CLIQ® Web Manager

Manual do usuário

IKON
ASSA ABLOY

assaabloy.com

Experience a safer
and more open world

ASSA ABLOY is committed to operating in compliance with data laws globally across its various divisions. The EU General Data Protection Regulation ("GDPR") requires us to meet principles of fairness, accountability and transparency in handling personal data.

ASSA ABLOY has a focused, structural and systemic approach to data protection and privacy. Our globally applicable ASSA ABLOY Data Protection Compliance Program has been developed to protect the integrity of the personal data of our employees, customers and partners worldwide. ASSA ABLOY has dedicated resources across the Group whose continual focus is the compliance with data laws globally including the GDPR.

We keep personal data secure using equipment operating in accordance with recognized security standards. In cases where the rights of individuals are at risk, we conduct impact assessments in accordance with our standard methodology.

We recognize that data laws are continuously evolving. ASSA ABLOY has invested considerable resources in raising awareness and rolling out training in relation to its Data Protection Compliance Program. We continuously monitor data protection developments to ensure our policies, processes and procedures are relevant and adequate.

We are committed to ensuring good data governance and are invested in data trust and security for the long-term.

ASSA ABLOY
Sicherheitstechnik GmbH

Attilastrasse 61-67
12105 Berlim
ALEMANHA
Tel. + 49 30 8106-0
Fax: + 49 30 8106-26 00
berlin@assaabloy.com

www.assaabloy.de

Program version: V 2025.1
Main document number: D001583864
Date published: 2025-05-22
Language: pt-BR

1 Visão geral

1.1 Introdução

O CLIQ Web Manager (CWM) é um sistema de software da Web que possibilita o gerenciamento e o controle do CLIQ, um Sistema Cliq eletromecânico que fornece controle total sobre autorizações de acesso e atividades do proprietário da chave. O sistema CLIQ apresenta a solução que assegura a confiabilidade de chaves e cilindros mecânicos, bem como a segurança e a flexibilidade inerente às fechaduras eletrônicas.

1.2 Recursos principais

- **Fácil de instalar** - o CLIQ é um sistema off-line eficiente em termos de custos que não exige fiação elétrica ou baterias.
- **Trilhas de auditoria** - O CLIQ possibilita o acesso a dados de auditoria precisos de cada cilindro e chave de um Sistema Cliq.
- **Chaves individuais** - Protegidas por poderosas chaves criptográficas, cada chave foi projetada para uso individual. Se a chave for perdida ela é simplesmente transformada em obsoleta e uma chave nova é gerada em seu lugar.
- **Autorização baseada em tempo** - O CLIQ permite a definição de uma Janela de programação com um intervalo de tempo específico durante o qual é permitido o acesso.
- **Gestão de chave**- O CLIQ Web Manager mantém um registro da entrega de chaves a vários proprietários de chaves.
- **Cancelamento eletrônico de chave** - As chaves podem ser canceladas sem a presença física da mesma.
- **Revalidação de autorizações** - Adiciona segurança ao Sistema Cliq forçando os proprietários de chaves a obterem atualizações das permissões a partir de um dispositivo de programação próximo. Isso também assegura que a trilha de auditoria seja gravada no servidor e que esteja disponível para os administradores do Sistema Cliq.
- **Funções de agrupamento** para facilitar a administração. O CLIQ Web Manager possibilita o fornecimento de acesso a grupos de cilindros e grupos de pessoas com base, por exemplo, na posição geográfica ou no cargo na organização.

1.3 Sobre este manual

Conteúdo deste manual
Este manual consiste nas seguintes partes destinadas a grupos diferentes:

Seção	Para administradores	Para super administradores	Descrição
1 Visão geral	✓	✓	Uma introdução rápida ao CLIQ e a este manual.
2 Como configurar clientes no CWM	✓	✓	Descreve como configurar um cliente CWM.
3 Como iniciar o CWM	✓	✓	Descreve como começar a trabalhar com o CWM pela primeira vez.
4 Como trabalhar com o CWM	✓	✓	Descreve como executar todas as tarefas relevantes aos administradores ao trabalhar com o Sistema Cliq.
5 Como configurar os Sistemas Cliq		✓	Descreve como configurar um Sistema Cliq novo.
6 Como configurar os Sistemas Cliq		✓	Descreve como configurar os diversos aspectos de um Sistema Cliq.
7 Hardware do CLIQ	✓	✓	Descreve a arquitetura e os componentes do CLIQ.
8 Conceitos e recursos do CLIQ	✓	✓	Descreve como funciona a autorização e os conceitos dos recursos do CWM. Alguns conceitos são muito técnicos e se destinam somente a Super administradores do sistema.
9 Apêndice	✓	✓	Contém informações de referência.

Terminologia
Consulte *Seção 9.1.1 "Termos", página 194* e *Seção 9.1.2 "Siglas", página 195* para obter uma definição de termos e siglas usados neste manual.

As opções de menu no CWM são escritas como **Menu principal » Opção de menu**.

Os nomes das chaves abaixo diferem dos nomes usados no CWM e neste manual:

Nome da chave	Nome no CWM e neste manual
E1	Chave normal
E2	Chave Quartz
E3	Chave dinâmica

2 Como configurar clientes no CWM

2.1 Visão geral da configuração de clientes CWM

1) Instale o Programador local.

   Consulte *Seção 2.2 "Como instalar Programadores locais", página 12*.

2) Instale o CLIQ Connect em um computador.

   Consulte *Seção 2.3 "Como instalar o CLIQ Connect no computador", página 12*.

3) Configure o CLIQ Connect em um computador.

   Consulte *Seção 2.4 "Como configurar o CLIQ Connect no computador", página 13*.

2.2 Como instalar Programadores locais

1) Certifique-se que a conta do usuário Windows conectado atualmente tenha direitos de acesso de Administrador.
2) Conecte o cabo USB do Programador local com o PC.
3) Verifique se os drivers serão baixados e instalados automaticamente.

> **ATENÇÃO!**
> Tome nota da porta CM atribuída que é exibida na área de notificações. Ao entrar no aplicativo CLIQ Express ou no CLIQ Go, selecione a porta COM atribuída caso esta não seja encontrada automaticamente.
>
> Exemplo: `Porta COM virtual STMicroelectronics (COM7).`

4) Entre em contato com o suporte técnico caso os drivers não sejam instalados automaticamente.

2.3 Como instalar o CLIQ Connect no computador

O CLIQ Connect no computador é um software que trata a comunicação entre o programador local e o CLIQ Web Manager e também gera os certificados das chaves de comando.

Pré-requisitos:

- A conta do usuário Windows conectada atualmente tenha direitos de acesso de Administrador
- A chave de comando já tenha sido entregue e o proprietário da chave tenha recebido um e-mail do CLIQ Web Manager.

1) Faça o download e inicie o arquivo de instalação do CLIQ Connect no computador.

   O link para o arquivo pode ser encontrado nos seguintes locais:

   - No e-mail do CLIQ Web Manager
   - Na página de login do CWM
   - Na página de Boas-vindas de inscrição

2) Quando o instalador estiver carregado, selecione **idioma** e clique em **OK**.

O Assistente de configuração do CLIQ Connect abrirá.

3) Clique em **Próximo**.

4) Leia o contrato de licença. Se aceitar o contrato, selecione o botão de opção **Eu aceito o contrato** (necessário para continuar o assistente de configuração) e clique em **Próximo**.

> **ATENÇÃO!**
> Leia o **Contrato de licença** com atenção.

5) Execute um dos seguintes procedimentos;

- Como instalar o CLIQ Connect no computador pela primeira vez: Selecione o destino diretamente e clique em **Próximo**.
- Para atualizar uma instalação existente: Selecione **Sim** para atualizar uma instalação existente ou **Não** para instalar em outro diretório. Depois clique em **Próximo** para continuar.

6) Configurar os seguintes serviços externos:

- **Ativar atualizações automáticas** permite que o CLIQ Connect baixe automaticamente e instale a versão mais recente do software no computador.
- Retire a seleção de **CLIQ Go** e selecione **CLIQ Web Manager (chave de comando)**.

> **ATENÇÃO!**
> As duas configurações acima não poderão ser alteradas após a instalação ou processo de atualização.

- **Integração do serviço de diretório** permite que o CLIQ Connect obtenha automaticamente os detalhes de conexão do CLIQ Remote do Serviço de diretório central no computador. Caso o CLIQ Connect no computador não deva se conectar a qualquer serviço externo, exclua a seleção **Integração do serviço de diretório**. Nesse caso, a **URL do CLIQ Remoto** e a **URL de Inscrição CLIQ** deverão ser fornecidas manualmente.

7) Clique em **Próximo** para continuar.

8) Como instalar o CLIQ Connect no computador pela primeira vez:

   Selecione ou crie uma **Pasta do menu iniciar** onde colocar os atalhos do programa e clique em **Próximo** para continuar.

9) Aguarde enquanto os arquivos são extraídos e instalados.

10) Selecione se deseja executar o programa ou não quando terminar a configuração.

11) Clique em **Concluir** para sair da configuração.

2.4 Como configurar o CLIQ Connect no computador

2.4.1 Como configurar o CLIQ Connect com Seletor COM no computador

1) Clique no ícone **CLIQ Connect** com botão direito na bandeja do sistema.

2) Clique em **Seletor COM**.

3) Selecione a porta COM onde o PD local será conectado ou clique em **Auto** (padrão) para seleção automática da porta COM.

2.4.2 Como configurar o servidor do CLIQ Connect no computador

1) Clique no ícone **CLIQ Connect** com botão direito na bandeja do sistema.

2) Clique em **Configuração** e encontre a seção **Configuração do servidor**.

3) Caso a Integração do serviço de diretório esteja ativada:

   a) Selecione **Automaticamente**.

   b) Insira a **URL do diretório**.

4) Caso a Integração do serviço de diretório **não** esteja ativada:

   a) Selecione **Manual**.

   b) Insira a **URL do CLIQ Remoto** e a **URL de Inscrição CLIQ**.

5) Clique em **OK** para salvar e sair.

2.4.3 Como configurar o proxy do CLIQ Connect no computador

1) Clique no ícone **CLIQ Connect** com botão direito na bandeja do sistema.

2) Clique em **Configuração**.

3) Para **Proxy**, selecione **Ativar**.

4) Insira as informações solicitadas e clique em **OK**.

3 Como iniciar o CWM

3.1 Visão geral de como iniciar o CWM

Para novos administradores: Passo a passo para começar a usar o CWM.

Pré-requisitos:

- O CWM está instalado e configurado.
- A Chave de comando, o certificado da Chave de comando e o PIN da Chave de comando estão disponíveis.

1) Instale o certificado da Chave de comando.

   Consulte *Seção 3.2 "Como inscrever e instalar Certificados da chave de comando", página 15*.

2) Entre no CWM.

   Consulte *Seção 3.3 "Como fazer o log-in", página 17*.

3) Configure o idioma do CWM.

   Consulte *Seção 3.4 "Configuração do idioma do CWM", página 18*.

4) Leia *Seção 3.5 "Introdução à interface do usuário do CWM", página 18*.

As tarefas mais comuns utilizadas no CWM estão listadas no *Seção 3.6 "Tarefas comuns", página 21*.

3.2 Como inscrever e instalar Certificados da chave de comando

Para usar uma Chave de comando com o CWM, é necessário instalar um certificado específico no cliente do CWM.

O procedimento para instalar um certificado depende do fato de você usar ou não **Integração DCS**.

Instalação do certificado com Integração DCS
A chave de comando é inscrita e seu certificado é gerado diretamente no navegador da internet. Não há necessidade de obter o certificado separadamente.

Consulte *Seção 3.2.1 "Registro do certificado da Chave de comando via CLIQ Connect no computador", página 16* para obter mais informações.

Instalação manual de certificados
Um arquivo de certificado deverá estar disponível para instalar o certificado da Chave de comando manualmente.

Consulte *Seção 3.2.2 "Como instalar o certificado da chave de comando manualmente", página 16* para obter mais informações.

3.2.1 Registro do certificado da Chave de comando via CLIQ Connect no computador

Pré-requisitos:

- O Programador local está instalado.
- O software do CLIQ Connect está instalado no computador.

  Consulte *Seção 2.3 "Como instalar o CLIQ Connect no computador", página 12*.
- A chave de comando foi entregue no CWM.
- A Chave de comando recebe a permissão de inscrição.

  Normalmente, uma Chave de comando pode ser inscrita uma vez, porém esta configuração pode ser alterada por um administrador com direito de autorizações. Consulte *Seção 6.11.4 "Como editar as informações de uma chave de comando", página 134* para obter mais informações.
- A Chave de comando e seu código PIN estão disponíveis.

1) Insira a Chave de comando na ranhura esquerda do Programador local.
2) Clique com o botão direito do mouse no ícone CLIQ Connect na bandeja do sistema e selecione **Iniciar inscrição do certificado**.
3) Insira o código PIN da Chave de comando e clique em **Próximo**.

   Se o PIN inserido for verificado, será enviada uma senha de uso único ao e-mail do usuário da chave de comando.
4) Insira a senha de uso único e clique em **Próximo**.

   O certificado da chave de comando é criado e adicionado automaticamente nos navegadores da internet.
5) Clique em **Finalizado** para concluir o registro da chave de comando.

3.2.2 Como instalar o certificado da chave de comando manualmente

Pré-requisito:

- Foi obtido um arquivo **.p12** para a Chave de comando juntamente com uma senha.

1) Clique duas vezes no arquivo **.p12**.

   É exibido o **Assistente de importação de certificado**.
2) Selecione **Usuário atual** e clique em **Próximo**.
3) Verifique se o certificado correto está selecionado e clique em **Próximo**.
4) Insira a senha que foi fornecida com o arquivo **.p12** e clique em **Próximo**.
5) Selecione **Coloque todos os certificados no seguinte local de armazenamento** e clique em **Procurar**.
6) Na janela pop-up, selecione **Pessoal** e clique em **Próximo**.
7) Confirme a configuração e clique em **Concluir**.

   O certificado da chave de comando é instalado nos navegadores de internet suportados.

ATENÇÃO!
O certificado da chave de comando deve ser reinstalado se a senha da conta do usuário do Windows for alterada por um administrador. (Não é necessário quando os usuários alteram suas senhas.)

3.2.3 Como renovar o certificado da chave de comando

Quando o certificado da chave de comando possui 60 dias ou menos remanescentes antes de expirar, é exibida uma mensagem de aviso após o log-in.

- **Com a Integração DCS ativada**:

  Será enviado ao proprietário da chave um e-mail com uma breve descrição sobre como renovar o certificado.

  O certificado é renovado no CLIQ Connect e o processo é o mesmo que o processo de inscrição. Para obter mais detalhes, consulte *Seção 3.2.1 "Registro do certificado da Chave de comando via CLIQ Connect no computador", página 16*.

- **Sem Integração DCS**:

  O certificado novo é gerado no DCS e fornecido ao proprietário da chave.

  Para instalar um certificado novo, consulte *Seção 3.2.2 "Como instalar o certificado da chave de comando manualmente", página 16*.

Dica
Recomendamos remover o certificado antigo do navegador.

3.3 Como fazer o log-in

Pré-requisitos:

- O Programador local está instalado. Consulte *Seção 2.2 "Como instalar Programadores locais", página 12*.
- É usado um navegador de internet suportado. Consulte *Seção 9.8 "Requisitos do PC cliente", página 210*.
- O software CLIQ Connect está instalado e sendo executado no computador.

  Consulte *Seção 2.3 "Como instalar o CLIQ Connect no computador", página 12*.
- O software CLIQ Connect está configurado e conectado ao CWM.

  Consulte *Seção 2.4 "Como configurar o CLIQ Connect no computador", página 13*.
- Está disponível uma chave de comando com um código PIN. A chave de comando deve ser entregue para um funcionário no CWM.

ATENÇÃO!
Para sistemas com logon único (SSO), não é necessária uma chave para fazer login em determinadas operações depois que o certificado da Chave de comando for instalado. Consulte *Seção 8.10 "Logon único (SSO)", página 190* para obter mais informações.

- Está instalado um certificado válido para a chave de comando. Consulte *Seção 3.2 "Como inscrever e instalar Certificados da chave de comando", página 15*.
- Está disponível uma URL correta para o CWM.

3.3.1 Como fazer login com a Chave de comando

1) Insira a Chave de comando na ranhura esquerda do Programador local.
2) Vá para a página inicial de CWM.
3) Selecione o certificado para a chave de comando.

   Será exibida a página de login do CWM.
4) Clique em **Acessar**.
5) Insira o código PIN para a Chave de comando.

   O CLIQ Connect solicita que o uso da chave seja confirmado no computador.
6) Clique em **Confirmar**.

3.3.2 Como fazer login sem a Chave de comando

1) Vá para a página inicial de CWM.
2) Selecione o certificado para a chave de comando.

   Será exibida a página de login do CWM.
3) Clique em **Acesso com SSO**.

   Na maioria dos casos, a autenticação automática ocorre se o navegador já estiver conectado com as credenciais do domínio corporativo, o que permite o acesso direto ao CWM sem nenhuma ação adicional.

   Caso contrário, a janela de acesso do provedor de identidade será exibida.

3.4 Configuração do idioma do CWM

1) Selecione **Configurações » Selecionar idioma**.
2) Selecione o idioma desejado.

O idioma também pode ser selecionado clicando na bandeira correspondente na tela de acesso.

3.5 Introdução à interface do usuário do CWM

3.5.1 Menus principais

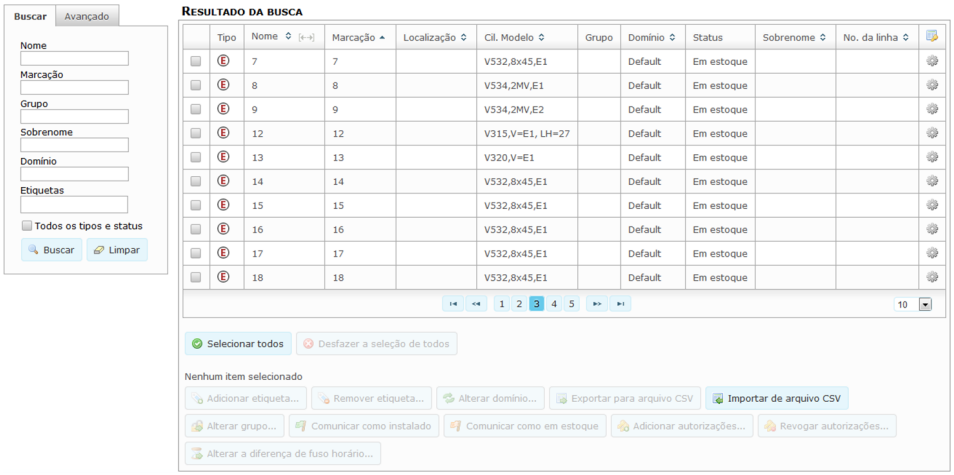
As opções do CWM estão divididas em quatro menus principais:

Tarefas	Contém as funções que são usadas mais comumente no trabalho diário.
Info do sistema	Contém funções para administrar direitos de acesso, informações sobre funcionários e visitantes, chaves, cilindros e programadores remotos.
Administração	Contém funções para configurar e ajustar o Sistema Cliq.
Configurações	Contém configurações pessoais relacionadas com o administrador conectado.

3.5.2 Como buscar objetos

Primeiro, use os critérios de pesquisa padrão
Para buscar objetos como cilindros ou chaves, selecione primeiro a opção de menu correspondente, por exemplo, **Informações do sistema » Cilindros**.

É exibido inicialmente um resultado de busca baseado no critério de busca padrão.



Em seguida, use as funções de pesquisa

Critério de busca		Para ajustar o critério de busca, insira um critério novo na caixa de busca à esquerda e clique em **Buscar**. Existem opções de busca menos comuns disponíveis na guia **Avançado**.
Wildcards		Ao digitar nos campos de busca, o CWM aceita a primeira parte de uma cadeia de caracteres de busca bem como um asterisco (*). Se a busca for para "Laboratório 1", escrever "Lab", "*1" ou "Lab*1" fornecerá resultados incluindo "Laboratório 1".
Etiquetas		Ao inserir o campo de busca **Etiquetas**, todas as etiquetas relacionadas aparecerão como uma lista selecionável.
Linhas por página		Use as setas sob o resultado da busca para navegar entre as páginas para resultados de busca grandes. O número de linhas exibidas por página pode ser ajustado na lista suspensa **Linhas por página**.
Classificação		Clique neste símbolo para classificar o resultado da busca pela coluna correspondente.
		O resultado da busca é classificado por essa coluna (ascendente).
		O resultado da busca é classificado por essa coluna (descendente).
Como expandir uma coluna		Clique neste símbolo para expandir as colunas onde algumas entradas são longas demais para serem exibidas.

Para visualizar as informações detalhadas sobre o objeto e para configurar esse objeto individualmente, clique na linha do objeto.

3.5.3 Como configurar vários objetos ao mesmo tempo

Algumas operações podem ser executadas em vários objetos ao mesmo tempo. As operações disponíveis variam dependendo do tipo de objeto.

Para configurar vários objetos simultaneamente:

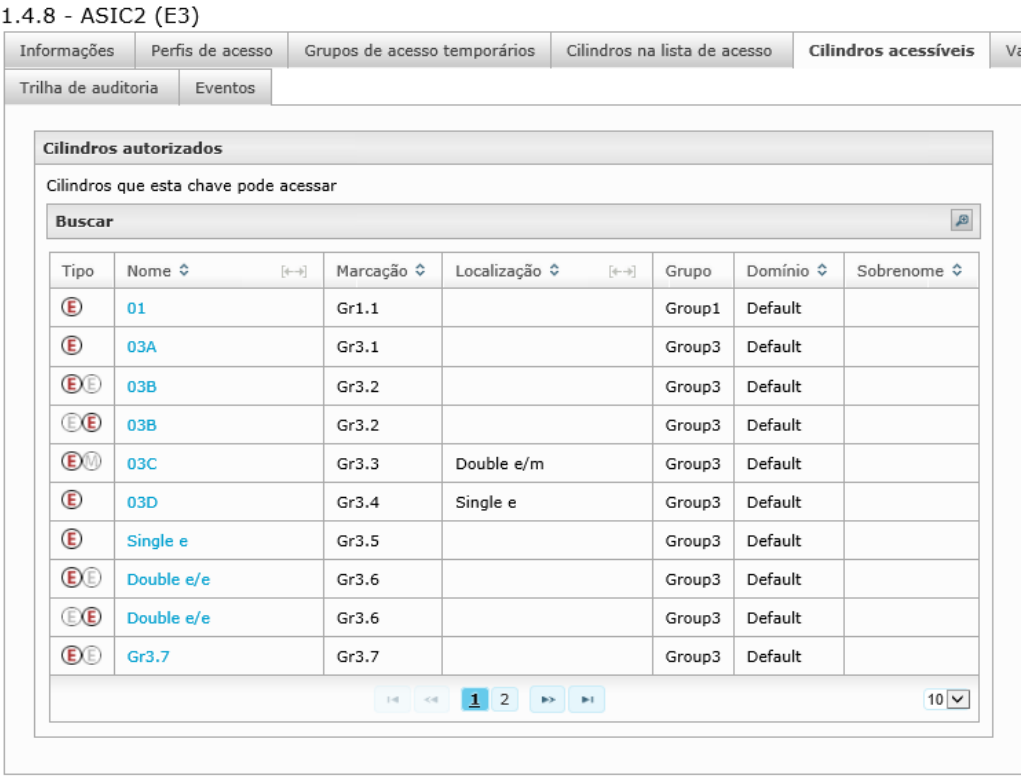
1) Selecione vários objetos na coluna à esquerda de uma ou mais páginas de resultados de busca.

   Clique em **Selecionar todos** para selecionar todos os objetos de todas as páginas no resultado de busca.

2) Clique no botão correspondente na caixa de resultados de busca para iniciar a operação nos objetos selecionados.

3.5.4 Como filtrar listas longas

Ao visualizar listas de, por exemplo, cilindros ou chaves em listas de acesso, existe um banner **Buscar** visível. Consulte o exemplo abaixo.



Clicar no símbolo  abre uma caixa de critérios de busca.

3.5.5 Acessibilidade

3.5.5.1 Acessibilidade do teclado

O CWM suporta navegação por meio do teclado para usuários que não podem usar um mouse ou outros dispositivos de seleção, ou que preferem usar o teclado o máximo possível.

Interação	Tecla	Notas
Navegar entre a maior parte dos elementos	• **Tab** • **Shift** + **Tab** (navegar para trás)	
Botões	• **Enter** ou **Barra de espaço**	
Caixa de seleção	• **Barra de espaço**	Marcar/desmarcar uma caixa de seleção.
Caixas combinadas	• **Barra de espaço** (Opcional. Abre a lista de valores). • **Para cima**/**Para baixo** ou **Esquerda**/**Direita**	Selecione um valor usando as teclas de seta (**Para cima**/**Para baixo** ou **Esquerda**/**Direita**), então aceite usando **Enter**.
Tabelas	• **Para cima**/**Para baixo** (Navegar pelas células de uma tabela) • **Enter** (Inserir e visualizar informações detalhadas)	Navegar pelas células de uma tabela usando as teclas de setas (**Para cima**/**Para baixo**).
Botões	• **Para cima**/**Para baixo** ou **Esquerda**/**Direita**	Selecionar uma opção usando as teclas de seta (**Para cima**/**Para baixo** ou **Esquerda**/**Direita**), então navegar para o próximo elemento usando **Tab**.
Menu principal	• **Esquerda**/**Direita** (Navegar entre as opções do menu principal) • **Para cima**/**Para baixo** (Expandir/recolher a opção do submenu) • **Enter** (Inserir uma opção do submenu)	Navegar pelas opções do menu principal e submenus, usando as teclas de seta (**Para cima**/**Para baixo** ou **Esquerda**/**Direita**).
Visualização de página	• **Page Up** e **Page Down**	Rolar para cima e para baixo na página.
Fluxos de trabalho	• **Alt** + **Esquerda**/**Direita** • **Alt** + **Q** • **Alt** + **Voltar**	Navegar entre etapas. Cancelar o fluxo de trabalho. Confirmar a etapa final.
Editor de texto	• **Alt** + **Q**	Sair do editor de texto.

3.5.5.2 Modos de visualização

Modo alto contraste
O CWM tem suporte para o modo de alto contraste.

Ampliação de 200% com resolução 1024x768
É possível ampliar até 200% no navegador sem perder a funcionalidade da interface do usuário.

3.6 Tarefas comuns

Esta é uma lista das tarefas mais comuns e onde encontrar as instruções correspondentes.

Como fazer o log-in
Seção 3.3 "Como fazer o log-in", página 17

Funcionários
Como adicionar um funcionário ou visitante: *Seção 4.1.2 "Como adicionar funcionários ou visitantes", página 23*

Chaves de usuário
Como fazer a entrega das chaves: *Seção 4.2.9 "Como fazer a entrega das chaves de usuário", página 38*

Como receber chaves (recebimento): *Seção 4.2.10 "Como receber chaves de usuário (devolução)", página 43*

Quando uma chave for perdida: *Seção 4.2.12.2 "Como comunicar e bloquear uma chave de usuário perdida", página 45*

Autorizações
Como visualizar chaves que podem acessar um cilindro ou grupo de cilindros: *Seção 3.6 "Tarefas comuns", página 21*

Como visualizar cilindros aos quais uma chave ou grupo de chaves tem acesso: *Seção 4.8.2 "Como visualizar chaves com acesso a cilindros ou grupos de cilindros", página 77*

Como alterar autorizações em uma chave: *Seção 4.9.1 "Como configurar autorizações em chaves", página 78*

Como alterar autorizações em um cilindro: *Seção 4.9.2 "Como configurar autorizações em cilindros", página 80*

Perfis de acesso
Como associar uma chave ou pessoa a um perfil de acesso: *Seção 4.9.5 "Como selecionar perfis de acesso para funcionários ou visitantes", página 84*

Como alterar as autorizações para um perfil de acesso: *Seção 4.9.4 "Como configurar autorizações de perfil de acesso", página 82*

Trilhas de auditoria
Como verificar as chaves que acessaram um cilindro: *Seção 4.11.3 "Como visualizar trilhas de auditoria de cilindro", página 92*

Programando
Como programar os cilindros: *Seção 4.4.13 "Como programar os cilindros", página 61*

4 Como trabalhar com o CWM

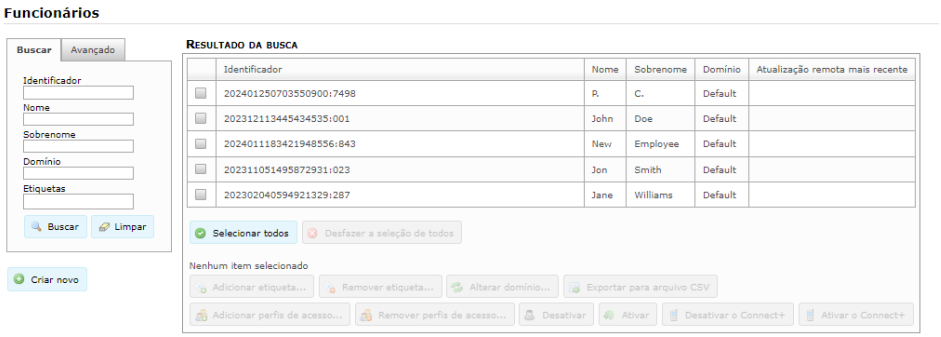
4.1 Como administrar funcionários e visitantes

4.1.1 Como procurar funcionários ou visitantes

1) Selecione **Informações do sistema » Funcionários** ou **Visitantes**.

   Será exibida uma lista de todos os funcionários ou visitantes.

   Caso a integração LDAP esteja ativada, o CWM busca automaticamente as últimas informações do LDAP a cada 24 horas. A data e hora atualizadas são exibidas e as informações detalhadas estão disponíveis clicando em **Exibir detalhes**. Clique em **Atualizar funcionários LDAP** para atualizar manualmente. Consulte *Seção 8.12 "Integração com o LDAP", página 191* para obter mais informações sobre a integração LDAP.



2) Selecione a guia **Buscar** ou **Avançado**.

   A guia **Avançado** inclui mais campos de busca bem como a opção de buscar por funcionários ou visitantes excluídos ou desativados, dependendo de como o CWM foi configurado para tratar pessoas excluídas. Consulte *Seção 8.9 "Exclusão de dados pessoais e conformidade com a GDPR", página 189* para mais detalhes.

3) Insira o critério de busca.

   Ao digitar nos campos de busca, o CWM aceita a primeira parte de uma cadeia de caracteres de busca bem como um asterisco (*). Se a busca for para "Laboratório 1", escrever "Lab", "*1" ou "Lab*1" fornecerá resultados incluindo "Laboratório 1".

   Ao inserir o campo de busca **Etiquetas**, todas as etiquetas relacionadas aparecerão como uma lista selecionável.

4) Clique em **Buscar**.

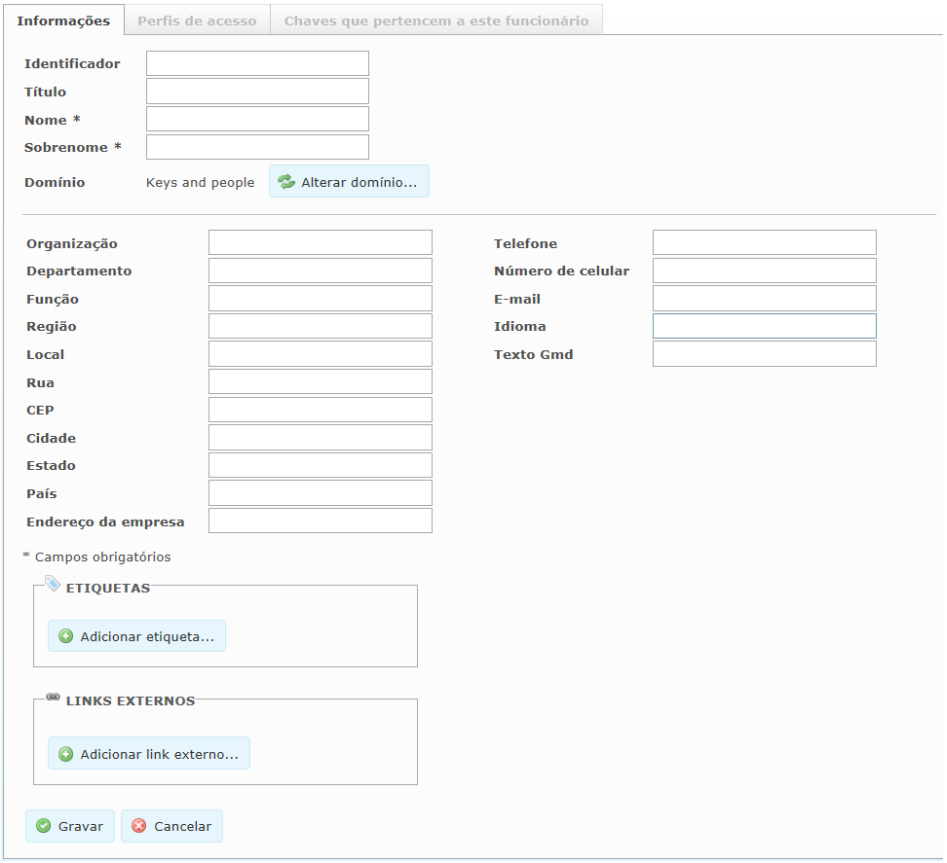
5) Para exibir informações detalhadas sobre um resultado de busca, clique no funcionário ou visitante específico.

4.1.2 Como adicionar funcionários ou visitantes

> **ATENÇÃO!**
> As informações do funcionário obtidas do servidor LDAP são apenas leitura. Os funcionários criados recentemente no CWM não estão adicionados ao servidor LDAP.

1) Selecione **Informações do sistema » Funcionários** ou **Visitantes**.

2) Clique em **Criar novo**.



3) Insira as informações.

   Nome e **Sobrenome** são campos obrigatórios.

   O endereço de **E-mail** é necessário para mandar lembretes para chaves vencidas e o uso do recurso de integração DCS para proprietários de chaves de comando novas.

   Se o recurso do CLIQ Connect+ está ativado para o sistema e será ativado para um funcionário ou visitante novo, o endereço de e-mail não deve ser o mesmo registrado para outro usuário do CLIQ Connect+.

   O campo **Identificador** também é usado para funcionários. O identificador deve ser exclusivo. Se este campo não for inserido, o CWM adicionará um identificador exclusivo no formato aaaa-mm-dd:número consecutivo.

4) Para adicionar uma etiqueta clique em **Adicionar etiqueta...**. Consulte também *Seção 4.1.7 "Como adicionar ou remover uma etiqueta de funcionário ou visitante", página 30*.

5) Para adicionar um link externo clique em **Adicionar link externo...**. Consulte também *Seção 4.1.8 "Como gerenciar links externos de funcionários ou visitantes", página 31*.

6) Clique em **Gravar**.

4.1.3 Desativação ou ativação de funcionários ou visitantes

Pré-requisitos:

- O administrador precisa ter a permissão para **Proprietário da chave: Desativar** para desativar, buscar e reativar funcionários ou visitantes desativados.

  Consulte *Seção 6.7 "Como gerenciar papéis e autorizações", página 127* para obter mais informações sobre o gerenciamento de permissões.
- Em **Configurações do sistema**, **Excluir permanentemente** está selecionado na seção **Ao excluir uma pessoa**.

  Consulte *Seção 6.4 "Como editar as configurações do sistema", página 99* para obter mais informações sobre o gerenciamento de **Configurações do sistema**.
- Os seguintes funcionários ou visitantes não podem ser desativados:
  - Funcionários ou visitantes com chaves entregues.
  - Funcionários integrados com o LDAP.
  - Usuários ativados do CLIQ Mobile Manager.

1) Selecione **Informações do sistema » Funcionários** ou **Informações do sistema » Visitantes**.

   Será exibida uma lista de todos os funcionários ou visitantes.

   > **Dica**
   > Os funcionários ou visitantes desativados ou ativos podem ser filtrados usando o filtro **Exibir desativado** na guia **Avançado**.

   Se necessário, insira os critérios de busca.

   Ao digitar nos campos de busca, o CWM aceita a primeira parte de uma cadeia de caracteres de busca bem como um asterisco (*). Se a busca for para "Laboratório 1", escrever "Lab", "*1" ou "Lab*1" fornecerá resultados incluindo "Laboratório 1".

   Ao inserir o campo de busca **Etiquetas**, todas as etiquetas relacionadas aparecerão como uma lista selecionável.

   - Para ativar ou desativar um funcionário ou visitante individual, acesse *Passo 2*.
   - Para ativar ou desativar vários funcionários ou visitantes simultaneamente, acesse *Passo 3*.

2) **Ativação ou desativação de funcionário ou visitante individual**

   1. Selecione o funcionário ou visitante e vá para sua tela de informações detalhadas.
   2. **Para desativar um funcionário ou visitante**

      a) Na tela de informações, clique em **Desativar**.

      b) Na janela pop-up, clique em **Desativar**.

      Para ativar um funcionário ou visitante

      a) Na tela de informações, clique em **Ativar**.

      b) Na janela pop-up, clique em **OK**.

3) **Ativação ou desativação de vários funcionários ou visitantes**

1. Selecione os funcionários ou visitantes a serem desativados ou ativados nos resultados da busca, marcando as caixas de seleção.
2. **Para desativar funcionários ou visitantes**

   a) Clique em **Desativar** nos resultados da busca.

   b) Na janela pop-up, clique em **Desativar**.

   Para ativar funcionários ou visitantes

   a) Clique em **Ativar** nos resultados da busca.

   b) Na janela pop-up, clique em **OK**.

4.1.4 Como excluir ou recuperar funcionários ou visitantes

Em **Configurações do sistema**, a exclusão de funcionários ou visitantes pode ser configurada para ser **Marcar como excluído** ou **Excluir permanentemente**.

- Quando é selecionado **Marcar como excluído**, os funcionários ou visitantes excluídos poderão ser recuperados, caso necessário.
- Quando **Excluir permanentemente** estiver selecionado, os funcionários ou visitante **não poderão** ser recuperados.

Consulte também *Seção 6.4 "Como editar as configurações do sistema", página 99* e *Seção 8.9 "Exclusão de dados pessoais e conformidade com a GDPR", página 189*.

1) Encontre o funcionário ou visitante e vá para sua tela de informações detalhadas.

   Consulte *Seção 4.1.1 "Como procurar funcionários ou visitantes", página 23*.

> **Dica**
> Usuários excluídos podem ser filtrados usando o filtro **Exibir excluído** na guia **Avançado**.

2) **Para excluir o funcionário ou visitante:**

> **ATENÇÃO!**
> As seguintes pessoas não podem ser excluídas:
> - Funcionários ou visitantes com chaves entregues.
> - Funcionários integrados no LDAP.
> - Usuários ativados do CLIQ Connect+.

1. Na tela de informações detalhadas, clique em **Excluir**.
2. Na janela pop-up, clique em **Excluir**.

Para restaurar o funcionário ou visitante:

1. Na tela de informações detalhadas, clique em **Recuperar**.
2. Na janela pop-up, clique em **Recuperar**.

4.1.5 Como ativar ou desativar o acesso ao CLIQ Connect+ para funcionários ou visitantes

Se o CLIQ Connect+ estiver ativado para o sistema então os funcionários e visitantes podem verificar as informações detalhadas para suas chaves através do CLIQ Connect. Para usar este recurso, o administrador precisa ativar o status de usuário do CLIQ Connect+.

Existem duas formas de ativar ou desativar o status de usuário:

- Para alterar o status individualmente, siga as instruções em *Seção 4.1.5.1 "Como configurar o acesso ao CLIQ Connect+ individualmente", página 27*.
- Para ativar ou desativar mais de um funcionário ou visitante ao mesmo tempo, siga as instruções em *Seção 4.1.5.2 "Como configurar o acesso ao CLIQ Connect+ para vários funcionários", página 28*.

Consulte *Seção 8.3.4 "CLIQ Connect e CLIQ Connect+", página 182* para obter mais detalhes sobre o CLIQ Connect+.

Pré-requisitos:

- O administrador obteve e instalou a licença **CLIQ Connect+**.

  Para instalar uma licença nova, consulte *Seção 6.1.1 "Como instalar licenças", página 98*.
- O endereço de e-mail do funcionário ou visitante não deve pertencer a outro usuário do CLIQ Connect+.

4.1.5.1 Como configurar o acesso ao CLIQ Connect+ individualmente

1) Encontre o funcionário ou visitante e vá para sua tela de informações detalhadas.

   Consulte *Seção 4.1.1 "Como procurar funcionários ou visitantes", página 23*.

> **Dica**
> Usuários desativados ou excluídos podem ser filtrados usando o filtro na guia **Avançado**.

2) Para ativar ou desativar o status de usuário do CLIQ Connect+:

   Para ativar o status de usuário do CLIQ Connect+:
   Clique em **Ativar o Connect+**.

> **ATENÇÃO!**
> O botão **Ativar o Connect+** estará desativado caso o endereço de e-mail não tenha sido inserido ou se já pertence a outro funcionário ou visitante que ativou o CLIQ Connect+.
>
> Clique em **Editar** e insira um endereço de e-mail exclusivo.

   Um e-mail com informações sobre a configuração do CLIQ Connect é enviado para o endereço de e-mail especificado.

   O administrador também pode enviar o e-mail manualmente para um usuário do CLIQ Connect+ clicando no botão **Enviar e-mail novamente**.

   - Se o CLIQ Connect+ não foi ativado pelo proprietário da chave, o e-mail contém informações sobre como ativar a conta.

- Se o CLIQ Connect+ foi ativado pelo proprietário da chave, o e-mail contém informações sobre como acessar a conta.

Para desativar o status de usuário do CLIQ Connect+:

1. Para desativar: Clique em **Desativar o Connect+**.
2. Clique em **Desativar** na janela pop-up.

4.1.5.2 Como configurar o acesso ao CLIQ Connect+ para vários funcionários

1) Encontre o funcionário ou visitante e vá para sua tela de informações detalhadas.

   Consulte *Seção 4.1.1 "Como procurar funcionários ou visitantes", página 23*.

> **Dica**
> Usuários desativados ou excluídos podem ser filtrados usando o filtro na guia **Avançado**.

2) Selecione os funcionários e os visitante verificando as caixas de seleção.

> **ATENÇÃO!**
> Poderão ser selecionados no máximo 500 funcionários ou visitantes por vez para desativar o status de usuário do CLIQ Connect+.

3) **Para ativar o status de usuário do CLIQ Connect+:**

> **ATENÇÃO!**
> O status de usuário do CLIQ Connect+ não será ativado para o funcionário ou visitante que:
>
> - não possui um endereço de e-mail registrado
> - possui o mesmo endereço de e-mail que outro funcionário ou visitante ativado no CLIQ Connect+.
> - já possui o status de usuário ativado.

1. Clique em **Ativar o Connect+**.

   Aparecerá a janela de informações na tela.
2. Clique em **Ativar** na janela pop-up.

   Um e-mail com informações sobre a configuração do CLIQ Connect é enviado para o endereço de e-mail especificado.

   O administrador também pode enviar o e-mail manualmente a um usuário do CLIQ Connect+ por meio da tela de informações individual clicando no botão **Enviar e-mail novamente**.

   – Se o CLIQ Connect+ não foi ativado pelo proprietário da chave, o e-mail contém informações sobre como ativar a conta.

   – Se o CLIQ Connect+ foi ativado pelo proprietário da chave, o e-mail contém informações sobre como acessar a conta.

Para desativar o status de usuário do CLIQ Connect+:

1. Clique em **Desativar o Connect+**.

   Aparecerá a janela de informações na tela.

2. Clique em **Desativar** na janela pop-up.

O resultado da operação é exibido acima da tabela **RESULTADO DA BUSCA**.

4.1.6 Como editar informações de funcionários ou visitantes

Consulte *Seção 4.1.6.2 "Como editar as informações do funcionário ou do visitante no CWM", página 30* para editar as informações de um funcionário ou visitante no CWM.

As informações do funcionário também podem ser editadas importando um arquivo CSV atualizado ou por meio de LDAP se o sistema é integrado ao LDAP. Consulte *Seção 4.1.11 "Como importar informações do funcionário", página 33* para obter mais informações sobre como importar as informações do funcionário. Consulte *Seção 8.12 "Integração com o LDAP", página 191* para obter mais informações sobre a integração LDAP.

ATENÇÃO!
Existem limitações para editar ou excluir o endereço de e-mail de um funcionário ou visitante com o status de usuário do CLIQ Connect+ ativado. Consulte *Seção 4.1.6.1 "Informações importantes sobre a edição ou exclusão de um endereço de e-mail", página 29* para obter mais informações.

4.1.6.1 Informações importantes sobre a edição ou exclusão de um endereço de e-mail

Quando o CLIQ Connect+ está ativado
Funcionários ou visitantes com o status de usuário do CLIQ Connect+ ativado acessam o CLIQ Connect com o endereço de e-mail registrado no CWM. Portanto, editar ou excluir o endereço de e-mail afetará o acesso ao CLIQ Connect.

Edição

- Editar o endereço de e-mail de um endereço de e-mail exclusivo altera as credenciais de acesso ao CLIQ Connect.

  Um e-mail com informações sobre a configuração do CLIQ Connect é enviado para o endereço de e-mail especificado.

  – Se a conta do CLIQ Connect+ não foi ativada pelo proprietário da chave, o e-mail contém o código de ativação da conta.

  – Se a conta do CLIQ Connect+ foi ativada pelo proprietário da chave, o e-mail contém informações sobre como acessar a conta.

- O CWM não permite editar o endereço de e-mail para um endereço de e-mail que já pertence a outro usuário do CLIQ Connect+.

  Tal alteração do endereço de e-mail por meio da integração LDAP ou arquivo CSV é ignorada ou tratada como erro.

Exclusão

- Exclusão do endereço de e-mail no CWM:

  A exclusão desativa o status de usuário do CLIQ Connect+.
- Exclusão do endereço de e-mail por meio da integração LDAP ou arquivo CSV:

  A exclusão não é permitida se a conta do CLIQ Connect+ foi ativada pelo proprietário da chave.

Quando o login SSO está ativado
Quando uma Chave de comando é atribuída a um funcionário, o endereço de e-mail associado não pode mais ser editado ou excluído.

4.1.6.2 Como editar as informações do funcionário ou do visitante no CWM

Esta seção mostra como editar as informações do funcionário ou do visitante no CWM.

Pré-requisitos:

- O funcionário ou visitante a ser editado deverá estar ativo.
- O funcionário a ser editado não está integrado no LDAP.

> **ATENÇÃO!**
> No caso de um funcionário integrado no LDAP, só poderão ser alterados **Domínio** e **ETIQUETAS**.

1) Encontre o funcionário ou visitante e vá para sua tela de informações detalhadas.

   Consulte *Seção 4.1.1 "Como procurar funcionários ou visitantes", página 23*.
2) Clique em **Editar**.
3) Atualize os campos.
   - Consulte *Seção 4.1.7 "Como adicionar ou remover uma etiqueta de funcionário ou visitante", página 30* para editar etiquetas.
   - Consulte *Seção 4.1.8 "Como gerenciar links externos de funcionários ou visitantes", página 31* para editar links externos.
4) Clique em **Gravar**.

> **ATENÇÃO!**
> A edição destas informações poderá resultar no envio de notificações por e-mail ao administrador do domínio para que sejam tomadas as ações apropriadas. As notificações só serão enviadas se ativadas nas **Configurações do sistema**.
>
> Consulte também *Seção 6.4 "Como editar as configurações do sistema", página 99*.

4.1.7 Como adicionar ou remover uma etiqueta de funcionário ou visitante

Consulte *Seção 8.2.6 "Etiquetas", página 179* para obter informações sobre etiquetas.

Pré-requisito:

- Os funcionários ou visitantes a serem editados deverão estar ativos.

1) Selecione **Informações do sistema » Funcionários** ou **Visitantes**.

Será exibida uma lista de todos os funcionários ou visitantes.

- Para adicionar ou remover etiquetas de um funcionário ou visitante individual, acesse *Passo 2*.
- Para adicionar ou remover etiquetas de vários funcionários ou visitantes simultaneamente, acesse *Passo 3*.

2) **Adicionar ou remover etiquetas de um funcionário ou visitante individual:**

1. Selecione o funcionário ou visitante e vá para sua tela de informações detalhadas.
2. Clique em **Editar**.
3. Adicione ou remova uma etiqueta de um funcionário ou visitante individual.

Para adicionar uma etiqueta:

a) Clique em **Adicionar etiqueta...**.
b) Insira um nome para a etiqueta.
c) Clique em **OK**.

Para remover uma etiqueta:
Clique na etiqueta a ser removida.

4. Clique em **Gravar**.

3) **Adicionar ou remover etiquetas de vários funcionários ou visitantes:**

1. Selecione os funcionários ou visitantes nos resultados da busca, marcando as caixas de seleção.
2. **Para adicionar uma etiqueta:**

a) Clique em **Adicionar etiqueta...**.
b) Insira o nome da etiqueta.
c) Clique em **OK**.

Para remover uma etiqueta:

a) Clique em **Remover etiqueta...**.
b) Insira o nome da etiqueta.
c) Clique em **OK**.

4.1.8 Como gerenciar links externos de funcionários ou visitantes

Para obter informações sobre links externos, consulte *Seção 8.4 "Links externos", página 182*.

Pré-requisito:

- Os funcionários ou visitantes a serem editados deverão estar ativos.

1) Encontre o funcionário ou visitante e vá para sua tela de informações detalhadas.

Consulte *Seção 4.1.1 "Como procurar funcionários ou visitantes", página 23*.

2) Clique em **Editar**.

3) **Para adicionar um link externo:**

1. Clique em **Adicionar.**
2. Insira o **Nome** da URL.
3. Insira **URL**. A **URL** deve começar com um protocolo (por exemplo http:// ou ftp://).

   Se foi definida uma URL raiz nas **Configurações do sistema** (item **URL raiz dos links externos**), só é necessário adicionar a última parte da URL.
   Consulte também *Seção 6.4 "Como editar as configurações do sistema", página 99*.
4. Clique em **OK**.

Para editar um link externo:

1. Clique em **Editar** no link externo a ser editado.
2. Atualize os campos.
3. Clique em **OK**.

Para remover um link externo:
Clique em **Remover** no link externo a ser removido.

4) Clique em **Gravar**.

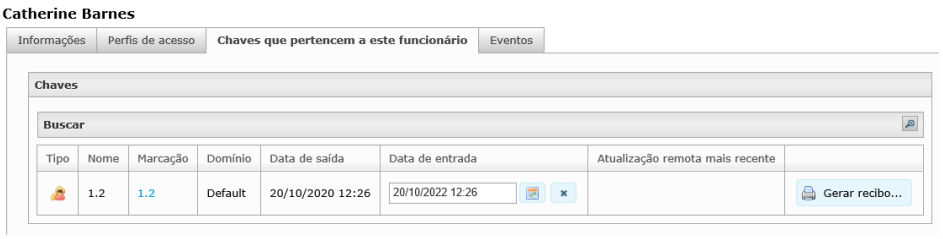
4.1.9 Como visualizar as chaves de um funcionário ou visitante

1) Encontre o funcionário ou visitante e vá para sua tela de informações detalhadas.

   Consulte *Seção 4.1.1 "Como procurar funcionários ou visitantes", página 23*.

2) Selecione a guia **Chaves que pertencem a este funcionário** ou **Chaves que pertencem a este visitante**.

   Serão exibidas as chaves fornecidas para o funcionário ou visitante.



3)
- Para alterar a data de entrega de uma chave, edite o campo **Data de entrada**.
- Para gerar um recibo de recebimento e devolução de uma chave clique em **Gerar recibo...**.
- Para exibir a tela de informações detalhadas da chave, clique na marcação da chave.

4.1.10 Como visualizar eventos de funcionários ou visitantes

A guia **Eventos** fornece um registro das atividades administrativas no CWM, incluindo ações como a criação de um funcionário ou visitante e a atualização do status do CLIQ

Connect+. Ela também registra os principais eventos relacionados ao funcionário ou visitante.

1) Encontre o funcionário ou visitante e vá para sua tela de informações detalhadas.

   Consulte *Seção 4.1.1 "Como procurar funcionários ou visitantes", página 23*.

2) Na tela de informações detalhadas, selecione a guia **Eventos**.

   Será exibida uma lista dos eventos do funcionário ou visitante.

4.1.11 Como importar informações do funcionário

Importar funcionários ativa a importação em massa de dados novos ou atualizados dos funcionários.

> **ATENÇÃO!**
> Funcionários adicionados por meio da integração LDAP não podem ser editados por meio da importação CSV.

Pré-requisito:

- Crie um arquivo de importação CSV seguindo as informações de formato em *Seção 9.9 "Formato de arquivo de importação de funcionário", página 211*.

1) Selecione **Administração » Importar funcionários**.
2) Clique em **Selecionar...**.
3) Escolha o arquivo a ser carregado e clique em **Abrir**.
4) Clique em **Carregar**.

   São exibidas as informações sobre quantas entradas válidas o arquivo contém. Caso exista qualquer entrada inválida, clique em **Detalhes** para obter mais informações.
5) Clique em **Importar**.

4.1.12 Como exportar informações do funcionário ou visitante

1) Busque os funcionários ou visitantes.

   Consulte *Seção 4.1.1 "Como procurar funcionários ou visitantes", página 23*.
2) A partir dos resultados da busca, selecione os funcionários ou visitantes cujas informações devem ser exportadas.
3) Clique em **Exportar para arquivo CSV**.

   Informações sobre funcionários ou visitantes desativados não poderão ser exportadas.

   > **ATENÇÃO!**
   > Para ser possível abrir o arquivo em Excel da maneira correta, o delimitador para o arquivo deverá ser configurado de acordo com as configurações regionais. Consulte *Seção 6.4 "Como editar as configurações do sistema", página 99* para alterar o delimitador.

4) Na janela pop-up de download do arquivo, clique em **Abrir** ou **Gravar**.

4.2 Gestão de chaves

4.2.1 Como buscar chaves de usuário

1) Selecione **Informações do sistema » Chaves**.

   Será exibida uma lista de todas as chaves.

   Os símbolos abaixo são utilizados:

   - Chave mecânica
   - Chave normal
   - Chave Quartz
   - Chave quartz do CLIQ Connect
   - Chave dinâmica
   - Chave dinâmica do CLIQ Connect
   - Existe uma atualização remota pendente para a chave

2) Selecione a guia **Buscar** ou **Avançado**.

   Por padrão, as chaves mecânicas e as chaves comunicadas como perdidas ou quebradas não são exibidas. Para incluir essas chaves também no resultado de busca, selecione **Todos os tipos e status**.

   A guia **Avançado** também inclui os campos de busca tipo de chave, chave do CLIQ Connect, status do inventário e status operacional.

3) Insira o critério de busca.

   Ao inserir o campo de busca **Etiquetas**, todas as etiquetas relacionadas aparecerão como uma lista selecionável.

   Ao digitar nos campos de busca, o CWM aceita a primeira parte de uma cadeia de caracteres de busca bem como um asterisco (*). Se a busca for para "Laboratório 1", escrever "Lab", "*1" ou "Lab*1" fornecerá resultados incluindo "Laboratório 1".

4) Clique em **Buscar**.

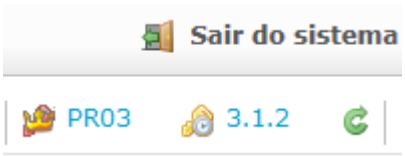
5) Clique na linha da chave específica para exibir informações detalhadas em um resultado de busca.

   Consulte *Seção 9.3.3 "Atributos de chaves", página 198* para obter informações sobre os atributos da chave.

4.2.2 Como escanear uma chave de usuário

1) Insira a chave na ranhura direita do Programador local.
2) Clique em no canto superior direito da página.

   Ambas as chaves no Programador local são mostradas abaixo da barra de navegação.



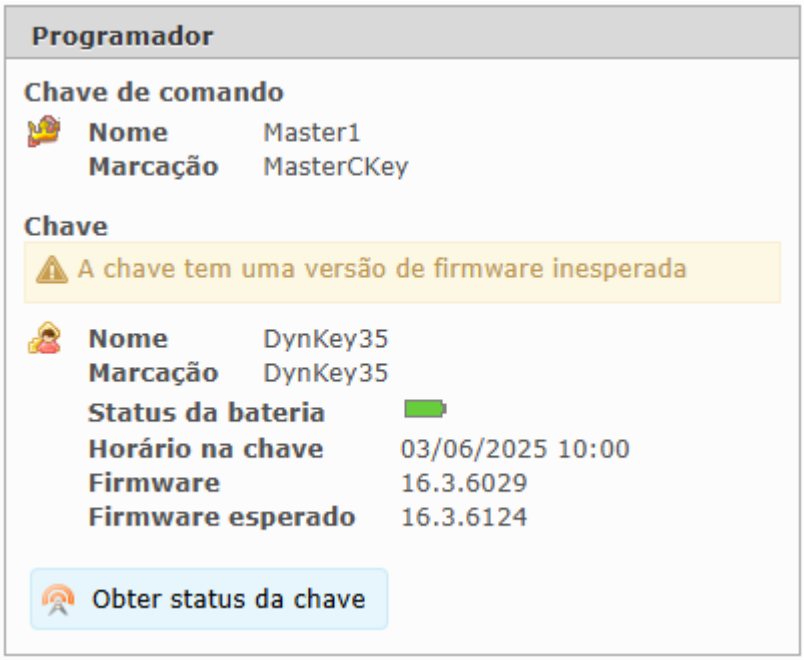
3) Clique na chave na ranhura direita do Programador local.

   A tela das informações detalhadas da chave é exibida, com **Nome** e **Marcação** da chave mostrados no lado direito da página.

4.2.3 Como visualizar o status da chave

1) Escaneie a chave. Consulte *Seção 4.2.2 "Como escanear uma chave de usuário", página 35*.
2) Clique em **Obter status da chave**.

   Serão exibidas as informações básicas sobre a chave. Para obter mais informações sobre o indicador de status da bateria, consulte *Seção 9.6 "Indicações do nível da bateria", página 209*.



4.2.4 Como editar as informações de uma chave de usuário

1) Encontre a chave e vá para sua tela de informações detalhadas.

   Consulte *Seção 4.2.1 "Como buscar chaves de usuário", página 34* para buscar a chave e exibir a tela informações detalhadas.

   Para escanear a chave no Programador local e exibir as informações detalhadas, consulte *Seção 4.2.2 "Como escanear uma chave de usuário", página 35*

2) Clique em **Editar**.
3) Para editar o nome da chave, atualize o campo **Nome**.
4) Para adicionar uma etiqueta clique em **Adicionar etiqueta**.

   Consulte também *Seção 4.2.5 "Como adicionar ou remover chave-etiquetas de usuário", página 36*.
5) Para adicionar um link externo clique em **Adicionar link externo**.

   Consulte também *Seção 4.2.6 "Como gerenciar links externos da chave de usuário", página 37*.
6) Clique em **Gravar**.

4.2.5 Como adicionar ou remover chave-etiquetas de usuário

Consulte *Seção 8.2.6 "Etiquetas", página 179* para obter informações sobre etiquetas.

1) Encontre a chave a ser editada.

   Consulte *Seção 4.2.1 "Como buscar chaves de usuário", página 34* para buscar uma chave.

   Clique em *Seção 4.2.2 "Como escanear uma chave de usuário", página 35* para escanear a chave no Programador local.
2) - Para adicionar ou remover etiquetas de uma chave individual, acesse *Passo 3*.
   - Para adicionar ou remover etiquetas de várias chaves, acesse *Passo 4*.
3) **Adicionar ou remover etiquetas de uma chave individual:**

   1. Selecione a chave e vá para sua tela de informações detalhadas.
   2. Clique em **Editar**.
   3. Adicione ou remova a etiqueta de uma chave individual.

      Para adicionar uma etiqueta:

      a) Clique em **Adicionar etiqueta...**.
      b) Insira um nome para a etiqueta.
      c) Clique em **OK**.

      Para remover uma etiqueta:
      Clique na etiqueta a ser removida.
   4. Clique em **Gravar**.
4) **Adicionar ou remover etiquetas de várias chaves:**

   1. Selecione as chaves nos resultados da busca, marcando as caixas de seleção.
   2. **Para adicionar uma etiqueta:**

      a) Clique em **Adicionar etiqueta...**.
      b) Insira o nome da etiqueta.
      c) Clique em **OK**.

      Para remover uma etiqueta:

      a) Clique em **Remover etiqueta...**.

b) Insira o nome da etiqueta.

c) Clique em **OK**.

4.2.6 Como gerenciar links externos da chave de usuário

Para obter informações sobre links externos, consulte *Seção 8.4 "Links externos", página 182*.

1) Encontre a chave e vá para sua tela de informações detalhadas.

   Consulte *Seção 4.2.1 "Como buscar chaves de usuário", página 34* para buscar a chave e exibir a tela informações detalhadas.

   Para escanear a chave no Programador local e exibir as informações detalhadas, consulte *Seção 4.2.2 "Como escanear uma chave de usuário", página 35*

2) Clique em **Editar**.
3) Para adicionar um link externo:
   a) Clique em **Adicionar**.
   b) Insira o **Nome** da URL.
   c) Insira **URL**. A **URL** deve começar com um protocolo (por exemplo http:// ou ftp://).

      Se foi definida uma URL raiz nas **Configurações do sistema** (item **URL raiz dos links externos**), só é necessário adicionar a última parte da URL. Consulte também *Seção 6.4 "Como editar as configurações do sistema", página 99*.

   d) Clique em **OK**.
4) Para editar um link externo:
   a) Clique em **Editar** no link externo a ser editado.
   b) Atualize os campos.
   c) Clique em **OK**.
5) Para remover um link externo: Clique em **Remover** no link externo a ser removido.
6) Clique em **Gravar**.

4.2.7 Como visualizar o histórico de atualizações de uma chave de usuário

A guia **Atualizar histórico** é usada para rastrear a programação da chave.

Pré-requisitos:

- O nível de permissão do usuário deverá ser **Visualizar** no papel **Chave: atualizar histórico**.

  Consulte *Seção 6.7 "Como gerenciar papéis e autorizações", página 127* para alterar o nível de permissão.
-

1) Encontre a chave e vá para sua tela de informações detalhadas.

   Consulte *Seção 4.2.1 "Como buscar chaves de usuário", página 34* para buscar a chave e exibir a tela informações detalhadas.

Para escanear a chave no Programador local e exibir as informações detalhadas, consulte *Seção 4.2.2 "Como escanear uma chave de usuário", página 35*

2) Selecione a guia **Atualizar histórico**.

Uma lista com todas as atualizações da chave será exibida.

> **ATENÇÃO!**
> Por padrão, atualizações de chaves, com exceção de atualizações de firmware, são excluídas após 3 meses.

Os símbolos abaixo são utilizados:

- Existe uma função de programação para um PD local mas ainda não foi iniciada.
- Existe uma atualização remota pendente para a chave
- A função de programação foi concluída
- Falha ou cancelamento da função de programação
- A função de programação foi substituída por uma nova função

3) Clique no link na coluna **Razão** para exibir mais detalhes sobre uma atualização específica.

4.2.8 Como visualizar eventos de uma chave de usuário

A guia Eventos é usada para rastrear as operações do administrador no CWM, como entrega de uma chave, associação de perfis de acesso, alteração de autorizações de chave, etc.

1) Encontre a chave e vá para sua tela de informações detalhadas.

Consulte *Seção 4.2.1 "Como buscar chaves de usuário", página 34* para buscar a chave e exibir a tela informações detalhadas.

Para escanear a chave no Programador local e exibir as informações detalhadas, consulte *Seção 4.2.2 "Como escanear uma chave de usuário", página 35*

2) Selecione a guia **Eventos**.

Será exibida uma lista com todos os eventos da chave.

4.2.9 Como fazer a entrega das chaves de usuário

O processo de entrega tem duas fases.

1. **Configurações de entrega**

   Nesta fase, as configurações de entrega são configuradas em três páginas diferentes: **Geral**, **Acessos** e **Configurações de tempo**.

   É obrigatório completar as configurações na página **Geral**, mas as configurações nas outras páginas são opcionais.

2. **Resumo da entrega**

   Nesta fase, os detalhes da entrega são confirmados e a chave é entregue. Se a chave entregue for inserida no programador ela também será programada.

1) Existem duas formas de iniciar o processo de entrega:

- Selecione **Tarefas » Entregar chave » Para funcionário** ou **Para visitante**.
- Na tela de informações detalhadas do funcionário ou do visitante:

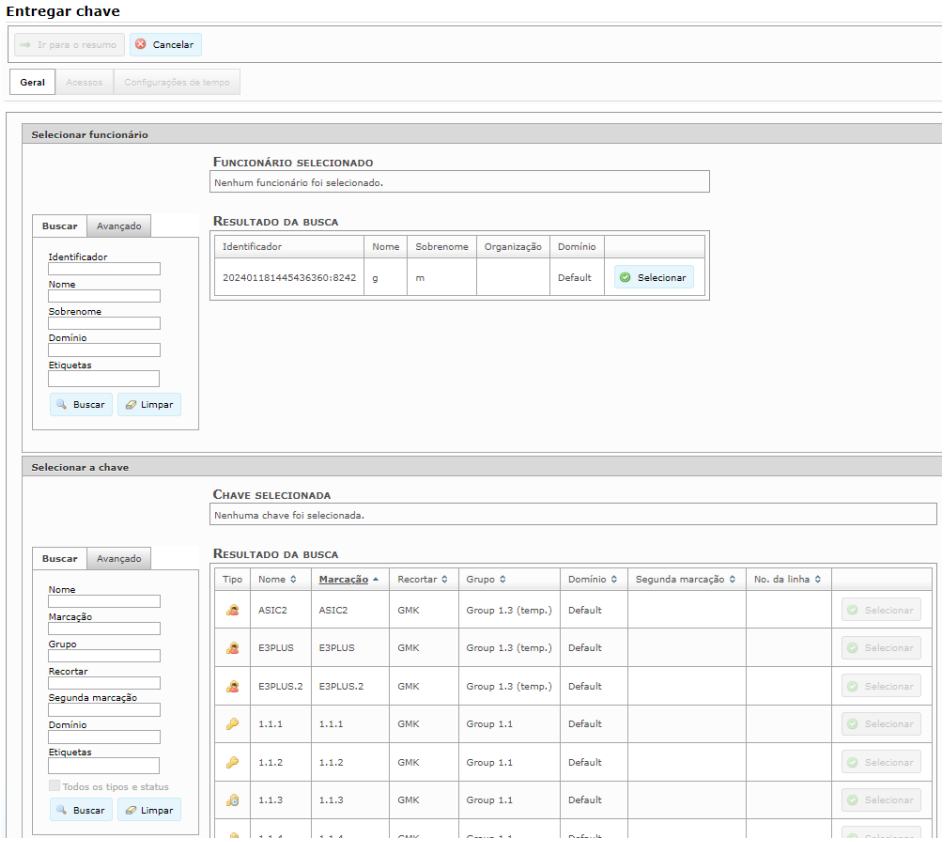
  a) Encontre a chave e vá para sua tela de informações detalhadas.

  Consulte *Seção 4.2.1 "Como buscar chaves de usuário", página 34* para buscar a chave e exibir a tela informações detalhadas.

  Para escanear a chave no Programador local e exibir as informações detalhadas, consulte *Seção 4.2.2 "Como escanear uma chave de usuário", página 35*

  b) Clique em **Entregar chave**.

As páginas **Entregar chave**, **Geral** serão abertas.



2) Caso não haja um funcionário ou hóspede selecionado na seção **Selecionar funcionário** ou **Selecionar visitante**, encontre a pessoa e clique em **Selecionar**.

   Consulte *Seção 4.1.1 "Como procurar funcionários ou visitantes", página 23* para buscar um funcionário ou visitante específico.

3) Selecione a chave a ser entregue de uma das seguintes formas:

   - Se a chave a ser entregue estiver à mão:

     a) Insira a chave na ranhura direita do Programador local.

     b) Clique em  no canto superior direito da página para escanear a chave.

     c) Na caixa **Chave de usuário no programador**, clique em **Selecionar**.

Entregar uma chave usando a função de escaneamento é, na maioria dos casos, a opção recomendada pois uma nova configuração pode ser programada imediatamente na chave. Isso é importante principalmente para sistemas não remotos.

- Se a chave a ser entregue não estiver à mão:

  a) Encontre a chave a ser entregue em uma das seguintes listas e clique em **Selecionar**.

  - A lista **CHAVE PRÉ-SOLICITADA**

    Caso existam chaves solicitadas para a pessoa selecionada, a lista de chaves solicitadas será exibida na tela de seleção de chaves.

    Dica
    Uma chave solicitada é uma chave ligada a uma pessoa específica quando a chave é solicitada.

    Conectar uma chave a uma pessoa específica ajuda os administradores a selecionar a chave certa para a pessoa selecionada durante o processo de entrega.

    O status da chave permanece **Em estoque** após a chave ser importada para o sistema independentemente se a chave física chegou ou não do fornecedor CLIQ.

    A chave pode ser entregue para qualquer pessoa e perde o recurso de solicitação assim que for entregue.

  - A lista **RESULTADO DA BUSCA**

    Para reduzir a lista, insira o critério de busca e clique em **Buscar**. Consulte também *Seção 4.2.1 "Como buscar chaves de usuário", página 34*.

4) Caso necessário, configure os detalhes na página **Acessos** e na página **Configurações de tempo**.

   Caso contrário, vá para *Passo 5*.

   ATENÇÃO!
   Todas as configurações abaixo se aplicam a Chaves dinâmicas nos sistemas remotos do grupo de cilindros. Algumas configurações não estão disponíveis para outros tipos e configurações de chaves.

Página de acessos

- **Selecionar os perfis de acesso**

  Selecione os perfis de acesso na lista.

  Por padrão, os perfis de acesso do funcionário ou do visitante estão selecionados.

- **Selecionar os grupos de cilindros**

  Selecione os grupos de cilindros para os quais a chave terá acesso explícito.

- **Selecionar cilindros**

  Selecione os cilindros para os quais a chave terá acesso explícito.

Página Configurações de tempo

- **Configurar validade da chave**

  - **SELECIONE AS DATAS DE ENTREGA E DE DEVOLUÇÃO.**

    Insira a data de entrega (**Data de saída**) e a data de devolução (**Data de entrada**):

    Se a data de devolução ainda não estiver determinada, clique em **X**.

  - **CONFIGURAR VALIDADE DA CHAVE**

    Ajuste as seguintes configurações para a validade da chave.

    - Selecione as configurações de ativação entre **Inativo**, **Ativo entre as datas selecionadas** e **Sempre ativo**.

      Se **Ativo entre as datas selecionadas** estiver selecionado, configure as datas **Chave ativa a partir de** e **Chave ativa até**.

      Se a data **Chave ativa até** ainda não estiver determinada, clique em **X**.

    - Para usar a revalidação, marque a caixa **Use a revalidação** e configure o intervalo de tempo.

      Quando estiver configurada, a chave deverá ser atualizada no intervalo de tempo especificado para que permaneça ativa.

    - **Somente chaves CLIQ Connect**:

      Para usar a **Validação do PIN**, marque a caixa e configure o intervalo de tempo.

      Quando estiver configurado, a chave deverá ser validada pelo PIN usando o CLIQ Connect nos intervalos de tempo especificados para que permaneça ativa.

    Consulte *Seção 8.1.4 "Validade da chave", página 165* para obter mais informações sobre a validade da chave.

- **Selecionar a agenda da chave**

  AGENDA DA CHAVE

  Configure a agenda da chave como descrito abaixo:

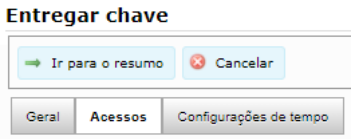
  a) Caso exista um modelo de agenda a ser usado, selecione na lista suspensa e clique em **Aplicar**.

b) Clique em **Adicionar período** para adicionar o intervalo de tempo ao modelo selecionado ou para personalizar a agenda.

c) Clique em **Adicionar cilindro** para configurar um intervalo de tempo específico a um cilindro.

Selecione um cilindro na lista exibida e clique em **Adicionar período** para configurar o intervalo.

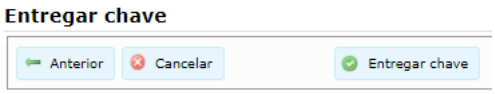
5) Clique em **Ir para o resumo**.



Será exibido um resumo dos direitos de acesso e das configurações.

6) Verifique as configurações.

Para alterar as configurações, clique em **Anterior** para voltar para as páginas de configuração.



7)
- Se a chave entregue está no programador local, clique em **Programar e Gravar**.

  A chave é programada diretamente no programador.
- Se a chave entregue não está no programador local, clique em **Entregar chave**.

  Uma função de atualização remota é criada em sistemas remotos.

8) Opcional: Crie um recibo.

Os recibos são criados como PDFs que podem ser impressos ou gravados.

Consulte *Seção 6.9 "Como gerenciar modelos de recibo", página 129* para criar ou editar modelos de recibos.

a) Clique em **Gerar recibo...**.

Aparecerá a janela **Seleção de recibo**.

b) Selecione o idioma adequado na lista suspensa.

c) Selecione o modelo adequado na lista suspensa.

Todos os modelos de recibos de entrega no idioma selecionado são exibidos na lista suspensa.

d) Clique em **Gerar recibo** ou **Fazer download**.

9) Opcional: Emita um código QR para configurar a URL do servidor do CLIQ Remote e entregue-o junto com a chave.

Se o proprietário da chave pretende usar o CLIQ Connect e o sistema CWM não está integrado ao DCS, o proprietário da chave deve inserir a URL do servidor do CLIQ Remote manualmente no CLIQ Connect. Gerar um código QR para a URL do servidor do CLIQ Remote e entregá-lo ao proprietário da chave simplifica o processo de configuração do aplicativo.

a) Abra qualquer tipo de gerador QR on-line.

b) Insira as informações na seguinte ordem: `<código da empresa operadora ASSA ABLOY>,<nome MKS>,<URL>`

Exemplo:
`3,CLIQConnectTeam,https://app-team-remote.cliqapps.aa.st:443/CLIQRemote`

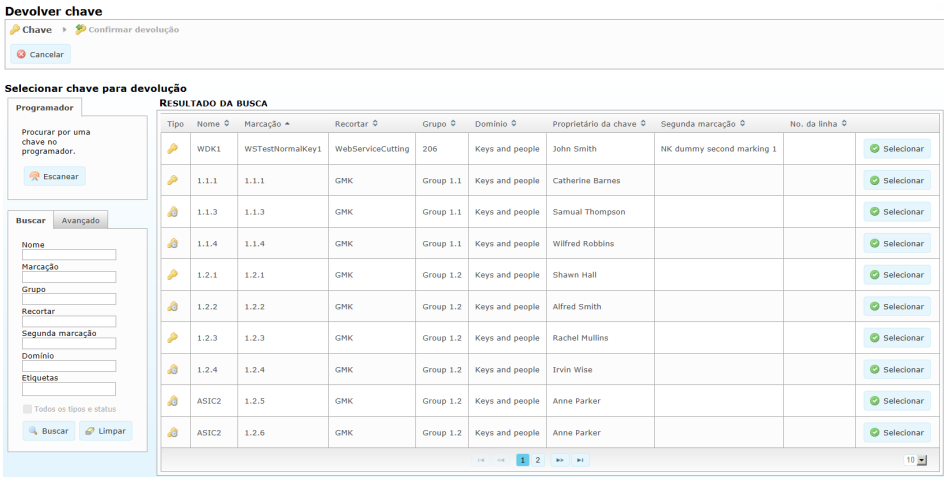
Consulte *Seção 9.10 "Código da empresa operadora ASSA ABLOY", página 213* para obter o código da empresa operadora ASSA ABLOY.

c) Imprima o código QR.

4.2.10 Como receber chaves de usuário (devolução)

1) Selecione **Tarefas » Devolver chave**.

Será exibida uma lista de todas as chaves entregues.



2) Encontre e selecione a chave a ser devolvida de uma das seguintes formas:

- A partir da lista, clique em **Selecionar** para a chave a ser devolvida.

  Para buscar uma chave, insira o critério de busca e clique em **Buscar**. Consulte também *Seção 4.2.1 "Como buscar chaves de usuário", página 34*.

- Se a chave a ser devolvida estiver na ranhura correta do programador local, clique em  no canto superior direito da página para escanear a chave.

  Devolver uma chave usando a função de escaneamento é, na maioria dos casos, a opção recomendada pois uma nova configuração pode ser programada imediatamente na chave. Isso é importante principalmente para sistemas não remotos.

3) Como devolver uma chave:

- Se a chave devolvida for escaneada no programador local, clique em **Redefinir chave e devolução** ou **Devolver chave sem redefinir**.

  A opção resetar é útil para chaves que terão configurações diferentes com cada entrega e devolução e é a opção recomendada na maioria dos casos.

- Se a chave devolvida não for escaneada, clique em **Aplicar**.

4) Opcional: Crie um recibo. Os recibos são criados como PDFs que podem ser impressos ou gravados.

ATENÇÃO!
Esta opção só está disponível se **Separar recibos de entrega e de devolução** estiver selecionado nas **Configurações do sistema**. Esta configuração é encontrada selecionando **Administração » Configurações do sistema » ADMINISTRAÇÃO » Recibos de chave**.

Consulte *Seção 6.4 "Como editar as configurações do sistema", página 99* para obter mais informações sobre como editar as configurações do sistema.

Consulte *Seção 6.9 "Como gerenciar modelos de recibo", página 129* para criar ou editar modelos de recibos.

a) Clique em **Gerar recibo...**.

   Aparecerá a janela **Seleção de recibo**.

b) Selecione o idioma adequado na lista suspensa.

c) Selecione o modelo adequado na lista suspensa.

   Todos os modelos de recibos de devolução no idioma selecionado são exibidos na lista suspensa.

d) Clique em **Imprimir recibo** ou **Fazer download**.

   Se **Fazer download** for selecionado, o download do recibo será feito na pasta **Downloads**.

4.2.11 Como imprimir um recibo em branco

Quando uma chave é entregue ou devolvida, o recibo é gerado no formato PDF com as informações de entrega e devolução. Também é possível gerar recibos com campos em branco para serem editamos manualmente.

1) **Tarefas » Recibo**.
2) Selecione **Imprimir recibo de entrega vazio...** ou **Imprimir recibo de devolução vazio...**.
3) Na janela pop-up:
   a) Selecione o idioma adequado na lista suspensa.
   b) Selecione o modelo adequado.

      Quando **Personalizar** está selecionado, a lista suspensa mostra todos os modelos do mesmo tipo (modelo para entrega ou devolução) no idioma selecionado.
4) Clique em **Gerar recibo** ou **Fazer download**.

4.2.12 Como lidar com uma chave perdida ou quebrada

Esta seção descreve como declarar chaves de usuário como perdidas ou quebradas. Para comunicar a perda ou quebra da Chave de comando, consulte *Seção 6.11.9 "Como comunicar e bloquear uma chave de comando perdida", página 137* ou *Seção 6.11.10 "Como comunicar uma chave de comando quebrada ou operacional", página 139*.

4.2.12.1 Como comunicar uma chave de usuário como quebrada

1) Há duas maneiras de iniciar a comunicação uma chave como quebrada:

- Selecione **Tarefas » Comunicar quebra da chave**. Vá para *Passo 2*.
- Na tela de informações detalhadas da chave quebrada (para pesquisar a chave, consulte *Seção 4.2.1 "Como buscar chaves de usuário", página 34*), clique no botão **Informar a quebra**. Vá para *Passo 4*.

2) Insira o critério de busca para encontrar o proprietário da chave e clique em **Buscar**.
3) Selecione a chave quebrada.
4) Clique em **Aplicar**.

   A tela de informações detalhadas para uma chave declarada quebrada conterá a opção para remover o status de quebrada.

Se a chave quebrada for substituída por uma chave clone, consulte *Seção 4.2.13 "Como substituir uma chave de usuário por um clone da fábrica", página 49* para obter mais instruções.

4.2.12.2 Como comunicar e bloquear uma chave de usuário perdida

Pré-requisito:

- Se algum cilindro precisar ser bloqueado e função de programação do cilindro estiver atribuída a uma chave de usuário, certifique-se de que a opção "Bloqueio de chave perdida com chaves de usuário" esteja ativada nas configurações do sistema. Consulte *Seção 6.4 "Como editar as configurações do sistema", página 99* para obter instruções sobre como alterar essa configuração. Isso só se aplica a um sistema remoto.

1) Há duas maneiras de iniciar a comunicação uma chave como perdida:

   - Selecione **Tarefas » Comunicar perda da chave**. Vá para *Passo 2*.
   - Na tela de informações detalhadas da chave perdida (para pesquisar a chave, consulte *Seção 4.2.1 "Como buscar chaves de usuário", página 34*), clique no botão **Comunicar como perdido**. Vá para *Passo 4*.

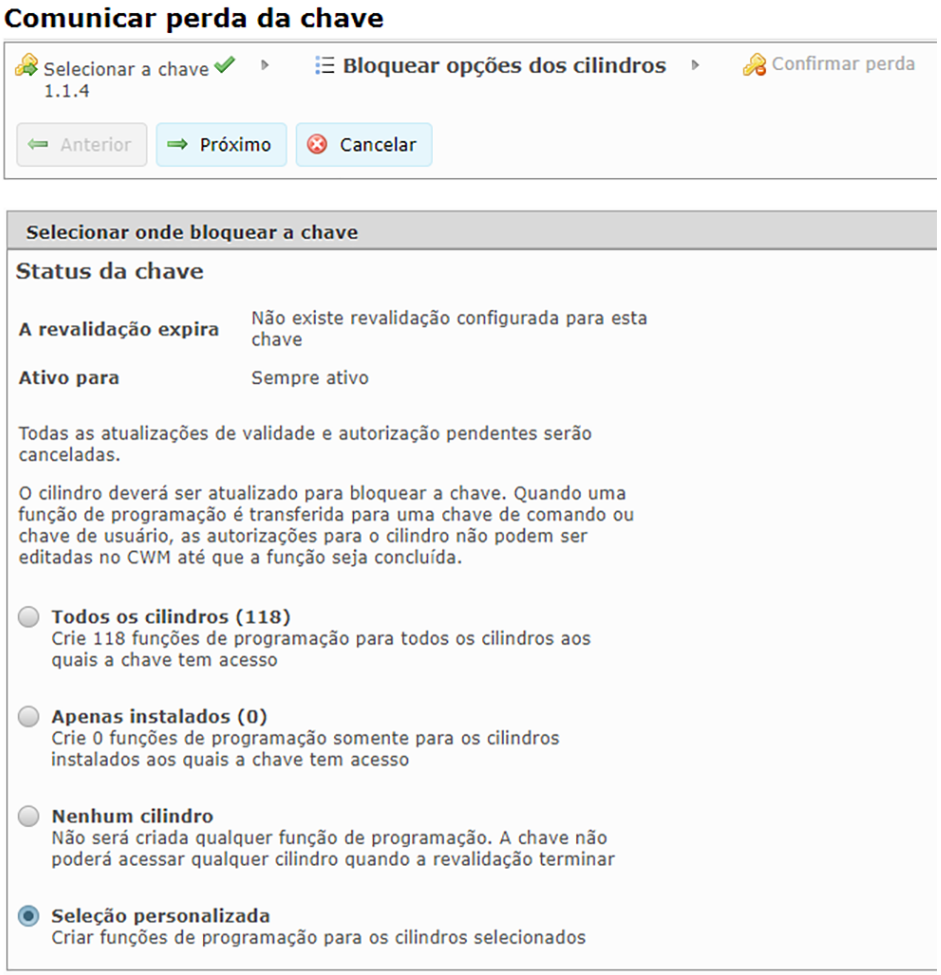
2) Insira o critério de busca para encontrar o proprietário da chave e clique em **Buscar**.
3) Selecione a chave perdida e clique em **Selecionar**.
4) Selecione os cilindros para os quais a chave será bloqueada:

   - Se for necessário programar os cilindros para bloquear imediatamente a chave perdida:

     Dica
     Para configurar o sistema para bloquear a chave perdida em cilindros recém-adicionados, ative **Bloquear chaves perdidas em cilindros novos durante a importação de extensão** nas Configurações do sistema. Consulte *Seção 6.4 "Como editar as configurações do sistema", página 99*.

     – Selecione **Todos os cilindros** ou **Apenas instalados** e vá para *Passo 7*.
     – Selecione **Seleção personalizada** e vá para *Passo 5* para selecionar os cilindros.

- Se a chave precisar ser comunicada como perdida no CWM sem bloquear seu acesso (por exemplo, enquanto aguarda a expiração do intervalo de revalidação atual), selecione **Nenhum cilindro**, clique em **Próximo** e vá para *Passo 11*.



5) Clique em **Próximo**.
6) Selecione os cilindros para os quais a chave perdida será bloqueada.
7) Clique em **Próximo**.
8) Opcional: Selecione a chave de bloqueio na lista clicando em **Selecionar**.

> **ATENÇÃO!**
> Se esse processo for ignorado, serão criadas funções de programação de cilindros para as chaves de comando.

Na guia **Buscar**, selecione **Todos os tipos e status** para mostrar as chaves de comando.

Na guia **Avançado**, em **Tipo**, selecione os tipos de chave para alterar o que é mostrado na lista.

ATENÇÃO!
Requisitos de bloqueio de chave:

- A chave de bloqueio deve ser da Geração 2 com versão do firmware 12.2 ou posterior.
- A chave de bloqueio deve ter memória suficiente.

9) Na página de confirmação, selecione o nível de prioridade em **Prioridade**.

As funções urgentes deverão ter um nível de prioridade alto.

10)

AVISO!
Por padrão, mesmo que nenhuma função de programação de cilindro seja criada para bloquear a chave perdida, a chave perdida ainda é adicionada no CWM à **Lista de chaves não autorizadas** para os cilindros afetados. No entanto, essas informações não são visíveis no CWM. Se esses cilindros forem reprogramados ou substituídos posteriormente, as informações sobre chaves não autorizadas armazenadas no CWM serão aplicadas, bloqueando, de fato, a chave perdida. Portanto, mesmo que a chave perdida seja comunicada como encontrada posteriormente, ela ainda será bloqueada por qualquer cilindro reprogramado ou substituído.

Para reautorizar a chave encontrada nesses cilindros, consulte *Seção 4.9.2 "Como configurar autorizações em cilindros", página 80*.

Para alterar essa configuração padrão, desative a configuração do sistema **Bloqueia silenciosamente chaves perdidas no cilindro durante a atualização da autorização**. Consulte *Seção 6.4 "Como editar as configurações do sistema", página 99*.

Depois de verificar todas as informações, clique em **Comunicar como perdido**.

11) Opcional: Clique em **Imprimir lista de cilindros** para gerar uma visualização resumida em PDF.

12)
- Se uma chave específica **NÃO** foi selecionada para programar os cilindros, continue a partir de *Passo 4* em *Seção 4.4.13 "Como programar os cilindros", página 61*.
- Se uma chave específica foi selecionada para programar os cilindros, siga as instruções abaixo.

13) Vá para a tela de informações detalhadas da chave de bloqueio selecionada.

Dica
Clicar em **Marcação da chave** em **Informações sobre bloqueio de chave** leva diretamente à tela de informações.

14) Vá para a guia **Programas** e confirme se a função do cilindro está atribuída à chave.

15)
- **Programação no PD local**

Insira a chave de bloqueio na ranhura direita do PD local e remova a chave de comando da ranhura esquerda do PD local.

- **Programação em um PD de parede**

  Insira a chave de bloqueio em um PD de parede.

A função de programação do cilindro é gravada automaticamente na chave de bloqueio.

16) Reprograme cada cilindro usando a chave de bloqueio.
17) Depois de programar os cilindros, comunique as funções concluídas do cilindro inserindo a Chave de bloqueio em um dos seguintes dispositivos:
    - A ranhura direita do PD local (remova a chave de comando da ranhura esquerda)
    - Um PD de parede

4.2.12.3 Como comunicar uma chave de usuário como encontrada

1) Encontre a chave perdida no CWM e exiba a tela informações detalhadas.

   Consulte *Seção 4.2.2 "Como escanear uma chave de usuário", página 35* ou *Seção 4.2.1 "Como buscar chaves de usuário", página 34*.

   ATENÇÃO!
   As chaves perdidas são filtradas usando o filtro **Perdido** na guia **Avançado**.

2) Clique em **Comunicar como encontrado**.

   O status da chave muda para **Em estoque**.

3) Reautorize a chave programando os cilindros afetados. Siga as instruções em *Seção 4.9.2 "Como configurar autorizações em cilindros", página 80*.

   Veja abaixo as informações sobre quais cilindros são afetados.

Cilindros afetados

Os cilindros que **devem ser programados** para reautorizar a chave:

- Cilindros que já foram programados para bloquear a chave perdida.
- Os cilindros que **não** foram programados para bloquear a chave perdida devem ser programados no seguinte caso:
  - O cilindro foi **reprogramado** ou **substituído**.

    E

  - A configuração do sistema **Bloqueia silenciosamente chaves perdidas no cilindro durante a atualização da autorização** é **ativada**.

ATENÇÃO!
Isso se aplica tanto aos cilindros para os quais os programas não foram criados quando a chave foi comunicada como perdida quanto aos cilindros para os quais os programas foram criados, mas ainda não foram executados.

Todos os outros cilindros:

A chave já tem acesso, portanto os cilindros não precisam ser programados. (Para cilindros para os quais foram criados programas, mas que ainda não foram executados, os programas são automaticamente cancelados).

4.2.13 Como substituir uma chave de usuário por um clone da fábrica

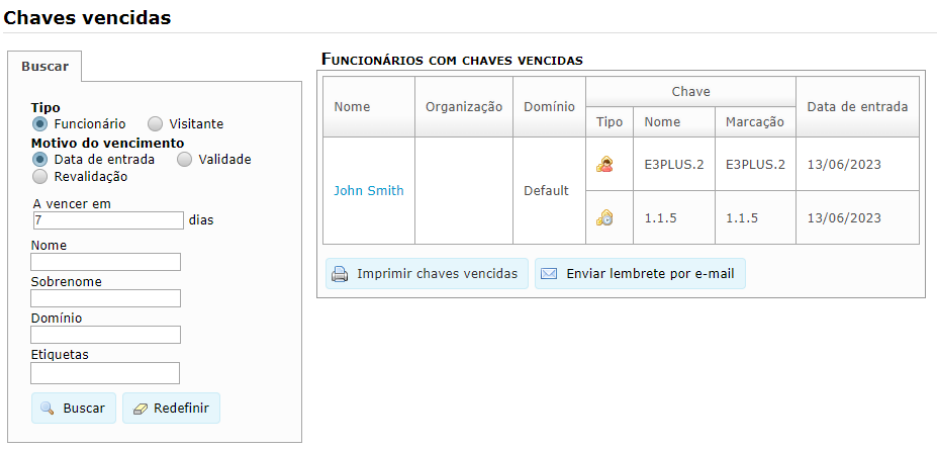
Caso um clone de reposição seja entregue da fábrica devido a uma chave quebrada, deverão ser executadas as etapas abaixo para assegurar o funcionamento da chave.

1) Quando a chave de reposição chega da fábrica, vá para **Administração » Importação de extensão » Carregar ou localizar arquivo(s) de importação de extensão** para carregar ou arquivo CWS fornecido no CWM (se a integração DCS estiver desativada) ou para buscar o arquivo a partir do DCS.
2) Crie e programe uma função de autorização para a chave de reposição. Consulte *Seção 4.9.1 "Como configurar autorizações em chaves", página 78*.
3) Crie e programe uma função de validade para a chave de reposição. *Seção 4.10.1 "Como configurar a validade de chave, a revalidação e a validação do PIN", página 86*.
4) Cancele qualquer função de agendamento existente para a chave antiga, recrie e programe as funções para a chave de reposição. Consulte *Seção 4.10.3 "Como configurar o cronograma de uma chave", página 89*.
5) A chave de reposição está pronta para uso.

4.2.14 Como visualizar chaves de usuário vencidas

1) Selecione **Tarefas » Chaves vencidas**.
2) Na guia **Buscar**, selecione **Funcionário** ou **Visitante** para escolher o tipo de proprietário da chave.

   Será exibida uma lista de todas as chaves entregues a funcionários ou visitantes com a data de devolução dentro do número de dias especificado.



   O número de dias padrão pode ser editado nas Configurações do sistema. Consulte *Seção 6.4 "Como editar as configurações do sistema", página 99*.
3) Selecione um **Motivo do vencimento**, insira outro critério de busca e clique em **Buscar**.

   Motivo do vencimento:

   - Se for selecionada a **Data de entrada**, serão listadas as chaves com a data de entrada dentro do número de dias especificado.

- Se for selecionada a **Validade**, serão listadas as chaves com o intervalo de validade que termina dentro do número de dias especificado.
- Se **Revalidação** estiver selecionado, serão listadas chaves com um intervalo de revalidação que termina entre as datas especificadas.

4) Clique em **Imprimir chaves vencidas** para imprimir uma lista das chaves vencidas ou que necessitam revalidação.

5) Clique em **Enviar lembrete por e-mail** para enviar um lembrete por e-mail para funcionários ou visitantes com chaves vencidas.

   Para que esta opção esteja disponível, deverá estar selecionado **Sistema de envio de mensagens do usuário** nas **Configurações do sistema**. Consulte *Seção 6.4 "Como editar as configurações do sistema", página 99*.

4.2.15 Como atualizar e revalidar uma chave de usuário

Por meio dos programadores locais
Se uma chave for inserida na ranhura direita do programador local, ela é atualizada diretamente durante a operação no CWM.

Quando as seguintes ações são operadas localmente, a chave é revalidada no programador local ao mesmo tempo:

- configurar **Cronograma**
- ler **Trilha de auditoria**
- alterar **Cilindros na lista de acesso**

Se as seguintes condições forem atendidas, a chave é atualizada e/ou revalidada na ranhura direita do programador local **sem** uma chave de comando:

- Chave geração 2 com versão do firmware 12.3 ou posterior
- O CLIQ Connect no PC está ativado

> **ATENÇÃO!**
> A chave de comando deve ser removida da ranhura esquerda do programador local antes da atualização e revalidação.

Por meio dos programadores remotos
Os proprietários de chave podem atualizar e/ou revalidar suas chaves inserindo-as em um PD de parede ou programador móvel CLIQ.

A chave também pode ser atualizada e/ou revalidada quando está conectada ao CLIQ Connect por meio de um programador móvel CLIQ Connect.

Consulte *Seção 8.1.5 "Revalidação de uma chave", página 165* e *Seção 8.1.6 "Revalidação flexível", página 168* para obter mais informações sobre a revalidação de chaves.

4.2.16 Como copiar as configurações da chave de usuário

A configuração em uma chave pode ser copiada para outra chave escaneada no Programador local. Quando aplicável, as seguintes configurações serão copiadas:

- Validade
- Agenda

- Configurações de revalidação
- Lista de acesso da chave
- Perfis de acesso

Para chaves incluídas em listas de acesso do cilindro:

- As funções de programação do cilindro são criadas para atualizar as listas de acesso do cilindro.

1) Encontre a chave da qual a configuração deverá ser copiada e vá para a tela de informações detalhadas.

   Consulte *Seção 4.2.1 "Como buscar chaves de usuário", página 34*.

2) Insira a chave alvo no Programador local.
3) Clique em **Copiar configurações da chave**.

   A chave está sendo escaneada.

4) Clique em **Selecionar**.
5) Selecione uma **Prioridade** para as funções de programação do cilindro necessárias.

   As funções urgentes deverão ter um nível de prioridade alto.

6) Clique em **Aplicar**.

   A configuração existente na chave alvo é substituída e, caso necessário, são criadas funções de programação do cilindro.

   Foram criados eventos especificando data e hora para a alteração e marcação a partir da chave fonte e chave de comando.

4.2.17 Impressão do relatório de chaves do usuário

1) Encontre a chave e vá para sua tela de informações detalhadas.

   Consulte *Seção 4.2.1 "Como buscar chaves de usuário", página 34* para buscar a chave e exibir a tela informações detalhadas.

   Para escanear a chave no Programador local e exibir as informações detalhadas, consulte *Seção 4.2.2 "Como escanear uma chave de usuário", página 35*

2) Clique em **Imprimir relatório de chave**.
3) Selecione se deseja incluir na lista os cilindros mecânicos ou não e clique em **OK**.
4) Uma visualização será apresentada na janela pop-up.

   - Para salvar, clique no ícone Gravar e especifique uma pasta para salvar.
   - Para imprimir, clique em **...** e selecione **Imprimir**.

4.2.18 Como exportar as informações de uma chave de usuário

1) Selecione **Informações do sistema » Chaves**.

   Será exibida uma lista de todas as chaves.

2) Busque as chaves.

   Consulte *Seção 4.2.1 "Como buscar chaves de usuário", página 34*.

3) Selecione as chaves cujos dados serão exportados a partir dos resultados de busca de chaves.

4) Clique em **Exportar para arquivo CSV**.

5) Na janela pop-up de download do arquivo, clique em **Gravar**.

O download de um arquivo CSV é feito na pasta **Downloads**.

ATENÇÃO!
Para ser possível abrir o arquivo em Excel da maneira correta, o delimitador para o arquivo deverá ser configurado de acordo com as configurações regionais. Consulte *Seção 6.4 "Como editar as configurações do sistema", página 99* para alterar o delimitador.

4.3 Como gerenciar grupos de chaves

4.3.1 Como buscar grupos de chaves

1) Selecione **Informações do sistema » Grupos de chaves**.

Será exibida uma lista de todos os grupos de chaves.

Os símbolos abaixo são utilizados:

- Grupo de chaves normais
- Grupo de chaves dinâmicas

2) Insira o critério de busca.

Ao digitar nos campos de busca, o CWM aceita a primeira parte de uma cadeia de caracteres de busca bem como um asterisco (*). Se a busca for para "Laboratório 1", escrever "Lab", "*1" ou "Lab*1" fornecerá resultados incluindo "Laboratório 1".

Ao inserir o campo de busca **Etiquetas**, todas as etiquetas relacionadas aparecerão como uma lista selecionável.

3) Clique em **Buscar**.

4) Clique na linha do grupo de chaves para exibir informações detalhadas sobre um resultado de busca.

4.3.2 Como editar as informações de um grupo de chaves

1) Encontre o grupo de chaves e vá para sua tela de informações detalhadas.

   Consulte *Seção 4.3.1 "Como buscar grupos de chaves", página 52*.

2) Clique em **Editar**.
3) Para editar o nome do grupo de chaves, digite o nome.
4) Para adicionar uma etiqueta clique em **Adicionar etiqueta**. Consulte também *Seção 4.3.3 "Como adicionar ou remover etiquetas de grupos de chaves", página 53*.
5) Clique em **Gravar**.

4.3.3 Como adicionar ou remover etiquetas de grupos de chaves

1) Encontre o grupo de chaves.

   Consulte *Seção 4.2.1 "Como buscar chaves de usuário", página 34* para buscar um grupo de chaves.

2) - Para adicionar ou remover etiquetas de um grupo de chaves individual, acesse *Passo 3*.
   - Para adicionar ou remover etiquetas de vários grupos de chaves, acesse *Passo 4*.

3) **Adicionar ou remover etiquetas de um grupo de chaves individual:**

   1. Selecione o grupo de chaves e vá para sua tela de informações detalhadas.
   2. Clique em **Editar**.
   3. Adicione ou remova a etiqueta de um grupo de chaves individual.

      Para adicionar uma etiqueta:

      a) Clique em **Adicionar etiqueta...**.
      b) Insira um nome para a etiqueta.
      c) Clique em **OK**.

      Para remover uma etiqueta:
      Clique na etiqueta a ser removida.

   4. Clique em **Gravar**.

4) **Adicionar ou remover etiquetas de vários grupos de chaves:**

   1. Selecione os grupos de chaves nos resultados da busca, marcando as caixas de seleção.
   2. **Para adicionar uma etiqueta:**

      a) Clique em **Adicionar etiqueta...**.
      b) Insira o nome da etiqueta.
      c) Clique em **OK**.

Para remover uma etiqueta:

a) Clique em **Remover etiqueta...**.

b) Insira o nome da etiqueta.

c) Clique em **OK**.

Consulte também *Seção 8.2.6 "Etiquetas", página 179*.

4.3.4 Como visualizar os membros de um grupo de chaves

1) Encontre o grupo de chaves e vá para sua tela de informações detalhadas.

   Consulte *Seção 4.3.1 "Como buscar grupos de chaves", página 52*.

2) Selecione a guia **Membros**.

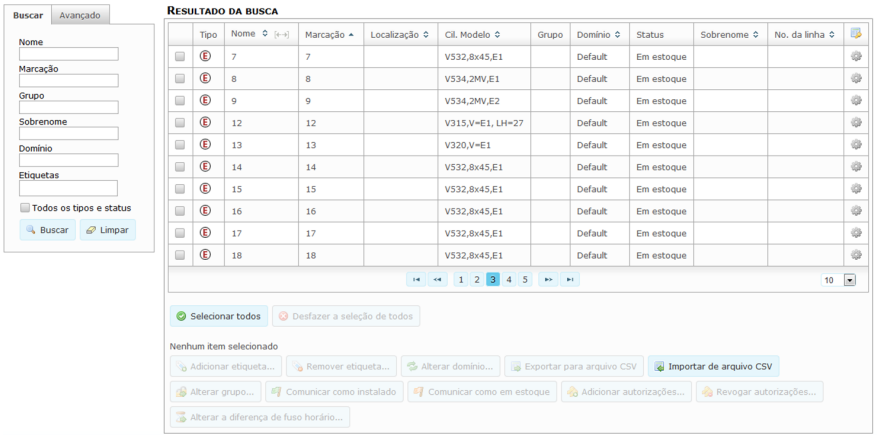
   Será exibida uma lista com todas as chaves desse grupo de chaves.

4.4 Como gerenciar cilindros

4.4.1 Como buscar por cilindros

1) Selecione **Informações do sistema » Cilindros**.

   Será exibida uma lista de todos os cilindros, excluindo os cilindros mecânicos e quebrados.



Os símbolos abaixo são utilizados:

- (E) Cilindro eletrônico
- (M) Cilindro mecânico
- (E)(M) Cilindro duplo (Exemplo: eletrônico no lado A e mecânico no lado B)

2) Selecione a guia **Buscar** ou **Avançado**.

   Por padrão, os cilindros mecânicos e quebrados não são exibidos. Para incluir esses cilindros também no resultado de busca, selecione **Todos os tipos e status**.

   A guia **Avançado** inclui também os campos de busca tipo de cilindro, status do inventário, status operacional, segunda marcação e, por meio de uma lista suspensa, campos personalizados (caso definidos em **Configurações do sistema**). Esta configuração é encontrada selecionando **Administração » Configurações do sistema » ADMINISTRAÇÃO » Campos personalizados dos cilindros**.).

3) Insira o critério de busca.

Ao digitar nos campos de busca, o CWM aceita a primeira parte de uma cadeia de caracteres de busca bem como um asterisco (*). Se a busca for para "Laboratório 1", escrever "Lab", "*1" ou "Lab*1" fornecerá resultados incluindo "Laboratório 1".

Ao inserir o campo de busca **Etiquetas**, todas as etiquetas relacionadas aparecerão como uma lista selecionável.

4) Clique em **Buscar**.

5) Clique na linha do cilindro específico para exibir informações detalhadas em um resultado de busca.

Consulte *Seção 9.3.5 "Atributos do cilindro", página 199* para obter informações sobre os atributos do cilindro.

4.4.2 Como editar as informações de um cilindro

1) Encontre o cilindro e vá para sua tela de informações detalhadas.

Consulte *Seção 4.4.1 "Como buscar por cilindros", página 54*.

Se for necessário editar **Sobrenome** ou **Campos personalizados**, prossiga para *Passo 6*.

2) Clique em **Editar**.

3) Edite os campos.

Consulte *Seção 9.3.5 "Atributos do cilindro", página 199* para obter mais informações sobre os atributos do cilindro.

4)
- Para adicionar uma etiqueta clique em **Adicionar etiqueta**. Consulte também *Seção 4.4.3 "Como adicionar ou remover etiquetas de cilindros", página 55*
- Para adicionar um link externo clique em **Adicionar link externo**. Consulte também *Seção 4.4.4 "Como gerenciar links externos de um cilindro", página 56*

5) Clique em **Gravar**.

6) **Sobrenome** e **Campos personalizados** são editados na guia **Informações adicionais**.

> **ATENÇÃO!**
> Campos personalizados (são definidos em **Configurações do sistema**) Consulte *Seção 6.4 "Como editar as configurações do sistema", página 99*.

a) Selecione a guia **Informações adicionais**.

b) Clique em **Editar**.

c) Atualize o campo .

d) Clique em **Gravar**.

4.4.3 Como adicionar ou remover etiquetas de cilindros

Consulte *Seção 8.2.6 "Etiquetas", página 179* para obter informações sobre etiquetas.

1) Selecione **Informações do sistema » Cilindros**.

Será exibida uma lista de todos os cilindros.

- Para adicionar ou remover etiquetas de um cilindro individual, acesse *Passo 2*.
- Para adicionar ou remover etiquetas de vários cilindros simultaneamente, acesse *Passo 3*.

2) **Para adicionar ou remover etiquetas de um cilindro individual:**

1. Selecione o cilindro e vá para sua tela de informações detalhadas.
2. Clique em **Editar**.
3. Adicione ou remova uma etiqueta de um cilindro individual.

   Para adicionar uma etiqueta:

   a) Clique em **Adicionar etiqueta...**.
   b) Insira um nome para a etiqueta.
   c) Clique em **OK**.

   Para remover uma etiqueta:
   Clique na etiqueta a ser removida.
4. Clique em **Gravar**.

3) **Para adicionar ou remover etiquetas de vários cilindros:**

1. Selecione os cilindros nos resultados da pesquisa, marcando as caixas de seleção.
2. **Como adicionar uma etiqueta:**

   a) Clique em **Adicionar etiqueta...**.
   b) Insira o nome da etiqueta.
   c) Clique em **OK**.

   Como remover uma etiquetas:

   a) Clique em **Remover etiqueta...**.
   b) Insira o nome da etiqueta.
   c) Clique em **OK**.

4.4.4 Como gerenciar links externos de um cilindro

Para obter informações sobre links externos, consulte *Seção 8.4 "Links externos", página 182*.

1) Encontre o cilindro e vá para sua tela de informações detalhadas.

   Consulte *Seção 4.4.1 "Como buscar por cilindros", página 54*.

2) Clique em **Editar**.

3) **Para adicionar um link externo:**

1. Clique em **Adicionar.**
2. Insira o **Nome** da URL.
3. Insira **URL**. A **URL** deve começar com um protocolo (por exemplo http:// ou ftp://).

Se foi definida uma URL raiz nas **Configurações do sistema** (item **URL raiz dos links externos**), só é necessário adicionar a última parte da URL. Consulte também *Seção 6.4 "Como editar as configurações do sistema", página 99*.

4. Clique em **OK**.

Para editar um link externo:

1. Clique em **Editar** no link externo a ser editado.
2. Atualize os campos.
3. Clique em **OK**.

Para remover um link externo:

Clique em **Remover** no link externo a ser removido.

4) Clique em **Gravar**.

4.4.5 Como visualizar grupos de chaves e exceções em uma lista de acesso dos cilindros

A guia **Chaves na lista de acesso** é usada para exibir grupos de chaves e exceções na lista de acesso dos cilindros.

1) Encontre o cilindro e vá para sua tela de informações detalhadas.

   Consulte *Seção 4.4.1 "Como buscar por cilindros", página 54*.

2) Selecione a guia **Chaves na lista de acesso**.

   Nessa lista de acesso do cilindro será exibida uma lista com todos os grupos de chaves e exceções. Consulte *Seção 4.9.2 "Como configurar autorizações em cilindros", página 80* para editá-la.

4.4.6 Como visualizar o histórico de atualizações do cilindro

A guia Atualizar histórico é usada para rastrear a programação da chave.

1) Encontre o cilindro e vá para sua tela de informações detalhadas.

   Consulte *Seção 4.4.1 "Como buscar por cilindros", página 54*.

2) Selecione a guia **Atualizar histórico**.

   Será exibida uma lista com todas as atualizações do cilindro.

   Os símbolos abaixo são utilizados:

   - Existe uma função de programação mas ainda não foi iniciada
   - Uma função de programação foi programada para uma chave de comando
   - A função de programação foi concluída
   - Falha ou cancelamento da função de programação
   - A função de programação foi substituída por uma nova função

3) Clique no link na coluna **Tipo** para exibir mais detalhes sobre uma atualização específica.

4.4.7 Como visualizar eventos do cilindro

A guia **Eventos** é usada para rastrear as operações do administrador no CWM, como comunicar um cilindro como quebrado.

1) Encontre o cilindro e vá para sua tela de informações detalhadas.

   Consulte *Seção 4.4.1 "Como buscar por cilindros", página 54*.

2) Selecione a guia **Eventos**.

   Será exibida uma lista com todos os eventos do cilindro.

4.4.8 Como editar diferença de fuso horário do cilindro

O fuso horário pode ter diferenças para cilindros em um domínio caso estejam localizados em fusos horários diferentes. Essa configuração só está disponível para cilindros geração 2.

Consulte *Seção 7.2.5 "Gerações das chaves", página 158* para obter mais informações sobre as gerações das chaves.

1) Encontre o cilindro e vá para sua tela de informações detalhadas.

   Consulte *Seção 4.4.1 "Como buscar por cilindros", página 54*.

2) Clique em **Alterar a diferença de fuso horário...**.
3) Configure a **Diferença de fuso horário** para o número de minutos desejado.
4) Configure a prioridade da função.
5) Clique em **OK**.

   Será criada uma função de programação de cilindro. Para programar o cilindro, consulte *Seção 4.4.13 "Como programar os cilindros", página 61*.

> **ATENÇÃO!**
> Enquanto o programa está aguardando a execução, o botão **Cancelar a alteração da diferença de fuso horário** é exibido nas informações detalhadas para o cilindro.
>
> Clique no botão, enquanto edita, para cancelar a alteração da diferença de fuso horário.

A diferença de fuso horário pode ser editada para vários cilindros simultaneamente. Selecione os cilindros na lista do resultado de busca e clique em **Diferença de fuso horário**.

4.4.9 Como alterar o status do cilindro

Os cilindros possuem um status de estoque como **em estoque** ou **instalado** e um status de operação como **operacional** ou **quebrado**.

1) Encontre o cilindro e vá para sua tela de informações detalhadas.

   Consulte *Seção 4.4.1 "Como buscar por cilindros", página 54*.

2) **Para mudar para o status Instalado**

   1. Clique em **Comunicar como instalado**.
   2. Clique em **OK**.

   Vários cilindros podem ser comunicados como instalados simultaneamente. Selecione os cilindros na lista do resultado de busca e clique em **Comunicar como instalado**.

Para alterar o status para Em estoque

1. Clique em **Comunicar como em estoque**.
2. Clique em **OK**.

   Vários cilindros podem ser comunicados como em estoque simultaneamente. Selecione os cilindros na lista do resultado de busca e clique em **Comunicar como em estoque**.

Para comunicar como quebrado

1. Clique em **Informar a quebra**.
2. Selecione **Somente informar a quebra**.

   Se for necessário um processo de substituição, consulte *Seção 4.4.10 "Como substituir um cilindro quebrado", página 59*.
3. Clique em **Próximo**.
4. Clique em **Aplicar**.

Para informar que o cilindro está novamente em operação

1. Clique em **Relatar operacional**.

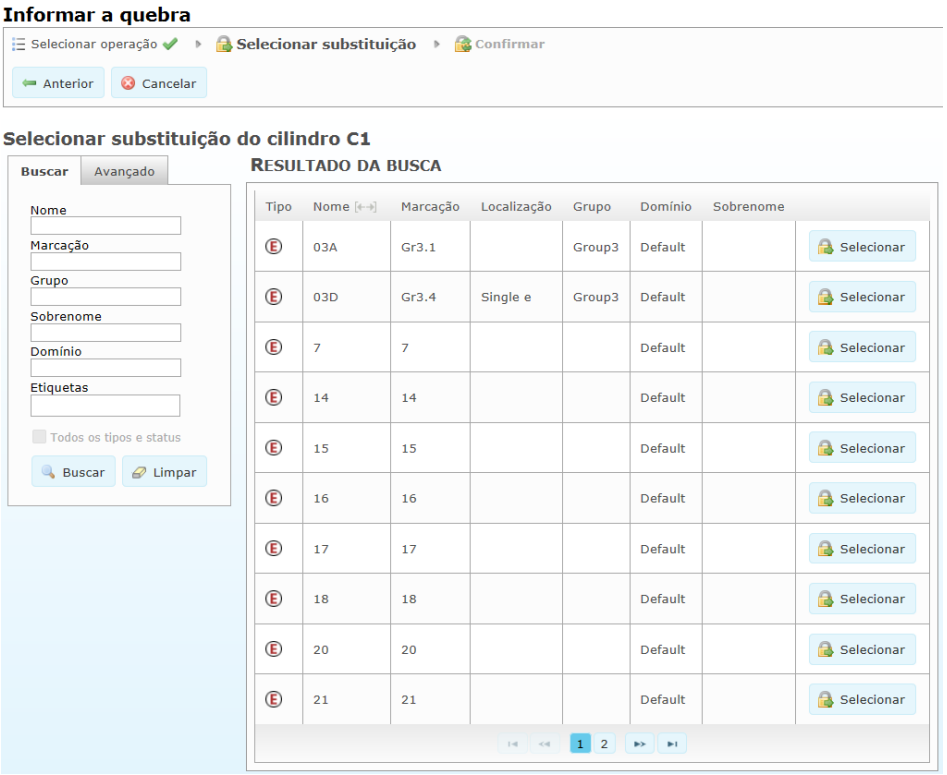
   Esta opção só está disponível para cilindros anteriormente comunicados como quebrados.
2. Clique em **OK**.
3. Será criada uma função de programação.

4.4.10 Como substituir um cilindro quebrado

1) Encontre o cilindro e vá para sua tela de informações detalhadas.

   Consulte *Seção 4.4.1 "Como buscar por cilindros", página 54*.
2) Clique em **Comunicar como quebrado**.
3) Selecione **Informar a quebra e substituir por outro cilindro**.
4) Clique em **Próximo**.

   Será exibida uma lista com todos os cilindros do mesmo tipo do cilindro informado, conforme encontrados em estoque.



5) Para buscar cilindros específicos, insira o critério de busca e clique em **Buscar**.

6) Selecione um cilindro de substituição clicando em **Selecionar**.

7) Selecione um nível de **Prioridade**.

   As funções urgentes deverão ter um nível de prioridade alto.

8) Clique em **Aplicar**.

   A configuração atual, incluindo atualizações pendentes, para o cilindro de reposição serão descartadas e substituídas pela configuração do cilindro quebrado.

   Serão criadas funções de atualização remotas para as chaves associadas e os perfis de acesso que dão acesso ao cilindro quebrado serão atualizados.

4.4.11 Como substituir um cilindro por um clone da fábrica

Caso um clone de reposição seja entregue da fábrica devido a um cilindro quebrado, deverão ser executadas as etapas abaixo para assegurar o funcionamento do cilindro.

1) Quando o cilindro clonado chega da fábrica, vá para **Administração » Importação de extensão » Carregar ou localizar arquivo(s) de importação de extensão** para carregar ou arquivo CWS fornecido no CWM (se a integração DCS estiver desativada) ou para buscar o arquivo a partir do DCS.

2) Crie uma função de reprogramação para o cilindro de reposição. Consulte *Seção 4.4.12 "Como solicitar a reprogramação do cilindro", página 61*.

3) Programe o cilindro de reposição. Consulte *Seção 4.4.13 "Como programar os cilindros", página 61*.

4) O cilindro de reposição está pronto para uso.

4.4.12 Como solicitar a reprogramação do cilindro

Quando um cilindro é reprogramado, seu conteúdo de memória é apagado, incluindo as trilhas de auditoria. A lista de acesso do cilindro é recuperada como parte da reprogramação. É necessária uma chave de comando mestre ou uma chave de comando normal com direitos de reprogramação de cilindro para executar a função de reprogramação.

1) Encontre o cilindro e vá para sua tela de informações detalhadas.

   Consulte *Seção 4.4.1 "Como buscar por cilindros", página 54*.

2) Clique em **Reprogramar**.

   Para cilindros duplos, clique em **Reprogramar o lado A**, **Reprogramar o lado B** ou ambos.

3) Selecione **Prioridade**.

   As funções urgentes deverão ter uma prioridade alta.

4) Clique em **OK**.

Consulte também *Seção 4.4.13 "Como programar os cilindros", página 61*.

4.4.13 Como programar cilindros com uma chave de comando

Pré-requisitos:

- Uma chave de comando com permissão para **Programar o cilindro**.
- Para funções que envolvem a troca do grupo de cilindros do cilindro: uma chave de comando com a capacidade para **Programar o grupo de cilindros**.
- Para funções de reprogramação: Uma chave de comando mestre ou uma chave de comando normal com a permissão **Reprogramação de cilindro**

Se a chave de comando a ser usada para a programação estiver imediatamente disponível, siga o procedimento em *Seção 4.4.13.1 "Como programar cilindros usando uma chave de comando com o Programador local", página 61*.

Se a chave de comando a ser usada para a programação não estiver imediatamente disponível, siga o procedimento em *Seção 4.4.13.2 "Como programar cilindros usando uma chave de comando Connect ou uma chave de comando com o Programador remoto", página 63*. Esse procedimento requer um Programador remoto ou uma Chave de comando do CLIQ Connect.

Consulte *Seção 8.5 "Programação do cilindro", página 183* para obter mais informações sobre a programação de cilindros.

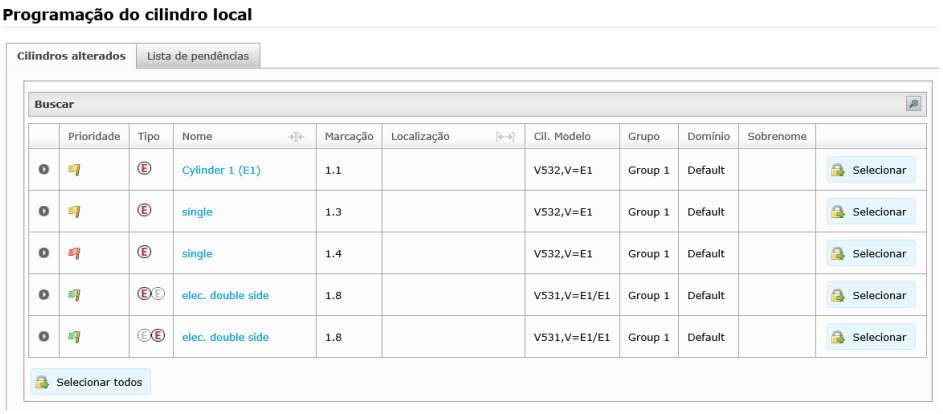
4.4.13.1 Como programar cilindros usando uma chave de comando com o Programador local

Para enviar programas para uma chave de comando imediatamente disponível e programar cilindros:

1) Selecione **Tarefas » Programação do cilindro**.

   Será exibida uma lista de todos os cilindros que necessitam programação. Os níveis de prioridade para as funções são listados na coluna mais à esquerda.

2) Para selecionar as funções a serem executadas, clique em **Selecionar** na lista ou em **Selecionar todos** que está localizado embaixo da lista.



3) Clique em **Enviar para chave de comando**.

ATENÇÃO!
Enquanto a função de programação de um cilindro é carregada para uma Chave de comando, as configurações de autorização para esse cilindro estão bloqueadas para edição no CWM.

- Selecione a guia **Lista de pendências** para ver uma lista das funções que estão atualmente na Chave de comando.

- Para imprimir a lista, clique em **Imprimir lista pendências**.

4) Insira a chave de comando nos cilindros a serem programados, um a um.

> **CUIDADO!**
> Mantenha a chave de comando inserida até que o programa seja concluído.
>
> Se a função falhar, insira a chave de comando em um Programador remoto conectado ao CWM para recarregar o programa novamente na chave de comando. Consulte também *"Reprogramação"*.

5) Entre novamente no CWM.

6) Selecione **Tarefas » Programação do cilindro**.

7) Selecione a guia **Lista de pendências**.

8) Clique em **Atualizar**.

   O status das funções de programação é carregado a partir da Chave de comando.

9) Opcional: Clique em **Remover programas concluídos**.

4.4.13.2 Como programar cilindros usando uma chave de comando Connect ou uma chave de comando com o Programador remoto

Ao longo do procedimento de programação das funções dos cilindros, o status da interação do programador remoto é indicado pelos LEDs. Consulte *Seção 9.5.1 "Indicações de programador de parede (Geração 1) e programador móvel", página 207* ou *Seção 9.5.2 "Indicações de programador de parede (geração 2)", página 208* para obter mais informações sobre o indicador de LED.

1) Atribua funções de programação do cilindro a uma chave de comando:

   a) Encontre a Chave de comando.

      Consulte *Seção 6.11.1 "Como buscar chaves de comando", página 133* para buscar a chave de comando e exibir a tela informações detalhadas.

   b) Selecione a guia **Programação do cilindro**.

   c) Clique em **Atribuir cilindros para programação**.

   d) Clique em **Selecionar** para cada função de programação do cilindro a ser executada.

      > **AVISO!**
      > Para funções que incluem alterações no grupo de cilindros, poderão ser atribuídas, no máximo, 100 funções a uma chave de comando. Atribuir mais funções poderá levar a erros de programação.

   e) Clique em **Aplicar**.

      Depois de atribuir a função de programação do cilindro à chave de comando, será gerado um e-mail para o proprietário da chave de comando com informações de que existem programas a serem coletados.

2) Insira a chave de comando em um Programador remoto ou conecte a chave de comando Connect ao CLIQ Connect para carregar as funções de programação do cilindro.

Assim que a função de programação do cilindro estiver transferida, será gerado um e-mail para o proprietário da chave de comando com informações sobre quais cilindros programar.

3) Insira a Chave de comando nos cilindros a serem programados.

> **CUIDADO!**
> Mantenha a chave inserida até que a função de programação seja concluída.
>
> Se a função falhar, insira a chave em um PD remoto conectado ao CWM para recarregar a função de programação novamente na chave. Consulte também *"Reprogramação"*.

4) Insira a chave de comando em um Programador remoto ou conecte a chave de comando Connect ao CLIQ Connect para atualizar o status dos programas.

4.4.14 Como importar informações do cilindro

As **Informações de importação de cilindros** possibilitam a importação em massa dos dados atualizados dos cilindros. A função só se aplica à atualização dos dados dos cilindros existentes.

O arquivo CSV é usado para a importação. Para gravar um arquivo CSV novo, a maneira mais simples é exportar um arquivo CSV com dos dados dos cilindros existentes e então editar o arquivo exportado com o Excel ou com um editor de texto. Consulte *Seção 4.4.15 "Como exportar informações do cilindro", página 65*.

> **ATENÇÃO!**
> As informações dos cilindros podem ser importadas tanto dos arquivos CSV como dos **Arquivos de importação de extensão** mas o conteúdo não se sobrepões. Os arquivos CSV atualizam as informações dos cilindros que os usuários podem alterar no GUI enquanto que os arquivos de importação de extensão atualizam dados de fábrica não editáveis. Como resultado, os arquivos CSV não podem sobrescrever as extensões ou vice-versa. Consulte *Seção 6.16 "Importação de extensões", página 151* para obter mais informações sobre extensões.

1) Clique em **Info do sistema » Cilindros**.
2) Clique em **Importar de arquivo CSV**.
3) Clique em **Selecionar** para encontrar o arquivo gravado localmente no computador.
4) Clique em **Abrir**.
5) Clique em **Importar** para importar e validar o arquivo.

   São exibidas as informações sobre quantas entradas válidas o arquivo contém. Se o arquivo não seguir as especificações, a importação não é possível.

ATENÇÃO!
Ao importar informações do cilindro, somente as seguintes colunas no arquivo CSV serão atualizadas.

- Nome
- Sobrenome
- Localização
- Status do inventário
- Campos personalizados (caso definidos em **Configurações do sistema**)

Os dados do cilindro existentes serão sobrescritos.

ATENÇÃO!
Para importar informações do cilindro a partir de um arquivo CSV, os valores em **Marcação** ou os valores combinados de **Marcação** e **Segunda marcação** devem ser exclusivos.

4.4.15 Como exportar informações do cilindro

1) Busque os cilindros.

   Consulte *Seção 4.4.1 "Como buscar por cilindros", página 54*.

2) Selecione os cilindros cujos dados serão exportados a partir dos resultados de busca de cilindros.

3) Clique em **Exportar para arquivo CSV**.

   ATENÇÃO!
   Para ser possível abrir o arquivo em Excel da maneira correta, o delimitador para o arquivo deverá ser configurado de acordo com as configurações regionais. Consulte *Seção 6.4 "Como editar as configurações do sistema", página 99* para alterar o delimitador.

4) Na janela pop-up de download do arquivo, clique em **Abrir** ou **Gravar**.

4.5 Como gerenciar grupos de cilindros

4.5.1 Como buscar grupos de cilindros

1) Selecione **Informações do sistema » Grupos de cilindros**.

   Será exibida uma lista de todos os grupos de cilindros.

2) Insira o critério de busca.

   Ao digitar nos campos de busca, o CWM aceita a primeira parte de uma cadeia de caracteres de busca bem como um asterisco (*). Se a busca for para "Laboratório 1", escrever "Lab", "*1" ou "Lab*1" fornecerá resultados incluindo "Laboratório 1".

   Ao inserir o campo de busca **Etiquetas**, todas as etiquetas relacionadas aparecerão como uma lista selecionável.

3) Clique em **Buscar**.

4) Para exibir informações detalhadas de um resultado de busca, clique no grupo de cilindros específico.

4.5.2 Como editar as informações de um grupo de cilindros

1) Encontre o grupo de cilindros e vá para sua tela de informações detalhadas.

   Consulte *Seção 4.5.1 "Como buscar grupos de cilindros", página 66*.

2) Clique em **Editar**.

3) Para editar o nome do grupo de cilindros, atualize o campo **Nome**.

4) Para adicionar uma etiqueta clique em **Adicionar etiqueta...**. Consulte também *Seção 4.5.3 "Como adicionar ou excluir etiquetas de grupos de cilindros", página 66*

5) Para alterar o domínio, clique em **Alterar domínio...**. Consulte também *Seção 6.6.8 "Como alterar o domínio dos Grupos de cilindros", página 126*.

6) Clique em **Gravar**.

4.5.3 Como adicionar ou excluir etiquetas de grupos de cilindros

1) Encontre o grupo de cilindros.

   Consulte *Seção 4.2.1 "Como buscar chaves de usuário", página 34* para buscar um grupo de cilindros.

2) - Para adicionar ou remover etiquetas de um grupo de cilindros individual, acesse *Passo 3*.
   - Para adicionar ou remover etiquetas de vários grupos de cilindros, acesse *Passo 4*.

3) **Adicionar ou remover etiquetas de um grupo de cilindros individual:**

1. Selecione o grupo de cilindros e vá para sua tela de informações detalhadas.
2. Clique em **Editar**.
3. Adicione ou remova a etiqueta de um grupo de cilindros individual.

   Para adicionar uma etiqueta:

   a) Clique em **Adicionar etiqueta...**.
   b) Insira um nome para a etiqueta.
   c) Clique em **OK**.

   Para remover uma etiqueta:
   Clique na etiqueta a ser removida.
4. Clique em **Gravar**.

4) **Adicionar ou remover etiquetas de vários grupos de cilindros:**

1. Selecione os grupos de cilindros nos resultados da busca, marcando as caixas de seleção.
2. **Para adicionar uma etiqueta:**

   a) Clique em **Adicionar etiqueta...**.
   b) Insira o nome da etiqueta.
   c) Clique em **OK**.

   Para remover uma etiqueta:

   a) Clique em **Remover etiqueta...**.
   b) Insira o nome da etiqueta.
   c) Clique em **OK**.

Consulte também *Seção 8.2.6 "Etiquetas", página 179*.

4.5.4 Como visualizar os membros de um grupo de cilindros

1) Encontre o grupo de cilindros e vá para sua tela de informações detalhadas.

   Consulte *Seção 4.5.1 "Como buscar grupos de cilindros", página 66*.

2) Selecione a guia **Membros**.

   Será exibida uma lista com todos os cilindros desse grupo.

4.5.5 Como visualizar eventos de um grupo de cilindros

A guia Eventos é usada para rastrear as operações do administrador no CWM, como alterar o domínio de um grupo de cilindros.

1) Encontre o grupo de cilindros e vá para sua tela de informações detalhadas.

   Consulte *Seção 4.5.1 "Como buscar grupos de cilindros", página 66*.

2) Selecione a guia **Eventos**.

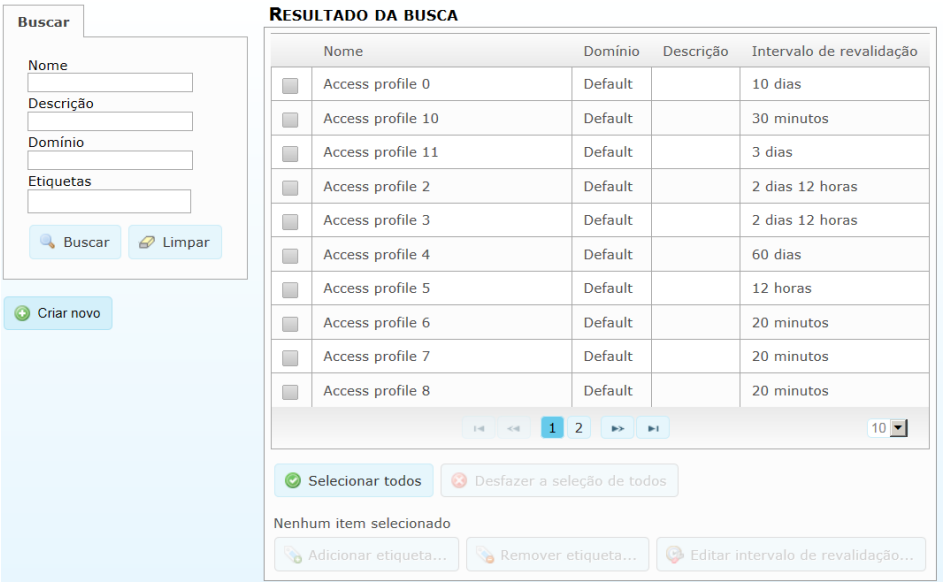
   Será exibida uma lista com todos os eventos do grupo de cilindros.

4.6 Como gerenciar perfis de acesso

4.6.1 Como buscar perfis de acesso

1) Selecione **Informações do sistema » Perfis de acesso**.

   Será exibida uma lista de todos os perfis de acesso.



2) Insira o critério de busca.

   Ao digitar nos campos de busca, o CWM aceita a primeira parte de uma cadeia de caracteres de busca bem como um asterisco (*). Se a busca for para "Laboratório 1", escrever "Lab", "*1" ou "Lab*1" fornecerá resultados incluindo "Laboratório 1".

3) Clique em **Buscar**.

4) Para exibir informações detalhadas de um resultado de busca, clique no perfil de acesso específico.

4.6.2 Como criar e apagar perfis de acesso

Os perfis de acesso se aplicam apenas a chaves dinâmicas que suportam atualizações remotas. Eles podem ser aplicados a uma chave ou a uma pessoa.

1) Selecione **Informações do sistema » Perfis de acesso**.

2) Para criar um perfil de acesso:

   a) Clique em **Criar Novo**.

   b) Insira **Nome** e um **Descrição** opcional.

   > **ATENÇÃO!**
   > O nome do campo deve ser exclusivo.

   c) Para alterar o domínio a partir do padrão:

   - Clique em **Alterar domínio**
   - Clique em **Selecionar** para o domínio específico.

d) Para adicionar uma etiqueta clique em **Adicionar etiqueta**. Consulte também *Seção 4.6.4 "Como adicionar ou excluir etiquetas de perfis de acesso", página 69*

e) Para adicionar um link externo clique em **Adicionar link externo**. Consulte também *Seção 4.6.5 "Como editar links externos de um perfil de acesso", página 70*

f) Clique em **Gravar**.

3) Para apagar um perfil de acesso:

a) Encontre o perfil de acesso e visualize as informações detalhadas.

Consulte *Seção 4.6.1 "Como buscar perfis de acesso", página 68*.

b) Clique em **Excluir**.

c)
- Caso não existam chaves ou pessoas associadas ao perfil:

  Clique em **Excluir perfil**.
- Caso existam chaves ou pessoas associadas ao perfil:

  a) Confirme que os perfis de acesso estão excluídos permanentemente, depois clique na caixa de seleção.

  b) Clique em **Excluir perfil**.

Consulte também *Seção 8.2.4 "Perfis de acesso", página 175*.

4.6.3 Como editar as informações do perfil de acesso

1) Encontre o perfil de acesso e vá para sua tela de informações detalhadas.

Consulte *Seção 4.6.1 "Como buscar perfis de acesso", página 68*.

2) Clique em **Editar**.

3) Atualize os campos.

4) Para adicionar etiquetas clique em **Adicionar Etiqueta...**. Consulte também *Seção 4.1.7 "Como adicionar ou remover uma etiqueta de funcionário ou visitante", página 30*.

5) Para editar links externos clique em **Adicionar link externo...**. Consulte também *Seção 4.1.8 "Como gerenciar links externos de funcionários ou visitantes", página 31*.

6) Clique em **Gravar**.

4.6.4 Como adicionar ou excluir etiquetas de perfis de acesso

1) Encontre o perfil de acesso.

Para buscar o perfil de acesso, consulte *Seção 4.6.1 "Como buscar perfis de acesso", página 68*.

2)
- Para adicionar ou remover etiquetas de um perfil de acesso individual, acesse *Passo 3*.
- Para adicionar ou remover etiquetas de vários perfis de acesso, acesse *Passo 4*.

3) **Adicionar ou remover etiquetas de um perfil de acesso individual:**

1. Selecione o perfil de acesso e vá para sua tela de informações detalhadas.
2. Clique em **Editar**.

3. Adicione ou remova a etiqueta de um perfil de acesso individual.

   Para adicionar uma etiqueta:

   a) Clique em **Adicionar etiqueta...**.
   b) Insira um nome para a etiqueta.
   c) Clique em **OK**.

   Para remover uma etiqueta:
   Clique na etiqueta a ser removida.

4. Clique em **Gravar**.

4) **Adicionar ou remover etiquetas de várias perfis de acesso:**

   1. Selecione os perfis de acesso nos resultados da busca, marcando as caixas de seleção.
   2. **Para adicionar uma etiqueta:**

      a) Clique em **Adicionar etiqueta...**.
      b) Insira o nome da etiqueta.
      c) Clique em **OK**.

      Para remover uma etiqueta:

      a) Clique em **Remover etiqueta...**.
      b) Insira o nome da etiqueta.
      c) Clique em **OK**.

Consulte *Seção 8.2.6 "Etiquetas", página 179* para obter mais informações sobre etiquetas.

4.6.5 Como editar links externos de um perfil de acesso

1) Encontre o perfil de acesso e vá para sua tela de informações detalhadas.

   Consulte *Seção 4.6.1 "Como buscar perfis de acesso", página 68*.

2) Clique em **Editar**.
3) Para adicionar um link externo:

   a) Clique em **Adicionar.**
   b) Insira o **Nome** da URL.
   c) Insira **URL**. A **URL** deve começar com um protocolo (por exemplo http:// ou ftp://).

      Se foi definida uma URL raiz nas **Configurações do sistema**, é suficiente adicionar a última parte da URL. Consulte também *Seção 6.4 "Como editar as configurações do sistema", página 99*.

   d) Clique em **OK**.

4) Para remover um link externo, clique em **Remover** a fim de remover o link externo.
5) Para editar um link externo:

   a) Clique em **Editar** no link externo a ser editado.

b) Atualize os campos.

c) Clique em **OK**.

6) Clique em **Gravar**.

Consulte também *Seção 8.4 "Links externos", página 182*.

4.6.6 Visualização das chaves associadas com um perfil de acesso

A guia **Chaves** exibe todas as chaves associadas ao perfil de acesso selecionado. Também exibe as chaves dos grupos de acesso temporários expirados que estão associados ao perfil de acesso selecionado.

1) Encontre o perfil de acesso e vá para sua tela de informações detalhadas.

   Consulte *Seção 4.6.1 "Como buscar perfis de acesso", página 68*.

2) Selecione a guia **Chaves**.

   Será exibida uma lista com todas as chaves que possuam o perfil de acesso.

4.6.7 Como visualizar eventos do perfil de acesso

A guia Eventos é usada para rastrear as operações do administrador no CWM, como adicionar e remover cilindros em um perfil de acesso.

1) Encontre o perfil de acesso e vá para sua tela de informações detalhadas.

   Consulte *Seção 4.6.1 "Como buscar perfis de acesso", página 68*.

2) Selecione a guia **Eventos**.

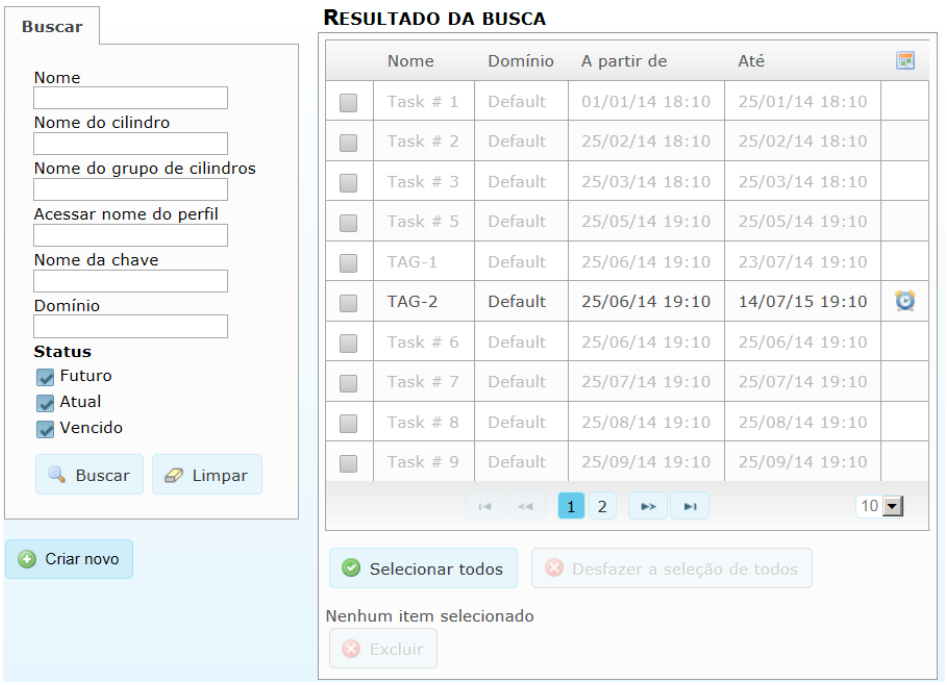
   Será exibida uma lista com todos os eventos do perfil de acesso.

4.7 Como gerenciar grupos de acesso temporário

4.7.1 Como buscar grupos de acesso temporário

1) Selecione **Informações do sistema » Grupos de acesso temporários**.

   Será exibida uma lista de todos os grupos de acesso temporário.



2) Insira o critério de busca.

   Ao digitar nos campos de busca, o CWM aceita a primeira parte de uma cadeia de caracteres de busca bem como um asterisco (*). Se a busca for para "Laboratório 1", escrever "Lab", "*1" ou "Lab*1" fornecerá resultados incluindo "Laboratório 1".

3) Para filtrar a busca:

   a) Marque a caixa **Vencido** para exibir os grupos de acesso temporário que não são mais válidos.

      Na lista de resultados, os grupos de acesso temporário que venceram são formatados com texto em cinza.

   b) Marque a caixa **Atual** para exibir os grupos de acesso temporário que ainda são válidos.

      Na lista de resultados, os grupos de acesso temporário que ainda são válidos são formatados com texto em preto e indicados por um ícone:

   c) Marque a caixa **Futuro** para exibir os grupos de acesso temporário que serão válidos no futuro.

      Na lista de resultados, os grupos de acesso temporário que serão válidos no futuro são formatados com texto em preto.

4) Clique em **Buscar**.

5) Para exibir informações detalhadas de um resultado de busca, clique no grupo de acesso temporário específico.

4.7.2 Como criar e apagar grupos de acesso temporário

Os grupos de acesso temporário se aplicam apenas a chaves dinâmicas que suportam atualizações remotas. Eles são aplicados em uma chave.

1) Selecione **Informações do sistema » Grupos de acesso temporários**.
2) Para criar um grupo de acesso temporário:
   a) Clique em **Criar Novo**.
   b) Insira **Nome**.
   c) Insira os valores de intervalos, datas **A partir de** e **Até**.

> **ATENÇÃO!**
> Quando o grupo de acesso temporário não for mais válido para uma chave, será criada automaticamente uma função para remover o acesso do grupo de acesso temporário da chave. Entretanto, o cancelamento do acesso da chave não será efetivo até que a chave seja atualizada em um programador remoto.

   d) Para alterar o domínio a partir do padrão:
      - Clique em **Alterar domínio**
      - Clique em **Selecionar** para o domínio específico.
   e) Clique em **Gravar**.
3) Para excluir um grupo de acesso temporário:
   a) Encontre o grupo de acesso temporário e visualize as informações detalhadas.

      Consulte *Seção 4.7.1 "Como buscar grupos de acesso temporário", página 71*.
   b) Clique em **Excluir**.
   c) Clique em **OK**.

Também é possível criar um grupo de acesso temporário a partir da tela da chave. Na tela de informações detalhadas, selecione a guia **Grupos de acesso temporários**, clique em **Criar novo** e siga as instruções acima, começando por *Passo 2 b*.

Consulte também *Seção 8.2.5 "Grupos de acesso temporários", página 177*.

4.7.3 Como editar grupos de acesso temporário

1) Encontre o grupo de acesso temporário e vá para sua tela de informações detalhadas.

   Consulte *Seção 4.7.1 "Como buscar grupos de acesso temporário", página 71*.
2) Na tela de informações detalhadas, clique em **Editar**.
3) Atualize os campos.
4) Clique em **Gravar**.

4.7.4 Como adicionar ou remover chaves dos grupos de acesso temporários

ATENÇÃO!
Quando um grupo de acesso temporário não for mais válido para uma chave, será criada automaticamente uma função para remover o acesso do grupo de acesso temporário da chave. Entretanto, o cancelamento do acesso da chave não será efetivo até que a chave seja atualizada em um programador remoto. Para cancelar a possibilidade do proprietário da chave usá-la após o vencimento do grupo de acesso temporário, faça um dos seguintes antes de adicionar chaves:

- Configure **Ativo entre as datas selecionadas** nas configurações de ativação, consulte *Seção 8.1.4 "Validade da chave", página 165*.
- Ative a **Revalidação** da chave, consulte *Seção 8.1.5 "Revalidação de uma chave", página 165*.

Recomendamos combinar os grupos de acesso temporário com a revalidação da chave.

1) Encontre o grupo de acesso temporário e vá para sua tela de informações detalhadas.

   Consulte *Seção 4.7.1 "Como buscar grupos de acesso temporário", página 71*.
2) Selecione a guia **Chaves**.
3) Clique em **Editar**.
4) Para adicionar chaves a um grupo de acesso temporário:
   a) Clique em **Adicionar chaves...**.
   b) Clique em **Selecionar** para as chaves específicas a serem adicionadas. Clique em **Selecionar todos** para adicionar todas as chaves.
   c) Clique em **Finalizado**.
   d) Clique em **Gravar**.

      Será criada uma função remota automaticamente.
5) Para remover chaves de um grupo de acesso temporário:
   a) Clique em **Remover** para as chaves específicas a serem removidas. Clique em **Remover todos** para remover todas as chaves.
   b) Clique em **Gravar**.

4.7.5 Como editar o acesso explícito para grupos de acesso temporário

1) Encontre o grupo de acesso temporário e vá para sua tela de informações detalhadas.

   Consulte *Seção 4.7.1 "Como buscar grupos de acesso temporário", página 71*.
2) Selecione a guia **Acesso explícito**.
3) Clique em **Editar**.
4) Para adicionar ou remover grupos de cilindros:
   a) Em **GRUPOS DE CILINDROS SELECIONADOS**, clique em **Adicionar grupos de cilindros...**.

Serão exibidos todos os grupos de cilindros disponíveis.

b) Para filtrar os grupos de cilindros disponíveis, insira o critério de busca e clique em **Buscar**.

c) Para adicionar grupos de cilindros, clique em **Selecionar** para os cilindros a adicionar ou clique em **Selecionar todos**.

d) Clique em **OK**.

e) Para remover grupos de cilindros, clique em **Remover** para os cilindros a remover ou clique em **Remover todos**.

5) Para adicionar ou remover cilindros:

a) Em **CILINDROS SELECIONADOS**, clique em **Adicionar cilindros...**.

A lista dos resultados de busca exibe os cilindros disponíveis.

> **ATENÇÃO!**
> Só estarão disponíveis cilindros em que a lista de acesso do cilindro inclua a chave selecionada.

b) Para filtrar os cilindros disponíveis, insira o critério de busca e clique em **Buscar**.

c) Para adicionar cilindros, clique em **Selecionar** para os cilindros a adicionar ou clique em **Selecionar todos**.

d) Clique em **OK**.

e) Para remover cilindros, clique em **Remover** para os cilindros a remover ou clique em **Remover todos**.

6) Clique em **Gravar**.

4.7.6 Como visualizar eventos do grupo de acesso temporário

A guia Eventos é usada para rastrear as operações do administrador no CWM, como adicionar e remover chaves em um grupo de acesso temporário.

1) Encontre o grupo de acesso temporário e vá para sua tela de informações detalhadas.

Consulte *Seção 4.7.1 "Como buscar grupos de acesso temporário", página 71*.

2) Selecione a guia **Eventos**.

Será exibida uma lista com todos os eventos do grupo de acesso temporário.

4.7.7 Como remover autorizações de chave redundantes

A remoção de autorizações redundantes é útil ao introduzir perfis de acesso em um Sistema Cliq onde as chaves já estão configuradas com autorizações explícitas. As autorizações explícitas são consideradas redundantes se a chave também está associada a um perfil de acesso que fornece acesso ao mesmo cilindro ou grupo de cilindros.

> **Dica**
> Recomendamos remover as autorizações redundantes para fornecer uma visão geral melhor das autorizações.

1) Busque as chaves.

   Consulte *Seção 4.2.1 "Como buscar chaves de usuário", página 34*.

2) Na lista de resultados de busca, selecione as chaves.

3) Clique em **Remover autorizações redundantes...**.

4) Clique em **OK**.

4.8 Como visualizar autorizações

4.8.1 Como visualizar cilindros acessíveis para chaves ou grupos de chaves

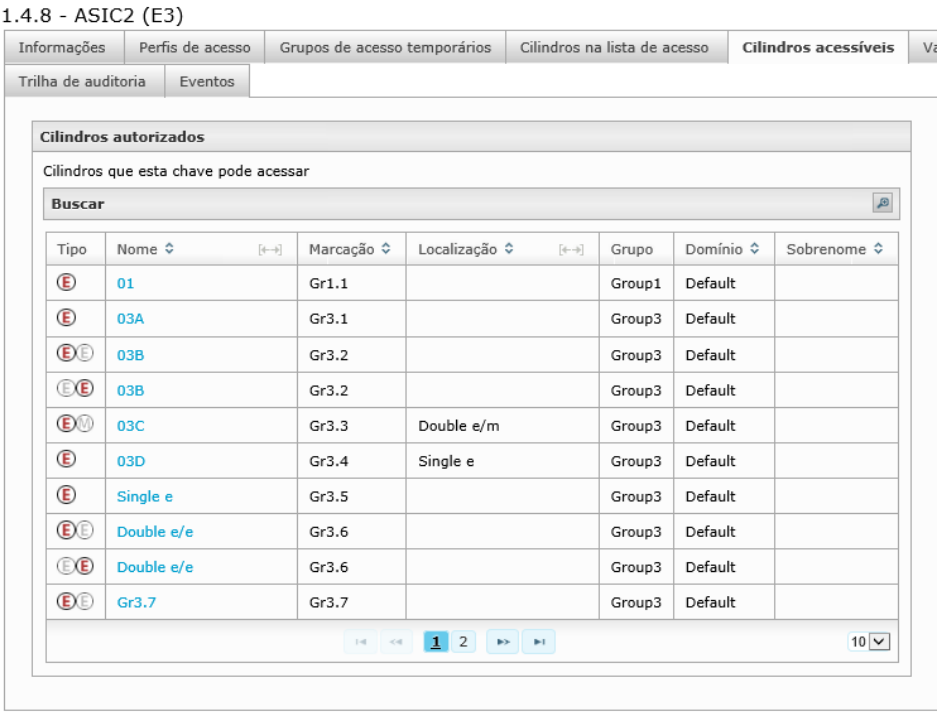
As autorizações reais mostram os cilindros que certa chave pode acessar, considerando tanto a lista de acesso da chave como as listas de acesso do cilindro. Estes são os cilindros que a chave pode abrir.

1) Encontre a chave ou o grupo de chaves e vá para sua tela de informações detalhadas.

   Consulte *Seção 4.3.1 "Como buscar grupos de chaves", página 52*.

2) Selecione a guia **Cilindros acessíveis**.

   Será exibida uma lista de todos os cilindros autorizados para o grupo de chaves.



Para cilindros duplos, o lado A e o lado B são listados separadamente. O símbolo indica a qual lado se refere (o outro lado está acinzentado).

- As informações se relacionam ao lado A
- As informações se relacionam ao lado B

ATENÇÃO!
Chaves específicas poderão ser excluídas do acesso. Consulte *Seção 8.1.2 "Autorização eletrônica", página 163*.

4.8.2 Como visualizar chaves com acesso a cilindros ou grupos de cilindros

Chaves com acesso significa chaves que podem acessar o cilindro considerando tanto as listas de acesso da chave como as listas de acesso do cilindro. Estas são as chaves que podem abrir o cilindro.

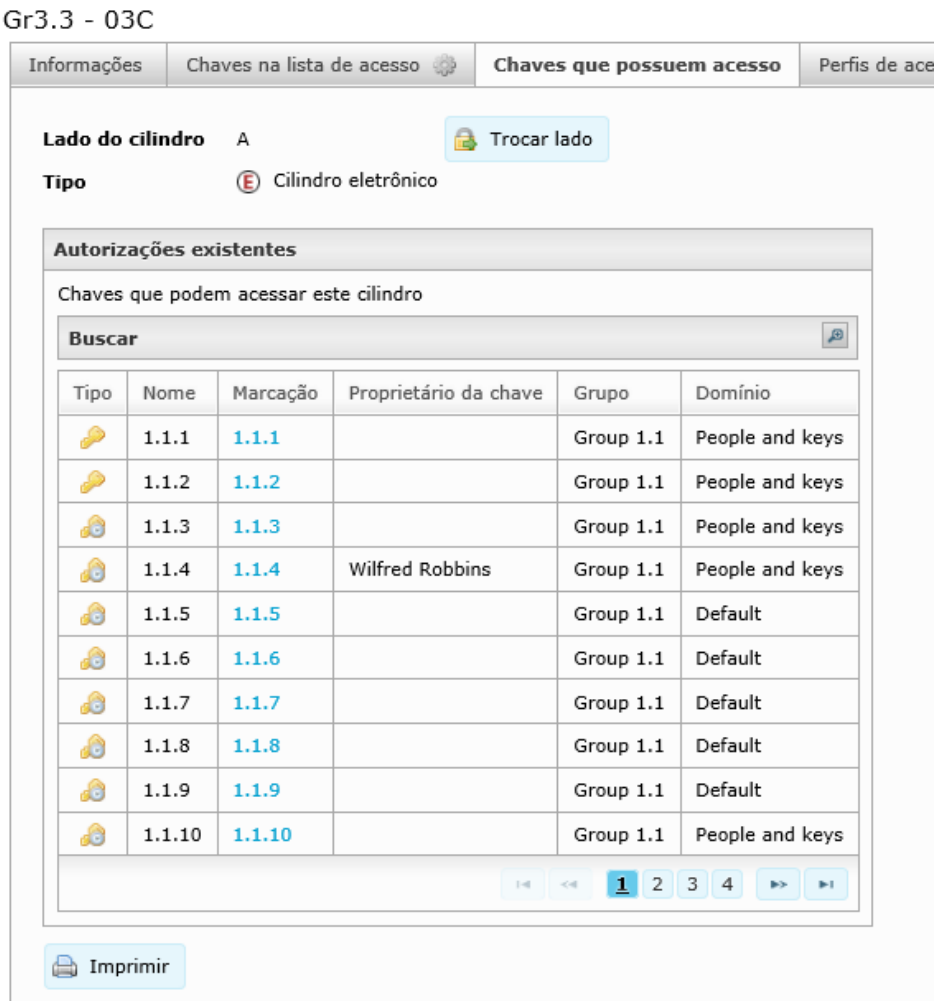
1) Encontre o cilindro ou o grupo de cilindros e vá para sua tela de informações detalhadas.

   - Consulte *Seção 4.4.1 "Como buscar por cilindros", página 54* para buscar um cilindro.
   - Consulte *Seção 4.5.1 "Como buscar grupos de cilindros", página 66* para buscar um grupo de cilindros.

2) Selecione a guia **Chaves que possuem acesso**.

   Será exibida uma lista de chaves com acesso ao cilindro ou ao grupo de cilindros.

   As chaves que pertencem aos grupos de chaves autorizadas são exibidas individualmente.



4.8.3 Como visualizar perfis de acesso que dão acesso a um cilindro ou grupo de cilindros

As chaves associadas com um perfil de acesso têm, automaticamente, acesso aos cilindros e grupos de cilindros especificados por esse perfil de acesso. Note que isto não significa necessariamente que a chave pode abrir o cilindro, pois o acesso depende também da lista de acesso do cilindro.

1) Encontre o cilindro ou o grupo de cilindros e vá para sua tela de informações detalhadas.
   - Consulte *Seção 4.4.1 "Como buscar por cilindros", página 54* para buscar um cilindro.
   - Consulte *Seção 4.5.1 "Como buscar grupos de cilindros", página 66* para buscar um grupo de cilindros.
2) Selecione a guia **Perfis de acesso que fornecem acesso**.

Consulte também *Seção 4.9.4 "Como configurar autorizações de perfil de acesso", página 82*.

4.9 Como configurar autorizações

4.9.1 Como configurar autorizações em chaves

As chaves dinâmicas possuem uma lista de acesso que inclui os cilindros e grupos de cilindros que a chave está autorizada a abrir. Configurar autorizações em chaves significa editar as autorizações explícitas nessa lista de acesso. A lista de acesso também pode conter autorizações implícitas que se originam dos perfis de acesso. Consulte *Seção 4.9.4 "Como configurar autorizações de perfil de acesso", página 82* para configurar as autorizações do perfil de acesso.

Note que um cilindro incluído na lista de acesso da chave não significa necessariamente que a chave tem acesso, pois o acesso depende também da lista de acesso do cilindro. Consulte *Seção 4.8.1 "Como visualizar cilindros acessíveis para chaves ou grupos de chaves", página 76* para visualizar os cilindros que a chave pode abrir.

Para remover todos os acessos a um cilindro, veja *Seção 4.9.3 "Como remover todos os acessos a um cilindro", página 82*.

Consulte *Seção 8.1 "Princípios de autorização", página 163* para obter mais informações sobre os princípios das autorizações.

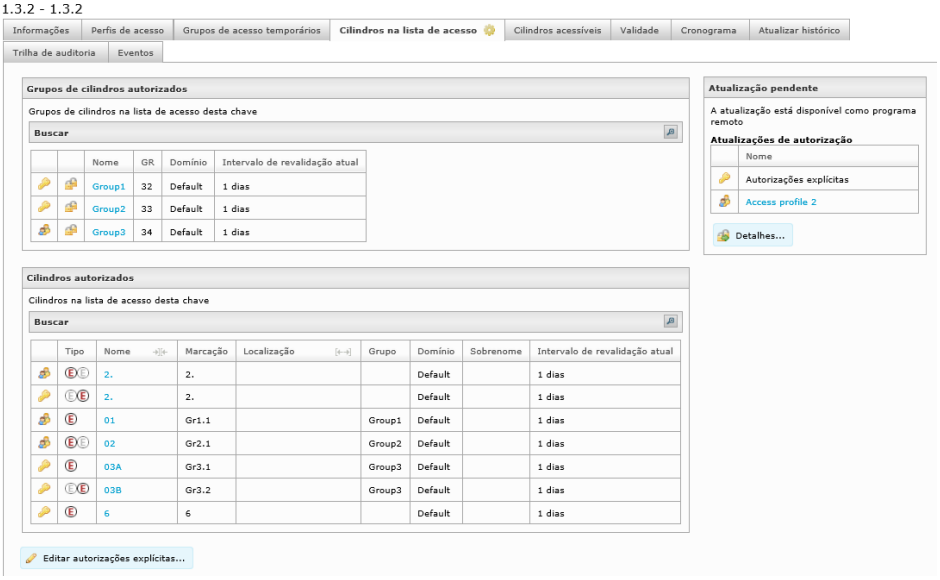
1) Encontre a chave e vá para sua tela de informações detalhadas.

   Consulte *Seção 4.2.1 "Como buscar chaves de usuário", página 34* para buscar a chave e exibir a tela informações detalhadas.

   Para escanear a chave no Programador local e exibir as informações detalhadas, consulte *Seção 4.2.2 "Como escanear uma chave de usuário", página 35*
2) Selecione a guia **Cilindros na lista de acesso**.

   São exibidos os grupos de cilindros e os cilindros autorizados no momento.

1.3.2 - 1.3.2



A lista de acesso contém autorizações explícitas.

 Autorização explícita

 Autorização do perfil de acesso

Para cilindros duplos, o lado A e o lado B são listados separadamente. O símbolo indica a qual lado se refere (o outro lado está acinzentado).

 As informações se relacionam ao lado A

 As informações se relacionam ao lado B

As atualizações remotas pendentes são listadas em **Atualização pendente**.

3) Clique em **Editar autorizações explícitas...**.

Serão exibidas as autorizações explícitas para a chave.

Dica

A remoção de grupos de cilindros e cilindros pode ser feita diretamente nesta tela clicando em **Remover** para o grupo de cilindros ou cilindros a remover.

Ao remover de chaves com listas de acesso longas, pode ser conveniente filtrar primeiro os grupos de cilindros e os cilindros.

4) Para adicionar ou remover grupos de cilindros:

a) Em **Autorizações de grupo de cilindros explícitas**, clique em **Alterar grupos de cilindros...**.

Serão exibidos todos os grupos de cilindros disponíveis.

b) Para filtrar os grupos de cilindros disponíveis, insira o critério de busca e clique em **Buscar**.

c) Clique em **Selecionar** para os grupos de cilindros a adicionar ou clique em **Selecionar todos**.

d) Clique em **Remover** para os grupos de cilindros a remover ou clique em **Remover todos**.

e) Clique em **OK**.

5) Para adicionar ou remover cilindros individuais:

a) Em **Autorizações de cilindro explícitas**, clique em **Alterar cilindros...**.

A lista dos resultados de busca exibe os cilindros disponíveis.

> **ATENÇÃO!**
> Só estarão disponíveis cilindros em que a lista de acesso do cilindro inclua a chave selecionada.

b) Para filtrar os cilindros disponíveis, insira o critério de busca e clique em **Buscar**.

c) Clique em **Selecionar** para os cilindros a adicionar ou clique em **Selecionar todos**.

d) Clique em **Remover** para os cilindros a remover ou clique em **Remover todos**.

e) Clique em **OK**.

6) Clique em **Gravar**.

O progresso é mostrado em uma janela pop-up com a duração estimada da operação.

7) Se a chave for escaneada, clique em **Gravar lista de acesso na chave localmente** para atualizar a chave.

> **ATENÇÃO!**
> Caso a revalidação esteja ativada para a chave, ela será revalidada no Programador local durante o processo de programação.

Caso contrário, será criada uma função de atualização da chave.

4.9.2 Como configurar autorizações em cilindros

Uma lista de acesso do cilindro é armazenada nos cilindros e inclui as chaves e grupos de chaves que estão autorizadas a abrir o cilindro. Configurar autorizações em cilindros significa editar essa lista de acesso.

Para chaves de usuário, o fato de uma chave estar incluída na lista de acesso do cilindro não significa necessariamente que a chave tem acesso, pois o acesso depende também da lista de acesso da chave. Consulte *Seção 4.8.2 "Como visualizar chaves com acesso a cilindros ou grupos de cilindros", página 77* para visualizar as chaves que podem abrir o cilindro.

Consulte *Seção 8.1 "Princípios de autorização", página 163* para obter mais informações sobre os princípios das autorizações.

1) Encontre o cilindro e vá para sua tela de informações detalhadas.

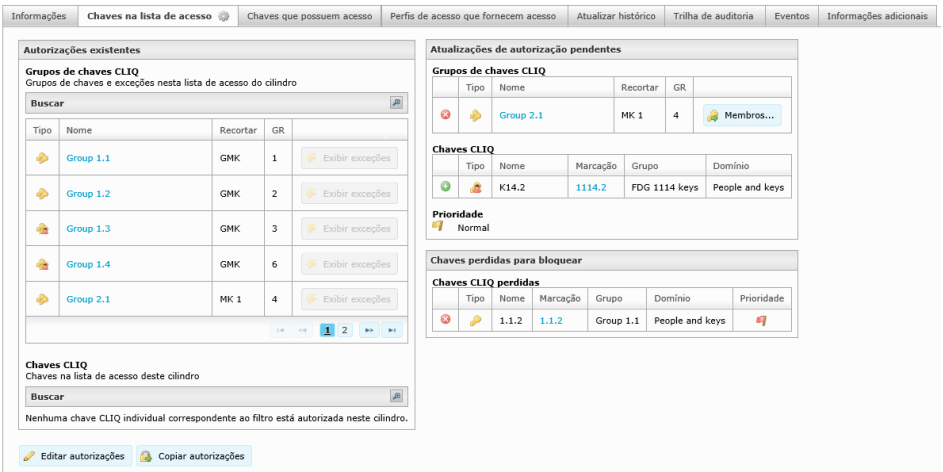
Consulte *Seção 4.4.1 "Como buscar por cilindros", página 54*.

2) Selecione a guia **Chaves na lista de acesso**.

Serão exibidas as chaves e grupos de chaves autorizadas.

Qualquer Função de programação de cilindro com atualizações de autorização é listada em **Atualizações de autorização pendentes**.

Qualquer Função de programação de cilindro devido à perda de chaves é listada em **Chaves perdidas para bloquear**.



3) Para visualizar chaves que pertencem a um grupo de chave autorizada mas que não tem acesso, clique em **Exibir exceções**.

4) Clique em **Editar autorizações**.

5) **Para adicionar grupos de chaves ou chaves individuais**

1. Clique em **Adicionar grupo de chaves CLIQ**.

   A lista dos resultados de busca exibe todos os grupos de chaves disponíveis.

2. Para filtrar os grupos de chaves disponíveis, insira o critério de busca e clique em **Buscar**.

3. Clique em **Selecionar** nos grupos de chaves a serem adicionados.

> **ATENÇÃO!**
> Quando um grupo de chaves é adicionado a uma lista de acesso, quaisquer entradas individuais de chaves desse grupo de chaves (agora redundantes) são removidas automaticamente. Isso significa que, se o grupo de chaves for adicionado e depois removido, todas as chaves do grupo perderão seu acesso, incluindo as chaves que tinham acesso individual anteriormente.

4. Clique em **Finalizado**.

Para excluir chaves de uma autorização de grupo de chaves

1. Clique em **Editar** no grupo de chaves.
2. Clique em **Desautorizar** nas chaves a serem excluídas do acesso.

Para reautorizar chaves de uma autorização de grupo de chaves

> **ATENÇÃO!**
> Para reautorizar a chave, ela precisa ser comunicada como encontrada.
>
> Clique em **Comunicar como encontrado** na visualização de informações detalhadas da chave.

1. Clique em **Editar...** no grupo de chaves.

2. Clique em **Autorizar** para que as chaves autorizem o acesso ao cilindro.

Para remover grupos de chaves ou chaves individuais
Clique em Remover para o grupo de chaves a ser removido.

6) Quando a edição estiver concluída, clique em **Para visualização**.

Será criada uma função de programação de cilindro.

Consulte *Seção 4.4.13 "Como programar os cilindros", página 61* para programar cilindros.

Podem ser editadas autorizações para vários cilindros ao mesmo tempo. Selecione os cilindros na lista do resultado de busca (consulte *Seção 4.4.1 "Como buscar por cilindros", página 54*) e clique em **Adicionar autorizações** ou **Revogar autorizações**.

4.9.3 Como remover todos os acessos a um cilindro

Os cilindros individuais podem ser removidos de todas as chaves, perfis de acesso e grupos de acesso temporário.

A possibilidade de remover todos os acessos de um cilindro exige um Sistema Cliq com chaves dinâmicas.

1) Encontre o cilindro e vá para sua tela de informações detalhadas.

Consulte *Seção 4.4.1 "Como buscar por cilindros", página 54*.

2) Selecione **Remova as autorizações do lado da chave**.

ATENÇÃO!
Para remover o acesso, todas as chaves que tinham acesso ao cilindro devem ser atualizadas.

ATENÇÃO!
Remova as autorizações do lado da chave remove somente o cilindro da lista de acesso nas chaves que suportam atualizações remotas.

Selecione a guia **Chaves que possuem acesso** para verificar se não existem chaves não remotas com acesso ao cilindro. Para cada uma dessas chaves, coloque a chave no programador local, escaneie a chave, selecione a guia **Cilindros na lista de acesso**, clique em **Editar autorizações explícitas** e remova o cilindro.

Consulte *Seção 8.3.1 "Visão geral do recurso remoto", página 179* para obter informações sobre recursos remotos.

3) Na janela pop-up, clique em **OK**.

4.9.4 Como configurar autorizações de perfil de acesso

Configurar autorizações de perfil de acesso significa editar as autorizações implícitas para chaves e pessoas associadas com o perfil de acesso.

1) Encontre o perfil de acesso e vá para sua tela de informações detalhadas.

Consulte *Seção 4.6.1 "Como buscar perfis de acesso", página 68*.

2) Selecione a guia **Lista de acesso**.

Serão exibidos os cilindros e grupos de cilindros autorizados.

3) Clique em **Editar**.

Para cilindros duplos, o lado A e o lado B são listados separadamente. O símbolo indica a qual lado se refere (o outro lado está acinzentado).

As informações se relacionam ao lado A

As informações se relacionam ao lado B

4) **Como adicionar cilindros ou grupos de cilindros**

1. Clique em **Adicionar cilindros...** ou **Adicionar grupos de cilindros...**.

   A janela pop-up mostra a lista de cilindros ou grupos de cilindros disponíveis.
2. Para filtrar o resultado, insira o critério de busca e clique em **Buscar**.
3. Clique em **Selecionar** para os itens a adicionar ou clique em **Selecionar todos**.
4. Clique em **OK**.

Como remover cilindros ou grupos de cilindros

1. Clique ni ícone de busca e insira os critérios de busca.
2. Clique em **Buscar**.

   A tabela mostra o resultado da busca.
3. – Como remover itens específicos:

     Clique em **Remover**.
   – Como remover todos os itens do resultado da busca:

     Clique em **Remover todos os listados**.

5) A Revalidação flexível também pode ser editada nesta tela. Consulte *Seção 4.10.2 "Como configurar a revalidação flexível", página 88*.

6) Clique em **Gravar** para sair do modo de edição.

Consulte também *Seção 8.2.4 "Perfis de acesso", página 175*.

4.9.5 Como selecionar perfis de acesso para funcionários ou visitantes

Os perfis de acesso só se aplicam a chaves dinâmicas, os outros tipos de chaves não serão incluídos.

1) Encontre o funcionário ou visitante e vá para sua tela de informações detalhadas.

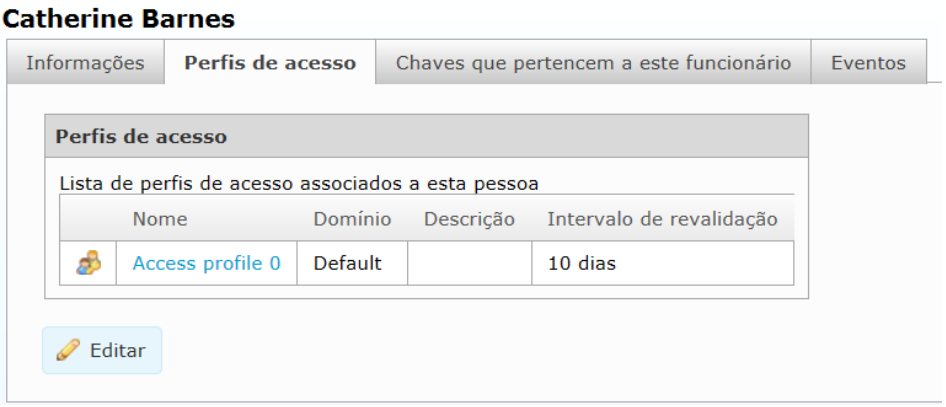
   Consulte *Seção 4.1.1 "Como procurar funcionários ou visitantes", página 23*.

2) Selecione a guia **Perfis de acesso**.

   A lista de resultados de busca exibe os perfis de acesso associados atualmente com o funcionário ou visitante.

3) Clique em **Editar**.

   Será exibida uma lista dos perfis de acesso associados.



4) Para adicionar perfis de acesso:

   a) Clique em **Adicionar perfis de acesso**.

      A lista dos resultados de busca exibe os Perfis de acesso disponíveis.

   b) Para filtrar os perfis de acesso disponíveis, insira **Nome**, **Descrição**, **Domínio** e ou **Etiquetas** no campo de busca.

   c) Clique em **Selecionar** para selecionar um perfil de acesso ou clique em **Selecionar todos**.

   d) Clique em **Finalizado**.

5) Para remover perfis de acesso, clique em **Remover** para remover um perfil de acesso ou clique em **Remover todos**.

6) Clique em **Gravar**.

Os perfis de acesso para vários funcionários ou visitantes podem ser adicionados ou removidos simultaneamente. Selecione os funcionários ou visitantes na lista do resultado de busca e clique em **Adicionar perfis de acesso** ou **Remover perfis de acesso**.

Consulte também *Seção 8.2.4 "Perfis de acesso", página 175*.

4.9.6 Como selecionar perfis de acesso para chaves

Os perfis de acesso se aplicam apenas a chaves dinâmicas.

1) Encontre a chave e vá para sua tela de informações detalhadas.

   Consulte *Seção 4.2.1 "Como buscar chaves de usuário", página 34* para buscar a chave e exibir a tela informações detalhadas.

Para escanear a chave no Programador local e exibir as informações detalhadas, consulte *Seção 4.2.2 "Como escanear uma chave de usuário", página 35*

2) Selecione a guia **Perfis de acesso**.

   A lista de resultados de busca exibe os perfis de acesso associados atualmente com a chave.

3) Clique em **Editar**.

4) Para adicionar perfis de acesso:

   a) Clique em **Adicionar perfis de acesso**.

      A lista dos resultados de busca exibe os Perfis de acesso disponíveis.

   b) Para filtrar os perfis de acesso disponíveis, insira o critério de busca e clique em **Buscar**.

   c) Clique em **Selecionar** para selecionar um perfil de acesso ou clique em **Selecionar todos**.

   d) Clique em **Finalizado**.

5) Para remover perfis de acesso, clique em **Remover** para remover um perfil de acesso ou clique em **Remover todos**.

6) Clique em **Gravar**.

Podem ser editados perfis de acesso para várias chaves ao mesmo tempo. Selecione as chaves na lista do resultado de busca e clique em **Adicionar perfis de acesso** ou **Remover perfis de acesso**.

Consulte também *Seção 8.2.4 "Perfis de acesso", página 175*.

4.9.7 Seleção de perfis de acesso de grupos de acesso temporários

1) Encontre o grupo de acesso temporário e vá para sua tela de informações detalhadas.

   Consulte *Seção 4.7.1 "Como buscar grupos de acesso temporário", página 71*.

2) Selecione a guia **Perfis de acesso**.

3) Clique em **Editar**.

4) Para adicionar perfis de acesso a um grupo de acesso temporário:

   a) Clique em **Adicionar perfis de acesso...**.

   b) Clique em **Selecionar** para os perfis de acesso específicos a serem adicionados. Clique em **Selecionar todos** para adicionar todos os perfis de acesso.

   c) Clique em **Finalizado**.

   d) Clique em **Gravar**.

5) Para remover perfis de acesso de um grupo de acesso temporário:

   a) Clique em **Remover** para os perfis de acesso específicos a serem removidos. Clique em **Remover todos** para remover todos os perfis de acesso.

   b) Clique em **Gravar**.

4.10 Como configurar a validade e o cronograma de uma chave

4.10.1 Como configurar a validade de chave, a revalidação e a validação do PIN

1) Encontre a chave e vá para sua tela de informações detalhadas.

   Consulte *Seção 4.2.1 "Como buscar chaves de usuário", página 34* para buscar a chave e exibir a tela informações detalhadas.

   Para escanear a chave no Programador local e exibir as informações detalhadas, consulte *Seção 4.2.2 "Como escanear uma chave de usuário", página 35*

2) Selecione a guia **Validade**.

   A guia Validade exibe:

   - Configurações de validade: Se a chave está sempre ativa, se está sempre inativa ou as datas entre as quais a chave está ativa.
   - Se for usada revalidação:
     - **Intervalo de revalidação**: o período em que a chave permanece ativa após revalidação, antes que tenha que ser revalidada novamente.
     - **Próximo vencimento**: data e hora em que a chave se torna inativa caso não seja revalidada.

       Ao ativar a revalidação remotamente em uma chave que está **Sempre ativo**, será exibido **A chave sempre poderá ser revalidada**, o próximo vencimento será **Nunca** até que a chave seja revalidada pela primeira vez.

       Ao ativar a revalidação remotamente em uma chave que está **Ativo entre as datas**, isto será igual a **Chave ativa até** até que a chave seja revalidada pela primeira vez.
   - Caso seja usada a validação do PIN:
     - **Intervalo de validação do PIN**: o intervalo de tempo durante o qual a chave permanece ativa após uma validação do PIN, antes que o código PIN necessite ser inserido novamente.
   - Configurações de horário de verão

3) Clique em **Editar validade**.

4) Selecione se a chave será **Inativo**, **Ativo entre as datas selecionadas** ou **Sempre ativo**.

5) Se for selecionado **Ativo entre as datas selecionadas**, insira **Chave ativa a partir de** e **Chave ativa até**.

6) Para configurar a revalidação:

a) Selecione **Usar a revalidação da chave**.

b) Insira o número de dias, horas e minutos para **Intervalo de revalidação**.

Este é o tempo em que a chave permanece ativa após a revalidação em um Programador remoto.

c) Para permitir a revalidação apenas uma vez, selecione **Atualização única**.

7) Como configurar a validação do PIN:

a) Selecione **Use a validação do PIN**.

b) Insira o número de dias, horas e minutos para **Intervalo de validação do PIN**.

Esse é o intervalo de tempo durante o qual a chave permanece ativa após uma validação com o PIN.

O intervalo especificado precisa estar entre um minuto e 45 dias.

c) É gerado automaticamente um código PIN aleatório para **PIN inicial novo**. Também é possível substituir o PIN gerado e inserir manualmente um PIN inicial novo.

Selecione **Exibir valor** para tornar o código PIN visível.

Será enviado um e-mail com o código PIN inicial caso o proprietário da chave possua um endereço de e-mail registrado. Esse código PIN deve ser alterado pelo usuário no primeiro uso.

8) Para confirmar as atualizações:

a) Se a chave for escaneada, clique em **Gravar na chave**.

A chave é atualizada com as configurações novas.

b) Se a chave não for escaneada, clique em **Enviar atualização remota**.

Será criada uma função de atualização remota.

A validade, a revalidação e a validação do PIN podem ser editadas simultaneamente para várias chaves. Selecione as chaves na lista de resultados de busca, clique em **Alterar configurações de validade...** e siga as instruções.

Consulte também *Seção 8.1.4 "Validade da chave", página 165*, *Seção 8.1.5 "Revalidação de uma chave", página 165* e *Seção 8.1.7 "Validação do PIN", página 169*.

4.10.2 Como configurar a revalidação flexível

CUIDADO!
Como a Revalidação flexível é um recurso avançado e complexo, recomendamos ler *Seção 8.1.6 "Revalidação flexível", página 168* com atenção antes de configurá-la.

Pré-requisitos:

- Pelo menos uma chave de usuário possui um firmware com suporte para a Revalidação flexível (consulte *Seção 9.7 "Função dependente do firmware", página 209*).
- O recurso é ativado nas **Configurações do sistema** (consulte *Seção 6.4 "Como editar as configurações do sistema", página 99*).

ATENÇÃO!
Ao usar a Revalidação flexível, todas as chaves que são afetadas pelas configurações de revalidação nos perfis de acesso ou nos grupos de cilindros devem ter a revalidação ativa.

1) Para configurar o intervalo de revalidação em um perfil de acesso:
   a) Encontre o perfil de acesso e vá para sua tela de informações detalhadas.
      Consulte *Seção 4.6.1 "Como buscar perfis de acesso", página 68*.
   b) Clique em **Editar**.
   c) Selecione a opção para **Revalidação**.
      - Para especificar um intervalo de revalidação, selecione **Usar intervalo específico**.
      - Para deixar o intervalo de revalidação não especificado, selecione **Usar intervalo de revalidação dos grupos de cilindros**.
        O intervalo de revalidação configurado nos grupos de cilindros é usado para os grupos de cilindros em que foi especificado um intervalo. Caso contrário, é usado o intervalo de revalidação configurado na chave.
   d) Se foi selecionado **Usar intervalo específico**, insira o intervalo como número de dias, horas e minutos.
   e) Clique em **Gravar**.
   f) O intervalo de revalidação pode ser editado simultaneamente para vários perfis de acesso. Selecione os perfis de acesso na lista do resultado de busca e clique em **Editar intervalo de revalidação**.
2) Para configurar o intervalo de revalidação em um grupo de cilindros:
   a) Encontre o grupo de cilindros e vá para sua tela de informações detalhadas.
      Consulte *Seção 4.5.1 "Como buscar grupos de cilindros", página 66*.
   b) Clique em **Editar**.
   c) Selecione a opção para **Revalidação**.

- Para especificar um intervalo de revalidação, selecione **Usar intervalo específico**.
- Para deixar o intervalo de revalidação não especificado, selecione **Use o intervalo de revalidação das chaves**.

  É usado o intervalo de revalidação configurado na chave.

d) Se foi selecionado **Usar intervalo específico**, insira o intervalo como número de dias, horas e minutos.

e) Clique em **Gravar**.

f) O intervalo de revalidação pode ser editado simultaneamente para vários grupos de cilindros. Selecione os grupos cilindros na lista do resultado de busca e clique em **Editar intervalo de revalidação**.

3) Para verificar se os intervalos de revalidação para uma chave estão configurados corretamente, visualize a coluna **Intervalo de revalidação atual** para cada cilindro na Lista de acesso da chave. Consulte *Seção 4.9.1 "Como configurar autorizações em chaves", página 78*.

Consulte também *Seção 8.1.6 "Revalidação flexível", página 168*.

4.10.3 Como configurar o cronograma de uma chave

Existem dois tipos de cronogramas, o Cronograma básico e o Cronograma de janelas de tempo múltiplas (consulte *Seção 8.1.8 "Cronogramas de chaves", página 170*). O firmware da chave determina qual tipo é usado. Para obter informações sobre qual versão de firmware de chave suporta qual tipo de cronograma, consulte *Seção 9.7 "Função dependente do firmware", página 209*

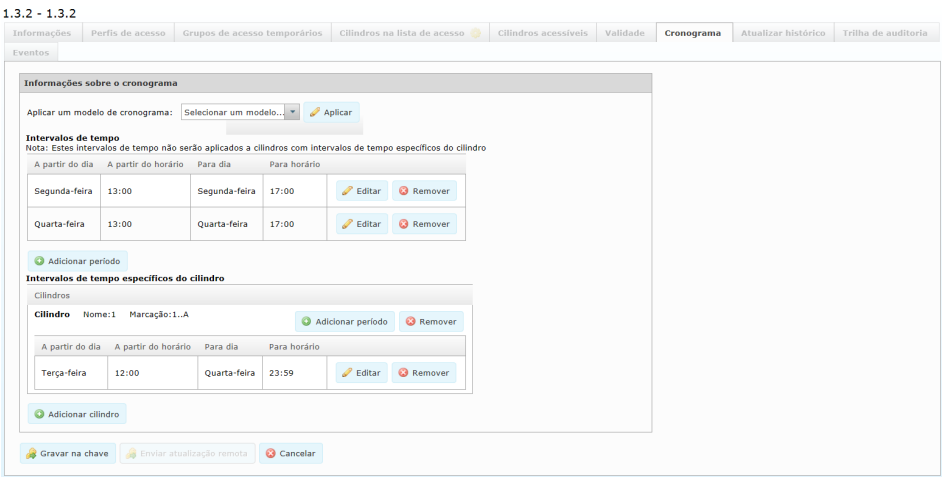
1) Encontre a chave e vá para sua tela de informações detalhadas.

   Consulte *Seção 4.2.1 "Como buscar chaves de usuário", página 34* para buscar a chave e exibir a tela informações detalhadas.

   Para escanear a chave no Programador local e exibir as informações detalhadas, consulte *Seção 4.2.2 "Como escanear uma chave de usuário", página 35*

2) Selecione a guia **Cronograma**.

3) Clique em **Editar cronograma**.



4) Para aplicar um modelo de cronograma, selecione um modelo no menu suspenso e clique em **Aplicar**.

   O modelo será aplicado, porém o cronograma ainda poderá ser editado.

5) Determine se a chave possui um Cronograma básico ou um Cronograma de várias janelas de tempo.

   Se a chave possui um cronograma de Janelas de tempo múltiplas, além de **Intervalos de tempo** são exibidos também **Intervalos de tempo específicos do cilindro**.

6) Para editar um Cronograma básico:

   a) Clique em **Editar** na linha do dia a editar.

   b) Selecione **O dia inteiro**, **Nunca** ou **Personalizar**.

   c) Se for selecionada a opção personalizar, insira os valores dos intervalos **A partir do horário** e **Para horário**.

   d) Clique em **Gravar**.

7) Para editar um Cronograma de janelas de tempo múltiplas:

   a) Para adicionar um intervalo:

      - Clique em **Adicionar período**.
      - Insira os valores dos intervalos **A partir da data** e **Até a data**.
      - Clique em **Gravar**.

   b) Para editar um intervalo, clique em **Editar intervalo**.

   c) Para remover um intervalo, clique em **Remover intervalo**.

   d) Para adicionar um intervalo para um cilindro específico:

      - Clique em **Adicionar cilindro**.

        A lista dos resultados de busca exibe todos os cilindros disponíveis.
      - Para filtrar os cilindros disponíveis, insira o critério de busca e clique em **Buscar**.
      - Clique em **Selecionar** no cilindro a ser adicionado.
      - Adicione, edite e remova intervalos para o cilindro.

ATENÇÃO!

Para chaves geração 1:

- Para cilindros incluídos individualmente na lista de acesso da chave (não como parte de um grupo de cilindros), especificar um ou mais períodos de tempo para um cilindro significa que o cronograma geral é ignorado para aquele cilindro.
- Para cilindros incluídos na lista de acesso da chave como parte de um grupo de cilindros, os períodos de tempo do cilindro são ignorados.

Para chaves geração 2:

- Especificar um ou mais períodos de tempo para um cilindro significa que o cronograma geral é ignorado para aquele cilindro.

8) Para confirmar as atualizações:
   a) Se a chave for escaneada, clique em **Gravar na chave**.

      A chave é atualizada com as configurações novas. Caso a revalidação esteja ativada para a chave, ela será revalidada ao mesmo tempo.
   b) Se a chave não for escaneada, clique em **Enviar atualização remota**.

      Será criada uma função de atualização da chave.

4.10.4 Como configurar o cronograma de um grupo de chaves

O cronograma pode ser configurado para todas as chaves em um grupo de chaves.

1) Encontre o grupo de chaves e vá para sua tela de informações detalhadas.

   Consulte *Seção 4.3.1 "Como buscar grupos de chaves", página 52*.
2) Clique em **Configuração de chave em massa**.
3) Selecione **Configurar cronograma**.
4) Clique em **Próximo**.
5) Insira as configurações de cronograma. Consulte *Seção 4.10.3 "Como configurar o cronograma de uma chave", página 89* para referência.
6) Clique em **Próximo**.

   Serão exibidas as configurações selecionadas.
7) Para confirmar as atualizações, clique em **Aplicar**.

   Serão criadas funções de atualização de chave.

4.11 Como administrar as trilhas de auditoria

Chaves quartz e dinâmicas e cilindros possuem um recurso de trilha de auditoria.

Uma trilha de auditoria é uma lista de eventos e mostra tentativas de acesso, o proprietário da chave no momento e os registro de programação do dispositivo. Consulte *Seção 8.6 "Trilhas de auditoria", página 185* para obter mais informações.

4.11.1 Como visualizar trilhas de auditoria de uma chave de usuário

1) Encontre a chave e vá para sua tela de informações detalhadas.

   Consulte *Seção 4.2.1 "Como buscar chaves de usuário", página 34* para buscar a chave e exibir a tela informações detalhadas.

   Para escanear a chave no Programador local e exibir as informações detalhadas, consulte *Seção 4.2.2 "Como escanear uma chave de usuário", página 35*

2) Selecione a guia **Trilha de auditoria**.

   Se qualquer trilha de auditoria tiver sido solicitada e lida por um Programador remoto, será exibida uma lista de eventos da trilha de auditoria.

3) Se o recurso **Aprovações** estiver ativado (consulte *Seção 6.4 "Como editar as configurações do sistema", página 99*):

   a) Para solicitar uma nova trilha de auditoria, clique em **Solicitar trilha de auditoria remota**.

   b) Insira um comentário para o aprovador e clique em **Enviar solicitação**.

4) Se o recurso **Aprovações** estiver desativado (consulte *Seção 6.4 "Como editar as configurações do sistema", página 99*):

   - Se a chave está no programador local, clique em **Ler trilha de auditoria**. Isto pode levar algum tempo.
   - Se a chave não está no programador local, clique em **Solicitar trilha de auditoria remota**.

     A trilha de auditoria será lida da próxima vez que a chave for inserida em um Programador remoto e gravada no CWM. Então ela será exibida na guia trilha de auditoria.

     ATENÇÃO!
     Solicitar trilha de auditoria remota é ligado automaticamente na entrega da chave e desligado na devolução da mesma.

5) Opcional: Exporte a tabela como PDF. Consulte *Seção 4.11.5 "Como exportar informações da trilha de auditoria", página 93*.

Consulte também *Seção 8.6 "Trilhas de auditoria", página 185*.

4.11.2 Como visualizar trilhas de auditoria de cilindro

ATENÇÃO!
As trilhas de auditoria que registram a tentativa de acesso por Chaves normais não exibem data e hora na coluna **Horário na chave**.

1) Encontre o cilindro e vá para sua tela de informações detalhadas.

   Consulte *Seção 4.4.1 "Como buscar por cilindros", página 54*.

2) Selecione a guia **Trilha de auditoria**.

   Se as trilhas de auditoria já tiverem sido coletadas, elas são exibidas como uma lista.

3) Para solicitar uma nova trilha de auditoria, clique em **Solicitar trilha de auditoria**.

Caso esteja ativado **Aprovações** (consulte *Seção 6.4 "Como editar as configurações do sistema", página 99*), insira um comentário para o aprovador.

4) Selecione **Prioridade**.

   As funções urgentes deverão ter uma prioridade mais alta.

5) Clique em **OK**.

   Será criada uma função de programação para coletar uma trilha de auditoria do cilindro.

   Consulte *Seção 4.4.13 "Como programar os cilindros", página 61* para obter a trilha de auditoria do cilindro.

6) Opcional: Exporte a tabela como PDF. Consulte *Seção 4.11.5 "Como exportar informações da trilha de auditoria", página 93*.

Consulte também *Seção 8.6 "Trilhas de auditoria", página 185*.

4.11.3 Como visualizar o arquivo da trilha de auditoria

O arquivo da trilha de auditoria contém todas as trilhas de auditoria coletadas das chaves e cilindros do Sistema Cliq. Selecionando uma chave ou cilindro, é possível visualizar todas as trilhas de auditoria coletadas para aquela chave ou cilindro.

Não existem restrições quanto à quantidade de trilhas de auditoria que caberão no arquivo da trilha de auditoria. O arquivo pode ser configurado para remover automaticamente trilhas de auditoria mais antigas que um número de dias definido, consulte *Seção 6.4 "Como editar as configurações do sistema", página 99*.

1) Selecione **Informações do sistema » Arquivo de trilha de auditoria**.

   Uma lista dos eventos da trilha de auditoria mostra interações entre chaves, cilindros, chaves de comando, programadores remotos e/ou o software.

   ATENÇÃO!
   Devido à grande escala dos dados da trilha de auditoria, algumas informações estendidas como proprietários de chaves históricos ou domínios históricos estarão disponíveis com atraso. Enquanto essas informações são processadas em segundo plano, será exibido **Dados de processamento** na lista.

2) Especifique o critério de busca e clique em **Buscar**.

   Por exemplo, para visualizar todas as interações da chave com um cilindro específico.

   Selecione **Chave** em **Obtido de**, depois selecione **Cilindro** especificando **Nome** ou **Marcação** do cilindro específico em **Evento por**.

3) Opcional: Exporte a tabela como PDF. Consulte *Seção 4.11.5 "Como exportar informações da trilha de auditoria", página 93*.

4.11.4 Como exportar informações da trilha de auditoria

1) Exibir uma lista de trilhas de auditoria:

   - Para visualizar a trilha de auditoria de uma chave específica, consulte *Seção 4.11.2 "Como visualizar trilhas de auditoria de uma chave de usuário", página 91*.

- Para visualizar a trilha de auditoria de um cilindro específico, consulte *Seção 4.11.3 "Como visualizar trilhas de auditoria de cilindro", página 92*.
- Para visualizar todo o arquivo de trilha de auditoria, consulte *Seção 4.11.4 "Como visualizar o arquivo da trilha de auditoria", página 93*.

2) Clique em **Imprimir trilha de auditoria completa** para imprimir ou gravar a tabela em formato PDF.

   A tabela aparece em uma janela pop-up.

3)
   - Para salvar, clique no ícone Gravar e especifique uma pasta para salvar.
   - Para imprimir, clique em **...** e selecione **Imprimir**.

4.11.5 Como aprovar solicitações de uma trilha de auditoria

Se o recurso **Aprovações** estiver ativado, as solicitações de trilhas de auditoria deverão ser aprovadas antes de serem executadas. Uma Chave de comando com o papel de aprovador deve ser usada para entrar no sistema para aprovar as solicitações de trilhas de auditoria pendentes.

Consulte *Seção 6.4 "Como editar as configurações do sistema", página 99* para alterar a configuração de **Aprovações**.

1) Insira a Chave de comando aprovador na ranhura esquerda do Programador local.
2) Entre no sistema.

   Só estarão disponíveis os menus **Tarefas** e **Configurações**.

3) Selecione **Tarefas » Programas para aprovação**.

   Será exibida uma lista de funções pendentes de aprovação.

4) Clique em **Responder**.
5) Para aprovar: Insira um comentário opcional, clique em **Aprovar**.

   Para rejeitar: Insira um comentário opcional, clique em **Rejeitar**.

Para visualizar as funções já aprovadas ou rejeitadas, selecione a guia **Histórico de aprovação**.

5 Como configurar os Sistemas Cliq

5.1 Visão geral da configuração de um Sistema Cliq

Esta visão geral descreve o fluxo de trabalho ao configurar o Sistema Cliq pela primeira vez.

Pré-requisitos:

- O banco de dados é preparado e o software do servidor é instalado no servidor CWM.
- Caso seja um sistema remoto, o banco de dados é preparado e o software do servidor também é instalado no servidor remoto.
- Os firewalls e proxys são configurados para permitir tráfego SSL.
  - A partir dos PCs clientes para o Servidor CWM (portas 443 e 8443).
  - A partir dos programadores remotos para o Servidor remoto (porta 443).
  - A partir do Servidor CWM para o servidor SMTP (porta 25).

1) Configure um Cliente CWM.

   Consulte *Seção 2.1 "Visão geral da configuração de clientes CWM", página 12*.
2) Instale o certificado da Chave de comando mestre.

   Consulte *Seção 5.2 "Como instalar o certificado da chave de comando mestre.", página 95*.
3) Entre no CWM.

   Consulte *Seção 5.3 "Fazer login em um novo Sistema Cliq", página 96*.
4) Configure o idioma do CWM.

   Consulte *Seção 3.4 "Configuração do idioma do CWM", página 18*.
5) Instale uma licença.

   Consulte *Seção 6.1.1 "Como instalar licenças", página 98*.
6) Execute a configuração inicial.

   Consulte *Seção 5.4 "Como executar a configuração inicial", página 97*.

5.2 Como instalar o certificado da chave de comando mestre.

Se a integração DCS estiver ativada:

Será especificado um endereço de e-mail para um Proprietário da chave de comando mestre no DCS. Dentro de uma hora após a preparação do banco de dados do Sistema CLIQ, será enviado um e-mail para esse endereço.

O número de vezes que um certificado da Chave de comando mestre pode ser gerado é determinado por uma configuração no DCS.

A instalação do certificado da chave de comando mestre é igual à instalação do certificado da chave de comando. Consulte *Seção 3.2.1 "Registro do certificado da Chave de comando via CLIQ Connect no computador", página 16* para obter mais informações.

Se a integração DCS não estiver ativada:

O certificado da chave de comando mestre já foi fornecido. Consulte *Seção 3.2.2 "Como instalar o certificado da chave de comando manualmente", página 16* para obter mais informações sobre como instalar o certificado.

5.3 Fazer login em um novo Sistema Cliq

Pré-requisitos:

- O Programador local está instalado. Consulte *Seção 2.2 "Como instalar Programadores locais", página 12*.
- É usado um navegador de internet suportado. Consulte *Seção 9.8 "Requisitos do PC cliente", página 210*.
- O CLIQ Connect PC está instalado e sendo executado no computador.

  Consulte *Seção 2.3 "Como instalar o CLIQ Connect no computador", página 12*.
- O CLIQ Connect no computador está configurado e conectado ao CWM.

  Consulte *Seção 2.4 "Como configurar o CLIQ Connect no computador", página 13*.
- Está disponível uma chave de comando mestre com um código PIN.
- Está instalado um certificado válido para a chave de comando mestre. Consulte *Seção 5.2 "Como instalar o certificado da chave de comando mestre.", página 95*.
- O URL para o CWM está disponível.

1) Insira a Chave de comando na ranhura esquerda do Programador local.
2) Vá para a página inicial de CWM.
3) Selecione o certificado para a chave de comando.

   Será exibida a página de login do CWM.
4) Clique em **Acessar**.
5) Insira o código PIN para a Chave de comando.

   O CLIQ Connect solicita que o uso da chave seja confirmado no computador.
6) Clique em **Confirmar**.
7) Selecione o **Fuso horário base** da lista suspensa.

   ATENÇÃO!
   Essa configuração não pode ser alterada depois de clicar em **Confirmar**.

8) Selecione as opções para as **Aprovação das solicitações de trilhas de auditoria** abaixo:

   - **Desativado**

     Caso isto seja selecionado, todos os administradores poderão solicitar informações sobre as trilhas de auditoria sem a aprovação de outro administrador.
   - **Ativado**

     Caso isto seja selecionado, todos os administradores necessitarão da aprovação de outro administrador para solicitar informações sobre as trilhas de auditoria.

   Para obter mais detalhes sobre o papel do aprovador para trilhas de auditoria, consulte *Seção 4.11.6 "Como aprovar solicitações de uma trilha de auditoria", página 94*.

9) Clique em **Ativar importação de extensão**.

A janela **Confirmação** será aberta.

10) Verifique as configurações com atenção.

> **AVISO!**
> As configurações não poderão mais ser alteradas.

11) Clique em **Confirmar**.

5.4 Como executar a configuração inicial

1) Destrave o Sistema Cliq. Consulte *Seção 6.3 "Como destravar o sistema.", página 99*.
2) Edite as configurações do sistema. Consulte *Seção 6.4 "Como editar as configurações do sistema", página 99*.
3) Configure os Programadores remotos. Consulte *Seção 6.5.1 "Como configurar Programadores remotos", página 104*.
4) Crie os domínios. Consulte *Seção 6.6.4 "Como criar e apagar domínios", página 124*.
5) Especifique o domínio para os cilindros e grupos de cilindros. Consulte *Seção 6.6.7 "Como alterar o domínio dos cilindros", página 125* e *Seção 6.6.8 "Como alterar o domínio dos Grupos de cilindros", página 126*.
6) Configure os perfis de acesso. Consulte *Seção 4.6.2 "Como criar e apagar perfis de acesso", página 68*.
7) Crie modelos de recibos para entregas e devoluções. *Seção 6.9 "Como gerenciar modelos de recibo", página 129*.
8) Crie modelos de cronogramas. Consulte *Seção 6.10 "Como gerenciar Modelos de cronograma", página 132*.
9) Adicione e exclua papéis de administrador e ajuste as permissões de papéis como desejado. Consulte *Seção 6.7 "Como gerenciar papéis e autorizações", página 127*.
10) Emita chaves de comando para os administradores do Sistema Cliq. Consulte *Seção 6.11.7 "Como fazer a entrega das chaves de comando", página 136*.
11) Importe informações do funcionário para o CWM. Consulte *Seção 6.8 "Como importar informações do funcionário", página 128*.

6 Como configurar os Sistemas Cliq

6.1 Como administrar as licenças

6.1.1 Como instalar licenças

Pré-requisitos:

- Está disponível um arquivo de licença novo.
  - Para instalação manual: Armazenado em um pen drive USB ou no disco rígido do computador.
  - Para recuperação automática nos sistemas com integração DCS: Armazenada no DCS.
- O número da licença do arquivo da licença nova é superior ao da licença instalada. Não é possível instalar uma licença mais antiga.

1) Selecione **Administração » Licença**.

   São exibidas informações sobre a licença instalada atualmente e os recursos que ela contém.

2) Para sistemas com integração DCS e onde o arquivo da licença está instalado no DCS:

   Clique em **Buscar licença**.

   A licença é baixada e instalada.

3) Para sistemas sem integração DCS ou onde o arquivo da licença está não está disponível no DCS:

   a) Clique em **Selecionar...**.

   b) Selecione o arquivo de licença.

   c) Clique em **Carregar**.

      A licença é carregada e instalada.

6.1.2 Como visualizar o status da licença

1) Selecione **Administração » Licença**.

   São exibidas informações sobre a licença instalada atualmente e os recursos que ela contém.

Para instalar uma licença nova, consulte *Seção 6.1.1 "Como instalar licenças", página 98*.

6.2 Como travar o sistema para manutenção

Um Sistema Cliq pode ser travado para executar manutenção.

1) Selecione **Administração » Manutenção**.
2) Selecione a data e hora para travar o sistema específico para manutenção.

   O horário escolhido deve estar a, pelo menos, 10 minutos no futuro.

3) Clique em **Bloquear Sistema Cliq**.

6.3 Como destravar o sistema.

1) Selecione **Administração » Manutenção**.
2) Clique em **Desbloquear o Sistema Cliq**.

6.4 Como editar as configurações do sistema

Algumas das configurações do sistema descritas se aplicam apenas a sistemas remotos.

1) Selecione **Administração » Configurações do sistema**.

   Serão exibidas as configurações do sistema.
2) Para editar as configurações do sistema, clique em **Editar**.
3) Atualize as configurações necessárias:

SISTEMA

- **Aprovações**. Caso seja selecionado as solicitações de trilhas de auditoria de cilindros e chaves deverão ser aprovadas antes que as trilhas de auditoria sejam coletadas.

  ATENÇÃO!

  Restrições:

  – Você fez login com a chave de comando mestre.
  – Para desativar o recurso de aprovação, primeiro verifique se todas as trilhas de auditoria pendentes foram canceladas ou concluídas.
  – Para ativar o recurso de aprovação, primeiro certifique-se de desativar **RECUPERAÇÃO AUTOMÁTICA DAS TRILHAS DE AUDITORIA** em todas as chaves de comando. Consulte *Seção 6.11.13 "Ativar ou desativar a recuperação automática das trilhas de auditoria para a chave de comando", página 141*.

  Mesmo depois de ativar o recurso de aprovação, as funções pendentes existentes não são afetadas e não precisam de aprovação. Somente as novas funções de trilhas de auditoria exigem aprovações.

- **Sistema CLIQ Remote** mostra se a funcionalidade Remoto está ativada.

  Só pode ser selecionado na primeira configuração do Sistema Cliq.
- **Suporta Grupos de cilindros** mostra se o uso de grupos de cilindros está ativado.

  Só pode ser selecionado na primeira configuração do Sistema Cliq.
- **Fuso horário base**. Fuso horário usado para as diversas impressões no aplicativo.

  Só pode ser selecionado na primeira configuração do Sistema Cliq.
- **Integração de serviços web** ativa a comunicação com outros sistemas, por exemplo, com sistemas de RH.

- **Sistema de envio de mensagens do usuário** ativa o CWM para enviar e-mails para funcionários e visitantes, por exemplo, lembretes de chaves vencidas.

  - **E-mails após a atualização remota** controla se é enviado um e-mail listando as novas informações de acesso para os proprietários de chaves após uma Atualização remota.

    Selecione a caixa e clique em **Configurar** para selecionar se deseja incluir os cilindros mecânicos neste e-mail ou não.

  - **E-mails após a alteração de dados dos funcionários** controla se é enviado um e-mail contendo a listagem das alterações das informações dos funcionários para o administrador dos domínios onde a chave do funcionário tem acesso atual ou pendente a no mínimo um cilindro.

    Selecione a caixa e clique em **Configurar** para selecionar qual tipo de alteração resultará em uma notificação.

  - **E-mails após a alteração de dados dos visitantes** controla se é enviado um e-mail contendo a listagem das alterações das informações dos visitantes para o administrador dos domínios onde a chave do visitante tem acesso atual ou pendente a no mínimo um cilindro.

    Selecione a caixa e clique em **Configurar** para selecionar qual tipo de alteração resultará em uma notificação.

  - **E-mails após o programador de parede ficar offline** controla se é enviado um e-mail para a pessoa especificada quando um programador de parede fica off-line.

    Selecione a caixa e clique em **Configurar** para inserir o destinatário do e-mail e configurar o número de pulsos consecutivos ausentes após o qual o aviso é enviado.

- **Revalidação flexível** torna possível configurar o intervalo de revalidação da chave por perfil de acesso e por grupo de cilindros.

- **Bloqueia silenciosamente as chaves perdidas no cilindro durante uma atualização de autorização.**

  Marque a caixa de seleção para permitir que o sistema adicione chaves perdidas silenciosamente à lista de chaves não autorizadas para bloqueá-las nos cilindros.

- **Bloqueio de chave perdida com chaves de usuário** permite que seja programada uma função de bloqueio de cilindro em qualquer chave de usuário (chave dinâmica) para bloquear uma chave perdida nos cilindros.

  Isso só se aplica a um sistema remoto.

- **Bloquear chaves perdidas em cilindros novos durante a importação de extensão** Ao adicionar cilindros a um sistema, qualquer chave comunicada como perdida anteriormente pode precisar ser bloqueada nos novos cilindros. Se essa configuração estiver ativada, o CWM gerará automaticamente funções de programação do cilindro para bloquear as chaves perdidas quando o arquivo de importação for ativado.

- **Administradores hierárquicos** (só pode ser editado por Super administradores)

  Marque a caixa de seleção para ativar a função de hierarquia do administrador, de modo que o usuário possa escolher uma estrutura simples ou hierárquica para as permissões.

CLIQ REMOTE

- **URL de serviço**. Servidor remoto usado pelo CWM e os Programadores remotos. Note que será exibido um aviso se a URL não corresponder ao nome do host definido no certificado do servidor remoto.
- **URL de serviço alternativa**. Opção para especificar uma URL de serviço alternativa para o servidor remoto usado pelo CWM e os programadores remotos. A URL é visível na guia **Configurações** da tela dos programadores remotos somente se a versão do firmware do programador de parede ou programador móvel CLIQ for 4.0 ou superior. Note que a **URL de serviço alternativa** leva ao mesmo servidor remoto que a **URL de serviço**.
- **Certificado do servidor CA**. O certificado da Autoridade de certificação (CA) que emite o certificado do servidor no servidor do CLIQ remote. São necessários direitos de administrador para importar o certificado.

CONFIGURAÇÕES DA CHAVE PADRÃO

- **Ativar revalidação na entrega**. Caso selecionado, a opção de revalidação está disponível no fluxo de entrega da chave.
- **Intervalo de revalidação**. A configuração padrão para o intervalo de revalidação da chave.
- **Ativar validação do PIN na entrega**. Caso selecionado, a opção de validação do PIN está disponível no fluxo de entrega da chave.
- **Intervalo de validação do PIN**. A configuração padrão para o intervalo de validação do PIN.
- **Tempo até a devolução**. A configuração padrão para o tempo até que a chave seja devolvida começando a partir da data de entrega. Insira `0` se o tempo final não deve ser especificado.
- **Configuração de validade**. Configuração padrão para a validade das chaves.
- **Tempo de validade**. A configuração padrão para quanto tempo deve ser o tempo de validade, se foi selecionada a opção de validade **Ativo entre as datas selecionadas**.

ADMINISTRAÇÃO

- **Dias padrão em busca de chave vencida**. Opção de busca padrão para chaves vencidas.
- **Idioma das mensagens do usuário**. O idioma usado quando o CWM envia e-mails, por exemplo, sobre chaves vencidas.
- **Recibos de chave** define se os recibos de entrega e devolução de chaves deverão ser impressos separadamente ou combinados.

- **URL raiz dos links externos**. Uma URL raiz que é usada para formar links externos para chaves, funcionários e etc...
- **Delimitador CSV**, é selecionado ponto e vírgula ou vírgula para delimitar entidades ao exportar arquivos CSV.
- **Trilhas de auditoria e eventos**. Trilhas de auditoria e eventos que são mais antigos que um número de dias definido são removidos automaticamente do arquivo das trilhas de auditoria e eventos. Os dias são contados a partir da data em que as trilhas de auditoria e eventos foram coletados.

  O intervalo de retenção das trilhas de auditoria e eventos pode ser configurado por padrão de um a 366 dias ou até 3660 dias com uma licença adicional.

  A partir do CWM 11.6, a exclusão segue a data de criação, que é quando a entrada foi gerada no elemento físico. Isso substitui o método anterior de usar a data de análise, que é quando a entrada foi armazenada no banco de dados do CWM.
- **Ao excluir pessoas**. Quando configurado para **Marcar como excluído**, excluir uma pessoa altera seu status para "excluído" mas todas as informações são mantidas no banco de dados. Quando configurado para **Excluir permanentemente** (configuração padrão para Sistemas Cliq novos), excluir uma pessoa remove a pessoa e as informações correspondentes do banco de dados. A configuração **Excluir permanentemente** suporta GDPR e ativa a capacidade de desativar uma pessoa. Consulte *Seção 8.9 "Exclusão de dados pessoais e conformidade com a GDPR", página 189* para obter mais informações.

  Ao alterar a configuração de **Marcar como excluído** para **Excluir permanentemente** todas as pessoas marcadas como excluídas serão removidas permanentemente.

  Para alterar a configuração de **Excluir permanentemente** para **Marcar como excluído** primeiro é necessário ativar todas as pessoas desativadas.
- **Obter última data de acesso** especifica se a última data de acesso foi coletada para o certificado de uma chave de comando. Quando ativado, é exibida a **Última data usada** na guia **Certificados** na tela detalhada da chave de comando. Consulte *Seção 6.11.14 "Como listar certificados de chaves de comando", página 141*.
- **Campos personalizados dos cilindros** define e adiciona ou edita os campos personalizados para armazenar informações adicionais do cilindro no CWM. Os valores do campo personalizado podem ser editados na tela de detalhes do cilindro para cada cilindro. Eles também podem ser usados para encontrar cilindros usando a busca avançada de cilindros.
- **Domínio do cilindro inicial** define o domínio atribuído para cilindros novos ou importados.
- **Domínio da pessoa inicial** define o domínio atribuído para funcionários ou visitantes novos ou importados.
- **Domínio da chave inicial** define o domínio atribuído para chaves novas ou importadas.

AUTENTICAÇÃO DA REDE PARA PROGRAMADOR DE PAREDE GERAÇÃO 2

- **Autenticação 802.1x**

  Caso a autenticação da rede para qualquer programador de parede no sistema esteja ativada, não é possível selecionar **Desativado** no nível de configuração do sistema. Clique em **Como desativar a autenticação?** e busque a lista dos programadores de parede cuja autenticação de rede está ativada. Consulte *Seção 6.5.7.1 "Como editar as configurações de um programador de parede", página 109* para desativar a autenticação da rede no nível do dispositivo.

- **Nome do servidor da autenticação 802.1x**

  Insira o nome do servidor.

- **Certificado CA do servidor 802.1x**

  Todos os certificados são listados aqui. Caso qualquer certificado seja inválido, será exibida uma mensagem embaixo do certificado.

  Poderão ser carregados até três certificados no formato .pem.

  Para carregar um certificado CA:

  a) Clique em **Selecionar novo...** e selecione um certificado CA (`. pem`).

  b) Clique em **Certificado de carregamento**.

     O certificado CA será exibido.

INTEGRAÇÃO COM O LDAP

- **Ativado**. Se selecionado, a integração como LDAP está disponível.
- **Tipo de servidor LDAP**. Seleciona o tipo de servidor LDAP da lista suspensa.
- **Tipo de conexão**. Selecione entre **START TLS** ou **LDAPS**
- **Host LDAP**. Insira o endereço do servidor LDAP na rede.
- **Porta LDAP**. Insira a porta específica necessária para acessar o servidor LDAP.
- **Usuário DN** é o administrados do LDAP que possui acesso à Base DN.
- **Senha** é a senha do administrador.
- **Base DN** especifica a raiz para buscas no Diretório ativo.
- **Filtro de busca** define os critérios de busca que possibilitam buscas mais eficientes e eficazes.

LOGON ÚNICO (SSO)

- **SAML ativado**Se selecionada, a opção de login SSO ficará disponível. Consulte *Seção 8.10 "Logon único (SSO)", página 190* para obter mais informações sobre SSO.

- **Recarregar a configuração SAML ao Gravar**: Se uma configuração SAML já existente for alterada no banco de dados e essa opção for selecionada, a configuração será recarregada quando o botão **Gravar** nessa página for clicado. Depois de gravar, o botão **Fazer download do certificado de verificação** será exibido.
- **Criar novamente o certificado de verificação**: Se já existir uma configuração SAML no sistema e essa opção estiver selecionada, o certificado será criado quando o botão **Gravar** nessa página for clicado. Isso pode ser necessário se o certificado tiver sido alterado ou expirado. Depois de gravar, o botão **Fazer download do certificado de verificação** será exibido. Faça o download do certificado e carregue-o no serviço do provedor de identidade.

CLIQ CONNECT+

- **Exibir cilindros acessíveis**. Caso selecionado, os usuários do CLIQ Connect+ poderão ver os cilindros que podem ser acessados por suas chaves no CLIQ Connect+.
- **Incluir cilindros mecânicos**. Caso selecionado, os cilindros mecânicos atribuídos ao proprietário da chave também poderão ser visualizados na lista de cilindros acessíveis no CLIQ Connect+.
- **Exibir perfis de acesso**. Caso selecionado, poderá ser visualizada uma lista de perfis de acesso atribuídos à chave no CLIQ Connect+.

  Para ativar esse recurso, o nível de permissão do usuário deverá ser **Visualizar** ou superior no papel **Chave: autorização**. Consulte *Seção 6.7 "Como gerenciar papéis e autorizações", página 127* para alterar o nível de permissão.

6.5 Como gerenciar Programadores remotos

6.5.1 Como configurar Programadores remotos

1) Encontre o Programador remoto e vá para sua tela de informações detalhadas.

   Consulte *Seção 6.5.2 "Como buscar Programadores remotos", página 104*.

2) Edite as informações, etiquetas e links externos do Programador remoto como desejado.

   Consulte *Seção 6.5.3 "Como editar as informações de um Programador remoto", página 105*, *Seção 6.5.5 "Como adicionar ou remover etiquetas de programador remoto", página 107* e *Seção 6.5.6 "Como gerenciar links externos de um Programador remoto", página 108*.

3) Edite as configurações do Programador remoto e carregue a configuração no Programador remoto. Isto inclui instalar o certificado.

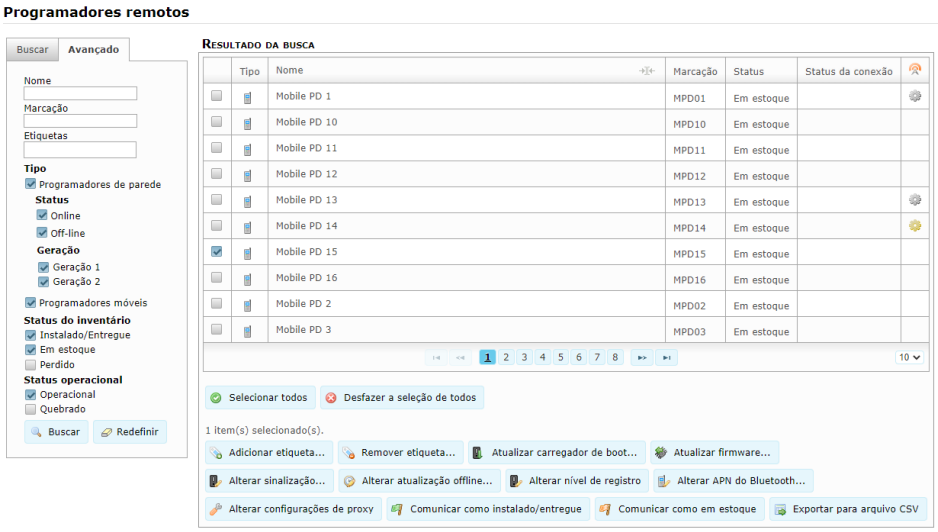
   Consulte *Seção 6.5.7 "Como configurar programadores de parede", página 109* para Programadores de parede.

   Consulte *Seção 6.5.8.1 "Como editar as configurações de um programador móvel CLIQ", página 116* para Programadores móveis CLIQ.

6.5.2 Como buscar Programadores remotos

1) Selecione **Informações do sistema » Programadores remotos**.

   O resultado da busca exibe uma lista de PDs remotos.



Os símbolos abaixo são utilizados:

Programador de parede

Programador móvel CLIQ

ATENÇÃO!
Os Programadores móveis CLIQ Connect não estão incluídos na lista.

2) Insira o critério de busca.

   Ao digitar nos campos de busca, o CWM aceita a primeira parte de uma cadeia de caracteres de busca bem como um asterisco (*). Se a busca for para "Laboratório 1", escrever "Lab", "*1" ou "Lab*1" fornecerá resultados incluindo "Laboratório 1".

   Para filtrar a lista do resultado de busca por tipo de programador remoto, marque a caixa **Programadores de parede** ou **Programadores móveis** na guia de busca **Avançado**.

   Os programadores de parede podem ser filtrados por status, **Online** ou **Off-line**.

3) Clique em **Buscar**.

4) Para exibir informações detalhadas, clique no Programador remoto específico.

Poderão ser configurados vários programadores remotos simultaneamente. Selecione os programadores remotos na lista do resultado de busca e clique em um dos botões para alterar as configurações correspondentes.

6.5.3 Como editar as informações de um Programador remoto

1) Encontre o Programador remoto e vá para sua tela de informações detalhadas.

   Consulte *Seção 6.5.2 "Como buscar Programadores remotos", página 104*.

2) Clique em **Editar**.

3) Para editar o nome do programador remoto, atualize o campo **Nome**.

4) Para adicionar etiquetas clique em **Adicionar Etiqueta...**. Consulte também *Seção 6.5.5 "Como adicionar ou remover etiquetas de programador remoto", página 107*.

5) Para editar links externos clique em **Adicionar link externo...**. Consulte também *Seção 6.5.6 "Como gerenciar links externos de um Programador remoto", página 108*.

6) Clique em **Gravar**.

6.5.4 Como editar o status de um PD remoto

Os PDs remotos possuem um status de inventário como em estoque, entregue ou perdido e um status de operação como operacional ou quebrado.

1) Encontre o Programador remoto e vá para sua tela de informações detalhadas.

   Consulte *Seção 6.5.2 "Como buscar Programadores remotos", página 104*.

2) **Para alterar o status do Programador de parede**

   - Como comunicar como **Instalado**
     - Vá para a visualização de informações detalhadas e clique em **Comunicar como instalado** e clique em **OK**.
     - Se houver vários dispositivos a serem comunicados, selecione Programadores de parede no resultado da pesquisa, clique em **Comunicar como instalado/entregue** e clique em **OK**.
   - Como comunicar como **Em estoque**
     - Vá para a visualização de informações detalhadas e clique em **Comunicar como em estoque** e clique em **OK**.
     - Se houver vários dispositivos a serem comunicados, selecione Programadores de parede no resultado da pesquisa, clique em **Comunicar como em estoque** e clique em **OK**.
   - Como comunicar como **Perdido**
     - Vá para a visualização de informações detalhadas e clique em **Comunicar como perdido** e clique em **OK**.
   - Como comunicar como **Encontrado**
     - Vá para a visualização de informações detalhadas e clique em **Comunicar como encontrado** e clique em **OK**.
   - Como comunicar como **Quebrado**
     - Vá para a visualização de informações detalhadas e clique em **Informar a quebra** e clique em **OK**.
   - Como comunicar como **Operacional**
     - Vá para a visualização de informações detalhadas e clique em **Relatar operacional** e clique em **OK**.

3) **Para alterar o status do Programador móvel CLIQ**

   - Como comunicar como **Entregue**
     - Vá para a visualização de informações detalhadas e clique em **Entrega** e clique em **OK**.

- Se houver vários dispositivos a serem comunicados, selecione Programadores de parede no resultado da pesquisa, clique em **Comunicar como instalado/entregue** e clique em **OK**.

- Como comunicar como **Em estoque**
  - Vá para a visualização de informações detalhadas e clique em **Devolver** e clique em **OK**.
  - Se houver vários dispositivos a serem comunicados, selecione Programadores de parede no resultado da pesquisa, clique em **Comunicar como em estoque** e clique em **OK**.
- Como comunicar como **Perdido**
  - Vá para a visualização de informações detalhadas e clique em **Comunicar como perdido** e clique em **OK**.
- Como comunicar como **Encontrado**
  - Vá para a visualização de informações detalhadas e clique em **Comunicar como encontrado** e clique em **OK**.
- Como comunicar como **Quebrado**
  - Vá para a visualização de informações detalhadas e clique em **Informar a quebra** e clique em **OK**.
- Como comunicar como **Operacional**
  - Vá para a visualização de informações detalhadas e clique em **Relatar operacional** e clique em **OK**.

6.5.5 Como adicionar ou remover etiquetas de programador remoto

1) Selecione **Informações do sistema » Programadores remotos**.

   Será exibida uma lista de programadores remotos

   - Para adicionar ou remover etiquetas de um programador remoto individual, acesse *Passo 2*.
   - Para adicionar ou remover etiquetas de vários programadores remotos simultaneamente, acesse *Passo 3*.

2) **Para adicionar ou remover etiquetas de um programador remoto individual:**

   1. Selecione o programador remoto e vá para sua tela de informações detalhadas.
   2. Clique em **Editar**.
   3. Adicione ou remova uma etiqueta de um programador remoto individual.

      Para adicionar uma etiqueta:

      a) Clique em **Adicionar etiqueta...**.
      b) Insira um nome para a etiqueta.
      c) Clique em **OK**.

Para excluir uma etiqueta:
Clique na etiqueta a ser removida.

4. Clique em **Gravar**.

3) **Para adicionar ou remover etiquetas de vários programadores remotos:**

1. Selecione os programadores remotos nos resultados da busca, marcando as caixas de seleção.
2. **Para adicionar uma etiqueta:**

a) Clique em **Adicionar etiqueta...**.
b) Insira o nome da etiqueta.
c) Clique em **OK**.

Para excluir uma etiqueta:

a) Clique em **Remover etiqueta...**.
b) Insira o nome da etiqueta.
c) Clique em **OK**.

Consulte também *Seção 8.2.6 "Etiquetas", página 179*.

6.5.6 Como gerenciar links externos de um Programador remoto

1) Encontre o Programador remoto e vá para sua tela de informações detalhadas.

Consulte *Seção 6.5.2 "Como buscar Programadores remotos", página 104*.

2) Clique em **Editar**.
3) **Para adicionar um link externo:**

1. Clique em **Adicionar.**
2. Insira o **Nome** da URL.
3. Insira **URL**. A **URL** deve começar com um protocolo (por exemplo http:// ou ftp://).

Se foi definida uma URL raiz nas **Configurações do sistema** (item **URL raiz dos links externos**), só é necessário adicionar a última parte da URL.
Consulte também *Seção 6.4 "Como editar as configurações do sistema", página 99*.

4. Clique em **OK**.

Para editar um link externo:

1. Clique em **Editar** no link externo a ser editado.
2. Atualize os campos.
3. Clique em **OK**.

Para remover um link externo:
Clique em **Remover** no link externo a ser removido.

4) Clique em **Gravar**.

Consulte também *Seção 8.4 "Links externos", página 182*.

6.5.7 Como gerenciar as configurações e o certificado de um programador de parede

Pré-requisitos:

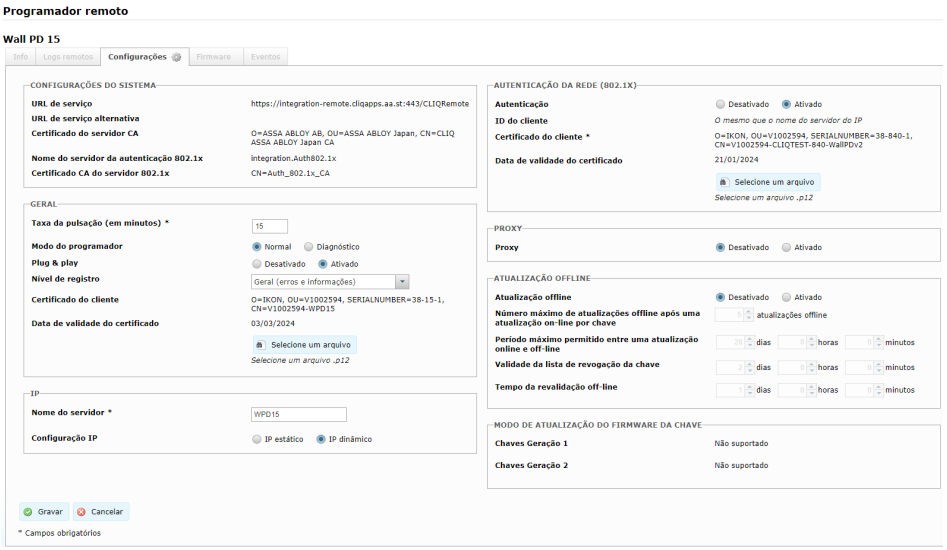
- Para um PD de parede que é configurado pela primeira vez com o **Plug & play** desativado, ou não puder se conectar com as configurações existentes:
  - Um cabo USB:
    - **Programador de parede geração 1:** Cabo USB On-The-Go (OTG) com USB mini macho (suportado tanto tipo A como tipo B) para USB padrão fêmea (tipo A).

    - **Programador de parede geração 2:** USB-C macho para USB padrão fêmea (tipo A).
  - Um pen drive USB:
    - **Programador de parede geração 1:** Formatado com o sistema de arquivos FAT32. Tamanho da memória recomendado é de 8-16 GB.
    - **Programador de parede geração 2:** Formatado com o sistema de arquivos FAT32. Não exite restrição de tamanho para o pen drive USB. Use um pen drive USB-C padrão ou conecte um pen drive USB-A com um adaptador ou cabo padrão.
- Para usar a atualização off-line:
  - Um programador de parede geração 1 com firmware 2.11 ou superior ou programador de parede geração 2.
- Para instalar ou renovar certificados **sem** integração DCS:
  - Um arquivo de certificado .p12. Isto é obtido do fornecedor local CLIQ.

6.5.7.1 Como editar as configurações de um programador de parede

1) Encontre o Programador remoto e vá para sua tela de informações detalhadas.

   Consulte *Seção 6.5.2 "Como buscar Programadores remotos", página 104*.
2) Selecione a guia **Configurações**.
3) Clique em **Editar**.



4) Atualize as configurações necessárias:

GERAL

- **Taxa da pulsação (em minutos)**

  Valor recomendado: 15.

  A frequência da pulsação é o número de minutos entre pulsações enviadas de um Programador de parede para o Servidor CLIQ remoto para avisar o CWM que está on-line. O Programador de parede verifica também as atualizações para Programadores de parede (atualizações de firmware ou de configuração) ao enviar a pulsação.

- **Modo do programador**

  Selecione **Normal**. Não selecione **Diagnóstico** a menos que aconselhado pelo suporte técnico.

- **Plug & play**

  > **ATENÇÃO!**
  > O **Plug & play** exige que a integração DCS seja ativada e que as **Configurações de proxy** seja desativadas para funcionar.

  O **Plug & play** possibilita ao programador remoto receber automaticamente um certificado de um servidor, caso ainda não tenha um. O certificado é baixado do DCS por meio do aplicativo de inscrição.

  Selecione **Ativado** (configuração padrão recomendada) caso esteja usando o PD remoto em uma rede conectada à internet sem restrições. Selecione **Desativado** caso esteja baixando um certificado para o programador remoto usando um pen drive.

- **Nível de registro** (Somente programador de parede geração 2)

  Os programadores de parede enviam registros de erro para o servidor remoto e os registros são mantidos em um local por 10 dias. O nível de registro pode ser configurado para o programador de parede geração 2 nos seguintes níveis:

- **Crítico (somente erros)**
- **Geral (erros e informações)**
- **Detalhado (erros, informações e debug)**
- **Nenhum registro**

> **Dica**
> Também é possível aplicar o mesmo nível de registro a vários programadores de parede geração 2 a partir da lista de programadores remotos.

IP

- **Nome do servidor**

  O nome do servidor é o nome do Programador de parede na rede. Recomendamos usar nomes do host descritivos para ajudar a identificar o programador remoto ao solucionar problemas.

- **Configuração IP**

  Selecione **IP estático** ou **IP dinâmico**.

  Se for selecionado **IP estático**, insira **Endereço IP**, **Máscara da sub-rede**, **Gateway** e **DNS**.

AUTENTICAÇÃO DA REDE (802.1X) (Somente programador de parede geração 2)

- **Autenticação**

  Selecione **Desativado** ou **Ativado**.

  > **ATENÇÃO!**
  > Após ativar a AUTENTICAÇÃO DA REDE (802.1X) pela primeira vez, o programador de parede precisa ser configurado usando um pen drive USB.
  >
  > Consulte *Seção 6.5.7.3 "Como configurar o programador de parede com a AUTENTICAÇÃO DA REDE (802.1X)", página 114* para obter mais detalhes.

- **ID do cliente** é o mesmo que o nome do servidor do IP
- **Certificado do cliente**

  Um certificado do cliente é listado aqui.

  Para carregar o certificado do cliente:

  a) Clique em **Selecione um arquivo...**.
  b) Em uma janela pop-up, insira a senha do arquivo do certificado e clique em **Selecionar...**.
  c) Na pop-up do file explorer, selecione um arquivo de certificado (`. 12`).
  d) Clique em **Carregar**.

São exibidos **Certificado do cliente** e **Data de validade do certificado**.

Consulte *Seção 6.4 "Como editar as configurações do sistema", página 99* para editar as configurações amplas de sistema para 802.1x.

PROXY

- **Proxy**

  Se for selecionado **Ativado**, insira **Host**, **Porta**, **Nome de usuário** e **Senha**.

  Host é o endereço do servidor proxy na rede.

  Porta é a porta específica necessária para acessar o servidor proxy. Normalmente essas portas são 8080.

ATUALIZAÇÃO OFFLINE

Consulte também *Seção 8.3.3 "Atualização off-line", página 181*.

> **ATENÇÃO!**
> Para atualizar uma chave no modo off-line a chave deverá ter um firmware versão 6 ou superior.

- **Número máximo de atualizações offline após uma atualização online por chave**

  Especifica o número de atualizações que podem ser feitas no modo offline para cada chave antes que seja necessária uma atualização online.

- **Período máximo permitido entre uma atualização online e off-line**

  Especifica o intervalo após a última atualização online durante o qual são permitidas atualizações offline.

  O valor define o intervalo de tempo quando a chave deve ter sido revalidada no modo online.

- **Validade da lista de revogação da chave**

  Especifica por quanto tempo a Lista de revogação da chave é armazenada no programador de parede e são permitidas atualizações offline. Consulte também *Seção 8.3.3 "Atualização off-line", página 181*.

  O valor define o intervalo no qual o programador remoto permite a revalidação offline. Depois desse intervalo, não poderão ser realizadas atualizações offline. Por exemplo, se for esperada uma interrupção de serviço de 48 horas, deverão ser configuradas no mínimo 48 horas.

- **Tempo da revalidação off-line**

  Especifica o intervalo de extensão da validade da chave. O intervalo de revalidação configurado na chave é ignorado nas atualizações off-line.

MODO DE ATUALIZAÇÃO DO FIRMWARE DA CHAVE

> **ATENÇÃO!**
> Os programadores remotos geração 2 não suportam a atualização do firmware para chaves geração 1.

Para ativar a desativar as atualizações da chave, consulte *Seção 6.5.11 "Como ativar e desativar as atualizações de chaves em programadores remotos", página 121*.

5) Clique em **Gravar**.

6) Transfira a configuração atualizada para o programador.

- Se o programador de parede estiver online ou puder se conectar com suas configurações atuais:

  As configurações de atualização são enviadas para o Programador de parede após a próxima pulsação. O Programador de parede é configurado automaticamente e se conecta ao servidor remoto.

  Para ver se um programador de parede está online, visualize as informações detalhadas.

- Se o PD for configurado pela primeira vez com o **Plug & play** desativado, ou não puder se conectar com as configurações atuais:

  a) Insira um pen drive USB no computador cliente.

  b) Clique em **Gravar para arquivo** e grave o arquivo na pasta raiz do pen drive USB.

  > **ATENÇÃO!**
  > Certifique-se de que não existam outros arquivos além dos arquivos de configuração na pasta raiz do pen drive.
  >
  > Poderão existir vários arquivos de configuração no mesmo pen drive.

  c) Conecte a unidade flash USB ao Programador de parede usando o cabo USB apropriado (consulte *Seção 6.5.7 "Como configurar programadores de parede", página 109*).

  O Programador é configurado automaticamente e se conecta ao servidor remoto. Isto deve levar menos de um minuto.

7) Verifique se o LED CLIQ se acende, indicando que o programador está online e configurado corretamente.

Consulte *Seção 9.5.1 "Indicações de programador de parede (Geração 1) e programador móvel", página 207* ou *Seção 9.5.2 "Indicações de programador de parede (geração 2)", página 208*.

6.5.7.2 Como instalar ou renovar o certificado de um programador de parede

1) Encontre o Programador remoto e vá para sua tela de informações detalhadas.

Consulte *Seção 6.5.2 "Como buscar Programadores remotos", página 104*.

2) Selecione a guia **Configurações**.

3)
- Se a Integração DCS estiver ativada, clique em **Gerar certificado do cliente**.

  Será gerado o certificado.

- Se a Integração DCS não estiver ativada:

  a) Clique em **Editar** para entrar no modo de edição.

  b) Na seção **GERAL**, clique em **Selecione um arquivo**.

c) Clique em **Selecionar...** e selecione o arquivo do certificado (.p12)

d) Insira a **Senha do arquivo do certificado**.

e) Clique em **Carregar**.

f) Clique em **Gravar** para sair do modo de edição.

4) Transfira a configuração atualizada para o programador.

- Se o programador de parede estiver online ou puder se conectar com suas configurações atuais:

  As configurações de atualização são enviadas para o Programador de parede após a próxima pulsação. O Programador de parede é configurado automaticamente e se conecta ao servidor remoto.

  Para ver se um programador de parede está online, visualize as informações detalhadas.

- Se o PD for configurado pela primeira vez com o **Plug & play** desativado, ou não puder se conectar com as configurações atuais:

  a) Insira um pen drive USB no computador cliente.

  b) Clique em **Gravar para arquivo** e grave o arquivo na pasta raiz do pen drive USB.

  > **ATENÇÃO!**
  > Certifique-se de que não existam outros arquivos além dos arquivos de configuração na pasta raiz do pen drive.
  >
  > Poderão existir vários arquivos de configuração no mesmo pen drive.

  c) Conecte a unidade flash USB ao Programador de parede usando o cabo USB apropriado (consulte *Seção 6.5.7 "Como configurar programadores de parede", página 109*).

  O Programador é configurado automaticamente e se conecta ao servidor remoto. Isto deve levar menos de um minuto.

5) Verifique se o LED CLIQ se acende, indicando que o programador está online e configurado corretamente.

   Consulte *Seção 9.5.1 "Indicações de programador de parede (Geração 1) e programador móvel", página 207* e *Seção 9.5.2 "Indicações de programador de parede (geração 2)", página 208*.

6.5.7.3 Como configurar o programador de parede com a AUTENTICAÇÃO DA REDE (802.1X)

Após ativar a AUTENTICAÇÃO DA REDE (802.1X) pela primeira vez, o programador de parede precisa ser configurado usando um pen drive USB.

> **ATENÇÃO!**
> Isso só se aplica aos Programadores de parede da geração 2.

Pré-requisito:

- **Autenticação 802.1x** está ativado em **Configurações do sistema**. Consulte *Seção 6.4 "Como editar as configurações do sistema", página 99*.

1) Encontre o Programador remoto e vá para sua tela de informações detalhadas.

   Consulte *Seção 6.5.2 "Como buscar Programadores remotos", página 104*.

2) Selecione a guia **Configurações**.

3) Clique em **Editar** para entrar no modo de edição.

4) Carregue o certificado do cliente de AUTENTICAÇÃO DA REDE (802.1X):

   a) Na seção **AUTENTICAÇÃO DA REDE (802.1X)**, clique em **Selecione um arquivo...**.

   b) Em uma janela pop-up, insira a senha do arquivo do certificado e clique em **Selecionar...**.

   c) Na pop-up do file explorer, selecione um arquivo de certificado (`. 12`).

   d) Clique em **Carregar**.

      São exibidos **Certificado do cliente** e **Data de validade do certificado**.

   e) Clique em **Gravar** para sair do modo de edição.

5) Transfira a configuração atualizada para o programador de parede:

   a) Insira um pen drive USB no computador cliente.

   b) Clique em **Gravar para arquivo** e grave o arquivo na pasta raiz do pen drive USB.

      ATENÇÃO!
      Certifique-se de que não existam outros arquivos além dos arquivos de configuração na pasta raiz do pen drive.

      Poderão existir vários arquivos de configuração no mesmo pen drive.

   c) Conecte a unidade flash USB ao Programador de parede usando o cabo (USB-C macho para USB fêmea padrão (tipo A)).

      O Programador é configurado automaticamente e se conecta ao servidor remoto.

   d) Verifique que o LED central na barra de progresso no programador de parede esteja aceso quando o processo estiver concluído.

      Se os indicadores LED se comportarem de outra forma, consulte *Seção 9.5.2 "Indicações de programador de parede (geração 2)", página 208* para verificar o status.

6.5.8 Como gerenciar as configurações e o certificado de um Programador móvel CLIQ

Pré-requisitos:

- Para uso com um iPhone ou celular Android.
  - Um programador móvel CLIQ com firmware versão 2.10 ou superior.
  - É necessário um cabo Mini USB para conectar o Programador móvel CLIQ ao telefone sem usar o Bluetooth. Para obter o cabo adequado, consulte *Seção 7.4.2 "Programadores remotos", página 159*.
- Para um programador móvel CLIQ que é configurado pela primeira vez com o **Plug & play** desativado, ou não puder se conectar com as configurações existentes,

– Um cabo USB On-The-Go (OTG): USB mini macho (suportado tanto tipo A como tipo B) para USB padrão fêmea (tipo A).

– Um pen drive formatado com sistema de arquivos FAT32. Tamanho da memória recomendado é de 8-16 GB.

- Para usar a atualização off-line:

  – Um programador móvel CLIQ com firmware 2.10 ou superior.

- Para instalar ou renovar certificados **sem** integração DCS:

  – Um arquivo de certificado .p12. Isto é obtido do fornecedor local CLIQ.

- A documentação fornecida com o programador móvel CLIQ está disponível.

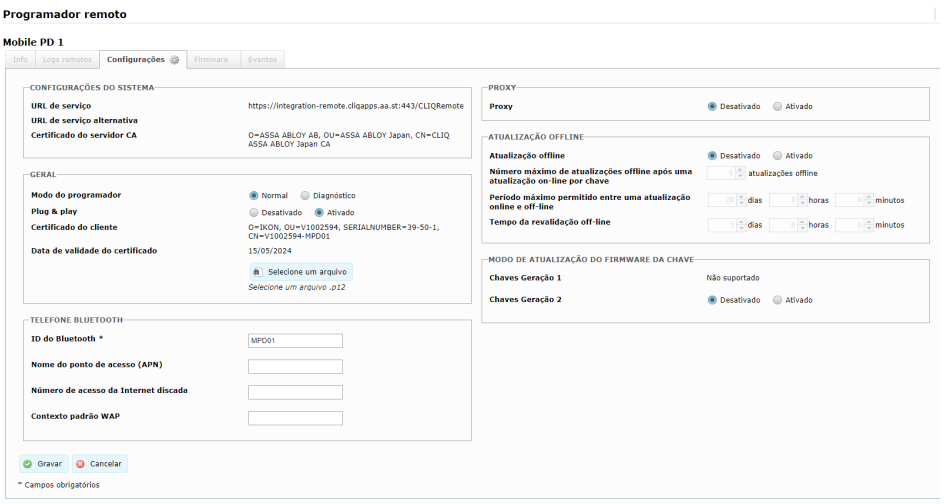
6.5.8.1 Como editar as configurações de um programador móvel CLIQ

1) Encontre o Programador móvel CLIQ e vá para sua tela de informações detalhadas.

   Consulte *Seção 6.5.2 "Como buscar Programadores remotos", página 104*.

2) Selecione a guia **Configurações**.

3) Clique em **Editar**.



4) Atualize as configurações necessárias:

GERAL

- **Modo do programador**

  Selecione **Normal**. Não selecione **Diagnóstico** a menos que aconselhado pelo suporte técnico.

- **Plug & play**

ATENÇÃO!
O **Plug & play** exige que a integração DCS seja ativada e que as **Configurações de proxy** seja desativadas para funcionar.

O **Plug & play** possibilita ao programador remoto receber automaticamente um certificado de um servidor, caso ainda não tenha um. O certificado é baixado do DCS por meio do aplicativo de inscrição.

Selecione **Ativado** (configuração padrão recomendada) caso esteja usando o PD remoto em uma rede conectada à internet sem restrições. Selecione **Desativado** caso esteja baixando um certificado para o programador remoto usando um pen drive.

TELEFONE BLUETOOTH

Seja como for que as **CONFIGURAÇÕES DE TELEFONE BLUETOOTH** estão configuradas, o programador móvel CLIQ sempre pode ser usado com um computador conectado com um cabo USB.

Para uso com

- iPhone
- Android
- Outro celular que suporte o perfil PAN Bluetooth.

Deixe todos os campos nas **CONFIGURAÇÕES DE TELEFONE BLUETOOTH** exceto **ID do Bluetooth** em branco.

Para usar com um telefone celular que suporte o perfil Bluetooth DUN, insira o seguinte:

- **ID do Bluetooth**

  Um nome do programador móvel CLIQ. Esse nome estará visível no celular ao parear com o programador móvel CLIQ.

- **Nome do ponto de acesso (APN)**

  O nome do gateway do operador da rede entre a rede móvel e a internet. Um exemplo é: "online.telia.se". Essa configuração é obtida com a operadora do celular.

- **Número de acesso da Internet discada**

  O número que deve ser usado para obter acesso à rede, por exemplo, `*99#`. Essa configuração é obtida da operadora do celular.

- **Contexto padrão WAP**

  O local no telefone celular onde são armazenadas as configurações da Internet. Essa é uma configuração específica do telefone celular e o valor correto é obtido na documentação do telefone. Na maioria dos casos as configurações podem ter o valor `1`.

PROXY

- **Proxy**

Se for selecionado **Ativado**, insira **Host**, **Porta**, **Nome de usuário** e **Senha**.

Host é o endereço do servidor proxy na rede.

Porta é a porta específica necessária para acessar o servidor proxy. Normalmente essas portas são 8080.

ATUALIZAÇÃO OFFLINE

ATENÇÃO!
Para atualizar uma chave no modo off-line a chave deve:

- ter sido atualizada recentemente no mesmo programador móvel CLIQ (estar entre as 10 últimas chaves atualizadas).
- ter firmware versão 6 ou superior.

- **Número máximo de atualizações off-line após uma atualização online**

  Especifica o número de atualizações que podem ser feitas no modo off-line antes que seja necessária uma atualização online. Insira `0` para desabilitar a Atualização off-line.

- **Período máximo permitido entre uma atualização online e off-line**

  Especifica quanto tempo após a última atualização online são permitidas as atualizações off-line.

- **Tempo da revalidação off-line**

  Especifica em quanto tempo a validade da chave é estendida. O intervalo de revalidação configurado na chave é ignorado nas atualizações off-line.

MODO DE ATUALIZAÇÃO DO FIRMWARE DA CHAVE
Para ativar a desativar as atualizações da chave, consulte *Seção 6.5.11 "Como ativar e desativar as atualizações de chaves em programadores remotos", página 121*.

5) Clique em **Gravar**.
6) Transfira a configuração atualizada para o programador móvel CLIQ.

- Se o programador móvel CLIQ foi configurado antes e pode se conectar com as configurações atuais:

  As configurações de atualização são enviadas para o programador móvel CLIQ na próxima vez em que for usado. O Programador é configurado automaticamente e se conecta ao servidor remoto. Isto deve levar menos de um minuto.

- Se o PD for configurado pela primeira vez com o **Plug & play** desativado, ou não puder se conectar com as configurações atuais:

  a) Insira um pen drive USB no computador cliente.
  b) Clique em **Gravar para arquivo** e grave o arquivo na pasta raiz do pen drive USB.

ATENÇÃO!
Certifique-se de que não existam outros arquivos além dos arquivos de configuração na pasta raiz do pen drive.

Poderão existir vários arquivos de configuração no mesmo pen drive.

c) Conecte a unidade flash USB ao Programador móvel CLIQ usando o cabo USB apropriado (consulte *Seção 6.5.8 "Como configurar Programadores móveis", página 115*).

d) Insira uma chave de usuário no programador móvel CLIQ.

Inicia-se a configuração do programador móvel CLIQ.

e) Quando o LED Download permanecer aceso, remova o pen drive.

7) Para configurar um telefone celular para uso com o programador móvel CLIQ, consulte a documentação separada fornecida com o programador móvel CLIQ.

8) Para configurar um computador para uso com o programador móvel CLIQ:

a) Instale o **ASSA ABLOY Network Provider** no computador cliente.

b) Use um cabo mini USB para conectar o computador cliente ao programador móvel CLIQ. Para saber sobre o cabo adequado, consulte *Seção 6.5.8 "Como configurar Programadores móveis", página 115*.

9) Para verificar se a configuração está correta,

a) Insira uma chave de usuário no programador móvel CLIQ.

O Programador liga e se conecta ao Servidor remoto. Isto deverá levar menos de um minuto.

b) Verifique que o LED CLIQ acenda de forma contínua.

Isto significa que o programador está online e configurado corretamente.

Consulte também *Seção 9.5.1 "Indicações de programador de parede (Geração 1) e programador móvel", página 207*.

6.5.8.2 Como instalar ou renovar o certificado de um programador móvel CLIQ

1) Encontre o Programador remoto e vá para sua tela de informações detalhadas.

Consulte *Seção 6.5.2 "Como buscar Programadores remotos", página 104*.

2) Selecione a guia **Configurações**.

3) Para instalar ou renovar um certificado:

- Se a Integração DCS estiver ativada, clique em **Gerar certificado**.

  Será gerado o certificado.
- Se a integração do DCS não estiver ativada e o arquivo de certificado for fornecido pelo revendedor local do CLIQ, você poderá usar o arquivo de certificado para obter mais informações:

a) Clique em **Editar** para entrar no modo de edição.

b) Na seção **GERAL**, clique em **Selecione um arquivo**.

c) Clique em **Selecionar...** e selecione o arquivo do certificado (.p12)

d) Insira a **Senha do arquivo do certificado**.

e) Clique em **Carregar**.

f) Clique em **Gravar** para sair do modo de edição.

4) Transfira a configuração atualizada para o programador.

- Se o programador móvel CLIQ foi configurado antes e pode se conectar com as configurações atuais:

  Clique em **Gravar**.

  As configurações de atualização são enviadas para o programador móvel CLIQ na próxima vez em que for usado. O Programador é configurado automaticamente e se conecta ao servidor remoto. Isto deve levar menos de um minuto.

- Se o Programador móvel CLIQ for configurado pela primeira vez com o **Plug & play** desativado, ou não puder se conectar com as configurações atuais:

  a) Insira um pen drive USB no computador cliente.

  b) Clique em **Gravar para arquivo** e grave o arquivo na pasta raiz do pen drive USB.

  ATENÇÃO!
  Certifique-se de que não existam outros arquivos além dos arquivos de configuração na pasta raiz do pen drive.

  Poderão existir vários arquivos de configuração no mesmo pen drive.

  c) Conecte a unidade flash USB ao Programador móvel CLIQ usando o cabo USB apropriado (consulte *Seção 6.5.8 "Como configurar Programadores móveis", página 115*).

  d) Insira uma chave de usuário no programador móvel CLIQ.

  Inicia-se a configuração do programador móvel CLIQ.

  e) Quando o LED Download permanecer aceso, remova o pen drive.

5) Para configurar um telefone celular para uso com o programador móvel CLIQ, consulte a documentação separada fornecida com o programador móvel CLIQ.

6) Para configurar um computador para uso com o programador móvel CLIQ:

   a) Instale o **ASSA ABLOY Network Provider** no computador cliente.

   b) Use um cabo mini USB para conectar o computador cliente ao programador móvel CLIQ. Para saber sobre o cabo adequado, consulte *Seção 7.4.2 "Programadores remotos", página 159*.

7) Para verificar se a configuração está correta,

a) Insira uma chave de usuário no programador móvel CLIQ.

O Programador liga e se conecta ao Servidor remoto. Isto deverá levar menos de um minuto.

b) Verifique que o LED CLIQ acenda de forma contínua.

Isto significa que o programador está online e configurado corretamente.

Consulte também *Seção 9.5.1 "Indicações de programador de parede (Geração 1) e programador móvel", página 207*.

6.5.9 Como visualizar o registro de eventos do Programador remoto

O Registro de eventos apresenta eventos e problemas que os Programadores remotos relataram ao CLIQ Web Manager.

1) Encontre o Programador remoto e vá para sua tela de informações detalhadas.

Consulte *Seção 6.5.2 "Como buscar Programadores remotos", página 104*.

2) Selecione a guia **Registro de eventos**.

6.5.10 Ativação e desativação de mensagens de programador de parede offline

Quando um programador de parede para de enviar pulsos durante um certo intervalo, o CLIQ Web Manager detecta que ele está offline e envia um e-mail a uma pessoa específica. Esta seção explica como configurar esse recurso.

1) Selecione **Administração » Configurações do sistema**.

Serão exibidas as configurações do sistema.

2) Clique em **Editar**.

3) Na seção SISTEMA, encontre **E-mails após o programador de parede ficar offline** em **Sistema de envio de mensagens do usuário**.

4) • Para parar o e-mail, exclua a seleção e vá para *Passo 8*.
   • Para receber o e-mail, selecione a caixa e vá para o próximo passo.

   O botão **Configurar** ao lado da caixa de seleção fica azul.

5) Clique em **Configurar**.

A janela de configuração se abre.

6) Insira o endereço de e-mail para onde o e-mail deve ser enviado quando um programador de parede fica off-line.

7) Insira o número de pulsos ausentes após o qual o e-mail é enviado.

8) Clique em **OK**.

6.5.11 Como ativar e desativar as atualizações de chaves em programadores remotos

Consulte *Seção 6.15.3 "Como atualizar o firmware em chaves", página 147* para obter informações sobre como atualizar chaves, incluindo as versões de firmware.

1) Encontre o Programador remoto e vá para sua tela de informações detalhadas.

Consulte *Seção 6.5.2 "Como buscar Programadores remotos", página 104*.

2) Selecione a guia **Configurações**.

3) Para atualizar chaves geração 1:

Para ativar atualizações da chave:
Em **Configurações de modo de atualização de firmware da chave**, clique em **Alterar para modo de atualização de chave**.

Este botão só estará visível assim que os arquivos de firmware necessários tiverem sido importados, consulte *Seção 6.15.3 "Como atualizar o firmware em chaves", página 147*.

Para desativar atualizações da chave:
Em **Configurações de modo de atualização de firmware da chave**, clique em **Alternar para modo normal**.

4) Para atualizar chaves geração 2:

Para ativar atualizações da chave:

1. Clique em **Editar**.
2. Em **Configurações de modo de atualização de firmware da chave**, selecione **Ativado**.
3. Clique em **Gravar**.

> **ATENÇÃO!**
> Poderão ser selecionados vários programadores remotos para a atualização de chaves geração 2.
>
> Repita *Passo 5 c* em *Seção 6.15.3 "Como atualizar o firmware em chaves", página 147* para cada programador remoto que atualizará chaves.

Para desativar atualizações da chave:

1. Clique em **Editar**.
2. Em **Configurações de modo de atualização de firmware da chave**, selecione **Desativado**.
3. Clique em **Gravar**.

6.5.12 Como exportar as informações de um Programador remoto

1) Encontre o Programador remoto e vá para sua tela de informações detalhadas.

Consulte *Seção 6.5.2 "Como buscar Programadores remotos", página 104*.

2) A partir dos resultados da busca, selecione os programadores remotos cujos dados devem ser exportados.

3) Clique em **Exportar para arquivo CSV**.

4) Na janela pop-up de download do arquivo, clique em **OK**.

O download de um arquivo CSV é feito na pasta **Downloads**.

ATENÇÃO!
Para ser possível abrir o arquivo em Excel da maneira correta, o delimitador para o arquivo deverá ser configurado de acordo com as configurações regionais. Consulte *Seção 6.4 "Como editar as configurações do sistema", página 99* para alterar o delimitador.

6.6 Como gerenciar domínios

6.6.1 Como buscar domínios

1) Selecione **Administração » Domínios**.

   Será exibida uma lista de todos os domínios.

2) Insira o critério de busca.

   Ao digitar nos campos de busca, o CWM aceita a primeira parte de uma cadeia de caracteres de busca bem como um asterisco (*). Se a busca for para "Laboratório 1", escrever "Lab", "*1" ou "Lab*1" fornecerá resultados incluindo "Laboratório 1".

3) Clique em **Buscar**.

4) Clique na linha do domínio específico para exibir informações detalhadas em um resultado de busca.

6.6.2 Como editar informações de domínio

1) Encontre o domínio a ser editado.

   Consulte *Seção 6.6.1 "Como buscar domínios", página 123*.

2) Na lista de resultados de busca, clique no nome do domínio.

3) Clique em **Editar**.

4) Insira o nome e a descrição do domínio.

5) Clique em **Gravar**.

6.6.3 Como configurar domínios iniciais para objetos novos ou importados

Os objetos novos ou importados são atribuídos ao domínio inicial correspondente.

Existem domínios iniciais para os seguintes objetos:

- chaves
- pessoas (funcionários e visitantes)
- cilindros (e grupos de cilindros)

ATENÇÃO!
Cilindros novos ou importados que pertencem a um grupo de cilindros serão incluídos no domínio do grupo de cilindros, não no domínio do cilindro inicial. Isso significa que todos os cilindros em um grupo de cilindros pertencem ao mesmo domínio. Consulte *Seção 8.2.2 "Domínios", página 173* para obter mais informações sobre domínios.

Os perfis de acesso e os grupos de acesso temporário novos ou importados são atribuídos ao domínio do cilindro inicial.

Cada domínio inicial possui um nome que pode ser editado. O nome padrão é `default`. Os domínios iniciais podem compartilhar o mesmo domínio ou ter domínios diferentes.

Para configurar os domínios iniciais para chaves, pessoas e cilindros:

1) Selecione **Administração » Configurações do sistema**.
2) Clique em **Editar**.
3) Em **ADMINISTRAÇÃO**, clique em **Alterar domínio...** para o domínio inicial específico.

   Será exibida uma lista de domínios para os quais o administrador tem autorização.
4) Clique em **Selecionar** na linha domínio novo.
5) Clique em **Gravar**.

6.6.4 Como criar e apagar domínios

1) Selecione **Administração » Domínios**.
2) Para criar um domínio:
   a) Clique em **Criar Novo**.
   b) Insira **Nome** e um **Descrição** opcional.
   c) Clique em **Gravar**.
3) Para apagar um domínio:

> **ATENÇÃO!**
> Um domínio só poderá ser excluído se não existirem cilindros, grupos de cilindros, funcionários, visitantes ou chaves conectados a ele. Antes de excluir, esvazie o domínio movendo os objetos para outro domínio.
>
> Certifique-se de mover tanto os funcionários ou visitantes ativos como os excluídos para outro domínio. Para encontrar funcionários ou visitantes, consulte *Seção 4.1.1 "Como procurar funcionários ou visitantes", página 23*.

   a) Encontre o domínio e visualize as informações detalhadas.

      Consulte *Seção 6.6.1 "Como buscar domínios", página 123*.
   b) Clique em **Excluir**.
   c) Clique em **OK**.

6.6.5 Como alterar o domínio das chaves

1) Selecione **Informações do sistema » Chaves**.

   Será exibida uma lista de todas as chaves.
2) Para buscar chaves específicas, preencha o critério de busca e clique em **Buscar**.
3) Clique na linha da chave específica.
4) Clique em **Editar**.
5) Clique em **Alterar domínio...**.

   Será exibida uma lista de domínios para os quais o administrador tem autorização.

6) Clique em **Selecionar** na linha domínio novo.

7) Clique em **Gravar**.

O domínio pode ser alterado para diversas chaves simultaneamente. Selecione as chaves na lista do resultado de busca e clique em **Alterar domínio...**.

Consulte também *Seção 8.2.2 "Domínios", página 173*.

6.6.6 Como alterar o domínio de funcionários e visitantes

1) Encontre o funcionário ou visitante a editar.

   Consulte *Seção 4.1.1 "Como procurar funcionários ou visitantes", página 23* para buscar o funcionário ou visitante e exibir a tela informações detalhadas.

2) Clique em **Editar**.

3) Clique em **Alterar domínio...**.

   Será exibida uma lista de domínios para os quais o administrador tem autorização.

4) Clique em **Selecionar** na linha domínio novo.

5) Clique em **Gravar**.

O domínio pode ser alterado para vários funcionários ou visitantes simultaneamente. Selecione os funcionários ou visitantes na lista do resultado de busca e clique em **Alterar domínio...**.

Consulte também *Seção 8.2.2 "Domínios", página 173*.

6.6.7 Como alterar o domínio dos cilindros

Para cilindros que pertencem a um grupo de cilindros, o domínio é alterado no grupo de cilindros. Consulte *Seção 6.6.8 "Como alterar o domínio dos Grupos de cilindros", página 126*.

1) Selecione **Informações do sistema » Cilindros**.

   Será exibida uma lista de todos os cilindros.

2) Para buscar um cilindro específico, preencha o critério de busca e clique em **Buscar**.

3) Clique na linha do cilindro específico.

4) Clique em **Editar**.

5) Clique em **Alterar domínio...**.

   Será exibida uma lista de domínios para os quais o administrador tem autorização.

6) Clique em **Selecionar** na linha domínio novo.

7) Clique em **Gravar**.

O domínio pode ser alterado para diversos cilindros simultaneamente. Selecione os cilindros na lista do resultado de busca e clique em **Alterar domínio...**.

ATENÇÃO!
Recomendamos certificar-se de que um perfil de acesso e todos os cilindros e grupos de cilindros incluídos pertencem ao mesmo domínio. Isto é para assegurar que os administradores para um domínio específico não possam obter acesso indireto a cilindros em outros domínios (por meio dos perfis de acesso).

Consulte também *Seção 8.2.2 "Domínios", página 173*.

6.6.8 Como alterar o domínio dos Grupos de cilindros

Para cilindros que não pertencem a um grupo de cilindros, o domínio é alterado em cada cilindro individualmente. Consulte *Seção 6.6.7 "Como alterar o domínio dos cilindros", página 125*.

1) Selecione **Informações do sistema » Grupos de cilindros**.

   Será exibida uma lista de todos os grupos de cilindros.
2) Para buscar grupos de cilindros específicos, preencha o critério de busca e clique em **Buscar**.
3) Clique na linha do grupo de cilindros específico.
4) Clique em **Editar**.
5) Clique em **Alterar domínio...**.

   Será exibida uma lista de domínios para os quais o administrador tem autorização.
6) Clique em **Selecionar** na linha domínio novo.
7) Clique em **Gravar**.

O domínio pode ser alterado para diversos grupos de cilindros simultaneamente.
Selecione os grupos cilindros na lista do resultado de busca e clique em **Alterar domínio...**.

ATENÇÃO!
Recomendamos certificar-se de que um perfil de acesso e todos os cilindros e grupos de cilindros incluídos pertencem ao mesmo domínio. Isto é para assegurar que os administradores para um domínio específico não possam obter acesso indireto a cilindros em outros domínios (por meio dos perfis de acesso).

Consulte também *Seção 8.2.2 "Domínios", página 173*.

6.6.9 Como alterar o domínio para os perfis de acesso

1) Encontre o perfil de acesso e visualize as informações detalhadas.

   Consulte *Seção 4.6.1 "Como buscar perfis de acesso", página 68*.
2) Na tela de informações detalhadas, clique em **Editar**.
3) Clique em **Alterar domínio**.
4) Clique em **Selecionar** para o domínio novo.
5) Clique em **Gravar**.

ATENÇÃO!
Recomendamos certificar-se de que um perfil de acesso e todos os cilindros e grupos de cilindros incluídos pertencem ao mesmo domínio. Isto é para assegurar que os administradores para um domínio específico não possam obter acesso indireto a cilindros em outros domínios (por meio dos perfis de acesso).

6.7 Como gerenciar papéis e autorizações

ATENÇÃO!
Consulte *Seção 6.11.4 "Como editar as informações de uma chave de comando", página 134* para atribuir papéis a uma chave de comando.

1) Selecione **Administração » Papéis**.

   Será exibida uma lista dos papéis existentes.

   Alguns dos papéis são predefinidos no CWM.

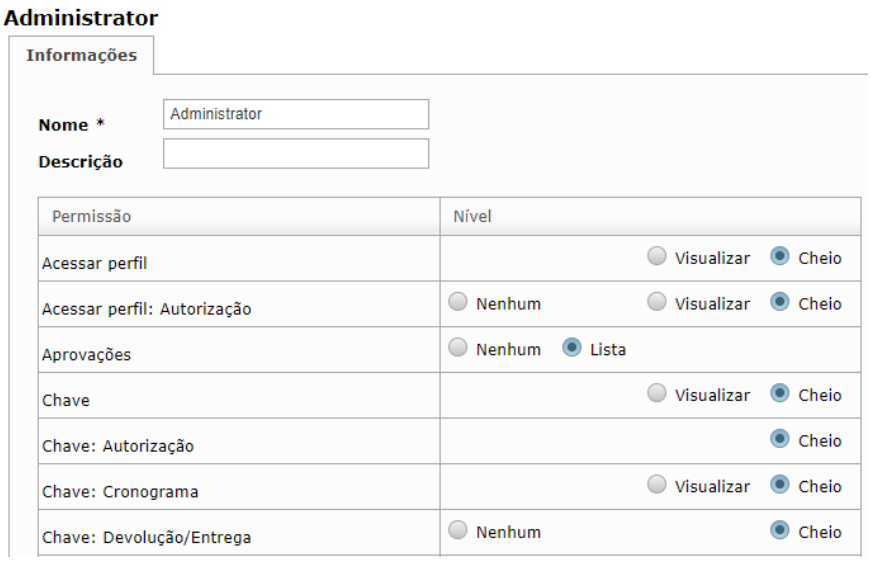
2) **Para criar um papel:**

   1. Clique em **Criar novo**.
   2. Insira o **Nome** e uma **Descrição** possível.
   3. Selecione as autorizações na lista.

ATENÇÃO!
Restrições:

- O acesso a algumas permissões depende do nível de outras permissões. Caso uma permissão específica não possa ser configurada, verifique o nível das permissões relacionadas.
- Se **Administradores hierárquicos** estiver ativado, o administrador não poderá conceder um nível de permissão superior ao seu próprio.

  Por exemplo, um administrador possui o nível **Lista** da permissão **Cilindro**, o administrador não pode autorizar papéis novos do nível **Visualizar** ou **Cheio** da permissão **Cilindro**.



Para editar um papel existente:

ATENÇÃO!
Restrições:

- Um administrador não pode editar seu próprio papel; somente o campo **Descrição** é editável.
- Caso **Administradores hierárquicos** esteja ativado, o administrador não pode editar o papel de um administrador com permissões mais altas.
- Se **Administradores hierárquicos** estiver ativado, o administrador não poderá conceder um nível de permissão superior ao seu próprio.
- Os papéis de **Super administrador**, **Aprovador** e **CLIQ Connect+** são somente leitura e não podem ser editados.

1. Clique na linha do papel específico.
2. Clique em **Editar** para atualizar o **Nome**, **Descrição** ou **Permissão** do papel.
3. Clique em **Gravar**.

Para excluir um papel

ATENÇÃO!
Restrições:

- Papéis associados a um ou mais membros não podem ser excluídos.
- Os papéis de **Super administrador**, **Aprovador** e **CLIQ Connect+** são somente leitura e não podem ser excluídos
- Se **Administradores hierárquicos** estiver ativado, o administrador não poderá excluir papéis um nível de permissão superior ao seu próprio.

1. Clique na linha do papel específico.
2. Clique em **Excluir**.
3. Clique em **OK**.

Para visualizar membros de chave de comando de um papel

1. Clique na linha do papel específico.
2. Selecione a guia **Membros**.

Consulte também:

- *Seção 8.8 "Papéis e autorizações do CWM", página 187*
- *Seção 9.4 "Permissões", página 201*

6.8 Como importar informações do funcionário

As informações do funcionário a serem importadas devem ser armazenadas em um arquivo CSV seguindo certas especificações. Consulte *Seção 9.9 "Formato de arquivo de*

importação de funcionário", página 211. As especificações exatas estão sujeitas a alterações e, portanto, recomendamos carregar o arquivo para validação.

ATENÇÃO!
Os seguintes funcionários não são adicionados ou atualizados no CWM durante o processo de importação:

- Funcionários desativados.
- Funcionários integrados no LDAP.

1) Selecione **Administração » Importar funcionários**.
2) Clique em **Selecionar** para encontrar o arquivo gravado localmente no computador.
3) Clique em **Abrir**.
4) Clique em **Carregar** para validar o arquivo.

   São exibidas as informações sobre quantas entradas válidas o arquivo contém. Se o arquivo não seguir as especificações, a importação não é possível.
5) Clique em **Importar** para importar o arquivo válido.

6.9 Como gerenciar modelos de recibo

O texto do modelo e o logo nos recibos de entrega e devolução podem ser criados e editados. Os recibos são criados no formato PDF que podem ser impressos ou gravados.

ATENÇÃO!
Para gerenciar os modelos de recibos, o nível de permissão do usuário deverá ser **Cheio** no papel **Modelos de recibo**. Consulte *Seção 6.7 "Como gerenciar papéis e autorizações", página 127* para alterar o nível de permissão.

6.9.1 Como criar um modelo de recibo

É possível adicionar modelos de recibos novos no sistema e configurá-los no modelo padrão ou não.

1) Selecione **Administração » Modelos de recibo**.

   Será exibida a lista de modelos de recibos.
2) Clique em **Criar novo** que está localizado embaixo da lista.
3) Insira os seguintes campos:

   - **Nome**: é usado como nome do modelo.
   - **Tipo**: selecione **Entrega** ou **Devolver**.
   - **Padrão para**: se o modelo criado é usado como padrão, selecione uma ou ambas as caixas.
   - **Idioma**: selecione o idioma adequado na lista suspensa.
   - **Cargo**: é impresso no recibo como o cabeçalho do conteúdo.
4) Selecione o logotipo:

- Logotipo do sistema: O logotipo padrão da organização. Consulte *Seção 6.9.3 "Como alterar o logotipo do sistema", página 131* para alterar o logotipo do sistema.
- Logotipo personalizado: Um logotipo separado da empresa em vez do logotipo do sistema.

  a) Selecione **Usar o logotipo personalizado**.

  b) Clique em **Selecionar**.

  c) Clique em **Selecionar...** e selecione o arquivo.

  A imagem a ser carregada deve ter menos de 2 MB e estar no formato JPEG, JPG, PNG, BMP ou GIF.

  d) Clique em **Carregar**.

  O logotipo aparece na tela pop-up.

  e) Clique em **Fechar** para sair.

5) Insira as sentenças na caixa **Texto**.

Recomendamos clicar em **Use o texto padrão** e editar o conteúdo ao criar um modelo novo baseado no texto padrão.

A caixa de texto possui botões de edição básicos para formatar os textos. Clique no botão e comece a digitar para aplicar esses estilos a um texto novo. Para aplicar esses estilos a um conteúdo existente no editor selecione o texto e clique no botão adequado. As tabelas abaixo mostram a lista de botões disponíveis.

B	Negrito
I	Itálico
U	Sublinhado
~~S~~	Tachado
x^2	Sobrescrito
x_2	Subscrito
	Lista sem classificação
	Lista com classificação
H1	Cabeçalho de 1° nível
H2	Cabeçalho de 2° nível
T_x	Excluir formatação

6) Opcional: Clique em **Visualizar modelo** para verificar o recibo.

7) Clique em **Gravar**.

6.9.2 Como editar um modelo de recibo

1) Selecione **Administração » Modelos de recibo**.

Será exibida a lista de modelos de recibos.

2) Clique no modelo a ser editado.

3) Clique em **Editar**.

4) Edite os seguintes campos:

- **Nome**: é usado como nome do modelo.
- **Tipo**: selecione **Entrega** ou **Devolver**.
- **Padrão para**: se o modelo sendo editado é usado como padrão, selecione uma ou ambas as caixas.
- **Idioma**: selecione o idioma adequado na lista suspensa.
- **Cargo**: é impresso no recibo como o cabeçalho do conteúdo.

5) Editar o logotipo:
   - Consulte *Seção 6.9.3 "Como alterar o logotipo do sistema", página 131* para alterar o logotipo do sistema.
   - Para alterar o logotipo personalizado, clique em **Selecionar** para carregar o novo logotipo.
6) Edite as sentenças na caixa **Texto**.

   Consulte *Seção 6.9.1 "Como criar um modelo de recibo", página 129* e *Passo 5* para obter mais informações sobre como formatar os textos.
7) Opcional: Clique em **Visualizar modelo** para verificar o recibo.
8) Clique em **Gravar**.

6.9.3 Como alterar o logotipo do sistema

Os modelos de recibos contêm o logotipo da marca como padrão mas é possível personalizar o logotipo padrão.

Pré-requisitos:

- O logo é um arquivo de imagem com perfil de cores RGB (CMYK não é suportado).
- O logotipo deve ter menos que 2 MB. O tamanho recomendado é de aproximadamente 120 x 60 pixels.

1) Selecione **Administração » Modelos de recibo**.
2) Clique em **Alterar logotipo do sistema** que fica embaixo da lista.
3)
   - Para alterar o logo personalizado:
     a) Clique em **Selecionar...**.
     b) Selecione o arquivo a ser carregado e clique em **Abrir**.
     c) Clique em **Carregar**.
   - Clique em **Recuperar padrão** para alternar para o logo padrão.
4) Clique em **Fechar**.

6.9.4 Como excluir um modelo de recibo

1) Selecione **Administração » Modelos de recibo**.

   Será exibida a lista de modelos de recibos.
2) Clique no modelo a ser excluído.
3) Clique em **Excluir**.
4) Na janela pop-up, clique em **OK**.

6.10 Como gerenciar Modelos de cronograma

Há dois tipos de modelos de cronograma: **Modelo básico** e **Modelo de intervalo de tempo múltiplo**.

- Um modelo básico permite a definição de um intervalo de tempo por dia da semana.
- Um modelo de vários intervalos de tempo permite que os dias e os intervalos de tempo sejam definidos livremente. Vários intervalos de tempo podem ser definidos para o mesmo dia da semana.

Os dois modelos são suportados por versões de firmware de chave diferentes. Para obter informações sobre qual versão de firmware de chave suporta qual tipo de modelo, consulte *Seção 9.7 "Função dependente do firmware", página 209*.

1) Selecione **Administração » Modelos de cronograma**.
2) Para criar um modelo de Cronograma básico:
   a) Clique em **Criar modelo básico**.

      Por padrão, os intervalos de tempo são configurados para o dia inteiro.
   b) Insira **Nome** e um **Descrição** opcional.
   c) Para alterar os intervalos de tempo padrão, clique em **Editar** na linha do dia específico.
   d) Selecione **O dia inteiro**, **Nunca** ou **Personalizar**.
   e) Se for selecionada a opção personalizar, preencha os valores de intervalos **A partir do horário** e **Para horário**.
   f) Clique em **Gravar**.

      Se necessário, repita *Passo 2 c* - *Passo 2 f* nos outros dias.
   g) Clique em **Gravar**.
3) Para criar um modelo de cronograma de intervalo de tempo múltiplo:
   a) Clique em **Criar modelo de intervalo de tempo múltiplo**.
   b) Insira **Nome** e um **Descrição** opcional.
   c) Clique em **Adicionar período**.
   d) Preencha os valores de intervalos **A partir da data** e **Até a data**.
   e) Preencha os valores de intervalos **A partir do horário** e **Para horário**.
   f) Clique em **Gravar**.
   g) Adicione mais intervalos conforme a necessidade.
   h) Clique em **Gravar**.
4) Para editar um modelo:
   a) Clique na linha do modelo específico.
   b) Clique em **Editar**.
   c) Atualize os campos e clique em **Gravar**.
5) Para apagar um modelo:
   a) Clique na linha do modelo específico.

b) Clique em **Excluir**.

c) Clique em **OK**.

Consulte também *Seção 8.1.8 "Cronogramas de chaves", página 170*.

6.11 Como gerenciar Chaves de comando

6.11.1 Como buscar chaves de comando

1) Selecione **Administração » Chaves de comando**.
2) Insira o critério de busca.

   Ao digitar nos campos de busca, o CWM aceita a primeira parte de uma cadeia de caracteres de busca bem como um asterisco (*). Se a busca for para "Laboratório 1", escrever "Lab", "*1" ou "Lab*1" fornecerá resultados incluindo "Laboratório 1".
3) Clique em **Buscar**.
4) Clique na linha da chave de comando específica para exibir informações detalhadas em um resultado de busca.

   Consulte *Seção 9.3.4 "Atributos da chave de comando", página 199* para obter informações sobre os atributos da chave de comando.

6.11.2 Como escanear uma chave de comando

1) Insira a chave de comando na ranhura direita do Programador local.

   ATENÇÃO!
   A chave de comando usada para login deve permanecer na ranhura esquerda do Programador local.

2) Clique em no canto superior direito da página.

   Ambas as chaves de comando no Programador local são mostradas abaixo da barra de navegação.

6.11.3 Como visualizar o status da chave de comando

1) Insira a chave de comando para visualização na ranhura direita do Programador local.

   ATENÇÃO!
   A chave de comando usada para login deve permanecer na ranhura esquerda do Programador local.

2) Clique em no canto superior direito da página.

   Ambas as chaves no Programador local são mostradas abaixo da barra de navegação.

3) Clique na chave de comando na ranhura direita do Programador local.

A tela das informações detalhadas da chave de comando é exibida, com **Nome** e **Marcação** da chave de comando mostrados no lado direito da página.

4) Clique em **Obter status da chave**.

São exibidas informações básicas sobre a chave de comando na ranhura direita. Para obter mais informações sobre o indicador de status da bateria, consulte *Seção 9.6 "Indicações do nível da bateria", página 209*.

6.11.4 Como editar as informações de uma chave de comando

1) Encontre a chave de comando e vá para sua tela de informações detalhadas.

Consulte *Seção 6.11.1 "Como buscar chaves de comando", página 133* para buscar a chave de comando e exibir a tela informações detalhadas.

Para escanear a chave de comando no Programador local e exibir as informações detalhadas, consulte *Seção 6.11.2 "Como escanear uma chave de comando", página 133*

2) Clique em **Editar**.

- Para editar o nome da chave de comando, atualize o campo **Nome**.
- Para bloquear a chave de comando, selecione **Bloquear**.
- Para alterar se o registro do certificado for permitido, selecione **Sempre permitida**, **Permitida uma vez** ou **Não permitida**.

  Consulte também *Seção 8.11 "Integração DCS", página 190*.
- Para atribuir ou alterar papéis de autorização de uma chave de comando, selecione um ou mais papéis.

ATENÇÃO!

Restrições:

- Não é possível alterar o papel da chave de comando que está sendo usada para fazer login.
- O papel de aprovador não pode ser combinado com outros papéis.
- Se **Administradores hierárquicos** estiver ativado, o administrador não poderá atribuir papéis um nível de permissão superior ao seu próprio.

3) Clique em **Gravar**.

6.11.5 Como selecionar domínios da Chave de comando

1) Encontre a chave de comando e vá para sua tela de informações detalhadas.

   Consulte *Seção 6.11.1 "Como buscar chaves de comando", página 133* para buscar a chave de comando e exibir a tela informações detalhadas.

   Para escanear a chave de comando no Programador local e exibir as informações detalhadas, consulte *Seção 6.11.2 "Como escanear uma chave de comando", página 133*

2) Encontre a Chave de comando.

   Consulte *Seção 6.11.1 "Como buscar chaves de comando", página 133* para buscar a chave de comando e exibir a tela informações detalhadas.

   Para escanear a chave de comando no Programador local e exibir as informações detalhadas, consulte *Seção 6.11.2 "Como escanear uma chave de comando", página 133*

3) Selecione a guia **Autorizações do domínio**.
4) Clique em **Editar** para alterar os domínios.
5) Para adicionar domínios:
   a) Clique em **Adicionar domínio...**.

      A lista dos resultados de busca exibe todos os domínios.

   b) Para filtrar os domínios, insira o critério de busca e clique em **Buscar**.
   c) Clique em **Selecionar** para os domínios a adicionar ou clique em **Selecionar todos**.
   d) Clique em **Finalizado**.
6) Para remover um domínio, clique em **Remover** para o domínio a remover ou clique em **Remover todos**.
7) Clique em **Gravar**.

   A alteração do domínio se efetivará no próximo acesso.

6.11.6 Como visualizar eventos de uma chave de comando

A guia Eventos é usada para rastrear algumas operações do administrador no CWM, como quando a Chave de comando foi entregue.

1) Encontre a chave de comando e vá para sua tela de informações detalhadas.

Consulte *Seção 6.11.1 "Como buscar chaves de comando", página 133* para buscar a chave de comando e exibir a tela informações detalhadas.

Para escanear a chave de comando no Programador local e exibir as informações detalhadas, consulte *Seção 6.11.2 "Como escanear uma chave de comando", página 133*

2) Selecione a guia **Eventos**.

Será exibida uma lista com todos os eventos da chave de comando.

6.11.7 Como fazer a entrega das chaves de comando

Pré-requisito:

- O administrador está totalmente autorizado a essa permissão; **Chave de comando: Devolução/entrega**.
- O funcionário que recebe uma chave de comando deve ter um endereço de e-mail válido.

1) Encontre a chave de comando e vá para sua tela de informações detalhadas.

Consulte *Seção 6.11.1 "Como buscar chaves de comando", página 133* para buscar a chave de comando e exibir a tela informações detalhadas.

Para escanear a chave de comando no Programador local e exibir as informações detalhadas, consulte *Seção 6.11.2 "Como escanear uma chave de comando", página 133*

2) Clique em **Entregar ao funcionário**.

A lista de funcionários é exibida.

3) Selecione o funcionário na lista e clique em **Selecionar**.

Um e-mail é enviado para o endereço de e-mail registrado do funcionário, contendo instruções sobre onde fazer o download do CLIQ Connect no computador e a URL do Sistema Cliq.

Para ser possível entrar no CWM, o funcionário deve instalar um certificado para a chave. Consulte *Seção 3.2 "Como inscrever e instalar Certificados da chave de comando", página 15* para obter mais informações sobre como instalar o certificado.

Dica
É altamente recomendável que o funcionário altere o PIN da chave de comando. Para obter instruções, consulte *Seção 6.11.11 "Como alterar o código PIN da Chave de comando", página 139*.

6.11.8 Como fazer a devolução das chaves de comando

Pré-requisito:

- O administrador está totalmente autorizado a essa permissão; **Chave de comando: Devolução/entrega**.

1) Encontre a chave de comando e vá para sua tela de informações detalhadas.

Consulte *Seção 6.11.1 "Como buscar chaves de comando", página 133* para buscar a chave de comando e exibir a tela informações detalhadas.

Para escanear a chave de comando no Programador local e exibir as informações detalhadas, consulte *Seção 6.11.2 "Como escanear uma chave de comando", página 133*

2) Clique em **Entregar a chave de comando**.

A Chave de comando não poderá mais ser usada para entrar no CWM.

6.11.9 Como comunicar e bloquear uma chave de comando perdida

1) encontre a chave de comando e exiba a tela informações detalhadas.

Consulte *Seção 6.11.1 "Como buscar chaves de comando", página 133*.

2) Clique em **Comunicar como perdido**.

3) As chaves de comando perdidas que contêm funções de programação do cilindro precisam ser bloqueadas para evitar a programação não autorizada de cilindros.

- Para bloquear uma chave de comando que contenha funções de programação do cilindro, selecione os cilindros nos quais a chave de comando será bloqueada:
  - Selecione **Todos os cilindros** ou **Apenas instalados** e vá para *Passo 6*.
  - Selecione **Seleção personalizada** e vá para *Passo 4* para selecionar os cilindros.
- Para informar a perda da chave de comando sem bloquear nenhum cilindro, selecione **Nenhum cilindro**, clique em **Próximo** e continue para *Passo 9*.

4) Clique em **Próximo**.

5) Selecione os cilindros para os quais a chave de comando perdida será bloqueada.

6) Clique em **Próximo**.

7) Opcional: Selecione a chave de programação do cilindro na lista, clicando em **Selecionar**.

> **ATENÇÃO!**
> Se esse processo for ignorado, serão criadas funções de programação de cilindros para as chaves de comando.

Na guia **Buscar**, selecione **Todos os tipos e status** para mostrar as chaves de comando.

Na guia **Avançado**, em **Tipo**, selecione chaves de usuário ou chaves de comando para alterar o que é mostrado na lista.

> **ATENÇÃO!**
> A chave de programação do cilindro deve ter memória suficiente.

8) Na página de confirmação, selecione o nível de prioridade em **Prioridade**.

As funções urgentes deverão ter um nível de prioridade alto.

9) Depois de verificar todas as informações, clique em **Comunicar como perdido**.

- Se **nenhum** trabalho for criado para bloquear a chave de comando perdida, os programas atribuídos à chave de comando perdida serão cancelados e listados em **Tarefas » Programação do cilindro**.
- Se forem criadas funções para bloquear a chave de comando perdida, a chave usada para o bloqueio também herdará as funções de bloqueio de cilindro originalmente atribuídas à chave de comando perdida. Outras funções de programação do cilindro que foram originalmente atribuídas à chave de comando perdida são canceladas e listadas em **Tarefas » Programação do cilindro**.

AVISO!
Por padrão, mesmo que nenhuma função de programação de cilindro seja criada para bloquear a chave de comando perdida, a chave de comando perdida ainda é adicionada no CWM à lista de **Chaves não autorizadas** para os cilindros afetados. No entanto, essas informações não são visíveis no CWM. Se esses cilindros forem reprogramados ou substituídos posteriormente, as informações sobre chaves não autorizadas armazenadas no CWM serão aplicadas a esses cilindros, bloqueando, de fato, a chave de comando perdida. Portanto, mesmo que a chave de comando perdida seja comunicada como encontrada posteriormente, ela ainda será bloqueada por qualquer cilindro reprogramado ou substituído.

Para reautorizar a chave de comando encontrada nessa lista de acesso ao cilindro, consulte *Seção 4.9.2 "Como configurar autorizações em cilindros", página 80*.

Para alterar essa configuração padrão, **Bloqueia silenciosamente chaves perdidas no cilindro durante a atualização da autorização** precisa ser desligado. Consulte *Seção 6.4 "Como editar as configurações do sistema", página 99*.

10)
- Se uma chave específica **NÃO** foi selecionada para programar os cilindros, continue a partir de *Passo 4* em *Seção 4.4.13 "Como programar os cilindros", página 61*.
- Se uma chave específica foi selecionada para programar os cilindros, siga as instruções abaixo.

11) Vá para a tela de informações da chave de usuário selecionada.

Dica
Clicar em **Marcação da chave** em **Como bloquear as informações da chave** leva diretamente à tela de informações.

12) Vá para a guia **Programas** e confirme se a função do cilindro está atribuída à chave.

13)
- **Programação no PD local**

  Insira a chave de usuário na ranhura direita do PD local e remova a chave de comando da ranhura esquerda do PD local.
- **Programação em um PD de parede**

  Insira a chave de usuário em um PD de parede.

A função de programação do cilindro é gravada automaticamente na chave de usuário.

14) Reprograme cada cilindro usando a chave de usuário.

15) Depois de programar os cilindros, comunique as funções concluídas do cilindro inserindo a Chave de usuário em um dos seguintes dispositivos:

- A ranhura direita do PD local (remova a chave de comando da ranhura esquerda)
- Um PD de parede

Depois de encontrar a chave de comando, informe-a clicando em **Comunicar como encontrado** na tela de informações detalhadas.

6.11.10 Como comunicar uma chave de comando quebrada ou operacional

1) encontre a chave de comando e exiba a tela informações detalhadas.

   Consulte *Seção 6.11.1 "Como buscar chaves de comando", página 133*.

2) **Para informar a quebra**

   1. Clique em **Informar a quebra**.
   2. Clique em **OK**.

   Para relatar operacional

   1. Clique em **Relatar operacional**.
   2. Clique em **OK**.

6.11.11 Como alterar o código PIN da Chave de comando

ATENÇÃO!
O código PIN deve ter seis caracteres. Os caracteres abaixo são permitidos:

- Maiúsculas (A, B, C, ...)
- Minúsculas (a, b, c, ...)
- Dígitos (0, 1, 2, ...)
- Menos (-)
- Sublinhado (_)
- Espaço ( )
- Especiais (!, $, %, &, ...)
- Parênteses ([,], {, }, (,), <, >)

Não são permitidos caracteres que não sejam ingleses.

1) Para alterar o PIN de qualquer Chave de comando normal usando a Chave de comando mestre com papel de Super administrador:

   a) Selecione **Administração » Chaves de comando**.

   b) Insira a chave de comando na porta direita do Programador local.

   c) Clique em **Escanear**.

d) Clique em **Mostrar** na Chave de comando.

e) Clique em **Definir novo PIN**.

f) Insira **PIN da chave de comando mestre**.

g) Insira um novo PIN no **Novo PIN**.

h) Insira o novo PIN novamente no **Confirmar o novo PIN**.

2) Para alterar o PIN de uma chave de comando normal da mesma chave usada para fazer o login:

a) Selecione **Configurações » Configurações da chave de comando**.

b) Clique em **Alterar PIN da chave de comando**.

c) Insira **PIN atual**.

d) Insira **Novo PIN**.

e) Insira um novo PIN no **Confirmar o novo PIN**.

3) Clique em **OK**.

6.11.12 Como destravar Chaves de comando

Após 5 tentativas de acesso com o PIN errado, a chave de comando ficará travada e deverá ser destravada inserindo o código PUK fornecido pelo fornecedor CLIQ. Consulte *Seção 6.11.12.1 "Como desbloquear chaves de comando usando o código PUK", página 140* para obter mais informações.

ATENÇÃO!
Após 25 tentativas de inserir o número PUK errado, a chave de comando se torna inutilizada e deverá ser substituída por uma chave de comando nova.

Se o administrador não possui o código PUK, o proprietário da chave de comando mestre pode desbloquear a chave de comando. Consulte *Seção 6.11.12.2 "Como desbloquear chaves de comando usando a chave de comando mestre", página 140* para obter mais informações.

6.11.12.1 Como desbloquear chaves de comando usando o código PUK

1) Selecione **Configurações » Configurações da chave de comando**.

2) Clique em **Desbloquear chave de comando**.

3) Insira **PUK**.

Se o administrador não possui o código PUK, entre em contato com o proprietário da chave de comando mestre.

4) Insira **Novo PIN**.

5) Insira **Confirmar o novo PIN**.

6) Clique em **OK**.

6.11.12.2 Como desbloquear chaves de comando usando a chave de comando mestre

O procedimento abaixo só pode ser executado pelo proprietário da chave de comando mestre.

1) Insira a chave de comando a ser desbloqueada na ranhura direita do programador local.

2) Encontre a chave de comando e vá para sua tela de informações detalhadas.

   Consulte *Seção 6.11.1 "Como buscar chaves de comando", página 133* para buscar a chave de comando e exibir a tela informações detalhadas.

   Para escanear a chave de comando no Programador local e exibir as informações detalhadas, consulte *Seção 6.11.2 "Como escanear uma chave de comando", página 133*

3) Clique em **Definir novo PIN**.

4) Insira o **PIN da chave de comando mestre**, o **Novo PIN** e **Confirmar o novo PIN** para a chave de comando bloqueada.

5) Clique em **OK** para gravar.

   O novo PIN está programado na chave de comando na ranhura direita do programador.

6.11.13 Ativar ou desativar a recuperação automática das trilhas de auditoria para a chave de comando

Pré-requisitos:

- O administrador tem permissão de ativar as trilhas de auditoria automáticas.
- Uma chave de comando geração 2 com firmware versão 12.6 ou superior.
- Para ativação, o recurso **Aprovações** deve ser desligado em **Configurações do sistema**.

1) Encontre a chave de comando e vá para sua tela de informações detalhadas.

   Consulte *Seção 6.11.1 "Como buscar chaves de comando", página 133* para buscar a chave de comando e exibir a tela informações detalhadas.

   Para escanear a chave de comando no Programador local e exibir as informações detalhadas, consulte *Seção 6.11.2 "Como escanear uma chave de comando", página 133*

2) Encontre a configuração de **RECUPERAÇÃO AUTOMÁTICA DAS TRILHAS DE AUDITORIA**.

3) - Para ativar a configuração de recuperação de trilhas de auditoria automática: Clique em **Ativar**.
   - Para desativar a configuração de recuperação de trilhas de auditoria automática: Clique em **Desativar**.

4) Se a chave de comando está no programador local, clique em **Atualizar a chave de comando localmente**.

6.11.14 Como listar certificados de chaves de comando

1) Encontre a chave de comando e vá para sua tela de informações detalhadas.

   Consulte *Seção 6.11.1 "Como buscar chaves de comando", página 133* para buscar a chave de comando e exibir a tela informações detalhadas.

   Para escanear a chave de comando no Programador local e exibir as informações detalhadas, consulte *Seção 6.11.2 "Como escanear uma chave de comando", página 133*

2) Selecione a guia **Certificados**.

A **Última data usada** para cada certificado é exibida se a configuração **Obter última data de acesso** estiver ativada. Consulte *Seção 6.4 "Como editar as configurações do sistema", página 99*.

6.11.15 Como revogar certificados de chaves de comando

A revogação de certificados de chave de comando é um recurso de segurança e usado, tipicamente, quando o computador de um administrador com um certificado de chave de comando é roubado, porém a chave de comando permanece segura. No exemplo com o computador roubado, o certificado da chave de comando instalado é revogado e depois inscrito novamente.

Consulte *Seção 3.2 "Como inscrever e instalar Certificados da chave de comando", página 15* para inscrever um certificado de chave de comando.

1) Encontre a chave de comando e vá para sua tela de informações detalhadas.

   Consulte *Seção 6.11.1 "Como buscar chaves de comando", página 133* para buscar a chave de comando e exibir a tela informações detalhadas.

   Para escanear a chave de comando no Programador local e exibir as informações detalhadas, consulte *Seção 6.11.2 "Como escanear uma chave de comando", página 133*

2) Selecione a guia **Certificados**.

3) Clique em **Revogar certificado** para cada certificado a ser revogado.

   Dica
   Para saber qual certificado a ser inscrito, olhe na coluna **Última data usada**. Caso tenha dúvida, revogue todos os certificados e inscreva-os novamente.

   ATENÇÃO!
   Não é possível revogar o certificado que foi usado para entrar no Sistema Cliq.

4) Clique em **OK**.

6.11.16 Como substituir uma Chave de comando mestre

Caso uma Chave de comando mestre seja perdida ou quebrada, deverá ser solicitada uma nova.

Siga estas instruções para registrar uma Chave de comando mestre nova e bloquear a chave de comando mestre perdida ou quebrada.

Pré-requisitos:

- O seguinte está disponível:
  - Uma chave de comando mestre nova juntamente com o código PIN.
  - Um certificado para a chave de comando mestre nova caso o DCS não esteja integrado.
  - Um arquivo de importação contendo a chave de comando mestre nova.

1) Instale o certificado da Chave de comando mestre.

Consulte *Seção 5.2 "Como instalar o certificado da chave de comando mestre.", página 95*.

2) Trave o CWM para manutenção.

   Consulte *Seção 6.2 "Como travar o sistema para manutenção", página 98*.

3) Importe o arquivo contendo a Chave de comando mestre nova usando a Ferramenta de manutenção CLIQ Web Manager. Para obter mais informações, consulte a Documentação de operação e manutenção do CWM.

   CUIDADO!
   Faça o login com a Chave de comando mestre nova imediatamente após importar o arquivo.

   Até que a Chave de comando mestre nova não tenha se conectado, a Chave de comando mestre antiga ainda poderá ser usada e, se usada para conectar, bloquear a Chave de comando mestre nova.

4) Faça o login no CWM usando a Chave de comando mestre nova.

   O CWM detecta que existe mais de uma Chave de comando mestre ativa e bloqueia automaticamente a outra chave de comando mestre e a marca como Perdida.

   A Chave de comando mestre ainda poderá ser usada para executar qualquer Tarefa de programação de cilindro já armazenada na chave, em cilindros em que está autorizada. O CWM agora fornece a opção de criar Tarefas de programação de cilindro para autorizar os cilindros da Chave de comando mestre bloqueada.

5) Clique em **Sim, criar programas agora** ou **Não, decidir mais tarde**.

Para criar tarefas de desautorização mais tarde, faça o login com a Chave de comando mestre nova e clique em **Crie tarefas de desautorização** a partir da tela de informações detalhadas da Chave de comando mestre bloqueada.

6.11.17 Como exportar informações da chave de comando

1) Faça a busca das chaves de comando.

   Consulte *Seção 6.11.1 "Como buscar chaves de comando", página 133*.

2) A partir dos resultados da busca, selecione as chaves de comando cujos dados devem ser exportados marcando as caixas de seleção.

3) Clique em **Exportar para arquivo CSV**.

4) Na janela pop-up de download do arquivo, clique em **Gravar**.

   O download de um arquivo CSV é feito na pasta **Downloads**.

   ATENÇÃO!
   Para ser possível abrir o arquivo em Excel da maneira correta, o delimitador para o arquivo deverá ser configurado de acordo com as configurações regionais. Consulte *Seção 6.4 "Como editar as configurações do sistema", página 99* para alterar o delimitador.

6.12 Como alterar o grupo de cilindros para cilindros

ATENÇÃO!
Alguns cilindros na lista de cilindros podem representar uma Saída livre potencial em uma programador de parede, que está conectado a um dispositivo externo, por exemplo, um controlador de relé. Nesse caso, não é possível realocar esses cilindros a outro grupo de cilindros.

Entre em contato com o representante local CLIQ para obter mais informações sobre a Saída livre.

1) Encontre o cilindro e visualize as informações detalhadas.

   Consulte *Seção 4.4.1 "Como buscar por cilindros", página 54*.

2) Clique em **Alterar grupo**.
3) Clique em **Selecionar** na linha do grupo de cilindros específico.
4) Selecione uma **Prioridade**. As funções urgentes deverão ter um nível de prioridade alto.

O grupo de cilindros pode ser alterado para diversos cilindros simultaneamente. Selecione os cilindros na lista do resultado de busca e clique em **Alterar grupo...**.

6.13 Como visualizar o status do sistema

1) Selecione **Administração » Status do sistema**.
2) Selecione a guia **Status atual** para visualizar online ou off-line os status dos Programadores remotos, do servidor remoto e do servidor de e-mail.
3) Selecione a guia **Histórico** para visualizar as alterações anteriores online ou off-line nos status dos Programadores remotos, do servidor remoto e do servidor de e-mail.

   Para visualizar eventos passados entre certas datas:

   a) Preencha a data de início em **Mostrar eventos a partir de**.
   b) Preencha a data final em **Mostrar eventos até**.
   c) Clique em **Buscar**.

6.14 Como visualizar estatísticas básicas

O CWM possui uma função de estatísticas embutida que fornece as estatísticas básicas do Sistema Cliq, como número de cilindros e chaves.

Pré-requisito:

- O administrador possui permissão para visualizar **Estatísticas**.

1) Selecione **Administração » Estatísticas**.
2) A página **Estatísticas** será aberta.
3) Opcional: clique em **Imprimir estatísticas** ou **Exportar estatísticas** caso necessário.

6.15 Como atualizar o firmware

A versão do firmware pode ser verificada na tela de informações detalhadas de cada equipamento.

6.15.1 Como atualizar o firmware para programadores remotos

> **ATENÇÃO!**
> Este capítulo não se aplica ao programador móvel CLIQ Connect.

Para atualizar um programador remoto, o CWM deve possuir o firmware. Ao usar a integração DCS, os arquivos de firmware são enviados automaticamente do DCS. Em outros contextos, isso é feito carregando um arquivo de firmware local fornecido pelo fornecedor local CLIQ. Depois de importado para o CWM, o firmware do programador remoto pode ser atualizado por meio do CWM ou de uma unidade flash USB.

O processo de atualização do firmware do programador remoto difere dependendo da integração DCS.

- Para usar a integração DCS, comece em *Passo 2*.
- Para usar um arquivo firmware local, comece em *Passo 1*.

1) Para carregar e importar um arquivo de firmware local sem integração DCS:
   a) Grave o firmware novo localmente no computador.
   b) Selecione **Administração » Firmware**.
   c) Clique em **Selecionar** para encontrar o firmware novo gravado no computador.
   d) Clique em **Abrir**.
   e) Clique em **Carregar firmware** para carregar o firmware no CWM.

      O firmware está carregado.
   f) Clique em **Importar firmware** para importar o firmware carregado.

      Caso seja bem sucedido, será exibido um resumo do firmware importado em um painel novo.
2) Selecione **Info do sistema » Programadores remotos**.
3) Clique na linha do Programador remoto a ser atualizado.

4) Selecione a guia **Firmware** e selecione a versão a partir da seção **FIRMWARE** ou **FIRMWARE DE CARREGADOR DE BOOT**.

ATENÇÃO!
A seção **FIRMWARE DE CARREGADOR DE BOOT** não é exibida para o programador de parede geração 2.

5)
- Para atualizar o firmware para Programadores remotos online por meio do CWM:

  a) Selecione a versão do firmware e clique em **Aplicar**.

  b) Ative a atualização.

  - Programadores móveis CLIQ:

    Insira uma chave de usuário para ligar o programador móvel CLIQ.
  - Programadores de parede:

    O firmware será atualizado na próxima pulsação (na próxima vez em que se conectar com o servidor remoto).
- Para atualizar o firmware para Programadores remotos offline por meio de um pen drive:

  ATENÇÃO!
  O pen drive USB deverá estar formatado com o sistema de arquivos FAT32 e o tamanho recomendado da memória é de 8-16 GB para programadores de parede geração 1 e programadores móveis. Não existe restrição no tamanho do pen drive para programadores de parede geração 2. O pen drive não deve conter qualquer outro arquivo.

  a) Selecione a versão do firmware e clique em **Gravar para arquivo** para gravar o arquivo na raiz do pen drive.

  b) Conecte a unidade flash USB ao Programador remoto usando o cabo USB apropriado (consulte *Seção 6.5.8 "Como configurar Programadores móveis", página 115* ou *Seção 6.5.7 "Como configurar programadores de parede", página 109*).

  A atualização inicia automaticamente.

  c) Ative a atualização.

  - Programadores móveis CLIQ:

    Insira uma chave de usuário para ligar o programador móvel CLIQ.

- Programadores de parede:

  A atualização inicia automaticamente.

A atualização do firmware estará concluída quando o LED de indicação de download parar de piscar e permanecer aceso. Consulte *Seção 9.5.1 "Indicações de programador de parede (Geração 1) e programador móvel", página 207* e *Seção 9.5.2 "Indicações de programador de parede (geração 2)", página 208* para obter informações sobre as indicações do Programador remoto.

6.15.2 Como atualizar o firmware para programadores móveis CLIQ Connect

1) Conecte o programador móvel CLIQ Connect ao PC cliente, no qual está instalado o PC CLIQ Connect, usando um cabo micro-USB.
2) O PC CLIQ Connect verificará automaticamente a versão do firmware do programador móvel CLIQ Connect.

   Caso exista uma versão mais nova disponível, o PC CLIQ Connect sugerirá a atualização do firmware.
3) Siga as instruções exibidas na tela.

6.15.3 Como atualizar o firmware em chaves

Para atualizar uma chave, o CWM deve possuir o firmware. Para sistemas com integração DCS, os arquivos de firmware são enviados automaticamente do DCS. Para sistemas sem integração DCS, isso é feito carregando um arquivo de firmware local fornecido pelo fornecedor local CLIQ. Assim que importado, o firmware é atualizado por meio do CWM usando um programador remoto.

Tabela 1. Tipo de programador remoto a ser usado para atualizar chaves

Versão da chave	Programador remoto	Versão do firmware do programador remoto
Chaves de usuário, geração 1	Programador de parede (geração 1)	
Chaves de usuário, geração 2	Programador de parede (geração 1 e 2) ou programador móvel CLIQ	
Chaves de comando, geração 2, com firmware 12.0 ou superior	Programador de parede (geração 1 e 2) ou programador móvel CLIQ	Firmware do programador de parede ou programador móvel CLIQ 6.3 ou superior
Chaves de comando, geração 2, com firmware inferior a 12.0	Não podem ser atualizadas por meio do CWM	
Chaves de comando, geração 1	Não podem ser atualizadas por meio do CWM	

A geração da chave pode ser visualizada nas telas de detalhes da chave de comando e chave de usuário, consulte *Seção 4.2.2 "Como escanear uma chave de usuário", página 35*, *Seção 4.2.1 "Como buscar chaves de usuário", página 34*, *Seção 6.11.2 "Como escanear uma chave de comando", página 133* ou *Seção 6.11.1 "Como buscar chaves de comando", página 133*.

O processo de atualização do firmware da chave difere dependendo da integração DCS.

- Para Sistemas Cliq com integração DCS, vá para *Passo 4*.
- Para Sistemas Cliq sem integração DCS, continue a partir de *Passo 1*.

1) Grave o firmware novo localmente no computador.
2) Selecione **Administração » Firmware**.
3) Como importar o novo firmware:
   a) Clique em **Selecionar** para encontrar o firmware novo gravado no computador.
   b) Clique em **Abrir**.
   c) Clique em **Carregar firmware** para carregar o firmware no CWM.

      Caso seja bem sucedido, será exibido um resumo do firmware carregado em um painel novo.
   d) Clique em **Importar firmware**.

> **ATENÇÃO!**
> Para ser possível atualizar chaves geração 1, o seguinte deve ser importado:
>
> - Firmware do carregador de boot do Programador de parede geração 1
> - Firmware do programador de parede geração 1, versão 2.11 ou superior
> - Firmware de atualização de chave do programador de parede geração 1, versão 2.11 ou superior
> - Firmware da chave nova, um para cada tipo de chave que será atualizada.

> **ATENÇÃO!**
> Para com a integração DCS ativada, os arquivos de firmware são localizados automaticamente a partir do DCS e listado entre os firmwares importados que estão prontos para ativação.

4) Para atualizar chaves de usuário geração 1:

> **ATENÇÃO!**
> Os programadores de parede geração 2 não suportam a atualização do firmware para chaves de usuário geração 1.

   a) Selecione **Informações do sistema » Programadores remotos**.
   b) Encontre o Programador de parede a ser usado para a atualização e visualize as informações detalhadas.

      Consulte *Seção 6.5.2 "Como buscar Programadores remotos", página 104*.

      Entre outros detalhes, são exibidos o firmware do carregador de boot atual e o firmware do Programador de parede.
   c) Se o firmware de carregador de boot do programador de parede e o firmware tiverem que ser atualizados, consulte *Seção 6.15.1 "Como atualizar o firmware para programadores remotos", página 145*.
   d) Ativação de atualizações de chaves no programador de parede, consulte *Seção 6.5.11 "Como ativar e desativar as atualizações de chaves em programadores remotos", página 121*.

O firmware de atualização de chave é enviado para o Programador de parede. Será possível atualizar as chaves quando o Programador de parede tiver carregado o firmware novo e reinicializado.

e) Para cada chave de usuário a ser atualizada:

- Insira a chave no programador de parede com atualização de chave.

  Primeiro, serão executadas as atualizações remotas pendentes para a chave e então a chave será atualizada com o firmware novo.

> **ATENÇÃO!**
> A configuração da chave, incluindo os direitos de acesso, é apagada durante a atualização do firmware. Ela é restaurada executando uma atualização remota da chave após a atualização.

  O Programador de parede indica que as atualizações foram concluídas. Consulte *Seção 9.5.1 "Indicações de programador de parede (Geração 1) e programador móvel", página 207* para obter informações sobre as indicações do Programador remoto.
- Remova a chave do Programador de parede.

  É criada uma nova função de atualização remota para restaurar a configuração de chave no CWM. Ela estará disponível após alguns minutos.
- Insira a chave em qualquer Programador remoto para restaurar a configuração da chave.

  O procedimento de atualização foi concluído para essa chave.

f) Desativação de atualizações de chaves no programador de parede, consulte *Seção 6.5.11 "Como ativar e desativar as atualizações de chaves em programadores remotos", página 121*.

Todas as funções de atualização remota de chaves pendentes são canceladas. O Firmware normal do programador de parede é enviado para o Programador de parede e quando ele tiver sido carregado e reinicializado o programador de parede funcionará como programador normal novamente.

5) Para atualizar chaves de usuário ou chaves de comando geração 2:

a) Selecione **Informações do sistema » Programadores remotos**.

b) Visualize as informações detalhadas para o programador remoto a ser utilizado para a atualização.

Consulte *Seção 6.5.2 "Como buscar Programadores remotos", página 104*.

- Se o firmware do programador remoto necessitar ser atualizado, consulte *Seção 6.15.1 "Como atualizar o firmware para programadores remotos", página 145*.

c) Na guia **Configurações**, ative as atualizações de chaves no programador remoto. Consulte *Seção 6.5.11 "Como ativar e desativar as atualizações de chaves em programadores remotos", página 121*

d) Selecione **Administração » Firmware**.

e) Selecione a guia **Firmware da chave de usuário importado** ou **Firmware da chave de comando importado** dependendo se está atualizando chaves de usuário ou chaves de comando.

f) Clique em **Aplicar** para o firmware importado para atualizar a chave.

Será criada uma função remota automaticamente.

ATENÇÃO!
Se o botão **Aplicar** estiver cinza para o firmware importado significa que existem atualizações remotas pendentes para o firmware existente, que são indicadas por um ícone na coluna **Status**. Faça o seguinte:

- Clique em **Cancelar** para o firmware com atualizações remotas pendentes.
- Clique em **OK**.
- Clique em **Aplicar** para o firmware mais atual.

ATENÇÃO!
A ordem de *Passo 5 c* e *Passo 5 f* pode ser invertida. É possível aplicar primeiro o firmware importado e então ativar as atualizações de chave para uma seleção de programadores remotos.

g) Atualize cada chave em um programador remoto:

ATENÇÃO!
Para chaves de usuário, primeiro serão executadas as atualizações remotas pendentes para a chave e então a chave será atualizada com o firmware novo.

- Via **Programador de parede** ou **Programador móvel CLIQ**

  Insira ou conecte a chave aos dispositivos que foram habilitados para atualização de chaves.

  O Programador remoto indica que as atualizações foram concluídas. Consulte *Seção 9.5.1 "Indicações de programador de parede (Geração 1) e programador móvel", página 207* ou *Seção 9.5.2 "Indicações de programador de parede (geração 2)", página 208* para obter informações sobre as indicações do Programador remoto.

- Sobre **Protocolo Bluetooth no aplicativo CLIQ Connect**

  Pré-requisitos:

  – A versão do firmware do CLIQ Connect deve ser 4.1 ou posterior.
  – A versão do firmware da chave deve ser 16.3.3 ou posterior.

  É possível atualizar o firmware de chaves com firmware mais antigo usando um PD de parede.

  Conecte a chave ao CLIQ Connect.

ATENÇÃO!
Se uma atualização de firmware for iniciada usando o CLIQ Connect e uma conexão BLE, ela deverá ser concluída usando o mesmo método (ou seja, conexão BLE a um dispositivo móvel). Durante o estado intermediário de atualização, a chave parecerá não funcional; ela não abrirá nenhuma fechadura e não responderá em nenhum dispositivo de programação.

6.15.4 Como atualizar informações de firmware da chave no banco de dados CWM

Quando o firmware da chave é atualizado, o banco de dados CWM atualiza automaticamente as informações de firmware da chave. As informações de firmware da chave podem ser visualizadas na tela **Informações da chave**.

Entretanto, se o firmware for atualizado fora do sistema CWM, por exemplo na fábrica, o banco de dados CWM não é atualizado com as informações de firmware da chave mais recentes.

Faça o seguinte para sincronizar as versões de firmware da chave no banco de dados CWM e na chave física:

- Escaneie a chave atualizada e obtenha o status da chave no Programador local. Consulte *Seção 4.2.2 "Como escanear uma chave de usuário", página 35* para obter mais informações.
- Insira a chave atualizada em um Programador remoto.

ATENÇÃO!
Somente chaves geração 2 com versão de firmware 12.3 ou superior podem atualizar as informações de firmware da chave via Programadores remotos.

ATENÇÃO!
Somente chaves de comando:

Se uma chave de comando possui uma versão do firmware mais antiga que a escrita no banco de dados do CWM, então o banco de dados do CWM no firmware não será atualizado. Essa situação também poderá levar a erros ao usar a chave de comando.

6.16 Importação de extensões

Para importar uma extensão, o CWM deve possuir um arquivo de importação de extensão. Isso é feito carregando um arquivo de importação de extensão local.

Ao usar a integração DCS, os arquivos de importação de extensão são automaticamente obtidos do DCS. Inicie o processo de importação de extensão em *Passo 2*.

A obtenção do DCS também pode ser forçada clicando manualmente em um botão. Depois de carregada, a importação de extensão deve ser ativada.

Pré-requisito:

- Se os cilindros recém-adicionados precisarem bloquear as chaves perdidas no sistema, ative **Bloquear chaves perdidas em cilindros novos durante a importação de extensão** em **Configurações do sistema**. Quando ativado, o sistema cria automaticamente funções de programação do cilindro para bloquear chaves perdidas para esses cilindros quando os arquivos de importação de extensão de cilindro são ativados. Para obter mais informações. Consulte *Seção 6.4 "Como editar as configurações do sistema", página 99*.

1) Forneça um arquivo de importação de extensão para o CWM.

Para carregar um arquivo de importação de extensão local

1. Selecione **Administração » Importação de extensão » Carregar ou localizar arquivo(s) de importação de extensão**.
2. Clique em **Selecionar...** para encontrar o arquivo de importação de extensão gravado localmente no computador. Os arquivos de importação de extensão possuem o sufixo ".cws".
3. Clique em **Abrir**.
4. Clique em **Carregar**. O arquivo de importação de extensão é carregado para o Web Manager Server e validado.

Para localizar manualmente um arquivo de importação de extensão a partir do DCS

1. Selecione **Administração » Importação de extensão » Carregar ou localizar arquivo(s) de importação de extensão**.
2. Clique em **Buscar arquivo(s) de importação de extensão**.

   É exibida uma nota de status sobre o processo de localização.

2) Ative um arquivo de importação de extensão carregado ou localizado:

> **ATENÇÃO!**
> Pode levar algum tempo para processar um arquivo de importação de extensão carregado ou localizado. Sempre que uma importação de extensão está pronta para ser ativada, é exibida uma notificação na página inicial do CWM e é enviada por e-mail a todos os administradores que possuem papéis com autorizações de manutenção.

a) Selecione **Administração » Importação de extensão » Ativar importação de extensão**.

   É exibida uma nota sobre as importações de extensões disponíveis, incluindo as informações do número de chaves, grupos de chaves, cilindros e grupos de cilindros e Programadores remotos a serem ativados.

b) Opcional: Para obter informações detalhadas sobre os elementos de extensão, clique em **Exportar para arquivo CSV** para cada elemento para criar um arquivo CSV e confirmar os detalhes no arquivo.

c) Clique em **Ativar importação de extensão** para ativar as extensões disponíveis.

ATENÇÃO!
Somente poderão ser ativadas importações de extensões carregadas ou localizadas que contêm dados novos. Dados antigos ou idênticos não poderão ser ativados.

Uma vez ativada, é exibida uma mensagem de confirmação na página inicial do CWM.

Se a função **Bloquear chaves perdidas em cilindros novos durante a importação de extensão** for ativada, serão criados funções de programação do cilindro. Para programar os cilindros, consulte *Seção 4.4.13 "Como programar os cilindros", página 61*.

7 Hardware CLIQ

7.1 Arquitetura do CLIQ

Figura 1 "Arquitetura do CLIQ", página 154 mostra a arquitetura básica de um sistema CLIQ.

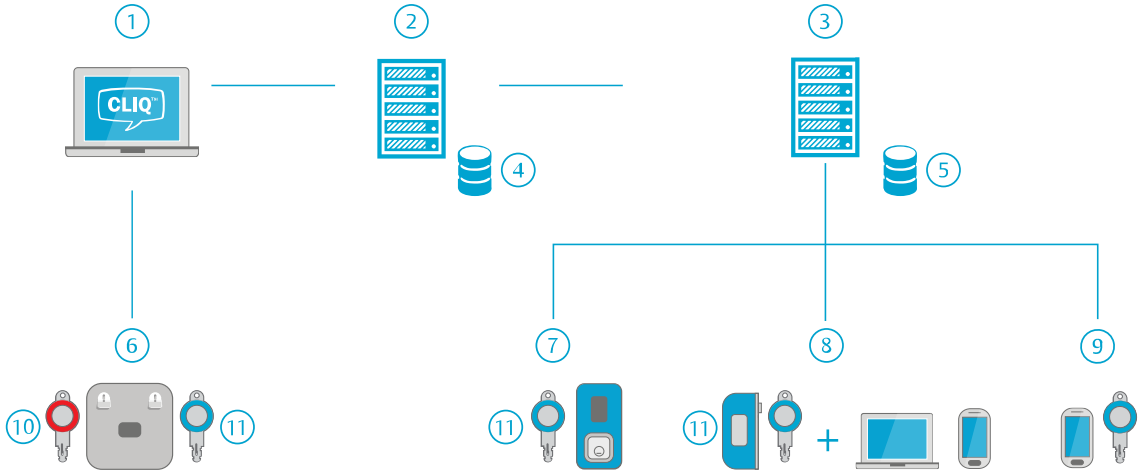


Figura 1. Arquitetura do CLIQ

1. **Cliente CWM**. É um computador com um navegador da Internet usado por um administrador para administrar um Sistema Cliq. Diversos clientes podem ser conectados ao servidor.

2. **Servidor do Web Manager**. Executa o software CWM e está conectado ao banco de dados do CLIQ com informações sobre todos os elementos do CLIQ, listas de acesso, trilhas de auditoria etc.

3. **Servidor remoto**. Em um sistema remoto, o Servidor remoto trata da atualização remota das chaves. As funções de atualização de chaves são enviadas do servidor do Web Manager para o Servidor remoto. As funções de atualização são armazenadas em um banco de dados até que sejam executadas a partir do Programador remoto.

4. **Banco de dados**. Banco de dados do servidor do gerenciador Web.

5. **Banco de dados**. Banco de dados do servidor remoto.

6. **Programadores locais**. Estão conectados ao cliente do Web Manager e são usados pelo administrador para entrar no CWM (usando uma chave de comando) e programar as chaves localmente. Consulte *Seção 7.4.1 "Programadores locais", página 159* para obter mais informações.

7. **Programadores de parede**. Um tipo de programador remoto. Ao inserir uma chave no programador de parede são executadas funções de atualização de chaves armazenadas no banco de dados do Servidor remoto. Consulte *Seção 7.4.2 "Programadores remotos", página 159*.

8. **Programadores móveis CLIQ** e **programadores móveis CLIQ Connect**. Dois tipos de programadores remotos. As funções de atualização da chave armazenadas no banco de dados do servidor remoto serão executadas ao inseri-la em um programador móvel CLIQ ou programador móvel CLIQ Connect. Consulte *Seção 7.4.2 "Programadores remotos", página 159*.

9. **Chaves CLIQ Connect**. Um tipo de chave. Conectando a chave a um equipamento móvel com o CLIQ Connect a chave CLIQ Connect poderá ser atualizada sem usar um programador. Consulte o manual separado do CLIQ Connect.

10. **Chaves de comando**. Consulte *Seção 7.2.4 "Chaves de comando", página 156*.

11. **Chaves de usuário**. Consulte *Seção 7.2.3 "Chaves de usuário", página 155*.

7.2 Chaves

7.2.1 Visão geral das chaves

As chaves CLIQ são chaves eletromecânicas que contêm componentes eletrônicos e uma bateria. Cada chave CLIQ é programada e pode ser controlada e administrada usando o CWM.

As chaves podem ser chaves do sistema, também chamadas de **chaves de comando**, usadas por administradores do Sistema Cliq, ou **chaves de usuário**, usadas por funcionários e visitantes.

7.2.2 Chaves CLIQ Connect

Algumas chaves de comando e chaves de usuário podem ser atualizadas por meio da tecnologia bluetooth usando um telefone celular ou um tablet. Essas chaves são chamadas **chaves CLIQ Connect**. As chaves que não possuem esse recurso só podem ser atualizadas em um programador.

7.2.3 Chaves de usuário

As **Chaves de usuários** são usadas por funcionários e visitantes para acessar as instalações. Existem vários tipos de Chaves de usuários.

	**Chave mecânica**	É uma chave tradicional sem componentes eletrônicos. Podem ser gerenciadas no CWM, porém não podem ser usadas com cilindros CLIQ.
	**Chave normal**	É uma chave eletromecânica que pode abrir cilindros mecânicos quando o corte é compatível e que podem ser autorizadas a abrir cilindros CLIQ com base na lista de acesso do cilindro (consulte *Seção 8.1.2 "Autorização eletrônica", página 163*).

 **Chave Quartz**	Além do descrito acima, esse tipo de chave também possui uma função de relógio de quartzo e pode ser programada para ficar ativa entre certas datas e exigir revalidação (consulte *Seção 8.1.4 "Validade da chave", página 165*). Elas também podem ser programadas para ter acesso a cilindros com base em um cronograma (consulte *Seção 8.1.8 "Cronogramas de chaves", página 170*). Chaves deste tipo também podem armazenar trilhas de auditoria (consulte *Seção 8.6 "Trilhas de auditoria", página 185*).
 **Chave dinâmica**	Além do descrito acima, esse tipo de chave também pode armazenar uma lista de acesso da chave de cilindros e grupos de cilindros que a chave está autorizada a abrir (consulte *Seção 8.1.2 "Autorização eletrônica", página 163*). Isso é útil em sistemas remotos porque permite o controle do acesso pelas chaves, que são atualizadas com facilidade em Programadores remotos.

Uma chave dinâmica e uma chave quartz pode ser uma **chave CLIQ Connect** (ícone direito) ou não (ícone esquerdo). As chaves normais nunca podem ser chaves CLIQ Connect. Consulte *Seção 7.2.2 "Chaves CLIQ Connect", página 155* para obter mais informações.

Consulte também *Seção 8.1 "Princípios de autorização", página 163*.

7.2.4 Chaves de comando

As Chaves de sistema, também chamadas de **Chaves de comando**, são chaves usadas pelos administradores do Sistema Cliq. As chaves de comando não abrem cilindros, porém são usadas somente para acessar o CWM e programar cilindros.

Existem dois tipos de chaves de comando: **Chaves de comando mestres** e **Chaves de comando normais**.

Chave de comando mestre

A Chave de comando mestre é usada pelo Super Administrador para gerenciar o Sistema Cliq. Existe apenas uma Chave de comando mestre por Sistema Cliq e deve ser mantida em um local seguro.

A Chave de comando mestre possui os seguintes direitos específicos que não podem ser fornecidos a qualquer outra Chave de comando:

- Alteração no código PIN de outras chaves de comando.
- Executar Tarefas de programação de cilindros que incluem o acesso atualizado para Chaves de comando.
- Declarar uma chave de comando perdida como achada.

Chave de comando sub-mestre

As chaves de comando sub-mestres são usadas pelos administradores. Pode haver várias chaves de comando sub-mestres em um Sistema Cliq.

Uma chave de comando sub-mestre tem funcionalidade restrita em comparação com a chave de comando mestre. Por exemplo, ela não pode ser usada para ativar importações iniciais e certas configurações do sistema não podem ser definidas.

Chave de comando normal

As Chaves de comando normais são entregues a Administradores. As Chaves de comando normais podem ser configuradas para acessar certas funções no CWM e bloqueadas para outras funções. Consulte *Seção 8.8 "Papéis e autorizações do CWM", página 187*).

Existe um tipo especial de Chave de comando normal que tem o direito de executar a reprogramação de cilindros. Outras Chaves de comando normais não possuem esse direito. Os direitos de reprogramação são programados na chave na fábrica e não podem ser alterados. Para ver se uma Chave de comando normal possui direitos e reprogramação, visualize as informações detalhadas da chave de comando. Consulte *Seção 6.11.1 "Como buscar chaves de comando", página 133* ou *Seção 6.11.2 "Como escanear uma chave de comando", página 133*.

Cada chave de comando normal também pode ser uma **chave CLIQ Connect** (ícone direito) ou não (ícone esquerdo). Consulte *Seção 7.2.2 "Chaves CLIQ Connect", página 155* para obter mais informações.

ATENÇÃO!

O termo **Chave de comando** é usado ao descrever uma funcionalidade que se aplica tanto a Chaves de comando mestres como Chaves de comando normais.

Dependendo do firmware, as Chaves de comando possuem a capacidade de **Programação do grupo de cilindros**. Somente Chaves de comando com essa capacidade podem executar Tarefas de programação de cilindros envolvendo a alteração do grupo de cilindros de um cilindro. Para ver se uma Chave de comando possui capacidade de

programação de grupo de cilindros, visualize as informações detalhadas da chave de comando. Consulte *Seção 6.11.1 "Como buscar chaves de comando", página 133* ou *Seção 6.11.2 "Como escanear uma chave de comando", página 133*. Em sistemas inicialmente fornecidos como sistemas de grupos de cilindros, todas as Chaves de comando possuem essa capacidade.

Para usar uma Chave de comando no CWM é necessário instalar um certificado específico no Cliente do CWM (consulte *Seção 2.1 "Visão geral da configuração de clientes CWM", página 12*). Cada Chave de comando também possui seus próprios códigos PIN e PUK.

7.2.5 Gerações das chaves

Existem duas gerações de chaves:

- Geração 1
- Geração 2

A geração de uma chave é definida por seu hardware. As chaves geração 2 são mais novas e mais desenvolvidas.

Todas as chaves geração 2 são compatíveis com as chaves geração 1.

A geração da chave pode ser vista na tela detalhada da chave, consulte *Seção 4.2.2 "Como escanear uma chave de usuário", página 35* ou *Seção 4.2.1 "Como buscar chaves de usuário", página 34*.

7.3 Cilindros

Existem dois tipos diferentes de cilindros: mecânicos e eletrônicos. Os tipos eletrônicos podem armazenar direitos de acesso para chaves e grupos de chaves, bem como informações de trilhas de auditoria.

Os cilindros podem ser simples ou duplos. Para cilindros duplos, os lados podem ser do mesmo tipo ou de tipos diferentes.

Os símbolos abaixo são utilizados ao listar cilindros:

- Ⓔ Cilindro eletrônico
- Ⓜ Cilindro mecânico
- ⒺⓂ Cilindro duplo (Exemplo: eletrônico no lado A e mecânico no lado B)

Figura 2. Cilindro CLIQ

Um cilindro pode ser instalado em vários tipos de fechaduras, portas, cadeados, fechaduras de gabinetes etc. Há um número de identificação em cada corpo do cilindro.

Um cilindro eletrônico armazena informações de:

- Grupos de chaves e chaves individuais autorizadas
- Chaves bloqueadas
- Trilhas de auditoria normal: Trilhas de auditoria para inserções de chaves, por chaves do mesmo Sistema Cliq.
- Trilhas de auditoria estrangeiras: Trilhas de auditoria para inserções de chaves, por chaves de outros Sistemas Cliq.

Configurações de cilindros diferentes têm capacidades de memória diferentes. Consulte as informações do produto para obter mais informações.

7.4 Dispositivos de programação

7.4.1 Programadores locais

O Programador local é usado para conectar chaves de comando e chaves de usuário ao CWM.

Figura 3. Equipamento de programação local

O Programador local é usado pelos administradores de um Sistema Cliq. Têm duas ranhuras; a ranhura esquerda é para chaves de comando e a ranhura direita é para chaves de usuários. Para acessar o CWM é necessário ter uma chave de comando juntamente com um Programador local conectado a um Cliente CWM. O programador pode ser conectado usando a porta USB.

O PD local possui duas portas:

- Uma porta USB
- Uma porta para conectar cilindros (não usada com CWM)

7.4.2 Programadores remotos

Os Programadores remotos são usados nos sistemas web para transferir dados entre o banco de dados remoto e a chave. Os programadores remotos podem ser programadores de parede ou programadores móveis. Os programadores de parede e os programadores móveis CLIQ são específicos do Sistema Cliq, enquanto que os programadores móveis CLIQ Connect podem ser usados com qualquer Sistema Cliq.

Note que cada dispositivo suporta um tipo diferente de cabo USB:

Dispositivo	Tipo de cabo USB
Programador de parede (geração 1)	Cabo mini-USB On-The-Go (OTG)
Programador de parede (geração 2)	Cabo USB-C
Programador móvel CLIQ	Cabo mini-USB
Programador móvel CLIQ Connect	Cabo micro-USB

Quando a chave é inserida em um Programador remoto, é executado o seguinte:

- As tarefas de atualização remota são executadas.
- O horário da chave é atualizado.
- Se estiver configurada, a trilha de auditoria é lida a partir da chave.

Consulte também *Seção 9.5.1 "Indicações de programador de parede (Geração 1) e programador móvel", página 207* e *Seção 9.5.2 "Indicações de programador de parede (geração 2)", página 208*.

Se a **Atualização offline** estiver ativada, uma chave pode ser revalidada através de um programador de parede ou programador móvel CLIQ mesmo se tiver perdido temporariamente sua conexão com a rede. Consulte também *Seção 8.1.5 "Revalidação de uma chave", página 165*. A atualização offline não está disponível para os programadores móveis CLIQ Connect.

Programadores de parede
Estão disponíveis dois tipos de Programadores de parede; Geração 1 e Geração 2. O programador de parede geração 2 possui os seguintes recursos adicionais:

- A autenticação da rede (802.1x) pode ser ativada. Consulte *"AUTENTICAÇÃO DA REDE (802.1X) (Somente programador de parede geração 2)"* e *Seção 6.4 "Como editar as configurações do sistema", página 99* para ativar ou desativar.
- Não é usado um carregador de boot, ou seja, não é necessário atualizar o firmware de carregador de boot.
- Consulte *"GERAL"* para obter mais detalhes sobre o nível de registro para o registro de equipamento.

Tipicamente, o programador de parede é instalado em uma parede e conectado ao servidor remoto via Ethernet.

Figura 4. Programador de parede geração 1

Figura 5. Programador de parede geração 2

O termo **Pulsação** significa que o Programador de parede envia um sinal ao servidor do CLIQ Remote para avisar o CLIQ Web Manager de que está on-line. O Programador de parede verifica também as atualizações para Programadores de parede (atualizações de firmware ou de configuração) ao enviar a pulsação. É possível configurar o tempo entre pulsações.

Quando um programador de parede falha em enviar alguns pulsos, o CLIQ Web Manager assume que o programador de parede está offline e envia um e-mail a uma pessoa específica. Consulte *Seção 6.5.10 "Ativação e desativação de mensagens de programador de parede offline", página 121* para obter mais informações sobre como ativar esse recurso.

Programadores móveis CLIQ

O programador móvel CLIQ é uma unidade de programação pessoal. Ele pode se conectar a um computador via cabo mini-USB ou a um telefone celular via Bluetooth Low Energy (BLE) para usar a conexão do celular à internet.

O programador móvel CLIQ necessita da alimentação de uma bateria ao se conectar com um telefone celular. Quando o programador móvel CLIQ é usado com um computador, é

necessário instalar um aplicativo especial, o **ASSA ABLOY Network Provider**, no computador.

Figura 6. Programador móvel CLIQ

Programadores móveis CLIQ Connect
O programador móvel CLIQ Connect é usado para atualizar chaves com o CLIQ Connect (somente chaves geração 2) ou PC CLIQ Connect.

Ele pode se conectar a um computador via cabo mini-USB ou a um telefone celular via Bluetooth Low Energy (BLE) para usar a conexão do celular à Internet.

O programador móvel CLIQ Connect necessita da alimentação de uma bateria ao se conectar com um telefone celular.

Figura 7. Programador móvel CLIQ Connect

8 Conceitos e recursos do CLIQ

8.1 Princípios de autorização

As exigências abaixo deverão ser atendidas para que uma chave possa abrir um cilindro:

- O código mecânico está correto. Consulte *Seção 8.1.1 "Autorização mecânica", página 163*.
- A chave está Ativa. Isso exige que a chave esteja ativa de acordo com as configurações de ativação e que, caso seja utilizada a revalidação, a chave seja revalidada no intervalo de revalidação. Consulte *Seção 8.1.4 "Validade da chave", página 165*.
- O cilindro é programado eletronicamente para fornecer acesso à chave. Consulte *Seção 8.1.2 "Autorização eletrônica", página 163*.
- A chave não está bloqueada no cilindro. Consulte *Seção 8.1.2 "Autorização eletrônica", página 163*.
- Para chaves dinâmicas: A chave foi programada para ter acesso ao cilindro. Consulte *Seção 8.1.2 "Autorização eletrônica", página 163*.
- Para Chaves dinâmicas e chaves Quartz: O cronograma da chave permite o acesso no momento. Consulte *Seção 8.1.8 "Cronogramas de chaves", página 170*.

8.1.1 Autorização mecânica

É um Sistema do tipo master-key, cada chave em um Sistema CLIQ possui um corte mecânico e cada cilindro é compatível com um ou mais cortes de chave. O CWM acompanha as chaves com acesso mecânico a determinado cilindro e leva isto em consideração ao determinar a possibilidade de fornecer acesso eletrônico.

8.1.2 Autorização eletrônica

A autorização eletrônica tem por base as informações armazenadas no cilindro e, para chaves dinâmicas, também na chave.

As informações abaixo podem ser armazenadas em cilindros:

- Uma **Lista de acesso ao cilindro** que contém as chaves e os grupos de chaves com acesso ao cilindro.
- É possível definir exceções para cada grupo de chaves na lista de acesso, ou seja, todas as chaves no grupo de chaves terão acesso, exceto as exceções definidas. Isso é útil quando um cilindro deve permitir o acesso a todas as chaves em um grupo de chaves exceto por algumas.

Para chaves Quartz e chaves normais, as informações nos cilindros determinam se uma chave possui acesso a um cilindro.

Poderão ser armazenadas as seguintes informações nas chaves dinâmicas:

- Uma **Lista de acesso da chave** que contém os cilindros e grupos de cilindros aos quais a chave tem acesso.

Para que uma chave dinâmica seja capaz de abrir um cilindro deve haver compatibilidade entre o cilindro e a chave. Em um sistema remoto típico com chaves dinâmicas, os cilindros são programados para proporcionar acesso a todas as chaves e o acesso real é controlado por uma lista de acesso da chave.

Figura 8 "Lista de acesso da chave", página 164 mostra as várias maneiras como os cilindros ou grupos de cilindros podem ser incluídos na lista de acesso na chave dinâmica.

1. diretamente
2. por meio de um perfil de acesso
3. por meio de um usuário que está associado a um perfil de acesso
4. por meio de um grupo de acesso temporário

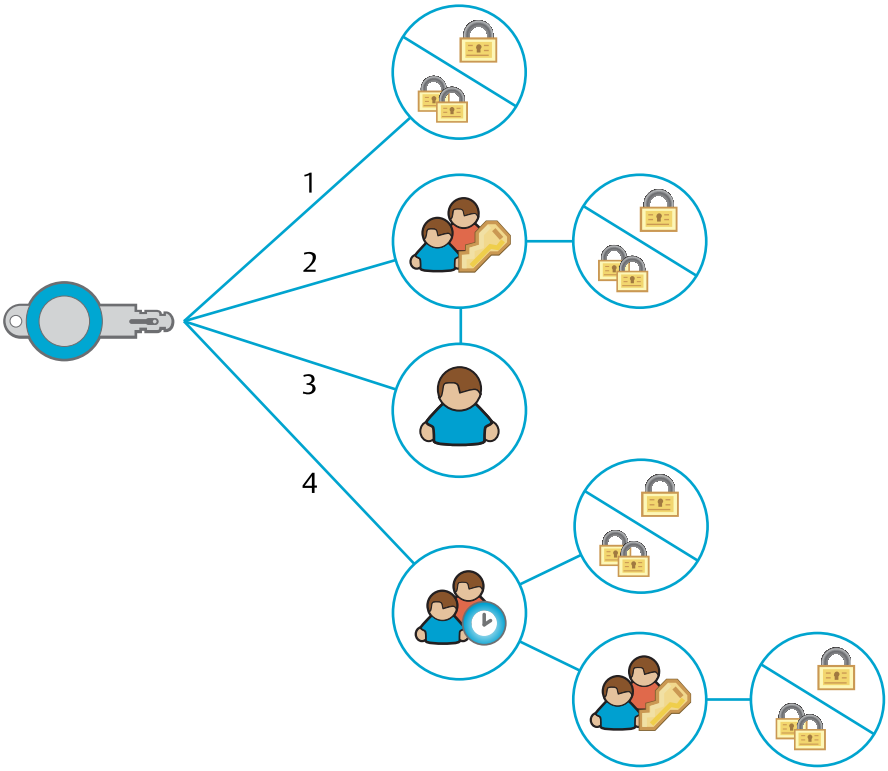


Figura 8. Lista de acesso da chave

A capacidade de uma Lista de acesso de chave é limitada. O número máximo de entradas e o número ocupado atualmente podem ser vistos na tela de informações detalhadas de uma Chave dinâmica. As funções de atualização remota que excederiam essa capacidade não serão executadas. Consulte também *Seção 8.3.2 "Atualização remota", página 180*.

Uma diferença entre as Listas de acesso de chave e as Listas de acesso de cilindro é como são tratadas as entradas de grupo. Nas listas de acesso de chave, os cilindros podem ser incluídos simultaneamente tanto individualmente como parte de um grupo de cilindros. Este não é o caso com as Listas de acesso de cilindro. Quando um grupo de chaves é adicionado a uma Lista de acesso de cilindros, quaisquer entradas individuais de chaves desse grupo de chaves (agora redundante) são removidas automaticamente. Isso significa que, se o grupo de chaves for adicionado e depois removido, todas as chaves do grupo perderão seu acesso, incluindo as chaves que tinham acesso individual anteriormente.

8.1.3 Acesso explícito e implícito

Existem duas formas de configurar as listas de acesso:

- O **Acesso explícito** é fornecido editando as listas de acesso diretamente nas chaves, cilindros e grupos de cilindros.

- O **Acesso implícito** é fornecido às chaves por meio dos perfis de acesso associados a uma pessoa ou diretamente a uma chave. Consulte também *Seção 8.2.4 "Perfis de acesso", página 175*.

As chaves dinâmicas possuem uma lista de acesso que inclui os cilindros e grupos de cilindros que a chave está autorizada a abrir. O acesso da chave a um cilindro ou grupo de cilindros pode ser explícito ou implícito. O acesso armazenado na lista de acesso de chave é a combinação dos acessos implícito e explícito.

Consulte *Seção 8.2.4 "Perfis de acesso", página 175* e *Seção 8.2.5 "Grupos de acesso temporários", página 177* para obter mais informações.

8.1.4 Validade da chave

Validade da chave significa que uma chave em certo momento está **Ativa** ou **Inativa**. Uma chave ativa tem acesso de acordo com as configurações de autorização e o cronograma, enquanto uma chave inativa está bloqueada para todos os acessos. Observe que a validade de uma chave e o cronograma de uma chave são conceitos diferentes. Consulte também *Seção 8.1.8 "Cronogramas de chaves", página 170*.

Existem três formas de controlar a validade de uma chave:

- **Configurações de ativação**. Uma chave pode ser configurada para estar **Inativa**, **Sempre ativa** ou **Ativa entre datas selecionadas**.

  Ativa entre as datas selecionadas só está disponível para Chaves dinâmicas e chaves Quartz.
- **Revalidação**, um recurso opcional. Com revalidação, as chaves devem ser atualizadas a intervalos de tempo específicos para permanecerem ativas.

  Quando a revalidação está selecionada, **A chave sempre poderá ser revalidada.** é exibido em **Configurações de validade** no CWM.

  Consulte também *Seção 8.1.5 "Revalidação de uma chave", página 165*.
- **Validação do PIN**, um recurso opcional para chaves CLIQ Connect. Com a validação do PIN, as chaves devem validar o PIN usando o CLIQ Connect a intervalos de tempo especificados para permanecerem ativas.

  Consulte também *Seção 8.1.7 "Validação do PIN", página 169*.

Para que uma chave permaneça ativa é necessário cumprir o seguinte:

- Deve estar ativa de acordo com as configurações de ativação.
- Deve ser revalidada no intervalo de revalidação especificado (caso seja usada a Revalidação).
- Ela deve ser validada com o PIN dentro de um intervalo de validação do PIN específico (caso seja usada a validação do PIN).

Consulte também *Seção 4.10.1 "Como configurar a validade de chave, a revalidação e a validação do PIN", página 86*.

8.1.5 Revalidação de uma chave

A **Revalidação da chave** é um recurso que assegura a atualização das chaves em determinados intervalos de tempo.

Este recurso está sujeito a licença.

Com a revalidação da chave, as chaves devem ser atualizadas ("revalidadas") a intervalos de tempo específicos para permanecerem ativas. Uma vez revalidada, a chave permanece ativa pelo número de dias, horas e minutos especificados como o intervalo de revalidação, a partir do momento em que foi revalidada. Se uma chave não for revalidada no intervalo especificado, ela se tornará inativa até que seja revalidada novamente.

Figura 9 "Revalidação de uma chave", página 167 mostra o princípio da revalidação de uma chave. Quando uma chave é revalidada em um programador remoto, um cronômetro é iniciado (1). A chave tem acesso desde que seja usada entro do intervalo de revalidação (2). Quando o intervalo de revalidação venceu (3) a chave precisa ser revalidada em um programador remoto (1). Quando a chave é revalidada o cronômetro é zerado.

As chaves também são revalidadas em um Programador local quando as seguintes ações são operadas localmente:

- configurar **Cronograma**
- ler **Trilha de auditoria**
- alterar **Cilindros na lista de acesso**

Se as seguintes condições forem atendidas, a chave é revalidada na ranhura direita do programador local **sem** uma chave de comando:

- Chave geração 2 com versão do firmware 12.3 ou posterior
- O CLIQ Connect no PC está ativado

ATENÇÃO!
A chave de comando deve ser removida da ranhura esquerda do programador local antes da atualização e revalidação.

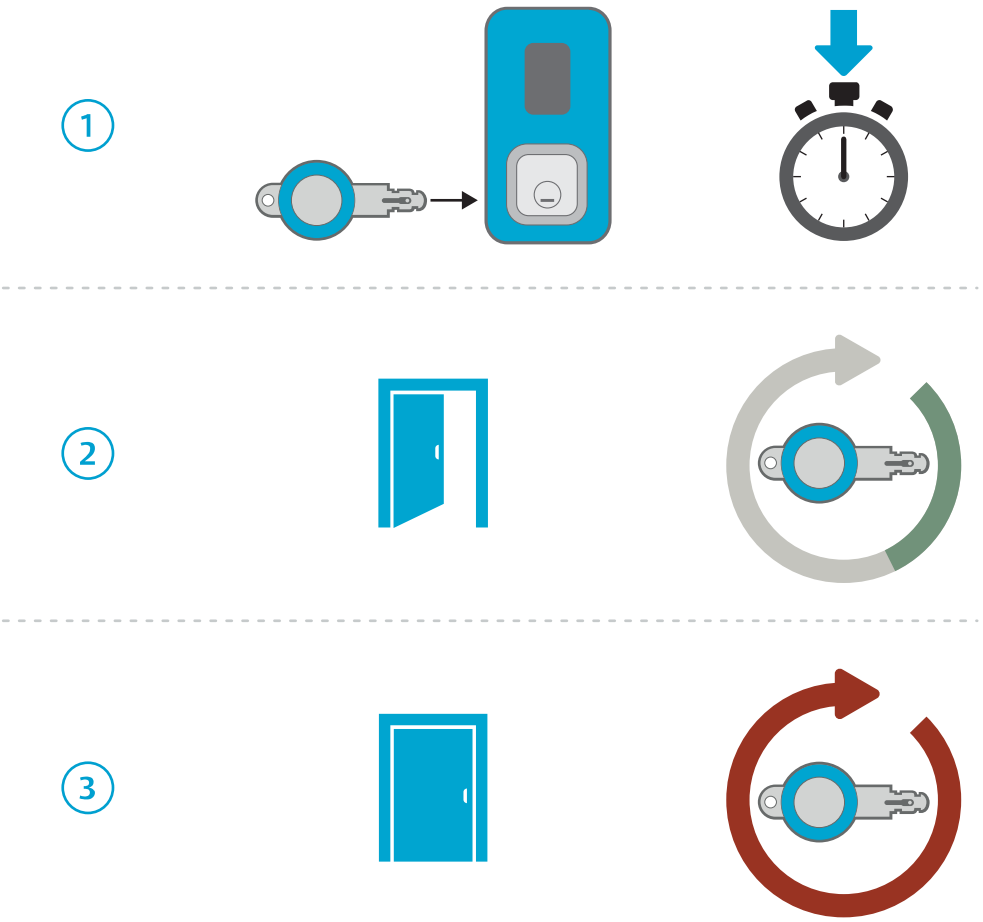


Figura 9. Revalidação de uma chave

Vantagens da revalidação:

- Garante que as atualizações pendentes das chaves sejam programadas regularmente nelas.
- Assegura a recuperação frequente das trilhas de auditoria das chaves.
- Limita a exposição de chaves perdidas. Uma chave perdida perde todo o acesso quando o tempo especificado expira e caso seja comunicada como perdida no CWM não poderá ser revalidada.

A configuração do intervalo de revalidação é uma compensação entre a conveniência para o proprietário da chave e a segurança do Sistema Cliq. Um intervalo de revalidação curto, como 24 horas, garante atualizações frequentes e exposição limitada de chaves perdidas, porém exige que o proprietário da chave a atualize diariamente. Um intervalo de revalidação longo é mais conveniente para o proprietário da chave, porém aumenta a exposição de chaves perdidas e resulta em atualizações menos frequentes dos acessos e das trilhas de auditoria.

Uma maneira de lidar com essa compensação é usar a revalidação da chave em conjunto com a **validação do PIN** (para chaves CLIQ Connect). Consulte *Seção 8.1.7 "Validação do PIN", página 169*.

Consulte também *Seção 4.10.1 "Como configurar a validade de chave, a revalidação e a validação do PIN", página 86*.

A **Revalidação flexível** é um recurso avançado que ajuda a tratar do problema da compensação. Consulte *Seção 8.1.6 "Revalidação flexível", página 168*.

A função **Atualização offline** em Programadores remotos ativa a revalidação de chaves mesmo se o Programador remoto tiver perdido temporariamente sua conexão com o servidor. Consulte *Seção 8.3.3 "Atualização off-line", página 181*.

8.1.6 Revalidação flexível

A **Revalidação flexível** é um recurso opcional avançado que torna possível configurar o intervalo de revalidação da chave por perfil de acesso e por grupo de cilindros. Consulte *Seção 8.1.5 "Revalidação de uma chave", página 165* para obter informações sobre a Revalidação de chaves.

Este recurso está sujeito a licença.

A revalidação flexível é útil nas seguintes situações:

- Cilindros com sensibilidades diferentes. Por exemplo, o acesso a uma sala de servidor pode ser mais sensível do que o acesso a uma sala de reunião.
- Os papéis associados aos perfis de acesso têm sensibilidades diferentes. Por exemplo, pode ser necessária a revalidação mais frequente a subcontratados em comparação a funcionários.
- Alguns cargos temporários podem exigir intervalos de revalidação diferentes. Por exemplo, uma pessoa de plantão pode necessitar de um intervalo de revalidação maior, porém deve ser muito cuidadosa com a chave.

CUIDADO!
Ao usar a Revalidação flexível, todas as chaves que são afetadas pelas configurações de revalidação nos perfis de acesso ou nos grupos de cilindros devem ter a revalidação ativa.

Com a Revalidação flexível, os intervalos de revalidação podem ser configurados em três níveis:

- **Configuração da chave**. O intervalo de revalidação configurado na chave constitui o máximo. Nenhuma outra configuração nos perfis de acesso ou nos grupos de cilindros pode fornecer um tempo de revalidação superior a este.

  Consulte *Seção 4.10.1 "Como configurar a validade de chave, a revalidação e a validação do PIN", página 86* para configurar o intervalo de revalidação da chave.
- **Configuração do grupo de cilindros**. O intervalo de revalidação nos grupos de cilindros pode ser usado quando os grupos de cilindros possuem sensibilidades diferentes.

  O intervalo de revalidação configurado em um grupo de cilindros limitará o intervalo configurado na chave para aquele grupo de cilindros. Por exemplo, se uma chave com intervalo de revalidação de 14 dias recebe acesso a um grupo de cilindros com um intervalo de revalidação de 7 dias, a configuração de 7 dias é aplicada a aquele grupo de cilindros. Porém se o grupo de cilindros possui intervalo de revalidação de 30 dias, a configuração de chave de 14 dias é aplicada para aquele grupo de cilindros, pois a configuração da chave sempre constitui o máximo.

  Cilindros de sistemas de grupos de cilindros herdam o intervalo de revalidação configurado no grupo de cilindros ao qual pertencem.

A configuração do intervalo de revalidação em grupos de cilindros não exige a programação do cilindro.

Consulte *Seção 4.10.2 "Como configurar a revalidação flexível", página 88* para configurar o intervalo de revalidação de um grupo de cilindros.

- **Configuração de perfil de acesso**. A configuração do intervalo de revalidação nos perfis de acesso pode ser usada quando os papéis associados com os diversos perfis de acesso possuem sensibilidades diferentes ou quando pessoas de plantão necessitam de intervalos mais longos de revalidação.

  O tempo configurado em um perfil de acesso cancela a configuração dos grupos de cilindros. Por exemplo, se um perfil de acesso com intervalo de revalidação de 10 dias fornece acesso a um grupo de cilindros com um intervalo de revalidação de 7 dias, 10 dias são aplicados para aquele grupo de cilindros para chaves com o perfil de acesso. A Configuração da chave continua sendo o máximo.

  Se uma chave ou pessoa é associada com mais de um perfil de acesso com intervalos de revalidação diferentes e esses perfis de acesso fornecem acesso ao mesmo grupo de cilindros, é aplicado o intervalo mais longo. Por exemplo, se dois perfis de acesso, com intervalos de revalidação de 10 dias e 20 dias respectivamente, ambos fornecem acesso ao mesmo grupo de cilindros, então será aplicado 20 dias para aquele grupo de cilindros. A configuração do grupo de cilindros, se especificada, é cancelada, porém a configuração da chave ainda constitui o máximo.

  Para grupos de cilindros em que o intervalo de revalidação de grupo de cilindros e o intervalo de revalidação de perfil de acesso não foram especificados, é aplicada a configuração da chave.

  Consulte *Seção 4.10.2 "Como configurar a revalidação flexível", página 88* para configurar um intervalo de revalidação de perfil de acesso.

Dica

Recomendamos o uso das configurações de revalidação principalmente em grupos de cilindros **ou em** perfis de acesso, **não em ambos**. Misturar os dois conceitos pode levar a efeitos difíceis de revisar. No caso típico, é usada a configuração de grupos de cilindros, com possíveis exceções em perfis de acesso.

8.1.7 Validação do PIN

A validação por meio de PIN não está disponível ao utilizar um programador móvel CLIQ Connect.

A **validação do PIN** é um recurso que permite a validação off-line usando um código PIN. Ela exige o uso do CLIQ Connect e só funciona com chaves de usuário CLIQ Connect.

Este recurso está sujeito a licença.

Quando a validação do PIN está ativada para uma chave, ela é desativada após um certo intervalo de tempo chamado de **Intervalo de validação do PIN**. O proprietário da chave então deve inserir um código PIN para ativá-la novamente. A validação do PIN é executada no CLIQ Connect, onde é chamada de **Ativar**. O mecanismo é similar à revalidação da chave, mas a validação do PIN tem um objetivo diferente:

A validação da chave força o proprietário da chave a atualizar a chave a certos intervalos para mantê-la ativa. Isso permite que o administrador se certifique que a chave possui as últimas atualizações e que a chave será desativada caso seja comunicada como perdida no

CWM. Além disso, quando a chave é atualizada, ela envia trilhas de auditoria caso essa função esteja ativada. A revalidação da chave exige uma conexão com a internet pois envolve a busca de atualizações a partir do servidor do CWM. Não é necessário qualquer código PIN ou senha para revalidar a chave, pois é sempre preferível que as chaves tenham as atualizações mais recentes. Consulte *Seção 8.1.5 "Revalidação de uma chave", página 165* para obter mais informações.

Usar um código PIN aumenta a segurança em vários aspectos:

- Exige que o usuário insira um código PIN.
- Protege contra perda e roubo de chaves mesmo que estas não sejam comunicadas como perdidas no CWM.
- Não exige conexão com a internet. Uma chave pode ser validada mesmo quando o servidor CWM está inativo ou se houve perda da conexão com a internet.
- Como é simples fazer a validação do PIN de uma chave, o intervalo de validação do PIN pode ser configurado para um período de tempo curto, por exemplo, 30 minutos, aumentando assim a segurança.

Para aumentar ainda mais a segurança pode-se combinar a revalidação da chave e a validação do PIN. A revalidação da chave assegura que a chave permanece atualizada e a validação do PIN assegura que a chave logo se tornará inutilizada para qualquer um que não tenha o código PIN.

Nas configurações do sistema é possível configurar se a validação do PIN deverá fazer parte do fluxo de entrega, bem como o intervalo padrão de validação do PIN. Consulte *Seção 6.4 "Como editar as configurações do sistema", página 99*.

Consulte também *Seção 8.1.4 "Validade da chave", página 165*, *Seção 8.1.5 "Revalidação de uma chave", página 165* e *Seção 4.10.1 "Como configurar a validade de chave, a revalidação e a validação do PIN", página 86*.

8.1.8 Cronogramas de chaves

Os **Cronogramas de chaves** são usados para limitar os acessos das chaves de acordo com um cronograma.

Poderá ser configurado um cronograma se o acesso da chave necessita ser limitado a certo cronograma, como por exemplo horas de expediente. Há dois tipos de cronograma, Cronograma básico e Cronograma de janelas de tempo múltiplas, dependendo da versão do firmware da chave. Para obter mais informações sobre as versões do firmware da chave, consulte *Seção 9.7 "Função dependente do firmware", página 209*.

- Com um Cronograma básico, poderá ser especificado um período de tempo por dia em uma semana. O cronograma é aplicado a todos os cilindros.
- Com um Cronograma de janelas de tempo múltiplas, poderão ser especificados diversos períodos de tempo separados por semana e cada período poderá ser estendido por vários dias. Os cronogramas também podem ser configurados para cilindros específicos.

ATENÇÃO!

Para chaves geração 1:

- Para cilindros incluídos individualmente na lista de acesso da chave (não como parte de um grupo de cilindros), especificar um ou mais períodos de tempo para um cilindro significa que o cronograma geral é ignorado para aquele cilindro.
- Para cilindros incluídos na lista de acesso da chave como parte de um grupo de cilindros, os períodos de tempo do cilindro são ignorados.

Para chaves geração 2:

- Especificar um ou mais períodos de tempo para um cilindro significa que o cronograma geral é ignorado para aquele cilindro.

Cada chave pode ser configurada com um cronograma específico ou um cronograma baseado em um modelo de cronograma.

Consulte também *Seção 4.10.3 "Como configurar o cronograma de uma chave", página 89* e *Seção 6.10 "Como gerenciar Modelos de cronograma", página 132*.

8.1.9 Travamento sequencial

O **Travamento sequencial** é um recurso que faz com que um cilindro necessite de duas chaves para ser destravado.

O travamento sequencial pode ser configurado na fábrica em cilindros específicos. Ele não pode ser configurado a partir do CWM.

Para cilindros com esse recurso habilitado, destravar o cilindro exige duas chaves com acesso. As chaves devem ser inseridas em sequência, dentro do intervalo de um minuto, para que o cilindro abra. Os cilindros com esse recurso podem, opcionalmente, ser configurados para exigir que as duas chaves pertençam a dois grupos de chaves diferentes.

8.1.10 Travamento com retardo

O **Travamento com retardo** é um recurso em que uma chave que foi revalidada recentemente obtenha acesso a um cilindro somente após um tempo de retardo específico.

O travamento com retardo pode ser configurado na fábrica em cilindros específicos. Ele não pode ser configurado a partir do CWM.

Para cilindros com este recurso habilitado, o tempo configurado (por exemplo 15 minutos), é adicionado aos tempos de ativação e expiração em qualquer chave que acesse o cilindro. Para cilindros de alta sensibilidade, recomendamos usar o travamento com retardo em conjunto com um intervalo curto de revalidação, por exemplo 30 minutos. Isso assegura que a chave permaneça inativa na maior parte do tempo (caso não seja revalidada muito frequentemente) e que haja um retardo após a validação antes que alguém possa abrir o cilindro.

Para casos em que os cilindros possuam sensibilidades diferentes, o recurso de revalidação flexível pode ser útil. Consulte *Seção 8.1.6 "Revalidação flexível", página 168*.

8.1.11 Abertura on-line

A **Abertura on-line** é um recurso usado com chaves CLIQ Connect que assegura que as chaves sejam sempre atualizadas antes de abrir cilindros. Isso impede o acesso para chaves com direitos de acesso revogados e para chaves marcadas como perdidas.

A abertura on-line pode ser configurada na fábrica em cilindros específicos ou chaves CLIQ Connect. Ele não pode ser configurado a partir do CWM.

Caso a abertura on-line esteja ativada em uma chave CLIQ Connect, será exigida a abertura on-line ao acessar qualquer cilindro com essa chave.

Caso a abertura on-line esteja ativada em um cilindro, todas as chaves que acessam o cilindro devem executar a abertura on-line. Isso significa que o acesso é limitado a chaves CLIQ Connect.

Quando é exigida a abertura on-line, a chave CLIQ Connect deve ser pareada com o CLIQ Connect antes de ser inserida no cilindro. Assim que a chave é inserida, o CLIQ Connect entra em contato com o servidor remoto do CWM, obtém as atualizações mais recentes para a chave e executa a atualização da chave. Se a chave tiver acesso ao cilindro após a atualização da chave, o cilindro destravará imediatamente.

Cilindros com o recurso de abertura on-line podem ser configuradas para aceitar **Chaves que sobreponham** sem exigir a abertura on-line. As chaves podem ser configuradas como chaves de substituição na fábrica.

8.2 Funções de agrupamento

8.2.1 Grupos de chaves

Os **Grupos de chaves** são usados para configurar direitos de acesso e outros atributos a um grupo de chaves ao invés de a cada chave individualmente.

Os grupos de chaves são usados principalmente ao usar listas de acesso em cilindros para controlar os acessos.

Benefícios dos grupos de chaves:

- Os grupos de chaves reduzem o número de entradas necessárias nas listas de acesso dos cilindros.
- É permitido adicionar uma chave a um grupo de chaves, além disso alguns cilindros fornecem acesso automaticamente à chave nova. Não é necessário programar os cilindros.
- Os grupos de chaves podem ser usados para a configuração de cronogramas de chaves.

Quando um grupo de chaves recebe acesso a um cilindro, todas as chaves desse grupo recebem acesso automaticamente. Entretanto, é possível definir exceções e excluir o acesso de chaves específicas.

ATENÇÃO!
Quando um grupo de chaves é adicionado a uma lista de acesso, quaisquer entradas individuais de chaves desse grupo de chaves (agora redundantes) são removidas automaticamente. Isso significa que, se o grupo de chaves for adicionado e depois removido, todas as chaves do grupo perderão seu acesso, incluindo as chaves que tinham acesso individual anteriormente.

Existem diversos tipos de grupos de chaves:

Grupo de chaves normais	Pode conter chaves Quartz e chaves normais.
Grupo de chaves dinâmicas	Pode conter Chaves dinâmicas.
Grupo de chaves de comando normais	Pode conter Chaves de comando normais.
Grupo de chaves de comando mestres	Pode conter Chaves de comando mestres.

As chaves mecânicas não podem pertencer a um grupo de chaves.

Consulte *Seção 4.10.4 "Como configurar o cronograma de um grupo de chaves", página 91* para configurar cronogramas em um grupo de chaves.

8.2.2 Domínios

O recurso **Domínios** é um recurso de agrupamento administrativo que permite aos administradores acessar e controlar regiões específicas de um Sistema Cliq.

Este recurso está sujeito a licença.

Os domínios são usados para dividir os seguintes elementos em regiões administrativas:

- chaves
- funcionários
- visitantes
- cilindros
- grupos de cilindros
- perfis de acesso
- grupos de acesso temporário

Os grupos de chaves e chaves de comando não podem pertencer a um domínio. Portanto, os grupos de chaves e as chaves de comando são visíveis para os administradores seja qual for seu domínio.

Um domínio consiste em um conjunto de grupos de elementos associados tipicamente com uma região geográfica ou organizacional. As Chaves de comando associadas com um domínio fornecem direitos de administração somente aos cilindros incluídos.

Benefícios do domínio:

- Conveniência: Administradores trabalhando com regiões de um Sistema Cliq, como uma região geográfica, não são preocupados com informações sobre elementos de outras regiões.
- Segurança: Os administradores não podem visualizar ou administrar elementos de outros domínios.

Fatos do domínio:

- Os cilindros que pertencem a um grupo de cilindros estão incluídos em um domínio por meio de seu grupo de cilindros. Ou seja, todos os cilindros em um grupo de cilindros pertencem ao mesmo domínio.
- Os cilindros que não pertencem a um grupo de cilindros, incluindo todos os cilindros mecânicos, estão incluídos em um domínio individualmente.

- Os elementos só podem pertencer a um domínio (chaves, funcionários, visitantes, cilindros, grupos de cilindros, perfis de acesso e grupos de acesso temporário).
- Para cilindros de dois lados, os dois lados devem pertencer ao mesmo domínio.
- Uma chave de comando de um administrador pode ser associada com um ou mais domínios, dependendo da atribuição.

> **ATENÇÃO!**
> Embora as chaves de comando não possam pertencer a um domínio, cada chave de comando possui uma lista de domínios que o administrador conectado está autorizado a acessar e controlar.

Consulte *Seção 6.11.5 "Como selecionar domínios da Chave de comando", página 135* para associar uma Chave de comando a um domínio.

8.2.3 Grupos de cilindros

Um **Grupo de cilindros** é um conjunto de cilindros que é usado para simplificar a administração em Sistemas Cliq com muitos cilindros.

Este recurso está sujeito a licença.

Os grupos de cilindros são usados em Sistemas Cliq que são definidos como **Sistemas de grupos de cilindros**, para os cilindros que possuem suporte ao grupo de cilindros. Consulte *Seção 9.7 "Função dependente do firmware", página 209*.

Os grupos de cilindros são predefinidos na fábrica, mas é possível mover cilindros entre os grupos depois disso. Isto, entretanto, exige a programação do cilindro e, portanto recomendamos planejar os grupos com cuidado com antecedência.

O acesso pode ser fornecido a um grupo de cilindro da mesma forma que para um cilindro. Poderá ser usada uma combinação de grupos de cilindros e cilindros para criar ainda mais flexibilidade.

Benefícios dos grupos de cilindros:

- Facilidade de administração dos Sistemas Cliq com muitos cilindros.
- Como apenas uma entrada na chave pode fornecer acesso a vários cilindros, uma chave pode acessar um grande número de cilindros.
- Quando um cilindro é adicionado ou removido de um grupo de cilindros, as chaves que têm acesso ao grupo de cilindros são afetadas de imediato. Não é necessária a atualização manual da lista de acesso de cada chave.

A configuração dos grupos de cilindros é uma compensação entre diversos fatores:

- Os grupos de cilindros devem ser configurados de forma que o acesso é fornecido normalmente a todos os cilindros do grupo.

  Não é possível fornecer acesso a todos os cilindros de um grupo e omitir alguns. Caso seja necessários fazer isso, as exceções dos cilindros deverão ser colocadas em um grupo separado.
- Os grupos de cilindros não deverão ser muito pequenos, pois é importante limitar o número de grupos. Quanto menos grupos, mais fácil será a administração e menor o número de entradas necessárias nas listas de acesso de chaves.
- Os grupos de cilindros deverão ainda ser pequenos o suficiente para serem estáveis, ou seja, que seja improvável ser necessário mover cilindros entre os grupos.

Fatos dos grupos de cilindros:

- Os cilindros só podem pertencer a um grupo de cilindros.
- Os grupos de cilindros só podem pertencer a um domínio.
- Para cilindros duplos, os dois lados devem pertencer ao mesmo grupo de cilindros.
- Os cilindros mecânicos não podem pertencer a um grupo de cilindros.

8.2.4 Perfis de acesso

Os **perfis de acesso** são usados para dar às pessoas que possuem um papel específico os acessos necessários sem ter que configurar cada chave individualmente. As chaves também podem ser associadas diretamente com os perfis de acesso.

Este recurso está sujeito a licença.

ATENÇÃO!
Os papéis definidos pelos perfis de acesso não devem ser confundidos com os papeis definidos para os administradores que trabalham com o CWM.

As pessoas que possuem papéis específicos, como limpeza do escritório, são associadas com um perfil de acesso correspondente. O perfil de acesso define um conjunto de cilindros e grupos de cilindros que deve ser acessados pelas pessoas com esse papel específico. As chaves entregues a pessoas associadas contêm automaticamente os direitos de acesso definidos no perfil de acesso.

Figura 10 "Perfis de acesso", página 176 mostra um exemplo com dois perfis de acesso (1, 2), cada um com acesso a certo número de cilindros ou grupos de cilindros ou a ambos (A, B). Os perfis de acesso podem ser associados com uma pessoa (3) ou com uma chave. Quando associados a uma pessoa, a chave entregue a essa pessoa recebe automaticamente acesso dos perfis de acesso associados (C).

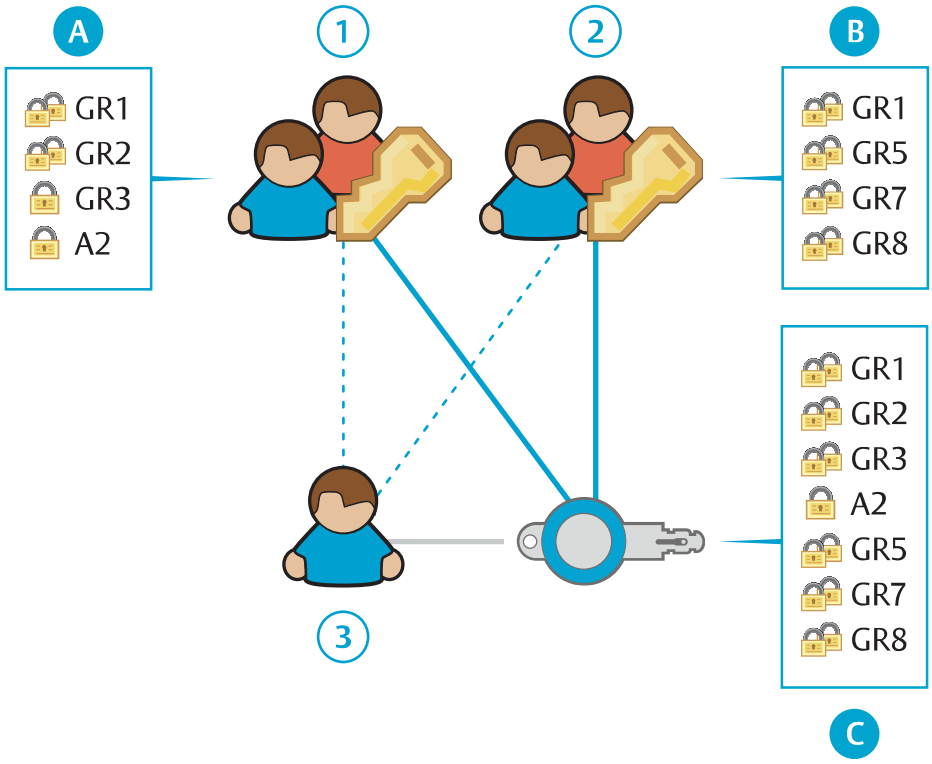


Figura 10. Perfis de acesso

Se um perfil de acesso é associado diretamente com uma chave, as outras chaves que pertencem ao mesmo proprietário da chave não herdam esse perfil de acesso.

Os perfis de acesso são dinâmicos no sentido que uma alteração no perfil de acesso atualiza automaticamente o estado das autorização de chave, pois são definidos no CWM (também chamado de **Estado definido**). Uma alteração no perfil de acesso gera funções de atualização remota para as chaves associadas. Não é necessário programar os cilindros. Para obter mais informações sobre o **Estado definido** e **Estado atual**, consulte *Seção 9.1.1 "Termos", página 194*.

Os perfis de acesso definem o **Acesso implícito** para as chaves, enquanto que os cilindros e grupos de cilindros autorizados definidos diretamente para a chave constituem o **Acesso explícito**. O acesso real armazenado na lista de acesso de chave é a combinação dos acessos implícito e explícito. Ou seja, a chave pode acessar tanto os cilindros definidos no perfil de acesso como os cilindros definidos explicitamente para aquela chave.

Benefícios do perfil de acesso:

- É possível gerenciar simultaneamente o acesso para várias pessoas ou chaves.
- É possível definir perfis correspondentes a papéis e fornecer acesso a pessoas que possuem um ou mais papéis.
- Quando um perfil de acesso é alterado são criadas funções de atualização remota associadas automaticamente.

Fatos do perfil de acesso:

- Uma chave ou uma pessoa pode ter vários papéis e portanto ser associado com mais de um perfil de acesso.
- Tanto cilindros individuais como grupos de cilindros podem ser incluídos em um perfil de acesso.

- Um perfil de acesso pertence a um domínio e somente poderão ser adicionados cilindros ou grupos de cilindros que pertencem a aquele domínio.

  ATENÇÃO!
  Recomendamos certificar-se de que um perfil de acesso e todos os cilindros e grupos de cilindros incluídos pertencem ao mesmo domínio. Isto é para assegurar que os administradores para um domínio específico não possam obter acesso indireto a cilindros em outros domínios (por meio dos perfis de acesso).

- Ao introduzir os perfis de acesso a um Sistema Cliq onde já foram usadas listas de acesso de chaves, essas listas podem incluir várias entradas do mesmo cilindro ou grupo de cilindros. Consulte *Seção 4.7.7 "Como remover autorizações de chave redundantes", página 75* para remover entradas redundantes.

Dica
Para manter uma visão geral melhor ao usar perfis de acesso, recomendamos minimizar o uso de acessos explícitos.

8.2.5 Grupos de acesso temporários

Os **Grupos de acesso temporário** são usados para expandir temporariamente o acesso de chaves associando-as com uma seleção de perfis de acesso. O acesso de um grupo de acesso temporário é o acesso combinado dos perfis de acesso incluídos durante um intervalo de tempo que é definido com uma data de início e uma data de término.

As chaves nos grupos de acesso temporário recebem acesso implícito aos cilindros e grupos de cilindros que são atribuídos aos perfis de acesso incluídos. Além disso, as chaves podem receber acesso explícito a cilindros específicos e grupos de cilindros que são atribuídos ao grupo de acesso temporário.

Figura 11 "Grupos de acesso temporários", página 178 mostra uma chave que foi adicionada a um grupo de acesso temporário (1) com três perfis de acesso (2, 3, 4) e um conjunto de cilindros específicos e grupos de cilindros (4). Cada perfil de acesso fornece acesso a diversos cilindros, grupos de cilindros ou ambos (A, B, C). Durante um intervalo de tempo definido a chave possui acesso a todos os cilindros e grupos de cilindros (D).

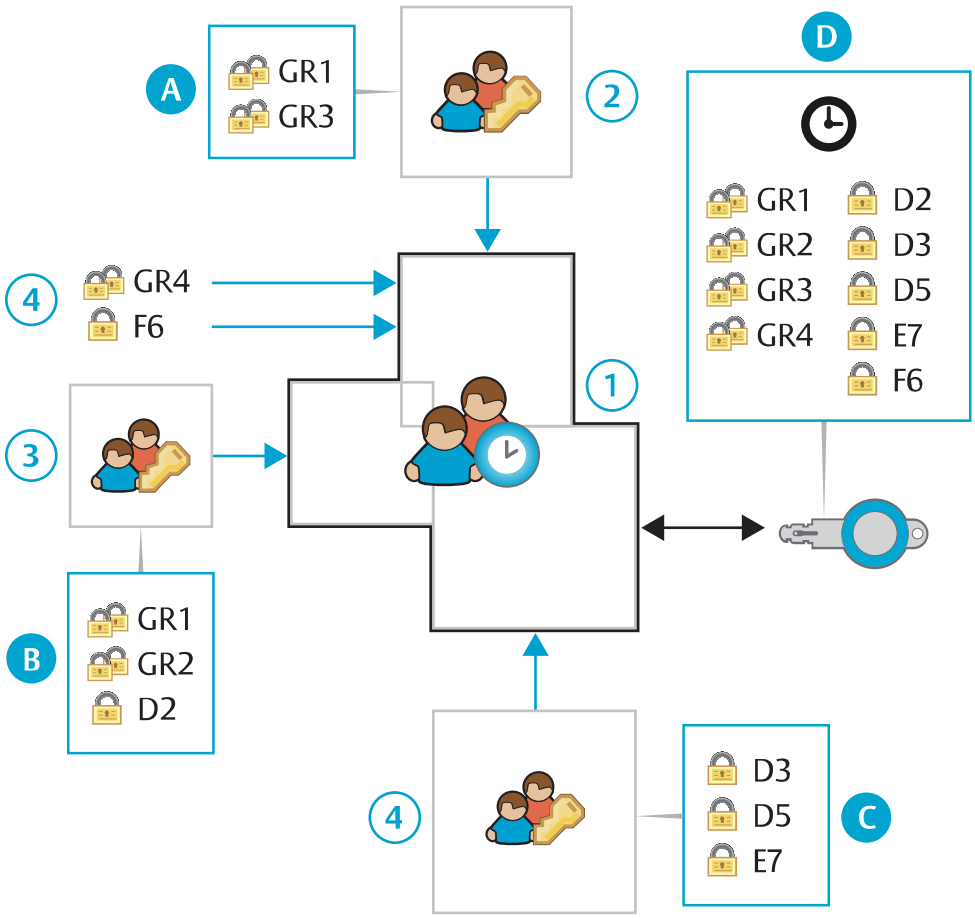


Figura 11. Grupos de acesso temporários

Um exemplo de uso é quando um ou vários técnicos de manutenção estão de prontidão e precisam acessar vários perfis de acesso durante o intervalo de prontidão.

Na prática, a chave é adicionada a um grupo de acesso temporário e programada em um programador local ou remoto. Quando o grupo de acesso temporário não for mais válido para uma chave, será criada automaticamente uma função para remover o acesso do grupo de acesso temporário da chave.

ATENÇÃO!
O cancelamento do acesso da chave não será efetivo até que a chave seja atualizada em um programador remoto. Para cancelar a possibilidade do proprietário da chave de usá-la após o vencimento do grupo de acesso temporário, faça um dos seguintes antes de entregar a chave:

- Configure **Ativo entre as datas selecionadas** nas configurações de ativação, consulte *Seção 8.1.4 "Validade da chave", página 165*.
- Ative a **Revalidação** da chave, consulte *Seção 8.1.5 "Revalidação de uma chave", página 165*.

Recomendamos combinar os grupos de acesso temporário com a revalidação da chave.

Benefícios do grupo de acesso temporário:

- É possível fornecer acesso a uma ou várias chaves a um grupo de perfis de acesso, cilindros específicos e grupos de cilindros.

Fatos do grupo de acesso temporário:

- Todos os perfis de acesso dentro do grupo de acesso temporário devem fazer parte do mesmo domínio.
- Os usuários atribuídos ao domínio padrão podem ver os grupos de acesso temporário a partir de todos os domínios. Os usuário que acessaram outros domínios só podem ver os grupos de acesso temporário dentro de seu próprio domínio.

8.2.6 Etiquetas

Uma **Etiqueta** é uma cadeia de caracteres que pode ser usada para marcar objetos e torná-los mais fáceis de achar e administrar.

Por exemplo, os perfis de acesso podem ser agrupados pelo tipo de papel ao qual estão associados e os cilindros podem ser agrupados pelo edifício onde estão instalados.

Ao procurar objetos, as etiquetas podem ser inseridas como critério de busca.

Algumas vezes as etiquetas já são adicionadas nos arquivos de extensão e estão disponíveis quando os arquivos são importados para o CWM. Também é possível adicionar ou excluir etiquetas manualmente para os seguintes objetos:

- Funcionários (consulte *Seção 4.1.7 "Como adicionar ou remover uma etiqueta de funcionário ou visitante", página 30*)
- Visitantes (consulte *Seção 4.1.7 "Como adicionar ou remover uma etiqueta de funcionário ou visitante", página 30*)
- Chaves (consulte *Seção 4.2.5 "Como adicionar ou remover chave-etiquetas de usuário", página 36*)
- Grupos de chaves (consulte *Seção 4.3.3 "Como adicionar ou remover etiquetas de grupos de chaves", página 53*)
- Cilindros (consulte *Seção 4.4.3 "Como adicionar ou remover etiquetas de cilindros", página 55*)
- Grupos de cilindros (consulte *Seção 4.5.3 "Como adicionar ou excluir etiquetas de grupos de cilindros", página 66*)
- Perfis de acesso (consulte *Seção 4.6.4 "Como adicionar ou excluir etiquetas de perfis de acesso", página 69*)
- Programadores remotos (consulte *Seção 6.5.5 "Como adicionar ou remover etiquetas de programador remoto", página 107*)

Cada objeto pode receber mais de uma etiqueta.

8.3 Recurso remoto

8.3.1 Visão geral do recurso remoto

O recurso remoto possibilita as atualizações remotas das configurações das chaves. Também permite a revalidação e a recuperação de trilhas de auditoria de um local remoto.

Este recurso está sujeito a licença.

- **Atualização remota das configurações das chaves.**

O administrador configura as autorizações e outras configurações em chaves sem a chave estar presente. A nova configuração é armazenada no banco de dados do servidor remoto como uma **Função de atualização remota**. Quando a chave é inserida em um Programador remoto, a função de atualização é executada e a chave é programada com a configuração nova.

- **Atualização remota da configuração de data e hora atual da chave**

  A configuração de data e hora atual da chave é atualizada a cada atualização da chave.

- **Recuperação remota das trilhas de auditoria**

  A trilha de auditoria da chave é recuperada a cada atualização da chave, desde que as configurações de Aprovações no sistema estejam ativadas.

- **Revalidação**.

  A revalidação assegura que as chaves sejam atualizadas a certos intervalos de tempo. Consulte *Seção 8.1.5 "Revalidação de uma chave", página 165* para obter mais informações sobre a revalidação.

Consulte também *Seção 8.3.2 "Atualização remota", página 180*.

Os sistemas são fornecidos como remotos ou não remotos. Um sistema não remoto que for convertido mais tarde para sistema remoto, poderá conter chaves que suportam e chaves que não suportam atualizações remotas. Em um sistema que é fornecido inicialmente como sistema remoto, todas as chaves suportam atualizações remotas desde o fornecimento.

8.3.2 Atualização remota

As **Funções de atualização remotas** são atualizações de chaves pendentes. Isto não deverá ser confundido com **Funções de programação de cilindros**, que são atualizações de cilindros pendentes. Consulte *Seção 8.5 "Programação do cilindro", página 183* para obter mais informações sobre as Funções de programação de cilindros.

A menos que uma chave seja escaneada no Programador local, todas as ações que exigem atualização das informações na chave resultarão em uma Função de atualização remota, que inclui a atualização de autorizações, validade, cronograma e etc... A Tarefa de atualização remota será executada da próxima vez que a chave seja inserida em um Programador remoto.

O programador remoto está, normalmente, online mas pode ser configurado para permitir atualizações de chaves sob certas condições também quando estiver off-line. Consulte *Seção 8.3.3 "Atualização off-line", página 181*.

O símbolo abaixo é usado ao longo do CWM para Funções de atualização remota:

 Existe uma atualização remota pendente para a chave

Consulte *Seção 4.9.1 "Como configurar autorizações em chaves", página 78* para visualizar as atualizações de autorização remota pendentes.

Excedendo a capacidade da chave
As Funções de atualização remota que excederiam a capacidade da Lista de acesso da chave não podem ser executadas. Quando tal função criada no CWM, é enviado um e-mail sobre isto a todos os administradores que possuem permissão total de **Autorizações de chaves** e que possuem um endereço de e-mail especificado. A tarefa é marcada também com o seguinte símbolo no CWM:

 Existe uma atualização remota pendente que excede a capacidade da chave

Ao executar operações em uma chave a partir da tela da chave, é criada instantaneamente uma Função de atualização remota e o administrador pode ver imediatamente se ela excede a capacidade da chave. Entretanto, ao executar operações em chaves a partir de outras telas, as Funções de atualização remota não são criadas instantaneamente e o administrador não tem feedback imediato.

As operações que podem gerar Funções de atualização remota que excedem a capacidade da chave e onde o administrador não recebe feedback imediato incluem:

- Adicionar acessos a um perfil de acesso
- Adicionar perfis de acesso a várias chaves
- Adicionar perfis de acesso a uma pessoa

Para solucionar a situação, o número de entradas na Lista de acesso da chave deverá ser reduzido. Isso é feito reduzindo o número de acessos explícitos, reduzindo o número de acessos em perfis de acesso associados ou removendo perfis de acesso associados. A Função de atualização remota é ajustada automaticamente de acordo.

8.3.3 Atualização off-line

A atualização offline não está disponível ao utilizar um programador móvel CLIQ Connect.

A **Atualização off-line** é uma função que habilita chaves para serem revalidadas através de um Programador remoto mesmo se tiver perdido temporariamente sua conexão com a rede. Isto é útil em situações em que é crítico que uma chave tenha sua validade estendida mesmo se a conexão com a rede esteja instável. As atualizações de acessos não podem ser feitas no modo off-line. A Atualização off-line é configurável por Programador remoto.

Para limitar o risco e a exposição de chaves perdidas, podem ser configuradas diversas condições para que seja permitida uma atualização off-line. O seguinte pode ser configurável:

- O número de atualizações consecutivas que podem ser feitas no modo off-line antes que seja necessária uma atualização online.
- Por quanto tempo são permitidas atualizações off-line após a última atualização online.
- Quanto a validade da chave é estendida em uma atualização off-line. O intervalo de revalidação configurado na chave é ignorado nas atualizações off-line.

Específico para Programadores de parede.

A chave não pode executar uma atualização off-line caso esteja incluída na **Lista de revogação de chave** armazenada em cada Programador de parede. Essa lista contém as chaves que foram comunicadas como perdidas e portanto não deve ser permitido que executem uma atualização off-line. O Programador de parede verifica quanto a versões novas da Lista de revogação de chave a cada pulsação e só permite atualizações off-line se a versão da lista armazenada no Programador remoto não seja muito velha. O tempo que uma Lista de revogação de chave é válida é configurável com um parâmetro do Programador de parede.

Específico para programadores móveis CLIQ

Somente chaves atualizadas recentemente no mesmo programador móvel CLIQ (chaves que estão entre as últimas 10 chaves atualizadas) podem ser revalidadas no modo offline.

Consulte também *Seção 8.1.5 "Revalidação de uma chave", página 165*.

Consulte *Seção 6.5.7 "Como configurar programadores de parede", página 109* e *Seção 6.5.8.1 "Como editar as configurações de um programador móvel CLIQ", página 116* para configurar Atualizações off-line.

8.3.4 CLIQ Connect e CLIQ Connect+

O CLIQ Connect é um aplicativo instalado em um dispositivo móvel, como um telefone celular ou um tablet. Ele permite que os proprietários de chaves de usuário, ou seja, visitantes e funcionários, gerenciem facilmente suas chaves de usuário. O CLIQ Connect está disponível para Android e iOS.

O CLIQ Connect oferece as seguintes funções:

- Validar e alterar o código PIN de uma chave Connect.
- Atualizar chaves Connect por meio da conexão Bluetooth da chave
- Atualizar outros tipos de chaves de usuário por meio do programador móvel CLIQ Connect.

CLIQ Connect+

O CLIQ Connect+ pode ser usado com o CLIQ Connect **versão 4.0 ou posterior**. Com esse recurso, qualquer proprietário de chave registrado pode ver mais detalhes de suas chaves, como validade, cronograma ou cilindros acessíveis, tanto para chaves conectadas quanto para chaves não conectadas.

Depois de ativado, o proprietário da chave segue as instruções por e-mail da CWM para concluir a configuração. O aplicativo é configurado usando um código QR incluído no e-mail.

Esta função exige as seguintes condições:

- Sistema CWM versão 11.2 ou posterior
- A licença **CLIQ Connect+** está autorizada para o sistema.

  Consulte *Seção 6.1 "Como administrar as licenças", página 98* para instalar a licença.
- O proprietário da chave é um usuário ativado do CLIQ Connect+.

  Consulte *Seção 4.1.5 "Como ativar ou desativar o CLIQ Connect+ para funcionários ou visitantes", página 27* para ativar proprietários da chave para acessar o CLIQ Connect+.
- O proprietário da chave ativa a conta do CLIQ Connect+ seguindo as instruções do e-mail enviado pelo CWM.

8.4 Links externos

Um **Link externo** é uma URL, um endereço da internet, que pode ser usado para ligar um objeto, como um funcionário ou um cilindro, a mais informações.

Por exemplo, um funcionário pode ser ligado à página do funcionário na intranet da empresa e um cilindro ou um Programador de parede pode ser ligado a um mapa de sua posição.

Os Links externos podem ser adicionados aos seguintes objetos:

- Funcionários (consulte *Seção 4.1.8 "Como gerenciar links externos de funcionários ou visitantes", página 31*)
- Visitantes (consulte *Seção 4.1.8 "Como gerenciar links externos de funcionários ou visitantes", página 31*)

- Chaves (consulte *Seção 4.2.6 "Como gerenciar links externos da chave de usuário", página 37*)
- Cilindros (consulte *Seção 4.4.4 "Como gerenciar links externos de um cilindro", página 56*)
- Perfis de acesso (consulte *Seção 4.6.5 "Como editar links externos de um perfil de acesso", página 70*)
- Programadores remotos (consulte *Seção 6.5.6 "Como gerenciar links externos de um Programador remoto", página 108*)

Cada objeto pode receber mais de um link externo.

8.5 Programação do cilindro

A programação do cilindro inclui a atualização de uma lista de acesso de cilindros ou a recuperação das trilhas de auditoria do cilindro.

Uma **Função de programação do cilindro** é criada no CWM nestas situações:

- As chaves autorizadas para o cilindro foram atualizadas.
- Uma chave incluída na lista de acesso do cilindro foi declarada como perdida ou quebrada.
- Foi selecionada a reprogramação de um cilindro.
- Foi selecionada a recuperação da trilha de auditoria do cilindro.
- O grupo de cilindros ao qual o cilindro pertence foi alterado.

Quando devem ser executadas Funções de programação do cilindro, elas são carregadas primeiro em uma chave de comando no programador local ou no programador remoto. Ao inserir a chave de comando no cilindro, a Função de programação é executada e, caso aplicável, as trilhas de auditoria do cilindro são carregadas na chave de comando. Assim que o programa é executado, a chave de comando é inserida novamente no programador local ou no programador remoto e o sistema Cliq pode ser atualizado com informações sobre os programas concluídos e as trilhas de auditoria recuperadas.

Figura 12 "Programação do cilindro", página 184 mostra duas maneiras de executar as funções de programação do cilindro:

- No primeiro caso (1) a função de programação do cilindro é carregada na chave de comando do administrador (A) por meio de um programador local. Então a chave é transportada e inserida no cilindro que precisa ser programado e devolvida quando a função foi executada para atualizar o Sistema Cliq.
- No segundo caso (2) um administrador acessa o CWM usando uma chave de comando (A) e prepara as funções de programação do cilindro que outros administradores coletam com suas chaves de comando (B) em um programador remoto. Então as chaves de comando são inseridas nos cilindros e devolvidas para o programador remoto para atualizar o Sistema Cliq.

  A opção de coletar, executar a confirmar as funções de programação do cilindro por meio de um programador remoto torna possível que um administrador prepare as tarefas no CWM e outro administrador programe os cilindros sem nunca acessar o CWM.

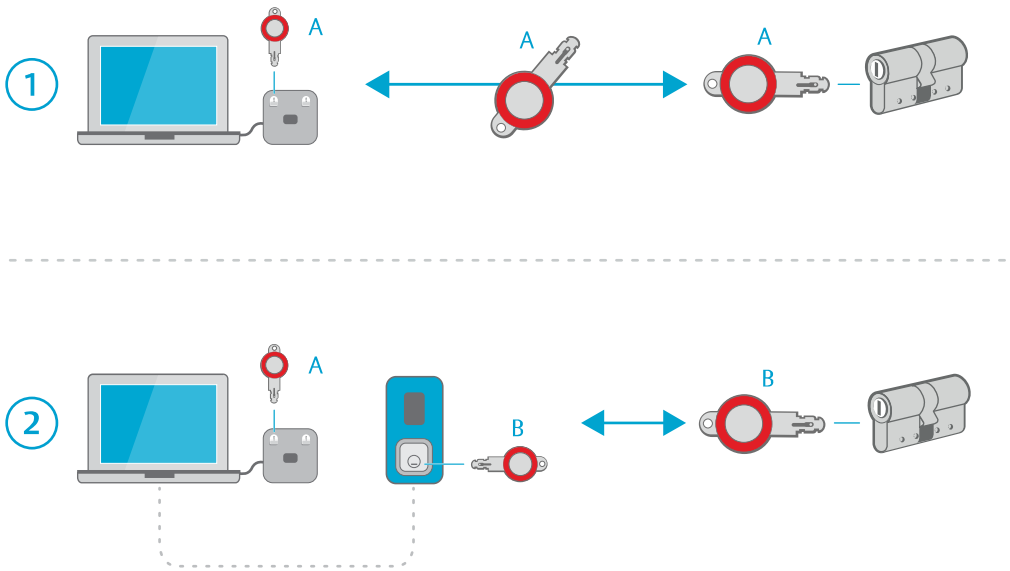


Figura 12. Programação do cilindro

São usados os seguintes símbolos ao longo do CWM para as Funções de programação do cilindro:

- Existe uma função de programação para o cilindro
- A função de programação do cilindro necessita aprovação
- Uma função de programação do cilindro foi programada para uma chave de comando
- A função de programação do cilindro foi concluída
- Falha ou cancelamento da função de programação do cilindro
- A função de programação do cilindro foi substituída por uma nova função

As funções de programação do cilindro podem ser carregadas apenas em uma Chave de comando com a autorização de **Programação do cilindro**.

Para Tarefas que envolvem a troca do grupo de cilindros do cilindro também exigem uma chave de comando com a capacidade para **Programar o grupo de cilindros**. Para ver se uma Chave de comando possui capacidade de programação de grupo de cilindros, visualize as informações detalhadas da chave de comando. Consulte *Seção 6.11.1 "Como buscar chaves de comando", página 133* ou *Seção 6.11.2 "Como escanear uma chave de comando", página 133*. Em sistemas inicialmente fornecidos como sistemas de grupos de cilindros, todas as Chaves de comando possuem essa capacidade.

Consulte também *Seção 4.4.13 "Como programar os cilindros", página 61* e *Seção 8.8 "Papéis e autorizações do CWM", página 187*.

Reprogramação
A reprogramação pode ser usada como primeira medida de solução de problemas se um cilindro não funciona como esperado. Por exemplo, se a chave de comando é removida

muito cedo ao programar um cilindro, o cilindro não funcionará adequadamente e a reprogramação resolve o problema.

Quando a chave de comando com uma função de programação com falha é inserida em um PD remoto, o CWM recria automaticamente a função de programação e a envia novamente para a chave. Isto possibilita que o proprietário da chave refaça a função de programação.

O CWM notifica também o administrador, por e-mail, com informações sobre qual chave foi usada, o cilindro afetado e o motivo porque a programação falhou. Essa função está sempre ligada e não pode ser desativada.

Quando um cilindro é reprogramado, seu conteúdo de memória é apagado, incluindo as trilhas de auditoria. A lista de acesso do cilindro é então rearmazenada como parte da reprogramação. Isto é diferente de uma programação normal de um cilindro, quando a lista de acesso do cilindro só é atualizada e a trilha de auditoria permanece intocada.

É necessária uma chave de comando mestre ou uma chave de comando normal com direitos de reprogramação de cilindro para executar a função de reprogramação.

Consulte também *Seção 4.4.12 "Como solicitar a reprogramação do cilindro", página 61*.

8.6 Trilhas de auditoria

Tanto as chaves como os cilindros possuem o recurso de trilha de auditoria. Uma Trilha de auditoria é uma lista de eventos que envolvem a solicitação de acesso pelas chaves em um cilindro e também a programação de chaves e cilindros. Existem dois tipos de Trilhas de auditoria:

- As **Trilhas de auditoria normais** contêm eventos em que os dispositivos envolvidos pertencem ao mesmo Sistema Cliq.
- As **Trilhas de auditoria estrangeiras** contêm eventos em que os dispositivos envolvidos pertencem a Sistemas Cliq diferentes.

Trilhas de auditoria de chaves
Somente chaves quartz ou dinâmicas podem armazenar trilhas de auditoria.

A trilha de auditoria da chave registra os cilindros que a chave tentou acessar, o proprietário da chave no momento (caso não tenha sido excluído ou desativado permanentemente) e as funções de programação que foram executadas na chave. Ela registra também a data e hora e o resultado desses eventos.

Trilhas de auditoria do cilindro
A trilha de auditoria do cilindro registra quais chaves tentaram acessar o cilindro, o proprietário da chave no momento (caso não tenha sido excluído permanentemente) e as funções de programação que foram executadas. Ela registra também a data e hora e o resultado desses eventos. Note que a trilha de auditoria não registra tentativas de acesso ao cilindro por meio de uma chave mecânica.

Recuperação da trilha de auditoria automática
Se uma chave de usuário pertencer a um sistema remoto, tiver suporte para atualizações remotas, for uma chave dinâmica ou de Quartzo e as aprovações de trilha de auditoria estiverem desativadas, a entrega da chave de usuário aciona a criação de uma função de trilha de auditoria de leitura remota.

Uma chave de comando pode ser programada para recuperar automaticamente as trilhas de auditoria do cilindro. Essa função possibilita que o proprietário da chave recupere de forma rápida e simples as trilhas de auditoria e cilindros arbitrários dentro do domínio.

Consulte também *Seção 6.11.13 "Ativar ou desativar a recuperação automática das trilhas de auditoria para a chave de comando", página 141*.

Remoção do arquivo da trilha de auditoria automática
O arquivo da trilha de auditoria pode ser configurado para remover automaticamente trilhas de auditoria mais antigas que um número de dias definido. Esse processo de exclusão se baseia na data de criação - a data em que a entrada foi gerada no elemento físico - e não na data de análise, que é quando a entrada foi armazenada no banco de dados do CWM.

Se a licença de **Arquivo da trilha de auditoria ampliada e eventos** não foi autorizada, o intervalo de remoção automático pode ser configurado para até 366 dias.

Se a licença de **Arquivo da trilha de auditoria ampliada e eventos** foi autorizada, o intervalo de remoção automático pode ser configurado para até 3660 dias.

Aprovações
Em sistemas Cliq em que o recurso **Aprovações** está ativado, todas as solicitações de trilhas de auditoria de chaves e cilindros devem ser aprovadas por um administrador com o papel de **Aprovador**. Assim que a trilha de auditoria é lida de uma chave ou cilindro, ela pode ser visualizada por qualquer administrador com autorização de visualização de **Trilhas de auditoria**. Consulte também *Seção 8.8 "Papéis e autorizações do CWM", página 187*.

O recurso é ativado ou desativado em **Configurações do sistema**. Consulte *Seção 6.4 "Como editar as configurações do sistema", página 99*.

8.7 Eventos

As operações executadas pelo administrados nos seguintes componentes do CWM são armazenadas como eventos e visualizadas na guia **Eventos** de cada componente.

- **Funcionário ou visitante**

  Consulte *Seção 4.1.10 "Como visualizar eventos de funcionários ou visitantes", página 32* para visualizar eventos de funcionários ou visitantes.

- **Chave**

  Consulte *Seção 4.2.8 "Como visualizar eventos de uma chave de usuário", página 38* para visualizar eventos de chaves.

- **Cilindro**

  Consulte *Seção 4.4.7 "Como visualizar eventos do cilindro", página 57* para visualizar eventos de cilindros.

- **Grupos de cilindros**

  Consulte *Seção 4.5.5 "Como visualizar eventos de um grupo de cilindros", página 67* para visualizar eventos de grupos de cilindros.

- **Perfil de acesso**: como adicionar ou remover cilindros em um perfil de acesso.

  Consulte *Seção 4.6.7 "Como visualizar eventos do perfil de acesso", página 71* para visualizar eventos de perfil de acesso.

- **Grupo de acesso temporário**

Consulte *Seção 4.7.6 "Como visualizar eventos do grupo de acesso temporário", página 75* para visualizar eventos de perfil de acesso.

- **Programador remoto**.

  Consulte *Seção 6.5.9 "Como visualizar o registro de eventos do Programador remoto", página 121* para visualizar eventos de programadores remotos.

- **Chave de comando**

  Consulte *Seção 6.11.6 "Como visualizar eventos de uma chave de comando", página 135* para visualizar eventos de chaves de comando.

Remoção automática do arquivo de eventos
O arquivo de eventos pode ser configurado para remover automaticamente eventos mais antigos que um número de dias definido.

Se a licença de **Arquivo da trilha de auditoria ampliada e eventos** não foi autorizada, o intervalo de remoção automático pode ser configurado para até 366 dias.

Se a licença de **Arquivo da trilha de auditoria ampliada e eventos** foi autorizada, o intervalo de remoção automático pode ser configurado para até 3660 dias.

ATENÇÃO!
Os seguintes eventos não estão sujeitos à remoção automática e permanecem no histórico mesmo após o término do intervalo de retenção:

- Ativação de chave, cilindro e programador remoto
- O evento de entrega de chave mais recente nos eventos do funcionário ou visitante e os eventos da chave.

8.8 Papéis e autorizações do CWM

Os papéis são definidos pela combinação das permissões fornecidas e atribuídas a chaves de comando.

Cada permissão fornece aos papéis diferentes níveis de direitos para executar uma certa função CWM.

Papéis
As funções visíveis no CWM dependem do papel atribuído para a chave de comando usada pelo administrador que está registrado. É altamente recomendado que os administradores só tenham acesso às funções necessárias em seu trabalho. Por exemplo, um administrador que executa somente tarefas de programação para cilindros deverá ter acesso somente a essa função. Um administrador responsável pela gestão de chaves deverá ter acesso somente à entrega/devolução de chaves e aos procedimentos de perda/quebra de chaves.

ATENÇÃO!
Os papéis definidos para administradores que trabalham com o CWM não devem ser confundidos com os papéis definidos nos perfis de acesso.

Os papéis abaixo são pré-definidos no CWM:

Tabela 2. Papéis pré-definidos

Papel	Descrição
Super administrador	Todas as permissões exceto a autorização para aprovar solicitações de trilhas de auditoria.
Administrador	Autorizações para funções importantes, como configuração de autorização, edição de modelos, etc...
Recepcionista	Autorizações necessárias para tarefas diárias mais simples, como a entrega e recebimento de chaves.
Aprovador	Autorizações somente para aprovar solicitações de trilhas de auditoria.
Programador de cilindro	Autorizações somente para executar a programação de cilindros.
Webservice	Usada para a integração de serviços web.

Os papéis de Super administrador e Aprovador não podem ser excluídos ou editados. O papel WebService pode ser editado porém não pode ser excluído.

Uma chave de comando pode receber mais de um papel, porém o papel de aprovador não pode ser combinado com outros papéis. Consulte *Seção 6.11.4 "Como editar as informações de uma chave de comando", página 134* para mais informações sobre como atribuir papéis.

ATENÇÃO!
Alguns direitos para as chaves de comando dependem do tipo de chave de comando e não podem ser configurados por meio de papéis e permissões. Consulte *Seção 7.2.4 "Chaves de comando", página 156*.

Por padrão, os papéis descritos acima estão em uma estrutura simples. Os administradores podem criar ou editar papéis com permissões mais altas que as que possuem e podem atribuir ou desatribuir esses papéis em uma chave de comando.

Quando a função administradores hierárquicos é ativada, é formada a hierarquia dos papéis e são aplicadas as seguintes restrições:

- o administrador não poderá conceder um nível de permissão superior ao seu próprio.
- o administrador não poderá atribuir ou excluir papéis com um nível de permissão superior ao seu próprio.

A classificação dos papéis na hierarquia é determinada pelo nível de permissão. Se um papel possui um nível de permissão superior ao do administrador, então assume-se que o papel possui um papel superior ao papel do administrados e não pode ser editado ou excluído pelo administrador.

A função de administradores hierárquicos pode ser ativada pelo Super administrador a partir da página **Configurações do sistema**.

Permissões
Para cada papel, são fornecidas autorizações específicas para cada função do CWM, como cuidar de chaves, cilindros, funcionários, firmware, configurações do sistema, Chaves de comando, etc...

As autorizações para uma função do CWM é configurada em um dos seguintes níveis:

Tabela 3. Níveis de autorização

Nível	Descrição
Nenhum	Não permite acesso.
Lista	Permite buscas e listagens.
Visualizar	Permite também a visualização de detalhes.
Cheio	Permite também editar informações.

Consulte *Seção 9.4 "Permissões", página 201* para uma lista completa de autorizações e do que é permitido em cada nível.

Consulte também *Seção 6.7 "Como gerenciar papéis e autorizações", página 127*.

8.9 Exclusão de dados pessoais e conformidade com a GDPR

O CWM pode ser configurado para tratar funcionários e visitantes excluídos de duas formas diferentes: **Excluir permanentemente** ou **Marcar como excluído**. O comportamento é controlado pela configuração do sistema **Ao excluir pessoas**.

Excluir permanentemente
Para que possa suportar GDPR, a configuração Exclusão de dados pessoais deve ser configurada para **Excluir permanentemente**. Quando configurado para isso, o seguinte se aplica:

- Ao excluir uma pessoa, os dados correspondentes são excluídos permanentemente do banco de dados e não podem ser recuperados. As referências a uma pessoa excluída nos registros de eventos e trilhas de auditoria são substituídas permanentemente por **N/D**.
- Além de **Excluir**, existe também a função **Desativar** uma pessoa. Desativação significa que todos os dados pessoais estão ocultos e não são processados de qualquer maneira desde que a pessoa continue desativada. As referências a uma pessoa desativada nos registros de eventos e trilhas de auditoria são substituídas temporariamente por **N/D**. Essas referências são recuperadas se uma pessoa for reativada. Somente administradores com permissão para **Desativar proprietário da chave** podem desativar pessoas, bem como visualizar e reativar pessoas desativadas.
- As informações sobre pessoas desativadas não podem ser editadas, excluídas, exportadas ou processadas de qualquer modo.
- Ao importar funcionários de um arquivo, os funcionários que estão desativados no CWM são ignorados mesmo se seus dados forem alterados no arquivo CSV.

Consulte também *Seção 4.1.3 "Desativação ou ativação de funcionários ou visitantes", página 25*.

Marcar como excluído
Configurado para **Marcado como excluído** a Exclusão de dados pessoais não segue o GDPR.

As pessoas excluídas não são removidas do banco de dados e uma pessoa excluída ainda será referenciados em, por exemplo, eventos e trilhas de auditoria. As pessoas excluídas podem ser recuperadas de acordo com *Seção 4.1.4 "Como excluir ou recuperar funcionários ou visitantes", página 26*. Uma pessoa que não foi marcada para ser excluída é descrita no

CWM como **Ativo** (não confundir com pessoas desativadas ou ativadas quando a configuração do sistema for **Excluir permanentemente**).

8.10 Logon único (SSO)

O Logon único (SSO) permite que os administradores acessem o sistema sem sua chave de comando.

A funcionalidade SSO deve ser configurada individualmente em cada sistema. Quando o SSO é compatível, o Super administrador pode ativar ou desativar o recurso conforme necessário. Consulte *"LOGON ÚNICO (SSO)"* em *Seção 6.4 "Como editar as configurações do sistema", página 99* para obter mais detalhes.

Quando ativada, um administrador que tenha recebido uma nova chave de comando deve primeiro registrar um certificado usando o CCPC e a chave de comando. Quando o registro do certificado for concluído com êxito, o administrador poderá fazer login no sistema sem a chave de comando.

Observe que determinadas operações no sistema, como os programas que exigem dados seguros armazenados na chave de comando, ainda exigem que o administrador faça login com a chave de comando. Nesses casos, uma mensagem pop-up solicitará que o usuário insira a chave de comando e faça a autenticação correspondente.

As funções a seguir exigem login com a chave de comando:

- Programação do cilindro local: envio de tarefas para a chave de comando, atualização de seu status e remoção de tarefas concluídas ou não concluídas
- Copiar configurações da chave
- Ativar importação de extensão
- Ativar ou desativar a recuperação de trilhas de auditoria automática na chave de comando
- Desbloquear a chave de comando
- Alterar PIN da chave de comando
- Atualize o status da chave de usuário inserida no programador local por meio da barra superior da página

8.11 Integração DCS

DCS é um aplicativo para servidor para gerenciar certificados e licenças em um Sistema CLIQ.

A **Integração DCS** ativa a geração automática de certificados para Chaves de comando e Programadores remotos e, portanto, elimina a necessidade de distribuir esses certificados separadamente. Também permite a obtenção de arquivos de licença, arquivos firmware e arquivos de extensão do DCS.

A integração DCS deve ser ativada durante a instalação do sistema.

Com a Integração DCS, são gerados certificados de Programadores remotos a partir do CWM, enquanto que os certificados das Chaves de comando são gerados por meio do **PC CLIQ Connect**.

O registro do certificado da chave de comando pode ser configurado para ser **Sempre permitida** (recomendado), **Permitida uma vez** ou **Não permitida**. Para a Chave de comando mestre isso é configurado no DCS e para configurações de Chaves de comando normais são feitos no CWM (consulte *Seção 6.11.4 "Como editar as informações de uma chave de comando", página 134*).

Tabela 4. Configuração do registro do certificado

Configuração	Descrição
Sempre permitida	O certificado da chave de comando pode ser inscrito várias vezes. Isso é útil se o proprietário da chave de comando precisa acessar o CWM a partir de mais de um computador.
Permitida uma vez	O certificado da chave de comando só pode ser inscrito uma vez.
Não permitida	O registro não é permitido.

ATENÇÃO!
A renovação do certificado é permitida seja qual for essa configuração.

Consulte *Seção 3.2.1 "Registro do certificado da Chave de comando via CLIQ Connect no computador", página 16* para gerar certificados para Chaves de comando.

Consulte *Seção 6.5.7 "Como configurar programadores de parede", página 109* ou *Seção 6.5.8 "Como configurar Programadores móveis", página 115* para gerar Certificados de Programadores remotos.

Consulte *Seção 6.1.1 "Como instalar licenças", página 98* para localizar um arquivo de licença a partir do DCS.

Consulte *Seção 6.16 "Importação de extensões", página 151* para localizar um arquivo de extensão a partir do DCS.

8.12 Integração com o LDAP

LDAP significa Protocolo de acesso ao diretório leve e é um protocolo de software que possibilita o acesso aos serviços de diretório. No contexto do CWM, o LDAP é usado como fonte principal das informações dos funcionários integrando com o CWM. O CWM suporta OpenLDAP, Microsoft Active Directory e Apache Directory.

Quando o LDAP está integrado, funcionários adicionados em um diretório ativo específico são sincronizados automaticamente (uma vez a cada 24 horas) ou manualmente com o CWM. No CWM, funcionários do LDAP coexistem com funcionários no CWM, e seus nomes, sobrenomes, e-mails e números de telefone celular estão visíveis e podem ser buscados.

Se o recurso do CLIQ Connect+ estiver ativado e o funcionário é um usuário ativado do CLIQ Connect+, não é possível desativar ou excluir o funcionário ou excluir o endereço de e-mail do funcionário. Consulte *Seção 8.3.4 "CLIQ Connect e CLIQ Connect+", página 182* para obter mais informações sobre o recurso do CLIQ Connect+.

Como as informações do LDAP são do tipo somente leitura, existem algumas restrições no gerenciamento do funcionário com CWM quando a integração com LDAP está ativada. *Tabela 34 "Atividades disponíveis no CWM quando o LDAP está integrado", página 191* exibe quais administradores podem gerir.

Tabela 5. Atividades disponíveis no CWM quando o LDAP está integrado

	Funcionário	
	com integração LDAP	**sem integração LDAP**
Adicionar	n/d	✓

Editar	✓* * somente **Domínio** e **ETIQUETAS** podem ser alterados no GUI.	✓
Excluir/desativar	n/d	✓

A integração com o LDAP é ativada ou desativada na página de **Configurações do sistema**. Consulte *Seção 6.4 "Como editar as configurações do sistema", página 99* para configurar a integração com o LDAP. Como pré-requisitos tanto a licença como a permissão para a integração com o LDAP devem ser concedidas aos administradores. Consulte *Seção 6.1 "Como administrar as licenças", página 98* para instalar a licença e *Seção 6.7 "Como gerenciar papéis e autorizações", página 127* para conceder a permissão.

8.13 Licenças

É necessária uma licença para poder usar o CWM. As licenças são emitidas por Sistema Cliq pelo fornecedor local CLIQ.

Uma licença básica sempre fornece acesso a funções básicas no CWM. Além disso, a disponibilidade dos seguintes recursos é controlada pelo conteúdo da licença.

- Remoto
- Domínios
- Perfis de acesso
- Grupos de acesso temporários
- Revalidação
- Revalidação flexível
- Grupos de cilindros
- Serviços de web
- Validação do PIN
- Integração com o LDAP
- Arquivo da trilha de auditoria ampliada e eventos
- CLIQ Connect+

Consulte *Seção 6.1.2 "Como visualizar o status da licença", página 98* para visualizar recursos licenciados disponíveis.

Para sistemas com **integração DCS** ativada, o CWM verifica automaticamente quanto a licenças disponíveis no DCS a cada 24 horas e na ativação do CWM. As licenças devem ser instaladas manualmente caso não exista uma licença disponível no DCS ou se a integração DCS são foi ativada. Consulte *Seção 6.1.1 "Como instalar licenças", página 98*.

Os arquivos de licença possuem um número de licença atribuído para que sejam criados. Só é possível instalar um arquivo de licença que foi criado depois que o arquivo instalado atualmente.

Vencimento da licença e notificação por e-mail

A licença possui uma **Data de vencimento leve** e uma **Data de vencimento rígida**.

Após o vencimento da data leve, serão enviados em-mail de notificação ao **Super administrador** todas as segundas-feiras até que a licença seja renovada. Por exemplo, se a data de vencimento leve for uma terça-feira, o primeiro e-mail será enviado na próxima

segunda-feira. Os administradores devem ter um endereço de e-mail registrado para que possam receber os e-mails. Também será exibida uma mensagem de aviso na interface do usuário do CWM. Entre em contato com o fornecedor local CLIQ para obter uma nova licença.

Se a data de vencimento rígida passar, o CWM será bloqueado na inicialização. Será exibida uma mensagem de aviso na página inicial e será enviado um e-mail para notificar sobre a data de vencimento. Entre em contato com o fornecedor local CLIQ para obter uma nova licença.

Consulte *Seção 6.1.1 "Como instalar licenças", página 98* para obter mais informações sobre como instalar as licenças.

Quando as licenças são controladas por um software externo (não o DCS), normalmente a renovação da licença é feita na data de vencimento leve. Nesse caso não é enviado qualquer e-mail de notificação.

9 Apêndice

9.1 Termos e siglas

9.1.1 Termos

Estado atual	Descreve o estado das autorizações de chave programadas atualmente nas chaves e cilindros. Consulte também **Estado definido**.
Lista de acesso do cilindro	Lista das chaves autorizadas, armazenada nos cilindros.
Sistema de grupo de cilindros	Um Sistema Cliq pré-definido para suportar grupos de cilindros.
Função de programação do cilindro	Uma função que contém atualizações para um cilindro, que pode ser executada no cilindro usando uma Chave de comando.
Reprogramação de cilindros	Essa operação limpa o conteúdo da memória de um cilindro e, em seguida, restaura a lista de acesso ao cilindro, a lista de chaves não autorizadas e outras configurações, como a diferença de fuso horário, do banco de dados.
Integração DCS	Um recurso no CWM que ativa a geração automática de certificados para Chaves de comando e programadores remotos.
Estado definido	Descreve o estado das autorizações de chave como definido no CWM. Este não é necessariamente o mesmo que o Estado atual, pois algumas autorizações podem não ter sido programadas ainda para chaves e cilindros. Consulte também **Estado atual**.
Elemento	As chaves e os cilindros CLIQ compõem os elementos CLIQ.
Acesso explícito	Entrada na Lista de acesso de uma chave dinâmica que é adicionada explicitamente a aquela chave. Consulte também **Acesso implícito**.
Extensão	Uma adição ao Sistema Cliq que contém chaves, grupos de chaves, cilindros, grupos de cilindros e programadores remotos novos.
Acesso implícito	Entrada na Lista de acesso de uma chave dinâmica que é adicionada por meio dos perfis de acesso associados com uma pessoa ou diretamente com uma chave. Consulte também **Acesso explícito**.
Lista de acesso da chave	Lista dos cilindros autorizados, armazenada nas Chaves dinâmicas.
Lista de chaves não autorizadas	Lista de chaves que foram bloqueadas para acesso a um cilindro, depois de terem sido comunicadas como perdidas.
Sistema Cliq	Um sistema de cilindros e chaves que são administrados em conjunto. Neste manual, o termo também está associado com os Programadores relacionados e informações relacionadas definidos no CWM (como autorizações eletrônicas, dados de funcionários e

	visitantes, definições de papéis de administrador, configurações do sistema, etc).
Objeto	Entidades que podem ser administradas por meio do CWM, como chaves, grupos de chaves, cilindros, grupos de cilindros, perfis de acesso, programadores remotos, funcionários e visitantes.
Sistema remoto	Um Sistema Cliq com a funcionalidade remota ativada.
Função de atualização remota	Uma função que contém atualizações para uma chave, que pode ser executada na chave inserindo-a em um Programador remoto.
USB On-The-Go	Um USB padrão que permite que os dispositivos USB atuem como host.

9.1.2 Siglas

CSV	Valores separados por vírgula (formato de arquivo)
CWM	CLIQ Web Manager
DCS	Servidor de conteúdo digital
GDPR	Norma geral de proteção de dados (uma norma da UE relacionada com o processamento de dados pessoais)
PD	Equipamento de programação
USB OTG	USB On-The-Go

9.2 Símbolos CWM

Chaves de usuário

 Chave mecânica

 Chave normal

 Chave Quartz

 Chave quartz do CLIQ Connect

 Chave dinâmica

 Chave dinâmica do CLIQ Connect

 Grupo de chaves normais

 Grupo de chaves dinâmicas

 Existe uma atualização remota pendente para a chave

 Existe uma atualização remota pendente que excede a capacidade da chave

Chaves de comando

 Chave de comando mestre

 Chave de comando normal

 Chave de comando normal CLIQ Connect

 Grupo de chaves de comando normais

 Grupo de chaves de comando mestres

 A função de programação não foi enviada a uma chave de comando

 A função de programação foi enviada a uma chave de comando mas ainda não foi iniciada

 Algumas funções de programação foram enviadas a uma chave de comando enquanto outras não

 A função de programação foi concluída

 Falha ou cancelamento da função de programação

 A função de programação foi substituída por uma nova função

Cilindros

 Cilindro eletrônico

 Cilindro mecânico

 Cilindro duplo (Exemplo: eletrônico no lado A e mecânico no lado B)

 As informações se relacionam ao lado A

 As informações se relacionam ao lado B

 Existe uma função de programação para o cilindro

 A função de programação do cilindro necessita aprovação

 Uma função de programação do cilindro foi programada para uma chave de comando

 A função de programação do cilindro foi concluída

 Falha ou cancelamento da função de programação do cilindro

 A função de programação do cilindro foi substituída por uma nova função

Autorizações

 Autorização explícita

 Autorização do perfil de acesso

Programadores remotos

 Programador de parede

 Programador móvel CLIQ

9.3 Atributos de objetos

9.3.1 Atributo de funcionário

Identificador	Um código ou ID exclusivo usado para distinguir essa pessoa individual de outras em um sistema
Cargo	Um prefixo de cortesia usado antes do nome, como Sr., Srta., Dr.
Nome	O nome de batismo da pessoa.

Sobrenome	A família ou o sobrenome da pessoa.
Domínio	O domínio ao qual a pessoa pertence.
Organização	A empresa ou instituição à qual a pessoa está afiliada.
Telefone	O número de telefone de contato da pessoa.
Departamento	A divisão ou unidade específica da organização em que a pessoa trabalha.
Função	O cargo ou o papel da pessoa na organização.
E-mail	O endereço de e-mail da pessoa.
Região	Uma área geográfica mais ampla na qual a pessoa está localizada (por exemplo, Europa, Oriente Médio e África (EMEA), Ásia-Pacífico (APAC)).
Idioma	O idioma principal que a pessoa usa para se comunicar.
Localização	Descrição geral do local onde a pessoa está baseada (pode se sobrepor a **Cidade** ou **Estado**).
Texto Gmd	
Rua	O endereço da rua onde a organização ou pessoa está localizada.
CEP	O código postal do endereço.
Cidade	A cidade onde a pessoa ou organização está localizada.
Estado	O estado, a província ou a região em um país.
Endereço da empresa	O endereço completo da organização ou local de trabalho da pessoa.

9.3.2 Atributo de visitante

Identificador	Um código ou ID exclusivo usado para distinguir essa pessoa individual de outras em um sistema
Cargo	Um prefixo de cortesia usado antes do nome, como Sr., Srta., Dr.
Nome	O nome de batismo da pessoa.
Sobrenome	A família ou o sobrenome da pessoa.
Domínio	O domínio ao qual a pessoa pertence.
Organização	A empresa ou instituição à qual a pessoa está afiliada.
Telefone	O número de telefone de contato da pessoa.
Departamento	A divisão ou unidade específica da organização em que a pessoa trabalha.

Função	O cargo ou o papel da pessoa na organização.
E-mail	O endereço de e-mail da pessoa.
Região	Uma área geográfica mais ampla na qual a pessoa está localizada (por exemplo, Europa, Oriente Médio e África (EMEA), Ásia-Pacífico (APAC)).
Idioma	O idioma principal que a pessoa usa para se comunicar.
Localização	Descrição geral do local onde a pessoa está baseada (pode se sobrepor a **Cidade** ou **Estado**).
Rua	O endereço da rua onde a organização ou pessoa está localizada.
CEP	O código postal do endereço.
Cidade	A cidade onde a pessoa ou organização está localizada.
Estado	O estado, a província ou a região em um país.
Endereço da empresa	O endereço completo da organização ou local de trabalho da pessoa.

9.3.3 Atributos de chaves

Nome	Nome de uma chave.
Proprietário da chave	A pessoa para quem a chave foi entregue atualmente.
Marcação	A marcação da chave.
Segunda marcação	Marcação alternativa (nem sempre é usada).
Formato da chave	O corte mecânico da chave.
Grupo	O grupo de chaves ao qual a chave pertence.
Tipo	O tipo de chave. Consulte *Seção 7.2.3 "Chaves de usuário", página 155* para obter mais informações.
Firmware	A versão do firmware.
Geração	A geração da chave.
Status	O status da chave (**Em estoque**, **Entregue**, **Perdida** ou **Quebrada**).
Número da linha	Não usado.
A última atualização remota	Data e hora da última atualização através de um Programador remoto.
Tamanho da lista de acesso	Entradas usadas / Número máximo de entradas na Lista de acesso da chave.
Suporte a diferença de fuso horário	Mostra se a funcionalidade de suporte a diferença de fuso horário é compatível.

Etiquetas	Etiquetas definidas para a chave.
Links externos	URLs associadas com a chave.

9.3.4 Atributos da chave de comando

Nome	Nome da chave de comando.
Proprietário da chave	O funcionário para quem a chave de comando foi entregue atualmente.
Marcação	A marcação da chave de comando.
Segunda marcação	Marcação alternativa (nem sempre é usada).
Grupo	O grupo de chaves ao qual pertence a chave de comando.
Tipo	O tipo da chave de comando. Consulte *Seção 7.2.4 "Chaves de comando", página 156* para obter mais informações.
Firmware	A versão do firmware.
Geração	A geração da chave de comando.
Suporte remoto	
Reprogramação de cilindro	Se a chave de comando possui o direito de executar Tarefas de reprogramação de cilindro.
Programação de grupo de cilindros	Se a chave de comando pode executar Tarefas de programação de cilindros que alteram o grupo de cilindros do cilindro.
Atualização do firmware do cilindro	Se a chave de comando pode atualizar o firmware do cilindro ou não (em desenvolvimento).
Status	O status da chave de comando (**Em estoque**, **Entregue**, **Perdida** ou **Quebrada**).
Bloqueado	Se a chave de comando está bloqueada para todos os acessos.
Configurações de validade	Configuração de validade da chave de comando.
Registro do certificado	Se é permitido o registro do certificado.
Papéis	Quais papéis estão associados com a chave de comando.

9.3.5 Atributos do cilindro

Nome	Nome do cilindro.
Marcação	A marcação do cilindro.
Status	O status do cilindro (**In Em estoque**, **Instalado** ou **Quebrado**).

Localização	A localização do cilindro.
Fuso horário de base	O fuso horário do local do cilindro.
Modelo do cilindro	O modelo do cilindro.
Comprimento	O comprimento físico do cilindro. Para cilindros duplos, o comprimento é representado por um número para cada lado. Para um cilindro com um lado cego ou uma maçaneta, o comprimento é representado por um número para o comprimento do cilindro e um número para o comprimento do lado cego/maçaneta.
Número da linha	Não usado.
Bloqueado por	A chave de comando para a qual estão carregadas funções de programação do cilindro pendentes. Enquanto a função de programação de um cilindro é carregada para uma Chave de comando, as configurações para esse cilindro estão bloqueadas para edição no CWM.
Lado do cilindro	**A** ou **B** (para cilindro duplos)
Tipo	**E** (Eletrônico) ou **M** (Mecânico).
Grupo	O grupo de cilindros a qual o cilindro pertence.
Firmware	A versão do firmware do cilindro.
Diferença de fuso horário	A diferença de fuso horário do cilindro, em comparação com o fuso horário base.
Domínio	O domínio a qual o cilindro pertence.
Etiquetas	Etiquetas definidas para o cilindro.
Links externos	URLs associadas com o cilindro.

9.3.6 Atributos do programador remoto

Nome	Nome do programador remoto.
Marcação	Marcação do programador remoto.
Tipo	**Programador móvel** ou **Programador de parede**.
Geração	Geração do programador de parede.
Endereço MAC	O endereço físico do programador remoto.
GR	ID do grupo (somente para uso interno).
UID	ID exclusiva (somente para uso interno).
Firmware	A versão do firmware.

Carregador de boot (somente geração 1) Versão do firmware do carregador de boot.

Status Status do inventário (**Em estoque**, **Instalado**, **Entregue** ou **Perdido**).

Status operacional (**Quebrado**).

Status da conexão **Offline** ou **On-line**.

Última conexão Programador móvel: a data e hora da última vez que o Programador móvel esteve on-line.

Último endereço IP conhecido Endereço IP onde o programador remoto esteve online da última vez.

Etiquetas Etiquetas definidas para o Programador remoto.

Links externos URLs associadas com o Programador remoto.

9.4 Permissões

Poderá ser selecionado, **Nenhum**, **Lista**, **Visualizar** ou **Total** para cada permissão. **Visualizar** inclui automaticamente **Lista** e **Total** inclui automaticamente **Visualizar** e **Lista**.

Caso existam dependências entre permissões, elas estão listadas na coluna **Dependências**. Por exemplo, são necessárias para ser possível dar permissões para Autorizações de chaves, Permissão de visualização para chaves e permissão de lista para cilindros.

Permissão	Nenhum	Lista Os elementos são listados	Visualizar Podem ser acessados detalhes para os elementos listados	Cheio Podem ser acessados e manipulados detalhes para os elementos listados	Dependências
Perfis de acesso Controla a administração de perfis de acesso (criar, excluir, editar).		⊗	Pode visualizar detalhes do perfil de acesso.	Pode criar perfis de acesso novos e editar os existentes, exceto a lista de acesso que é controlada pela permissão de autorização de perfil de acesso.	
Perfil de acesso: Autorização Controla a configuração de autorizações para um perfil de acesso.		⊗	Pode visualizar autorizações em um perfil de acesso.	Pode adicionar ou remover autorizações em um perfil de acesso.	Requer permissão de visualização para **Acessar perfil**.

Permissão	Nenhum	Lista Os elementos são listados	Visualizar Podem ser acessados detalhes para os elementos listados	Cheio Podem ser acessados e manipulados detalhes para os elementos listados	Dependências
Aprovações		Opção de menu **Programas para aprovação** disponível. Pode visualizar uma lista das solicitações de trilhas de auditoria para aprovação.	⊗	Pode aprovar as solicitações de trilhas de auditoria. Somente papel de aprovador e não pode ser editado.	Aplicável somente se a configuração de aprovação é ativada durante a instalação inicial.
Trilha de auditoria			Guia trilha de auditoria é visível na tela de chaves e na tela de cilindros.	Pode solicitar trilhas de auditoria para cilindros e chaves via guia de trilhas de auditoria.	
Trilha de auditoria: Automático		⊗	Permissão para visualizar o status de recuperação das trilhas de auditoria automáticas para chaves de comando.	Permissão para visualizar o status de recuperação das trilhas de auditoria automáticas para chaves de comando.	Exige no mínimo permissão de visualização para **Chave de comando**.
Chave de comando	⊗	⊗	Pode visualizar os detalhes da Chave de comando.	Pode editar os detalhes e entregar as chaves de comando.	
Chave de comando: devolução/entrega		⊗	⊗	Pode entregar e devolver chaves de comando.	Exige permissão de lista para **Proprietário da chave: funcionário** e permissão de visualização para **Chave de comando**.

Permissão	Nenhum	Lista Os elementos são listados	Visualizar Podem ser acessados detalhes para os elementos listados	Cheio Podem ser acessados e manipulados detalhes para os elementos listados	Dependências
Cilindro		Pode ser selecionado quando **Cilindro: autorização** é Nenhum.	Pode visualizar detalhes de cilindros.	Pode editar detalhes do cilindro e alterar o status do cilindro.	
Cilindro: Autorização			Pode visualizar autorizações para um cilindro.	Pode editar autorizações para um cilindro e solicitar reprogramação de cilindros.	Exige permissão de visualização para **Cilindro** e permissão de lista para **Chave**.
Cilindro: Programando		⊗	⊗	Pode enviar funções de programação a Chaves de comando.	Requer permissão de lista para **Cilindro**.
Domínio (Não é necessária permissão para visualizar os membros de domínios e autorizações de domínios para chaves de comando.)		⊗	⊗	Pode administrar domínios (adicionar, remover, editar) e alterar autorizações de domínios para chaves de comando.	
Firmware		⊗	⊗	Pode importar firmware.	A atualização de firmware exige permissão total para **Programadores remotos**.
Revalidação flexível (Pode ver os intervalos de revalidação caso a revalidação flexível esteja ativada.)		⊗	⊗	Pode editar intervalos de revalidação para perfis de acesso e grupos de cilindros.	

Permissão	Nenhum	Lista Os elementos são listados	Visualizar Podem ser acessados detalhes para os elementos listados	Cheio Podem ser acessados e manipulados detalhes para os elementos listados	Dependências
Chave	Pode ser selecionado quando **Cilindro: autorização** é Nenhum.	Pode listar chaves indiretamente.	Opção de menu **Chaves** disponível. Pode visualizar detalhes de chaves.	Pode editar detalhes da chave e o status de operação.	
Chave: Autorização		Pode ser selecionado quando **Chave: autorização** é Nenhum.	Pode visualizar autorizações para uma chave.	Pode editar autorizações para uma chave.	Exige permissão de visualização para **Chave** e permissão de lista para **Cilindro**.
Chave: Devolução/Entrega		⊗	⊗	Opções de menu **Devolver chave** e **Entregar chave** disponíveis. Pode executar devoluções e entregas.	Exige permissões de lista para **Proprietário da chave: funcionário**, **Proprietário da chave: visitante**, , **Chave** e **Cilindro** e permissões totais para **Chave: autorização**.
Chave: Agenda	⊗	⊗		Pode editar o cronograma para uma chave, configurar um cronograma para um grupo de chaves e configurar o cronograma ao entregar a chave.	Exige permissão total para **Modelo: aplicar cronograma conforme o modelo** e permissão de visualização para **Chave**.
Chave: Atualizar histórico		⊗	Pode visualizar a atualização de histórico na guia **Atualizar histórico**.	⊗	Requer permissão de visualização para **Chave**.

Permissão	Nenhum	Lista Os elementos são listados	Visualizar Podem ser acessados detalhes para os elementos listados	Cheio Podem ser acessados e manipulados detalhes para os elementos listados	Dependências
Chave: Validade	⊗	⊗		Pode editar configurações de validade em lotes para chaves, editar as configurações de validade da chave e configurar a validade ao entregar a chave.	Requer permissão de visualização para **Chave**.
Proprietário da chave: Desativar		⊗	⊗	Pode desativar pessoas, bem como buscar e ativar pessoas desativadas.	Necessita de permissão total para **Proprietário da chave: funcionário** e **Proprietário da chave: visitante**
Proprietário da chave: Funcionário	⊗	⊗	⊗	Pode editar detalhes de funcionários.	
Proprietário da chave: Importação de funcionários		⊗	⊗	Pode importar dados de funcionários.	Exige permissão total para **Proprietário da chave: funcionário**.
Proprietário da chave: Visitante	⊗	⊗	⊗	Pode editar detalhes de visitantes.	
Integração com o LDAP		⊗	Pode visualizar as configurações da **Integração com o LDAP** na página de configurações do sistema.	Pode editar as configurações da **Integração com o LDAP** na página de configurações do sistema.	Requer permissão de visualização para **Configurações do sistema**.
Manutenção		⊗	⊗	Pode travar e destravar o sistema.	

Permissão	Nenhum	Lista Os elementos são listados	Visualizar Podem ser acessados detalhes para os elementos listados	Cheio Podem ser acessados e manipulados detalhes para os elementos listados	Dependências
Programadores remotos		Pode listar os Programadores remotos indiretamente.	Opção de menu **Programadores remotos** disponível. Pode visualizar os detalhes dos Programadores remotos.	Pode editar as configurações, atualizar o firmware dos programadores remotos e alternar os Programadores de parede para o modo de atualização de chave para uso com a atualização do firmware da chave.	
Papéis	⊗		Opção de menu **Papéis** disponível. Pode visualizar a lista de papéis e ver detalhes de um papel.	Pode administrar papéis (criar, editar, excluir) e atribuir papéis a chaves de comando.	
Estatísticas		⊗	Pode visualizar as estatísticas do sistema.	⊗	
Configurações do sistema	⊗	⊗			
Status do sistema		⊗	Opção de menu **Status do sistema** disponível. Pode visualizar o status do sistema.	⊗	Requer permissão de lista para **Programadores remotos**.
Modelo: Aplicar cronograma conforme o modelo	⊗	⊗	⊗	Pode aplicar o modelo de cronograma para uma chave e aplicar o modelo de cronograma ao entregar uma chave.	Requer permissão de visualização para **Chave**.
Modelo: Recibo			Opção de menu **Modelos de recibo** disponível. Pode imprimir recibos e visualizar modelos de recibos.	Pode criar, editar e excluir modelos de recibos	

Permissão	Nenhum	Lista Os elementos são listados	Visualizar Podem ser acessados detalhes para os elementos listados	Cheio Podem ser acessados e manipulados detalhes para os elementos listados	Dependências
Modelo: Agenda	⊗		Pode visualizar os modelos de cronograma.	Pode editar os modelos de cronograma.	
Grupo de acesso temporário		⊗	Pode visualizar os grupos de acesso temporários.	Pode editar os grupos de acesso temporários.	

9.5 Indicações do programador remoto

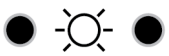
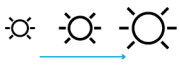
9.5.1 Indicações de programador de parede (Geração 1) e programador móvel

Indicações LED		Aviso sonoro	Interpretação
 Branco sólido			**Ligado e online**
 Piscando rápido em branco			**Programador de parede: adquirindo endereço IP** **Programador móvel: inicializando a conexão por USB ou Bluetooth**
 Piscando devagar em branco			**Conexão ao servidor remoto durante a sequência de configuração**
	 Sólido	1 bipe longo	**Atualização off-line concluída OK**
 Vermelho sólido			**Bateria do Programador móvel fraca**
 Uma piscada em vermelho	 Uma piscada		**Bateria do Programador móvel extremamente fraca**
 Sólido			**Bateria da chave fraca**
 Piscando			**Conectando durante a atualização remota**
 Sólido			**Conectado durante a atualização remota**

Indicações LED	Aviso sonoro	Interpretação
		Atualização de firmware concluída
 Sólido	1 bipe	**Operação concluída com êxito** **Configurações do programador remoto atualizadas**
 Piscando		**Baixando e processando**
 Sólido	1 bipe	**E-mail enviado**
 Sólido	3 bipes	**Operação concluída com erro**

Para operações que envolvem uma chave, emite bipes a cada três segundos até que a chave seja removida.

9.5.2 Indicações de programador de parede (geração 2)

Indicações LED	Aviso sonoro	Interpretação
 Esquerda: Pulso azul Centro: Desligado Direta: Desligado		**Verificação das configurações 802.1x**
 Esquerda: Azul sólido Centro: Pulso azul Direta: Desligado		**Adquirindo endereço IP**
 Esquerda: Azul sólido Centro: Azul sólido Direta: Pulso azul		**Estabelecendo conexão com o servidor**
 Esquerda: Desligado Centro: Branco sólido Direta: Desligado		**Conectado e pronto para uso**
 Esquerda: Desligado Centro: Pulso branco Direta: Desligado		**Perda de conexão**
 LEDs começam a piscar em branco a partir da esquerda		**Atualização de chave em andamento**
 LEDs começam a piscar em azul a partir da esquerda		**Atualização de firmware ou de parâmetro em andamento**

Indicações LED		Aviso sonoro	Interpretação
	Marca de seleção verde	2 bipes aumentando	**Operação concluída com êxito**
	Cruz vermelha	2 bipes diminuindo	**Operação concluída com erro para operações**
	Bateria vermelha		**Bateria da chave fraca**

9.6 Indicações do nível da bateria

O nível da bateria da chave atualmente digitalizada na ranhura direita é indicado pelos seguintes símbolos.

Indicação do nível da bateria	Interpretação
	**Nível da bateria excelente**
	**Nível da bateria bom**
	**Nível da bateria baixo**
	**Nível da bateria muito fraco**

9.7 Função dependente do firmware

Tabela 51 "Exigências de firmware", página 209 lista os recursos do CWM e a versão mais antiga de firmware necessária para os programadores, chaves e cilindros.

Tabela 6. Exigências de firmware

Recurso	Menor FW suportado	
Recuperação de trilhas de auditoria automática	Chave e chave de comando	12.7.0
Atualização do firmware da chave de comando	Programador de parede e programador móvel CLIQ	6.3
	Chave de comando	12.0.0
Compatibilidade do programador móvel CLIQ Connect	Chave	12.3
Suporte ao grupo de cilindros	Chave	6.3.1
	Cilindro	5.3.1

Recurso	Menor FW suportado	
Revalidação flexível	Chave	6.3.1
Atualização das informações de firmware da chave via Programador remoto	Chave	12.3
Atualização offline	Chave	6.3.1
Validação do PIN	Chave	16.0.0
Plug & Play para programadores remotos	Programador de parede e programador móvel CLIQ	6.2.1
Suporte de proxy para programadores remotos	Programador de parede e programador móvel CLIQ	6.2.1
Atualização remota da chave de comando	Chave de comando	12.0.0
Suporte remoto	Chave	3.0
	Chave de comando	12.0.0
Revalidação	Chave	3.0
Tipo de cronograma - básico	Chave	Somente 1.x, 3.x, 5.x
Tipo de cronograma - várias janelas de tempo	Chave	2.x, 4.x, 6.x, 10 ou superior
Diferença de fuso horário	Chave, chave de comando e cilindro	10.0.0
Atualização de firmware da chave de usuário (geração 2)	Chave	10.1

Para visualização da versão do firmware de uma chave, visualize as informações detalhadas. Consulte *Seção 4.2.1 "Como buscar chaves de usuário", página 34* ou *Seção 4.2.2 "Como escanear uma chave de usuário", página 35*.

Para visualizar a versão do firmware de um Programador de parede, visualize as informações detalhadas. Consulte *Seção 6.5.2 "Como buscar Programadores remotos", página 104*.

Para visualizar a versão do firmware de um programador móvel CLIQ, visualize as informações detalhadas. Consulte *Seção 6.5.2 "Como buscar Programadores remotos", página 104*.

9.8 Requisitos do PC cliente

Produto	Requisitos
Sistema operacional	• Windows 10 (64-bit) • Windows 11
Navegador da Internet	• Firefox ESR 138 ou posterior • Firefox 138 ou posterior • Google Chrome 136 ou posterior • Microsoft Edge 136 ou posterior * O suporte para o Internet Explorer está sendo descontinuado devido ao final de vida útil desse navegador.
PDF Reader	Qualquer (Testado com Adobe Reader)

9.9 Formato de arquivo de importação de funcionário

É necessário um arquivo com o formato e conteúdo corretos para ser possível importar os dados de funcionários.

Formato de arquivo
O formato do arquivo é CSV (valores separados por vírgula), com codificação de caracteres **Unicode UTF-8**.

> **Dica**
> Para se certificar de que o arquivo CSV possui a codificação correta, poderá ser usado ou **Windows Notepad**. Abra o arquivo CSV no Notepad, selecione **Arquivo » Salvar como ...**, selecione codificação **UTF-8** e clique em **Gravar**.

Tamanho do arquivo
O tamanho máximo permitido do arquivo a ser importado para o CWM é 7,0 MB.

Conteúdo do arquivo
O delimitador necessário é a vírgula (,) ou ponto e vírgula (;). A configuração do sistema **delimitador CSV** não afeta a importação.

A primeira linha é um cabeçalho que representa todos os campos de nomes separados por vírgula (uma descrição dos campos) O cabeçalho é validado e específico do idioma, ou seja, o texto no cabeçalho deve estar de acordo com as definições do idioma selecionado.

> **Dica**
> Um cabeçalho correto pode ser localizado exportando os funcionários para um arquivo CSV e então removendo todas as informações exceto a primeira linha. Ao exportar os funcionários, um campo extra, **Etiquetas**, é adicionado após os outros campos. Esse campo pode ser mantido no arquivo porém será ignorado durante a importação.
>
> Consulte *Seção 4.1.12 "Como exportar informações do funcionário ou visitante", página 33*.

Cada uma das linhas abaixo representa um funcionário. Os valores do campo são separados com o delimitador e a ordem dos campos deve corresponder a do cabeçalho. Se um campo deve incluir o caractere do delimitador (vírgula ou ponto e vírgula), todo o campo de dados deve ser colocado entre aspas ("), por exemplo `"11 Wall St, New York, NY"`.

> **ATENÇÃO!**
> Se um campo está vazio, o delimitador ainda deverá estar presente.

Os campos e as exigências estão listados em *Tabela 53 "Estrutura do arquivo CSV", página 211*.

Tabela 7. Estrutura do arquivo CSV

Nº. do campo	Nome	Obrigatório	Nº. de caracteres
1	Identificador		1-50
2	Cargo		0-100
3	Nome	✓	1-49

Nº. do campo	Nome	Obrigatório	Nº. de caracteres
4	Sobrenome	✓	1-49
5	Domínio		0-100
6	E-mail		0-100
7	Telefone		0-100
8	Organização		0-100
9	Departamento		0-100
10	Rua		0-100
11	CEP		0-100
12	Idioma		0-100
13	Região		0-100
14	Função		0-100
15	Cidade		0-100
16	Estado		0-100
17	País		0-100
18	Endereço da empresa		0-100
19	Localização		0-100
20	Número de celular		0-100
21	Texto Gmd		0-100

O **identificador** deve ser exclusivo. As informações no sistema são substituídas pelas informações no arquivo para funcionários no arquivo que possuem o **identificador** idêntico a um funcionário que já está no sistema. Entretanto, se um funcionário é adicionado no CWM e então importado sem que o **identificador** seja especificado no campo, o resultado serão entradas duplicadas para esse funcionário.

ATENÇÃO!
Funcionários no arquivo CSV com o mesmo identificador que um funcionários desativado no CWM são ignorados e não são importados.

O **E-mail** deverá ser especificado em um formato de e-mail correto.

ATENÇÃO!
Existem limitações para editar ou excluir o endereço de e-mail de um funcionário ou visitante com o status de usuário do CLIQ Connect+ ativado. Consulte *Seção 4.1.6.1 "Informações importantes sobre a edição ou exclusão de um endereço de e-mail", página 29* para obter mais informações.

O número máximo de funcionários em uma página é 10 000.

Arquivo de exemplo

```
Identificador,Título,Nome ,Sobrenome,Domínio,
E-
mail,Telefone,Empresa,Departamento,Endereço,CEP,Idioma,Região,C
argo,Cidade,Estado,País,Endereço
da empresa,Local,Celular ,Texto gmd

P0,Professor,George,Whitmore,Stockholm,George.Whitmore@assaablo
y.com,3719253729973267730,ASSA ABLOY,Shared Technologies,,,Swed
ish,,System Developer,Stockholm,,Sweden,"Formansvagen 11, 117 4
3 Stockholm",,070-6972135783866065282,GmdText
```

9.10 Código da empresa operadora ASSA ABLOY

Código	Empresa operadora
0	Nenhuma empresa especificada
1	ASSA ABLOY Opening Solutions Sweden (ASSA)
2	ABLOY
3	IKON
4	VACHETTE
6	MEDECO
7	SARGENT
8	ARROW
9	LAPERCHE
10	ASSA ABLOY Opening Solutions Norway (TRIOVING)
11	ASSA ABLOY Opening Solutions Denmark (RUKO)
12	MUL-T-LOCK
13	ASSA US
14	ASSA UK
15	ASSA BALT
16	MEDECO CANADA
17	FAB
18	AA Japan
19	TESA
20	AA Nova Zelândia
21	AA Australia
22	AA Singapore
23	AA Hong Kong
24	AA China
25	AA India
26	KESO
27	Corbin Russwin
28	ABLOY UK
29	ABLOY US

9.11 Informações de suporte de software

9.11.1 Como contatar o suporte de software

Caso tenha algum problema ao usar o CLIQ Web Manager ou qualquer dispositivo de hardware como chaves, cilindros ou dispositivos de programação, entre em contato com o fornecedor CLIQ. Tenha em mãos o número do sistema da chave mestre e a versão do Web Manager em uso para todas as comunicações relacionadas com manutenções. Ao escrever e-mails adicione sempre o número do sistema de chave mestre no cabeçalho do e-mail.

ASSA ABLOY is the global leader in door opening solutions, dedicated to satisfying end-user needs for security, safety and convenience.

IKON
ASSA ABLOY

ASSA ABLOY Sicherheitstechnik GmbH

Attilastrasse 61-67
12105 Berlin
GERMANY
Tel. + 49 30 8106-0
Fax: + 49 30 8106-26 00
berlin@assaabloy.com

www.assaabloy.de

Sujeito a alterações técnicas. Program version: V 2025.1. Document number: PB00023 00017 0PT. Language: pt-BR. Published: 2025-05-22.