www.virdi.com.br

Software VIRDI UNIS

Guia rápido de Utilização

e-mail: sales@virdi.com.br - Tel.: +55 11 4368-3800 - www.virdi.com.br
Av. Paulista, 2.300 - andar Pilotis - Bela Vista - São Paulo - 01310-300 - Brasil

© 2010 Virdi

Rev. A.0

Índice

Introdução 03
Instalação do Software VIRDI UNIS 04
Exceções do Firewall no Windows XP 07
Exceções do Firewall no Windows Vista 10
Exceções do Firewall no Windows 7 17
Métodos de Autenticação 24
Cadastro e Posicionamento Adequado do Dedo 24
Usando o Software VIRDI UNIS 27
Monitoração 27
Gerenciamento do Terminal 30
Adicionar um Terminal 31
Configurações da Rede e do Terminal 32
Configurações do Terminal 33
Atribuir Administrador ao Terminal 37
Atualização do Firmware do Terminal 38
Gerenciamento dos Usuários 39
Adicionar um Usuário 40
Procedimento para Cadastro da Digital 42
Mandando Informações dos Usuários para o Terminal 44
Mandando Informações dos Usuários para o Servidor 45
Gerenciamento de Visitantes 46
Adicionar um Visitante 47
Notas 36

Tabela de Revisões

Revisão	Data	Descrição
A.0	26/07/10	Criação deste documento

Guia rápido de utilização do Software VIRDI UNIS

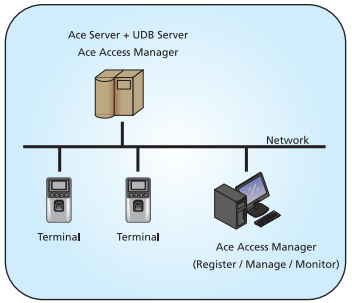
Introdução

UNIS é um programa que gerencia os terminais de biometria / cartão da VIRDI.

Integra e gerencia cada terminal e os usuários através da rede. A monitoração da autenticação dos usuários pode ser feita em tempo real e permite a busca de histórico de autenticações dos usuários.

Esse manual explica como instalar o UNIS, como comunicar com o terminal e cadastrar usuários e visitantes.
Para outras informações veja o manual completo do UNIS.

A figura abaixo mostra a configuração do Sistema.



Instalação do Software VIRDI UNIS

Execute o arquivo 'setup.exe' dentro da pasta Setup.



Clique em "Continuar".



Clique em "Sim".



Selecione o caminho de instalação padrão: C: \ Program Files \ UNIS
Clique em "Continuar".



Server: Instala a versão completa do programa no computador principal (versão servidor)
Client: É instalado as opções mínimas requeridas, para ser instalado em outro computador, somente para gerenciamento do programa.

Selecione a opção desejada e clique em Continuar.

© 2010 Virdi



Favor aguardar até o término da instalação.



Instalação completa.

Nota: Favor verificar as exceções do Firewall após a instalação, caso o Software não conecte com o Leitor.

- Tipo de S.O. do PC: [Windows XP] [Windows Vista] [Windows 7]

Exceções do Firewall no Windows XP

1.Windows Disable Firewall: [Painel de Controle] Firewall do Windows.



Na janela de Alerta de Segurança do Windows, clicar em "Desbloquear".

© 2010 Virdi



Em Painel de Controle, entrar em Firewall do Windows.



Na aba "Geral" desmarcar a opção "Não permitir exceções" e manter selecionado a opção "Ativado".



Guia rápido de utilização do Software VIRDI UNIS

Na aba "Exceções" clicar no botão "Adicionar Programa".



Na janela "Adicionar Programa" que abrir, procurar e selecionar o programa "UNIS Remote Manager". Clicar em "OK".



Selecione o UNIS Remote Manager e clique em OK.

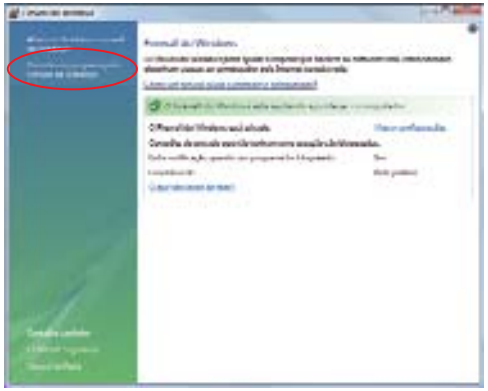
Exceções do Firewall no Windows Vista

1. Programa de Alerta de segurança: Desbloquear
2. Desativar o Firewall do Windows: [Painel de Controle] Firewall do Windows

© 2010 Virdi



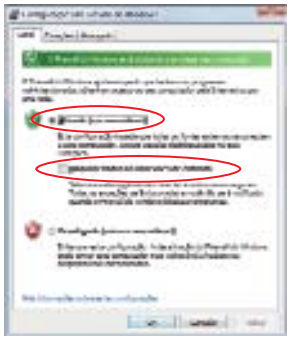
Em Painel de Controle, entrar em Firewall do Windows.



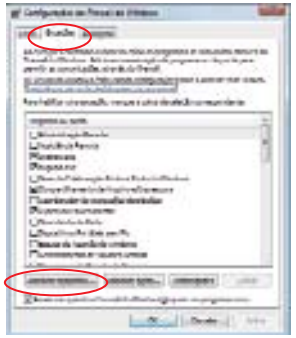
Na janela do Firewall do Windows, clicar em "Allow a program through Windows Firewall".

© 2010 Virdi

Guia rápido de utilização do Software VIRDI UNIS



Na aba "Geral" desmarcar a opção "Não permitir exceções" e manter selecionado a opção "Ativado".

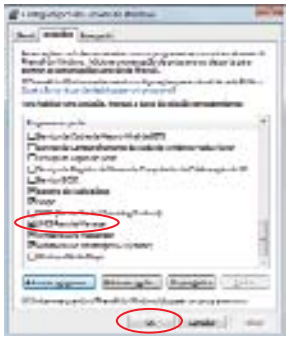


Na aba "Exceções" clicar no botão "Adicionar Programa".



Na janela "Adicionar Programa" que abrir, procurar e selecionar o programa "UNIS Remote Manager". Clicar em "OK".

© 2010 Virdi



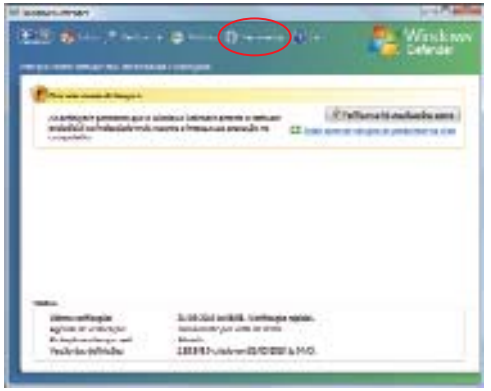
Selecione o UNIS Remote Manager e clique em OK.

3.Desabilitando o Windows Defender: [Painel de Controle] Windows Defender

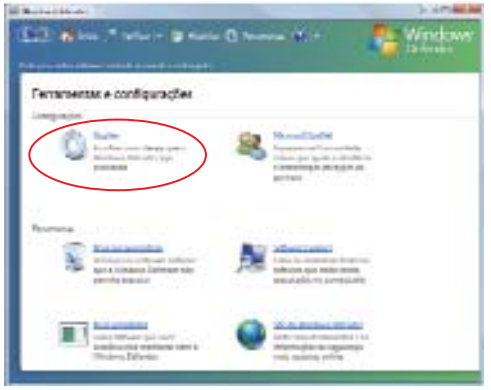


Em Painel de controle, selecione o Windows Defender

© 2010 Virdi

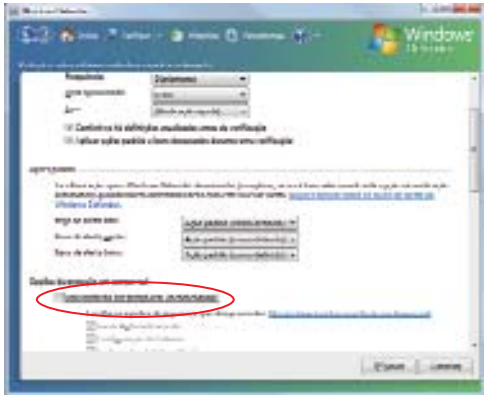


Em Windows Defender, entrar na opção "Ferramentas"



Em seguida, entrar em Opções.

© 2010 Virdi



Na janela em que abrir, desmarcar a opção "Usar proteção em tempo real". E em seguida clicar em Salvar.



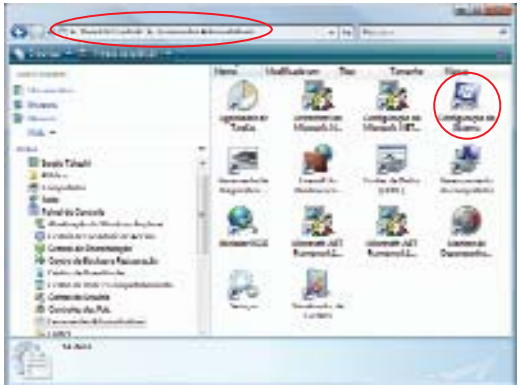
O Windows Defender foi desativado.

4.Desabilitando Controle de Conta de Usuário: Configurações UAC

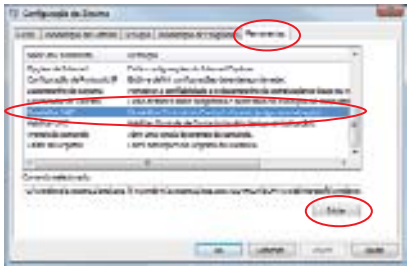


Em Painel de Controle, entrar em "Ferramentas Administrativas."

Guia rápido de utilização do Software VIRDI UNIS

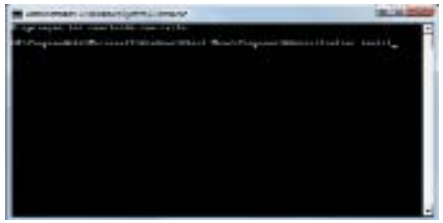


Em Ferramentas Administrativas, entrar em Configuração do Sistema.



Na janela de Configuração do sistema, na aba Ferramentas, selecionar o item "Disabilitar UAC".

Clicar em OK.



© 2010 Virdi

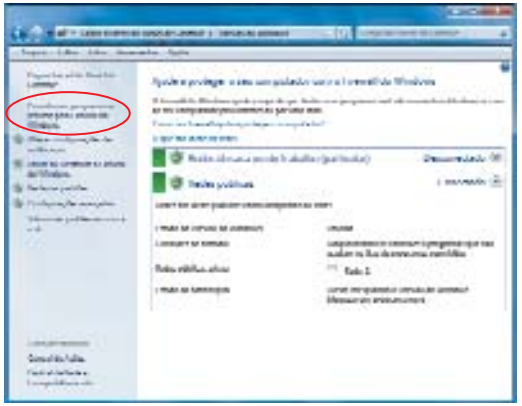
5.Reinicie seu PC em seguida.
6.Caso o software não conecte com o leitor após reiniciar, favor reinstalar o programa.

Exceções do Firewall no Windows 7

1.Desabilitando o Firewall: [Painel de Controle] Firewall do Windows

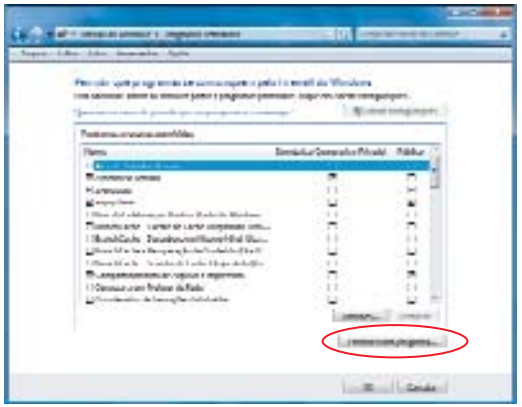


Em Painel de Controle, entre em Firewall do Windows.



© 2010 Virdi

No Firewall do Windows, clicar em "Allow a program or a feature through Windows Firewall".

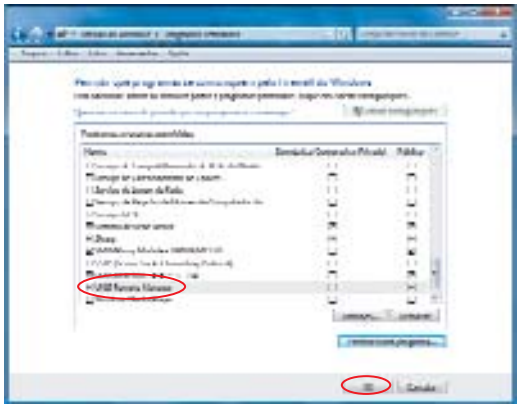


Clicar em "Allow another program".



Na janela "Adicionar Programa" que abrir, procurar e selecionar o programa "UNIS Remote Manager". Clicar em "OK".

© 2010 Virdi



Selecione o UNIS Remote Manager e clique em OK.

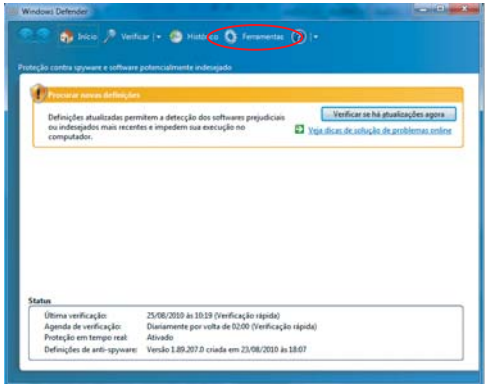
2.Desabilitando o Windows Defender: [Painel de Controle] Windows Defender



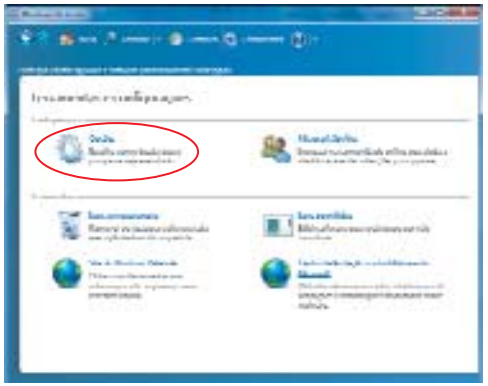
Em Painel de controle, selecione o Windows Defender.

© 2010 Virdi

Guia rápido de utilização do Software VIRDI UNIS

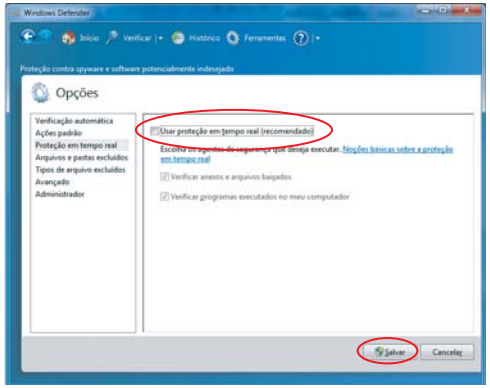


Na Janela do Windows Defender, clicar em "Ferramentas".



Em seguida entrar em Opções.

© 2010 Virdi



Na janela em que abrir, desmarcar a opção "Use real-time protection".



O Windows Defender está desabilitado.

3.Desabilitando User Account Control: UAC settings

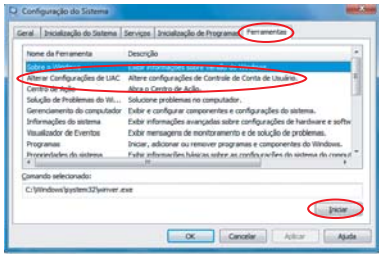


Guia rápido de utilização do Software VIRDI UNIS

Em Painel de Controle entrar em "Ferramentas Administrativas".

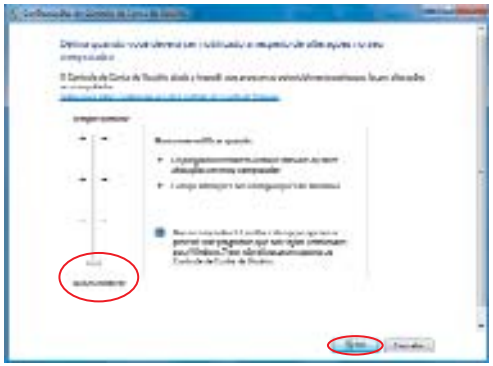


Em ferramentas administrativas, entrar em Configurações do Sistema.



Em Configurações do Sistema, na aba "Ferramentas", entrar em "Change UAC Settings" e clicar em "Launch".

© 2010 Virdi



Na janela que abrir, mudar o cursor para "Never Notify" e clicar em OK.

4. Reinicie o computador em seguida.

5. Caso o software não conecte com o leitor após reiniciar, favor reinstalar o programa.

Métodos de Autenticação

Os seguintes métodos de autenticação são válidos e também a combinação desses métodos também podem ser usadas.

- Autenticação biométrica

Autenticação 1:1
- Refere-se ao método no qual a digital inserida é autenticada após inserir o ID do usuário ou Cartão. O tempo de autenticação é menor.

Autenticação 1:N
- Refere-se ao método no qual a digital inserida é comparada com o banco de dados do terminal, sem que haja uma referência da digital com o ID ou cartão RFID do usuário. Esse método é mais simples comparado com a identificação 1:N, mas o tempo de comparação é maior.

© 2010 Virdi

Autenticação com template no cartão
Após gravar a informação do template no Cartão Mifare, a digital inserida para autenticação é comparada com a digital gravada no cartão para a autenticação.

- Autenticação por senha

A autenticação é feita usando uma senha de 4 a 8 dígitos. Normalmente é usado esse método quando não pode ser usada a biometria.

- Autenticação por cartão RFID

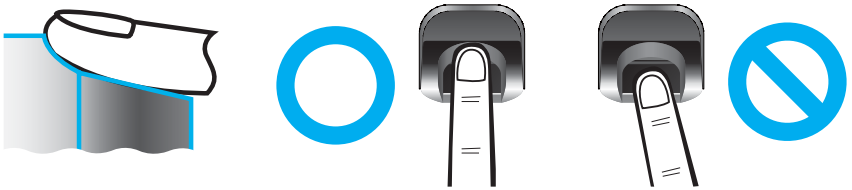
Esse método usa o cartão RFID para autenticação. O cartão deve estar cadastrado no sistema.

Cadastro e Posicionamento Adequado do Dedo

O cadastro da digital é o processo mais importante para usar o dispositivo de reconhecimento biométrico. A digital deve ser cadastrada devidamente para obter sucesso na autenticação.

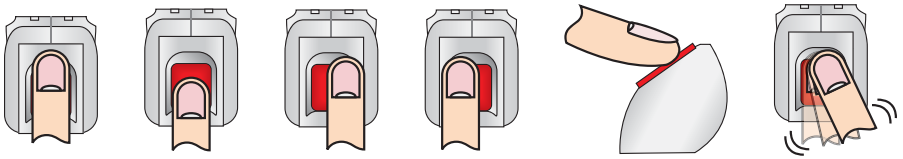
- Posicionamento adequado do dedo
  Se possível, use o dedo indicador e pressione o dedo como se estivesse carimbando sua digital. Somente encostar o dedo no sensor não é suficiente para efetuar o cadastro.
  A forma adequada é encostar e pressionar o centro da digital no sensor biométrico.

  Quando piscar a luz do sensor biométrico, insira a digital.



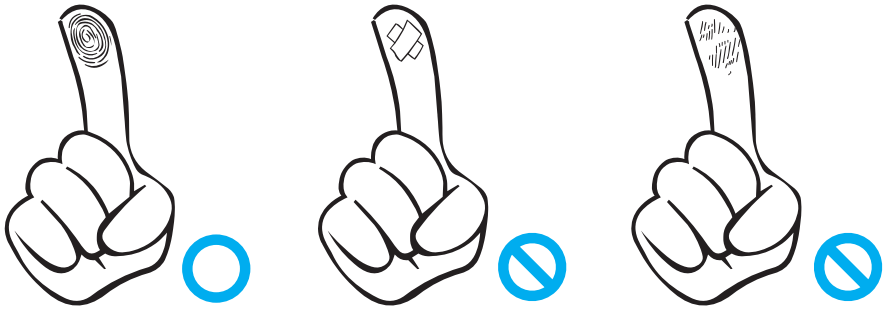
© 2010 Virdi

O dedo não deve encostar somente em um canto do sensor, não encostar somente a ponta do, dedo nem rotacione o dedo durante a leitura da digital.



- Se possível use o dedo indicador.
  Usando o dedo indicador, pode-se obter uma impressão digital mais precisa e estável.

- Verifique se a digital está apagada ou se há cicatriz.
  Dedos muito secos ou molhados, com digital apagada ou com cicatriz são difíceis de serem reconhecidos. Nesses casos, use um dedo diferente para cadastro.



- Condições das digitais dos usuários

  A digital pode não ser reconhecida ou ser inconveniente seu uso, dependendo das suas condições.

  - Esse produto é um sistema de reconhecimento biométrico. Se a digital estiver danificada ou fraca, não pode ser usada. Nesse caso, use cartão RFID.
  - **Se a sua pele estiver muito seca, abafe sobre seu dedo para umedecê-lo.**

© 2010 Virdi

- As digitais de crianças normalmente são muito pequenas ou são um pouco apagadas. É necessário recadastrar a digital a cada 6 meses.
- As digitais de idosos podem ser difíceis de ser cadastradas por possuírem as linhas das digitais muito finas.
- É recomendado o cadastro de pelo menos 2 digitais por pessoa.

Usando o Software VIRDI UNIS

Somente usuários cadastrados como Administradores possuem acesso ao Software VIRDI UNIS.
Como não há nenhum administrador cadastrado logo após a instalação, é necessário fazer o acesso ao Software como Administrador Mestre.
Para entrar no programa, clique duas vezes no ícone do UNIS no desktop.
Quando abrir a tela para fazer Logon, marque a opção Master Admin Logon.

A senha inicial para o Administrador Mestre é '1'.



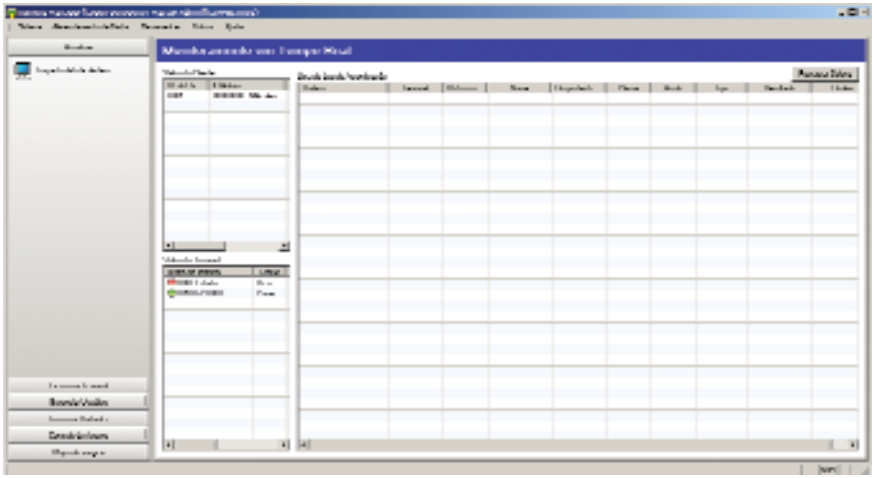
A senha inicial pode ser mudada em "Alterar senha do Master Admin" no Menu "Sistema".

Monitoração

Os eventos de autenticação do usuário pelo Terminal biométrico, as informações de acesso e o estado da conexão do terminal podem ser monitorados em tempo real.

© 2010 Virdi

•Limpar toda a lista de Itens: Todos os eventos de acesso são limpados da tela.



Lista de log de autenticação

Na lista de Acesso são mostrados:

- Horário: mostra a data e horário do acesso
- Terminal ID: ID do terminal que está fazendo a autenticação
- ID do usuário: ID do usuário autenticado
- Nome: Nome do usuário autenticado
- Grupo de Acesso: Grupo de acesso do usuário
- Classe: Usuários e visitantes
- Modo: Modo da autenticação F1, F2, F3, F4.
- Tipo: Tipo da autenticação 1:N, 1:1, biometria, cartão, senha.
- Resultado: Resultado da autenticação: Sucesso ou Falha.
- Tempo gerado: Mostra o tempo da autenticação.

© 2010 Virdi

Guia rápido de utilização do Software VIRDI UNIS

Status do Cliente

Mostra o status da conexão do cliente (UNIS) ao servidor.

- ID do cliente: Mostra o ID do programa cliente conectado ao servidor.
- ID do Admin: ID do Admin que está usando o Programa cliente.
- End. IP: Endereço de IP do computador cliente.
- Versão: Mostra a versão do programa.

Status do Terminal

Mostra o status do terminal

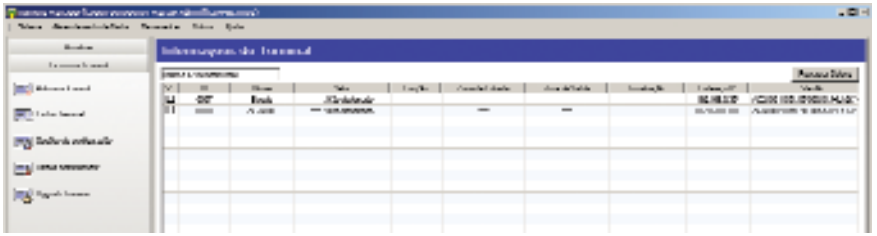
- Nome do Terminal: Mostra o ID e nome do terminal cadastrado.
- Status: Mostra o status da conexão do terminal.
- Conectado: Se o terminal estiver conectado, é mostrado uma lâmpada verde .
- Desconectado: Se o terminal estiver desconectado, é mostrado uma lâmpada vermelha .
- End. de IP: aparece o IP do terminal.
- Versão: Mostra a versão do terminal no formato (firmware) (protocolo) (leitor de cartão).
- Status da conexão do programa cliente e se o estado do terminal pode ser configurado para [Tool] - [Environment Setting] -[Local Environment Setting].

Gerenciamento do Terminal

É possível fazer cadastro / modificação / remoção e configuração para cada terminal.
É necessário fazer o cadastro do terminal no UNIS para ver os status do terminal.

- Adicionar terminal: Selecionar [Adicionar Terminal] no menu [Gerenciar Terminal].
- Modificar terminal: Clicar duas vezes sobre o terminal a ser modificado na janela de lista de terminais.
- Remover terminal: Após marcar o terminal a ser removido na lista dos terminais, selecione [Excluir Terminal].

© 2010 Virdi



- ID: ID do terminal.
- Nome: Nome do terminal.
- Setor: Setor do terminal
- Função: Mostra qual a função do terminal: controle de ponto, controle de refeição ou controle de acesso.
- Anti Pass Back: Mostra se a função anti-pass back está ou não habilitada.
- Zona de Entrada: Mostra o anti pass back da Zona de entrada.
- Zona de Saída: Mostra o anti pass back da Zona de saída.
- Localização: Local onde está instalado o leitor.
- End. de IP: Endereço de IP do terminal.
- Versão: Versão de firmware do terminal.

Adicionar um Terminal



Guia rápido de utilização do Software VIRDI UNIS

Informações básicas:

- ID: Informar o ID do terminal
- Nome: Informar um nome para o terminal.
- Setor: Selecionar um setor. Cadastrar setor em "Gerenciar Cadastro de Empresas - Setor"
- Localização: Local aonde o terminal vai ser instalado.
- Outros: Inserir informações adicionais.
- Data do Registro: data e horário em que foi cadastrado o leitor.

Função:

- T/A: Usar o terminal para controle de ponto.
- Meal: Usar o terminal para controle de refeição.
- Escola: Usar o terminal para gerenciamento de escola.

Anti Pass Back

- Zona de entrada: Colocar o código cadastrado em [Gerenciar Anti Pass Back]
- Zona de saída: Colocar o código cadastrado em [Gerenciar Anti Pass Back]
- Designar Administrador para o terminal: Atribuir um administrador para o terminal.

Mostra uma lista de usuários em "Admin. Não cadastrado" com acesso para Gerenciar terminal e direito de Controle de Acesso em [Gerenciar Administradores].

Após selecionar o usuário a ser designado como administrador, mova o usuário para a Lista "Admin. Cadastrado" clicando no botão .

Configurações da Rede e do Terminal

Atenção: Para que o terminal seja cadastrado corretamente é importante que no Menu do Leitor Biométrico, em configurações de Rede, sejam preenchidos adequadamente os campos:

© 2010 Virdi

- ID do Terminal: Atribuir um ID único para o Leitor Biométrico na rede;
- Endereço de IP: atribuir um Endereço de IP único para o Leitor Biométrico na rede;
- Máscara de Subrede e Gateway;
- IP do Servidor: é o IP do Computador onde está instalado o Software UNIS ao qual o terminal vai estabelecer uma conexão.

Caso o Firewall esteja habilitado, é importante desbloquear a Porta do Servidor, ao qual o Leitor Biométrico vai comunicar com o Computador que está instalado o Software UNIS. Essa porta do Servidor é configurada no Menu do Leitor Biométrico.

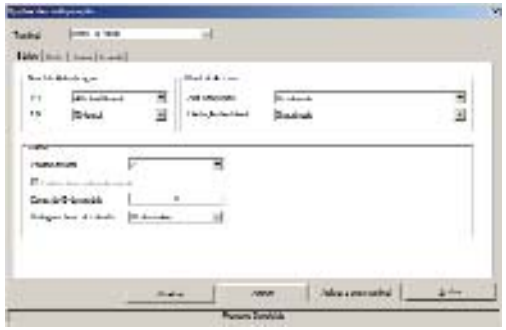
Desbloquear também as portas usadas pelo Computador, para "Servidor de Banco de dados" e "Servidor de Autenticação". Essas portas são configuradas em "Configurações Cliente / Servidor" no Menu "Ferramentas" no Software UNIS.

Configurações do Terminal

Quando o terminal está conectado, é possível modificar as configurações do terminal.

Selecione o terminal desejado na lista de terminais e clique em "Opções de Configuração".

- Básica



© 2010 Virdi

Guia rápido de utilização do Software VIRDI UNIS

Nível de Autenticação

- 1:1: É o nível de segurança para ser usado na autenticação 1:1 no terminal.
- 1:N: É o nível de segurança para ser usado na autenticação 1:N no terminal.

Nível de Acesso

- Anti Pass Back: configurar o anti pass back para o terminal.
  - Sem uso: O anti pass back não está ativado no terminal
  - Acesso permitido quando servidor estiver desconectado: o acesso é permitido para todos os usuários quando houver perda na conexão.
  - Acesso negado quando o servidor estiver desconectado: o acesso é proibido para todos os usuários quando houver perda na conexão.

Restrição de autenticação: tipo de autenticação em dispositivos que são limitados a biometria e senha.

Outros

- Volume do som (0~20): Volume da voz de notificação do terminal.
- Entrar chave automaticamente: após digitar o ID no terminal, pode-se prosseguir com a autenticação sem precisar apertar o botão Enter.
- Comp. do ID do usuário (1~8): Escolha o comprimento do ID do usuário para o terminal.
- Distinguir chave de entrada: Escolher qual o tipo do número a ser digitado na autenticação 1:1: ID do usuário ou ID único. ID do usuário é o número padrão usado no programa e pode conter até 8 dígitos.

© 2010 Virdi

- Rede



- Aquisição automática de IP: O terminal é configurado com IP dinâmico.
- IP em uso:
  - IP do terminal: Mostra o IP fixo do Terminal
  - Másc. Sub Rede: Mostra a Máscara de subrede do terminal.
  - Gateway Padrão: Mostra o Gateway do terminal.
- Servidor de Autenticação
  - Endereço de IP: Mostra o endereço de IP do servidor de autenticação conectado ao terminal.
  - Porta: Mostra a porta do servidor de autenticação para se conectar ao terminal. (Padrão 9870)
- Modo de autenticação: Mostra o modo de autenticação do terminal

  NS: A autenticação é feita primeiramente pelo servidor. Se estiver desconectado devido a algum erro na rede, a autenticação é feita usando a memória do terminal.

  SN: Mesmo com o servidor conectado, primeiro é feito tentativa de autenticação usando a memória do terminal e o resultado é mandado para o servidor em tempo real. Mas se o usuário não estiver cadastrado no terminal, a autenticação é feita pelo do servidor.

  NO: Mesmo que o usuário esteja cadastrado no terminal, a autenticação é feita somente pelo servidor. Se o servidor estiver desconectado, não vai ser possível fazer nenhuma autenticação.
- Modo de Operação: Mostra o modo de operação do terminal: Controle de Ponto ou Controle de refeição.

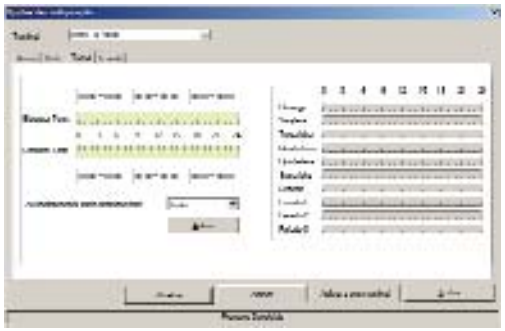
© 2010 Virdi

Guia rápido de utilização do Software VIRDI UNIS

- Texto para imprimir no controle de refeição: Configura o texto a ser impresso na impressora conectado ao terminal.

- Travar

Essa função é usada para configurar o bloqueio e desbloqueio de uma entrada / saída caso o terminal seja usado para entrada / saída.



- Bloquear terminal: Usado para restringir acesso do usuário (autenticação) durante algum horário do dia.
- Desbloquear terminal: Usado para manter o terminal aberto sem a necessidade de restrição de autenticação.

  Configurar o horário selecionado com o mouse o intervalo de tempo na barra de tempo. É possível configurar até 3 intervalos. Os intervalos de Bloqueio e Desbloqueio não podem coincidir. Configurado os intervalos, selecione o dia da semana a receber essa configuração e em seguida clique em Aplicar.

- Feriado

É necessário cadastrar os feriados para bloquear ou desbloquear o terminal. O tipo de Feriado pode ser classificado e atribuído como 1~3.

© 2010 Virdi



1) Selecione o número na lista a ser cadastrado e atribua um tipo de feriado.
2) O tipo de Feriado pode ser classificado e atribuído como 1~3.
3) Selecione a data para ser cadastrada como feriado e aperte [Registrar] para completar.

Podem ser feitos até 100 cadastros de feriado. Duas ou mais datas no mesmo feriado serão designado como tipo de número (Sequencial).

Atribuir administrador ao Terminal



© 2010 Virdi

Pode ser designado um administrador para cada terminal. O administrador do terminal é o usuário que tem acesso ao menu do terminal, podendo modificar as configurações. É necessário fazer a autenticação do administrador para entrar no menu do terminal.

Após selecionar o administrador, selecione o terminal a ser atribuído da lista "Terminal não designado" e aperte o botão para mover para a lista "Terminal designado".

É mostrado uma lista de usuários que possuem direitos de Administrar o Terminal em Gerenciamento de Administradores.

Atualização do Firmware do Terminal

Para fazer atualização do Firmware clique no botão , procure o arquivo e depois clique em "Abrir".
Na Janela seguinte, selecione o Terminal a ser feito o upgrade, e clique em "Enviar".

- Atenção ao atualizar o Firmware. Não opere o terminal durante a atualização do Firmware se não pode parar de funcionar.

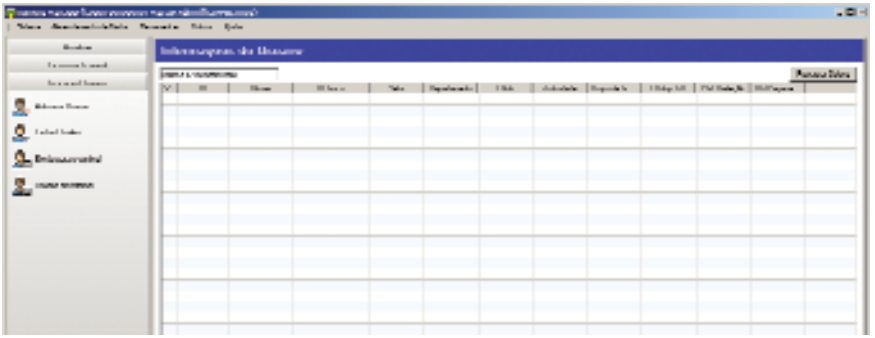


© 2010 Virdi

Gerenciamento dos Usuários

Mostra a lista de usuários cadastrados no Software VIRDI UNIS.

- Adicionar usuário: Selecione "Adicionar usuários" em "Gerenciar usuários"
- Modificar usuário: Dê um duplo clique sobre o usuário que está na lista de usuário.
- Excluir Usuário: Selecione um usuário da lista a ser apagado, e clique em "Excluir usuário".



- ID: Mostra o ID do usuário
- Nome: Nome do usuário
- ID único: ID único do usuário
- Setor: Setor do usuário
- Departamento: Departamento do usuário
- Título: Título do usuário na empresa
- Autoridade: Autoridade de administração do usuário
- Grupo de Acesso: Grupo de controle de acesso do usuário
- Código T/A: Código de Controle de Acesso do usuário
- Código de Refeição: Código de Refeição do usuário
- Código de Pagamento: Código de pagamento do usuário

© 2010 Virdi

Guia rápido de utilização do Software VIRDI UNIS

Adicionar um Usuário



Informações Básicas

- ID: Digitar o ID para o usuário (Máx 8 dígitos)
- Nome: Digitar o nome do usuário
- ID único: ID único do usuário
- Setor: Informe qual o Setor do usuário. Cadastrar setor em "Gerenciar Cadastro de Empresa - Setor".
- Departamento: Informe o departamento do usuário. Cadastrar departamento em "Gerenciar Cadastro de Empresa - Departamento".
- Título: Informar o título do usuário na empresa. Cadastrar Título em "Gerenciar Cadastro de Empresa - Título"
- Autoridade: Informar a autoridade de administração do usuário. Configurar administradores em "Gerenciar Administradores".
- Grupo de Acesso: Informar o grupo de controle de acesso do usuário
- Código T/A: Informar o código de Controle de Acesso do usuário
- Código de Refeição: Informar o código de Refeição do usuário
- Código de Pagamento: Informar o código de pagamento do usuário
- Telefone: Informe o telefone
- E-mail: Informe o e-mail

© 2010 Virdi

- Endereço: Informe o endereço
- Outros: Outras informações
- Data do registro: A data e hora do cadastro do usuário são preenchidas automaticamente.
- Localização: Para gerenciamento de anti-pass back de uma área.
- Mensagem: Marcar o Checkbox. Mostra uma mensagem quando o usuário fizer autenticação.

Faixa da Data de Acesso:

- Sem período de restrição: O usuário pode acessar o terminal a qualquer horário
- Período permitido: Período de acesso permitido ao usuário
- Período restringido: Período que o usuário não pode acessar o terminal. (O acesso é negado, caso seja informado algum dado inválido de período)

Tipos de Autenticações:

- FP: Autenticação biométrica
- FP-Card: Autenticação com Template no Cartão
- PWD: Autenticação por senha
- CARD: Autenticação por cartão
- CARD OR FP: Autenticação por Cartão ou Biometria
- CARD AND FP: Autenticação por Cartão e Biometria
- CARD OR PWD: Autenticação por Cartão ou Senha
- CARD AND PWD: Autenticação por Cartão e Senha
- (ID OR CARD) AND FP: Autenticação por ID ou Cartão, e biometria
- (ID OR CARD) AND PWD: Autenticação por ID ou Cartão, e senha
- FP AND PWD: Autenticação por Biometria e Senha
- FP OR PWD: Autenticação por Biometria ou Senha
- CARD AND PWD AND FP: Autenticação por Cartão e Senha e Biometria

Informações da Digital:

Aperte o botão "Cadastrar" para cadastrar a impressão digital. Veja o item "Procedimentos para Cadastro da Digital", para maiores informações de cadastro da digital.

© 2010 Virdi

Guia rápido de utilização do Software VIRDI UNIS

- Permissão para autenticação 1:N: A autenticação é feita somente por biometria sem a necessidade de digitar o ID do usuário.

Informações de Senha:

Digite uma senha para ser usada na autenticação.

Informações do Cartão:

Aperte o botão "Lendo" e aproxime o cartão do Leitor FOH02RF/SC com leitor RFID. Quando aparecer o ID do cartão, pressione o botão "Adicionar" para cadastrar o Cartão.

Informação da Foto:

Para cadastrar uma foto de um arquivo existente no computador, aperte o botão "Adicionar" (Tamanho recomendável 320 x 240) A foto pode conter até 7 Kbytes. Para capturar a imagem da Webcam conectada ao computador em tempo real, clique no botão "Capturar Imagem".

Procedimento para cadastro da digital

As figuras seguintes mostram o procedimento para cadastro da impressão digital usando o Leitor Biosmart com o UNIS. Para cadastro de usuário veja o item "Cadastro de usuário".





© 2010 Virdi

1.Tela inicial do programa de cadastro. Para não mostrar essa tela novamente, clicar no checkbox. Clique em Next.
2.Selecione o dedo a ser cadastrado. Clique em Next.





3.Coloque o dedo no sensor biométrico.
4.Aguarde e remova o dedo do sensor.





5.Coloque o dedo no sensor novamente.
6.Se o cadastro for feito corretamente, é mostrado "OK"!





Guia rápido de utilização do Software VIRDI UNIS

7.Os dedos cadastrados estão com um círculo verde em cima. Clique em Next para terminar o processo de cadastramento.
8.Cadastro completo. Clique em "Finish" para terminar.

Mandando Informações dos Usuários para o Terminal

Pode-se mandar o cadastro de um usuário selecionado na lista, para o Terminal. Ao mandar um usuário, somente os usuários autorizados para autenticação são mandados para o terminal selecionado. Quando o usuário selecionado não tiver autorização para autenticação, ele vai ser automaticamente removido e não vai ser mandado. Quando o usuário é removido, aparece a quantidade no status "Skip" na lista dos terminais.



Selecione os usuários a serem enviados para um Terminal, clique em "Enviar para Terminal".
Na janela "Enviar informações do Usuário", marque o Terminal desejado. E Clique em "Enviar".
Para os usuários que não possuem **Direito de Acesso**, eles não são mandados para o terminal. E são pulados na lista.
Visitantes não são mandados para o Terminal. (Veja: "Adicionando Visitantes").

© 2010 Virdi

Mandando Informações dos Usuários para o Servidor

Os usuários cadastrados no terminal podem ser visualizados ou enviados para o servidor, porém esses usuários não possuem nome. Caso o usuário já esteja cadastrado no servidor, não é possível enviá-lo para o servidor.




Atualiza a informação do usuário que está armazenada no terminal.


Apaga o usuário que está no terminal.


Carrega o usuário para o servidor.

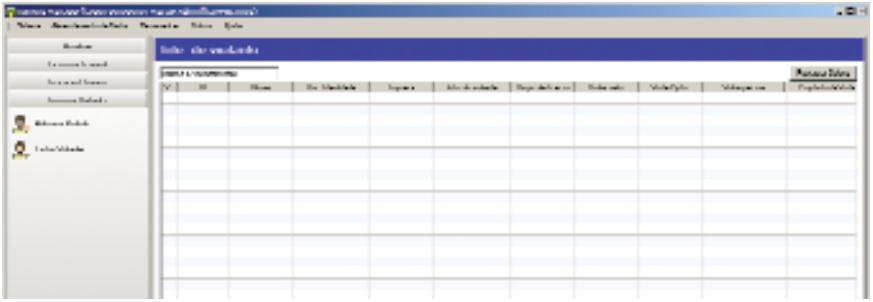
Gerenciamento de Visitantes

Aparece uma lista de visitantes cadastrados.

- Adicionar Visitante: Selecione [Adicionar Visitante] em [Gerenciar Visitante]. O ID do Visitante é diferenciado o ID os usuário e pode ser configurado no menu [Opção do Servidor].
- Apagar Visitante: Após selecionar o visitante a ser removido, selecione [Excluir Visitante]

© 2010 Virdi

Guia rápido de utilização do Software VIRDI UNIS



- ID: ID do visitante.
- Nome: Nome do visitante
- Doc. Identidade: Documento de identidade do visitante.
- Empresa: Empresa do visitante
- Info. do visitante: Outras informações
- Grupo de acesso: Grupo de acesso do visitante
- Visitar setor: Setor visitado
- Visitar departamento: Departamento visitado.
- Visitar pessoa: Pessoa responsável pelo visitante
- Propósito da visita: Propósito do visitante.

Adicionar um Visitante



© 2010 Virdi

Informações Básicas

- ID: Informar ID único para o visitante
- Nome: Informar nome do visitante.
- Doc. Identidade: Informar documento de Identidade do visitante.
- Empresa: Informar a empresa do visitante.
- Informação do visitante: Informação sobre o visitante.
- Telefone: Telefone do visitante.
- E-mail: Endereço de e-mail do visitante.
- Endereço: Informar endereço.
- Outros: Outras informações
- Data do Registro: A data e hora do cadastro do visitante são preenchidas automaticamente.
- Localização: Informação de acesso do visitante.

Informações do Visitante

- Visitar setor: Informar o setor a ser visitado. Cadastrar o setor em "Gerenciar Cadastros de Empresa - Setor"
- Visitar Departamento: Informar o departamento a ser visitado. Cadastrar departamentos em "Gerenciar Cadastros da Empresa - Departamento".
- Visitar pessoa: Informar a pessoa a ser visitada.
- Propósito da visita: Informar o propósito da visita.
- Grupo de Acesso: Informar o grupo de acesso. Cadastrar os grupos em "Adicionar Grupo de Acesso".
- Período da Visita: Informar o período que o visitante tem acesso permitido.

Tipos de Autenticações:

- FP: Autenticação biométrica
- FP-Card: Autenticação com Template no Cartão
- PWD: Autenticação por senha
- CARD: Autenticação por cartão
- CARD OR FP: Autenticação por Cartão ou Biometria
- CARD AND FP: Autenticação por Cartão e Biometria

© 2010 Virdi

Guia rápido de utilização do Software VIRDI UNIS

- CARD OR PWD: Autenticação por Cartão ou Senha
- CARD AND PWD: Autenticação por Cartão e Senha
- (ID OR CARD) AND FP: Autenticação por ID ou Cartão, e biometria
- (ID OR CARD) AND PWD: Autenticação por ID ou Cartão, e senha
- FP AND PWD: Autenticação por Biometria e Senha
- FP OR PWD: Autenticação por Biometria ou Senha
- CARD AND PWD AND FP: Autenticação por Cartão e Senha e Biometria

Informações da Digital:

Aperte o botão "Cadastrar" para cadastrar a impressão digital. Veja os procedimentos para "Cadastro da Digital", para maiores informações de cadastro da digital.

- Permissão para autenticação 1:N: A autenticação é feita somente por biometria sem a necessidade de digitar o ID do usuário.

Informações de Senha:

Digite uma senha para ser usada na autenticação.

Informações do Cartão:

Aperte o botão "Lendo" e aproxime o cartão do Leitor FOH02RF/SC com leitor RFID.
Quando aparecer o ID do cartão, pressione o botão "Adicionar" para cadastrar o Cartão.

Informação da Foto:

Para cadastrar uma foto de um arquivo existente no computador, aperte o botão "Adicionar" (Tamanho recomendável 320x240) A foto pode conter até 7Kbytes.

Para capturar a imagem da Webcam conectada ao computador em tempo real, clique no botão "Capturar Imagem".

© 2010 Virdi