Riversoft
Integração e Inovação

STCP OFTP Client
versão 3.0.0

STCP OFTP Client

Riversoft
Integração e Inovação

STCP OFTP CLIENT
VERSÃO 3.0.0

Manual do Usuário
rev-1.1

Riversoft Integração e Desenvolvimento de Software Ltda.
Av. Dr. Delfim Moreira, 356/Sala 103 – Centro – Santa Rita do Sapucaí – MG – CEP 37540-000
Tel./Fax: 35 3471-0282
E-mail: riversoft@riversoft.com.br
Suporte: suporte@riversoft.com.br
Web: www.riversoft.com.br

Índice

ÍNDICE ---------- **2**

1) INTRODUÇÃO ---------- **3**

O QUE É O STCP OFTP? ---------- 3
O PROTOCOLO OFTP (ODETTE FILE TRANSFER PROTOCOL) ---------- 3
ONDE USAR O STCP OFTP? ---------- 4
QUAIS AS VANTAGENS? ---------- 4
CARACTERÍSTICAS? ---------- 4
REQUISITOS DE SOFTWARE E HARDWARE ---------- 5
ESTRUTURA DOS DIRETÓRIOS ---------- 5

2) INSTALAÇÃO ---------- **6**

COMO INSTALAR O STCP OFTP CLIENT? ---------- 6

3) CONFIGURAÇÃO ---------- **13**

COMO CONFIGURAR O STCP OFTP CLIENT? ---------- 13

4) UTILIZAÇÃO ---------- **47**

COMO UTILIZAR O STCP OFTP? ---------- 47
COMO EXECUTAR O STCP OFTP ATRAVÉS DA LINHA DE COMANDO? ---------- 48
TABELAS COM OS CÓDIGOS DE ERRO DO STCP OFTP ---------- 49

5) SEGURANÇA ---------- **70**

COMO É A SEGURANÇA DO STCP OFTP? ---------- 70
AUTENTICAÇÃO DO USUÁRIO PELA APLICAÇÃO (ODETTE ID)? ---------- 70
CRIPTOGRAFIA? ---------- 70
MESSAGE DIGESTS (SUMÁRIO DA MENSAGEM)? ---------- 70
ASSINATURA DIGITAL? ---------- 71
CERTIFICADO? ---------- 71
AUTORIDADE CERTIFICADORA (CA)? ---------- 71
SECURE SOCKET LAYER (SSL)? ---------- 71
CRIPTOGRAFIA NO STCP OFTP? ---------- 72
A CRIPTOGRAFIA NATIVA? ---------- 72
A CRIPTOGRAFIA SSL3 NO STCP OFTP? ---------- 73
ARQUITETURA DE COMUNICAÇÃO DO STCP OFTP ---------- 73
PORQUE A IMPLEMENTAÇÃO OPENSSL? ---------- 77
LICENÇA OPENSSL ---------- 77
REFERÊNCIAS ---------- 80

1) Introdução

O que é o STCP OFTP?

O STCP OFTP Client é um cliente de transferência de arquivos seguro e multiprotocolo para aplicações de e-business e troca de informações corporativas. Baseado na especificação OFTP (ODETTE File Transfer Protocol).

O Protocolo OFTP (ODETTE File Transfer Protocol)

Este protocolo foi especificado pelo Grupo de Trabalho 4 da Organização **ODETTE** (**O**rganisation for **D**ata **E**xchange by **T**ele **T**ransmission in **E**urope) nos anos 80, para atender a indústria automotiva européia e padronizar a forma de comunicação entre as diferentes empresas da cadeia produtiva (supply-chain) do setor.

O **OFTP** foi primeiramente especificado com as premissas do modelo de interconexão de sistemas abertos (**OSI**) utilizando o serviço de rede recomendado pela norma **CCITT X.25**.

Com o crescimento da utilização do **OFTP** por diferentes setores (bancos, comércio, governo e etc.) e em diferentes plataformas (mainframes, mini e microcomputadores) a organização **ODETTE** ampliou o escopo da padronização e incorporou a utilização do protocolo TCP/IP.

A RFC (Request for Comments) 2204 orienta a utilização do **OFTP** em redes TCP/IP.

Onde usar o STCP OFTP?

O STCP OFTP pode ser utilizado por diferentes aplicações para:

- Integração com parceiros para transferência de informações.
- Integração de sistemas através de transferência de arquivos.
- Integração com bancos para transferência de cobrança, pagamento, extratos e outros.
- Integração com montadoras para transferência de ordens de embarque e produção.
- Integração com associações comerciais para transferência de lista negra.
- Integração com atacadistas para transferência de pedidos de compras.
- Integração com VANS (Embratel, Proceda, Interchange e outras).
- Outras aplicações

Quais as vantagens?

O STCP OFTP oferece as seguintes vantagens:

- Facilidade de integração com as aplicações existentes.
- Automatização do processo de envio/recepção de arquivos.
- Execução através de linha de comando ou agendamento.
- Aumento da segurança no transporte dos arquivos
- Compatibilidade com outros produtos que seguem a especificação OFTP (RFC2204).

Características?

O STCP OFTP oferece as seguintes características:

- Protocolo de transferência OFTP (ODETTE File Transfer Protocol).
- Autenticação através do protocolo OFTP.
- Autenticação através de certificado digital X.509 (SSL3).
- Criptografia RSA, 3DES,. DES, AES (SSL3).
- Multiprotocolo de comunicação TCP, SSL3, X.25, PAD e Discado.
- Transferência de todos os tipos de arquivos.
- Registros de logs de auditoria (bilhetagem) e eventos.
- Recuperação de transferência interrompida.
- Comunicação através de Proxy HTTP, SOCKS4 ou SOCKS5.
- Compressão padrão OFTP ou GZIP
- Versões Windows 95/98/NT/2000/XP/Pocket PC/ActiveX.

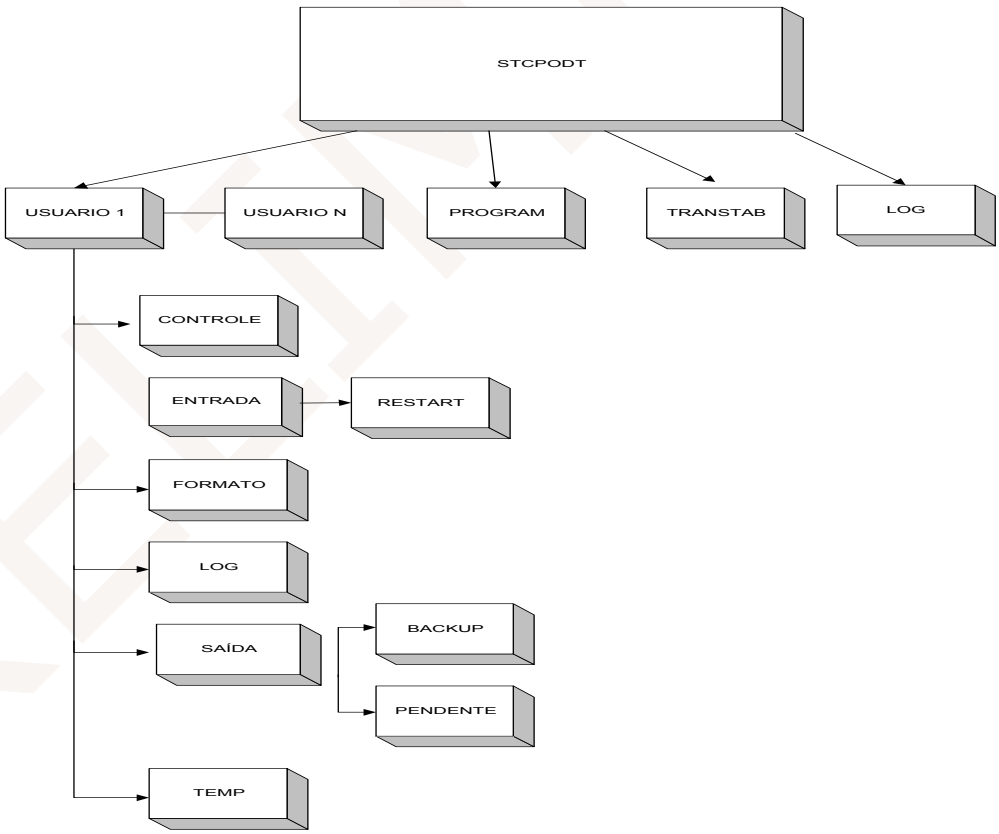
Requisitos de software e hardware

O STCP OFTP necessita dos seguintes requisitos de software e hardware para a sua instalação:

- Microcomputador 486 ou superior
- Memória de 64 Mbytes ou superior
- Espaço no disco rígido de 10 Mbytes
- Drive de CD-ROM
- Sistema operacional Windows 95/98/Me/NT 4.0/2000/2003/XP
- Net Open Wan Connect X.25 (opcional)

Estrutura dos diretórios

O STCP OFTP após a sua instalação e configuração irá criar a seguinte árvore de diretório, onde serão armazenadas as informações de configuração e os subdiretórios de cada perfil configurado para o envio e recebimento dos arquivos:

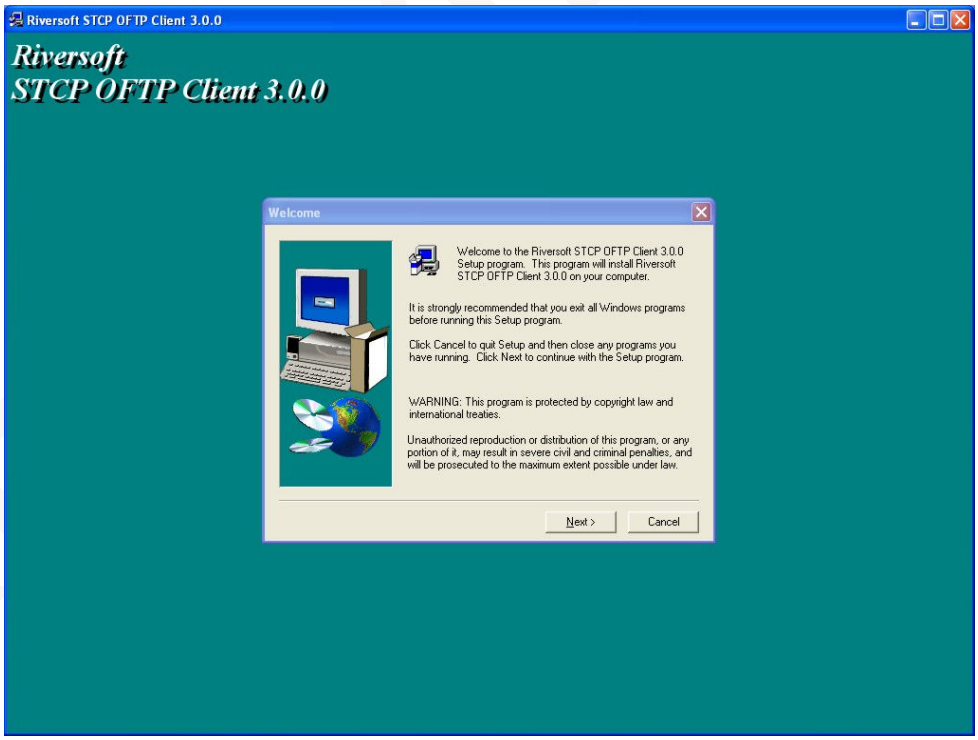


2) Instalação

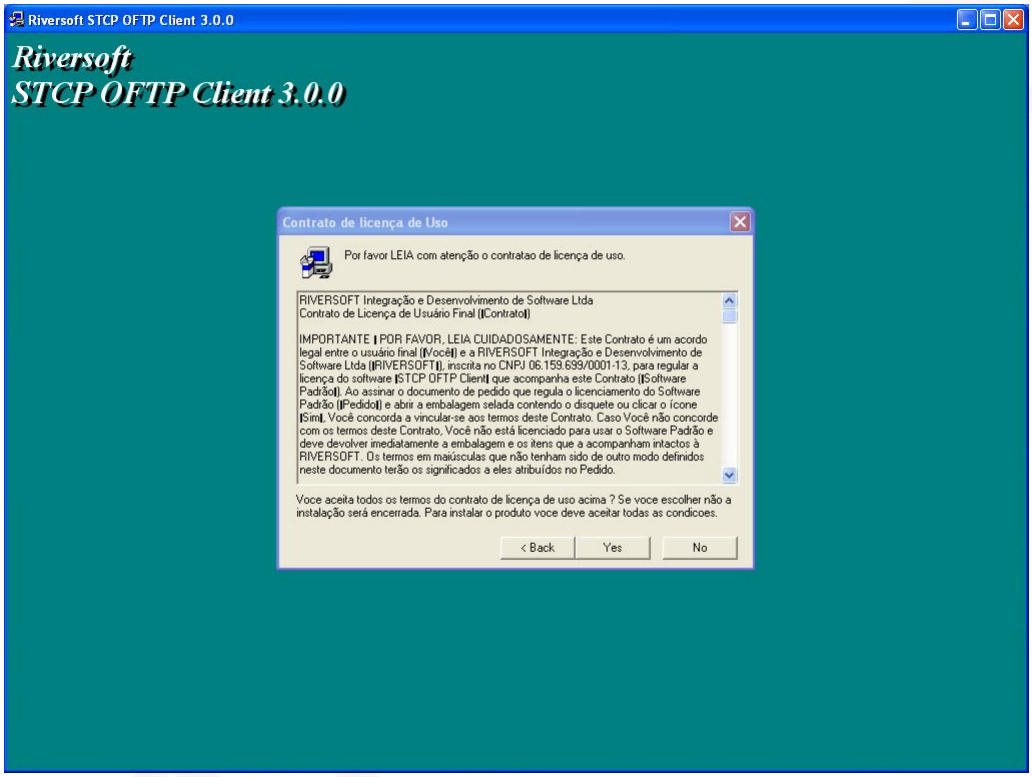
Como instalar o STCP OFTP Client?

O STCP OFTP Client é distribuído através de uma mídia CD-ROM, onde encontra-se o programa SETUP.EXE, os seguintes passos devem ser executados para iniciar o processo de instalação:

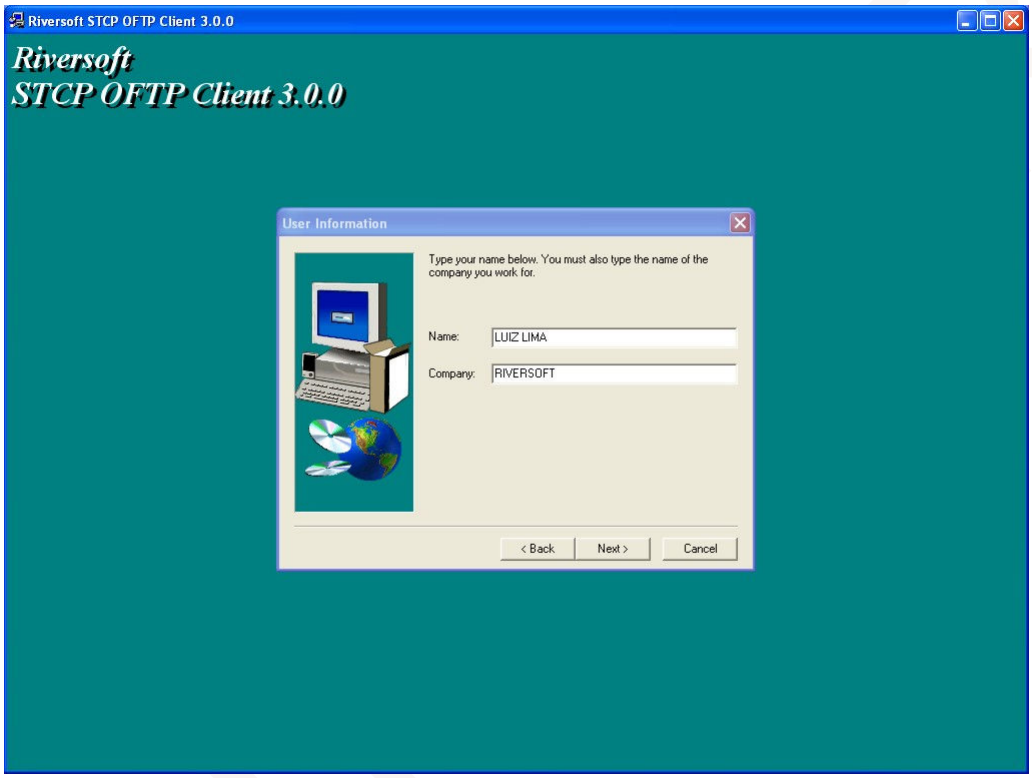
1. Insira o CD na unidade de leitura
2. No cardápio ***Iniciar*** escolha a opção ***Executar.***
3. Utilize o botão **[Procurar]**, e selecione a unidade de leitura do CD.
4. Encontre e selecione o programa **SETUP.EXE**.
5. Agora execute o programa com o botão **[OK].**
6. A tela do inicio do processo de instalação será apresentada.
7. Esta é a tela de boas-vindas, caso você deseje continuar, pressione o botão **[Next]** ou pressione o botão **[Cancel]** para interromper a instalação.



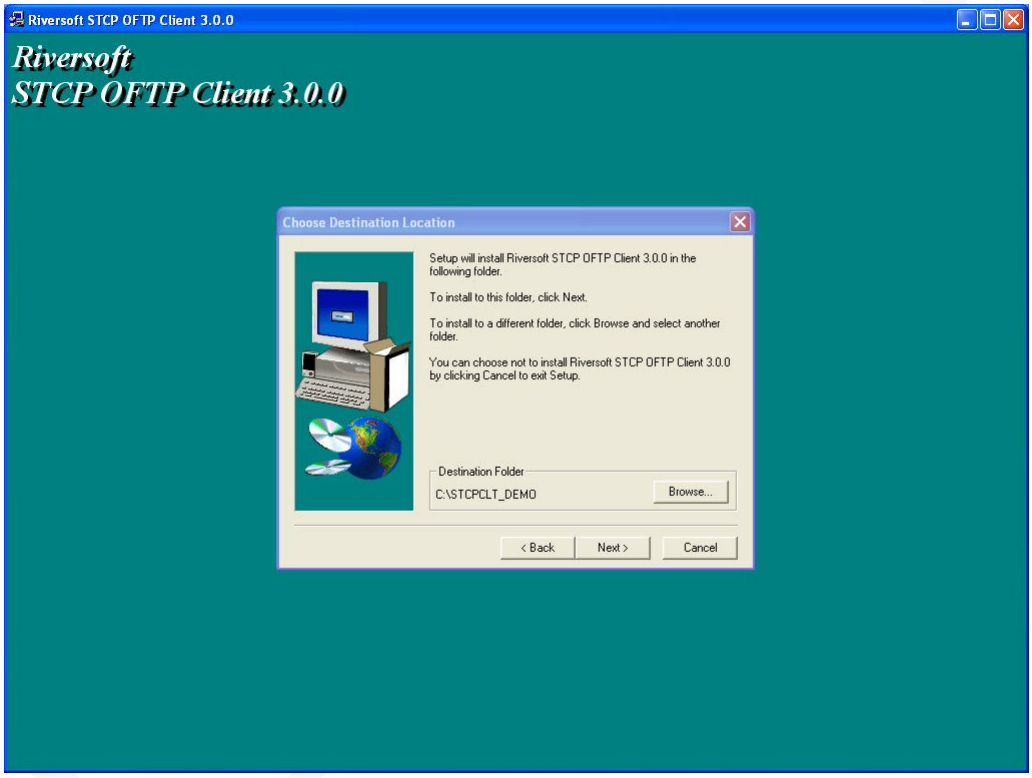
8. Nesta tela você deve cuidadosamente ler o Contrato de Licença de Uso do Usuário Final e caso concorde com os termos propostos pressionar o botão **[Yes]** para continuar com a instalação.



9. A tela ***User Information*** é exibida, conforme mostra a figura abaixo, você deve informar o nome do usuário e empresa; pressione **[Next]** para continuar, **[Back]** para retornar à tela anterior ou **[Cancel]** para cancelar todo o processo de instalação.

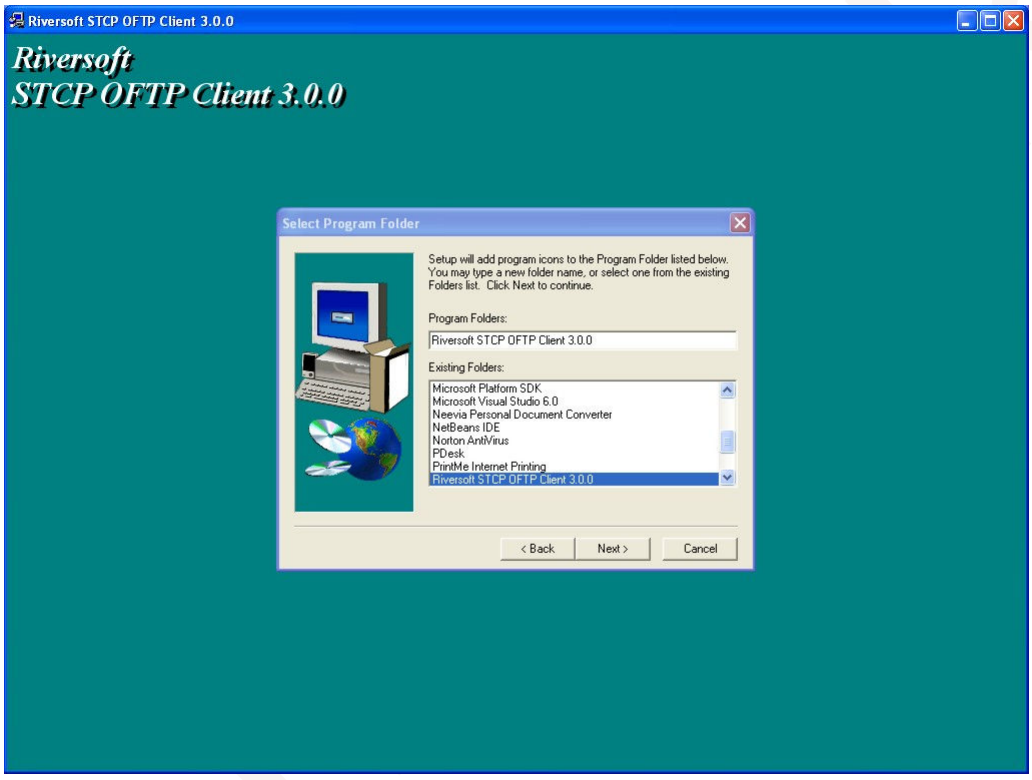


10. A tela ***Choose Destination Location*** será exibida, conforme mostra figura abaixo. Caso você não queira instalar no diretório padrão, então clique em **[Browse]** para selecionar outro diretório ou crie um novo e clique **[OK]**; pressione **[Next]** para continuar, **[Back]** para retornar à tela anterior ou **[Cancel]** para cancelar todo o processo de instalação.

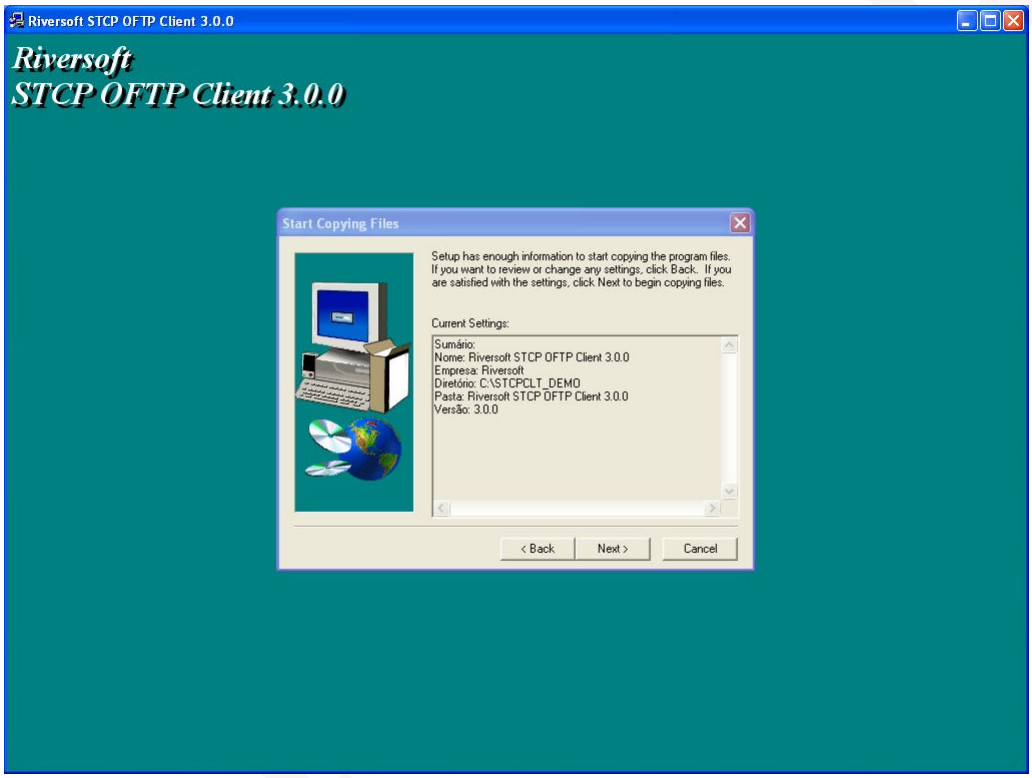


Você pode selecionar outro diretório para instalação do produto ou criar um novo

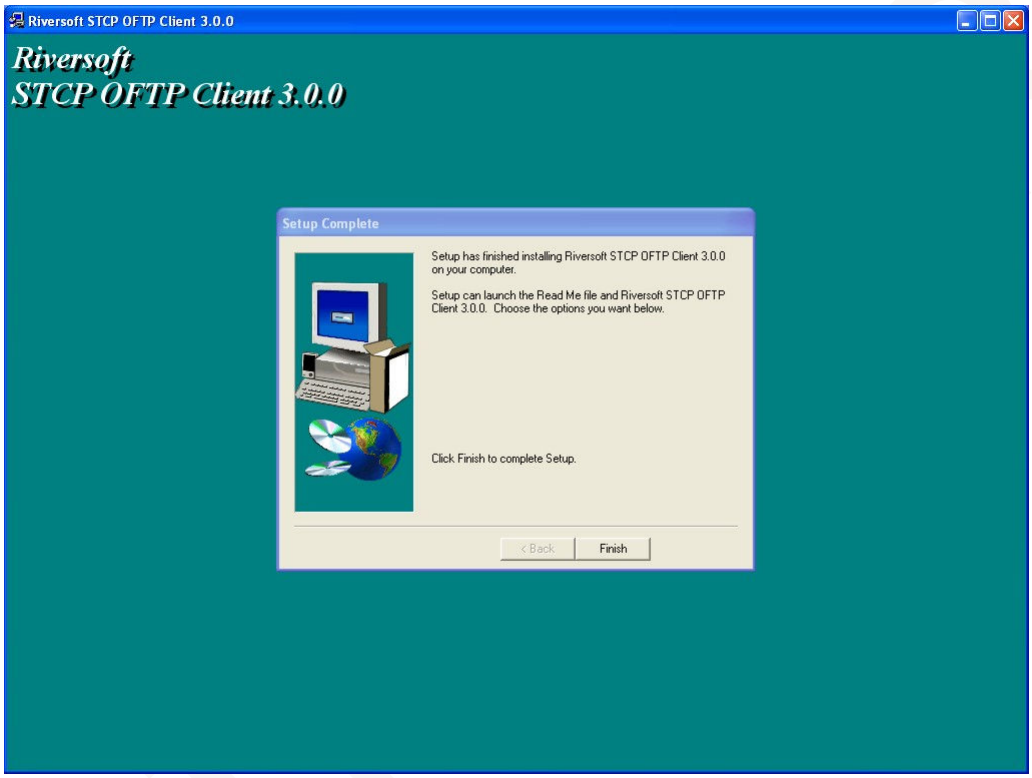
11. A tela ***Select Program Folder*** é exibida, conforme mostra figura abaixo, escolha o grupo de programa no qual deseja instalar o produto, crie um novo ou aceite o padrão, pressione **[Next]** para continuar, **[Back]** para retornar à tela anterior ou **[Cancel]** para cancelar todo o processo de instalação.



12. A tela ***Start Copying File*** é exibida, conforme mostra figura abaixo. Neste momento verifique se as configurações escolhidas estão corretas, pressione **[Next]** para continuar, **[Back]** para retornar à tela anterior ou **[Cancel]** para cancelar todo o processo de instalação.



13. A tela ***Setup Complete*** é exibida, conforme mostra figura abaixo. Pressione **[Finish]** para terminar a instalação do produto.

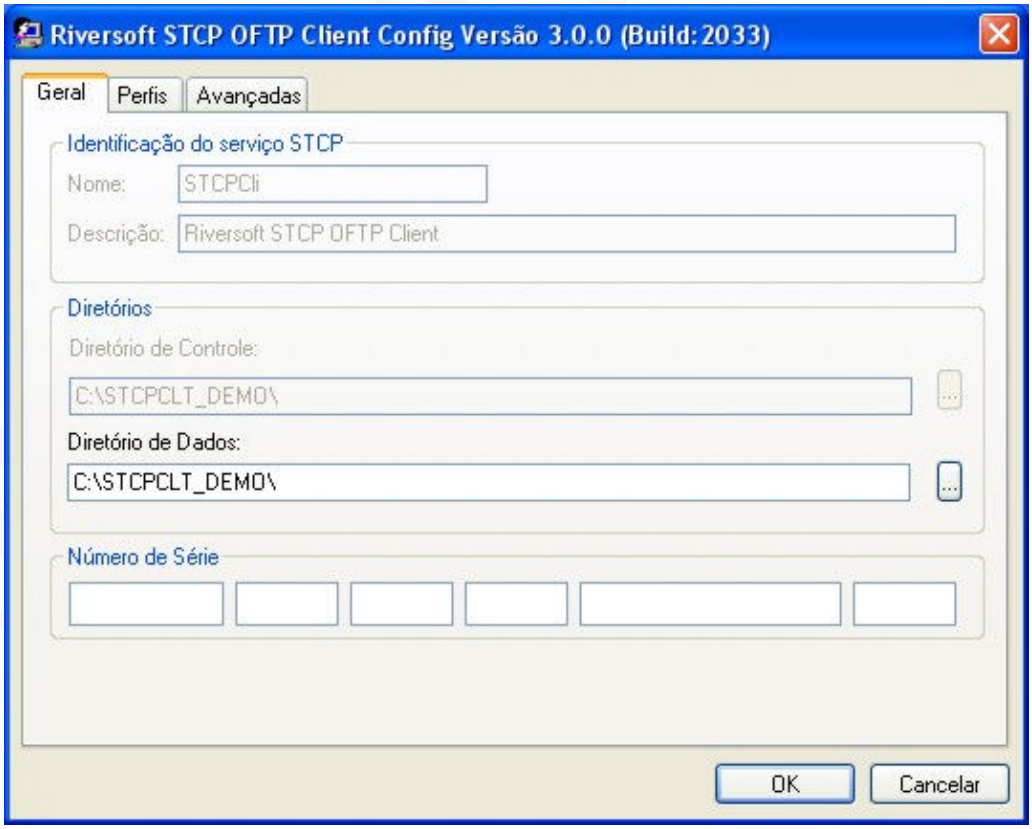


3) Configuração

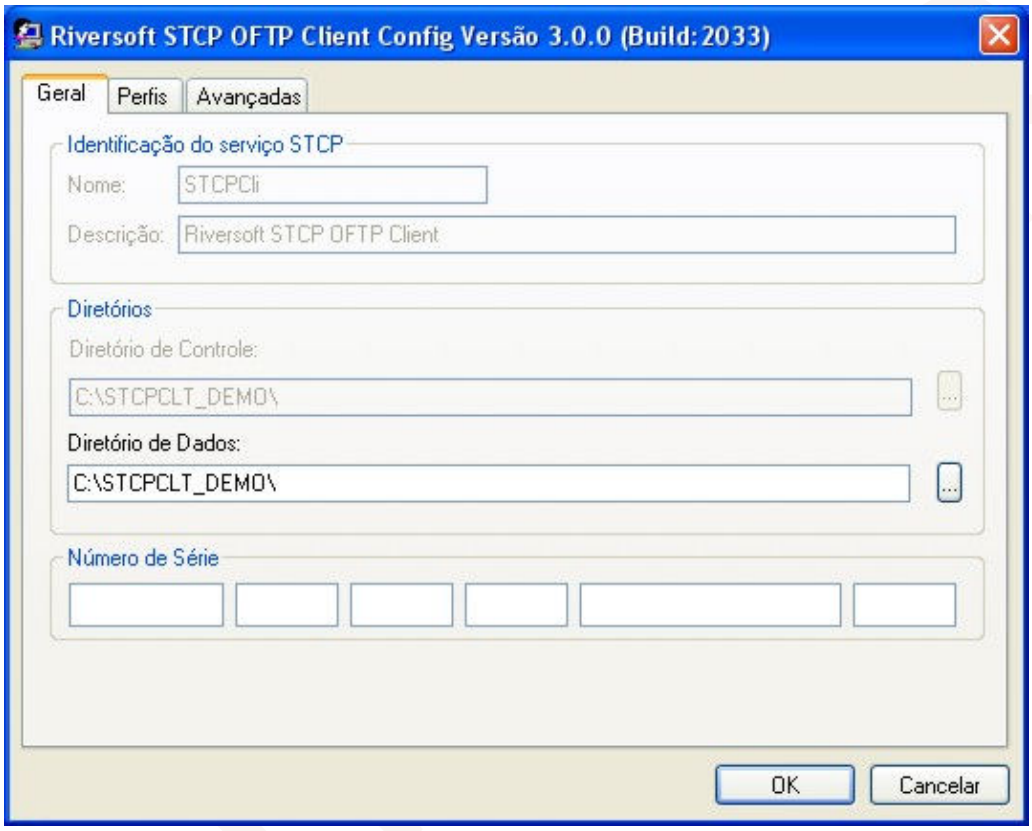
Como configurar o STCP OFTP Client?

O Programa de configuração do STCP OFTP Client foi instalado na pasta selecionada durante o processo de instalação e pode ser acessado através do menu ***Iniciar***. Caso você não tenha alterado a pasta padrão execute os seguintes passos:

1. No cardápio ***Iniciar*** escolha a opção ***Executar.***
2. Selecione T***odos os Programas***.
3. Selecione ***Riversoft STCP OFTP Client 3.0.0***.
4. Click no programa ***Riversoft STCP OFTP Client Configurador***.
5. A tela de configuração inicial é exibida, conforme figura abaixo:



6. A tela de configuração da guia **Geral** é exibida, conforme mostra a figura abaixo:



Nesta tela você irá visualizar as configurações e/ou modificar o subdiretório onde serão criados os perfis de comunicação.

Descrição dos campos para configuração

Nome

Este campo informa o nome do serviço do STCP OFTP.

Obs.: Para a versão STCP OFTP Client este parâmetro não pode ser modificado.

Descrição

Este campo informa a descrição do serviço do STCP OFTP.

Obs.: Para a versão STCP OFTP Client este parâmetro não pode ser modificado.

Diretório de Controle

Este campo informa o nome do diretório de instalação do STCP OFTP, onde serão armazenadas as configurações dos perfis, logs e arquivos de depuração da comunicação.

Obs.: Para a versão STCP OFTP Client este parâmetro não pode ser modificado.

Diretório de Dados

Preencha este campo com o diretório onde a estrutura de subdiretórios para envio e recepção dos arquivos de cada perfil será criada.

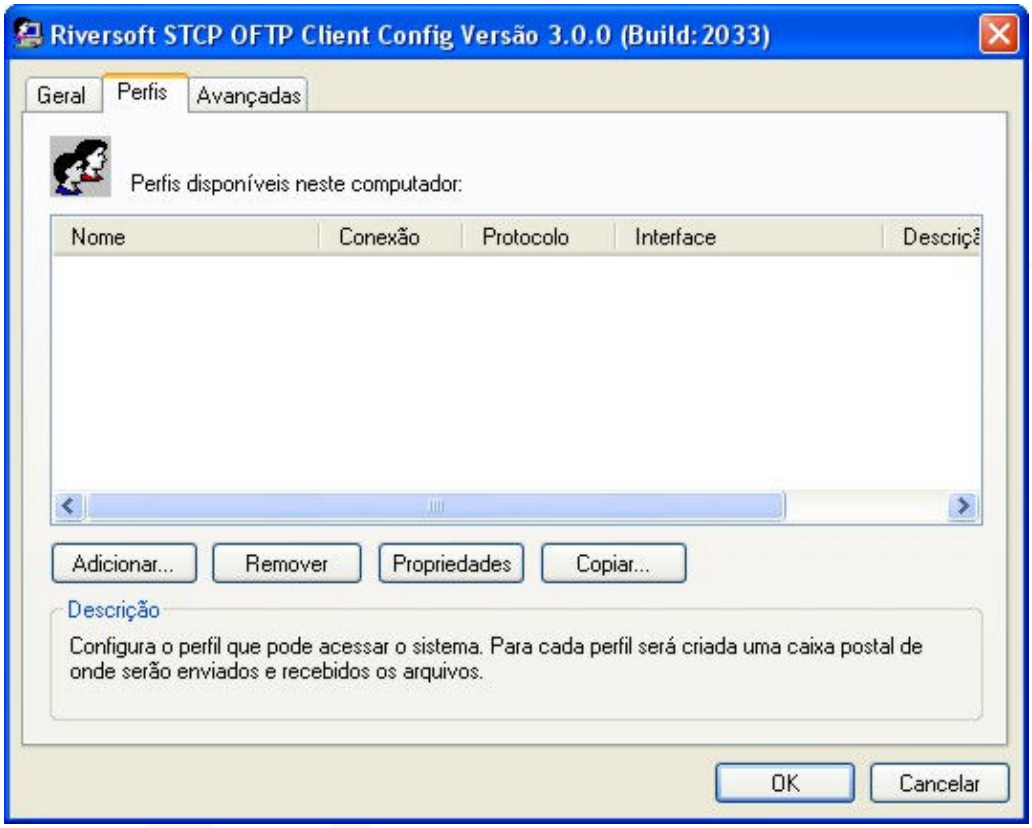
Obs.: Esta configuração deve ser alterada antes da criação dos Perfis.

Número de Série

Preencha este campo com o número de série que se encontra localizado no "Contrato de Licença de Uso" ou na parte traseira da embalagem do CD.

Obs.: O preenchimento deste campo é obrigatório.

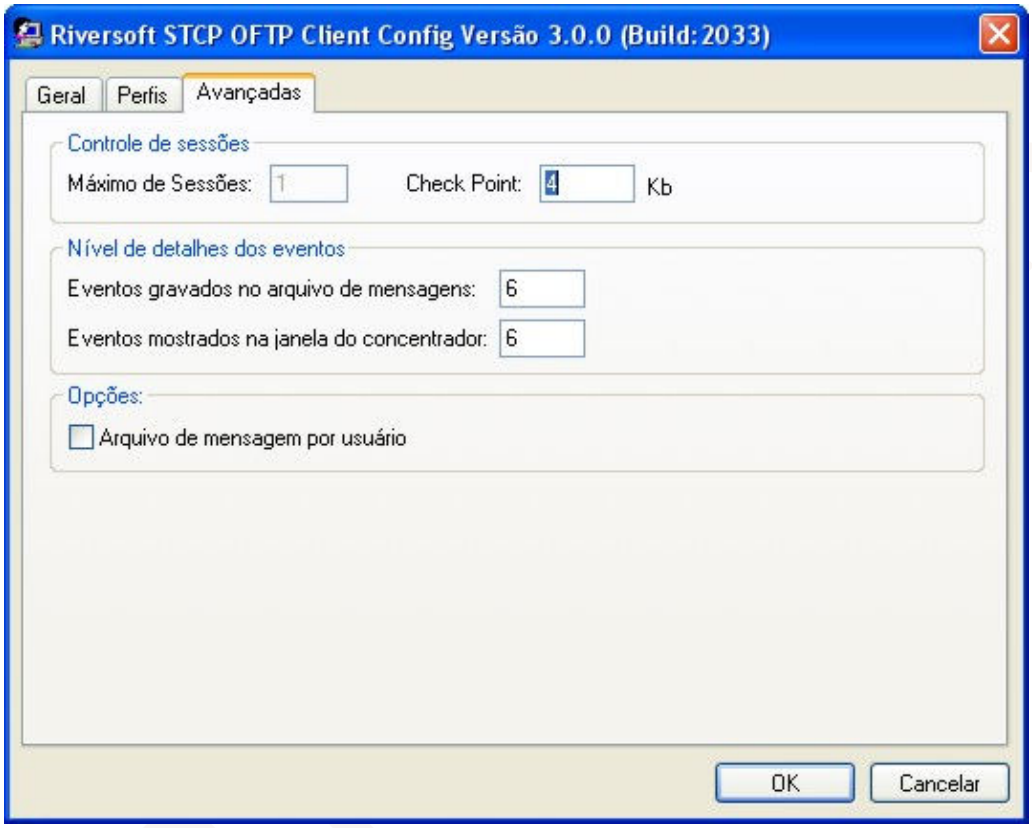
7. A tela de configuração da guia **Perfis** é exibida, conforme mostra a figura abaixo:



Nesta tela você pode adicionar modificar, remover ou copiar um perfil de comunicação.

Ao ser adicionado um novo Perfil, será automaticamente criada uma estrutura de subdiretórios para o envio e recepção dos arquivos dentro do ***Diretório de Dados*** que foi previamente configurado na guia **Geral**.

8. A tela de configuração da guia **Avançadas** é exibida, conforme mostra a figura abaixo:



Nesta tela você irá preencher os campos com as informações descritas abaixo e ao final pressionar o botão **[OK]** para gravar as configurações ou a qualquer momento **[Cancelar]** para abandonar sem alterar as configurações.

Descrição dos campos para configuração

Máximo de sessões

Este campo informa a quantidade máxima de sessões simultâneas de transferência que podem ser ativadas.

Obs.: Para a versão STCP OFTP Client este parâmetro não pode ser modificado.

Check Point

Preencha este campo com o múltiplo da quantidade de dados recebidos para que o STCP OFTP force uma gravação física do arquivo. No caso de uma interrupção da transferência, a sua recuperação ocorrerá a partir da última posição de check point corretamente gravada.

Eventos gravados no arquivo de mensagens

Preencha este campo com o nível de evento que será armazenado no arquivo de mensagens.

Eventos mostrados na janela do concentrador

Preencha este campo com o nível de evento que será mostrado na janela de mensagens do STCP OFTP.

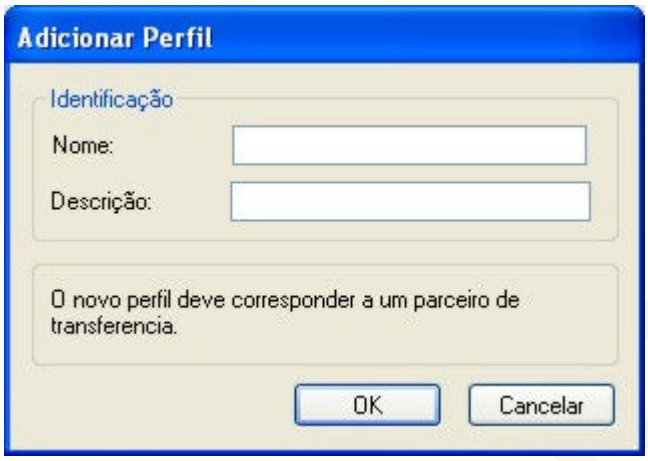
Nível do Evento	Descrição
0	Os eventos de inicio e término da aplicação.
1	Os eventos que contenham algum erro.
2	Os eventos de término da operação de cancelamento de espera de uma conexão.
3	Os eventos de inicio e término de cancelamento das conexões.
4	Os eventos com sucesso de inicio e término de conexão, inicio e término de sessão, inicio e término de transmissão ou inicio e término de recepção.
5	Não definido
6	Não definido
7	Os eventos de inicio e término da unidade de processamento (threads).
8	Os eventos de inicio e término da agenda.

Obs.: Os eventos associados a um nível inferior ou igual ao selecionado serão processados.

Arquivo de mensagens por usuário

Esta opção habilita ou inibe a geração do arquivo de mensagens separadamente por Perfil.

9. Ao pressionar o botão ***Adicionar*** é exibida uma nova tela, conforme mostra a figura abaixo:



Nesta tela você irá preencher os campos com as informações descritas abaixo e ao final pressionar o botão **[OK]** para prosseguir ou a qualquer momento **[Cancelar]** para abandonar sem alterar as configurações.

Descrição dos campos para configuração

Nome

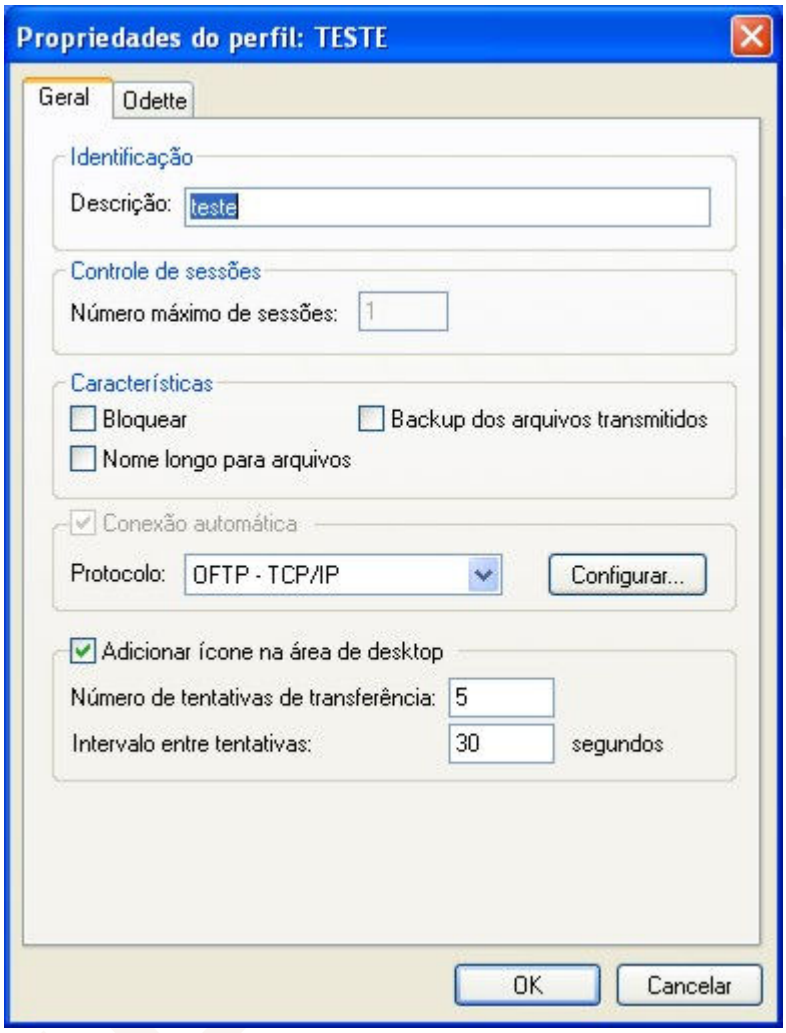
Preencha este campo com o nome desejado para este Perfil, que pode ser: a identificação ODETTE (OID) do parceiro, o nome da aplicação, a sua identificação ODETTE (OID) ou qualquer outra.

Obs.: Não utilize caracteres especiais ou espaços em branco.

Descrição

Preencha este campo com a descrição de sua livre escolha.

10. Ao pressionar o botão **[OK]** na tela Adicionar Perfil, uma nova tela será exibida, conforme mostra a figura abaixo:



Nesta tela você irá preencher os campos com as informações descritas abaixo e ao final pressionar o botão **[OK]** para gravar as configurações ou a qualquer momento **[Cancelar]** para abandonar sem alterar as configurações.

Descrição dos campos para configuração

Descrição

Preencha este campo com a descrição de sua livre escolha.

Número máximo de sessões

Este campo informa a quantidade máxima de sessões simultâneas de transferência que podem ser ativadas.

Obs.: Para a versão STCP OFTP Client este parâmetro não pode ser modificado.

Bloquear

Esta opção habilita ou inibe temporariamente este Perfil de realizar as operações de transferência.

Backup dos arquivos transmitidos

Esta opção habilita ou inibe temporariamente este Perfil de mover os arquivos transmitidos com sucesso para o subdiretório de backup.

Obs.: Os arquivos movidos para o diretório de backup contêm uma extensão no final do nome com a seguinte característica: YYYYMMDDhhmmss, onde YYYY é o ano, MM é o mês, DD é o dia, hh é a hora, mm são os segundos do término da transferência.

Nome longo para arquivos

Esta opção habilita ou inibe temporariamente este Perfil de transferir arquivos com nome maiores que 26 (vinte e seis) posições.

Obs.: Não habilite esta opção se você não tiver absoluta certeza que o parceiro remoto é um outro STCP OFTP e que esteja também com esta característica habilitada.

Conexão automática

Esta opção habilita ou inibe que este Perfil possa iniciar uma conexão.

Obs.: Para a versão STCP OFTP Client esta opçao não pode ser modificado.

Protocolo

Este campo seleciona o tipo de protocolo de comunicação que este Perfil irá utilizar para conexão. Após selecionar pressione o botão **[Configurar]** para acessar a tela de configuração específica do protocolo de comunicação.

Adicionar ícone na área de desktop (trabalho)

Esta opção habilita ou inibe a criação na área de desktop (trabalho) do ícone com o atalho para executar o STCP OFTP Client e realizar a operação de transferência.

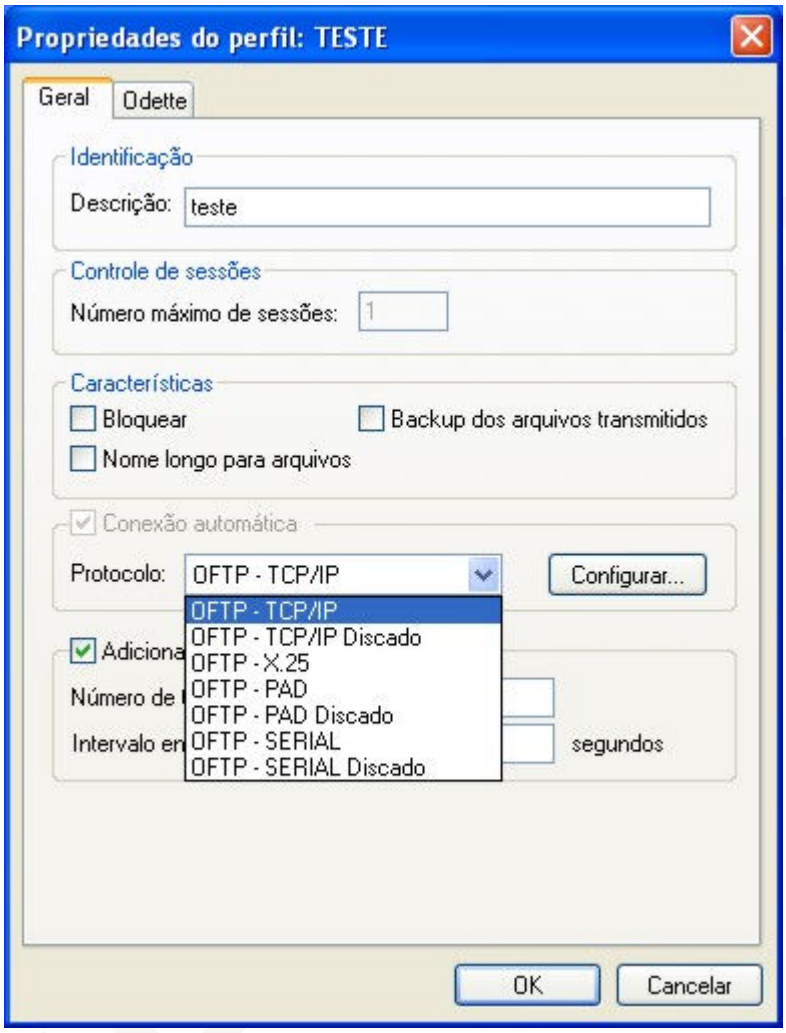
Número de tentativas de transferência

Preencha este campo com a com o número máximo de tentativas de conexão que este Perfil irá executar em caso de falha.

Intervalo entre tentativas (segundos)

Preencha este campo com o intervalo mínimo (segundos) de espera entre a realização de uma nova tentativa de conexão.

11. As seguintes opções de ***Protocolo*** podem ser selecionadas, conforme mostra a figura abaixo:



Após selecionar a opção desejada, você deverá pressionar o botão **[Configurar],** para acessar a tela de configuração específica de cada protocolo.

OFTP - TCP/IP

Configura o STCP OFTP para utilizar o protocolo de comunicação TCP/IP através de uma rede local.

OFTP - TCP/IP Discado

Configura o STCP OFTP para utilizar o protocolo de comunicação TCP/IP através de uma rede de acesso discado (dial-up).

OFTP – X.25

Configura o STCP OFTP para utilizar o protocolo de comunicação X.25 através de uma rede de acesso dedicada.

Obs.: Para utilizar esta opção você deve ter instalado um cartão de comunicação WCK2000 fornecido pela Net Open (www.net-open.com.br).

OFTP – PAD

Configura o STCP OFTP para utilizar o protocolo de comunicação PAD (X.28) através de uma rede de acesso dedicada.

OFTP – PAD Discado

Configura o STCP OFTP para utilizar o protocolo de comunicação PAD (X.28) através de uma rede de acesso discada.

OFTP – SERIAL

Configura o STCP OFTP para utilizar diretamente uma porta serial.

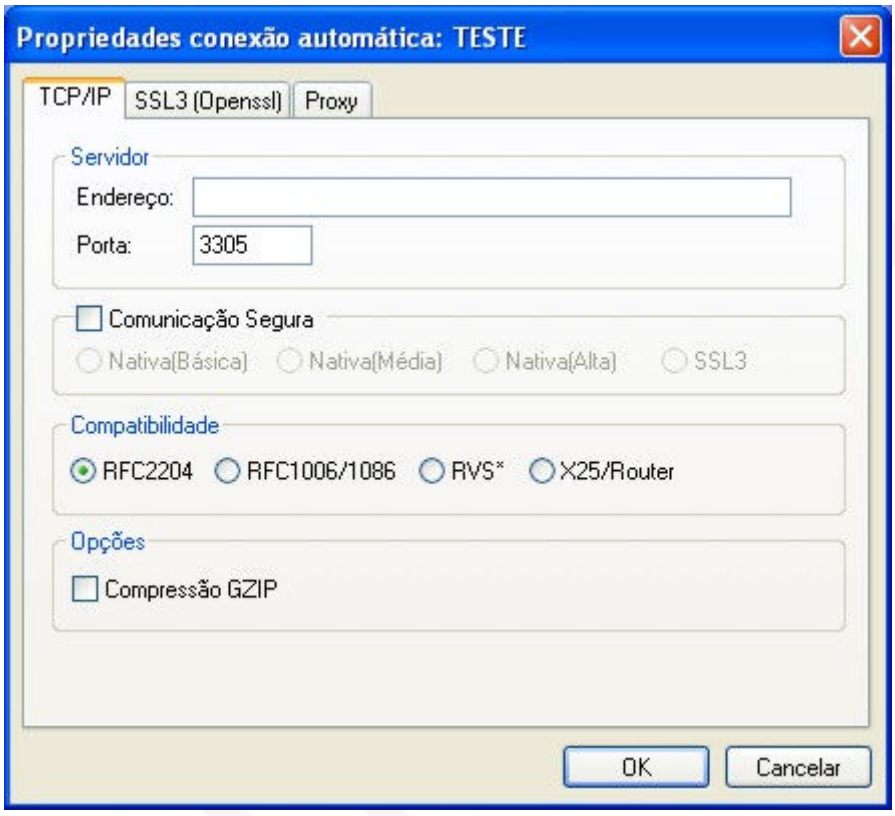
Obs.: Esta opção não usa protocolo TCP/IP.

OFTP – SERIAL Discada

Configura o STCP OFTP para utilizar uma porta serial com um modem ou uma placa de Fax/Modem.

Obs.: Esta opção não usa protocolo TCP/IP.

12. As seguintes opções de configuração para o protocolo ***OFTP – TCP/IP*** podem ser selecionadas na guia **TCP/IP**, conforme mostra a figura abaixo:



Nesta tela você irá preencher os campos com as informações descritas abaixo e ao final pressionar o botão **[OK]** para prosseguir ou a qualquer momento **[Cancelar]** para abandonar sem alterar as configurações.

Descrição dos campos para configuração

Endereço

Preencha este campo com o endereço TCP/IP ou nome (DNS) do servidor STCP OFTP.

Porta

Preencha este campo com a porta TCP/IP do servidor STCP OFTP.

Comunicação Segura

Esta opção habilita ou inibe a utilização de criptografia na comunicação com o servidor STCP OFTP, você pode escolher entre a opção **Nativa** ou **SSL3**.

Obs.: Antes de habilitar esta opção leia atentamente o capítulo sobre Segurança.

Nativa (Básica)

Configura a comunicação segura com criptografia com nível de segurança básico.

Obs.: Antes de habilitar esta opção confirme se o servidor com quem você deseja se comunicar suporta esta característica.

Nativa (Média)

Configura a comunicação segura com criptografia com nível de segurança médio.

Obs.: Antes de habilitar esta opção confirme se o servidor com quem você deseja se comunicar suporta esta característica.

Nativa (Alta)

Configura a comunicação segura com criptografia com nível de segurança médio.

Obs.: Antes de habilitar esta opção confirme se o servidor com quem você deseja se comunicar suporta esta característica.

SSL3

Configura a comunicação segura com criptografia e certificação digital, com a utilização da padronização definida na RFC2246 (TLS1/SSL3). O TLS1/SSL3 é comumente encontrado nos servidores de sites seguros (HTTPS) e oferece o maior grau de segurança atualmente disponível

Obs.: Antes de habilitar esta opção confirme se o servidor com quem você deseja se comunicar suporta esta característica.

Compatibilidade

Esta opção possibilita compatibilizar o STCP OFTP com diferentes produtos atualmente existentes no mercado.

RFC2204

Esta opção de compatibilidade permite a comunicação do STCP OFTP com outros produtos que seguem a recomendação RFC2204.

RFC1006/RFC1086

Esta opção de compatibilidade permite a comunicação do STCP OFTP através de gateways de comunicação TCP-IP/X.25, que seguem a recomendação RFC1006/1086.

*RVS**

Esta opção de compatibilidade permite a comunicação do STCP OFTP com o produto RVS*.

Obs.: Esta opção não deve ser habilitada quando o servidor RVS* for uma versão do mainframe (grande porte).

*** As marcas citadas são propriedade dos seus respectivos donos.**

X25/Router

Esta opção de compatibilidade permite a comunicação do STCP OFTP através de roteadores com suporte à comunicação X.25 através de socket.

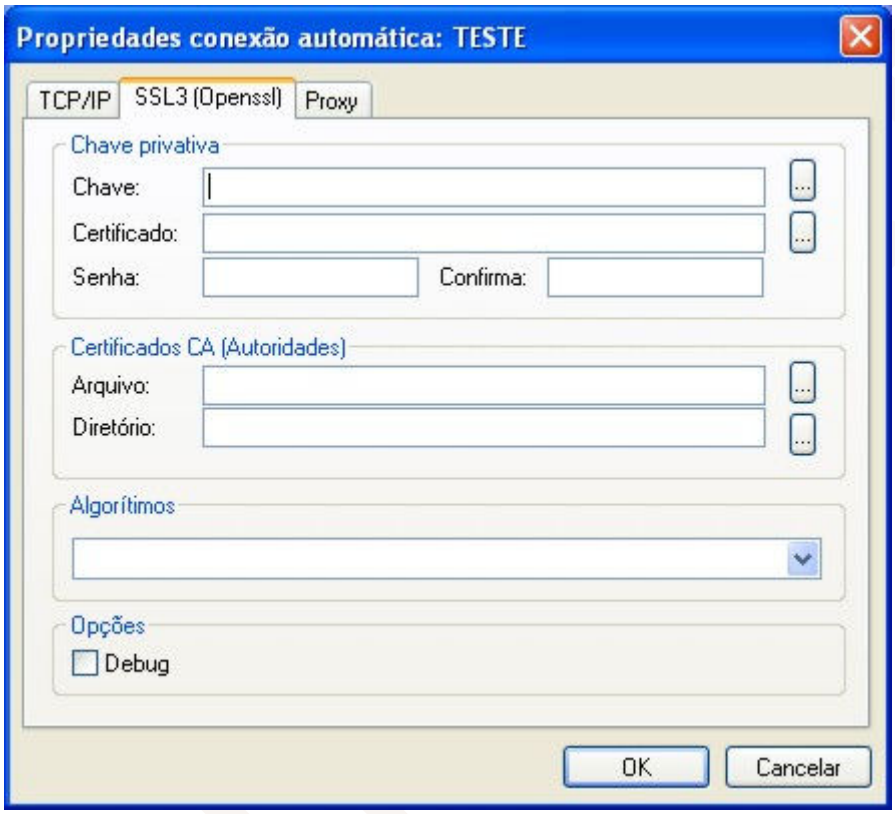
Obs.: Consulte a Riversoft sobre esta configuração, se você estiver em dúvidas.

Compressão GZIP

Esta opção habilita ou inibe a utilização da compressão GZIP on-the-fly (durante a transferência).

Obs.: Antes de habilitar esta opção confirme se o servidor com quem você deseja se comunicar suporta esta característica.

13. As seguintes opções de configuração para o protocolo ***OFTP – TCP/IP*** podem ser selecionadas na guia **SSL3**, conforme mostra a figura abaixo:



Nesta tela você irá preencher os campos com as informações descritas abaixo e ao final pressionar o botão **[OK]** para prosseguir ou a qualquer momento **[Cancelar]** para abandonar sem alterar as configurações.

Descrição dos campos para configuração

Chave Privativa

As opções deste grupo, estão relacionadas as chaves pública e privada, utilizadas pelo protocolo **TLS1/SSL3** para autenticação e criptografia dos dados.

Obs.: O arquivo da chave privativa deve estar no formato PKCS#12 e os certificados no formato DER ou PEM.

Chave

Preencha este campo com o nome do arquivo (caminho completo) onde se encontra instalado a chave privativa.

Certificado

Preencha este campo com o nome do arquivo (caminho completo) onde se encontra instalado o certificado digital (X509) associado à chave privativa.

Senha

Preencha este campo com a senha que protege o arquivo da chave privativa.

Confirma Senha

Preencha este campo com a senha informada no campo ***senha*** para validação.

Certificados CA (Autoridade)

As opções deste grupo estão relacionadas aos certificados digitais das autoridades certificadoras (CA) que servirão para validar a autenticidade do certificado apresentado pelo servidor.

Obs.: O arquivo da chave privativa deve estar no formato PKCS#12 e os certificados no formato DER ou PEM.

Arquivo

Preencha este campo com o nome do arquivo (caminho completo) onde se encontra instalado o certificado digital (X509) contendo a chave pública que assina o certificado apresentado pelo servidor.

Diretório

Preencha este campo com o nome do diretório (caminho completo) onde se encontram instalado os certificados digitais (X509) contendo a chave pública que assina o certificado apresentado pelo servidor.

Algoritmos

Preencha este campo com os nomes dos algoritmos suportados para assinatura digital, hashing e criptografia dos dados.

Obs.: Caso este campo não seja configurado, o protocolo TLS1/SSL3 irá selecionar automaticamente.

14. As seguintes opções de configuração para o protocolo ***OFTP – TCP/IP*** podem ser selecionadas na guia **Proxy,** conforme mostra a figura abaixo:

Nesta tela você irá preencher os campos com as informações descritas abaixo e ao final pressionar o botão **[OK]** para prosseguir ou a qualquer momento **[Cancelar]** para abandonar sem alterar as configurações.

Descrição dos campos para configuração

Servidor Proxy

As opções deste grupo possibilitam a configuração da comunicação através de um servidor Proxy.

Habilitar

Esta opção habilita ou inibe a utilização de um servidor Proxy..

SOCKS4

Esta opção habilita a utilização de um servidor Proxy em conformidade com a especificação SOCKS4.

SOCKS5

Esta opção habilita a utilização de um servidor Proxy em conformidade com a recomendação RFC1928 (SOCKS5) e RFC1929.

Obs.: O processo de autenticação utilizado é o definido na RFC1929.

HTTP

Esta opção habilita a utilização de um servidor Proxy em conformidade com a recomendação RFC2817 (HTTP).

Obs.: O processo de autenticação utilizado é o *Basic*.

Autenticação

As opções deste grupo possibilitam a configuração do usuário e senha que serão informados ao servidor Proxy.

Usuário

Preencha este campo com o nome do usuário autorizado a utilizar o serviço de Proxy.

Senha

Preencha este campo com a senha do usuário autorizado a utilizar o serviço de Proxy.

Confirma Senha

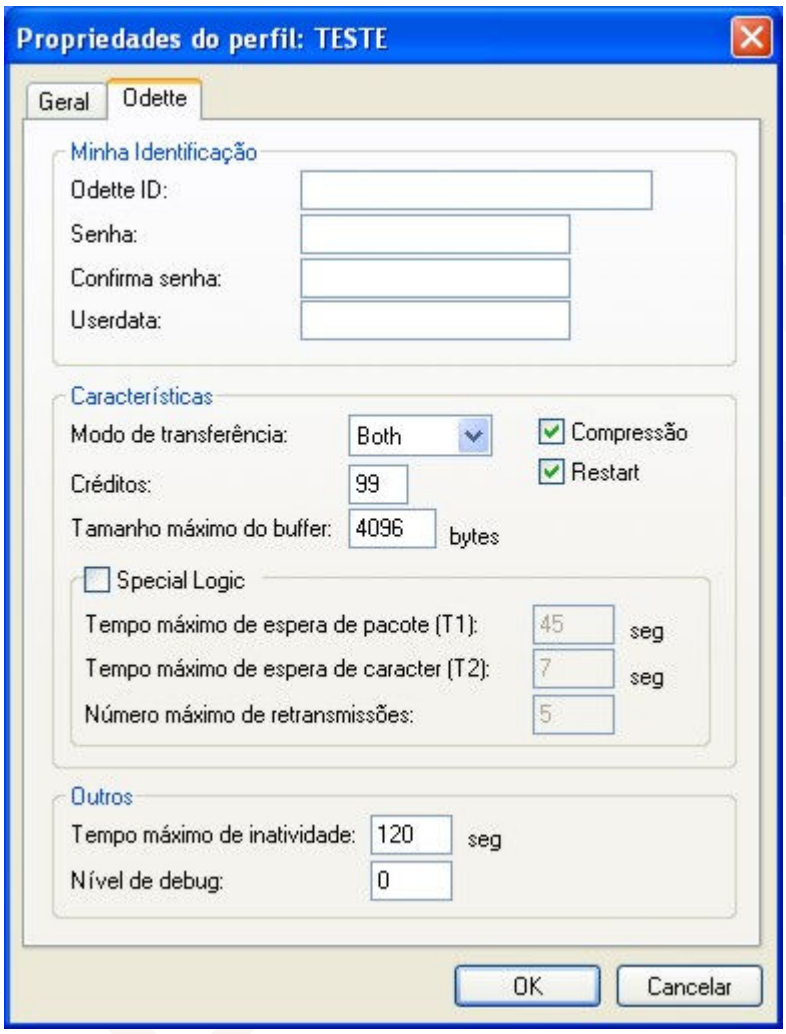
Preencha este campo com a senha informada no campo ***Senha*** para validação.

Lê configuração Proxy do IE

Pressione este botão para ler as configurações de Proxy configuradas no Internet Explorer.

Obs.: As informações de autenticação não serão lidas do IE.

15. As seguintes opções de configuração para o perfil podem ser selecionadas na guia **Odette**, conforme mostra a figura abaixo:



Nesta tela você irá preencher os campos com as informações descritas abaixo e ao final pressionar o botão **[OK]** para gravar as configurações ou a qualquer momento **[Cancelar]** para abandonar sem alterar as configurações.

Descrição dos campos para configuração

Minha Identificação

As opções definidas neste grupo serão utilizadas pelo STCP OFTP na identificação deste Perfil para o servidor Odette.

Odette ID (OID)

Preencha este campo com a identificação Odette associada a este Perfil. Este campo poderá ter no máximo 25 (vinte e cinco) caracteres.

Senha

Preencha este campo com a senha associada a identificação Odette. Este campo poderá ter no máximo 8 (oito) caracteres.

Confirma Senha

Preencha este campo com a senha informada no campo ***Senha*** para validação.

Userdata

Preencha este campo com os dados extra associados a identificação Odette informada.

Obs.: Preencha este campo somente se for requerido pelo servidor.

Características

As opções definidas neste grupo serão utilizadas pelo STCP OFTP na comunicação com o servidor Odette.

Obs.: Não modifique estas características sem ler atentamente o que significa cada uma delas e ter certeza que realmente deseja faze-lo.

Modo de transferência

Esta opção permite selecionar o modo de transferência que será utilizado para comunicação com o servidor, são eles: ***Both*** (transmissão e recepção de arquivos), ***Sender*** (somente transmissão de arquivos) e ***Receiver*** (somente recepção de arquivos).

Créditos

Preencha este campo com a quantidade de blocos de dados que serão transferidos até aguardar uma nova autorização para envio. O intervalo válido é de 1 até 99.

Tamanho máximo do buffer

Preencha este campo com o tamanho máximo dos blocos de dados que serão transferidos. O intervalo válido é de 1 até 65535.

Compressão

Esta opção habilita ou inibe a compressão dos dados (padrão Odette) de uma transferência.

Restart

Esta opção habilita ou inibe o controle de recuperação automática na interrupção de uma transferência. Com esta opção habilitada o STCP OFTP irá recuperar a transferência do ponto de interrupção.

Special Logic

Esta opção habilita ou inibe o controle o regime de comunicação lógica especial. Somente deve ser habilitado para comunicação através do protocolo PAD ou SERIAL.

Obs.: Não habilite esta opção quando não for utilizado o Protocolo PAD ou SERIAL.

Outros

As opções definidas neste grupo serão utilizadas localmente pelo STCP OFTP para controlar o tempo de inatividade e a geração do arquivo de depuração da comunicação.

Tempo máximo de inatividade

Preencha este campo com o tempo máximo de inatividade de comunicação entre o STCP OFTP Client e o servidor Odette.

Debug

Preencha este campo com o nível de detalhamento das informações que serão gravadas no arquivo de depuração. Para obter no mesmo arquivo de depuração a informação dos diferentes níveis, preencha este campo com a soma dos níveis desejados.

Para cada tentativa de conexão será criado um novo arquivo de depuração no subdiretório **DEBUG,** com a seguinte sintaxe:

ODTDEB.<Protocolo>.<Perfil>.YYYMMDDhhmmssnnn.

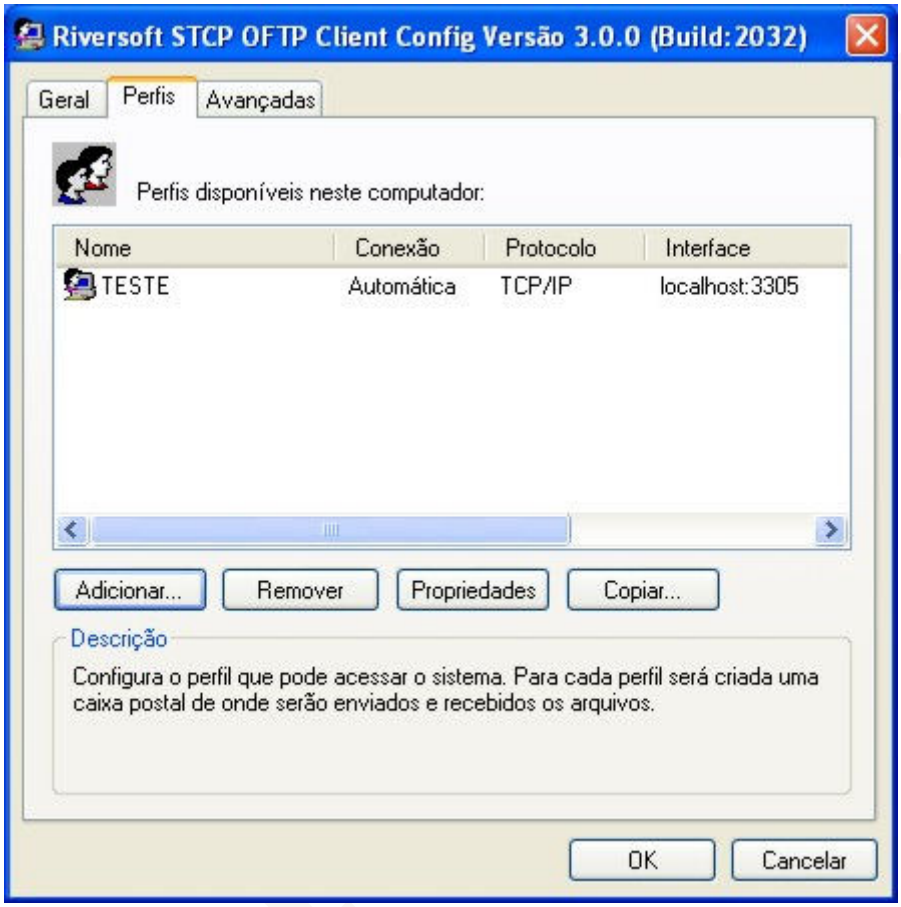
Protocolo	TCPIP, X25, SERIAL ou PAD
Perfil	Nome do perfil utilizado
YYYY	Ano
MM	Mês
DD	Dia
hh	Hora
mm	Minuto
ss	Segundos
nnn	Milésimos de segundos

A tabela a seguir contém a relação entre o nível de detalhamento e as informações que serão geradas.

Nível	Descrição
0	Não grava o arquivo de depuração.
1	Grava as informações de entrada e saída das subrotinas.
2	Grava as informações de mudanças do estado do protocolo.
4	Grava as informações dos pacotes recebidos e enviados, formatado por campo.
8	Grava as informações dos pacotes recebidos e enviados, formatado em hexadecimal.
16	Grava as informações dos eventos ocorridos.
32	Grava as informações dos subregistros.

Obs.: Somente habilite esta opção quando for solicitado por pessoal especializado.

16. Após Adicionar o perfil a guia **Perfis** será apresentada, conforme mostra a figura abaixo:



Nesta tela você pode adicionar modificar, remover, copiar um perfil de comunicação, pressionar o botão **[OK]** para gravar as configurações ou **[Cancelar]** para abandonar sem alterar as configurações.

Obs.: Ao pressionar o botão [OK] somente as configurações da guia *Geral* e *Avançadas* serão gravadas.

17. Após o Perfil ser adicionado corretamente estará disponível para configuração das **Propriedades do perfil**, uma nova guia: **Tipos de Arquivos**, conforme mostra a figura abaixo:

Nesta tela você pode: adicionar, remover, modificar ou copiar um novo **Tipo de Arquivo**, pressionar o botão **[OK]** para prosseguir ou a qualquer momento **[Cancelar]** para retornar.

A configuração de um **Tipo de Arquivo** possibilita alterar algumas características na transferência do arquivo, tais como: conversão do nome ou formato do arquivo, conversão da codificação dos dados, iniciarem uma aplicação ou bat entre outras.

O tipo **Default** sempre deverá existir e será utilizado nos casos onde não haja um tipo específico definido para a transferência em andamento.

A associação entre um **Tipo de Arquivo** e o arquivo propriamente dito poderá ser estabelecida de duas formas: 1 - através do ***nome do arquivo*** e o ***nome do tipo***, ou 2 - ***parte do nome do arquivo*** e os valores definidos nas propriedades ***Prefixo*** e ***Sufixo*** do tipo.

Para melhor compreensão como será a associação entre o nome do arquivo e o tipo de arquivo, veja os exemplos demonstrados no quadro abaixo:

Nome Arquivo	Nome Tipo	Prefixo	Sufixo	Associação
TESTE.TXT	TESTE.TXT	-	-	1.
TESTE.TXT	TESTE	-	-	Default
TESTE.TXT	TESTE	**TES**	-	2
TESTE.**TXT**	TESTE	-	**TXT**	2
TESTE.TXT	TESTE	TXT	-	Default
TE**STE**.TXT	TESTE	-	**STE**	2

18. Ao pressionar o botão ***Adicionar*** é exibida uma nova tela, conforme mostra a figura abaixo:

Nesta tela você irá preencher os campos com as informações descritas abaixo e ao final pressionar o botão **[OK]** para prosseguir ou a qualquer momento **[Cancelar]** para retornar.

Descrição dos campos para configuração

Nome do novo tipo de arquivo

Preencha este campo com o nome desejado para o novo tipo.

Obs.: Leia atentamente o item 17. Não utilize caracteres especiais ou espaços em branco.

19. Ao pressionar o botão **[OK]** na tela Adicionar **Tipo de Arquivo**, uma nova tela será exibida, conforme mostra a figura abaixo:

Nesta tela você irá preencher os campos com as informações descritas abaixo e ao final pressionar o botão **[OK]** para gravar as configurações ou a qualquer momento **[Cancelar]** para abandonar sem alterar as configurações.

Descrição dos campos para configuração

Verificar nome do Arquivo por:

As opções definidas neste grupo serão utilizadas pelo STCP OFTP para definir a forma de associação do nome do arquivo com o tipo (conforme descrito no item 17): **Padrão (Default)**, **Prefixo/Sufixo** ou **Nome do tipo**.

Prefixo

Preencha este campo com o prefixo do nome do arquivo que deve ser associado a este tipo.

Sufixo

Preencha este campo com o sufixo do nome do arquivo que deve ser associado a este tipo.

Informações sobre o arquivo

As opções definidas neste grupo serão utilizadas pelo STCP OFTP para definir as características gerais do arquivo na transmissão ou recepção.

Originador

Preencha este campo com o a identificação Odette (OID) que originou o arquivo.

Obs.: Quando o perfil é criado este campo contém a identificação Odette do cliente.

Destino

Preencha este campo com o a identificação Odette (OID) do destino deste arquivo.

Obs.: Quando o perfil é criado este campo contém a identificação Odette do servidor.

Formato

Esta opção permite selecionar o formato do registro do arquivo, são eles: ***Não Formato***, ***Fixo*** e ***Variável***..

Obs.: Somente utilize Fixo ou Variável quando o servidor Odette for uma versão de mainframe (grande porte) e esta característica estiver habilitada.

Tamanho do registro

Preencha este campo com a quantidade de caracteres (bytes) que compõem o registro.

Obs.: Somente utilize esta opção quando o formato do registro for Fixo ou Variável.

Arquivos Transmitidos

As opções definidas neste grupo serão utilizadas pelo STCP OFTP para definir as características do arquivo na transmissão.

Comando a ser executado

Preencha este campo com o nome de uma aplicação ou arquivo de lote (bat) a ser executado após o envio com sucesso do arquivo.

Tabela de conversão

Esta opção permite selecionar a tabela de conversão dos dados na transmissão, são elas: ***Nenhuma***, ***ASC2EBC.TAB (converte de ASCII para EBCDIC)*** e ***EBC2ASC.TAB (converte de EBCDIC para ASCII)***.

Remover CR+LF

Esta opção permite habilitar ou inibir a remoção dos caracteres CR (Carriage Return) e LF (Line Feed) na transmissão do arquivo.

Obs.: Somente utilize esta opção quando o formato do registro for Fixo ou Variável.

Remover Timestamp

Esta opção permite habilitar ou inibir a remoção do timestamp externo do nome do arquivo.

Converter nome do arquivo

Esta opção permite selecionar a conversão do nome do arquivo antes de transmitir, são elas: ***Não***, ***maiúscula*** ou ***minúscula***.

Arquivos Recebidos

As opções definidas neste grupo serão utilizadas pelo STCP OFTP para definir as características do arquivo na recepção.

Comando a ser executado

Preencha este campo com o nome de uma aplicação ou arquivo de lote (bat) a ser executado após a recepção com sucesso do arquivo.

Tabela de conversão

Esta opção permite selecionar a tabela de conversão dos dados na recepção, são elas: ***Nenhuma***, ***ASC2EBC.TAB*** (converte de ASCII para EBCDIC) e ***EBC2ASC.TAB*** (converte de EBCDIC para ASCII).

Inserir CR+LF

Esta opção permite habilitar ou inibir a inserção dos caracteres CR (Carriage Return) e LF (Line Feed) na recepção do arquivo.

Obs.: Somente utilize esta opção quando o formato do registro for Fixo ou Variável.

Inserir Timestamp

Esta opção permite habilitar ou inibir a inserção do timestamp externo no nome do arquivo.

Sobrepor arquivo

Esta opção permite habilitar ou inibir a sobreposição do arquivo, quando já existir um arquivo com o mesmo nome.

Inibir EERP

Esta opção permite habilitar ou inibir o envio do comando Odette EERP (End to End Response) ao final da recepção do arquivo com sucesso.

Obs.: Somente utilize esta opção se o servidor suportar esta carcterística.

Converter nome do arquivo

Esta opção permite selecionar a conversão do nome do arquivo após a recepção, são elas: ***Não***, ***maiúscula*** ou ***minúscula***.

Formato do Timestamp externo do arquivo

A utilização do timestamp externo do arquivo tem o seguinte formato:

<nome do arquivo>.YYYYMMDDhhmmssnnn

<nome do arquivo>	Nome do arquivo sem caracteres especiais ou espaços.
YYYY	Ano
MM	Mês
DD	Dia
Hh	Hora
mm	Minuto
ss	Segundos
nnn	Milésimos de segundos

4) Utilização

Como utilizar o STCP OFTP?

A Cada Perfil configurado o STCP OFTP cria um conjunto individual de subdiretórios para controle das transferências e integração com as aplicações externas, conforme mostra figura abaixo:

<Diretório de Dados>	Subdiretório de dados configurado.
<Diretório do Perfil>	Subdiretório individual do Perfil.
CONTROLE	Subdiretório de controle da aplicação.
ENTRADA	Subdiretório onde os arquivos recebidos com sucesso serão disponibilizados.
RESTART	Subdiretório onde os arquivos que estão em processo de recepção são armazenados temporariamente.
FORMATO	Subdiretório que contêm as definições dos tipos de arquivos.
LOG	Subdiretório onde serão armazenados os arquivos de eventos e registro das transferências.
SAIDA	Subdiretório onde os arquivos a serem enviados devem ser disponibilizados.
BACKUP	Subdiretório onde os arquivos enviados com sucesso serão armazenados, se a opção de backup do Perfil estiver habilitada.
PENDENTE	Subdiretório onde o arquivo de controle da transmissão será armazenado temporariamente.
TEMP	Subdiretório de uso geral

Para transmitir, os arquivos devem ser disponibilizados no subdiretório "**SAIDA**" e os arquivos recebidos serão disponibilizados no subdiretório "**ENTRADA**".

Como executar o STCP OFTP através da linha de comando?

A sintaxe para executar o STCP OFTP através de linha de comando é a seguinte:

STCPCLT.EXE <Arquivo de configuração> [-p –r –t –m –f –w]

Parâmetro	Descrição
<arquivo de configuração>	Define o nome do arquivo de configuração de instalação **"CTCP.INI"** com o caminho completo.
-p <nome do perfil>	Define o nome do perfil de conexão.
-r <número de tentativas>	Define a quantidade de tentativas de conexão.
-t <intervalo de tentativas>	Define o intervalo em segundos entre as tentativas.
-m <modo>	Define o modo de transferência a ser executado: **B**, **S** ou **R**. **B** = Transmissão e recepção **S** = Somente transmissão **R** = Somente recepção
-f <filtro de arquivos>	Define o filtro de arquivos através da utilização de expressão regular.
-w <Fecha caixa de dialogo>	Define se a caixa de dialogo será fechada automaticamente no final da execução: **0** ou **1**. 0 = Não fecha caixa de dialogo. 1 = Fecha a caixa de dialogo.

Exemplo:

C:\STCPCLT\STCPCLT.EXE C:\STCPCLT\CTCP.INI –p TESTE

No exemplo acima será executada a conexão para o Perfil TESTE para envio e recepção.

Ao término da execução do STCP OFTP o arquivo ***CLCP.ERR.TXT*** será criado no subdiretório de instalação, contendo a seguinte linha:

<código de erro><branco><descrição>

Tabelas com os códigos de erro do STCP OFTP

Códigos de erro geral:

Código	Descrição
1	Operação não permitida, conflito de permissões para o processo. (EPERM)
2	O arquivo ou diretório selecionado não existe. (ENOENT)
3	O processo selecionado não foi encontrado. (ESRCH)
4	A função foi interrompida. (EINTR)
5	Falha de acesso de entrada ou saída. (EIO)
6	Falha de acesso ao dispositivo. (ENXIO).
7	Argumento passado para executar o processo excede o limite permitido. (E2BIG).
8	Formato inválido do arquivo executável. (ENOEXEC).
9	Descritor utilizado para acesso ao arquivo é inválido. (EBADF).
10	Não existe processo filho. (ECHILD).
11	Recurso temporariamente indisponível. (EAGAIN).
12	Não existe memória disponível. (ENOMEM).
13	Falha de permissão para a operação desejada. (EACCESS).
14	Endereço de memória inválido. (EFAULT).
16	Recurso está ocupado. (EBUSY).
17	Arquivo já existe. (EEXIST).
18	Falha para executar um link através do sistema de arquivos. (EXDEV).
19	O tipo de dispositivo para operação solicitada é inválido (ENODEV).
20	O tipo de arquivo informado não é um diretório. (ENOTDIR).
21	O tipo de arquivo informado é um diretório. (EISDIR).
22	Argumento inválido para a função. (EINVAL).
23	Existe excesso de arquivos abertos no sistema. (ENFILE).
24	Existe excesso de arquivos abertos no processo. (EMFILE).
25	Falha de operação para o dispositivo selecionado. (ENOTTY).
27	Tamanho do arquivo excede o permitido. (EFBIG).

28	Não existe espaço disponível no dispositivo selecionado. (ENOSPC).
29	Operação inválida de posicionamento (seek) no dispositivo. (ESPIPE).
30	Operação inválida em um dispositivo somente de leitura. (EROFS).
31	Excedido número de referências para o mesmo arquivo. (EMLINK).
32	Pipe interrompido. (EPIPE).
33	Falha para executar uma função matemática. (EDOM).
34	Falha de overflow ou underflow. (ERANGE).
36	(EDEADLK)
39	Recurso de lock não disponível. (ENOLCK).
40	Função não implementada. (ENOSYS).
42	Falha na decodificação de um caractere multibyte. (EILSEQ).

Códigos de erro de transferência do protocolo Odette

Código	Descrição
401	Nome do arquivo inválido
402	Parâmetro Destination da seção Odette inválido
403	Parâmetro Originator da seção Odette inválido
404	Formato do registro não suportado
405	Tamanho do registro não suportado
406	Tamanho do arquivo excede o máximo permitido
410	Contador do registro inválido
411	Contador de bytes inválido
412	Falha no método de acesso
413	Arquivo duplicado ou diretório RESTART não existe
499	Código não especificado: um erro foi detectado, mas não pode ser adequadamente descrito pelos códigos disponíveis.

Códigos de erro de sessão do protocolo Odette

Código	Descrição
501	Comando inválido no pacote ODETTE.
502	Violação de protocolo: comando especificou uma função inválida no estado atual.
503	Código do usuário não cadastrado no concentrador.
504	Senha inválida.
505	Erro no computador local, comunicação sendo terminada.
506	Comando contém dados inválidos.
507	Tamanho do pacote ODETTE inválido.
508	Excedido o limite máximo de conexões do usuário.
509	Excedido tempo limite de inatividade.
510	Modo incompatível.
599	Código não especificado: um erro foi detectado, mas não pode ser adequadamente descrito pelos códigos disponíveis.

Códigos de erro da transferência:

Código	Descrição
1100	O arquivo contém a extensão de timestamp externa inválida. Verifique a opção ***Remover timestamp***.
1101	O nome do arquivo excedeu o limite máximo de 26 (vinte e seis) caracteres. Verifique a opção ***Nome longo para arquivos***.
1102	O nome do arquivo contém caractere inválido ou espaço em branco.
1103	O nome do arquivo está bloqueado. Verifique a opção de ***Filtro de arquivos***.
1104	O tamanho do arquivo excedeu o limite. Verifique a opção de ***Tamanho máximo***.

Códigos de erro genérico da interface de comunicação:

Código	Descrição
6801	Falha alocação de memória.
6802	Parâmetro com a localização da biblioteca de comunicação (DLLName) não foi informado no arquivo de configuração.
6803	Falha na carga da biblioteca de comunicação.
6804	Biblioteca de comunicação inválida ou corrompida.

Códigos de erro da interface de comunicação TCP/IP (RAS):

Código	Descrição
9005	Acesso negado. Verifique usuário e senha.
9600	Uma operação está pendente.
9601	Descritivo para porta é inválido.
9602	A porta já está aberta.
9603	Buffer é pequeno.
9604	Erro na informação especificada.
9605	Não pode configurar informação para porta.
9606	A porta não está conectada.
9607	Evento inválido.
9608	O dispositivo não existe.
9609	O tipo de dispositivo não existe.
9610	Buffer inválido.
9611	A rota não está disponível.
9612	A rota não está alocada.
9613	Compressão especificada é inválida.
9614	Não existe buffers disponíveis.
9615	A porta não foi encontrada.
9616	Requisição assíncrona está pendente.
9617	A porta ou dispositivo já está desconectando.
9618	A porta não está aberta.
9619	A porta está desconectada.

9620	Não existem endpoints.
9621	Não pode abrir o arquivo do phone book.
9622	Não pode carregar o arquivo do phone book.
9623	Não pode achar a entrada do phone book.
9624	Não pode escrever no arquivo do phone book.
9625	Informação inválida encontrada no arquivo do phone book.
9626	Não pode carregar uma string
9627	A chave não foi encontrada.
9628	A porta foi desconectada.
9629	A conexão foi terminada pelo computador remoto.
9630	A porta foi desconectada em virtude de uma falha no hardware.
9631	A porta foi desconectada pelo usuário.
9632	O tamanho da estrutura está incorreto.
9633	A porta já está em uso ou não foi configurada para acesso remoto.
9634	O seu computador não pode ser registrado na rede remota.
9635	Erro desconhecido.
9636	Um dispositivo errado foi associado à porta.
9637	A string não pode ser convertida.
9638	Excedido tempo limite.
9639	Rede assíncrona não disponível.
9640	Erro de NETBIOS.
9641	O servidor não pode alocar recursos de NETBIOS necessários para o cliente.
9642	Um de seus nomes NETBIOS já está registrado na rede remota.
9643	O adaptador de rede no servidor falhou.
9644	Não receberá mensagem da rede de popups.
9645	Erro de autenticação.
9646	A conta não está permitida a fazer logon nessa hora do dia.
9647	A conta está desabilitada.
9648	A senha expirou.
9649	A conta não tem permissão para fazer acesso remoto.
9650	O servidor de acesso remoto não está respondendo.

9651	Seu modem (ou outro dispositivo conectado) reportou erro.
9652	Resposta não reconhecida do dispositivo.
9653	Uma macro requisitada pelo dispositivo não foi encontrada no arquivo de configuração do dispositivo.
9654	Um comando ou resposta no arquivo de configuração do dispositivo faz referência a uma macro indefinida.
9655	A macro não foi encontrada no arquivo de configuração do dispositivo.
9656	A macro no arquivo de configuração do dispositivo está indefinida.
9657	O arquivo de configuração do dispositivo não pode ser aberto.
9658	O nome do dispositivo no de configuração é muito longo.
9659	O arquivo de configuração faz referência a um nome de dispositivo desconhecido.
9660	O arquivo de configuração do dispositivo não contém respostas para o comando.
9661	O arquivo de configuração do dispositivo está faltando um comando.
9662	Tentativa de configurar uma macro não listada no arquivo de configuração do dispositivo.
9663	O arquivo de configuração faz referência a um tipo de dispositivo desconhecido.
9664	Não pode alocar memória.
9665	A porta não está configurada para acesso remoto.
9666	Seu modem (ou outro dispositivo conectado) não está funcionando.
9667	Não pode ler o arquivo de configuração.
9668	A conexão caiu.
9669	O parâmetro 'usage' no arquivo de configuração é inválido.
9670	Não pode ler o nome da seção do arquivo de configuração.
9671	Não pode ler o tipo de dispositivo do arquivo de configuração.
9672	Não pode ler o nome do dispositivo do arquivo de configuração.
9674	Não pode ler a velocidade máxima de conexão do arquivo de configuração.
9675	Não pode ler a velocidade máxima da portadora do arquivo de configuração.
9676	A linha está ocupada.

9677	Uma pessoa respondeu em vez do modem.
9678	Não existe resposta.
9679	Portadora não detectada.
9680	Não existe tom de linha.
9681	Erro geral reportado pelo dispositivo.
9691	Acesso negado porque o usuário e/ou senha está inválida no domínio.
9692	Falha de hardware.
9699	A resposta do dispositivo causou estouro de buffer.
9701	O dispositivo mudou para uma velocidade não suportada pelo driver COM.
9702	Resposta recebida do dispositivo quando nenhuma resposta era esperada.
9703	A aplicação não permite interação com o usuário. A conexão requer interação com o usuário para completar com sucesso.
9708	A conta expirou.
9709	Erro trocando a senha no domínio. A senha deve estar curta ou já foi utilizada.
9710	Erros de overrun na serial foram detectados durante a comunicação com seu modem.
9711	Falha na inicialização do RASMAN. Verifique o log de evento.
9712	Porta biplex inicializando. Aguarde alguns minutos e redisque.
9713	Linhas ISDN não estão disponíveis.
9714	Canais ISDN não estão disponíveis para fazer a chamada.
9715	Muitos erros ocorreram em virtude da baixa qualidade de linha.
9717	Endereços IP's não estão disponíveis na lista de IP's estáticos do acesso remoto.
9718	Timeout aguardando por uma resposta válida do PPP remoto.
9719	PPP terminado pela máquina remota.
9720	Nenhum protocolo de controle configurado.
9721	PPP remoto não está respondendo.
9722	O pacote PPP é inválido.
9723	O número do telefone incluindo o prefixo e o sufixo é muito longo.
9724	O protocolo IPX não pode discar na porta porque a máquina é um

	roteador IPX.
9725	O protocolo IPX não pode discar na porta porque o roteador IPX não está instalado.
9726	O protocolo IPX não pode ser usado para dial-out por mais de uma porta ao mesmo tempo.
9727	Não pode acessar o arquivo TCPCFG.DLL.
9728	Não pode encontrar um adaptador IP para acesso remoto.
9729	SLIP não pode ser usado a menos que o protocolo IP seja instalado.
9730	Registro do computador não está completo.
9731	O protocolo não está configurado.
9732	A negociação PPP não está convergindo.
9733	O protocolo de controle PPP não está disponível no servidor.
9734	O protocolo de controle PPP terminou.
9735	O endereço requisitado foi rejeitado pelo servidor.
9736	O computador remoto terminou o protocolo de controle.
9737	Detectado loopback.
9738	O servidor não associou um endereço.
9739	O protocolo de autenticação requerido pelo servidor remoto não pode usar a senha com criptografia do Windows NT. Disque novamente, entrando com a senha.
9740	Configuração TAPI inválida.
9741	O computador local não suporta o tipo de criptografia requerida.
9742	O computador remoto não suporta o tipo de criptografia requisitada.
9743	O computador remoto requer criptografia.
9744	O número da rede IPX associado pelo servidor remoto não pode ser usado. Verifique o log de evento.
9745	SMM inválido.
9746	SMM não inciado.
9748	SMM Timeout
9749	Número do telefone errado.
9750	Módulo errado.
9751	Número do callback inválido. Somente os caracteres de 0 até 9, T, P, W, (,), -, @ e espaço são permitidos no número.

9752	Um erro de sintaxe foi encontrado durante processamento de um script.
9753	A conexão não pode ser desconectada porque foi criada pelo Multi-Protocol Router.
9804	A conexão RAS não foi estabelecida.
9805	O usuário para autenticação do RAS não foi configurado.

Códigos de erro da interface de comunicação TCP/IP:

Código	Descrição
10004	A função foi interrompida. (WSAEINTR)
10009	Descritor utilizado para acesso é inválido. (WSAEBADF).
10013	Falha de permissão para a operação desejada. (WSAEACCESS).
10014	Endereço de memória inválido. (WSAEFAULT).
10022	Argumento inválido para a função. (WSAEINVAL).
10024	Excesso de sockets abertas no processo. (WSAEMFILE).
10035	Recurso temporariamente indisponível. (WSAEWOULDBLOCK).
10036	Existe uma operação em andamento. (WSAEINPROGRESS).
10037	Existe uma operação em andamento. (WSAEALREADY).
10038	Operação solicitada em um handle inválido. (WSAENOTSOCK).
10039	Um endereço IP é requerido. (WSAEDESTADDREQ).
10040	Mensagem excede o tamanho permitido. (WSAEMSGSIZE).
10041	Protocolo inválido para a socket. (WSAEPROTOTYPE).
10042	Opção inválida para o protocolo. (WSAENOPROTOOPT).
10043	Protocolo não é suportado. (WSAEPROTONOSUPPORT).
10044	Tipo de socket não é suportado. (WSAESOCKTNOSUPPORT)
10045	Operação não é suportada. (WSAEOPNOTSUPP).
10046	Família de protocolo não é suportada. (WSAEPFNOSUPPORT).
10047	Família de endereço não é suportada pela família de protocolo. (WSAEAFNOSUPPORT).
10048	Endereço já esta em uso. (WSAEADDRINUSE).
10049	Endereço não está disponível. (WSAEADDRNOTAVAIL).
10050	A rede está inoperante. (WSAENETDOWN).

10051	A rede não foi localizada. (WSAENETUNREACH).
10052	A conexão de rede foi abortada por um reset. (WSAENETRESET).
10053	A conexão de rede foi abortada pelo software. (WSAECONNABORTED).
10054	A conexão de rede foi abortada pelo computador remoto. (WSAECONNRESET).
10055	A operação solicitada não pode ser concluída por falta de memória. (WSAENOBUFS).
10056	Foi solicitada uma conexão em uma socket já conectada. (WSAEISCONN).
10057	A socket não está conectada, a operação de transmissão e recepção está desabilitada. (WSAENOTCONN).
10058	A socket está conectada em shutdown, a operação de transmissão e recepção está desabilitada (WSAESHUTDOWN).
10059	(WSAETOOMANYREFS).
10060	A solicitação de conexão falhou porque o computador remoto não respondeu durante um período de tempo. (WSAETIMEDOUT).
10061	A solicitação de conexão foi recusada porque o computador remoto não tem o serviço solicitado disponível. (WSAECONNREFUSED).
10062	(WSAELOOP).
10063	(WSAENAMETOOLONG).
10064	A operação falhou porque o computador remoto encontra-se desativado. (WSAEHOSTDOWN).
10065	Uma operação foi solicitada para um computador remoto desconhecido. (WSAEHOSTUNREACH).
10066	(WSAENOTEMPTY).
10067	Excedeu o limite de processos. (WSAEPROCLIM).
10068	(WSAEUSERS).
10069	(WSAEDQUOT).
10070	(WSAESTALE).
10071	(WSAEREMOTE).
10091	Subsistema de rede não está disponível. (WSASYSNOTREADY).
10092	Versão da winsock.dll não é suportada.

	(WSAVERNOTSUPPORTED).
10093	A winsock não foi iniciada. (WSANOTINITIALISED).
10101	O comando de shutdown está em andamento. (WSAEDISCON)
10801	A alocação de memória de controle falhou.
10805	A criação da semáfora de controle da recepção falhou.
10806	A criação da semáfora de controle do término da recepção falhou.
10807	A alocação do buffer de recepção falhou.
10808	A alocação do buffer de transmissão falhou.
10809	Identificador da conexão já foi liberado ou está inválido.
10811	A biblioteca de comunicação RAS não carregou corretamente.
10822	A conexão já foi encerrada.
10830	A configuração do modo de comunicação está inválida.
10831	O endereço do computador remoto não foi configurado.
10900	A compressão dos dados não foi concluída com sucesso.
10901	A descompressão dos dados não foi concluída com sucesso.

Códigos de erro da interface de comunicação TCP/IP (Criptografia Nativa):

Código	**Descrição**
18001	A execução da criptografia não foi concluída com sucesso.
18002	A execução da de-criptografia não foi concluída com sucesso.
18003	A importação da chave pública não foi concluída com sucesso.
18004	A exportação da chave de sessão não foi concluída com sucesso.
18005	A importação da chave de sessão não foi concluída com sucesso.
18006	A criação do contexto de criptografia não foi concluída com sucesso.
18007	A geração da chave pública não foi concluída com sucesso.
18008	A geração da chave de sessão não foi concluída com sucesso.
18009	A exportação da chave pública não foi concluída com sucesso.
18900	O tempo limite de negociação das chaves expirou.
18901	A negociação das chaves foi cancelada.
18902	Falha interna.

Códigos de erro da interface de comunicação TCP/IP (Proxy):

Código	Descrição
19001	O servidor informou um erro geral. (SOCKS5)
19002	A conexão com o endereço solicitado está bloqueada. (SOCKS5)
19003	A rede não foi encontrada. (SOCKS5)
19004	O endereço solicitado não foi encontrado. (SOCKS5)
19005	A Solicitação de conexão foi recusada. (SOCKS5)
19006	O TTL expirou. (SOCKS5)
19007	O comando solicitado não é suportado. (SOCKS5)
19008	O tipo de endereço não é suportado. (SOCKS5)
19091	A solicitação foi rejeitada ou falhou. (SOCKS4)
19092	A solicitação foi rejeitada porque o servidor SOCKS não conseguiu comunicar com o identd. (SOCKS4)
19093	A solicitação foi rejeitada porque o servidor SOCKS não conseguiu comunicar com o identd. (SOCKS4)
19256 a 19399	A autenticação do usuário não foi aceita. (SOCKS5)
19401	A solicitação foi recusada pelo proxy. (HTTP)
19403	O usuário/senha não foi autenticado. (HTTP)
19512	A versão informada não é suportada. (SOCKS4, SOCKS5)
19513	O método de autenticação solicitado não é suportado. (SOCKS5)
19514	O tempo limite de resposta expirou. (SOCKS4, SOCKS5, HTTP)
19515	Falha interna.

Códigos de erro da interface de comunicação TCP/IP (Criptografia SSL3):

Código	Descrição
20001	A negociação do protocolo SSL3 não foi concluída com seucesso.
20002	O protocolo está aguardando uma leitura.
20003	O protocolo está aguardando uma escrita.
20004	O protocolo está aguardando verificação do certificado (X509).
20005	O protocolo reportou um erro na pilha TCP/IP.

20006	O protocolo está em operação.
20007	O protocolo está aguardando um comando de CONNECT.
20008	O protocolo está aguardando um comando de ACCEPT.

Códigos de erro da interface de comunicação X.25:

Código	Descrição
15001	Erro interno do sistema.
15002	Erro interno do sistema.
15004	Erro interno do sistema.
15005	O link de comunicação não está ativo.
15007	A rede enviou um reset, então verifique se o sinal 104 no modem está ligado, caso contrário entre em contato com provedor da rede.
15008	Comando para interface X.25 inválido.
15009	Todos os canais lógicos do circuito estão ocupados.
15010	A operação desejada não pode ser realizada.
15014	O nível 2 do X.25 não está ativo.
15015	O número de transmissões ou recepções pendentes excedeu o limite máximo das filas internas do X.25.
15016	Foi recebido um pacote de confirmação de CLEAR em resposta a um RESET.
15017	Chegou uma mensagem com o tamanho maior do que o buffer especificado na aplicação.
15018	Foi recebida uma mensagem com o bit qualificado ligado, porém isto não afeta na utilização da aplicação.
15019	O usuário enviou uma desconexão para o remoto.
15020	O assinante chamado solicitou a desconexão ou o reinício.
15021	Todos os canais lógicos do número chamado estão ocupados.
15022	Recebeu uma desconexão do remoto, após a conexão ter sido estabelecida.
15023	Não existe esta facilidade.

15025	A rede está congestionada. Tente mais tarde.
15029	O número chamado está fora de serviço.
15031	O número chamado pertence a um grupo fechado.
15033	O número chamado não existe.
15037	Recebeu uma desconexão do remoto.
15039	A rede detectou um erro de procedimento do assinante local.
15041	RPOA desconectado.
15045	O número chamado não aceita uma chamada a cobrar.
15053	O número chamado não é válido.
15061	Esta facilidade não foi contratada.
15070	O usuário enviou um reset.
15073	Recebeu um reset do remoto.
15075	A rede detectou um erro do assinante local.
15077	A rede está congestionada. Tente mais tarde.
15079	O número chamado está fora do ar.
15085	A rede enviou um reset.
15087	O número chamado não é válido.
15090	Não respondeu a uma conexão.
15091	Foi enviado um reinício.
15092	Não respondeu a um comando de reset.
15093	Não respondeu a um comando de interrupção.
15094	Não foi possível alocar memória para dicionário de compressão para recepção.
15095	Não foi possível alocar memória para dicionário de compressão para transmissão.
15099	O número chamado está fora de serviço.
15801 á 15808	Erro interna na APIX25
15809	Comunicação encerrada pelo remoto.
15902	Erro no encapsulamento do pacote.

Códigos de erro da interface de comunicação Serial:

Código	Descrição
17601	Não há memória disponível
17602	Erro interno.
17603	Erro na abertura da porta serial
17604	Acesso à porta serial não é permitido
17605	Porta serial não encontrada
17606	Erro na configuração da porta serial
17607	Erro na porta serial ao receber
17608	Erro na porta serial ao enviar
17631	Não há número para discar
17632	Não foi informado o endereço (DTE) para conexão
17633	Erro de alocação de memória
17634	Comando de modem inválido (ERROR)
17635	Modem ocupado (BUSY)
17636	Modem sem portadora (NO CARRIER)
17637	Modem sem tom de discagem (NO DIAL TONE)
17638	Modem recebendo chamada (RING)
17639	Excedeu tempo limite de espera por uma resposta do modem.
17640	Porta serial inválida, cabo não conectado ao modem, qualquer reposta inválida do PAD ou do modem.
17661	Clear recebido do remoto
17662	Comando do PAD inválido
17663	RESET enviado pelo PAD
17664	PAD já conectado (ENGAGED)
17665	Excedeu tempo limite de espera por uma resposta do PAD.
17671	Queda dos sinais do MODEM. Não é possível transmitir ou receber.
17672	PAD não ativo. Não é possível transmitir ou receber.
17673	Processo cancelado pelo usuário.

Códigos de eventos gerados no arquivo de mensagens:

Código	Nível Evento	Descrição
MSG0001	1	Erro ao configurar conversao de caracteres
MSG0002	1	Erro ao configurar conversao de caracteres
MSG0003	1	Erro arquivo duplicado
MSG0004	1	Erro ao eliminar o arquivo
MSG0005	7	NAO DEFINIDA
MSG0006	1	Erro ao eliminar o arquivo
MSG0007	7	Verificado restart para arquivo de recepção
MSG0008	1	Erro nao foi possivel criar o objeto ODETTE
MSG0009	1	Erro na alocacao do UCB para usuário
MSG0010	7	Excedido o limite de '%d' conexoes para o usuário
MSG0011	7	Arquivo ja esta sendo transmitido
MSG0012	1	Erro ao abrir diretorio de pendências
MSG0013	1	Erro ao eliminar arquivo da area de pendência
MSG0014	1	Erro ao mover arquivo para area de backup
MSG0015	1	Erro ao configurar parametros de transmissao maxrecsize
MSG0016	7	NAO DEFINIDA
MSG0017	1	Erro ao configurar conversao de caracteres
MSG0018	1	Erro ao obter o tamanho do arquivo
MSG0019	4	Inicio de transmissão
MSG0020	1	Erro no formato do timestamp
MSG0021	1	Fim de transmissao com erro
MSG0022	1	Erro excedido tamanho do nome do arquivo
MSG0023	1	Fim de transmissao com erro
MSG0024	1	Fim de transmissao com erro
MSG0025	1	Erro na confirmacao de pendencia do arquivo
MSG0026	4	Transmissão confirmada com sucesso
MSG0027	1	Erro na execucao da linha de comando
MSG0028	1	Fim de transmissao com erro

MSG0029	1	Erro ao criar referencia na area de pendencia
MSG0030	1	Erro ao eliminar o arquivo
MSG0031	4	Fim de transmissao com sucesso
MSG0032	7	Arquivo não encontrado na area de pendencia
MSG0033	7	NAO DEFINIDA
MSG0034	1	Erro na execucao da linha de comando
MSG0035	4	Inicio de recepção
MSG0036	1	Fim de recepcao com erro
MSG0037	1	Erro ao remover arquivo
MSG0038	1	Erro ao mover arquivo
MSG0039	4	Fim de recepcao com sucesso
MSG0040	1	Erro na execucao da linha de comando
MSG0041	7	Inicio do processo de cancelamento das conexoes"
MSG0042	1	Erro no processo de cancelamento das conexao"
MSG0043	0	Fim do serviço
MSG0044	0	Inicio do servico
MSG0045	1	Erro na alocacao de memoria para usuários
MSG0046	4	Inicio do login do servidor
MSG0047	1	Erro ao fazer o login do servidor
MSG0048	4	Sucesso no login do servidor
MSG0049	7	Verificado diretorio de saida do usuario
MSG0050	7	NAO DEFINIDA
MSG0051	7	NAO DEFINIDA
MSG0052	1	Erro ao configurar o objeto ODETTE
MSG0053	1	Erro nos parametros extras do objeto ODETTE
MSG0054	1	Erro ao tentar conexao remota
MSG0055	4	Inicio de conexao sainte
MSG0056	1	Erro de conexao sainte
MSG0057	7	Inicio da thread de conexao sainte
MSG0058	1	Erro usuario esta bloqueado para conexão
MSG0059	1	Erro ao configurar a conversao de caracteres
MSG0060	1	Fim de conexao sainte com erro

MSG0061	1	Erro acesso rejeitado no logon local para conexao sainte
MSG0062	1	Fim de conexao sainte com erro
MSG0063	4	Inicio de sessao sainte
MSG0064	4	Fim de sessao sainte
MSG0065	4	Fim de conexao sainte
MSG0066	4	Fim da thread de conexao sainte
MSG0067	7	NÃO DEFINIDA
MSG0068	7	NÃO DEFINIDA
MSG0069	7	NÃO DEFINIDA
MSG0070	8	Verificando agenda automática
MSG0071	1	Erro falha na criacao da thread (stcpSchedService)
MSG0072	7	Lendo arquivo de configuracao
MSG0073	7	NAO DEFINIDA
MSG0074	1	Erro na abertura do arquivo de log
MSG0075	7	Usuario XX autenticado para monitoracao
MSG0076	1	Erro usuario XX nao foi autenticado para monitoracao
MSG0077	1	Erro na recepcao de monitoração
MSG0078	1	Erro timeout na recepcao de monitoracao
MSG0079	1	Cancelamento ou erro ao aguardar conexao de monitoracao
MSG0080	7	Inicio de conexao de monitoracao
MSG0081	7	Fim de conexao de monitoração
MSG0082	7	Inicio da thread de monitoracao
MSG0083	7	Fim da thread de monitoração
MSG0084	1	Erro ao configurar o objeto ODETTE
MSG0085	1	Erro nos parametros extra do objeto ODETTE
MSG0086	1	Cancelamento ou erro ao aguardar conexao
MSG0087	7	Inicio de conexao entrante
MSG0088	1	Erro acesso rejeitado usuario ja esta conectado
MSG0089	1	Erro acesso rejeitado usuario esta bloqueado
MSG0090	1	Erro ao configurar o objeto ODETTE

MSG0091	1	Erro ao configurar a conversao de caracteres
MSG0092	1	Erro acesso rejeitado no logon local para conexao entrante
MSG0093	7	NAO DEFINIDA
MSG0094	7	Inicio de sessao entrante
MSG0095	7	Fim de sessao entrante
MSG0096	7	Fim de conexao entrante
MSG0097	7	Inicio da thread conexao entrante
MSG0098	1	Fim de conexao entrante com erro
MSG0099	7	Fim da thread conexao entrante
MSG0100	1	Erro na criacao do evento para processo assíncrono
MSG0101	7	NAO DEFINIDA
MSG0102	1	Erro na alocacao de UCB para rede
MSG0103	1	Erro na criacao da thread (stcpSrvServer)
MSG0104	1	Fim de conexao entrante com erro
MSG0105	1	Erro acesso rejeitado usuario nao cadastrado
MSG0106	1	Erro acesso rejeitado usuario XX invalido
MSG0107	1	Erro na alocacao de memoria para nome do arquivo de debug
MSG0108	1	Erro na abertura do arquivo de debug
MSG0109	7	Fim do processo de cancelamento das conexoes
MSG0110	1	Erro arquivo de configuracao CTCP.INI/CTCP.AUX nao existe
MSG0111	7	Iniciado agenda automatica 'xx' usuario 'xx' modo 'xx' sessoes 'xx' filtro 'xx' comando 'xx'
MSG0112	1	Erro conexao automatica nao esta habilitada
MSG0113	0	Configuracao '%s' maximo de sessoes '%d'
MSG0114	0	Versao de Demonstracao com limite de '%d' sessoes simultaneas
MSG0115	1	Erro nome do arquivo invalido
MSG0116	1	Erro ao abrir diretorio de saida 'xx' do usuario 'xx'
MSG0117	1	Erro ao abrir diretorio de saida 'xx'
MSG0118	1	Erro ao abrir diretorio de formato 'xx'

MSG0119	1	Erro recepcao do arquivo 'xx' bloqueado pelo filtro
MSG0120	1	Erro recepcao do arquivo 'xx' bloqueado pelo tamanho
MSG0121	1	Erro na execucao da linha de comando 'xx' da agenda
MSG0122	1	Erro ao compilar expressao regular(regex) '%s'
MSG0123	1	Erro transmissao do arquivo 'xx' bloqueado pelo filtro
MSG0124	1	Erro transmissao do arquivo 'xx' bloqueado pelo tamanho
MSG0125	1	Erro conexao bloqueada 'xx' pelo filtro
MSG0126	1	Erro acesso rejeitado usuario nao cadastrado
MSG0127	1	Erro na execucao da linha de comando '%s'
MSG0128	1	Erro na execucao da linha de comando
MSG0129	1	Nao foi possivel carregar o Configurador
MSG0130	1	NÃO DEFINIDA
MSG0131	1	Erro ao modificar senha para 'xx', usuario ou senha invalida
MSG0132	1	Erro comando nao definido
MSG0133	1	Erro parametros inválidos
MSG7001	1	Erro quantidade de parametros insuficientes
MSG7002	1	Erro nome do arquivo invalido
MSG7003	1	Erro arquivo de regras 'xx' nao tem definicao para arquivo
MSG7004	1	Erro servico de log nao foi aberto
MSG7005	1	Erro regra 'xx' com parametro invalido no arquivo
MSG7006	7	Inicio STCPREN para arquivo
MSG7007	1	Erro ao copiar o arquivo 'xx' para 'yy'
MSG7008	4	Copia do arquivo 'xx' para 'yy' destino 'zz'
MSG7009	4	Copia do arquivo 'xx' para 'yy' origem 'zz'"
MSG7010	1	Erro ao remover o arquivo 'xx'
MSG7011	1	Erro ao executar o comando
MSG7012	1	Erro ao executar o comando

MSG7013	1	Erro ao conectar recurso
MSG7014	1	Erro ao desconectar recurso

5) Segurança

Como é a segurança do STCP OFTP?

O STCP OFTP implementa a segurança em dois níveis: autenticação do usuário pela aplicação e a criptografia dos dados.

Autenticação do usuário pela aplicação (ODETTE ID)?

A autenticação do usuário é realizada pela aplicação através do reconhecimento de um usuário com até 26 (vinte e seis) caracteres e senha com até 8 (oito) caracteres antes do início da transferência.

Criptografia?

Criptografia é a codificação dos dados com o objetivo de proteger o seu conteúdo das pessoas indesejadas. Os algoritmos matemáticos usados para proteger os dados são chamados de codificadores.

Existem dois tipos de codificadores: assimétricos (chave pública) e simétricos (convencionais).

Os codificadores assimétricos operam com um par de chaves: pública e privada. A chave que codifica os dados não é a mesma que decodifica.

Os codificadores simétricos utilizam uma única chave. A chave que codifica os dados é a mesma que decodifica.

Os codificadores simétricos são mais rápidos do que os assimétricos e por isso são utilizados para codificar grandes volumes de dados, porém os assimétricos servem para manter a privacidade durante a troca das chaves simétricas e a assinatura digital.

Message Digests (sumário da mensagem)?

A representação de uma mensagem de tamanho variável em uma mensagem pequena de tamanho fixo é chamada de 'hash' ou 'Message Digests' (Sumário da Mensagem).

Os algoritmos de 'hash' foram desenhados de maneira a produzirem uma representação única para cada mensagem e tornar extremamente difícil o processo de reconstrução da mensagem a partir do seu 'hash'. É impossível diferentes mensagens produzirem o mesmo 'hash'.

Assinatura Digital?

A Assinatura Digital é o processo de codificar o 'hash' de uma determinada mensagem com a chave privativa do emissor. Qualquer um que receba a mensagem digitalmente assinada pode através da chave pública do emissor decodificar o 'hash' e verificar a origem da mesma.

Certificado?

O Certificado é a associação da chave pública com a identificação do seu possuidor (nome do indivíduo, endereço do servidor ou outro) emitido e assinado por uma Autoridade Certificadora (CA).

O Certificado inclui também as informações da autoridade certificadora e o seu período de validade. Adicionalmente mais informações (extensões) podem ser associadas (número de série e outras).

Autoridade Certificadora (CA)?

A Autoridade Certificadora é a empresa responsável pela verificação e processamento das solicitações de certificado (certificate request), emissão e manutenção deles. Estas empresas mantêm uma lista de procedimentos e exigências para garantir a autenticidade do possuidor da chave pública.

É possível a criação de sua própria autoridade certificadora (CA) em geral para utilização dentro da própria rede (Intranet).

Secure Socket Layer (SSL)?

O SSL é uma camada de protocolo para utilização entre a aplicação e a camada de comunicação TCP/IP. O SSL fornece os serviços de comunicação seguro entre a aplicação cliente e servidor, permitindo a mútua autenticação, assinatura digital (integridade) e criptografia (privacidade).

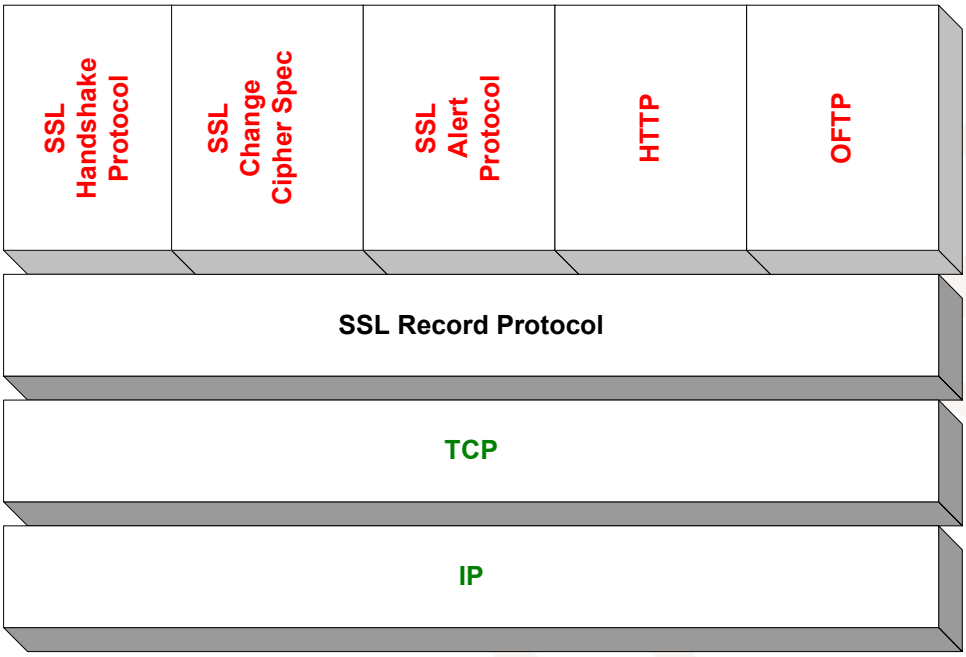


Figura 1 - Arquitetura SSL

O SSL suporta a escolha específica dos algoritmos utilizados para criptografia, 'hash' e assinatura digital. A seleção dos algoritmos entre o cliente e servidor é realizada no estabelecimento da sessão do protocolo.

O SSL tem diferentes versões, a adotada pelo STCP OFTP é a versão 3.0.

Criptografia no STCP OFTP?

O STCP OFTP utiliza a criptografia no nível de transporte onde um túnel seguro é estabelecido entre o cliente e o servidor e todos os dados trafegados são codificados. A escolha do tipo de criptografia: Nativa ou SSL3 é realizada na configuração do produto.

A Criptografia Nativa?

A "criptografia nativa" é uma implementação proprietária de troca de chaves e criptografia dos dados utilizando os algoritmos de chaves simétricas e assimétricas onde as chaves são negociadas dinamicamente. São 3 (três) as opções de configuração para os níveis de criptografia: Normal, Média e Alta, com as seguintes características:

- Normal - Chave assimétrica de 512 bits e chave simétrica de 48 bits
- Média - Chave assimétrica de 1024 bits e chave simétrica de 56 bits
- Alta - Chave assimétrica de 2048 bits e chave simétrica de 128 bits

A criptografia SSL3 no STCP OFTP?

O STCP OFTP inicia o processo de comunicação segura com a solicitação para a camada SSL3 da abertura de uma nova sessão com a troca da chave pública (assimétrica) seguida da troca da chave de sessão (simétrica).

Estes são os passos realizados para a troca de chaves:

1. O cliente solicita a abertura de uma sessão segura com o servidor. O servidor tem um certificado (X.509), contendo a chave pública e uma chave privada.
2. O servidor envia uma cópia do seu certificado contendo a chave pública, para o cliente.
3. O cliente gera uma nova chave simétrica para esta sessão.
4. O cliente codifica a chave de sessão com a chave pública do servidor e envia a chave de sessão codificada para o servidor.
5. O servidor utiliza a sua chave privativa para decodificar a chave de sessão.

O STCP OFTP possibilita a configuração do conjunto de algoritmos para codificação a serem utilizados para criptografia, assinatura digital e hash.

Arquitetura de comunicação do STCP OFTP

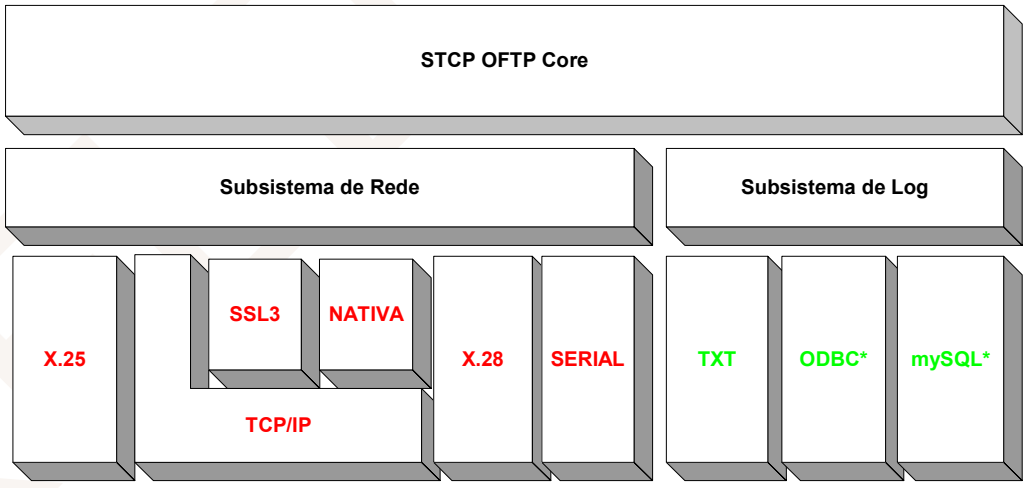


Figura 2 – Arquitetura do STCP OFTP

O STCP OFTP tem uma arquitetura modular e possibilita a configuração de diferentes tipos de comunicação.

Quais os algoritmos suportados na comunicação SSL3?

O STCP OFTP permite a configuração de diferentes algoritmos e grupos de algoritmos para comunicação SSL3, abaixo segue a lista e definições:

Algoritmos	Descrição
ALL	Todos os algoritmos.
HIGH	Codificadores com chave maiores que 128 bits.
MEDIUM	Codificadores com chave de 128 bits.
LOW	Codificadores com chave de 56 ou 64 bits.
EXP EXPORT	Codificadores exportáveis com 40 ou 56 bits.
EXPORT40	Codificadores exportáveis com 40 bits.
EXPORT56	Codificadores exportáveis com 56 bits.
eNULL NULL	Sem codificadores. (não recomendado).
aNULL	Sem autenticação. Corresponde ao algoritmo DH anonymous. Esta configuração é vulnerável ao ataque "man in the middle". (não recomendado).
RSA	Codificadores que utilizam RSA para troca de chave.
kEDH	Codificadores que utilizam EDH (Ephemeral Diffie Helman) para validação da chave.
kDHr	Codificadores que utilizam DH (Diffie Helman) para validação da chave e certificado DH assinado por uma CA com chave RSA.
kDHd	Codificadores que utilizam DH para validação da chave e certificado DH assinado por uma CA com chave DSS.
aRSA	Autenticação RSA com certificado com chave RSA.
aDSS DSS	Autenticação DSS com certificado com chave DSS.
aDH	Autenticação DH com certificado com chave DH.
kFZA aFZA eFZA FZA	Codificadores, autenticação com algoritmo FORTEZZA. (não disponível)
DH	Codificadores DH incluindo o DH anônimo.
ADH	Codificadores DH anônimo.
3DES	Codificadores triple DES.
DES	Codificadores DES (Data Encryption Standard).
RC4	Codificadores RC4.
RC2	Codificadores RC2.
IDEA	Codificadores IDEA.
AES	Codificadores AES (Advanced Encryption Standard)
MD5	MD5
SHA SHA1	SHA1

Conjunto de Algoritmos	Descrição
ADH-AES256-SHA	Troca de chaves = Diffie-Helman Autenticação = Sem Criptografia = AES com 256 bits Mac = SHA1
DHE-RSA-AES256-SHA	Troca de chaves = Diffie-Helman Autenticação = RSA Criptografia = AES com 256 bits Mac = SHA1
DHE-DSS-AES256-SHA	Troca de chaves = Diffie-Helman Autenticação = DSS Criptografia = AES com 256 bits Mac = SHA1
AES256-SHA	Troca de chaves = RSA Autenticação = RSA Criptografia = AES com 256 bits Mac = SHA1
ADH-AES128-SHA	Troca de chaves = Diffie-Helman Autenticação = Sem Criptografia = AES com 128 bits Mac = SHA1
DHE-RSA-AES128-SHA	Troca de chaves = Diffie-Helman Autenticação = RSA Criptografia = AES com 128 bits Mac = SHA1
DHE-DSS-AES128-SHA	Troca de chaves = Diffie-Helman Autenticação = DSS Criptografia = AES com 128 bits Mac = SHA1
AES128-SHA	Troca de chaves = RSA Autenticação = RSA Criptografia = AES com 128 bits Mac = SHA1
DHE-DSS-RC4-SHA	Troca de chaves = DH Autenticação = DSS Criptografia = RC4 com 128 bits Mac = SHA1
EXP1024-DHE-DSS-RC4-SHA	Troca de chaves = DH (1024) Autenticação = DSS Criptografia = RC4 com 56 bits Mac = SHA1
EXP1024-RC4-SHA	Troca de chaves = RSA (1024) Autenticação = RSA Criptografia = RC4 com 56 bits Mac = SHA1
EXP1024-DHE-DSS-DES-CBC-SHA	Troca de chaves = DH (1024) Autenticação = DSS Criptografia = DES com 56 bits Mac = SHA1
EXP1024-DES-CBC-SHA	Troca de chaves = RSA (1024) Autenticação = RSA Criptografia = DES com 56 bits Mac = SHA1
EXP1024-RC2-CBC-MD5	Troca de chaves = RSA (1024) Autenticação = RSA Criptografia = RC2 com 56 bits Mac = MD5
EXP1024-RC4-MD5	Troca de chaves = RSA (1024) Autenticação = RSA Criptografia = RC4 com 56 bits Mac = MD5
EDH-RSA-DES-CBC3-SHA	Troca de chaves = DH Autenticação = RSA Criptografia = 3DES com 168 bits Mac = SHA1

EDH-RSA-DES-CBC-SHA	Troca de chaves = DH Autenticação = RSA Criptografia = DES com 56 bits Mac = SHA1
EXP-EDH-RSA-DES-CBC-SHA	Troca de chaves = DH (512) Autenticação = RSA Criptografia = DES com 40 bits Mac = SHA1
EDH-DSS-DES-CBC3-SHA	Troca de chaves = DH Autenticação = DSS Criptografia = 3DES com 168 bits Mac = SHA1
EDH-DSS-DES-CBC-SHA	Troca de chaves = DH Autenticação = DSS Criptografia = DES com 56 bits Mac = SHA1
EXP-EDH-DSS-DES-CBC-SHA	Troca de chaves = DH (512) Autenticação = DSS Criptografia = DES com 40 bits Mac = SHA1
DES-CBC3-SHA	Troca de chaves = RSA Autenticação = RSA Criptografia = 3DES com 168 bits Mac = SHA1
DES-CBC-SHA	Troca de chaves = RSA Autenticação = RSA Criptografia = DES com 56 bits Mac = SHA1
EXP-DES-CBC-SHA	Troca de chaves = RSA (512) Autenticação = RSA Criptografia = DES com 40 bits Mac = SHA1
IDEA-CBC-SHA	Troca de chaves = RSA Autenticação = RSA Criptografia = IDEA com 128 bits Mac = SHA1
EXP-RC2-CBC-MD5	Troca de chaves = RSA (512) Autenticação = RSA Criptografia = RC2 com 40 bits Mac = MD5
RC4-SHA	Troca de chaves = RSA Autenticação = RSA Criptografia = RC4 com 128 bits Mac = SHA1
RC4-MD5	Troca de chaves = RSA Autenticação = RSA Criptografia = RC4 com 128 bits Mac = MD5
EXP-RC4-MD5	Troca de chaves = RSA(512) Autenticação = RSA Criptografia = RC4 com 40 bits Mac = MD5
ADH-DES-CBC3-SHA	Troca de chaves = DH Autenticação = Sem Criptografia = 3DES com 168 bits Mac = SHA1
ADH-DES-CBC-SHA	Troca de chaves = DH Autenticação = Sem Criptografia = DES com 56 bits Mac = SHA1
EXP-ADH-DES-CBC-SHA	Troca de chaves = DH(512) Autenticação = Sem Criptografia = DES com 40 bits Mac = SHA1
ADH-RC4-MD5	Troca de chaves = DH Autenticação = Sem Criptografia = RC4 com 128 bits

	Mac = MD5
EXP-ADH-RC4-MD5	Troca de chaves = DH(512) Autenticação = Sem Criptografia = RC4 com 40 bits Mac = MD5
NULL-SHA	Troca de chaves = RSA Autenticação = RSA Criptografia = Sem Mac = SHA1
NULL-MD5	Troca de chaves = RSA Autenticação = RSA Criptografia = Sem Mac = MD5

Porque a implementação OpenSSL?

A Riversoft optou pela utilização da implementação do SSL3 OpenSSL na sua linha de produtos por ser esta atualmente uma das mais utilizada no mercado mundial (Apache, Squid, Tivoli, VPN-1, Firewall-1 entre diversos outros produtos) e ao mesmo tempo possibilitar o acesso aos seus códigos fontes pela comunidade internacional.

Adotar as padronizações mundiais OFTP e TLS1/SSL3 é um compromisso da Riversoft para garantir a interoperabilidade do produto STCP OFTP.

Licença OpenSSL

OpenSSL License

```
 * 4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to
 *    endorse or promote products derived from this software without
 *    prior written permission. For written permission, please contact
 *    openssl-core@openssl.org.
 *
 * 5. Products derived from this software may not be called "OpenSSL"
 *    nor may "OpenSSL" appear in their names without prior written
 *    permission of the OpenSSL Project.
 *
 * 6. Redistributions of any form whatsoever must retain the following
 *    acknowledgment:
 *    "This product includes software developed by the OpenSSL Project
 *    for use in the OpenSSL Toolkit (http://www.openssl.org/)"
 *
 * THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT ``AS IS" AND ANY
 * EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO,
THE
 * IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A
PARTICULAR
 * PURPOSE ARE DISCLAIMED.  IN NO EVENT SHALL THE OpenSSL PROJECT OR
 * ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL,
 * SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT
 * NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES;
 * LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
 * HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN
CONTRACT,
 * STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE)
 * ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED
 * OF THE POSSIBILITY OF SUCH DAMAGE.
 *
==========================================================
============
 *
 * This product includes cryptographic software written by Eric Young
 * (eay@cryptsoft.com).  This product includes software written by Tim
 * Hudson (tjh@cryptsoft.com).
 *
 */

 Original SSLeay License
 -----------------------

/* Copyright (C) 1995-1998 Eric Young (eay@cryptsoft.com)
 * All rights reserved.
 *
 * This package is an SSL implementation written
 * by Eric Young (eay@cryptsoft.com).
 * The implementation was written so as to conform with Netscapes SSL.
 *
 * This library is free for commercial and non-commercial use as long as
 * the following conditions are aheared to.  The following conditions
 * apply to all code found in this distribution, be it the RC4, RSA,
 * lhash, DES, etc., code; not just the SSL code.  The SSL documentation
 * included with this distribution is covered by the same copyright terms
```

```
 * except that the holder is Tim Hudson (tjh@cryptsoft.com).
 *
 * Copyright remains Eric Young's, and as such any Copyright notices in
 * the code are not to be removed.
 * If this package is used in a product, Eric Young should be given attribution
 * as the author of the parts of the library used.
 * This can be in the form of a textual message at program startup or
 * in documentation (online or textual) provided with the package.
 *
 * Redistribution and use in source and binary forms, with or without
 * modification, are permitted provided that the following conditions
 * are met:
 * 1. Redistributions of source code must retain the copyright
 *    notice, this list of conditions and the following disclaimer.
 * 2. Redistributions in binary form must reproduce the above copyright
 *    notice, this list of conditions and the following disclaimer in the
 *    documentation and/or other materials provided with the distribution.
 * 3. All advertising materials mentioning features or use of this software
 *    must display the following acknowledgement:
 *    "This product includes cryptographic software written by
 *     Eric Young (eay@cryptsoft.com)"
 *    The word 'cryptographic' can be left out if the rouines from the library
 *    being used are not cryptographic related :-).
 * 4. If you include any Windows specific code (or a derivative thereof) from
 *    the apps directory (application code) you must include an acknowledgement:
 *    "This product includes software written by Tim Hudson (tjh@cryptsoft.com)"
 *
 * THIS SOFTWARE IS PROVIDED BY ERIC YOUNG ``AS IS" AND
 * ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO,
THE
 * IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A
PARTICULAR PURPOSE
 * ARE DISCLAIMED.  IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE
LIABLE
 * FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR
CONSEQUENTIAL
 * DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF
SUBSTITUTE GOODS
 * OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
 * HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN
CONTRACT, STRICT
 * LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN
ANY WAY
 * OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY
OF
 * SUCH DAMAGE.
 *
 * The licence and distribution terms for any publically available version or
 * derivative of this code cannot be changed.  i.e. this code cannot simply be
 * copied and put under another distribution licence
 * [including the GNU Public Licence.]
 */
```

Referências

www.openssl.org

www.modssl.org

http://oss-institute.org/newspdf/OSSIFIPSRef.pdf

www.odette.org

www.oftp.net