Procedimento para integração de Sistemas de Informação a Senha Única / Autenticação Central (CAD-A-005/2017)

I) Glossário

CAD-A-005/2017	Artigo 1º - A Unicamp adotará um mecanismo de senha única para acesso em todos os seus sistemas computacionais.
CLIENTE	Órgão, instituto, faculdade ou unidade administrativa da universidade que, segundo a CAD-A-005/2017, deve integrar seus Sistemas de Informação na Autenticação Central.
SISTEMA CLIENTE	Sistema de informação ou software do CLIENTE que vai ser integrado a esta solução.
Usuário Unicamp	Usuário e senha cadastrados no Senha Unicamp. O repositório de usuários é o LDAP / SiSe provido pelo CCUEC que atende serviços de amplo uso pela comunidade, compreendendo assim a maior parte dos colaboradores e todos alunos da universidade.

II) Solução

Permitir que sistemas desenvolvidos em diferentes linguagens e plataformas possam utilizar, de maneira padronizada e segura, um repositório único de usuários para autenticação. A partir de um serviço central de autenticação, unificado entre os sistemas (*Single Sign On*), será melhorada a experiência do usuário, bem como eliminada a criação redundante de usuário e senha.
Foi selecionado o software Red Hat SSO (baseado no Keycloak, porém com suporte técnico e com garantia de eventuais correções necessárias) para ser o pilar desse serviço. Ele trabalha com protocolos padrão de mercado como OAuth 2, OpenId Connect e SAML para reforçar a segurança da autenticação.
A infra-estrutura computacional deste serviço provê redundância ativa em dois datacenters da universidade, distribuição de carga e tolerância a falhas pelo virtualizador.

III) Pré-requisito

Os utilizadores dos SISTEMAS CLIENTES devem possuir um usuário Unicamp criado.

- Os representantes de usuários podem criar este para servidores e docentes;
- No processo de ingresso de alunos (DAC, Colégios Técnicos, Escola de Extensão) já é criado este.

O CLIENTE deve avaliar se todo o conjunto de utilizadores dos SISTEMAS CLIENTES está no repositório de usuários do Senha Unicamp.

- Criar usuário / senha
- Consultar dados do usuário Unicamp
- Na seção **Ajuda** do portal Senha Unicamp você pode obter mais informações

IV) Questões técnicas para ciência dos administradores dos SISTEMAS CLIENTES

Premissas

1. A página de autenticação é genérica para todos os sistemas integrados nesta solução e, portanto, não constará logotipo de nenhuma unidade ou órgão, apenas o logotipo da Unicamp. Os usuários já estão familiarizados com ela, pois o acesso aos recursos do G Suite / Workspace (e-mail, drive etc.), por exemplo, é por meio desta autenticação;

2. A página de autenticação não tem disponível o recurso do recaptcha, pois não suporta;

3. A página de autenticação é responsiva e também provê acessibilidade padrão;

4. Sistemas clientes desta autenticação devem suportar TLS v1.2. Sistemas que usam Java versão 5, 6 ou 7 não suportam.

5. Caso ocorra a troca ou atualização do certificado SSL (em virtude de **EXPIRAÇÃO** por exemplo), seja para o SISTEMA CLIENTE ou para a Autenticação Central, isto exigirá **PLANEJAMENTO PRÉVIO**, das partes envolvidas, para evitar possíveis interrupções dos serviços / sistemas envolvidos. A emissão de certificados pode ser requisitada aqui.

6. No certificado de Produção do SISTEMA CLIENTE devem constar apenas aliases referentes aos servidores do ambiente de produção deste, ou aliases que representam diferentes URLs para acessar o sistema. Qualquer referência diferente disto, caracteriza uma violação de segurança conforme Instrução Normativa ConTIC-IN- 01/2019;

7. Atenção para má prática de não exigir perfil (role) obrigatório para controle de acesso a determinadas aplicações ou funcionalidades do seu sistema. Neste cenário, ao invés de se especificar que o usuário autenticado deveria ter pelo menos um perfil dentre os existentes no sistema, apenas se omite esta exigência, assim todo usuário autenticado tem acesso. Contudo, quando este sistema passa a usar a Autenticação Central, consequentemente todos os usuários do LDAP corporativo (isto é, não setorial) da universidade podem se autenticar no sistema. É importante avaliar se esse universo mais abrangente de usuários deveriam ter acesso aos recursos neste cenário.

8. A política de expiração do token do usuário autenticado é geral, mas a política de revalidação é por SISTEMA CLIENTE;

9. As aplicações podem definir o tempo de expiração da sessão do usuário, ao expirar ocorre o logout da autenticação central;

10. O CLIENTE deve avaliar se sistemas ou aplicações para o público ALUNO devem ser vinculadas a Autenticação Central. Como este público usa computadores compartilhados, laboratórios de informática por exemplo, no caso de um ALUNO autenticar-se em um

sistema e deixar o computador sem encerrar a sessão do usuário, outros alunos terão acesso enquanto a sessão do mesmo permanecer ativa. O mesmo se aplica para outros públicos que utilizam computadores compartilhados.

V) Sincronismo da Autenticação Central com LDAP

Por padrão é realizada uma sincronização com o servidor de LDAP do CCUEC a cada 30 minutos. Desse modo, novos usuários poderão acessar os sistemas os quais utilizam a Autenticação Central, após um período de 30 minutos depois de criados no ambiente do LDAP do CCUEC. A atualização das informações dos usuários cadastrados previamente também está sujeita a este intervalo de tempo.

VI) Cadastrar SISTEMA CLIENTE no SiSe (obrigatório)

É necessário criar uma solicitação para o CCUEC para que seu sistema seja incluído no SiSe e vinculado a Autenticação Central.
Favor preencher esse formulário (clique aqui), caso não tenha feito via página deste serviço que o trouxe a este guia.
Após atendida a solicitação, a partir do SiSe seu usuário poderá cadastrar informações complementares (URL's do seu sistema e aliases) para integração com a Autenticação Central e administrar os usuários e perfis de acesso para cada sistema (clique aqui).

Será encaminhado no e-mail do responsável a chave secreta a ser utilizada no seu sistema para conexão. O responsável pelo SISTEMA CLIENTE deve manter esta chave sob sigilo e guardada de forma segura.

VII) Cadastrar permissões de acesso do SISTEMA CLIENTE no SiSe (opcional)

Este passo é opcional.

O SISTEMA CLIENTE pode utilizar **autorização de acesso** (para Sistemas JEE que usam JAAS) junto com a Autenticação Central.

> **Vantagem para Sistemas que já usam JAAS**
>
> As credenciais do usuário que realizou login com sucesso, como seus perfis de acesso (roles), são carregados automaticamente no container JEE do SISTEMA CLIENTE e junto a um Access Token; recursos estes úteis para o SISTEMA CLIENTE trabalhar as permissões (sem demandar alteração de código) e para integração entre sistemas.

Cadastrar no SiSe: SISTEMAS CLIENTES, perfis de acesso destes, vincular estes perfis aos usuários dos SISTEMAS CLIENTES etc.

Pré-requisito

Acesse o SiSe para cadastrar as permissões de cada SISTEMA CLIENTE. Clique aqui

Observação: O controle do que cada perfil permite acessar é **tratado pelo** SISTEMA CLIENTE.

VIII) Configurações técnicas gerais

Requisitos de confiança entre servidor do SISTEMA CLIENTE com o servidor de Autenticação Central

a. CLIENTE deve **importar** o certificado SSL (parte pública) da Autenticação Central

> A importação dos certificados pode variar dependendo da plataforma utilizada.
> Segue abaixo o comando que pode ser necessário executar para realizar a importação do certificado dentro da keystore da JVM:
>
> **keytool -import -alias <alias> -keystore cacerts -file <file>.crt**
>
> No caso de outras plataformas, em geral, basta referenciar o certificado no arquivo principal de configuração do servidor WEB.

Solicite o certificado para **ctmq@ccuec.unicamp.br**.

b. CLIENTE deve **fornecer** o certificado SSL (parte pública) do(s) servidor(es) do(s) SISTEMA(s) CLIENTE(s):

- Enviar e-mail para **ctmq@ccuec.unicamp.br** com a URL principal do(s) SISTEMA(s) CLIENTE(s); ou
- Enviar e-mail com certificado SSL do servidor de aplicação ou proxy do(s) SISTEMA(s) CLIENTE(s).

IMPORTANTE

Caso ocorra a troca ou atualização do certificado SSL (em virtude de **EXPIRAÇÃO** por exemplo), seja para o SISTEMA CLIENTE ou para a Autenticação Central, isto **exigirá PLANEJAMENTO PRÉVIO**, das partes envolvidas, para evitar possíveis interrupções dos serviços / sistemas envolvidos.

No certificado de Produção do SISTEMA CLIENTE devem constar **apenas aliases referentes aos servidores do ambiente de produção deste, ou aliases que representam diferentes URLs para acessar o sistema**.
Qualquer referência diferente disto, caracteriza uma violação de segurança conforme Instrução Normativa ConTIC-IN- 01/2019.

IX) Integração de Sistemas JEE

Para realizar a integração destes com a Autenticação Central, favor verificar a documentação existente no GitLab da Unicamp.
Realize **primeiro** o login em https://gitlab.unicamp.br, **depois** de autenticado acesse diretamente as URLs abaixo.
Para sistemas utilizando servidor Wildfly 7 ou superior:
https://gitlab.unicamp.br/rdenadai/integracao-sistemas-java-com-autcentral

É necessário a instalação de componente do Keycloak no servidor do SISTEMA CLIENTE:
https://www.keycloak.org/docs/3.2/getting_started/topics/secure-jboss-app/install-client-adapter.html

Para sistemas utilizando JBoss 5 (legado):
https://gitlab.unicamp.br/enzotp/integracao-sistemas-java-legado-com-autcentral

X) Integração de Sistemas PHP

Realize **primeiro** o login em https://gitlab.unicamp.br, **depois** de autenticado acesse diretamente as URLs abaixo.

https://gitlab.unicamp.br/enzotp/integracao-sistemas-php-com-autcentral

XI) Integração de Sistemas Python

Consulte: https://pypi.org/project/python-keycloak/

XII) Integração de Sistemas construídos em outras plataformas

Favor contatar **ctmq@ccuec.unicamp.br**.