

REDE IFC

Configuração da rede IFC no Windows





Este manual é destinado a servidores, tercerizados e estagiários, os quais possuem Login e Senha ativos no IFC Luzerna







		– 🗆 X		
÷	🂐 Conectar-se manualm	nente a uma rede sem fio		
	Digite as informaçõ	ões da rede sem fio que deseja adicionar 5 - Em Nome da re	de insira IFC ,	
	Nome da rede:	IFC WPA2-Enterprise em Avance	e e clique	
	Tipo de segurança:	WPA2-Enterprise ~		
	Tipo de criptografia:	AES		
	Chave de Segurança:	Ocultar caracteres		
	🔽 Iniciar esta conexã	ão automaticamente		
	Conectar mesmo	que a rede não esteja difundindo		
	Aviso: com esta o	pção, a privacidade do computador poderá estar em risco.		
Avançar Cancelar 6 -Clique em Alterar configuraçõe de conexão para configurar os últimos detalhes. hamento - □ × ← S Conectar-se manualmente a uma rede sem fio - □ × ar as contractor				
		IFC adicionado(a) com êxito		
		i rece		
		→ Alterar configurações de conexão Abre as propriedades da conexão para que eu possa alterar as configurações.	nfigure um roteador ou ponto	
		orma	ões sobre como solucionar	
		Fecha Opções da Internet	Fio	
		Windows Defender Firewall	Ação necessária para IFC Conectar?	

IFC Propriedades de Rede Sem Fio Conexão Segurança Tipo de segurança: WPA2-Enterprise Tipo de criptografia: AES	× Se a opção EAP p está selecionad Configu	irança , verifique rotegido (PEAP) da e clique em rações .
Escolha um método de autenticação de rede: Microsoft: EAP protegido (PEAP) V Configurações Lembrar minhas credenciais para esta conexão sempre que fizer logon	Propriedades EAP Protegidas × Ao conectar: Verificar a identidade do servidor validando o certificado Conectar a estes servidores (exemplos: srv1;srv2;,*srv3\.com):	8 - Desmarque o checkbox Verificar a identidade do servidor validando o
Configurações avançadas OK Cance	Autoridades de certificação raiz confiávels: AAA Certificate Services Baltimore CyberTrust Root Certification Authority of WoSign Certurn Trusted Network CA Class 3 Public Primary Certification Authority COMDOD RSA Certification Authority DigiCert Assured ID Root CA DiniCert Global Root CA	certificado. Confirme se o Método de Autenticação é o EAP-MSCHAPv2 e clique em OK .
	Notificações antes da conexão: Informar ao usuário se a identidade do servidor não puder ser ver Selecionar Método de Autenticação: Senha segura (EAP-MSCHAP v2) Configurar Ativar Reconexão Rápida Desconectar se o servidor não tiver TLV com cryptobinding Habilitar Privacidade de	IFC Propriedades de Rede Sem Fio X Conexão Segurança Tipo de segurança: WPA2-Enterprise Tipo de criptografia: AES
9 - De volta à aba Segura clique em Configuraçõ avançadas.	OK Cancelar	Escolha um método de autenticação de rede: Microsoft: EAP protegido (PEAP) V Configurações Lembrar minhas credenciais para esta conexão sempre que fizer logon Configurações avançadas
	Configurações avançadas × Configurações 802.1X Configurações do padrão 802.11 Sepecificar o modo de autenticação: Autenticação de usuário Salvar credenciais Cuduis padra cipio para tada cipi	OK Cancelar
IFC Propriedades de Rede Sem Fio Conexão Segurança Tipo de segurança: WPA2-Enterprise Tipo de criptografia: AES Escolha um método de autenticação de rede: Microsoft: EAP protegido (PEAP) Configurações Lembrar minhas credenciais para esta conexão sempre que fizer logon	Excurr credencials para todos os devários Habilitar logon único para esta rede Executar imediatamente antes do logon de usuário Executar imediatamente após o logon de usuário Atraso máximo (segundos): 10 Permitir que caixas de diálogo adicionais sejam exibidas durante o logon único Esta rede usa LANs separadas virtuais para autenticação de máquina e de usuário	10 - Na aba Configurações 802.1X, selecione Autenticação de usuário como Modo de Autenticação e
Configurações avançadas	OK Cancelar	- De volta à aba Segurança ,
ОК Сапсе	lar l	clique em OK .

No Windows 7, os seguintes passos extra precisarão ser seguidos para efetivação da conexão

Propriedades EAP Protegidas					
Ao conectar:					
Validar certificado do servidor					
Conectar-se a estes servidores:					
Autoridades de certificação raiz confiáveis:					
AAA Certificate Services					
Baltimore CyberTrust Root					
Class 3 Public Primary Certification Authority					
DigiCert Assured ID Root CA					
DigiCert High Aggurance EV Deet CA					
Não solicitar ao usuário autorização para novos servidores ou					
autoridades de certificação confiáveis.					
Selecionar Método de Autenticação:					
Senha segura (EAP-MSCHAP v2)					
Ativar Decenevão Dázida					
Impor Proteção de Acesso à Rede					
Desconectar se o servidor não tiver TLV com ligação de criptografia					
Habilitar Privacidade de					
OK Cancelar					

No **passo 8**, clique em **Configurar...** e desmarque o checkbox que aparecer e dê **OK**. Ao retornar para a janela **Propriedades EAP Protegidas**, clique em **OK** para efetivar as alterações.

Propriedades EAP Protegidas	×				
Ao conectar:					
Validar certificado do servidor					
Conectar-ce a ester considerer					
Autoridades de certificação raiz confiáveis:					
AAA Certificate Services	_				
Baltimore CyberTrust Root					
Class 3 Public Primary Certification Authority	=				
DigiCert Assured ID Root CA					
DigiCert High Argurance EV Boot CA					
E FC-ACC	-				
< III >>					
Não solicitar ao usuário autorização para novos servidores ou autoridades de certificação confiáveis.					
Selecionar Método de Autenticação:					
Athur Perspecte Pields					
Impor Proteção de Acerco à Rede					
Deconectar se o servidor não tiver TIV com Unção de cristografia					
Habilitar Privacidade de					
Identidade					
OK	celar				



No **passo 10**, clique em **Salvar credenciais** e insira o **usuário** e **senha** e dê **OK**. Ao retornar para a janela **Configurações 802.1X**, clique em **OK** para efetivar as alterações.



23

.

.

•

Configurar...

OK Cancelar

X

Propriedades EAP Protegidas

An conectar-se

EC-ACC

•

Propriedades de EAP MSCHAPv2

Usar automaticamente meu nome e senha de logon do Windows (e o domínio, se houver).

3 OK Cancelar

DigiCert High Assurance EV Root CA

.....

Não solicitar ao usuário autorização para novos servidores ou autoridades de certificação confiáveis.

______Impor Proteção de Acesso à Rede _____Desconectar se o servidor não tiver TLV com ligação de criptografia

DigiCert Assured ID Root CA DigiCert Global Root CA

Selecionar Método de Autenticação: Senha segura (EAP-MSCHAP v2)

V Ativar Reconexão Rápida

Habilitar Privacidade de Identidade



12 - Na Área de Trabalho, ative a rede Wi-Fi e selecione a rede IFC e clique em
Conectar. Os servidores devem informar o usuário e senha
do SIG. Estagiários/terceirizados o usuário e senha fornecidos pela CTIC.





Segurança do Windows	×
Entrar	
Nome de usuário	
Senha	
OK Cancelar	
eduroam	
Municipio - Luzerna	
Mais configurações de Wi-Fi	
^ (⊕ ⊄) ⊡ _{05/0}	08:51 09/2022 2

13 - Pronto! Você está conectado!



EM CASO DE DÚVIDAS, **ENTRE EM CONTATO POR UM DE NOSSOS** CANAIS

<u>(49)352</u>3-4322 / 3523-4<mark>310</mark> suporte.luzerna.ifc.edu.br