A informação abaixo descreve as revisões ocorridas neste manual.

Revisão	Descrição
R00	Primeira edição.

1	INTRODUÇÃO	1-1
1.1	SOBRE O DOCUMENTO	1-1
1.2	AVISO IMPORTANTE SOBRE SEGURANÇA CIBERNÉTICA E COMUNICAÇÕES	1-1
2	CONCEITOS FUNDAMENTAIS DE CIBERSEGURANÇA	2-1
2.1	VISÃO GERAL	2-1
2.2	MUITO ALÉM DA TI: A NOVA FRONTEIRA DA SEGURANÇA CIBERNÉTICA	2-1
2.3	DEFESA EM PROFUNDIDADE	2-2
2.3.1	Ambiente Externo	2-2
2.3.1.1	Segurança da Planta	2-2
2.3.1.2	Segurança do Ambiente de Rede	2-2
2.3.1.3	Segurança da Integração de Sistemas	2-2
2.3.2	Operação do Produto	2-2
2.4	MANUTENÇÃO GERAL DE SEGURANÇA	2-3
2.5	ANÁLISE DE RISCO E MECANISMO DE REPORTE	2-3
3	RISCOS DURANTE A EDIÇÃO DE PROGRAMAS	3-1
3.1	VERIFICAÇÃO DO ARQUIVO DE INSTALAÇÃO	3-1
3.1.1	Assinatura Digital	3-1
3.1.2	Diretório de Instalação	3-1
3.1.3	Atualização de Versão do EasyBuilder Pro	3-2
3.2	CONFIGURAÇÕES DE SEGURANÇA DO SOFTWARE	3-3
3.2.1	Habilitar Comunicação Segura	3-3
3.2.2	Utilizar o Modo de Segurança Avançado	3-3
3.2.3	Utilizar Senhas de Usuário Fortes	3-3
3.2.4	Proteção das Configurações de Senha	3-4
3.2.5	Habilitar Logout Automático	3-4
3.2.6	Sincronização de Tempo via Servidor NTP	3-5
3.2.7	Segurança de Objetos	3-5
3.2.8	Registro de Operações	3-6
4	RISCOS DURANTE A OPERAÇÃO DO PRODUTO	4-1
4.1	AUTORIZAÇÃO DE LOGIN	4-1
4.2	SEGURANÇA DOS ARQUIVOS DE LOG	4-1
4.2.1	Prolongar a Vida Útil da Memória Flash	4-1
4.2.1.1	Recomendações para reduzir a velocidade de escrita	4-2
4.2.2	Salvar ou Fazer Backup dos Logs em Dispositivo Externo	4-2
4.2.2.1	Recomendações para uso de USB e SD	4-3
4.2.2.2	Recomendações para uso de servidor de banco de dados	4-3
4.2.3	Habilitar Checksum para Integridade dos Dados	4-3
5	RISCOS DURANTE A MANUTENÇÃO REMOTA	5-1
5.1	SEGURANÇA DE COMUNICAÇÃO	5-1
5.1.1	Desabilitar Funções Desnecessárias	5-1
5.1.2	Servidor Modbus	5-1
5.1.3	MQTT	5-2
5.1.4	Servidor OPC UA	5-3
5.1.5	Servidor de Banco de Dados	5-3
5.1.6	E-mail	5-4
5.1.7	Monitoramento Remoto cMT Viewer	5-4
5.2	SEGURANÇA DA PÁGINA WEB	5-5
5.2.1	Habilitar Criptografia HTTPS	5-5
5.2.2	Habilitar Regras de Força de Senha	5-5
5.2.3	Habilitar Expiração de Senha	5-6
5.2.4	Bloqueio Automático após Tentativas de Login	5-6

5.2.5	Alterar Senha do Sistema	5-6
5.3	ATIVIDADES REGULARES DE MANUTENÇÃO DE SEGURANÇA	5-7
6	DIRETRIZES PARA DESCARTE SEGURO DO PRODUTO	6-1
6.1	RECOMENDAÇÕES PARA DESCARTE SEGURO	6-1

1 INTRODUÇÃO

1.1 SOBRE O DOCUMENTO

A WEG leva a segurança cibernética e da informação com máxima seriedade. Reconhecemos a crescente necessidade de proteger nossos clientes e nossas operações em um ambiente cada vez mais complexo. Atuamos em setores essenciais, nos quais ataques cibernéticos não são meros transtornos, pois podem impactar comunidades inteiras e colocar vidas em risco.

Essa realidade nos impulsiona a adotar uma abordagem abrangente de segurança cibernética, integrando a proteção de nossos produtos e serviços ao fortalecimento de parcerias com outros líderes do setor. O desenvolvimento e a evolução contínua dos produtos são orientados pelas recomendações de normas reconhecidas internacionalmente, de forma a atender aos níveis de proteção exigidos por nossos clientes e pelos mercados em que atuam.

Desta forma, este manual tem como objetivo fornecer diretrizes práticas para a configuração segura, o comissionamento e a operação de IHMs ao longo de todo o seu ciclo de vida, abrangendo desde a fase inicial até a operação contínua em campo. O conteúdo foi desenvolvido com foco na linha cMTx, considerando suas funcionalidades e capacidades específicas. Ainda assim, muitos dos conceitos e mecanismos aqui apresentados podem ser aplicados, total ou parcialmente, às IHMs da linha MT.

Ressalta-se que podem existir diferenças de funcionalidades, recursos suportados e capacidades entre as linhas. Dessa forma, cabe ao usuário avaliar a aplicabilidade de cada recomendação conforme o modelo específico de IHM utilizado e consultar a documentação técnica correspondente para validação das características disponíveis.

São consolidadas orientações práticas e medidas mitigatórias, com ênfase na configuração segura das IHMs, na redução da superfície de ataque, no fortalecimento dos mecanismos de defesa e no gerenciamento de riscos cibernéticos ao longo do ciclo de vida do equipamento, contribuindo para uma operação resiliente e alinhada às melhores práticas de segurança em sistemas de automação industrial.

1.2 AVISO IMPORTANTE SOBRE SEGURANÇA CIBERNÉTICA E COMUNICAÇÕES

As IHMs da WEG, modelos cMTx, possuem a capacidade de se conectar e trocar informações por meio de redes e protocolos de comunicação. Embora tenham sido projetados e testados para garantir o funcionamento adequado com outros sistemas de automação utilizando os protocolos mencionados neste manual, é essencial que o cliente compreenda as responsabilidades associadas à informação e à cibersegurança ao utilizar este equipamento.

Portanto, é de inteira responsabilidade do cliente adotar estratégias de defesa em profundidade e implementar políticas e medidas para garantir a segurança do sistema como um todo, incluindo as comunicações enviadas e recebidas pelo equipamento. Essas medidas incluem, mas não se limitam a, instalação de firewalls, programas antivírus e antimalware, criptografia de dados, controle de autenticação e controle físico de acesso dos usuários.

A WEG e suas afiliadas não se responsabilizam por danos ou perdas decorrentes de violações de segurança cibernética, incluindo, mas não se limitando a, acesso não autorizado, intrusão, vazamento e/ou roubo de dados ou informações, negação de serviço ou qualquer outra forma de violação de segurança. A utilização deste produto em condições para as quais não foi especificamente projetado não é recomendado e pode acarretar danos ao produto, à rede e ao sistema de automação.

Neste sentido, é imprescindível que o cliente compreenda que intervenções externas por meio de programas de terceiros, a exemplo dos sniffers ou programas com ações semelhantes, possuem o potencial de ocasionar interrupções ou restrições na funcionalidade do equipamento.

2 CONCEITOS FUNDAMENTAIS DE CIBERSEGURANÇA

2.1 VISÃO GERAL

Em uma era cada vez mais digital e interconectada, as infraestruturas industriais passam a depender fortemente de dispositivos de automação integrados, como inversores de frequência, controladores lógicos programáveis (CLPs), interfaces homem-máquina (IHMs), gateways industriais, etc. Nesse cenário, a segurança cibernética deixa de ser uma opção e se torna um requisito essencial à operação segura, confiável e contínua dos sistemas.

Com o avanço constante das ameaças cibernéticas, cada vez mais sofisticadas e direcionadas, as abordagens tradicionais e puramente reativas de segurança tornaram-se insuficientes. Novas técnicas de ataque surgem diariamente, exigindo que fabricantes, integradores e operadores industriais adotem medidas proativas e resilientes para proteger seus ativos.

Essa crescente complexidade leva governos a estabelecer regulamentações que reforcem a resiliência, isto é, a capacidade de se recuperar de um ataque, adaptar-se às ameaças em constante mudança e aprimorar seus mecanismos de defesa, minimizando os impactos e preservando a continuidade das operações. Isso envolve não apenas a implementação de medidas de segurança robustas, mas também a capacidade de antecipar e responder efetivamente a incidentes. Nesse contexto, adotar uma estratégia de resiliência cibernética robusta não é mais uma vantagem competitiva, é uma necessidade crítica para os negócios e para a proteção das operações industriais e de missão crítica.

Diversas jurisdições ao redor do mundo têm desenvolvido regulamentações voltadas à segurança de sistemas industriais. Nos Estados Unidos, o conjunto de normas NERC-CIP estabelece requisitos rigorosos para a proteção de sistemas de automação em instalações críticas. Na União Europeia, o recém-aprovado Cyber Resilience Act (CRA) impõe obrigações diretas aos fabricantes de produtos digitais, incluindo equipamentos de automação industrial.

Essas iniciativas estão fundamentadas em normas e frameworks internacionalmente reconhecidos, como a série ISA/IEC 62443, o framework do NIST, a família ISO/IEC 27000, além de diretrizes específicas como a IEC 62351, voltada à segurança de protocolos de automação. A adoção dessas referências permite mitigar riscos relevantes, fortalecer a segurança dos dispositivos de automação e garantir a resiliência das operações industriais frente a ameaças complexas, assegurando a continuidade dos serviços essenciais e a integridade dos dados e sistemas envolvidos.

2.2 MUITO ALÉM DA TI: A NOVA FRONTEIRA DA SEGURANÇA CIBERNÉTICA

Tradicionalmente, o termo segurança cibernética se refere ao conjunto de medidas adotadas para proteger sistemas computacionais e redes contra acessos não autorizados ou ataques maliciosos. No entanto, quando aplicado ao contexto das tecnologias de automação e energia, esse conceito se amplia significativamente. Nesse cenário, a segurança cibernética passa a abranger práticas destinadas a garantir a confiabilidade, a integridade e a disponibilidade dos sistemas de controle e automação, princípios amplamente conhecidos no universo da Tecnologia da Informação (TI) pela sigla "CIA" (Confidentiality, Integrity, Availability).

Em ambientes industriais, essas medidas são essenciais para prevenir uma série de riscos, como o vazamento de informações sensíveis, danos físicos a equipamentos ou sistemas, corrupção de dados e interrupções nas operações. Tais incidentes podem comprometer não apenas a eficiência, mas também a segurança de processos críticos.

Na TI, a prioridade costuma ser a confidencialidade dos dados, seguida da integridade e, por fim, da disponibilidade. Já na Tecnologia Operacional (OT), essa ordem se inverte: a disponibilidade é o fator mais importante, seguida da integridade e da confidencialidade, formando a sigla "AIC". Isso se deve ao fato de que, em ambientes industriais, manter os sistemas em funcionamento contínuo e seguro é mais crucial do que proteger informações contra acessos indevidos.

2.3 DEFESA EM PROFUNDIDADE

O conceito de defesa em profundidade envolve mais do que confiar em apenas uma única medida de segurança. Ele consiste em implementar mecanismos de segurança em vários níveis para fornecer proteção robusta. Essa abordagem reduz significativamente riscos potenciais, como vazamento de informações e ataques de hackers, aumentando a segurança geral dos produtos durante instalação, operação, manutenção e descarte.

2.3.1 Ambiente Externo

A IHM deve ser instalada e operada em ambientes industriais com infraestrutura de rede segura para evitar acessos não autorizados. Para garantir desempenho ideal e minimizar riscos de segurança, siga as seguintes recomendações. A estrutura de segurança externa consiste em três camadas principais:

- Segurança da planta
- Segurança do ambiente de rede
- Segurança da integração de sistemas

2.3.1.1 Segurança da Planta

Garanta o uso seguro da IHM por meio de verificações completas do sistema.

- Instalar perímetros controlados com controle de acesso em instalações industriais.
- Implementar controle de acesso biométrico ou sistemas de bloqueio em laboratórios ou salas de servidores.
- Utilizar sistemas de alarme ou videomonitoramento.

2.3.1.2 Segurança do Ambiente de Rede

Um ambiente de rede seguro é uma configuração controlada na qual o acesso é limitado a dispositivos, usuários e serviços autorizados, prevenindo acesso não autorizado, vazamentos de dados e ataques maliciosos.

O produto foi projetado para ser utilizado dentro de redes internas protegidas. Evite expô-lo diretamente a redes públicas.

Se conectividade externa for necessária, implemente as seguintes medidas de segurança, as quais ajudam a separar o tráfego de comunicação interno do externo.

- Monitorar a comunicação entre redes de escritório e de fábrica utilizando firewalls.
- Utilizar roteadores para evitar acesso direto via IP público.
- Se o produto possuir duas portas Ethernet, conectar:
 - LAN 1 à rede externa
 - LAN 2 aos dispositivos internos

2.3.1.3 Segurança da Integração de Sistemas

Garanta que os mecanismos internos de proteção permaneçam eficazes durante a integração do sistema.

- Manter sistemas atualizados regularmente
- Utilizar antivírus
- Implementar autenticação de usuários

2.3.2 Operação do Produto

As configurações do sistema IHM geralmente são gerenciadas por pessoal responsável pela criação de arquivos e integração de sistemas. Durante a operação pelos usuários, é essencial impedir modificações não autorizadas nos parâmetros que possam interromper o funcionamento normal.

Medidas recomendadas:

- Ocultar configurações do sistema
- Alterar senhas padrão de login
- Utilizar comunicação criptografada HTTPS na página de configuração web

A IHM possui recursos internos de segurança habilitados por padrão, os quais podem ser configurados conforme necessário para atender aos requisitos da instalação. Essa configuração deve ser realizada apenas por pessoal qualificado, pois alterações incorretas podem comprometer a segurança do sistema e da rede.

2.4 MANUTENÇÃO GERAL DE SEGURANÇA

Esta seção fornece diretrizes e recomendações para garantir a segurança do produto. Ela auxilia os usuários no planejamento e na execução eficaz de tarefas rotineiras de manutenção da segurança da informação.

- Atualize regularmente o produto para garantir que tanto o software quanto o firmware estejam sempre atualizados. Isso inclui aplicações, sistemas operacionais e outros componentes. Essa prática previne a exploração de vulnerabilidades conhecidas e introduz novos recursos de segurança.
- Realize testes rotineiros de vulnerabilidades de segurança, como varredura de vulnerabilidades e testes de intrusão. Essa abordagem auxilia na identificação e correção de possíveis fragilidades.
- Utilize as capacidades de monitoramento do produto para supervisionar sua operação, identificar comportamentos anormais e acompanhar eventos de segurança. Além disso, mantenha registros de todos os eventos de segurança para posterior análise e investigação.
- Empregue mecanismos adequados de criptografia para o tratamento de dados sensíveis e comunicações. Isso garante a confidencialidade e a integridade dos dados durante a transmissão e o armazenamento.
- Elabore planos de contingência para responder de forma eficaz a possíveis eventos de segurança e executar rapidamente medidas de resposta. Paralelamente, estabeleça um processo de gestão de vulnerabilidades para avaliar, acompanhar e corrigir vulnerabilidades periodicamente.
- Caso este produto conceda acesso a prestadores de serviços terceirizados, assegure que eles sigam os mesmos padrões de segurança e avalie regularmente sua postura de segurança. Consulte normas internacionais para gestão de fornecedores terceirizados (por exemplo, ISO 28000 / ISO 27001).

2.5 ANÁLISE DE RISCO E MECANISMO DE REPORTE

Ao utilizar o produto, caso surjam riscos relacionados à segurança, siga o procedimento abaixo:

- Realizar análise de risco.
- Consultar o manual de segurança do produto.
- Avaliar a eficácia das medidas de mitigação.
- Caso não seja possível resolver o problema, entre em contato com os canais de atendimento da empresa.

3 RISCOS DURANTE A EDIÇÃO DE PROGRAMAS

3.1 VERIFICAÇÃO DO ARQUIVO DE INSTALAÇÃO

3.1.1 Assinatura Digital

Antes de instalar o EasyBuilder Pro, verifique se o arquivo de instalação (setup.exe) possui uma assinatura digital válida e se ela não foi adulterada. Clique com o botão direito no arquivo de instalação, abra a aba *Digital Signatures* e selecione *Details* para confirmar a integridade da assinatura digital. A [Figura 3.1](#) mostra as propriedades do instalador e os detalhes da assinatura digital.

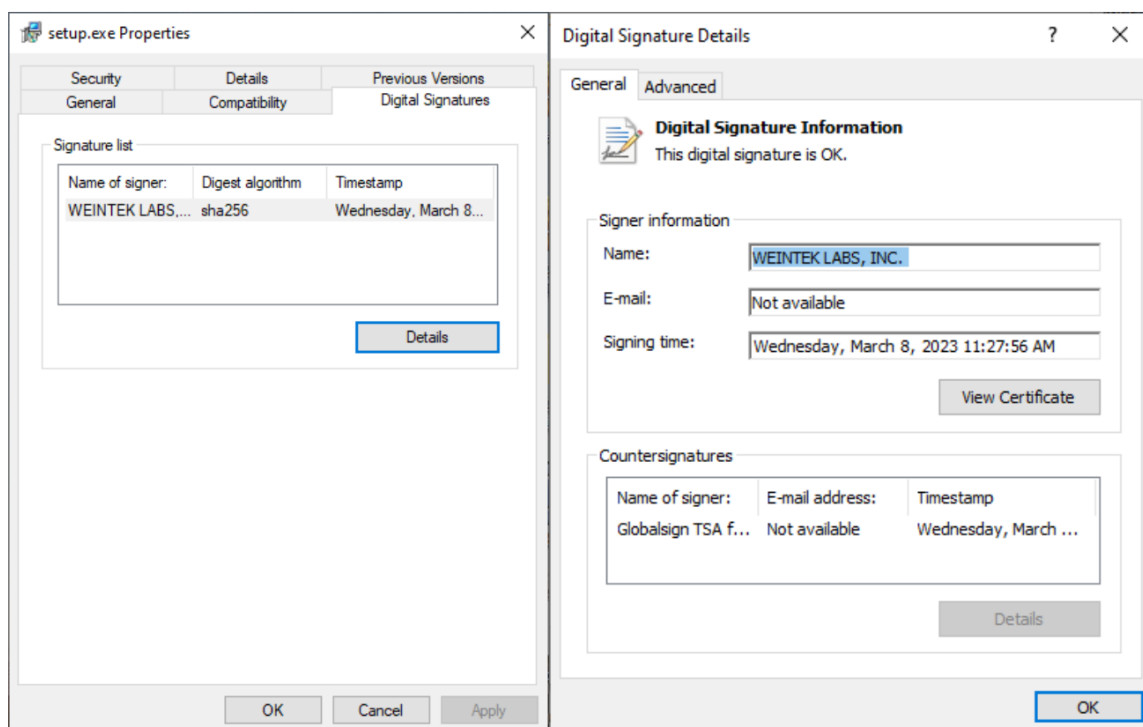


Figura 3.1: Assinatura digital do instalador.

3.1.2 Diretório de Instalação

Instale o EasyBuilder Pro em uma pasta com permissões de acesso restritas (por exemplo, C:\Program Files (x86)), como mostrado na [Figura 3.2](#).

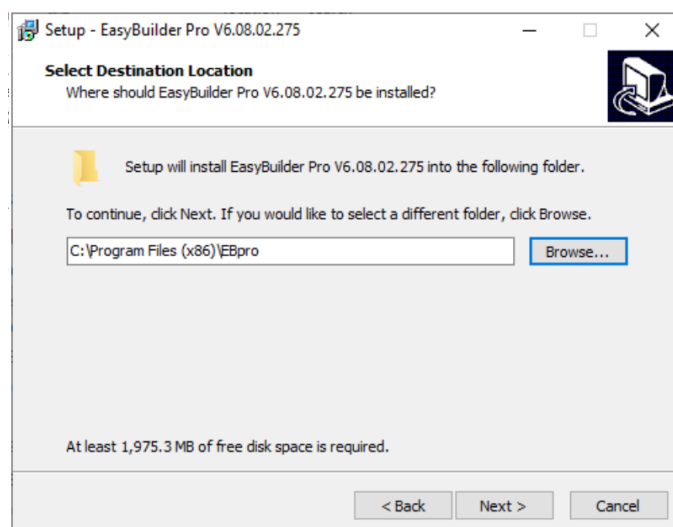


Figura 3.2: Diretório de instalação.

3.1.3 Atualização de Versão do EasyBuilder Pro

Garanta que o software esteja atualizado para as versões mais recentes que corrijam vulnerabilidades de segurança. Para verificar sua versão atual e buscar novas atualizações abra o EasyBuilder Pro e clique em *File* → *About* → *Check for updates...*, conforme a [Figura 3.3](#).

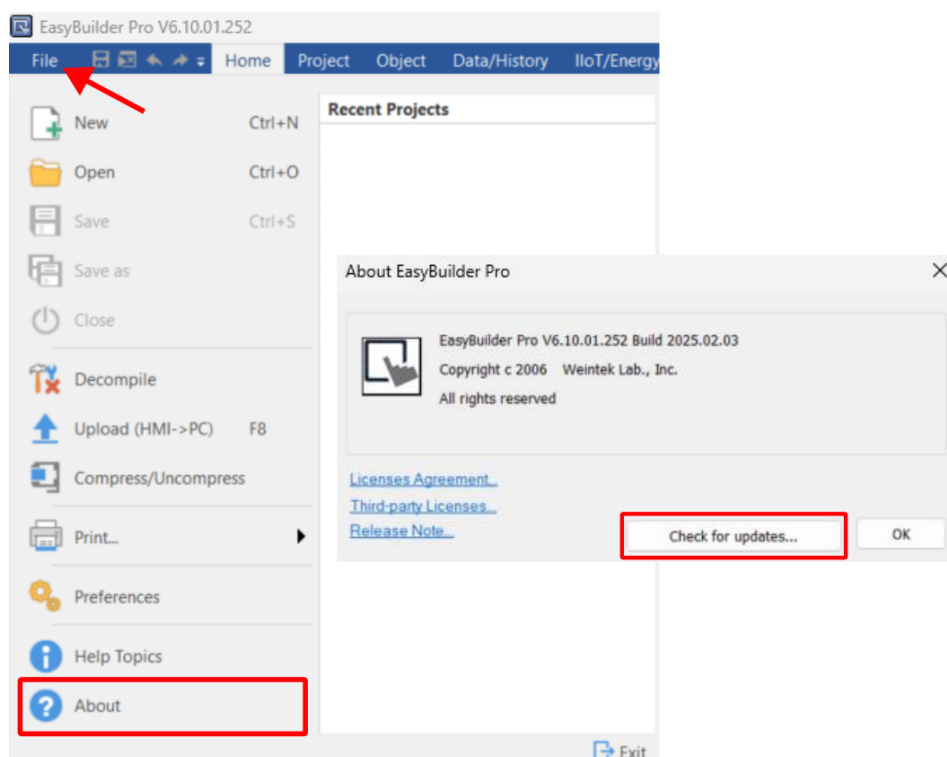


Figura 3.3: Verificando versão atual e novas atualizações do EasyBuilder Pro.

É possível habilitar a notificação para ser informado automaticamente de novas atualizações disponíveis ao inicializar o programa. Para isso, clique em *File* → *Preferences* → *Misc* e habilite a opção *Notify when new version of EasyBuilder Pro is available*, como indicado na [Figura 3.4](#).

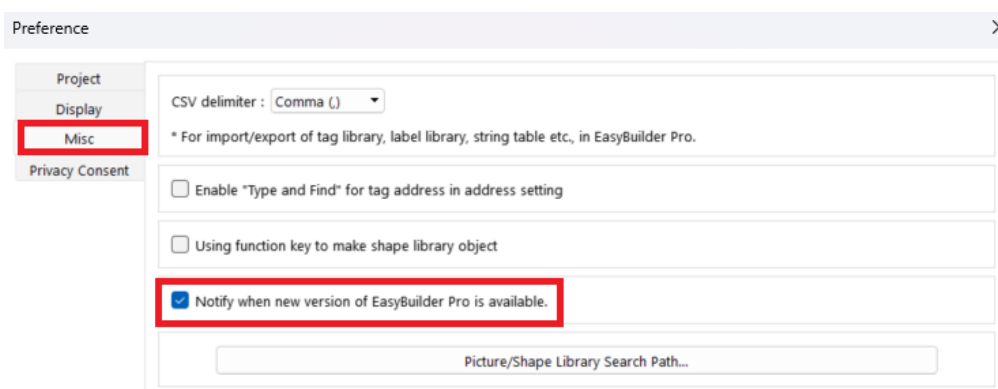


Figura 3.4: Notificar quando uma nova versão do EasyBuilder Pro está disponível.

3.2 CONFIGURAÇÕES DE SEGURANÇA DO SOFTWARE

3.2.1 Habilitar Comunicação Segura

Ative comunicação segura para garantir que a comunicação entre a IHM e outros dispositivos seja criptografada. Em um projeto aberto no EasyBuilder Pro, clique em *Home* → *System Parameters*, abra a aba *Devices*, selecione a IHM, clique em *Settings/Security* e ative *Enable secure communication*, conforme a [Figura 3.5](#).

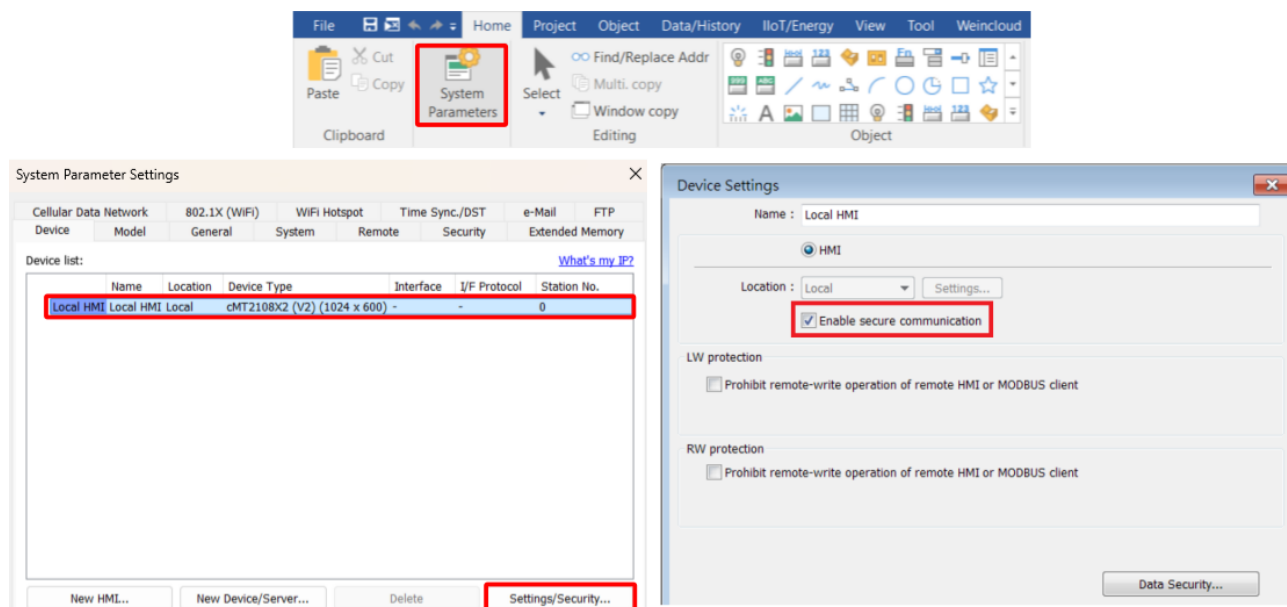


Figura 3.5: Habilitar comunicação segura.

3.2.2 Utilizar o Modo de Segurança Avançado

O modo de segurança avançado é recomendado para que projetistas possam atribuir diferentes privilégios a diferentes usuários e controlar o acesso aos objetos. No EasyBuilder Pro, clique em *Home* → *System Parameters*, abra a aba *Security* e ative *Enhanced security mode*, como demonstrado na [Figura 3.6](#). Para configurações detalhadas, consulte o capítulo *User Password and Object Security* do manual do EasyBuilder Pro.

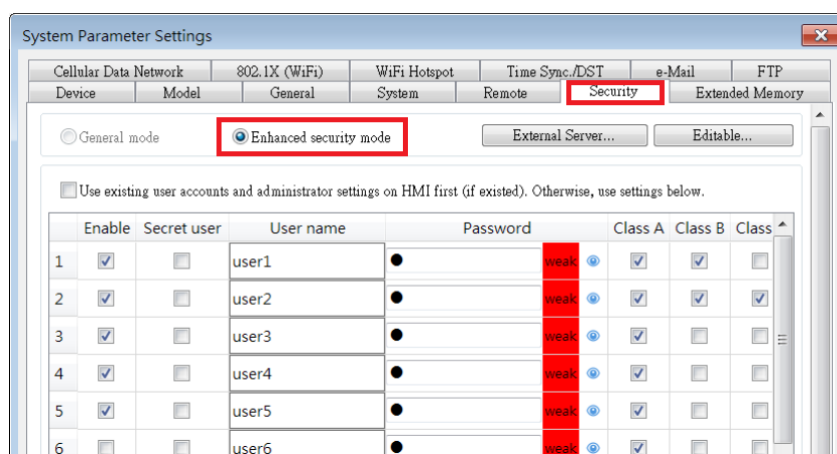


Figura 3.6: Habilitar comunicação segura.

3.2.3 Utilizar Senhas de Usuário Fortes

Senhas fortes são menos vulneráveis a tentativas de quebra por agentes maliciosos. A robustez de uma senha está relacionada à quantidade e à diversidade de caracteres utilizados. Entre os tipos de caracteres que podem ser empregados, destacam-se:

- Letras maiúsculas

RISCOS DURANTE A EDIÇÃO DE PROGRAMAS

- Letras minúsculas
- Números
- Caracteres especiais

Classificação da força da senha:

- **Forte:** três ou mais tipos de caracteres e comprimento igual ou superior a 8 caracteres.
- **Média:** pelo menos dois tipos de caracteres e comprimento igual ou superior a 6 caracteres.
- **Fraca:** apenas um tipo de caractere ou comprimento inferior a 6 caracteres.

A [Figura 3.7](#) apresenta a classificação da força de alguns exemplos de senhas.

	Enable	Secret user	User name	Password		Class A	Class B
1	☒	☐	user1	5A@C4@6B5	strong	☒	☒
2	☒	☐	user2	5AC46B	medium	☒	☒
3	☒	☐	user3	3	weak	☒	☐

Figura 3.7: Exemplos de classificação da força de senhas.

Diretrizes para criação de senhas fortes:

- Utilizar no mínimo oito caracteres
- Combinar letras maiúsculas, minúsculas, números e caracteres especiais
- Evitar palavras presentes em dicionários
- Evitar sequências do teclado, como 123456 ou asdfg
- Evitar caracteres repetidos, como AAAA
- Evitar sequências alfabéticas, como ABCD

3.2.4 Proteção das Configurações de Senha

Habilitar o modo *Read-only* impede que usuários não autorizados modifiquem configurações de segurança ao obter o arquivo original do projeto. Nesse modo:

- As configurações de segurança não podem ser alteradas
- As senhas são exibidas de forma mascarada
- O acesso administrativo requer a senha original

Para ativar acesse a aba *Security*, clique em *Editable* e configure as opções de *Read-only Settings*, conforme mostrado na [Figura 3.8](#).

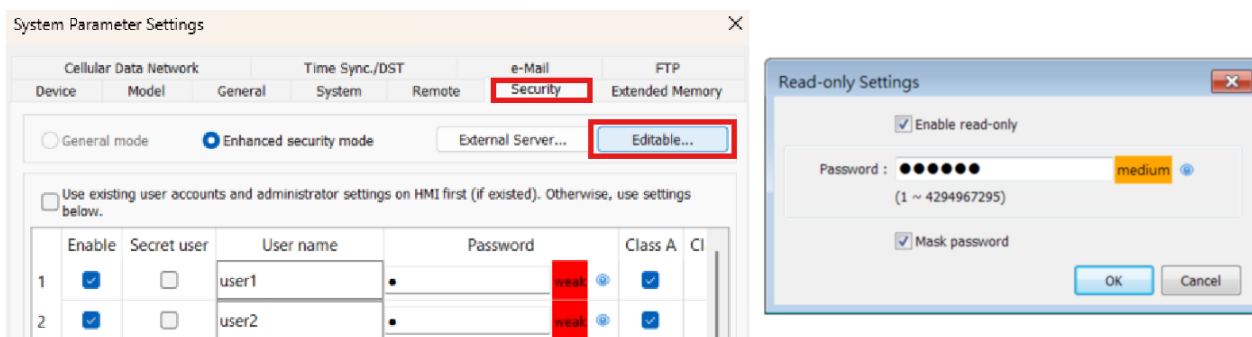


Figura 3.8: Habilitando modo somente leitura.

3.2.5 Habilitar Logout Automático

Para evitar acesso não autorizado utilizando sessões abertas, recomenda-se habilitar logout automático em IHMs inativas. No EasyBuilder Pro, clique em *Home* → *System Parameters* → *System* e ative *Auto logout*. A [Figura 3.9](#) apresenta a tela para habilitar o logout automático.

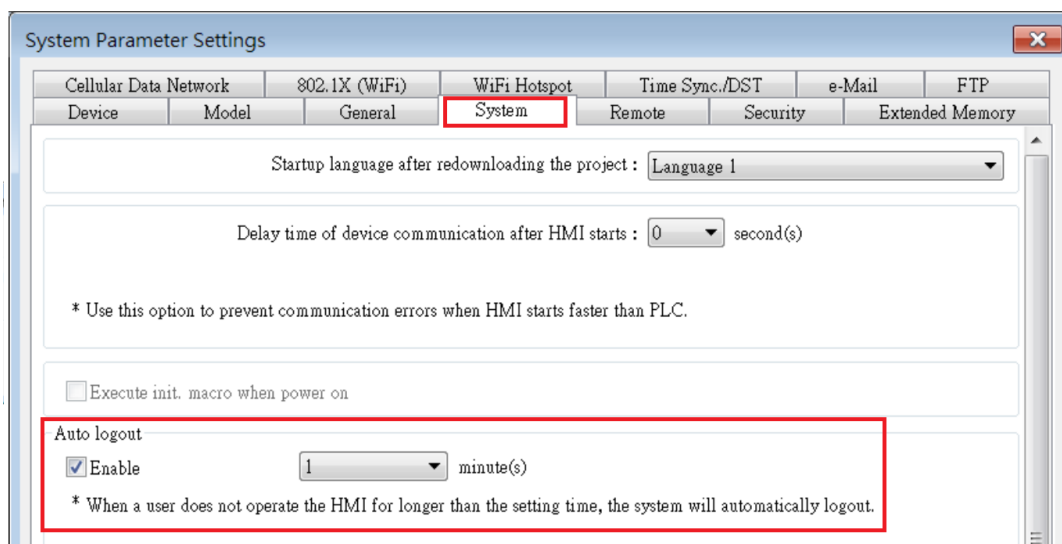


Figura 3.9: Habilitando logout automático.

3.2.6 Sincronização de Tempo via Servidor NTP

Para manter registros e logs corretos, recomenda-se sincronizar regularmente o horário da IHM com um servidor NTP. No EasyBuilder Pro, clique em *Home* → *System Parameters* → *Time Sync/DST* e Active *Enable time synchronization via NTP server*, como indicado na Figura 3.10.

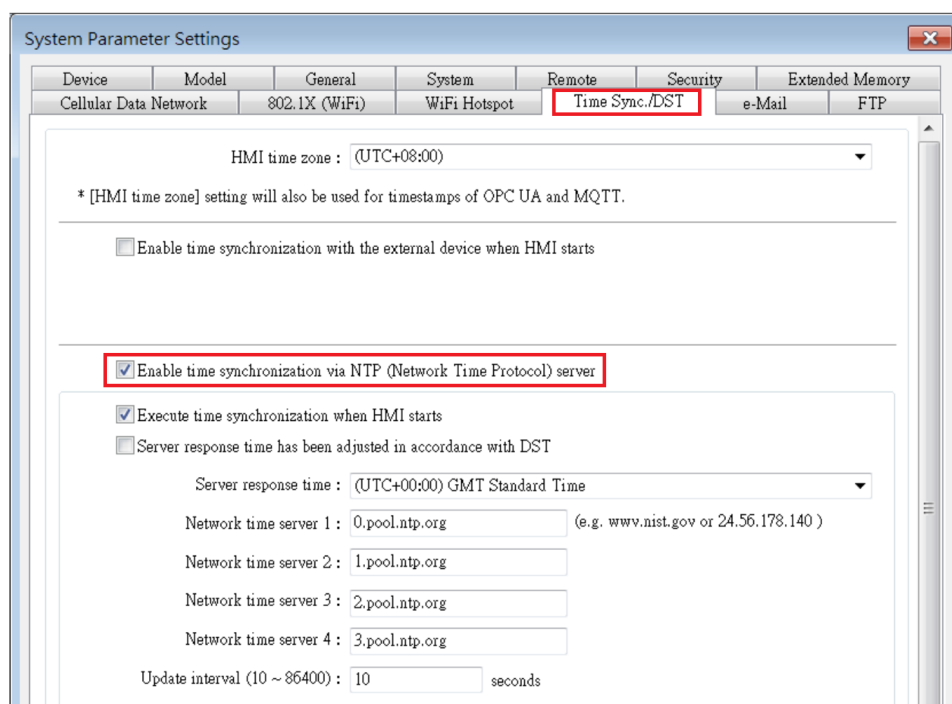


Figura 3.10: Sincronização de data e hora.

3.2.7 Segurança de Objetos

O elemento operacional básico de uma IHM é o objeto. Recomenda-se habilitar o controle de segurança para cada objeto operável, permitindo confirmação antes da execução de comandos e restrição baseada em permissões de usuário. Para configurar, crie um novo objeto ou abra as propriedades do objeto com um duplo clique sobre ele, acesse a aba *Security*. A Figura 3.11 mostra a tela para configuração da segurança dos objetos.

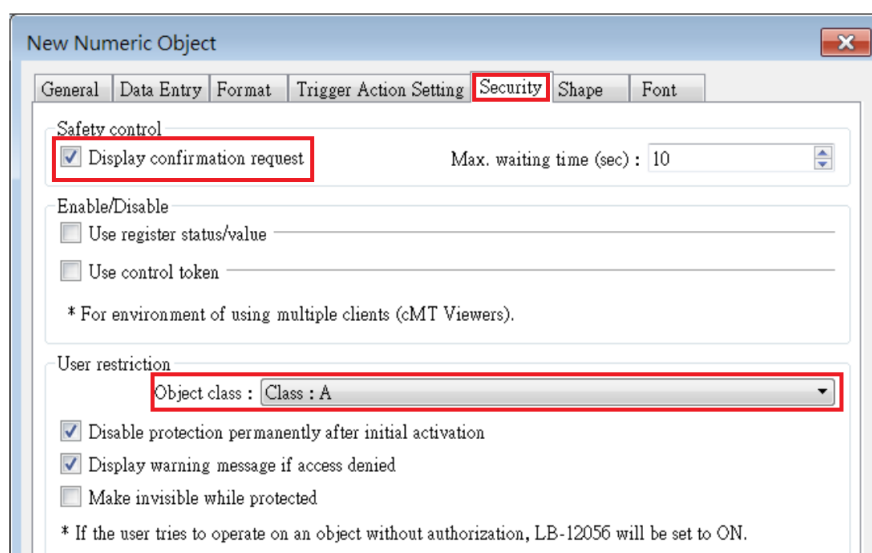


Figura 3.11: Configurando a segurança de objetos.

3.2.8 Registro de Operações

Sempre que uma operação for executada em objetos da IHM, o *Operation Log* pode registrar informações como:

- Data e hora
- Nome do usuário
- Classe do objeto
- Número da janela
- Nome do objeto
- Comentários definidos pelo usuário
- Tipo de ação executada
- Endereço de memória
- Alterações realizadas

Os registros são armazenados por padrão na memória da IHM em formato de banco de dados SQLite e também podem ser copiados para dispositivos externos como unidades USB. Para habilitar o registro acesse *Data/History* → *Operation Log Settings* e configure os objetos que terão suas operações registradas, como mostrado na Figura 3.12.



NOTA!

Utilize a função *Object Filter* para definir quais objetos devem ser exibidos.



ATENÇÃO!

Recomenda-se cautela ao configurar essa página, pois configurações incorretas podem causar perda de dados. Também é recomendável sincronizar registros com dispositivos externos caso o espaço da IHM seja insuficiente.

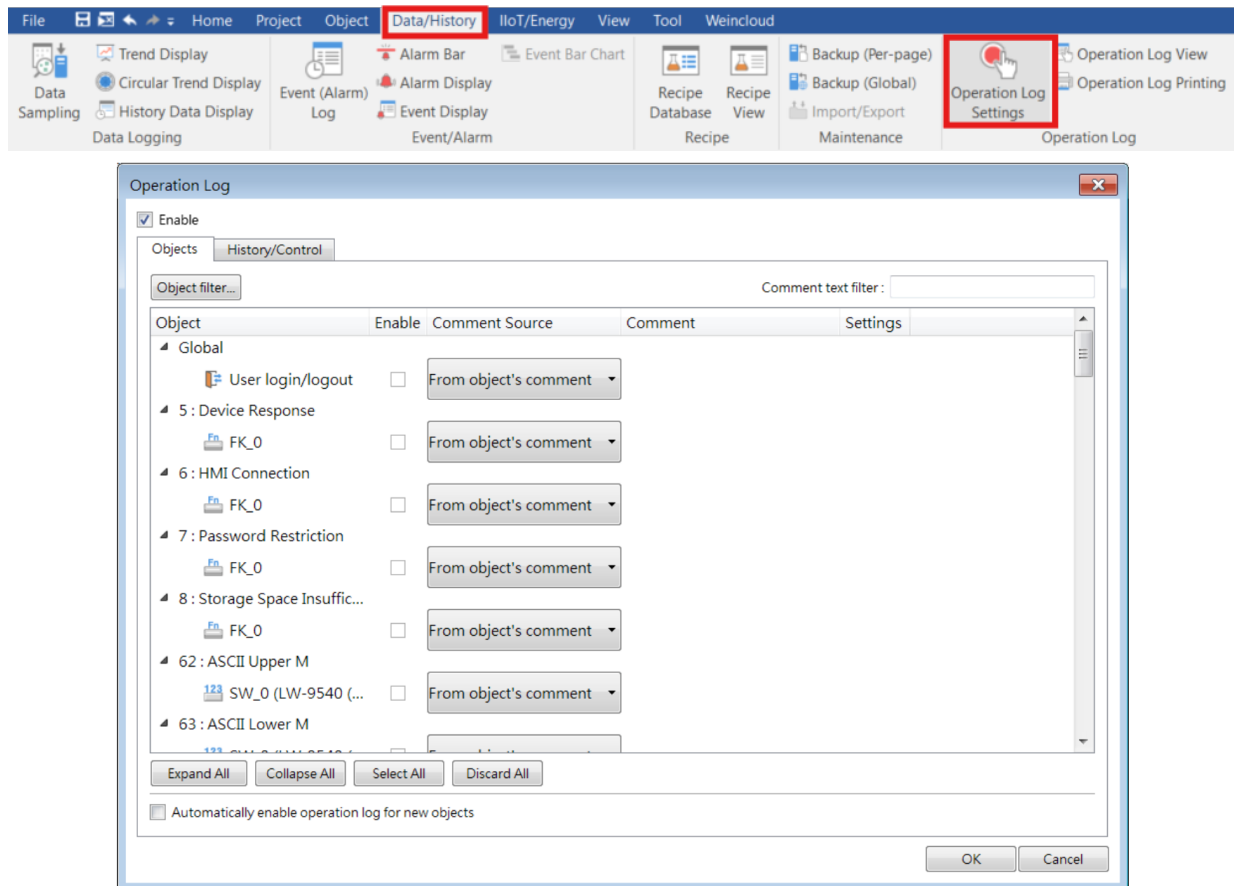


Figura 3.12: Configurando registros de operações.

4 RISCOS DURANTE A OPERAÇÃO DO PRODUTO

4.1 AUTORIZAÇÃO DE LOGIN

Para acessar a página de configuração web da IHM da série cMTx, abra um navegador (como Edge, Chrome ou Firefox) e insira o endereço IP do dispositivo. Caso a interface WebView apareça após inserir o IP, utilize o endereço: https://<ihm_ip>/admin para acessar a página de login de parâmetros do sistema EasyWeb 2.0.

A autorização dentro do sistema é dividida em três níveis:

- **Admin:** possui o nível máximo de autorização e pode modificar todas as configurações.
- **Update:** possui permissões limitadas para alteração de configurações.
- **History:** possui permissões para acessar os dados de log e seu backup.



NOTA DE CIBERSEGURANÇA!

Recomenda-se configurar senhas distintas para administradores e operadores, a fim de evitar que contas de operador obtenham privilégios administrativos.

Por motivos de segurança, a confirmação de senha é exigida antes do acesso às configurações. Além disso, o acesso à seção *History* também requer autenticação de senha, permitindo visualizar os logs armazenados. A [Figura 4.1](#) apresenta a página de login do sistema.

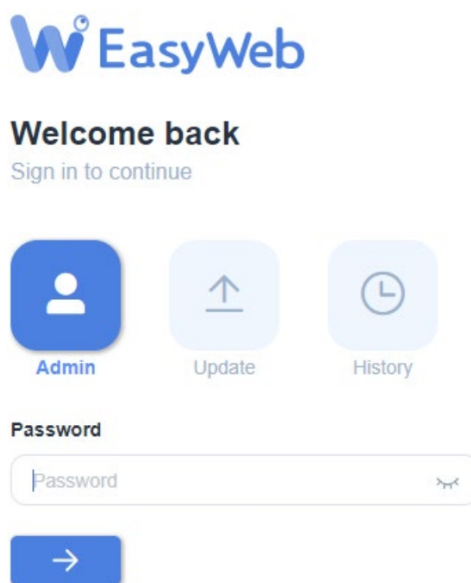


Figura 4.1: Autorização de login no sistema.

4.2 SEGURANÇA DOS ARQUIVOS DE LOG

A segurança dos arquivos de log gerados por *Data Sampling*, *Event Log* e *Operation Log* pode ser aprimorada utilizando as medidas descritas nas seções seguintes.

4.2.1 Prolongar a Vida Útil da Memória Flash

Devido ao número limitado de ciclos de escrita da memória flash interna da IHM, escritas frequentes ou em grande volume de dados podem reduzir a vida útil da memória. Isso pode resultar em:

- Dados ilegíveis
- Falha de inicialização da IHM

Recomenda-se manter a velocidade média de escrita na memória flash abaixo de 1200 KB/min. Essa informação pode ser consultada nas configurações do sistema da IHM, conforme indicado na [Figura 4.2](#).

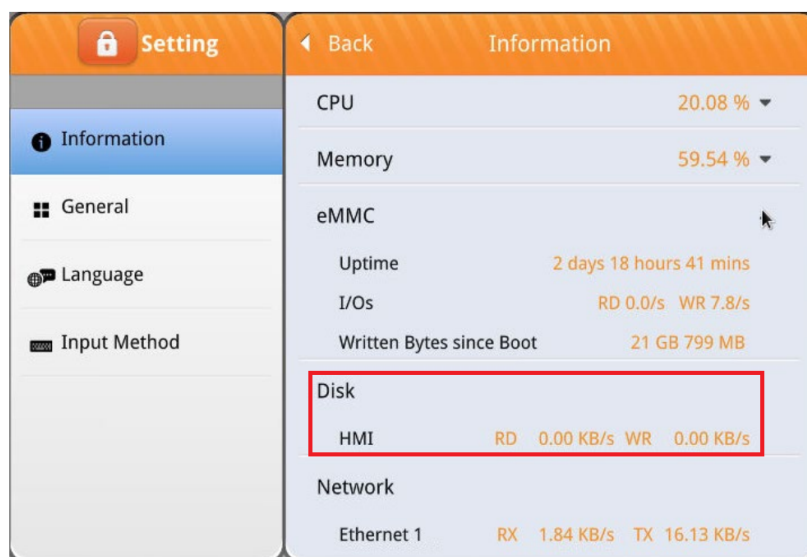


Figura 4.2: Velocidade média de escrita na memória flash.

4.2.1.1 Recomendações para reduzir a velocidade de escrita

Data Sampling

- Se logs não forem necessários, desabilite a opção de salvar logs.
- Configure intervalos de amostragem maiores.
- Reduza a frequência de envio de comandos síncronos para endereços de controle.
- Caso utilize tratamento personalizado de arquivos, reduza a frequência de troca de arquivos.
- Caso utilize sincronização automática periódica, aumente o intervalo de sincronização.

Event Log

- Se logs não forem necessários, desabilite o armazenamento de logs.
- Caso não seja utilizado para alarmes, evite habilitar a opção *Save to history*.
- Reduza a frequência de envio de comandos síncronos.
- Utilize o modo *Aggregate* para limitar a frequência de escrita na memória flash.

Operation Log

- Reduza a frequência de envio de comandos síncronos para endereços de controle.
- Utilize o modo *Aggregate* para limitar a frequência de escrita.



NOTA!

Antes de desligar a IHM, configure o registrador de sistema **LB-9034** como ON para garantir que os logs sejam completamente gravados na memória flash.

4.2.2 Salvar ou Fazer Backup dos Logs em Dispositivo Externo

Recomenda-se salvar ou realizar backup dos logs em dispositivos externos, como:

- Unidades USB
- Cartões SD
- Servidores de banco de dados

Isso ajuda a evitar perda de dados quando o espaço de armazenamento da IHM for insuficiente. Na [Figura 4.3](#) são mostradas as opções de armazenamento disponíveis para os logs e backup global da IHM.

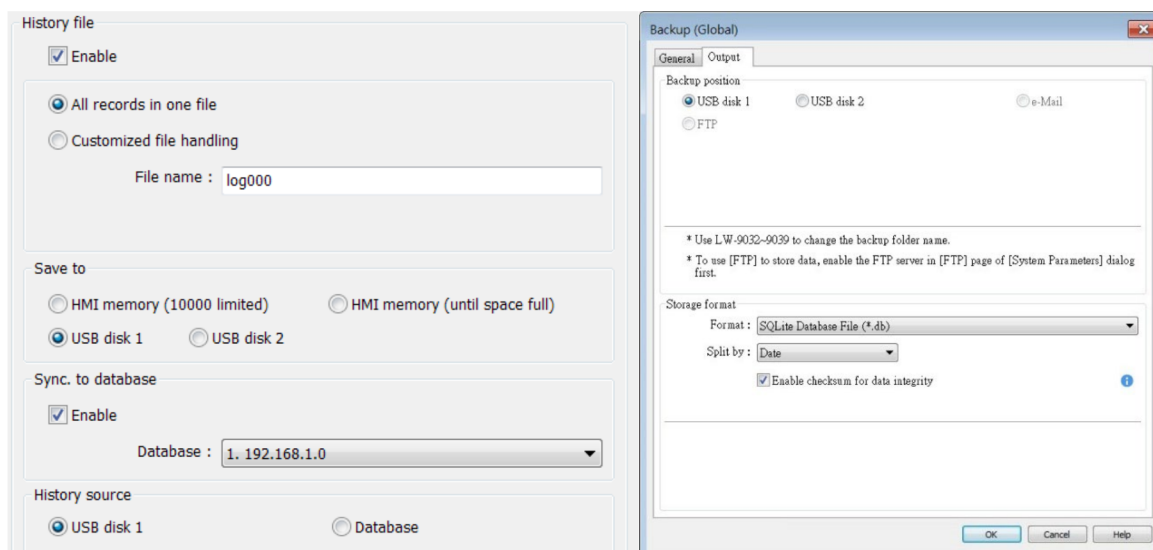


Figura 4.3: Exemplo de backup de logs.

4.2.2.1 Recomendações para uso de USB e SD

Dispositivos USB e cartões SD também possuem limites de ciclos de escrita.

- Utilize dispositivos com maior capacidade (por exemplo, 32 GB).
- Realize backups remotos periodicamente (por exemplo, anualmente).

4.2.2.2 Recomendações para uso de servidor de banco de dados

- Habilitar RAID.
- Realizar backups remotos periódicos.

4.2.3 Habilitar Checksum para Integridade dos Dados

A ferramenta *EasyConverter* permite abrir arquivos SQLite em um computador e visualizar dados de backup, além de exportá-los para formatos Excel ou CSV. Caso os arquivos de backup contenham *checksums*, o EasyConverter poderá verificar a integridade dos dados. Para habilitar esse recurso, ative a opção *Enable checksum for data integrity* ao gerar arquivos de backup, como indicado na Figura 4.4. Esse recurso é suportado apenas nas séries cMTx.

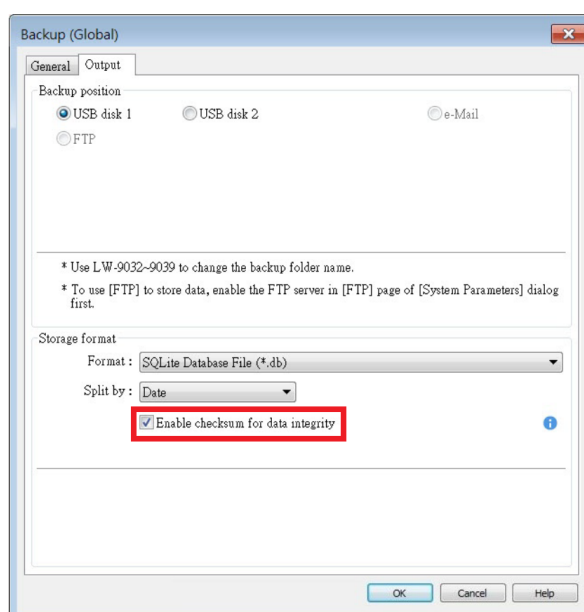


Figura 4.4: Configuração de checksum para arquivos de backup.

O EasyConverter também pode verificar a integridade dos arquivos de backup. Caso qualquer alteração indevida seja detectada durante a verificação, um alerta será exibido.

5 RISCOS DURANTE A MANUTENÇÃO REMOTA

5.1 SEGURANÇA DE COMUNICAÇÃO

5.1.1 Desabilitar Funções Desnecessárias

Ao utilizar uma IHM, recomenda-se desabilitar funções que não estejam sendo utilizadas ou pelo menos protegê-las por senha. Dentre as funções que podem ser desabilitadas, podem-se citar:

- Remote HMI
- PLC Control (change page)
- Modbus Server
- VNC Server
- cMT Diagnoser (cMTx Series)
- OPC UA Server (em alguns modelos cMTx)

As funções de acesso remoto da IHM, VNC server e cMT Diagnoser podem ser habilitados e desabilitados em *System Parameter* → *Remote*, conforme mostrado na imagem [Figura 5.1](#).

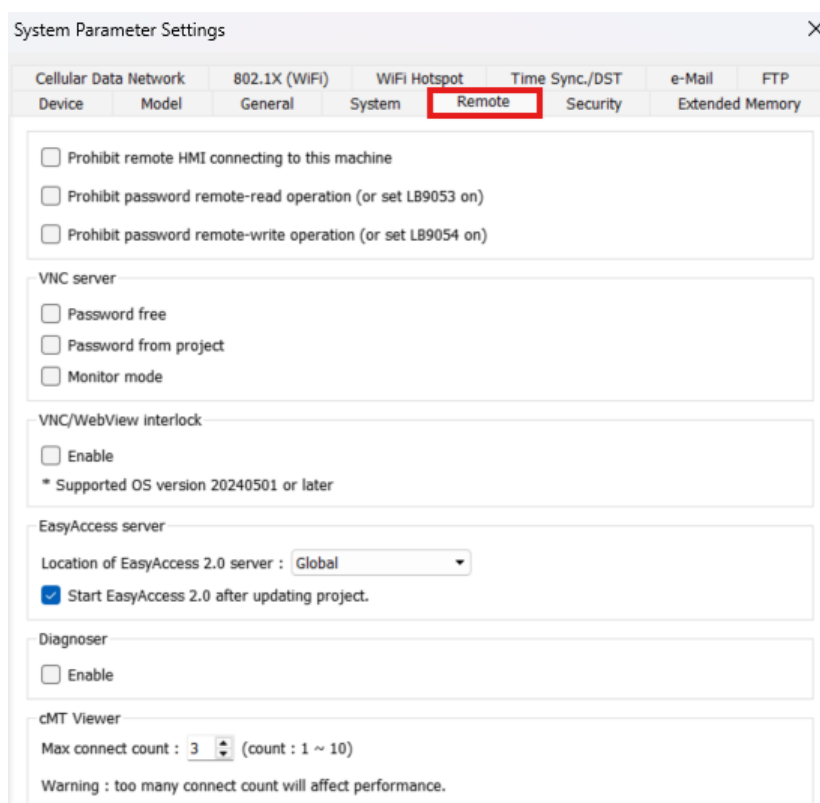


Figura 5.1: Opções de acesso remoto da IHM.

5.1.2 Servidor Modbus

Quando um servidor Modbus é utilizado em um projeto IHM, acesse *System Parameters* → *Device* → *Settings/Security*. Ative as opções *LW Protection* e *RW Protection*, como demonstrado na [Figura 5.2](#). Isso evita alterações não intencionais nos registradores do sistema durante a comunicação entre a IHM e clientes Modbus.



NOTA!

Para configurar o intervalo de LW ou RW protegido, consulte o intervalo suportado pelos parâmetros de sistema.

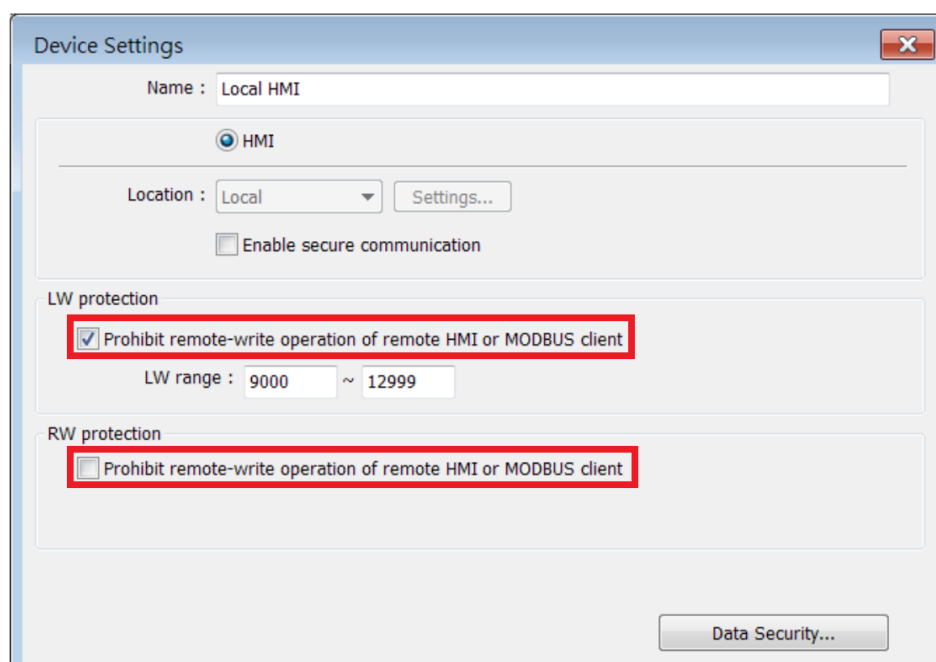


Figura 5.2: Configuração de proteção LW para comunicação Modbus.

5.1.3 MQTT

Quando MQTT é utilizado em um projeto IHM, recomenda-se utilizar criptografia TLS 1.2. Também é necessário importar:

- Certificado da Autoridade Certificadora (CA)
- Certificado do cliente
- Chave privada

Nas configurações do objeto MQTT Server, habilite os recursos de criptografia e verificação na aba *TLS/SSL*, como indicado na Figura 5.3.

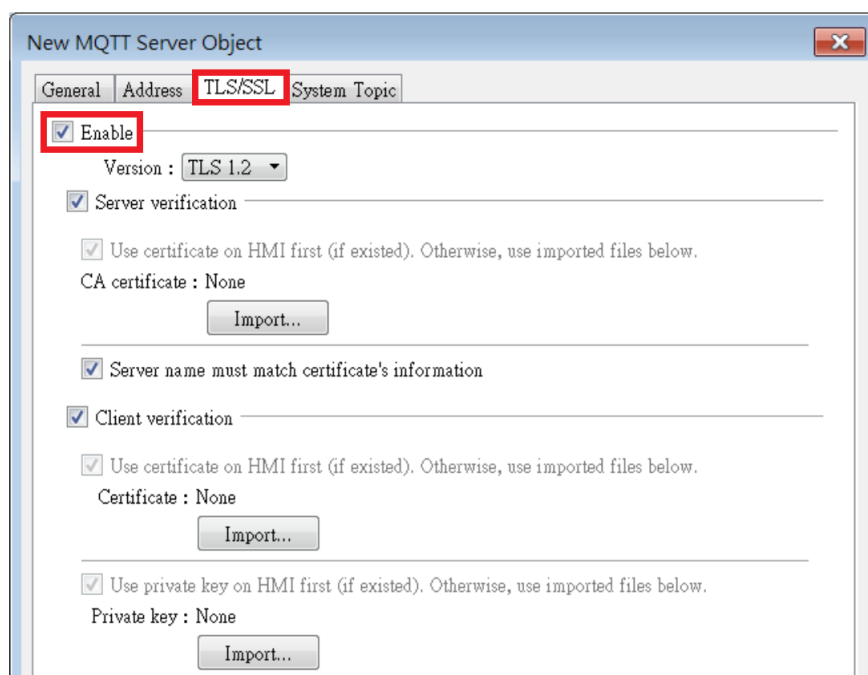


Figura 5.3: Configuração de criptografia TLS/SSL para MQTT.

5.1.4 Servidor OPC UA

Caso um servidor OPC UA seja utilizado no projeto IHM, recomenda-se desabilitar comunicação em texto simples e utilizar apenas comunicação criptografada. Na aba *General* das configurações do servidor OPC UA, *desabilite* a opção *None* na política de segurança, como mostrado na [Figura 5.4](#). Isso garante que os clientes se comuniquem apenas com dados criptografados.

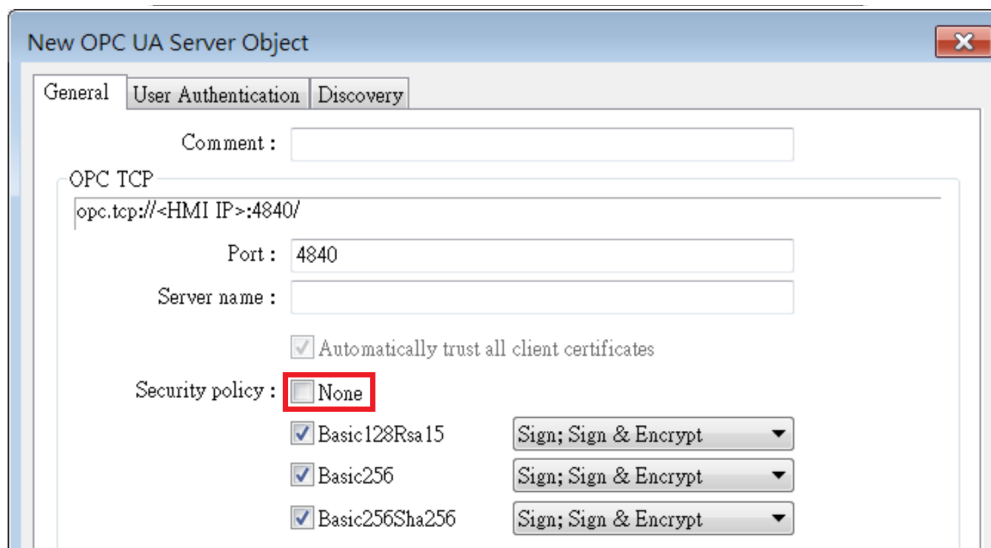


Figura 5.4: Configuração de política de segurança do servidor OPC UA.



NOTA DE CIBERSEGURANÇA!

As políticas de segurança Basic128Rsa15 e Basic256 não são mais consideradas seguras por conta do algoritmo de hash SHA-1. Essas políticas são suportadas apenas para fins de compatibilidade.

5.1.5 Servidor de Banco de Dados

Quando um servidor de banco de dados é utilizado em um projeto com IHM, recomenda-se habilitar criptografia TLS 1.2. Também deve ser importado o certificado da autoridade certificadora (CA).

Nas configurações do objeto Database Server, habilite criptografia e verificação na aba *TLS/SSL*, conforme a [Figura 5.5](#).

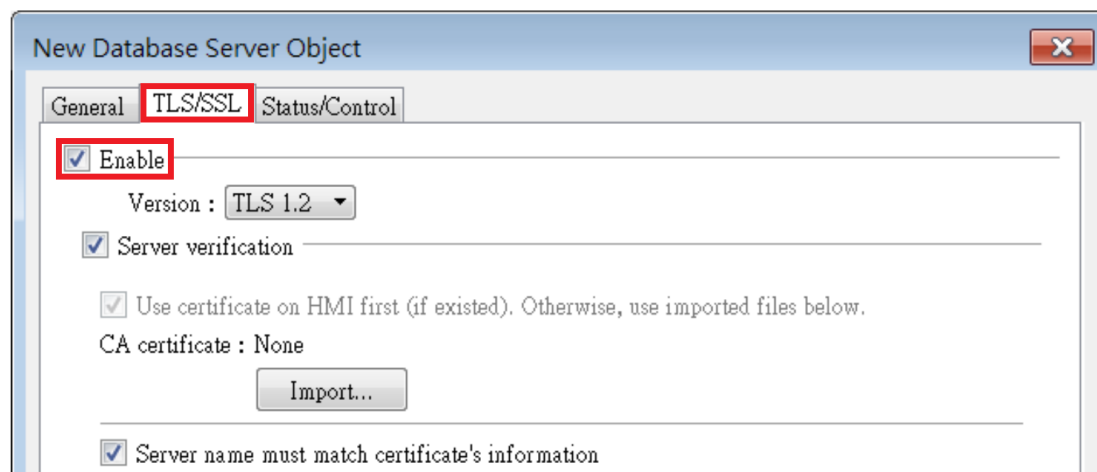


Figura 5.5: Configuração de criptografia TLS/SSL para servidor de banco de dados.

RISCOS DURANTE A MANUTENÇÃO REMOTA

5.1.6 E-mail

Quando a funcionalidade de envio de e-mail for utilizada no projeto IHM, recomenda-se:

- Utilizar um servidor SMTP que exija autenticação
- Utilizar conexão criptografada TLS/SSL

Após habilitar a função de e-mail nas configurações do sistema, marque a opções *SMTP server requires authentication* e *Use the following type of encrypted connection*, conforme a [Figura 5.6](#).

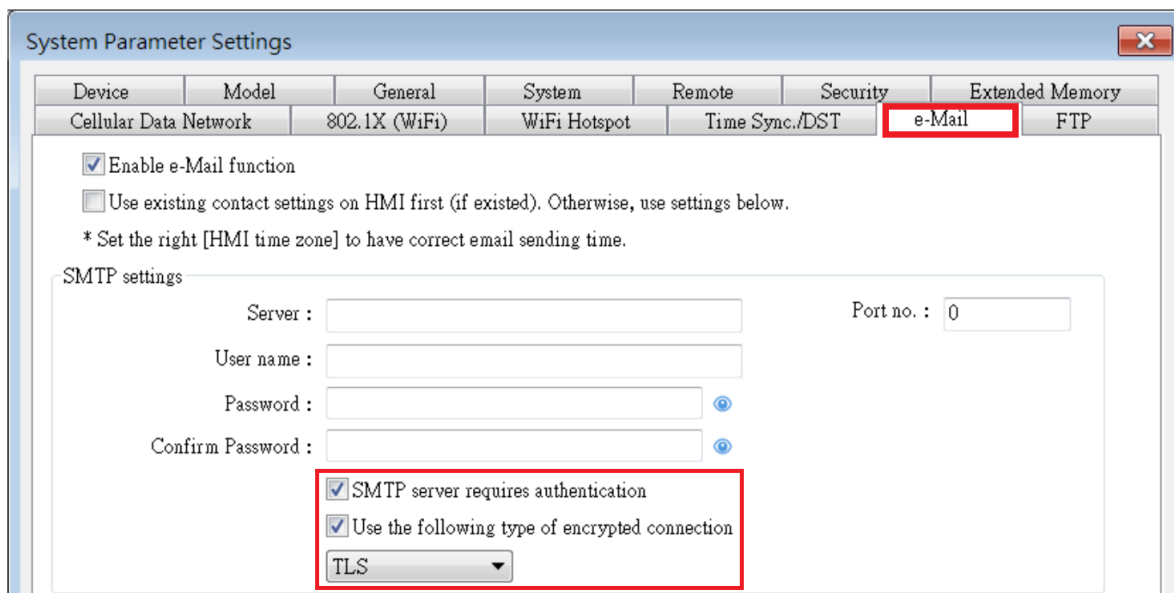


Figura 5.6: Configuração de criptografia para envio de e-mails.

5.1.7 Monitoramento Remoto cMT Viewer

Caso seja necessário monitoramento remoto das IHMs da séries cMTx, é possível utilizar o aplicativo *cMT Viewer*. Recomenda-se configurar senhas para diferentes níveis de permissão nas configurações do sistema da IHM, como mostrado na [Figura 5.7](#). Essas mesmas senhas devem ser utilizadas no *cMT Viewer* para acesso às telas.



Figura 5.7: Configuração de senha do sistema para acesso remoto.



NOTA!

O número máximo de acessos simultâneos da IHM pelo *cMT Viewer* pode ser limitado em *System Parameters* → *Remote*, como mostrado na [Figura 5.1](#).

5.2 SEGURANÇA DA PÁGINA WEB

Quando uma IHM da série cMTx é utilizada, o usuário pode acessar a interface EasyWeb 2.0 por meio de um navegador. Nessa interface é possível:

- Configurar o endereço IP da rede
- Fazer upload ou download de projetos
- Realizar backup de dados

Como essas funcionalidades envolvem operações críticas, recomenda-se aplicar as seguintes configurações de segurança.

5.2.1 Habilitar Criptografia HTTPS

Recomenda-se habilitar comunicação criptografada HTTPS. Após acessar o EasyWeb 2.0 acesse o menu *Administration*, abra a página *Security* e habilite a opção *Force HTTPS*, como demonstrado na [Figura 5.8](#).

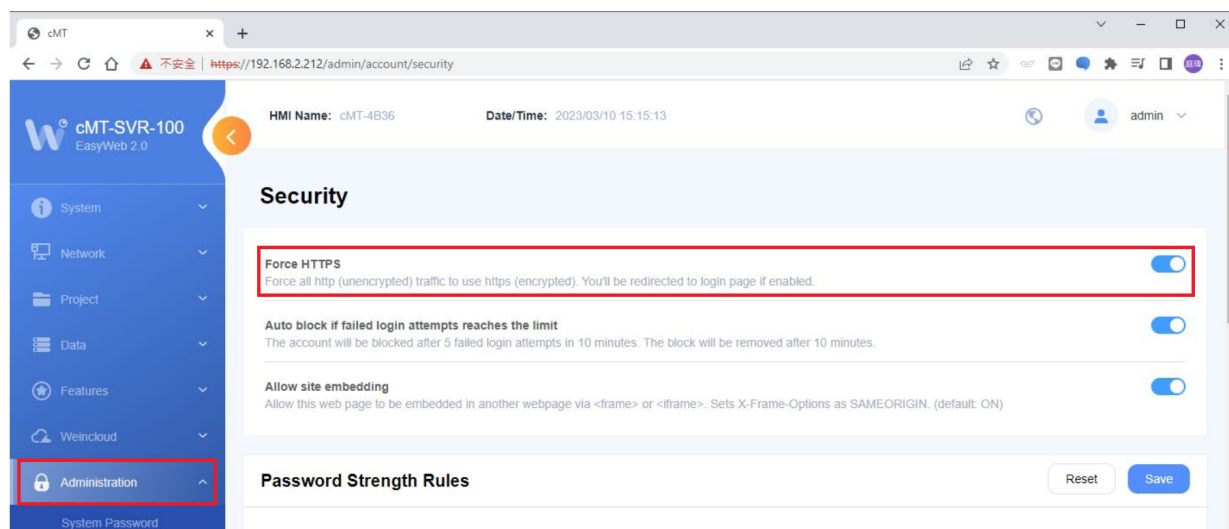


Figura 5.8: Configuração para forçar uso de HTTPS.

5.2.2 Habilitar Regras de Força de Senha

Recomenda-se habilitar regras de força de senha para impor requisitos de:

- Comprimento mínimo
- Uso de letras maiúsculas e minúsculas
- Números
- Caracteres especiais

Na seção *Password Strength Rules*, configure as opções destacadas na [Figura 5.9](#) e clique em *Save*.

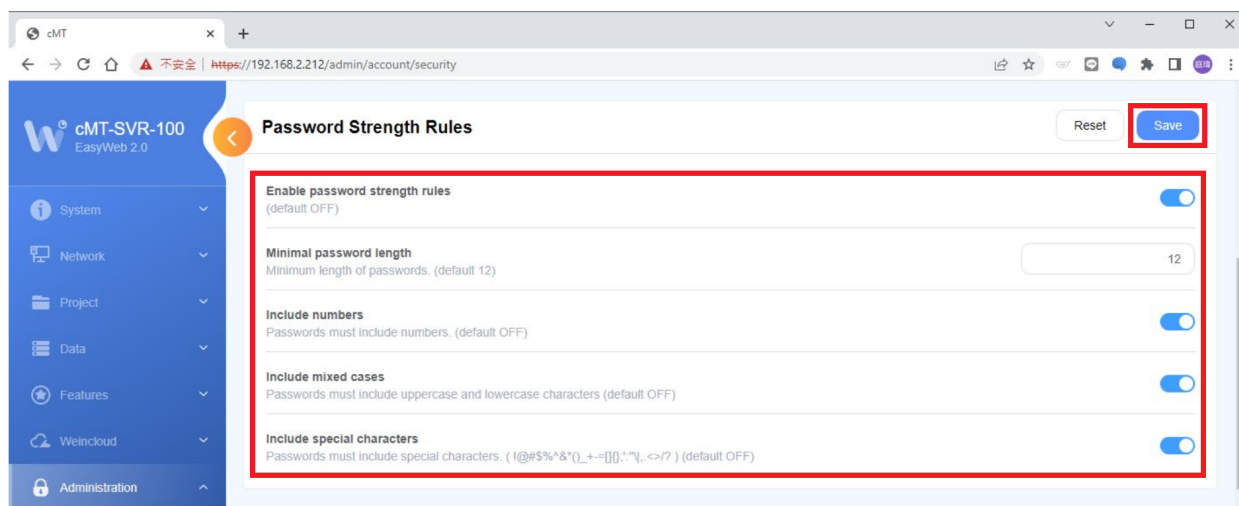


Figura 5.9: Configuração de regras de força de senha.

RISCOS DURANTE A MANUTENÇÃO REMOTA

5.2.3 Habilitar Expiração de Senha

Recomenda-se habilitar expiração de senha para exigir atualização periódica das credenciais. Na seção *Password Expiration*, configure o número de dias de validade da senha, como indicado na [Figura 5.10](#) e clique em **Save**.

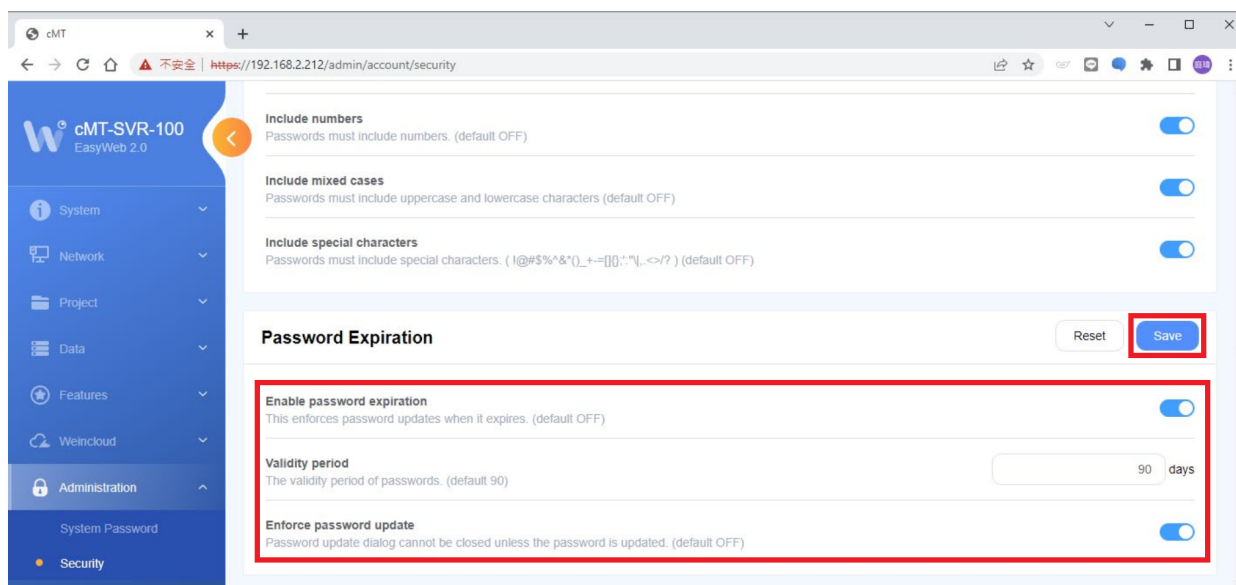


Figura 5.10: Configuração de expiração de senha.

5.2.4 Bloqueio Automático após Tentativas de Login

Recomenda-se habilitar bloqueio automático quando ocorrerem várias tentativas de login com senha incorreta. Quando essa opção está habilitada, o sistema é bloqueado após 5 tentativas consecutivas de login inválido e o bloqueio permanece ativo por aproximadamente 10 minutos. A configuração pode ser feita na página *Security* do menu *Administration*, como demonstrado na [Figura 5.11](#).

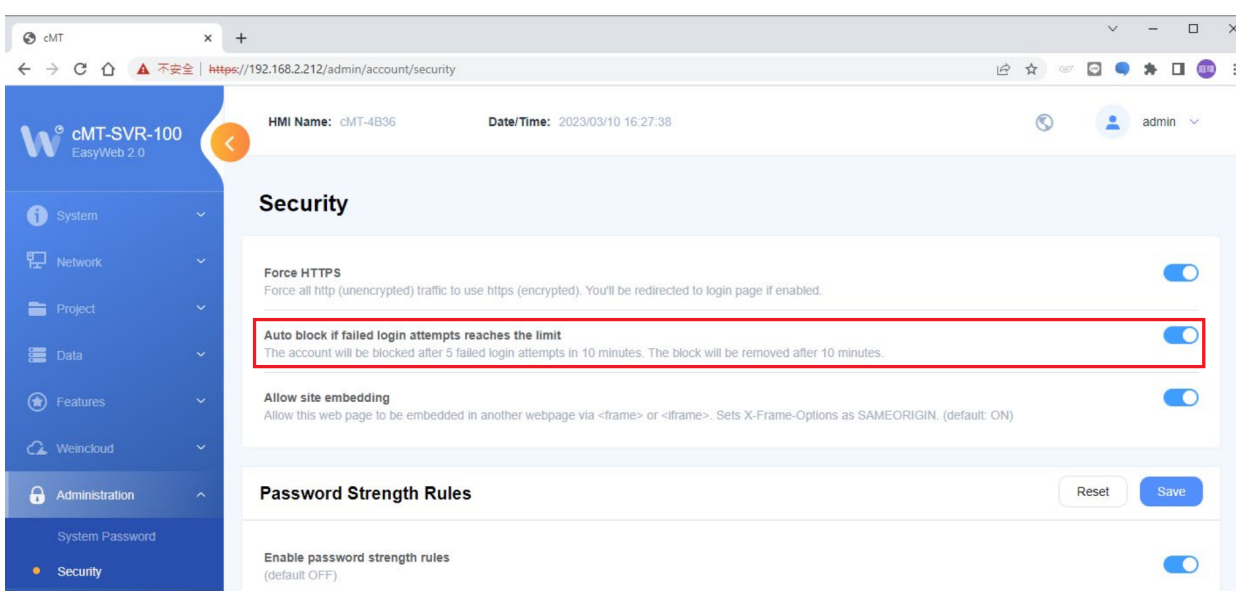


Figura 5.11: Configuração de bloqueio automático após falhas de login.

5.2.5 Alterar Senha do Sistema

Após configurar as opções de segurança da interface web, recomenda-se alterar a senha do sistema para uma senha mais forte. Para alterar, acesse *Administration*, abra a página *System Password* e configure a nova senha, como mostrado na [Figura 5.12](#).

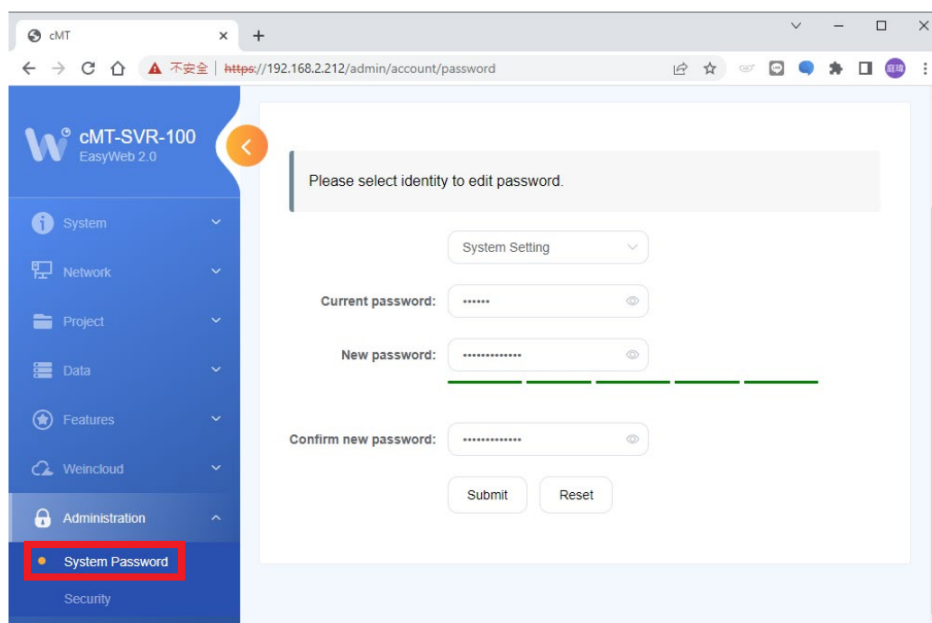


Figura 5.12: Configuração de alteração de senha do sistema.

5.3 ATIVIDADES REGULARES DE MANUTENÇÃO DE SEGURANÇA

A realização de atividades regulares de manutenção de segurança da informação é essencial para manter a proteção contínua do sistema e dos dados. Práticas recomendadas incluem:

- Atualizações regulares de software para garantir que sistemas operacionais, aplicações e firmware estejam atualizados com os últimos patches de segurança.
- Alteração periódica de senhas utilizando combinações robustas de letras, números e caracteres especiais.
- Execução de backups regulares de dados e armazenamento em locais seguros.
- Fortalecimento de firewalls e sistemas de prevenção de intrusão.
- Execução periódica de varreduras de vulnerabilidade e testes de segurança.
- Revisão periódica de permissões de acesso para garantir que apenas usuários autorizados tenham acesso a recursos sensíveis.
- Monitoramento regular de logs do sistema e aplicações para detectar incidentes ou comportamentos anormais.
- Realização de auditorias de segurança internas ou externas para verificar a conformidade com boas práticas e padrões de segurança.

6 DIRETRIZES PARA DESCARTE SEGURO DO PRODUTO

Esta seção descreve os procedimentos para descarte seguro do produto, a fim de evitar problemas de segurança da informação, como vazamento de dados sensíveis, quando um produto IHM é retirado de operação ou desativado.

6.1 RECOMENDAÇÕES PARA DESCARTE SEGURO

Ao desativar permanentemente uma IHM, recomenda-se seguir as práticas abaixo para garantir que informações armazenadas no dispositivo não sejam expostas.

- Remover a IHM do equipamento ou sistema sem causar danos físicos ao dispositivo.
- Apagar completamente programas e dados de configuração armazenados na IHM realizando um reset do sistema.
- Excluir de forma segura os logs armazenados tanto na IHM quanto em dispositivos externos de armazenamento.
- Realizar o descarte físico seguro do equipamento, se necessário por meio de destruição física, para evitar possível vazamento de dados que não possam ser completamente removidos do dispositivo.



BRASIL

WEG DRIVES & CONTROLS - AUTOMAÇÃO LTDA.

Av. Prefeito Waldemar Grubba, 3000

89256-900 - Jaraguá do Sul - SC

Telefone: 55 (47) 3276-4000

Fax: 55 (47) 3276-4060

www.weg.net