

UNILAB-Acadêmico – Tutorial para Windows

Segue passo-a-passo para se conectar na nova rede WiFi da Universidade da Integração Internacional da Lusofonia Afro-Brasileira (UNILAB)



1. Buscar todas as redes sem fio disponíveis clicando no ícone do WiFI;

2. Clicar em "Abrir a Central de Rede e Compartilhamento";



3. Clicar em "Gerenciar redes sem fio";

	B	-	1 10 10 10 10		00	×
G	📶 🕨 Painel de Controle 🕨 F	lede e Internet 🔸	Gerenciar Redes Sem Fio	• \$ 9	Pesquisar Gerenciar Redes Sem Fia	Q
Geren 4 ^{O Winde}	ciar redes sem fio que u ows tenta se conectar a essas n	usem (Conexã edes na ordem list	o de Rede sem Fio) ada abaixo.			
Adicionar	Propriedades do adaptador	Tipos de perfil	Central de Rede e Compartilhamento			0
Ad	icionar uma rede sem fio					
lui.	0 itens					

4. Clicar em "Adicionar";

Como	deseja adicionar a rede?
2	Criar um perfil de rede manualmente Isso cria um novo perfil de rede ou localiza uma rede existente e salva um perfil para ela no computador. Vocé precisa conhecer o nome da rede (SSID) e a chave de segurança (se aplicável).
4	Criar rede ad hoc Cria uma rede temporária para o compartilhamento de arquivos ou de uma conexão com a Internet

5. Clicar em "Criar um perfil de rede manualmente";

9	3		
Nome da rede:	6	UNILAB-Academico	
Tipo de segurança:	7	WPA2-Enterprise	
Tipo de criptografia:	8	AES	
Chave de Segurança	:	Ocultar caracteres	
📝 Iniciar esta co	onexão a	utomaticamente	
🕅 Conectar mes	smo que	e a rede não esteja transmitindo	
Aviso: com e	sta opçã	ão, a privacidade do computador poderá estar em risco.	



dtı

6. Digitar o Nome da rede: "UNILAB-Academico";

7. Selecionar o Tipo de segurança: **WPA2-Enterprise**;

- 8. Selecionar o tipo de criptografia: AES;
- 9. Clique em "Avançar";



10. Clique em "Alterar configurações de conexão";

Conexão Segurança	
Nome:	UNILAB-Academico
SSID:	UNILAB-Academico
Tipo de rede:	Ponto de acesso
Disponibilidade de rede:	Todos os usuários
Conectar autom	aticamente quando esta rede estiver ao alcance
Conectar a uma	rede preferencial, se disponível
Conectar mesmo	que a rede não esteja transmitindo seu nome
(SSID)	raçãos do conovião MILAN
	ações de conexão WEAN
Configurar	

11. Clicar na aba "Segurança";

Tipo de segurança:	WPA2-Enterprise	•
Tipo de criptografia:	AES	•]
Lembrar minhas cr sempre que fizer lo	edenciais para esta cone; ogon	kão
	wancadas	
Configurações a		

12. Do lado de "Microsoft: EAP protegido (PEAP)" clique em "Configurações";

conectar:		- 11 C	
Validar c	ertificado do servid	or	
Conecta	r-se a estes servid	ores:	
1			
202.47.17	()		
	s de cerdificação rai	+ connaveis:	
Autoric	ade Certificadora B	aiz Brasileira v2	1
Baltimo	re CyberTrust Root		1
Class 3	Public Primary Cert	tification Authority	
DigiCer	t Assured ID Root (CA	
DigiCer	t Global Root CA		
DigiCer	t High Assurance E	V Root CA	-
4		m	
autorida	des de certificação todo de Autenticaç	confláveis. ão:	14
enha segur	a (EAP-MSCHAP v2))	Configurar.
Ativar Rec	onexão Rápida		-
Impor Pro	eção de Acesso à F	Rede	
10000000000000	ar se o servidor nã	o tiver TLV com ligaç	ção de criptografia
Desconect	rivaridade de		
Desconect Habilitar P Identidade			

13. Desmarcar a caixa "Validar certificado do servidor";

14. Do lado de "Senha segura (EAP-MSCHAPv2)" Clique em "Configurar";



Propriedades	de EAP MSC	HAPv2	
Ao conectar:	e:		
.5 Usar au	tomaticamente o Windows (e	e meu nome e senha de o domínio, se houver).	
		1	
16	ОК	Cancelar	

15. Desmarcar a caixa "Usar automaticamente meu nome e senha de logon do Windows";

16. Clique em "OK" para confirmar;

Validar certificado do servidor Conectar-se a estes servidores: Autoridades de certificação raiz confiáveis: AddTrust External CA Root Autoridade Certificadora Raiz Brasileira v2 Baltimore CyberTrust Root Class 3 Public Primary Certification Authority DigiCert Assured ID Root CA DigiCert Global Root CA DigiCert Global Root CA DigiCert High Assurance EV Root CA Mão solicitar ao usuário autorização para novos servidores ou autoridades de certificação confiáveis.	o conectar:		
Conectar-se a estes servidores: Autoridades de certificação raiz confiáveis: Autoridade Certificadora Raiz Brasileira v2 Baltimore CyberTrust Root Class 3 Public Primary Certification Authority DigiCert Assured ID Root CA DigiCert Global Root CA DigiCert Global Root CA DigiCert High Assurance EV Root CA Mão solicitar ao usuário autorização para novos servidores ou autoridades de certificação confiáveis. elecionar Método de Autenticação: senha segura (EAP-MSCHAP v2) Configurar. Ativar Reconexão Rápida Impor Proteção de Acesso à Rede Desconectar se o servidor não tiver TLV com ligação de criptografia	Validar cert	tificado do servidor	
Autoridades de certificação raiz confiáveis: AddTrust External CA Root Autoridade Certificadora Raiz Brasileira v2 Baltimore Cyber Trust Root Class 3 Public Primary Certification Authority DigiCert Assured ID Root CA DigiCert High Assurance EV Root CA DigiCert High Assurance EV Root CA Mão solicitar ao usuário autorização para novos servidores ou autoridades de certificação confiáveis. elecionar Método de Autenticação: Senha segura (EAP-MSCHAP v2) Ativar Reconexão Rápida Impor Proteção de Acesso à Rede Desconectar se o servidor não tiver TLV com ligação de criptografia	Conectar-	se a estes servidores:	
AddTrust External CA Root Autoridade Certificadora Raiz Brasileira v2 Baltimore CyberTrust Root Class 3 Public Primary Certification Authority DigiCert Assured ID Root CA DigiCert Global Root CA DigiCert High Assurance EV Root CA Mão solicitar ao usuário autorização para novos servidores ou autoridades de certificação confiáveis.	L	de certificação raiz confiáveis:	
Autoridade Certificadora Raiz Brasileira v2 Baltimore CyberTrust Root Class 3 Public Primary Certification Authority DigiCert Assured ID Root CA DigiCert Global Root CA DigiCert High Assurace EV Root CA Mão solicitar ao usuário autorização para novos servidores ou autoridades de certificação confiáveis. elecionar Método de Autenticação: Senha segura (EAP-MSCHAP v2) Configurar. Ativa Reconexão Rápida Impor Proteção de Acesso à Rede Desconectar se o servidor não tiver TLV com ligação de criptografia Habilitar Privacidade de	AddTrust	External CA Root	*
Baltimore CyberTrust Root Class 3 Public Primary Certification Authority DigiCert Assured ID Root CA DigiCert Global Root CA DigiCert High Assurance EV Root CA viii Não solicitar ao usuário autorização para novos servidores ou autoridades de certificação confiáveis. elecionar Método de Autenticação: Senha segura (EAP-MSCHAP v2) Configurar. Ativar Reconexão Rápida Impor Proteção de Accesso à Rede Desconectar se o servidor não tiver TLV com ligação de criptografia Habilitar Privacidade de	Autoridad	de Certificadora Raiz Brasileira v2	2
Class 3 Public Primary Certification Authority DigiCert Assured ID Root CA DigiCert Global Root CA DigiCert High Assurance EV Root CA Não solicitar ao usuário autorização para novos servidores ou autoridades de certificação confláveis. elecionar Método de Autenticação: Senha segura (EAP-MSCHAP v2) Configurar. Ativar Reconexão Rápida Impor Proteção de Acesso à Rede Desconectar se o servidor não tiver TLV com ligação de criptografia Habilitar Privacidade de	🗐 Baltimore	CyberTrust Root	1.0
DigiCert Assured ID Root CA DigiCert Global Root CA DigiCert High Assurance EV Root CA Initial Assurance EV Root CA Não solicitar ao usuário autorização para novos servidores ou autoridades de certificação confiáveis. elecionar Método de Autenticação: Senha segura (EAP-MSCHAP v2) Ativar Reconexão Rápida Impor Proteção de Acesso à Rede Desconectar se o servidor não tiver TLV com ligação de criptografia	Class 3 Pu	ublic Primary Certification Author	ity
DigiCert Global Root CA DigiCert High Assurance EV Root CA Inão solicitar ao usuário autorização para novos servidores ou autoridades de certificação confiáveis. elecionar Método de Autenticação: Senha segura (EAP-MSCHAP v2) Configurar. Ativar Reconexão Rápida Impor Proteção de Acesso à Rede Desconectar se o servidor não tiver TLV com ligação de criptografia	📃 DigiCert A	Assured ID Root CA	
DigiCert High Assurance EV Root CA DigiCert High Assurance EV Root CA	DigiCert 0	Global Root CA	
III Não solicitar ao usuário autorização para novos servidores ou autoridades de certificação confiáveis. elecionar Método de Autenticação: Senha segura (EAP-MSCHAP v2) Configurar. Ativar Reconexão Rápida Impor Proteção de Acesso à Rede Desconectar se o servidor não tiver TLV com ligação de criptografia Habilitar Privacidade de			
Não solicitar ao usuário autorização para novos servidores ou autoridades de certificação confiáveis. elecionar Método de Autenticação: ienha segura (EAP-MSCHAP v2) Ativar Reconexão Rápida Impor Proteção de Acesso à Rede Desconectar se o servidor não tiver TLV com ligação de criptografia Habilitar Privacidade de	DigiCert H	ligh Assurance EV Root CA	+
	DigiCert H	tigh Assurance EV Root CA III ar ao usuário autorização para n	• • •
	DigiCert I DigiCert I DigiCert I DigiCert I DigiCert I DigiCert I Não solicit autoridade elecionar Métod enha segura (Ativar Recon Impor Proteç Desconectar Habilitar Priv. Identidade	tigh Assurance EV Root CA III ar ao usuário autorização para n es de certificação confiáveis. do de Autenticação: EAP-MSCHAP v2) mexão Rápida ção de Acesso à Rede se o servidor não tiver TLV com acidade de	vovos servidores ou Configurar. ligação de criptografia

17. Clique em "OK" novamente.

Conexão Segurança			
Tipo de segurança:	WPA2-Er	nterprise	2
Tipo de criptografia:	AES		8
the second se	IO (PEAP)	· · ·	Configurações
Lembrar minhas crede sempre que fizer logo	enciais p <mark>ara</mark> e on	sta cone	Configurações xão
Lembrar minhas cred sempre que fizer logo S Configurações ava	enciais para e on ançadas	sta cone	Configurações xão
Lembrar minhas cred sempre que fizer logo Sempre que fizer logo Configurações ava	ançadas	sta cone	Configurações xão

18. Clique em "Configurações Avançadas";

nfigurações 802.1X Configurações d	o padrão 802,11
🕼 Especificar o modo de autenticaçã	ăo:
Autenticação de usuário	Salvar credenciais
Excluir credenciais para todos	os usuários
🔲 Habilitar logon único para esta rec	de
Executar imediatamente antes	s do logon de usuário
🕖 Executar imediatamente após	o logon de usuário
Atraso máximo (segundos):	10
Permitir que caixas de diálogo exibidas durante o logon único	adicionais sejam o
Esta rede usa LANs separadas autenticação de máquina e de	s virtuais para : usuário

19. Marque a caixa "Especificar o modo de autenticação" e selecione a opção Autenticação de usuário.

20. Clique em "OK".



Conexão Segurança	
Tipo de segurança:	WPA2-Enterprise
Tipo de criptografia:	AES
Microsoft: EAP protegic	do (PEAP) Configurações
Lembrar minhas cred	denciais para esta conexão
Lembrar minhas cred sempre que fizer log	denciais para esta conexão on
Lembrar minhas cred sempre que fizer log Configurações ave	denciais para esta conexão on
Lembrar minhas cred sempre que fizer log Configurações ave	denciais para esta conexão on
Lembrar minhas cred sempre que fizer log Configurações avi	denciais para esta conexão on

21. Clique em "OK" para finalizar a configuração";



22. Clique neste balão que irá surgir solicitando informações adicionais;

egurança do W	lindows	
Autenticae Digite as cree	ção de Rede Ienciais do usuário	
	Nome de usuário	23
	Senha	

23. Insira seu usuário e senha dos sistemas SIG;

Conectado no momento a:	47 *
HILAB-Academico Acesso à Internet	
Conexão de Rede sem Fio	1
UNILAB-Academico Conect	tado 📶
unilab_wf_proplan	liter
Unilab_Rede_Administrativa	lites
UnilabNet	201
unilab_wf_protocolo	
	*
Abrir a Central de Rede e Compa	rtilhamento
er 🗃 🔺 📫 🕪	13:37 13/11/2015

24. Finalizando os procedimentos anteriores, sua conexão deve ser realizada com sucesso e já pode navegar na Internet pela rede "UNILAB-Academico".

Observações: Para Windows 8 e posteriores, seguir apenas os passos 22, 23 e 24

Caso vier a ter dificuldades em algum procedimento, pode-se pedir auxílio nos laboratórios de informática na Universidade.

Qualquer dificuldade no processo estamos à disposição para ajudar!

DIRETORIA DE TECNOLOGIA DA INFORMAÇÃO