



FINGERTECH

Tecnologia que deixa você no controle.

Manual de Configuração do NAC 1500 (SW101M2)

Este manual tem por objetivo auxiliar o usuário a realizar as primeiras configurações no NAC 1500 (SW101M2) e também no programa de gerenciamento Access Manager (ACM). Além disso será explicadas as principais funcionalidades do dispositivo.

INDÍCE

Terminal NAC	2
Menu de Opções (Português) - NAC 1500 (SW101M2)	2
Ligando o NAC pela Primeira Vez	4
Configurando Idioma	5
Configurando NAC - Modo STAND ONLY (SO)	5
Configurando NAC - Modo Network Local (NL)	6
Cadastrando um Novo Usuário	7
Removendo Usuários do NAC	8
Alterar Informações do Usuário	8
Alertas Sonoros (Voz e Beeps)	9
Formatar o NAC	9
Perdi o Acesso de Administrador do NAC - Não Consigo Acessar o Menu de Opções	10
Access Manager Profissional	13
Instalando o ACM	14
Configurações Iniciais do Access Manager (ACM)	20
Sincronizando Terminal	23
O Access Manager não Reconhece o Terminal NAC	24
Gerenciando Usuários	25
Inserindo Usuário Através do ACM	25
Inserindo Usuário Através do Terminal NAC	31
Editar/Alterar Informações do Usuário	31
Options Menu (English) - NAC 1500 (SW101M2)	36



Terminal NAC



O terminal NAC corresponde ao dispositivo em si. Embora exista o software *Access Manager (ACM)* que permite realizar as configurações do terminal, de uma maneira mais prática, o terminal NAC já possui um sistema onde é possível realizar todas as configurações a partir dele próprio sem a necessidade do ACM.

1. Menu de Opções (Português) - NAC 1500 (SW101M2)

1. Adm Utilizadores				
1. Registrar Utilizador	1. Inserir ID :		* Insira um novo ID para o usuário.	
	2. Tipo de Utilizador :		Normal / Master (O 1º é sempre Master)	
	3. FP / PW (Digital / Senha):		1. FP (Somente Digital)	
			2. PW (Somente Senha)	
			3. FP / PW (Digital OU Senha)	
			4. FP & PW (Digital E Senha)	
	4. Inserir a Palavra Passe:		* Senha (Somente Números)	
4. Inserir a Palavra Passe:		* Repita a Senha (Somente Números)		
5. Cadastrar Impressão Digital		* Cadastrar Digital		
5. Cadastrar Impressão Digital		* Coloque novamente a Digital		
2. Alterar Utilizador	1. Inserir ID :		* Insira o ID do Usuário que deseja alterar	
	1. Modo Autentic'		1. FP (Somente Digital)	
			2. PW (Somente Senha)	
			3. FP / PW (Digital OU Senha)	
			4. FP & PW (Digital E Senha)	
2. FP		* Cadastre Duas Vezes a Mesma Digital		
3. Tipo de Utilizador		Normal / Master		
4. Palavra Passe		* Cadastre duas vezes a Senha (Somente Números)		
3. Apagar Utilizador	1. Inserir ID :		* Insira o ID do Usuário que deseja apagar	
	Confirma?		Sim / Não	
4. Apagar Todos	Confirma?		Sim / Não	



FINGERTECH

Tecnologia que deixa você no controle.

2. Opções de FP	1. Nível Segurança	1. Modo 1:1	(1-9) : 5	
	2. Modo Captura	Normal/LFD_1/LFD_2/LFD_3		
	3. Tempo Captura	(1-30): 5		
	4. Modo Auto On	Ligado/Deslig'		
	5. Temp' Cap' 1:N	1. Usar TimeOut		Ligado/Deslig'
		2. Config' TimeOut		(2-9): 3
6. Modo Freescan	Ligado/Deslig'			

3. Opções de UI	1. Idioma	2. English
		7. Portuguese
	2. Voz	Ligado/Deslig'
	3. Beep	Ligado/Deslig'
	4. Funckey Disp	Deslig'/Modo1/Modo2
	5. Menu Timeout	Ligado/Deslig'
	6. LCD BL Timeout	Ligado/Deslig'
7. Backlight Level	(1-4) : 2	

4. Opções do Sistema	1. Log	Ligado/Deslig'
	2. Cartão RF	Deslig'/HID/MIFARE/EM/iClass
	3. Wiegand	Deslig'/26bit/34bit/37bit
	4. Modo de Operação	AC/T&A
	5. Autenticação	SO/NL
	6. Data/Hora	201X/XX/XX XX:XX:XX
	7. Modo Terminal	Leitor/Terminal
	8. Fuso Horário	Ligado/Deslig'

5. Network	1. ID do Terminal	(1 ~ 2000) : 1		
	2. TCP/IP	1. Utilizar DHCP		Ligado/Deslig'
		2. IP do Terminal		0.0.0.0
		3. Máscara Sub-Rede		0.0.0.0
		4. Gateway		0.0.0.0
		5. IP do Servidor		192.168.0.2
	3. Timeout Comunic'	(2-60) : 10		
4. N° 'Da Porta	: 7332			
5. Connect Ver	3 / 4			

6. Inform' do Sistema	1. N° Utilizadores	Normal: 0 Master: 0
	2. Versao f/w	6.000-0061
	3. 485 ID	: 0



7. Formatos	1. Apagar a DB	Sim/Não
	2. Formato Inicial	Sim/Não
	3. Número do FP	1 / 2
	4. Tamanho ID	(4-15): 4
	5. Limpar Memória	Sim/Não

2. Ligando o NAC pela Primeira Vez

Ao ligar o NAC 1500 (SW101M2) pela primeira vez, será solicitado duas informações obrigatórias e que não podem ser alteradas depois, por isso atenção ao preenchê-las. Essas informações são “*FP Number*” que representa a quantidade de impressões digitais (dedos) que serão cadastrados por usuário, você poderá escolher entre cadastrar uma ou duas impressões digitais. O outro valor requisitado ao ligar o NAC pela primeira vez é o “*ID Length*”, este valor representa a quantidade de dígitos que o ID de cada usuário terá, ou seja, o tamanho do identificador (ID) de cada um dos usuários, esse tamanho pode variar entre 4 e 15 dígitos.

1. FP Number	(1 / 2)	* Número de Impressões Digitais (Dedos), por usuário. (Não pode ser alterado depois)
2. ID Length	(4-15) : 0	* Quantos dígitos terá o ID de cada usuário. (Não pode ser alterado depois)

Após o preenchimento destas duas opções, você poderá ter acesso ao menu de opções do NAC, onde poderá terminar de realizar as configurações do dispositivo.



3. Configurando Idioma

O NAC 1500 (SW101M2) oferece dez opções de idiomas para sua interface, dentre elas o português. Caso você deseje mudar sua interface do Inglês para o Português, basta ir na opção 3 (*UI Option*) do menu principal, no submenu que será apresentado escolha a opção 1 (*Language*) e por último escolha a opção 7 (*Portuguese*) que representa o português, entre os idiomas listados. Lembrando que você pode encontrar o menu em Inglês no final deste material.

3. UI Option		1. Korean
		2. English
		3. Japanese
		4. Arabic
		5. French
		6. Spanish
		7. Portuguese
		8. Indonesian
		9. Thai
		0. Farsi
	1. Language	
	2. Voice	ON / OFF
	3. Beep	ON / OFF
	4. Funckey Disp	OFF/Modo1/Modo2
	5. MenuTimeout	ON / OFF
	6. LCD BL Timeout	ON / OFF
	7. Backlight Level	(1-4) : 2

4. Configurando NAC - Modo STAND ONLY (SO)

O NAC 1500 (SW101M2) permite sua utilização sem a necessidade da utilização de uma rede local (*Network Local - NL*), para isso é necessário configurá-lo para trabalhar no modo *Stand Only (SO)*. Essa configuração é recomendada apenas em casos onde a integração dele com uma rede local não possível.

Para realizar essa configuração, basta ir na opção número 4 (Opções do Sistema) do menu principal, escolher a opção 5 (Autenticação) do submenu e por último escolher a opção “**SO**”, conforme mostrado abaixo.

4. Opções do Sistema	1. Log	Ligado/Deslig'
	2. Cartão RF	Deslig'/HID/MIFARE/EM/iClass
	3. Wiegand	Deslig'/26bit/34bit/37bit
	4. Modo de Operação	AC/T&A
	5. Autenticação	SO/NL
	6. Data/Hora	201X/XX/XX XX:XX:XX
	7. Modo Terminal	Leitor/Terminal
	8. Fuso Horário	Ligado/Deslig'



5. Configurando NAC - Modo Network Local (NL)

Normalmente o NAC 1500 (SW101M2) é utilizado integrado a uma rede local (*Network Local - NL*) e conjunto com o software de gerenciamento *Access Manager (ACM)*. Isso permite uma maior controle e facilidade na hora de cadastrar ou remover usuário, gerar relatórios, visualizar registros de acesso (log), dentre outras vantagens.

Para você configurar o NAC para funcionar em um rede, primeiro certifique-se de que o modo de autenticação do dispositivo está configurado para *Network Local (NL)*, esta é a opção padrão de fábrica, porém caso você tenha alterado para funcionar como *Stand Only (SO)*, mude novamente para *Network Local (NL)*, acessando o menu principal do dispositivo, e indo na opção mostrada na imagem abaixo.

4. Opções do Sistema	1. Log	Ligado/Deslig'
	2. Cartão RF	Deslig'/HID/MIFARE/EM/iClass
	3. Wiegand	Deslig'/26bit/34bit/37bit
	4. Modo de Operação	AC/T&A
	5. Autenticação	SO/NL
	6. Data/Hora	201X/XX/XX XX:XX:XX
	7. Modo Terminal	Leitor/Terminal
	8. Fuso Horário	Ligado/Deslig'

Após isso, você precisará fazer as configurações de rede localizadas na opção 5 (Network) do menu principal.

5. Network	1. ID do Terminal	(1 ~ 2000) : 1	
	2. TCP/IP	1. Utilizar DHCP	Ligado/Deslig'
		2. IP do Terminal	0.0.0.0
		3. Máscara Sub-Rede	0.0.0.0
		4. Gateway	0.0.0.0
		5. IP do Servidor	192.168.0.2
	3. Timeout Comunic'	(2-60) : 10	
4. N° 'Da Porta	: 7332		
5. Connect Ver	3 / 4		

Primeiro defina o "*ID do Terminal*", este ID é para identificar cada um dos terminais presentes na rede, caso sua rede possua mais de um. Este ID pode variar entre 1 e 2000, porém cuidado para não utilizar um ID que outro terminal já esteja utilizando, isso ocasionará conflito nos terminais.

Na opção "*TCP/IP*", você poderá optar por utilizar ou não as configurações vindas de um DHCP, para isto basta ativar ou desativar o uso do DHCP na opção "*1. Utilizar DHCP*". Se optar por utilizar o *DHCP*, você precisará definir apenas a opção "*5. IP do Servidor*", pois as demais opções serão fornecidas automaticamente para o NAC por meio do *DHCP*.

Caso você opte por desativar as opções de DHCP, será necessário definir o "*2. IP do Terminal*", ou seja, o IP do NAC em questão, cuidado também para não definir um IP que outro terminal esteja utilizando. Depois é necessário definir a "*3. Máscara de Sub-rede*", normalmente é definida como 255.255.255.0, porém pode



variar de acordo com as configurações da rede. Em seguida configure o “4. Gateway” da rede. E por último configure o “5. IP do Servidor” onde o *Access Manager* está configurado.

Também pode ser necessário alterar o número da porta de comunicação do NAC, caso algum outro serviço ou aplicação esteja utilizando a mesma porta, a porta padrão do NAC é a 7332. Para alterar o número da porta basta ir na opção “4. N° ‘Da Porta” e mudar para uma porta que esteja livre.

6. Cadastrando um Novo Usuário

1. Adm Utilizadores	1. Registrar Utilizador	1. Inserir ID :	* Insira um novo ID para o usuário.
		2. Tipo de Utilizador :	Normal / Master (O 1° é sempre Master)
		3. FP / PW (Digital / Senha):	1. FP (Somente Digital)
			2. PW (Somente Senha)
			3. FP / PW (Digital OU Senha)
			4. FP & PW (Digital E Senha)
		4. Inserir a Palavra Passe:	* Senha (Somente Números)
		4. Inserir a Palavra Passe:	* Repita a Senha (Somente Números)
5. Cadastrar Impressão Digital	* Cadastrar Digital		
5. Cadastrar Impressão Digital	* Coloque novamente a Digital		

Para cadastrar um novo usuário você precisa ir na opção “1. Adm Utilizadores” do menu principal e em seguida na opção “1. Registrar Utilizador” do submenu. A partir daí você precisará adicionar um novo ID para este usuário, lembrando que este ID não pode estar sendo utilizado por outro usuário.

Em seguida será perguntado sobre o tipo de utilizador, nesta opção você pode selecionar entre *Normal* e *Master*, os usuários *Master* tratam-se dos administradores e podem modificar qualquer configuração do NAC, inclusive deletar ou adicionar usuário, ou mesmo formatar o NAC, por isso é preferível que a maioria dos usuários sejam cadastrados como *Normal*, estes usuários não podem acessar o menu de opções, dessa maneira não podendo alterar as configurações, este usuário podem apenas realizar o acesso (autenticação) através do NAC.

Após o cadastro do tipo de utilizador, será solicitado o meio de autenticação (*FP / PW*) que poderá ser realizado por impressão digital (*FP*) ou por senha (*PW*). Você poderá escolher entre quatro opções: 1. *FP* (Somente Digital) | 2. *PW* (Somente Senha) | 3. *FP / PW* (Digital OU Senha) | 4. *FP & PW* (Digital E Senha). Na opção 3 (*FP / PW*) o usuário pode escolher se irá realizar a autenticação através da digital ou através da senha, já na opção 4 (*FP & PW*) o usuário será obrigado a validar por meio da digital e da senha, caso um dos dois não coincida o acesso será negado.

Logo após escolher o meio de autenticação, será solicitado que você cadastre a senha e/ou a impressão digital dependendo dos meios de autenticação que você escolheu anteriormente. Será solicitado que você cadastre duas vezes o meio de autenticação escolhido, seja senha e/ou impressão digital, ou ambos.



7. Removendo Usuários do NAC

1. Adm Utilizadores	3. Apagar Utilizador	1. Inserir ID :	* Insira o ID do Usuário que deseja apagar
		Confirma?	Sim / Não
	4. Apagar Todos	Confirma?	Sim / Não

Para remover um único usuário que foi cadastrado, você precisará ir na opção “1. Adm Utilizadores” do menu principal, em seguida escolher a opção “3. Apagar Utilizador”. Será solicitado que você informe o ID (Identificador) do usuário que deseja remover e em seguida será solicitado que você confirme a operação de exclusão, para isso escolha a opção “Sim”, para que o usuário seja removido do NAC.

Agora caso você deseje remover todos os usuários cadastrados no NAC, basta escolher a “1. Adm Utilizadores” do menu principal, em seguida escolher a opção “4. Apagar Todos”. Será solicitado que você confirme a operação, se você realmente desejar excluir todos os usuários clique em “Sim” para confirmar, caso contrário clique em “Não”.

8. Alterar Informações do Usuário

1. Adm Utilizadores	2. Alterar Utilizador	1. Inserir ID :	* Insira o ID do Usuário que deseja alterar
		1. Modo Autentic'	1. FP (Somente Digital)
			2. PW (Somente Senha)
			3. FP / PW (Digital OU Senha)
			4. FP & PW (Digital E Senha)
		2. FP	* Cadastre duas vezes a mesma Digital
3. Tipo de Utilizador	Normal / Master		
	4. Palavra Passe	* Cadastre duas vezes a Senha (Somente Números)	

Há casos onde é necessário alterar as informações de um usuário, como por exemplo, trocar ou cadastrar uma nova senha ou digital, alterar o tipo de utilizador entre *normal* e *master*, ou mesmo alterar o meio de autenticação. Todas essas mudanças são realizadas indo na opção “1. Adm Utilizadores” do menu principal, e em seguida na opção “2. Alterar Utilizador”, ao entrar nesta opção, será solicitado que você informe o ID (Identificador) do usuário no qual você deseja realizar a alteração.

Após inserir o ID do usuário que será alterado, na opção “1. Modo Autentic” você pode alterar a forma de autenticação do usuário entre utilizar somente digital (1. FP), utilizar somente senha (2. PW), utilizar digital ou senha (3. FP/ PW), ou ainda utilizar digital e a senha (4. FP & PW), sendo que nesta última maneira o usuário será forçado a realizar os dois tipos de autenticação.

Além disso o usuário pode cadastrar ou recadastrar a digital que ele usará para realizar a autenticação no NAC, indo na opção “2. FP”, onde será solicitado que ele posicione duas vezes a digital sobre o leitor biométrico.

Na opção “3. Tipo de Utilizador”, pode ser alterado o tipo do usuário entre *Normal* e *Master*. Lembrando que *Master* trata-se do administrador do NAC, dessa forma ele tem permissão para modificar o NAC como quiser, já o usuário do tipo “*Normal*”, ele somente pode realizar a autenticação no NAC, não podendo mudar as configurações do dispositivo.



Por último também é possível cadastrar ou alterar a senha do usuário indo na opção “4. Palavra Passe”. Será solicitado que o usuário digite duas vezes a senha para que a alteração seja realizada.

9. Alertas Sonoros (Voz e Beeps)

3. Opções de UI	1. Idioma	2. English 7. Portuguese
	2. Voz	Ligado / Deslig'
	3. Beep	Ligado / Deslig'
	4. Funckey Disp	Deslig' / Modo1 / Modo2
	5. Menu Timeout	Ligado / Deslig'
	6. LCD BL Timeout	Ligado / Deslig'
	7. Backlight Level	(1-4) : 2

Em alguns casos alguns usuários optam por ativar ou desativar os alertas sonoros (Voz e Beeps) do dispositivo, para isto basta ir na opção “3. Opções de UI” e em seguida nas opções “2. Voz” e “3. Beep”, e então marcar como “Ligado” para ativar e “Deslig” para desativar os alertas sonoros.

10. Formatar o NAC

7. Formatos	1. Apagar a DB	Sim / Não
	2. Formato Inicial	Sim / Não
	3. Número do FP	1 / 2
	4. Tamanho ID	(4-15): 4
	5. Limpar Memória	Sim / Não

Há casos onde é necessário formatar o NAC, ou seja, voltar ele para as configurações originais de fábrica. Para isso entre na opção “7. Formatos” do menu principal, e em seguida escolha a opção “2. Formato Inicial”, caso você realmente deseja formatar o dispositivo, basta selecionar a opção “Sim”, caso contrário selecione a opção “Não”.

***Atenção**, este procedimento levará alguns minutos e irá apagar todos os usuários e configurações existentes no dispositivo, retornando tudo ao padrão de fábrica. O processo é irreversível, então tenha certeza que você realmente deseja formatar o dispositivo.



11. Perdi o Acesso de Administrador do NAC - Não Consigo Acessar o Menu de Opções

Existem casos onde por motivos não relacionados ao funcionamento do NAC, é perdido o acesso de administrador (*Master*) do dispositivo, não sendo possível acessar o menu de opções, um exemplo comum, é quando o administrador (usuário *Master*) do dispositivo, trata-se de um funcionário de uma organização e por algum motivo acaba se desligando dela, levando consigo a digital e a senha de administrador. Não permitindo o acesso ao menu principal do NAC para realizar alterações.

Para evitar este problema recomendamos fortemente que mais de um usuário de confiança da organização, seja cadastrado como *Master* (Administrador) no dispositivo, de preferência sendo um deles o dono ou sócio majoritário da organização. A fim de que caso um dos administradores venha a se desligar da organização, outro consigo ter o acesso ao menu do NAC e fazer as alterações que julgar necessário, como por exemplo, desvincular o antigo colaborador dos usuário cadastrados no dispositivo.

Mas em caso onde realmente não tenha mais ninguém com permissão de administrador para acessar o menu de opções do NAC, é possível realizar o acesso ao menu de opções e cadastrar um novo administrador para o dispositivo, porém para isso será necessário abrir o NAC fisicamente. Para isto siga os passos abaixo.

- 1) Abra o NAC, para isto, retire os 6 (seis) parafusos da parte de trás do dispositivo, conforme mostrado na imagem abaixo.

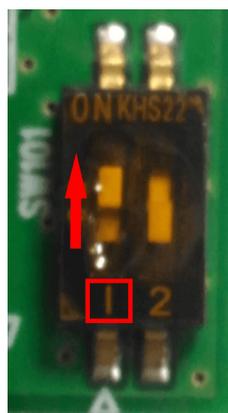




2) Ao abrir o dispositivo, localize a chave SW101 mostrada na imagem abaixo.



3) Para liberar o acesso ao menu de opções do NAC, você precisará romper o lacre (transparente e bem fino) localizado sobre a chave, e então mudar apenas o pino 1 de posição, conforme a imagem abaixo.



* **Atenção**, o pino 2 não deve ter sua posição alterada. Mantenha ele em sua posição original.



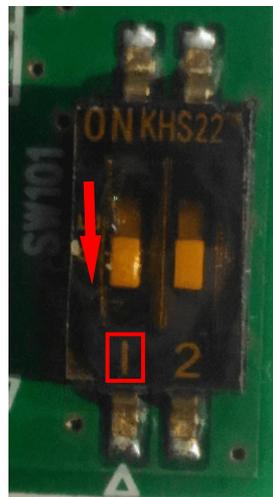
FINGERTECH

Tecnologia que deixa você no controle.

- 4) Agora ligue o NAC normalmente (não é necessário parafusá-lo), e clique sobre o botão “MENU” presente no dispositivo, você notará que o menu de opções estará liberado, agora basta adicionar um nova administrador (vide tópico 6) ou mesmo formatá-lo (vide tópico 10) se for o caso.



- 5) Após realizar as configurações desejada, volte o pino 1 da chave SW101 para a posição original, conforme mostrado na imagem abaixo.



- 6) Agora basta parafusar o NAC novamente e o processo terá sido finalizado.

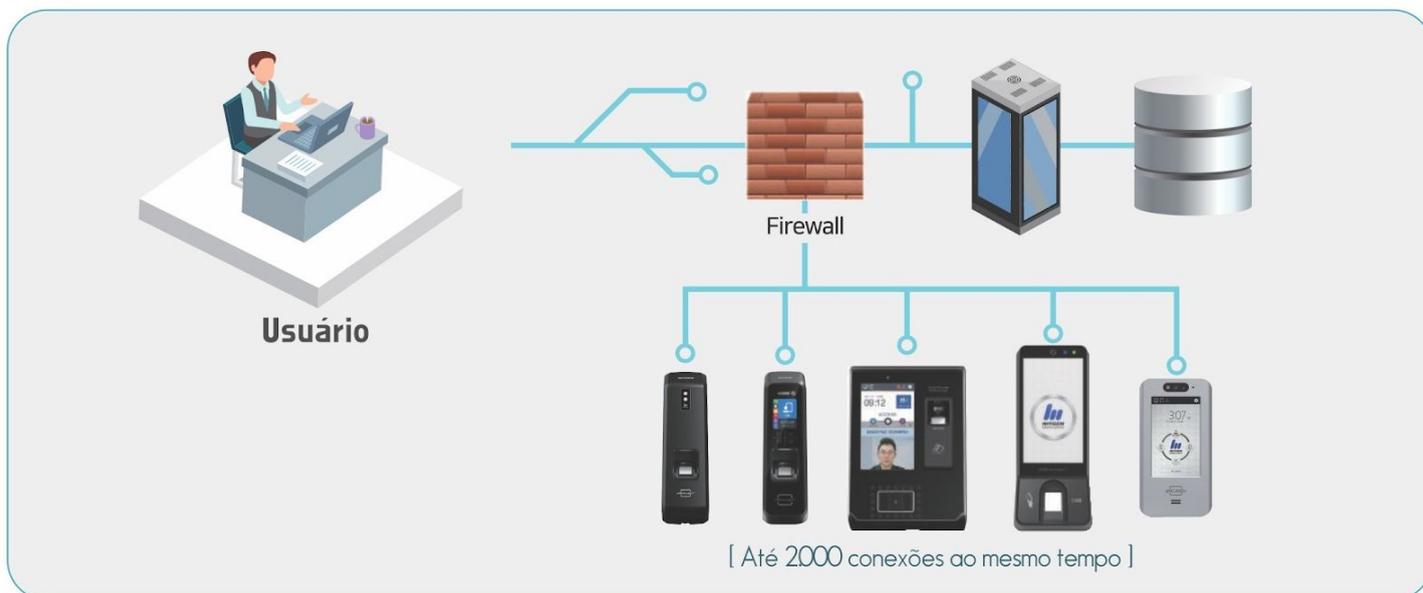
Access Manager Profissional

O Access Manager (ACM) trata-se do programa de gerenciamento e controle do NAC, quando este está configurado para trabalho no modo *Network Local (NL)*, ou seja, quando ele está configurado em rede. Através do ACM é possível adicionar ou remover usuários, cadastrar senha e impressão digital, criar grupos de acesso, visualizar logs de acesso, ter acesso a relatórios, dentre outras diversas funcionalidades. Neste documento a intenção é mostrar o processo de instalação do software, e também as funcionalidades básicas, como cadastro do NAC no ACM, cadastro e remoção de usuários do NAC através do ACM e sincronizar o ACM e o NAC.

AccessManager Pro

O AccessManager Pro é uma solução de controle de acesso por impressão digital que pode gerenciar múltiplos terminais de autenticação, com foco em pequenas, médias e grandes empresas. Podem gerenciar facilmente até 2000 terminais conectados a uma única rede, e a função de acesso remoto aumenta a conveniência dos usuários.

Funcionamento



Características

Download Automático

- Download de usuários para vários terminais de uma única vez
- Cadastro e modificação de usuários de maneira simplificada

Autenticação no servidor do tipo 1:N

- Aplicação integrada para buscas do tipo 1:N
- Autenticação 1:N realizada diretamente no servidor

Acompanhamento e análise de eventos

Busca Automática de Terminais

- Busca automaticamente terminais conectados a rede
- Acesso remoto a terminais e servidores

Sistema de Gestão Eficaz

- Monitoramento em tempo real
- Gerenciamento automático de até 2000 terminais

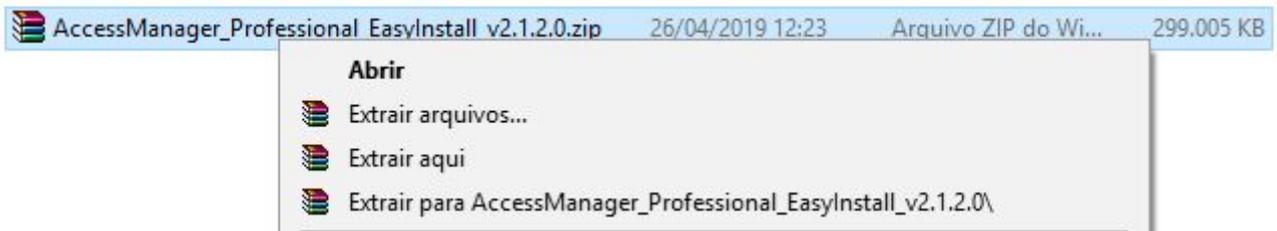


1. Instalando o ACM

1) Baixe o “Access Manager Professional”, no link abaixo.

<https://bit.ly/2JB0drL>

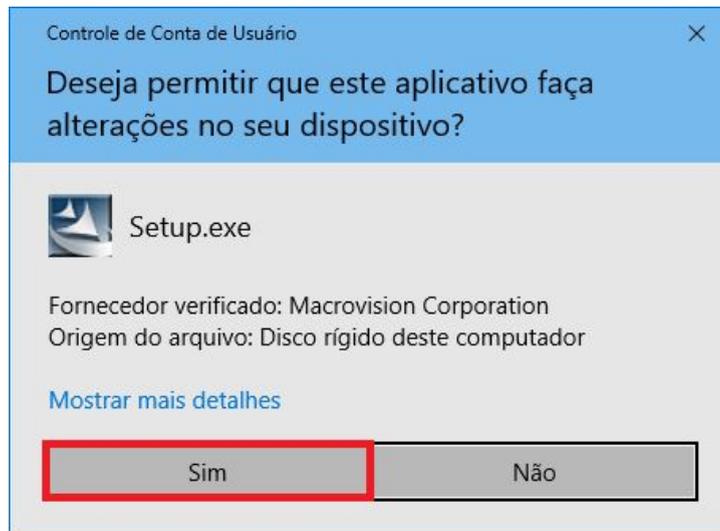
2) Descompacte o arquivo “AccessManager_Professional_EasyInstall_v2.1.2.0.zip” da forma como preferir. Você poderá utilizar o Winrar, para isto, basta clicar com o botão direito sobre o arquivo e selecionar a opção “*Extrair Aqui*”.



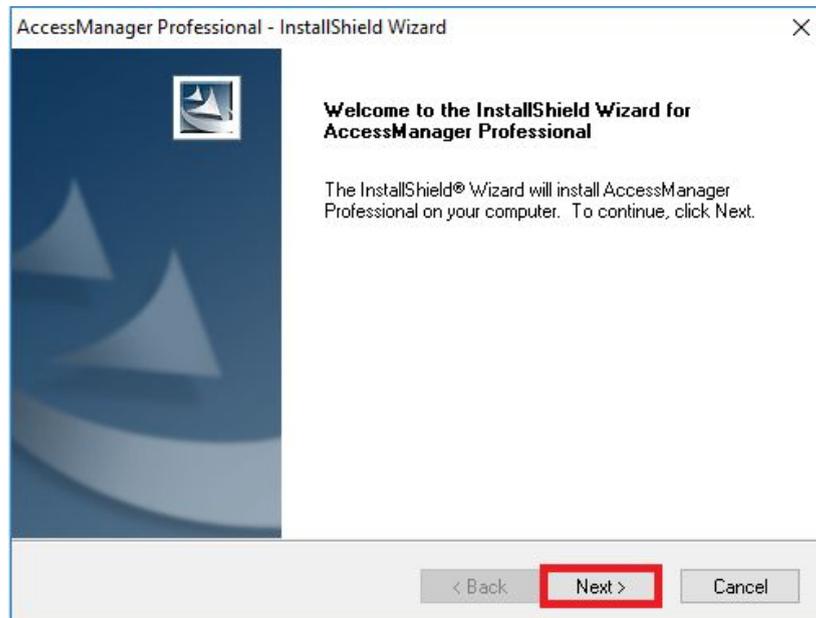
3) Dentro da pasta criada execute o arquivo “*setup.exe*”.

SQLE	07/03/2019 08:05	Pasta de arquivos	
data1.cab	11/02/2016 17:54	Arquivo do WinRAR	8.271 KB
data1.hdr	11/02/2016 17:54	Arquivo HDR	47 KB
data2.cab	11/02/2016 17:54	Arquivo do WinRAR	14.227 KB
engine32.cab	06/04/2005 18:39	Arquivo do WinRAR	531 KB
layout.bin	11/02/2016 17:54	Arquivo BIN	1 KB
serial_ACM.txt	24/06/2015 10:47	Arquivo TXT	1 KB
setup.exe	06/04/2005 18:39	Aplicativo	119 KB
setup.ibt	11/02/2016 17:54	Arquivo IBT	460 KB
setup.ini	11/02/2016 17:54	Parâmetros de co...	1 KB
setup.inx	11/02/2016 17:54	Arquivo INX	237 KB
SQLE.exe	14/01/2016 14:24	Aplicativo	271.493 KB

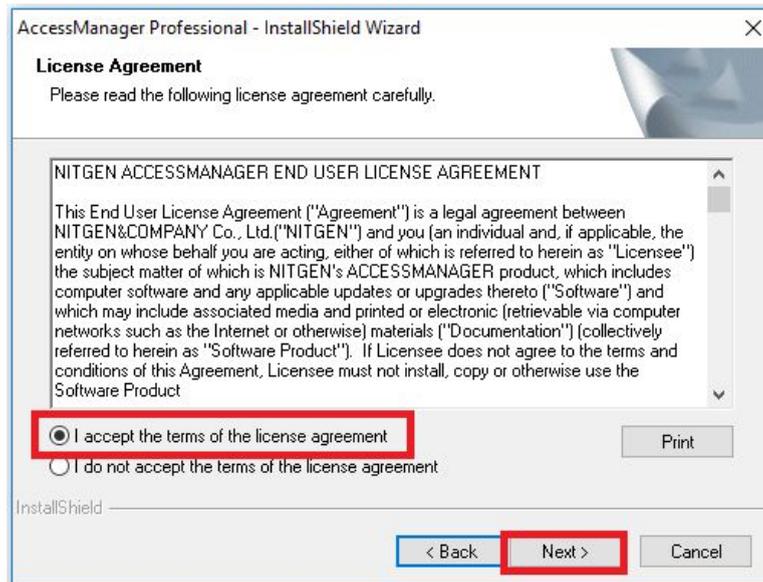
4) Se a mensagem abaixo aparecer, clique em “Sim” para continuar a instalação.



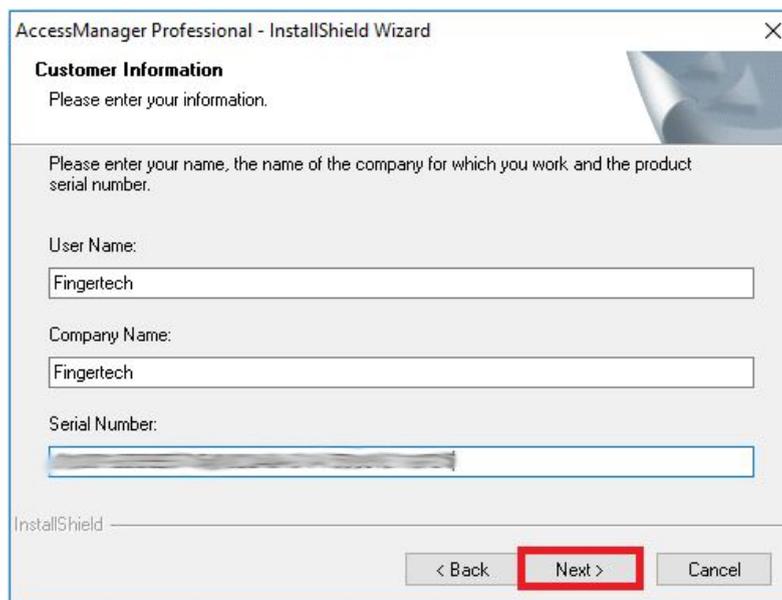
5) Na tela seguinte, clique em “Next”.



6) Aceite os termos de uso e clique em “Next” para prosseguir.



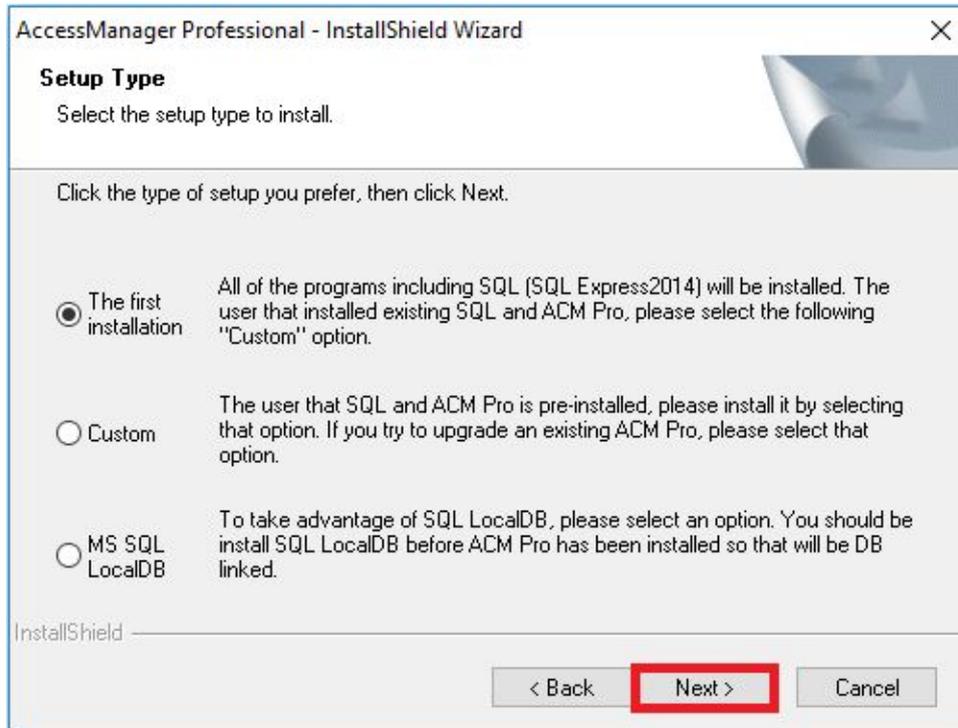
7) Na tela abaixo preencha os campos com o nome do usuário, nome da empresa e por último adicione no campo “Serial Number” a chave de ativação presente dentro do arquivo “serial_ACM.txt” presente dentro da pasta que você descompactou. Por fim clique em “Next” para avançar.



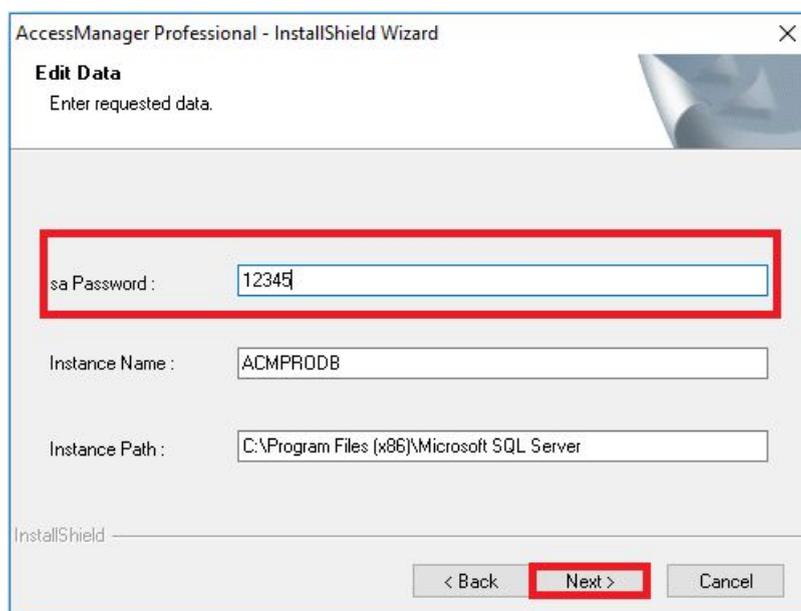
8) Na tela seguinte você terá 3 opções de instalação. A primeira “The first installation” irá realizar uma instalação completa, onde serão instalados além do ACM, o MSSQL Server e os demais componentes necessários. A segunda instalação “Custom”, você tem a opção de instalar os componentes desejados. E por último “MS SQL LocalDB” irá instalar apenas o ACM, presumindo que você já tenha um outro banco de dados MSSQL instalado no computador e que será usado pelo ACM. Sempre que possível recomendamos a



instalação da primeira opção “The first installation”, a fim de evitar problemas, as outras opções só devem ser utilizadas em casos onde o usuário entende bem o que está fazendo.

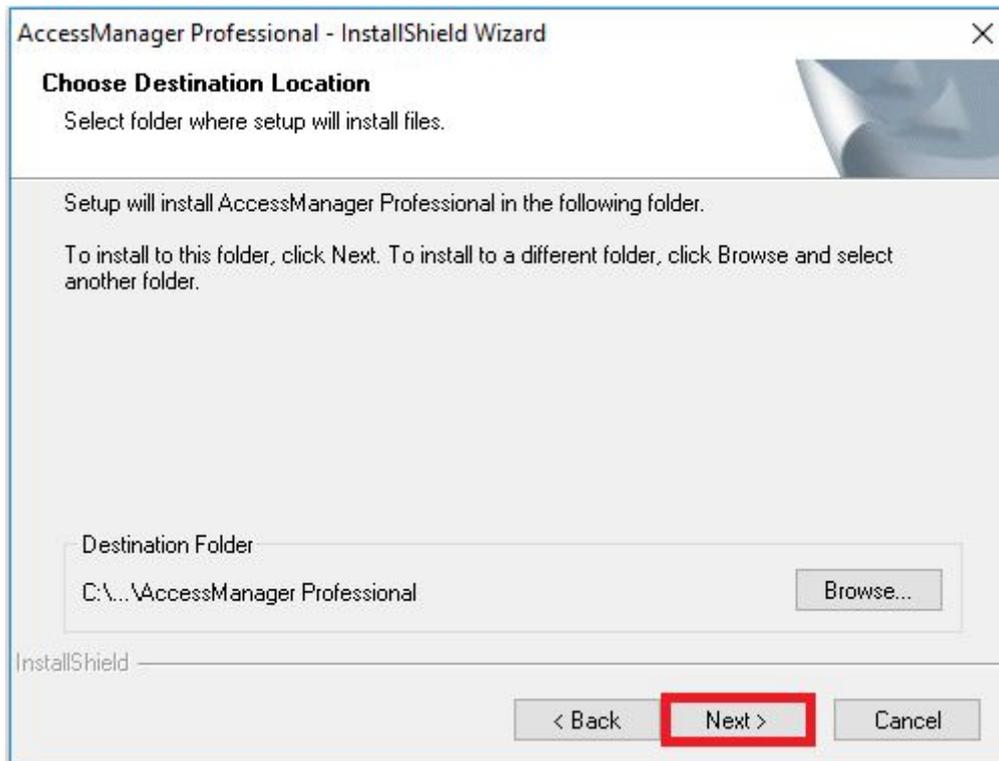


9) Na próxima tela, será solicitado a senha do banco de dados, o nome da instância do banco e por último o caminho de instalação do MSSQL Server. Recomendamos a alteração somente da senha (*sa Password*), os demais campos, deixe como estão, caso você não saiba o que significa.

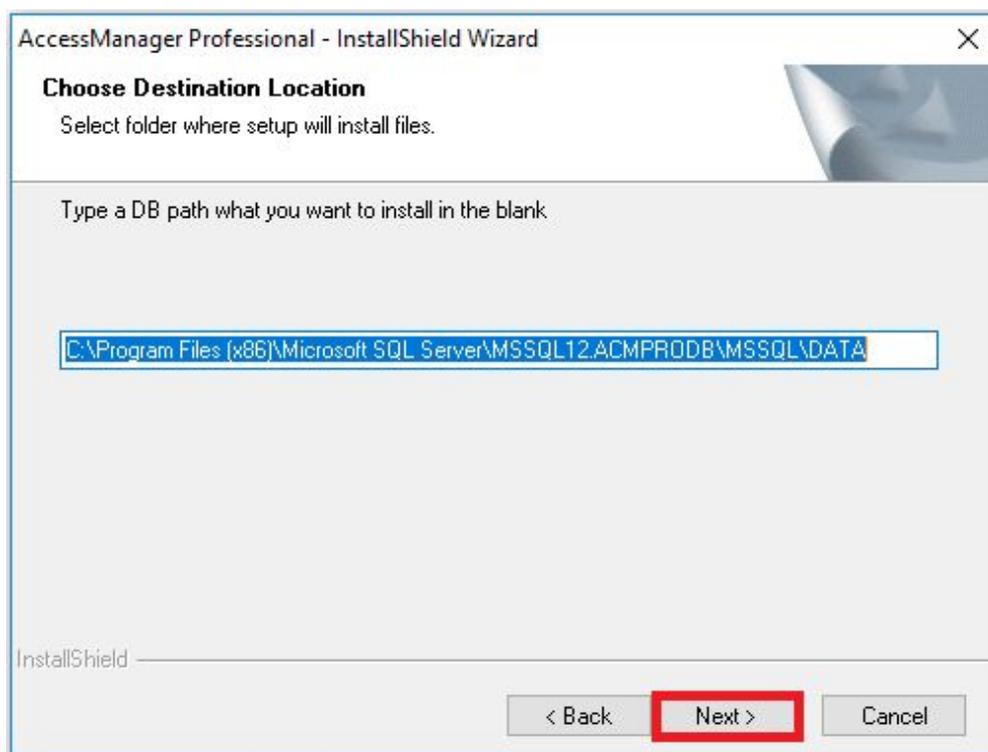




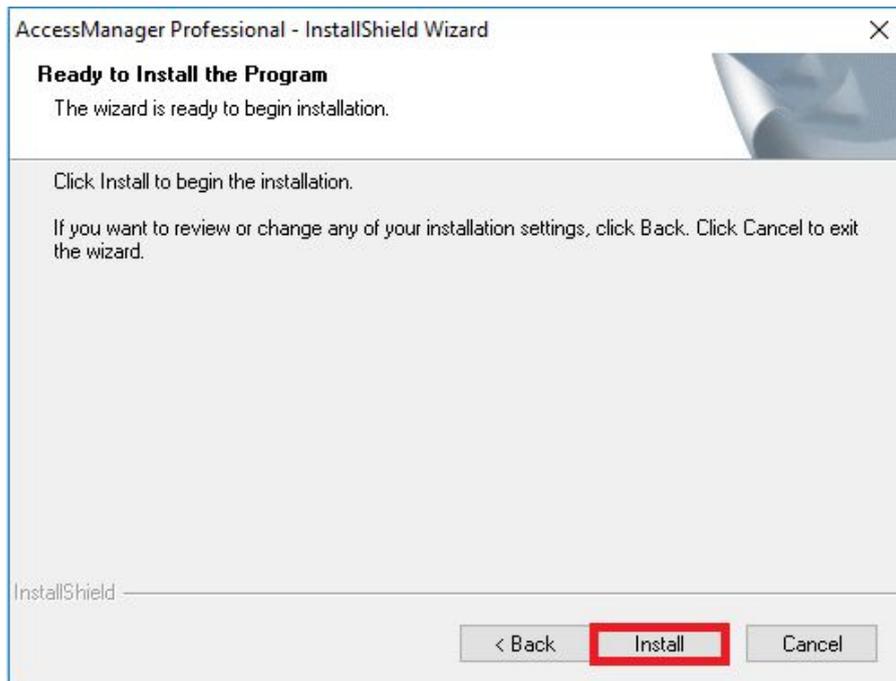
10) Na tela abaixo, você tem a opção de modificar o endereço de instalação do ACM, recomendamos que este endereço não seja alterado. Clique em “Next” para continuar. A etapa seguinte da instalação poderá levar alguns minutos, aguarde.



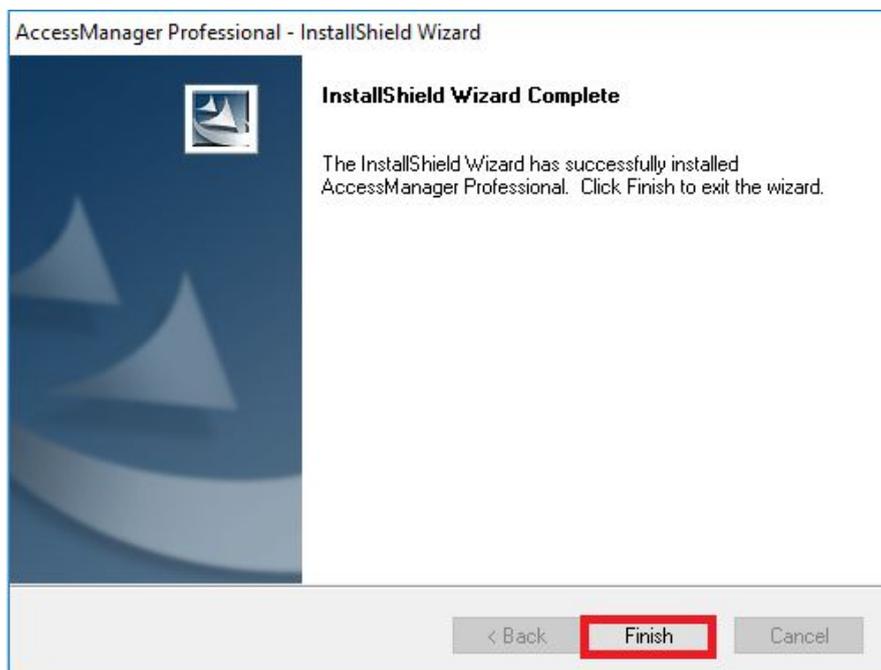
11) Quando a etapa anterior da instalação for finalizada, a tela abaixo aparecerá, clique em “Next” para continuar.



12) Na próxima tela, clique em “*Install*”.

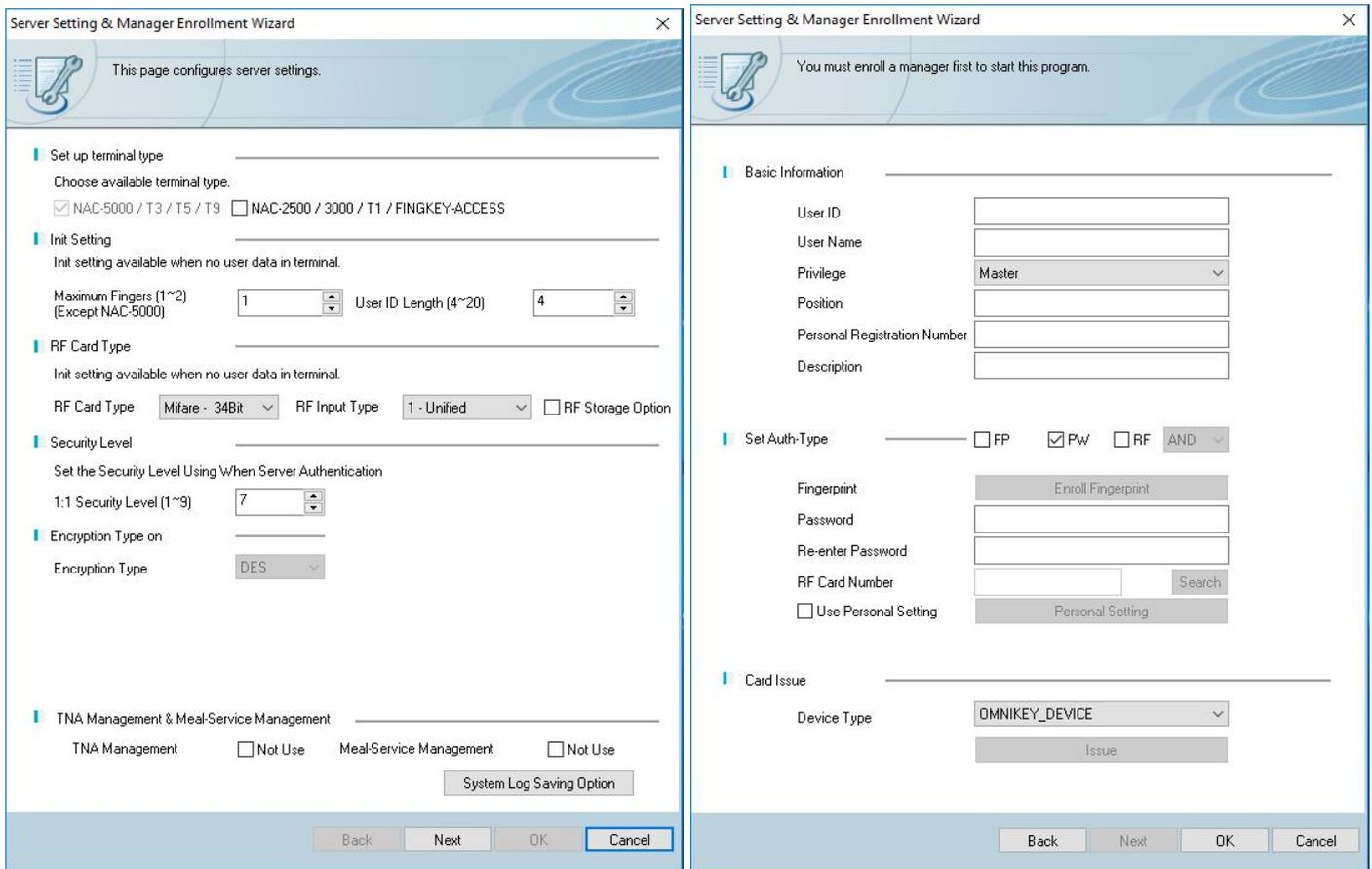


13) E por último, clique em “*Finish*” na tela abaixo, para finalizar a instalação.



2. Configurações Iniciais do Access Manager (ACM)

Ao executar o ACM pela primeira vez, será solicitado que você faça algumas configurações iniciais, dividida em duas telas, a primeira relacionado a configurações do dispositivo e na segunda será solicitado a criação de um usuário administrador para o sistema.



Na primeira tela relacionada a configurações, temos seis áreas, sendo a primeira a “Set up terminal type” mostrada na imagem abaixo. Nesta área você pode determinar quais tipos de dispositivos (NACs) que você terá em sua rede, caso você tenha um NAC 1500 (FINGKEY-ACCESS) você precisará selecionar também a opção “NAC-2500/3000/T1/FINGKEY-ACCESS”.





FINGERTECH

Tecnologia que deixa você no controle.

Na segunda região “*Init Setting*”, você deverá configurar quantos dedos por usuário deverão ser cadastrados, e também qual deverá ser o tamanho do ID do usuário, lembrando que este tamanho precisar ser o mesmo que foi cadastrado no dispositivo NAC (vide tópico 2).

Init Setting

Init setting available when no user data in terminal.

Maximum Fingers (1~2)
(Except NAC-5000) User ID Length (4~20)

Já a terceira região está relacionada ao uso de cartões de acesso. Você poderá escolher entre os tipos de cartões disponíveis (Mifare, HID, EM, IClass, CEPAS, etc), se o cartão utilizará ou não “*Facility Code*” no campo “*RF Input Type*”, e por último se o cartão irá ou não armazenar informações.

RF Card Type

Init setting available when no user data in terminal.

RF Card Type RF Input Type RF Storage Option

A quarta área “*Security Level*” é relacionada ao nível de segurança da autenticação, quanto maior o nível de segurança, mais pontos de minúcias serão analisados, diminuindo assim possíveis casos de falso aceite, mas em contrapartida o usuário precisará posicionar o dedo sobre o leitor de maneira mais cuidadosa.

Security Level

Set the Security Level Using When Server Authentication

1:1 Security Level (1~9)

Já na quinta região “*Encryption Type on*” está relacionado a criptografia dos dados, recomendamos manter desabilitado.

Encryption Type on

Encryption Type

Por último, na região “*TNA Management & Meal-Service Management*”, você poderia desabilitar o serviço de ponto ou desabilitar o gerenciamento de pausas para refeição. É recomendado não alterar essas configurações caso não saiba exatamente o que está fazendo.

TNA Management & Meal-Service Management

TNA Management Not Use Meal-Service Management Not Use



Na tela seguinte, referente a criação do usuário, a tela é dividida em apenas 3 regiões. Na primeira região “*Basic Information*”, basta adicionar as informações do usuário, atenção na hora de definir o usuário como *Master* ou *Normal*, lembrando que master se refere ao administrador.

Basic Information

User ID	<input type="text"/>
User Name	<input type="text"/>
Privilege	Master <input type="button" value="v"/>
Position	<input type="text"/>
Personal Registration Number	<input type="text"/>
Description	<input type="text"/>

Na segunda área desta tela “*Set Auth-Type*” você poderá definir quais serão os meios de autenticação que o usuário poderá utilizar, na hora de se identificar no NAC. Poderá ser utilizado impressão digital (FP), senha (PW) ou cartão (RF), você também poderá permitir que o usuário utilize mais de uma opção de autenticação, para isso você precisará utilizar os operadores “*AND*” e “*OR*”. O operador “*AND*” obriga o usuário a toda vez que for realizar a autenticação apresentar todos os meios selecionados, já o operador “*OR*” permite que o usuário escolha uma das maneira para se autenticar.

Set Auth-Type

FP PW RF AND

Fingerprint	<input type="button" value="Enroll Fingerprint"/>
Password	<input type="text"/>
Re-enter Password	<input type="text"/>
RF Card Number	<input type="text"/> <input type="button" value="Search"/>
<input type="checkbox"/> Use Personal Setting	<input type="button" value="Personal Setting"/>

Na terceira região você poderá adicionar configurações sobre os cartões que serão emitidos.

Card Issue

Device Type	OMNIKEY_DEVICE <input type="button" value="v"/>
	<input type="button" value="Issue"/>



3. Sincronizando Terminal

Após a instalação do software Access Manager e com ele conectado a rede após realizar as configurações mostradas no Tópico 5 (*Configurando NAC - Modo Network Local (NL)*), deverá ser mostrada a mensagem “*Não registrado/Not registered*” no visor do dispositivo NAC. Já no Access Manager o terminal aparecerá automaticamente no menu “*Gerenciador de Terminal / Terminal Management*”, conforme mostrado abaixo.

Terminal ID	Terminal Name	Status	IP Address	Description	Entry zone	Exit zone
1		Not Enrolled	192.168.1.190		Init value	Init value

Embora o terminal esteja aparecendo na tela de “*Gerenciador de Terminal / Terminal Management*”, ele ainda não foi registrado devidamente. Para que você consiga gerenciar o NAC através do ACM você precisará registrar o terminal NAC no Access Manager, para isso clique com o botão direito do mouse sobre o terminal que está aparecendo em “*Gerenciador de Terminal / Terminal Management*” e em seguida escolha a opção “*Propriedades/Properties.*”, conforme mostrado abaixo.

Terminal ID	Terminal Name	Status	IP Address	Description	Entry zone	Exit zone
1		Not Enrolled	192.168.1.190		Init value	Init value

Na tela que aparecerá, preencha o nome do terminal e a descrição, lembrando que o ID do terminal já vem preenchido e que deve permanecer o mesmo que foi cadastrado no dispositivo NAC, e também que não pode estar duplicado na rede.

Enroll Terminal

Please enroll terminal information

Basic Information

Terminal ID (1 ~ 2000)

Terminal Name

Description

OK Cancel

Após isso, seu terminal será registrado, dessa forma sumindo a mensagem “*Não registrado/Not registered*” do dispositivo NAC e no Access Manager ele será mostrado conforme a imagem abaixo.

Terminal ID ▲	Terminal Name	Status	IP Address	Description	Entry zone	Exit zone
1	Entrada Principal ...	Normal	192.168.1.190	NAC localizado na ...	Init value	Init value

A partir de agora, você conseguirá gerenciar os dispositivos a partir do software Access Manager, seja para incluir ou remover usuário, gerar relatórios, controlar horários de acesso, dentre as demais funcionalidades disponíveis.

4. O Access Manager não Reconhece o Terminal NAC

Embora não seja comum, há casos onde o terminal NAC não é reconhecido pelo Access Manager, de forma que quando acessado o menu “*Gerenciador de Terminal / Terminal Management*” ele não aparece na lista de dispositivos. Em geral o que leva isso a ocorrer trata-se de alguma Aplicação/Serviço (antivírus, firewall) bloqueando o dispositivo, alguma configuração da rede, ou alguma configuração no dispositivo realizada de maneira errada.

Para tentar solucionar este problema, solicitamos que você verifique os pontos apresentados abaixo.

- 1) Verifique se o terminal NAC utilizado está conectado a um ponto de rede.
- 2) Verifique se foi definido um ID para o terminal NAC, e se esse ID não está sendo utilizado por outro terminal.
- 3) Verifique se a quantidade de dedos (*FP Number*) por usuário cadastrada no terminal NAC é a mesma cadastrada no Access Manager.
- 4) Verifique se o tamanho do ID (*ID Length*) dos usuários cadastrado no terminal NAC é o mesmo do cadastrado no Access Manager.
- 5) Verifique se as configurações de rede foram definidas de forma correta (DHCP, IP, Máscara de Sub-rede, Gateway e IP do Servidor).
- 6) Verifique se o IP definido para o terminal NAC, não está sendo utilizado por outro dispositivo na rede.
- 7) Verifique se o IP do Servidor para o qual o terminal NAC está apontado, de fato é o correto, ou seja, se é o IP da máquina no qual o Access Manager está instalado.
- 8) Verifique se o terminal NAC e o Servidor estão na mesma rede.
- 9) Se foi adicionado algum terminal NAC manualmente no Access Manager, apague ele e veja se o dispositivo NAC que está tentando instalar aparece na lista de terminais.
- 10) Verifique se não tem algum serviço ou aplicação impedindo a comunicação entre o terminal NAC e o Access Manager, se for o caso crie uma exceção na aplicação ou serviço permitindo a comunicação entre os dois.
 - a) **Firewall** - Tente desativar o firewall por alguns minutos e veja se funcionou.
 - b) **Antivírus** - Tente desativar o antivírus por alguns minutos e veja se funcionou.
 - c) **Roteador** - Verifique a configuração do seu roteador.



5. Gerenciando Usuários

É possível adicionar, alterar ou remover usuário a partir do próprio terminal NAC, conforme mostrado nos tópicos 6, 7 e 8. Mas também é possível realizar todo o gerenciamento dos usuários através do Access Manager, evitando o trabalho de se deslocar muitas vezes até o terminal NAC.

Primeira coisa que precisamos entender sobre o gerenciamento de usuários através do Access Manager é que os usuários cadastrados no ACM não vão para o terminal NAC de maneira automática, e nem o contrário, os usuários cadastrados no terminal NAC não estarão disponíveis no ACM automaticamente. Após adicionar, alterar ou remover um usuário em qualquer uma das pontas, será sempre necessário sincronizar os dois (ACM e terminal NAC).

Para ficar mais claro vamos a alguns exemplos práticos. Inicialmente vamos adicionar um usuário ao ACM e em seguida enviá-lo para o terminal NAC. E após isso o processo inverso, inserir um usuário através do terminal NAC e sincronizá-lo com o ACM.

Inserindo Usuário Através do ACM

Vá no menu “Gerenc. Usuár./User Management” localizado do lado esquerdo da tela. Nesta tela será mostrada a lista de todos os usuários cadastrados no ACM, inclusive o primeiro usuário que criamos na hora da instalação do programa. Como exemplo criaremos um novo usuário, para isso clique no botão “Insc. Usuár./Enroll User”, conforme mostrado na tela abaixo.

ID Usuár.	Nome Usuár.	Privilégio	Tipo Aut.	Grupo ID	Nome Grupo	Departamento	APB Status
0001	Fingertech	Master	PW	0			

Na tela abaixo preencha as informações de maneira mais detalhada e correta possível, lembrando que o ID do usuário não pode ser um ID já existente no ACM ou no terminal NAC. No campo “Privilégio/Privilege” os usuários são cadastrados por padrão como o tipo “Normal”, vale ressaltar que apenas os usuários administradores, ou seja, aqueles que podem alterar as configurações do ACM e do terminal NAC, devem ser cadastrados como “Master”, mas recomendamos novamente cuidado ao cadastrar um usuário como “Master”. Algumas informações são obrigatórias e outras opcionais, então atenção ao preencher as informações.



FINGERTECH

Tecnologia que deixa você no controle.

Informação Básica	
ID Usuário	0002
Nome Usuário	João
Grupo	Numero Grupo sem Nu. <input type="button" value="Selec."/>
Access Group	No Accessgroup
Posição	Sem posição
Privilegio	Usuár. Normal
Código Timezone	Não selecionado
Departamento	Comercial
Numero Pessoal Registro	987
Country Code / Phone Number	55 4333744700
Descrição	Funcionário do departamento comercial d
Data Registrada	06/05/2019
<input type="checkbox"/> Data Expirada	06/05/2019
EMAIL	joao@fingertech.com.br

Def. Tipo Aut.			
<input type="checkbox"/> FP	<input checked="" type="checkbox"/> PW	<input type="checkbox"/> RF	AND
Imp. Digital	Insc. Imp. Digital		
Senha	●●●●●●		
Dig. Novamente Senha	●●●●●●		
Numero Cartão RF	<input type="checkbox"/> HEX		Procurar
<input type="checkbox"/> Usando Def pessoal	Def. Pessoal		

Edição Cartão		
Tipo de Dispositivo	OMNIKEY_DEVICE	Questão

Sobre os tipos de autenticação do usuário, dependendo do modelo de seu dispositivo NAC é possível cadastrar até 3 tipos de autenticação para cada usuário, são eles: FP (Impressão Digital), PW (Senha) e RF (Cartão). Você pode definir mais de um tipo de autenticação para cada usuário, basta marcar os tipos desejados, e então fazer o cadastro dos tipos de autenticação desejado.

O cadastro da senha é realizado logo abaixo, no campo “*Senha/Password*” e “*Dig. Novamente Senha/Re-enter Password*”. Já para cadastrar uma impressão digital você precisará ter um leitor biométrico de impressão digital conectado diretamente a máquina onde o ACM foi instalado, você pode realizar o cadastro através dele na opção “*Insc. Imp. Digital/Enroll Fingerprint*”, sem a necessidade de se deslocar até o terminal, caso você não tenha o leitor biométrico, você precisará se deslocar até o NAC e então cadastrar a digital conforme explicado no tópico 8 deste material. E para cadastrar o acesso através de cartão, você precisará marcar a opção “*RF*”, preencher o campo “*Numero Cartão RF/RF Card Number*”, e então realizar o cadastro do cartão no terminal NAC, conforme explicado também no tópico 8.

Caso você opte por mais de um método de autenticação você precisará também escolher um tipo de operador (*AND / OR*) que irá determinar como será gerenciada os tipos de autenticação escolhidos. Por exemplo, caso seja decidido que o usuário terá dois tipos de autenticação, “*FP*” e “*PW*” por exemplo, e o operador escolhido for o “*AND*” significa que sempre será solicitado ao usuário que ele passe a digital e também que digite a senha, e caso um dos dois não confira, o acesso dele será negado. Agora caso o operador escolhido seja o “*OR*”, significa que o usuário poderá apresentar apenas um dos tipo cadastrados para realizar a autenticação, bastando que apenas um deles seja autenticado corretamente.



Def. Tipo Aut. Imp. Digital

FP PW RF AND
 Insc. Imp. Digital AND
 OR

Após realizar o cadastro do usuário ele aparecerá na lista de usuários cadastrados conforme mostrado na imagem abaixo.

ID Usuár.	Nome Usuár.	Privilégio	Tipo Aut.	Grupo ID	Nome Grupo	Departamento	APB Status
0001	Fingertech	Master	PW	0			
0002	João	Usuár. Normal	PW	0		Comercial	

Porém se você tentar autenticar agora este usuário no terminal NAC, ele não será reconhecido (“*ID NOT EXIST!*”), isto porque ele ainda não foi sincronizado ao terminal NAC. Para adicionar este usuário ao terminal NAC vá em “*Gerenc. Terminal / Terminal Management*”, selecione o terminal desejado, e clique na opção “*List Aut./Authentication List*”, conforme mostrado abaixo.

Terminal ID	Terminal Name	Status	IP Address	Descrição	Zona Entrada	Zona Saída
1	Entrada Principal ...	Normal	192.168.1.55	NAC localizado na ...	Inic. Valor	Inic. Valor

Na tela apresentada existem duas listas “*Lista Usuários usando Aut. Servidor / User List Using Server Authentication*” e “*Lista Usuário usando Aut. Terminal / User List Using Terminal Authentication*”. Para que um usuário possa ser autenticado no terminal NAC ele precisa pertencer a alguma das duas listas, a diferença é que na primeira a autenticação ocorre do lado do servidor, ou seja, é necessário que o NAC esteja na rede para que a autenticação seja realizada. Já na segunda lista a autenticação ocorre no próprio terminal NAC, ou seja, mesmo que o terminal não esteja conectado a rede, seja por problemas ou qualquer outro motivo, ainda sim o usuário conseguirá realizar a autenticação, porque seus dados de acesso estão também localizados no próprio terminal.



Informações do usuário autenticado lista (Terminal ID : 1)

Lista de usuárs. no Terminal selecionado.

Lista Usuários usando Aut. Servidor Pessoas : 0

ID Usuár. Δ	Nome Usuár.	IG Grupo	Reserv...
-------------	-------------	----------	-----------

Lista Usuários usando Aut. Terminal Pessoas/FP : 0/0

ID Usuár. Δ	Nome Usuár.	IG Grupo	Master	FP Co...	Reserv...
-------------	-------------	----------	--------	----------	-----------

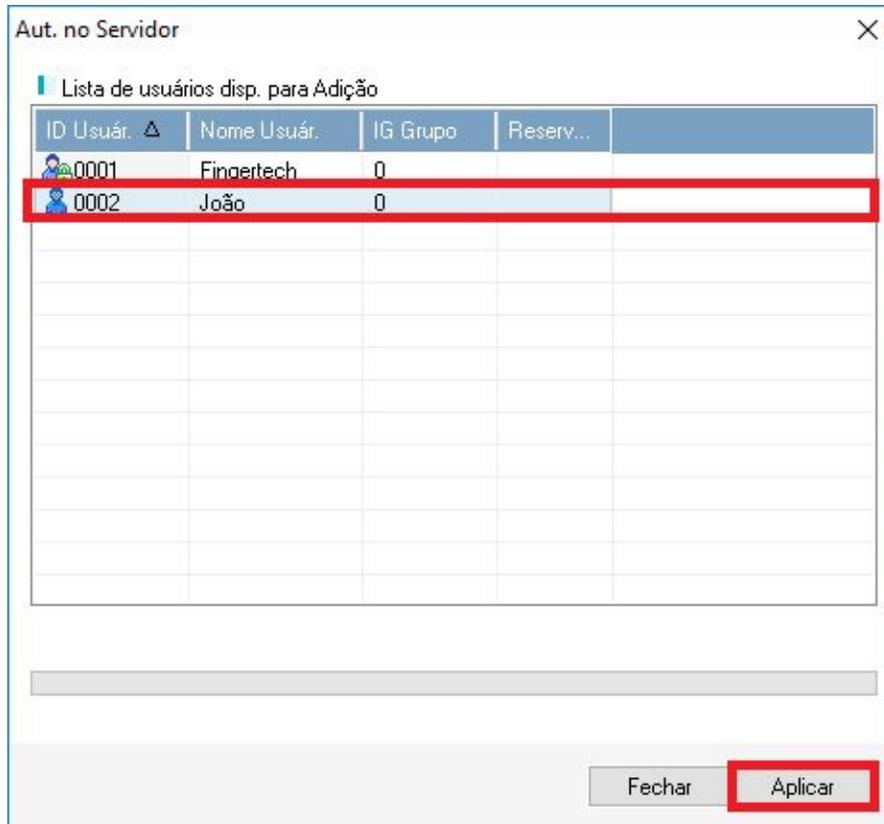
Adc Delete

Adicionar Deletar Master Aplicar

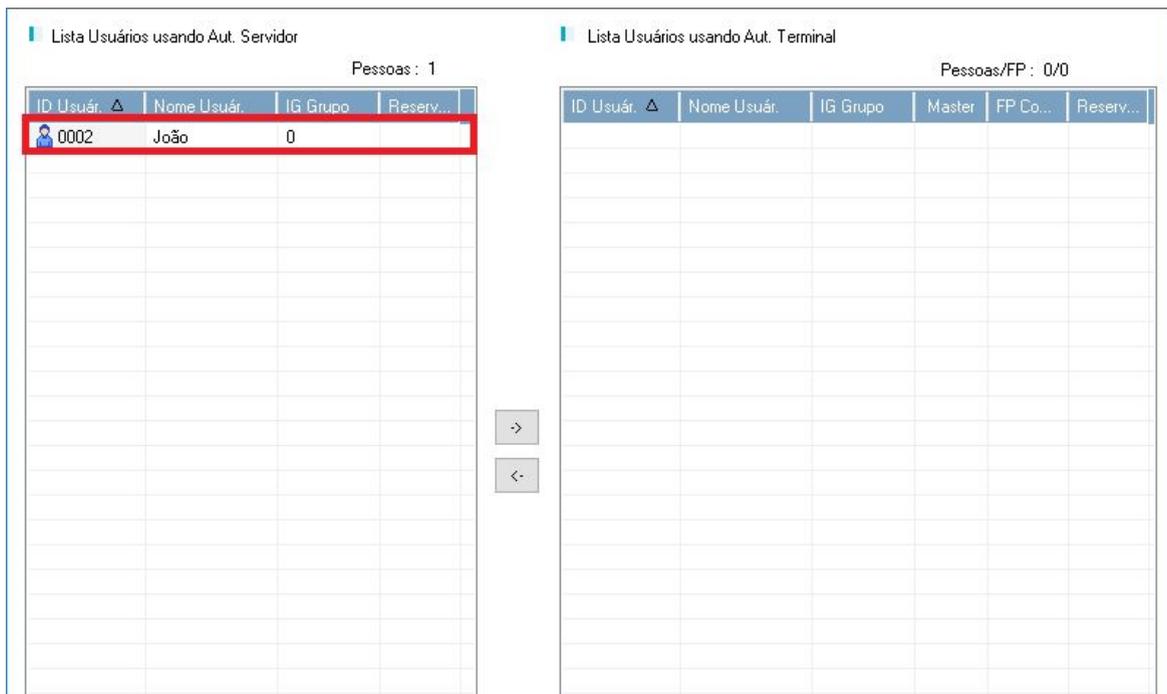
Cancela

OK Fechar

Para permitir que o usuário realize a autenticação via terminal NAC, você precisará primeiro escolher em qual das listas ele fará parte, ou mesmo se ele fará parte das duas listas. Para adicionar o usuário em uma lista você precisará selecionar a opção de adicionar/Add localizada logo abaixo da lista desejada, conforme mostrada na imagem anterior. Será exibida uma tela onde aparecerá todos os usuário cadastrados no ACM, basta selecionar o usuário que deseja adicionar à lista e clicar sobre o botão "Aplicar".



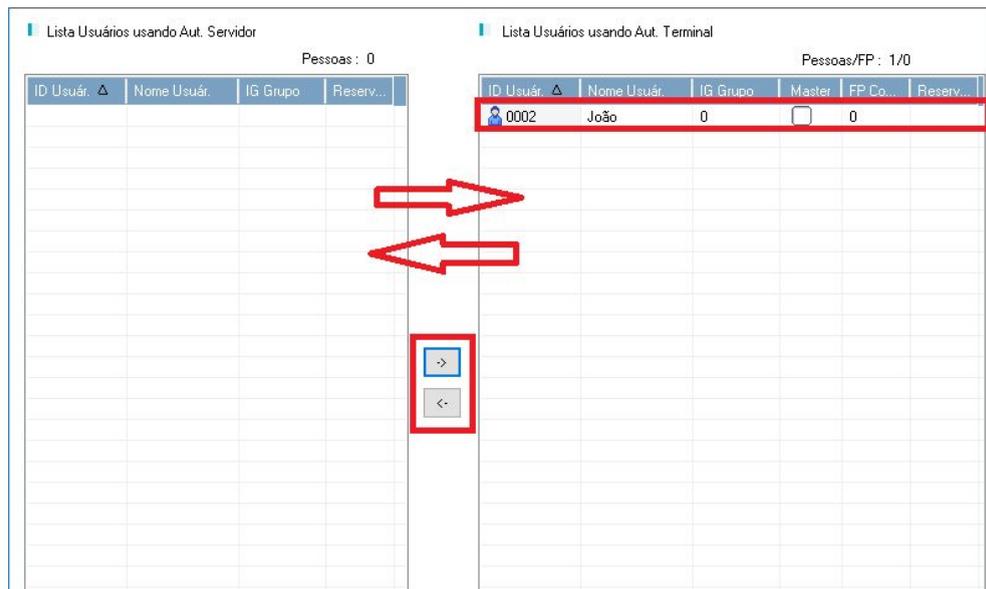
O usuário será automaticamente adicionado à lista desejada conforme mostrado abaixo.



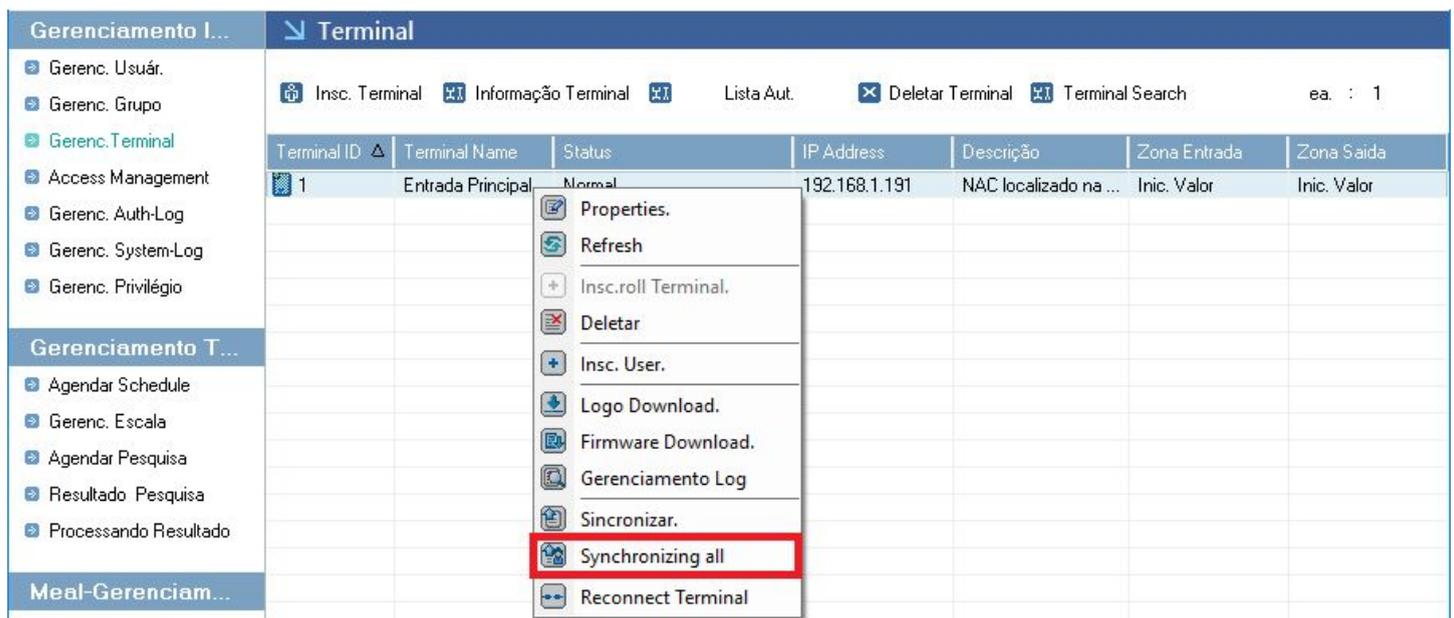


Com isso o usuário já poderá realizar a autenticação no terminal NAC, de acordo com as especificações de cada lista.

Você também poderá mover o usuário entre uma lista e outra, através das setas localizadas entre as duas listas.



Obs.: Pode ser necessário realizar a sincronização do ACM com o terminal NAC, dependendo das mudanças realizadas. Para isso clique com o botão direito do mouse sobre o terminal desejado e em seguida clique na opção “Synchronizing all”, conforme mostrado abaixo.





Inserindo Usuário Através do Terminal NAC

Para inserir um usuário através do terminal NAC basta ir até o terminal, clicar sobre o botão “MENU”, realizar a autenticação como usuário “Master/Administrador” e então seguir os passos apresentados no tópico 6 deste documento “6. Cadastrando um Novo Usuário”.

Após cadastrar o novo usuário no terminal ele aparecerá automaticamente no ACM, para verificar o novo usuário cadastrado basta ir no menu “Gerenc. Usuár./User Management” localizado no lado esquerdo do ACM, que o usuário será mostrado conforme a imagem abaixo, onde o usuário de ID “0003” foi cadastrado via terminal.

ID Usuár.	Nome Usuár.	Privilégio	Tipo Aut.	Grupo ID	Nome Grupo	Departamento
0001	Fingertech	Master	PW	0		
0002	João	Usuár. Normal	PW	0		Comercial
0003	0003	Usuár. Normal	FP/PW (OR)	0		

Caso o usuário não apareça, tente atualizar os dados (tela) apertando a tecla de função “F5”. Vale lembrar também que isso vale apenas para dispositivos configuração para trabalhem em rede (Network Local - NL).

Editar/Alterar Informações do Usuário

Caso você precise editar/alterar as informações de um usuário, seja ele cadastrado através do ACM ou através do terminal NAC, você precisará ir no menu “Gerenc. Usuár./User Management”, e então clicar duas vezes com o botão esquerdo do mouse sobre o usuário que deseja alterar ou clicar com o botão direito do mouse e em seguida escolher a opção “Properties.”.

ID Usuár.	Nome Usuár.	Privilégio	Tipo Aut.	Grupo ID	Nome Grupo	Departamento
0001	Fingertech	Master	PW	0		
0002	João	Usuár. Normal	PW	0		Comercial
0003	0003	Usuár. Normal	FP/PW (OR)	0		

- Properties.
- Authentication List
- Config.timezone código para cada usuário.
- Deletar
- Refresh
- Iniciar APB Status

Será aberta então, a tela para edição das informações conforme mostrado abaixo. Basta alterar os dados desejados do usuário e em seguida clicar em “OK”.

Informação Usuár. (User ID : 0003)

Informação Básica

ID Usuário: 0003

Nome Usuário: Maria

Grupo: Numero Grupo sem Nt. [Selec.]

Access Group: No Accessgroup [Definir]

Posição: Sem posição

Privilegio: Usuár. Normal

Código Timezone: Não selecionado

Departamento: Financeiro

Numero Pessoal Registro: 321

Country Code / Phone Number: 55 4333744700

Descrição: Responsável pelo departamento financeiro.

Registrado / Data Expirada: 07/05/2019 08/05/2019

EMAIL:

Def. Tipo Aut.

Mobile Key FP PW RF Face OR

Imp. Digital: Insc. Imp. Digital

Senha: ●●●●●●

Dig. Nov. Senha: ●●●●●●

Numero Cartão RF: HEX Procurar

Usando Def pessoal Def. Pessoal

Edição Cartão

Tipo de Dispositivo: OMNIKEY_DEVICE Questão

OK Cancela

ID Usuár. Δ	Nome Usuár.	Privilegio	Tipo Aut.	Grupo ID	Nome Grupo	Departamento
0001	Fingertech	Master	PW	0		
0002	João	Usuár. Normal	PW	0		Comercial
0003	Maria	Usuár. Normal	FP/PW (OR)	0		Financeiro



Deletar/Remover Usuário

Primeiramente você precisa ter em mente se você deseja de fato apagar o registro do usuário do sistema, ou apenas não permitir que o usuário consiga realizar a autenticação em um terminal NAC. Geralmente se opta por apenas não permitir que o usuário consiga se autenticar nos terminais, mantendo o histórico de seus registros armazenado, mas a decisão pertence aos usuários “*Master/Administradores*”.

Caso você deseje apenas remover o acesso do usuário ao terminal NAC, basta você ir até o menu “*Gerenc. Terminal / Terminal Management*”, selecionar o terminal no qual o usuário perderá o acesso e então clicar em “*List Aut./Authentication List*”.

The screenshot shows the 'Gerenciamento I...' menu on the left with 'Gerenc. Terminal' highlighted. The main area is titled 'Terminal' and contains a table of terminals. The 'Lista Aut.' button is highlighted with a red box.

Terminal ID	Terminal Name	Status	IP Address	Descrição	Zona Entrada	Zona Saida
1	Entrada Principal ...	Normal	192.168.1.52	NAC localizado na ...	Inic. Valor	Inic. Valor

Na nova janela remova o usuário de ambas as listas, para isso selecione o usuário e clique no botão “Delete/Deletar” localizado abaixo da lista da qual ele pertence.

The screenshot shows a window titled 'Informações do usuário autenticado lista (Terminal ID : 1)'. It contains two tables of users. The right table, 'Lista Usuários usando Aut. Terminal', has two users: João (ID 0002) and Maria (ID 0003). The row for João is highlighted with a red box. Below the tables are buttons for 'Delete' and 'Deletar', both highlighted with red boxes.

ID Usuár.	Nome Usuár.	IG Grupo	Master	FP Co...	Reserv...
0002	João	0	<input checked="" type="checkbox"/>	0	
0003	Maria	0	<input type="checkbox"/>	2	



Com isso ele já perderá acesso ao dispositivo, porém seu registro irá continuar localizado no menu “Gerenc. Usuár./User Management”, caso você deseje reativar o acesso, ou apenas para manter um histórico de registro.

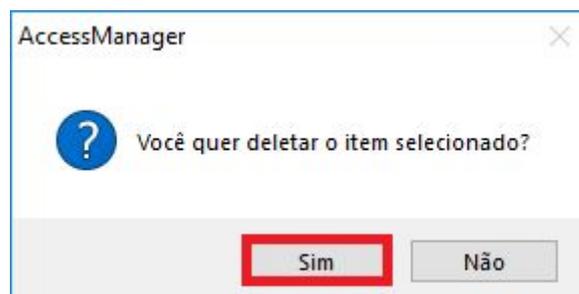
ID Usuár.	Nome Usuár.	Privilegio	Tipo Aut.	Grupo ID	Nome Grupo	Departamento
0001	Fingertech	Master	PW	0		
0002	João	Usuár. Normal	PW	0		Comercial
0003	Maria	Usuár. Normal	FP/PW (OR)	0		Financeiro

Agora caso você deseje deletar o usuário completamente, removendo seu acesso aos terminais NAC e apagando seu histórico de registro, basta você ir no menu “Gerenc. Usuár./User Management”, escolha o usuário que deseja apagar, e clique com o botão direito do mouse sobre o usuário e em seguida escolha a opção “Deletar”.

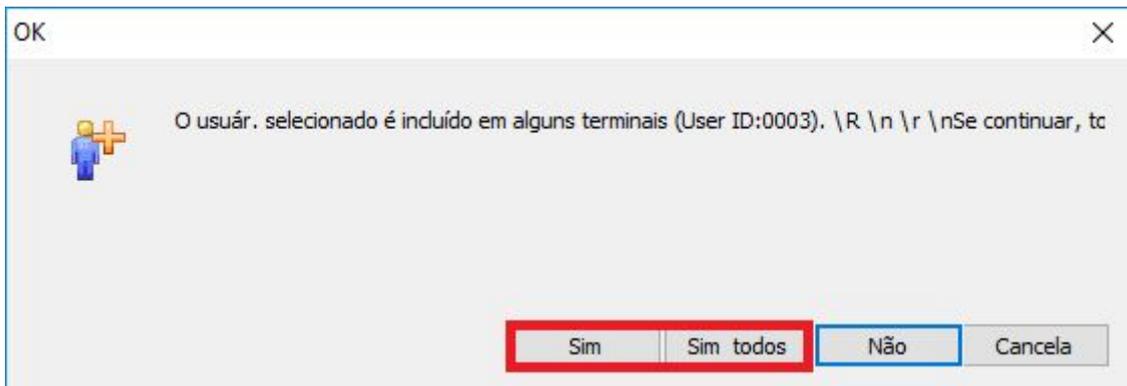
ID Usuár.	Nome Usuár.	Privilegio	Tipo Aut.	Grupo ID	Nome Grupo	Departamento
0001	Fingertech	Master	PW	0		
0002	João	Usuár. Normal	PW	0		Comercial
0003	Maria	Usuár. Normal	FP/PW (OR)	0		Financeiro

- Properties.
- Authentication List
- Config.timezone código para cada usuário.
- Deletar**
- Refresh
- Iniciar APB Status

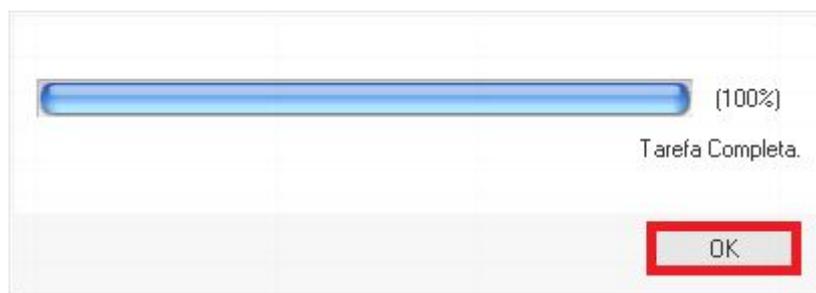
Na janela que aparecerá basta clicar em “Sim” para confirmar.



Se o usuário estiver cadastrado em algum terminal NAC, a mensagem abaixo aparecerá perguntando se você realmente deseja excluir o usuário, e que isso removerá o acesso dele a todos os terminais NAC cadastrados.

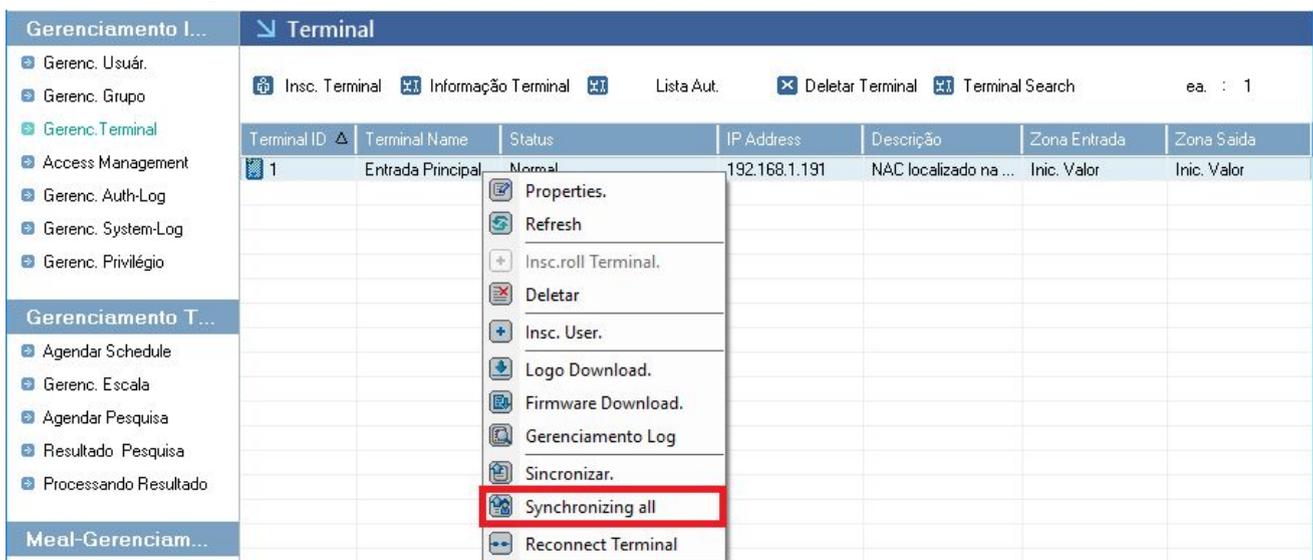


Caso você realmente tenha certeza que deseja excluir este usuário, clique em “Sim todos”, que o usuário será removido automaticamente, e então a mensagem abaixo aparecerá, basta clicar em “Ok” e pronto, o processo foi finalizado.



Se o usuário tentar agora realizar a autenticação em algum terminal NAC, ele já não conseguirá.

Obs.: Pode ser necessário realizar a sincronização do ACM com o terminal NAC, dependendo das mudanças realizadas. Para isso clique com o botão direito do mouse sobre o terminal desejado e em seguida clique na opção “Synchronizing all”, conforme mostrado abaixo.





Options Menu (English) - NAC 1500 (SW101M2)

1. User Manager	1. Register User	1. Input ID :	* Input a new ID for user
		2. User Type :	Normal / Master (The first ID is always master)
		3. FP / PW (Fingerprint / Password):	1. FP (Only Fingerprint)
			2. PW (Only Password)
			3. FP / PW (Fingerprint OR Password)
			4. FP & PW (Fingerprint AND Password)
		4. Input Passwd 1:	* Password (Only Numbers)
		4. Input Passwd 2:	* Repeat Password (Only Numbers)
	5. Place FP 1:	* Register Fingerprint	
	5. Place FP 2:	* Repeat Fingerprint	
	2. Modify User	1. Input ID :	* Input the user ID you want to change
		1. Authen. Mode	1. FP (Only Fingerprint)
			2. PW (Only Password)
			3. FP / PW (Fingerprint OR Password)
			4. FP & PW (Fingerprint AND Password)
2. FP (Fingerprint)	* Register twice the same fingerprint		
3. User Type	Normal / Master		
4. Password	* Only Numbers		
3. Delete User	1. Input ID :	* Input the user ID you want to delete	
	Are You Sure?	YES / NO	
4. Delete All	Are You Sure?	YES / NO	

2. FP Option	1. Secu. Level	1. 1:1 Mode	(1-9) : 5
	2. Capture Mode	Normal/LFD_1/LFD_2/LFD_3	
	3. SensorTimeout	(1-30): 5	
	4. Auto-On Check	ON / OFF	
	5. 1:N Timeout	1. Use Timeout	ON / OFF
		2. Set Timeout	(2-9): 3
6. FreeScan Mode	ON / OFF		

3. UI Option	1. Language	2. English
		7. Portuguese
	2. Voice	ON / OFF
	3. Beep	ON / OFF
	4. Funckey Disp	OFF/Modo1/Modo2
	5. MenuTimeout	ON / OFF
	6. LCD BL Timeout	ON / OFF
7. Backlight Level	(1-4) : 2	



FINGERTECH

Tecnologia que deixa você no controle.

4. System Option	1. Log	ON / OFF
	2. RF Card	OFF/HID/MIFARE/EM/iClass
	3. Wiegand	OFF/26bit/34bit/37bit
	4. Function Mode	AC / T&A
	5. Auth Mode	SO / NL
	6. Time Setting	201X/XX/XX XX:XX:XX
	7. Terminal Mode	Reader / Terminal
	8. Timezone Mode	ON / OFF

5. Network	1. Terminal ID	(1 ~ 2000) : 1	
	2. TCP/IP	1. Use DHCP?	ON / OFF
		2. Terminal IP	0.0.0.0
		3. Subnet Mask	0.0.0.0
		4. Gateway	0.0.0.0
		5. Server IP	192.168.0.2
	3. N/W Timeout	(2-60) : 10	
	4. Port Number	: 7332	
5. Connect Ver	3 / 4		

6. Information	1. # of User	Normal: 0 Master: 0
	2. F/W Version	6.000-0061
	3. 485 ID	: 0

7. Factory Init	1. DB Format	YES / NO
	2. Factory Format	YES / NO
	3. FP Number	1 / 2
	4. ID Length	(4-15): 4
	5. Reset Term	YES / NO