Autenticação mútua (certificado digital)

O Cronapp dá suporte a autenticação mútua adicionando um novo fator de segurança a sua aplicação.

Nessa página

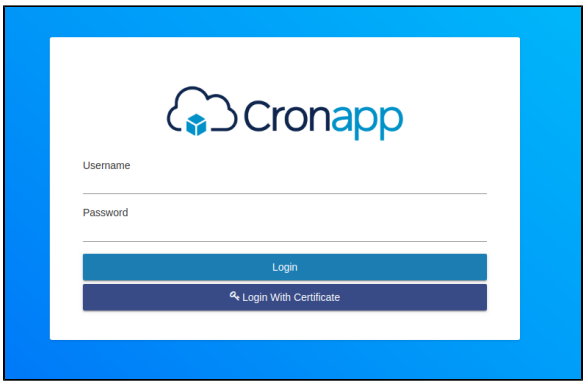

Figura 1 - Login com Certificado digital

A autenticação mútua (certificado digital) no Cronapp não funciona com as aplicações mobile.
As configurações apresentadas nessa documentação se aplicam ao ambiente servidor da aplicação.

Instalar e configurar seu certificado SSL

Depois de validar e emitir seu certificado SSL, você pode instalá-lo no servidor Apache (onde o CSR foi gerado) e configurar o servidor para usar o certificado.

Como instalar e configurar seu certificado SSL no servidor Apache

- Copie os arquivos do certificado para o seu servidor.
- Copie os arquivos (SeuCert.crt) e seu certificado primário (Seu_Dominio.crt).
- Copie esses arquivos, juntamente com o arquivo *.key que você gerou ao criar o CSR, para o diretório no servidor em que você mantém o certificado e os arquivos de chave.

  Nota

  Torne-os legíveis pela raiz apenas para aumentar a segurança
- Encontre o arquivo de configuração do Apache (httpd.conf) que você precisa editar.
- O local e o nome do arquivo de configuração podem variar de servidor para servidor, especialmente se você estiver usando uma interface especial para gerenciar a configuração do servidor.
- O arquivo de configuração principal do Apache geralmente é chamado httpd.conf ou apache2.conf. Os locais possíveis para esse arquivo incluem `/etc/httpd/ou/etc/apache2/`.

Geralmente, a configuração do certificado SSL está localizada em um bloco <VirtualHost> em um arquivo de configuração diferente. Os arquivos de configuração podem estar em um diretório como `/etc/httpd/vhosts.d/`, `/etc/httpd/sites/` ou em um arquivo chamado httpd-ssl.conf. Uma maneira de localizar a configuração SSL nas distribuições do Linux é pesquisar usando grep, conforme mostrado no exemplo abaixo:

```
grep -i -r "SSLCertificateFile" /etc/httpd/
```

Nota

Certifique-se de substituir / etc / httpd / pelo diretório base para sua instalação do Apache.

- Identifique o bloco SSL <VirtualHost> que você precisa configurar.
- Se o seu site precisar ser acessível por conexões seguras (https) e não seguras (http), você precisará de um host virtual para cada tipo de conexão. Faça uma cópia do host virtual não seguro existente e configure-o para SSL, conforme descrito acima.

- Se seu site precisar ser acessado apenas com segurança, configure o host virtual existente para SSL, conforme descrito acima.
- Configure o bloco <VirtualHost> para o site habilitado para SSL

Abaixo está um exemplo muito simples de um host virtual configurado para SSL.

```
<VirtualHost 192.168.0.1:443>
        <Location "/mutual">
                SSLVerifyClient require
                SSLVerifyDepth 5
                SSLOptions +StdEnvVars
                RequestHeader set SSL_CLIENT_S_DN "%{SSL_CLIENT_S_DN}s"
        </Location>

        DocumentRoot /var/www/html2
        ServerName www.seudominio.com
        SSLEngine on
        SSLProtocol TLSv1.2
        SSLCipherSuite HIGH:!aNULL:!MD5
    SSLHonorCipherOrder on
        SSLCertificateFile /caminho/para/Seu_Dominio.crt
        SSLCertificateKeyFile /caminho/para/Sua_chave_privada.key
        SSLCertificateChainFile /caminho/para/SeuCert.crt
</VirtualHost>
```

Certifique-se de ajustar os campos e os nomes dos arquivos para corresponder aos seus arquivos de certificado.

- **SSLEngine**: habilita o protocolo SSL.
- **SSLProtocol**: determina quais os protocolos SSL serão permitidos, estamos definindo apenas o TLSv1.2.
- **SSLCipherSuite**: algoritmo utilizado para encriptação. Nessa configuração não será usado o MD5.
- **SSLHonorCipherOrder**: estabelece que a ordem do *cipher* deve ser respeitada.
- **SSLCertificateFile**: seu arquivo de certificado (por exemplo, Seu_Dominio.crt).
- **SSLCertificateKeyFile**: arquivo .key gerado no memento que você criou o CSR (por exemplo, Sua_chave_privada.key).
- **SSLCertificateChainFile**: arquivo de certificado intermediário (por exemplo, SeuCert.crt).

Nota

Se a diretiva SSLCertificateChainFile não funcionar, tente usar a diretiva SSLCACertificateFile.

Teste seu arquivo de configuração do Apache antes de reiniciar.

Como prática recomendada, verifique se há erros no arquivo de configuração do Apache antes de reiniciar o Apache.

Cuidado

O Apache não será iniciado novamente se seus arquivos de configuração tiverem erros de sintaxe.

- Execute o seguinte comando para testar seu arquivo de configuração (em alguns sistemas, é apache2ctl):
  `apachectl configtest`
- Reinicie o Apache

Você pode usar os comandos apachectl para parar e iniciar o Apache com suporte a SSL. Mas antes, verifique se possui algum erro de sintax no que foi configurado:

```
apachectl configtest
```

Após o Apache retornar a mensagem "`Syntax OK`", pare e inicie em seguida usando os comandos:

```
apachectl stop
apachectl start
```

Reinicie o Notes

Se o Apache não reiniciar com o suporte SSL, tente usar o `apachectl beginsl` em vez do `apachectl start`. Se o suporte a SSL for carregado apenas com `apachectl runssl`, recomendamos que você ajuste a configuração de inicialização do apache para incluir suporte SSL no comando `apachectl start` regular. Caso contrário, seu servidor poderá exigir a reinicialização manual do Apache usando o a `pachectl winssl` no caso de uma reinicialização do servidor. Isso geralmente envolve a remoção das tags <IfDefine SSL> e </IfDefine> que incluem sua configuração SSL.

Parabéns! Você instalou seu certificado SSL com sucesso.

Configurando o apache como proxy Reverso

Para utilizar a autenticação mútua com certificado SSL, precisaremos configurar um servidor de Web como Proxy Reverso.

Adicione as seguintes configurações no seu Virtual Host

```
ProxyPreserveHost on
RequestHeader set X-Forwarded-Proto https
RequestHeader set X-Forwarded-Port 443
ProxyPass / http://<URL_DO_Servidor>:<PORTA>/
ProxyPassReverse / http://<URL_DO_Servidor>:<PORTA>/
```

Habilitando o login com certificado no Cronapp

Faça o login utilizando seu usuário e senha.

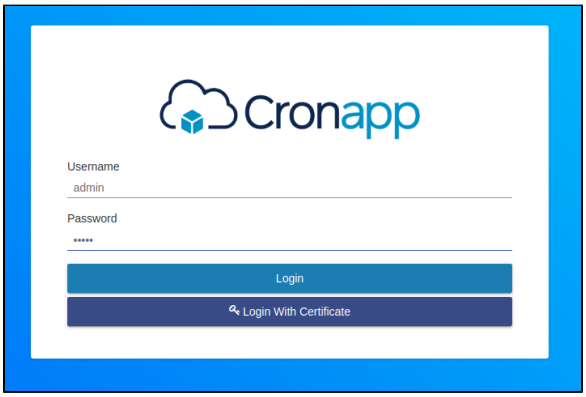

Figura 2 - Login com Certificado digital (habilitando o certificado)

Na página **Home**, clique em **Perfil** (profile) > **Vincular Certificado** (Link certificate), como na figura 2.1.

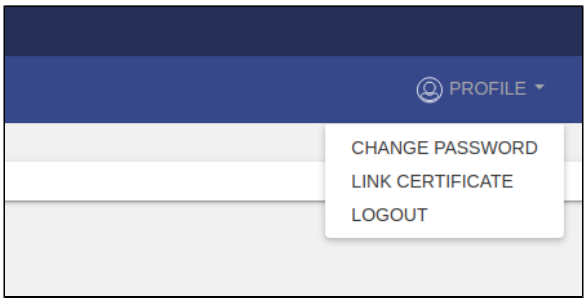

Figura 2.1 - Opção de vincular certificado

Aguarde a confirmação da aplicação (Figura 2.2).

Neste passo a aplicação irá referenciar o certificado que consta no servidor com o certificado que está sendo enviado pela aplicação.

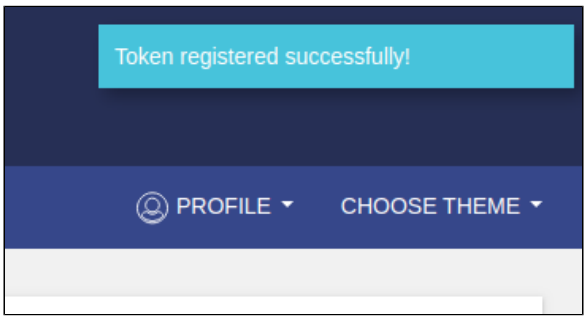

Figura 2.2 - Notificação de vinculo do certificado

Pronto! Seu certificado estará vinculado ao seu usuário e você poderá logar na próxima vez a partir do botão **Login with certificate** na tela de **Login** da aplicação (Figura 2).