



TOTVS

Guia de Instalação – TOTVS Segurança e Acesso 11.6.7

10/2013

Sumário

1. Prefácio	3
1.1. Finalidade	3
1.2. Público Alvo	3
1.3. Organização deste Guia	3
1.4. Documentações Importantes	4
2. Introdução	5
2.1. Arquitetura Distribuída do Produto	5
2.2. Tipos de Instalação	5
3. Requisitos Básicos	6
3.1. Visão Geral dos Requisitos	6
3.2. Requisitos de Hardware	7
3.2.1. Requisitos para estação cliente	7
3.2.2. Requisitos para servidor	8
3.3. Requisitos de Dispositivos (Controle de Acesso e Ponto Eletrônico)	8
3.4. Requisitos de Software	9
3.4.1. SQL Server	9
3.4.2. Oracle	9
3.4.3. Progress	9
3.4.4. Java	10
3.5. Requisitos de Usuário (Servidor)	10
4. Instalação	11
4.1. Detalhes da Mídia de Instalação	11
4.2. Planejando a Instalação	11
4.3. Instalação do Servidor de Aplicação	11
4.3.1. Objetos Criados na Instalação do Servidor de Aplicação	21
4.4. Instalação de Banco de Dados	22
4.5. Inicializando o TOTVS Segurança e Acesso	22
4.6. Acesso ao TOTVS Segurança e Acesso	22
5. Reinstalação	23
6. Desinstalação	24

1. Prefácio

1.1. Finalidade

Este guia tem como finalidade descrever de forma objetiva os procedimentos necessários para a instalação do produto TOTVS Segurança e Acesso 11.6, bem como configurar o produto nas plataformas suportadas.

1.2. Público Alvo

Por este processo de instalação ser complexo, a instalação requer pessoas que tenham conhecimentos da arquitetura do Java, JBoss e ambiente de rede.

1.3. Organização deste Guia

Capítulo 2, “Introdução”

Este capítulo apresenta uma visão geral da arquitetura distribuída, tipos de instalação e exemplos de topologias no uso do produto.

Capítulo 3, “Requisitos”

Este capítulo apresenta a lista de requisitos básicos de hardware e software exigidos na instalação e configuração do produto.

Capítulo 4, “Instalação”

Este capítulo descreve os procedimentos que deverão ser executados para a instalação do produto. Abrange desde o planejamento da instalação, ou seja, escolher o tipo de instalação adequado, até as configurações necessárias para acesso remoto.

Capítulo 5, “Reinstalação”

Este capítulo descreve os procedimentos a serem executados para a reinstalação do TOTVS Segurança e Acesso, bem como os cuidados necessários para a execução dessa rotina.

Capítulo 6, “Desinstalação”

Este capítulo descreve os procedimentos necessários para a desinstalação do TOTVS Segurança e Acesso.

1.4. Documentações Importantes

Manuais JBoss

- ✓ Installation Guide;
- ✓ Getting Started Guide;
- ✓ Server Configuration Guide.

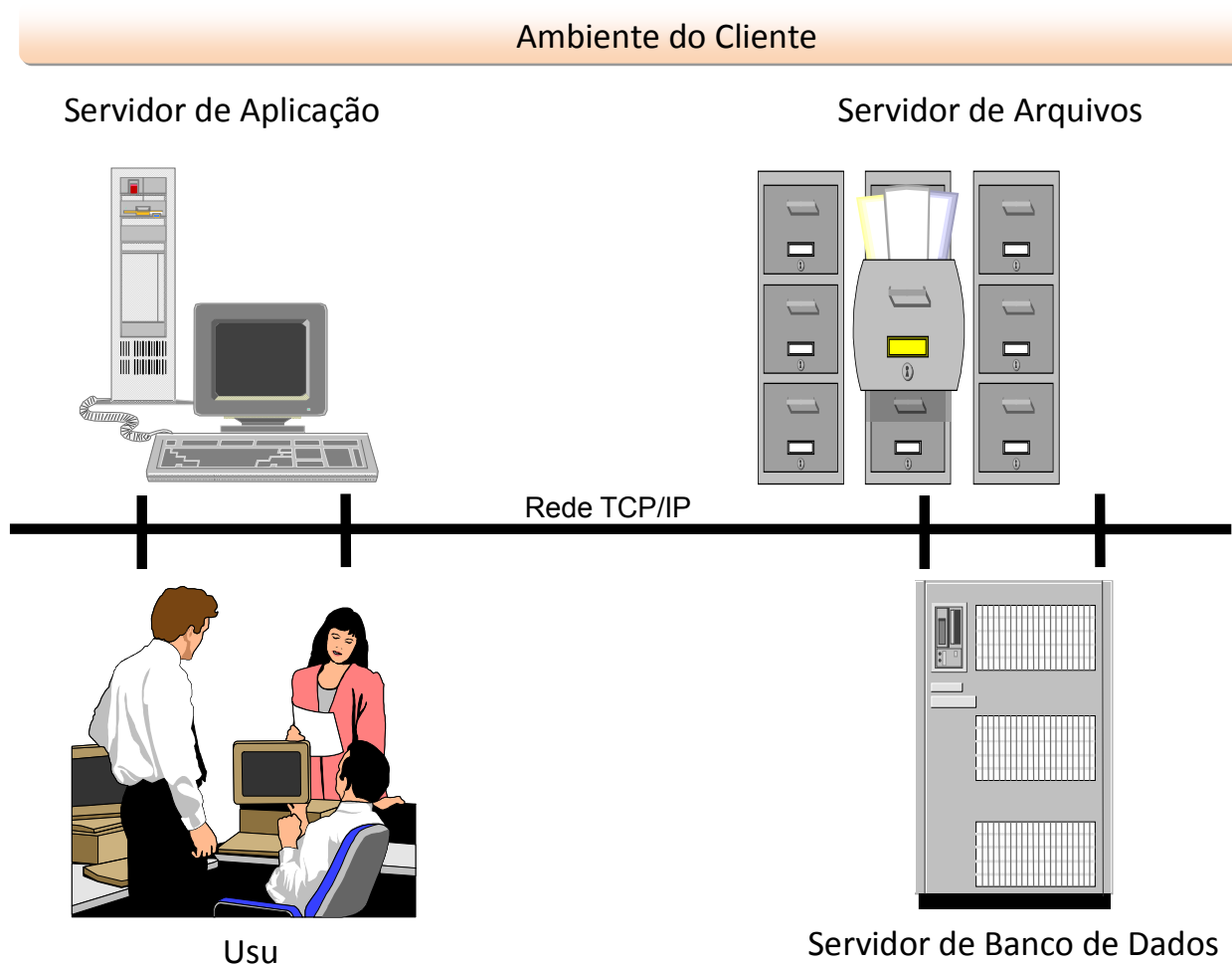
Estas e outras documentações podem ser obtidas em [JBoss AS Documentation](#) e [JBoss Wiki](#).

2. Introdução

2.1. Arquitetura Distribuída do Produto

A arquitetura distribuída consiste em separar os componentes em plataformas independentes que interagem entre si, permitindo que os recursos sejam compartilhados enquanto se obtém ao máximo os benefícios de cada dispositivo. Basicamente, funciona da seguinte forma: as máquinas dos usuários estarão conectadas aos servidores pela rede e cada servidor fornecerá recursos diferentes para que os programas possam ser executados da máquina do usuário.

A figura abaixo mostra os quatro componentes básicos utilizados pelo produto.



2.2. Tipos de Instalação

Para o funcionamento do produto, é necessário executar os procedimentos de Bancos de Dados e a instalação do Servidor de Aplicação:

- ✓ Servidor de Aplicação

Instala e configura o JBoss e o Java, assim como o TOTVS Segurança e Acesso, sendo esses componentes essenciais para o funcionamento do produto.

- ✓ Banco de Dados

Procedimentos para configurar os bancos de dados utilizados pelo produto.



ATENÇÃO: Esta mídia é preparada para instalar várias instâncias do produto TOTVS Segurança e Acesso no mesmo servidor. Este procedimento consiste em instalar múltiplas cópias das opções de Banco de Dados e Servidor de Aplicação, respeitando o limite máximo de quatro instâncias. Cada instância instalada será nomeada com base na porta principal utilizada pelo JBoss, seguindo a sequência 8080, 8180, 8280 e 8380. Cada instância deverá ser instalada em um caminho independente.

3. Requisitos Básicos

Este capítulo tem como objetivo divulgar recomendações sobre o uso de hardware e software relacionados ao TOTVS Segurança e Acesso.

As recomendações e exemplos citados adiante levam em consideração somente os softwares relacionados ao TOTVS Segurança e Acesso e softwares de uso genérico, como Office e e-mail. Caso sejam instalados outros softwares no mesmo ambiente, eles devem ser levados em consideração, sendo que os requisitos descritos podem não ser o suficiente para a execução de todas as rotinas.

As versões homologadas de software, banco de dados, sistema de gestão de pessoas (Datasul, Protheus ou RM) e a *firmware* dos dispositivos são exatamente as citadas abaixo. Qualquer item que seja utilizado com alguma versão diferente das citadas não é considerado homologado, podendo prejudicar a execução das rotinas do produto.

3.1. Visão Geral dos Requisitos

Para dar início ao processo de atualização para o Datasul, o sistema deve obedecer a versão de pacote de origem (entre parênteses) suportado pela atualização, conforme definições da tabela a seguir:

Servidor	
30 equipamentos	
Hardware (mínimo)	
Disco	100 GB disponíveis
Memória	6 GB disponíveis
Processador	Intel Core i5 3.00 GHz (ou compatível) 64 Bits
Banda de Dados	100 Mbps
Software	

Java	JRE 6u37 64 Bits (embutido na instalação). Java 7 (ou superior) não está homologado.
Sistema Operacional	Windows ou Linux (verificar compatibilidade dos softwares de integração do fabricante do equipamento)
Bancos de Dados	
Oracle	10g R1, 10g R2, 11g R1, 11g R2
Microsoft SQL Server	2005, 2008 R2
Informix	10, 11.5
DB2	9.1, 9.5, 9.7
MySQL	5.1

Sistema de Gestão de Pessoas

Sistema de Gestão de Pessoas (Sistema Externo)

Datasul HCM	11.2.2
Protheus 10	10.x.x, serie-3
Protheus 11	11.1.x, serie-3
Logix 10	10.2.x
RM Chronus 11	11.50.0

Estação Client

Windows / Linux

Hardware

Memória	1 GB
Processador	1.00 GHz
Resolução de Tela	1024 x 768 ou superior

Software

Navegadores	Internet Explorer 8 Firefox 3.6 Chrome 10
Webcam	Deverá possuir o plugin da Macromedia Flash instalado e uma Webcam compatível com o flash.

3.2. Requisitos de Hardware

3.2.1. Requisitos para estação cliente

É necessário que a estação cliente possua o sistema operacional Windows ou Linux instalado.

Não recomendamos o uso de estações menores que o mínimo acima citado, pois o desempenho não atenderá às necessidades dos usuários.

Para todos os casos recomendamos a utilização de placas de rede de fornecedores de primeira linha.

3.2.2. Requisitos para servidor

A configuração acima é para servidor dedicado, não recomendamos que o servidor dos aplicativos de integração com os dispositivos seja compartilhado com alguma outra aplicação. Pelo fato da comunicação com os equipamentos ser *real-time*, a execução de outros aplicativos no mesmo servidor poderá gerar lentidão na liberação dos acessos.

3.3. Requisitos de Dispositivos (Controle de Acesso e Ponto Eletrônico)

Abaixo são exibidos os equipamentos suportados pelo software TOTVS Segurança e Acesso. As versões homologadas são somente as citadas abaixo. Caso seja lançada uma nova versão de *firmware* de qualquer dispositivo, esta não é homologada e não deve ser usada antes que seja verificada sua compatibilidade com o produto.

Caso tenha a necessidade de solicitar a homologação de um novo *firmware*, por favor, abra um chamado com a equipe de atendimento.

Controle de Acesso		
Fabricante	Modelo	Firmware
Dimep	Todos os modelos compatíveis com a versão de firmware homologada.	Biopoint: 2.16 Micropoint: 3.2, 3.6
Henry	Todos os modelos do protocolo 7.x compatíveis com a versão de firmware homologada.	7101
Telemática	Todos os modelos compatíveis com o software da Telemática Conex (que operem com a tabela MATCODIN e que não possuam ARLON).	*
TopData	Linha de produto Inner Net e Inner Plus	Inner Net: 2.03 Inner Plus: 8.58, 9.0.2



ATENÇÃO: Todos os dispositivos, independente de fabricante, devem ter funcionamento ON-LINE e REAL TIME.

Ponto Eletrônico (Portaria 1.510/2009)		
Fabricante	Modelo	Firmware
Dimep	Todos os modelos compatíveis com as versões de firmware homologadas.	REP 48 01.00.0002 REP 48 02.04.0000
	Este fabricante possui equipamentos para a Portaria 373/11 do MTE.	
Madis	Todos os modelos compatíveis com as versões de firmware homologadas.	REP 48 01.00.0002 REP 48 02.04.0000
	Este fabricante possui equipamentos para a	

Telemática	Portaria 373/11 do MTE. Todos os modelos compatíveis com o software da Telemática (CONEX REP)	CONEX REP 01.00.01A
------------	--	---------------------



ATENÇÃO: Todos os dispositivos devem estar homologados na Portaria 1.510/2009 (<http://portal.mte.gov.br/pontoeletronico/rep-registrados-no-mte.htm>).

3.4. Requisitos de Software

Recomenda-se criar um usuário específico para o produto TSA para configuração do sistema. Apenas para o banco de dados Progress, no qual deverá ser utilizado o usuário “pub”.

3.4.1. SQL Server

Deverá ser configurada uma porta fixa para a instância nomeada. Essa porta deverá ser fornecida no processo de instalação do Segurança e Acesso TOTVS descrito no capítulo “**4.3 Instalação do Servidor de Aplicação**”.

Recomendamos que a collation do banco “tsa” e do banco do “sistema externo” seja CASE-INSENSITIVE: Latin1_General_CI_AI, sem restrição de maiúsculo e minúsculo e sem restrição de acentos.

3.4.2. Oracle

É necessário criar um usuário para o TOTVS Segurança e Acesso (TSA) e utilizar esse usuário para efetuar a carga das tabelas/dados no capítulo “**4.4 Instalação de Banco de Dados**”.

3.4.3. Progress

O sistema TOTVS Segurança e Acesso (TSA) poderá utilizar apenas o banco de dados do Datasul, sendo o banco de dados do sistema externo.

Sistema Externo: Sistema de gestão de pessoas (Datasul, Protheus, RM ou Logix). Quando Datasul será o banco de dados **HCM**.

Para esse banco de dados é necessário efetuar a criação do broker SQL e a criação dos usuários sysprogress e pub, ambos com permissão de DBA, conforme passos descritos abaixo:

- ✓ Criar o usuário “sysprogress”, senha “sysprogress” e o usuário “pub”, senha “pub” pelo “Admin > Security > Edit User List”;
- ✓ Fechar a sessão Progress e carregar o banco com um broker SQL:

```
proserve <banco> -S <porta> -N TCP -H <nome servidor banco> <parâmetros>
```

```
proserve <banco> -S <porta> -N TCP -H <nome servidor banco> -m3 -ServerType SQL
<parâmetros>
```

- ✓ Acessar um computador cliente windows com Progress instalado;
- ✓ Acessar o “proenv” do Progress em “Iniciar > Programas > Progress > Proenv”;



DICA: A porta do broker é a porta definida para o parâmetro “-S” ao carregar o banco com o parâmetro “-ServerType SQL”.

3.4.4. Java

O instalador disponibiliza automaticamente o Java na versão homologada com o sistema. Em nenhuma hipótese o Java deve ser atualizado. O TSA não está homologado com a versão Java 7 (nem superiores).

Todos os serviços necessários pelo TSA são configurados utilizando o Java disponibilizado na mídia de instalação.

O Java disponibilizado na mídia de instalação é a versão “**JRE 1.6.0_45 64 Bits**”. A localização do Java será: %TSA_HOME%\jre.

3.5. Requisitos de Usuário (Servidor)

Recomenda-se que a instalação do produto TSA seja efetuada com o usuário “administrador”, ou com um usuário que esteja incluso no grupo de administradores do servidor.

4. Instalação

4.1. Detalhes da Mídia de Instalação

A mídia de instalação do TOTVS Segurança e Acesso são disponibilizados em DVD e pelo [Portal do Cliente](#). Nesta mídia estão disponíveis:

- ✓ Guia de Instalação do produto.
- ✓ Setup e arquivos necessários para instalação do produto.

4.2. Planejando a Instalação

Mostraremos agora as etapas que devem ser seguidas para a instalação e configuração do TOTVS Segurança e Acesso 11.6.

- ✓ Defina a topologia do ambiente. Nesta etapa, deve ser definido onde cada componente será instalado. Escolha o hardware que será utilizado como servidor de banco de dados, servidor de arquivos, servidor de aplicação e também as máquinas que estarão disponíveis aos usuários. Para cada um destes componentes, verifique se os requisitos de hardware e software são atendidos.
- ✓ Instale os bancos de dados.
- ✓ Instale o servidor de aplicação.

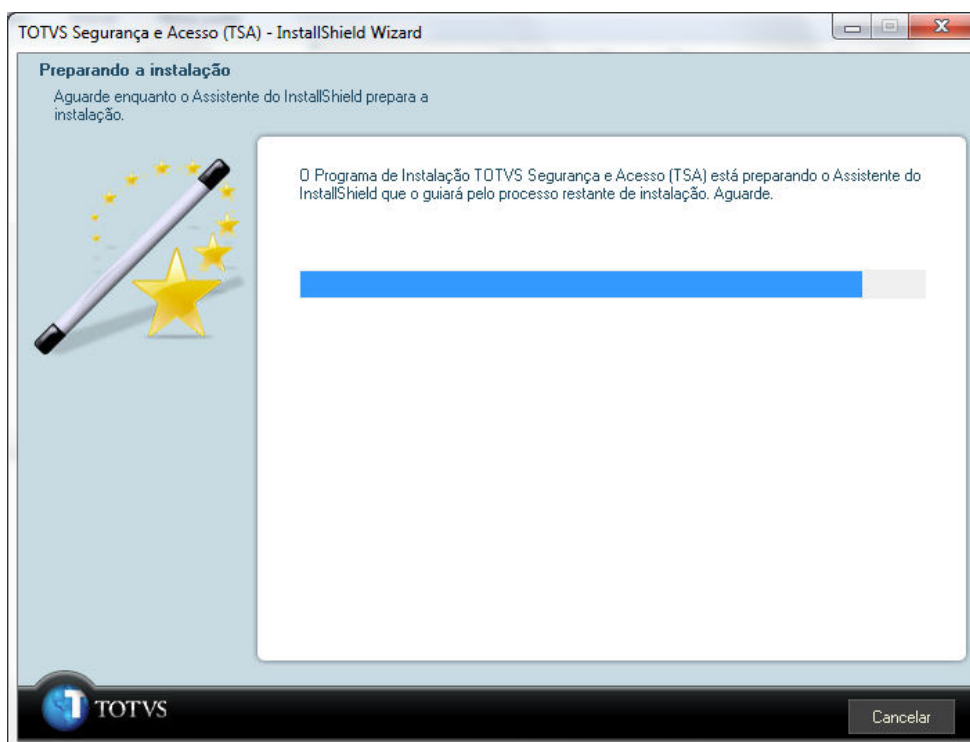
A mídia só faz uma instalação dos bancos e servidor de aplicação de uma vez só.

- ✓ Carregue os bancos de dados utilizando os scripts.

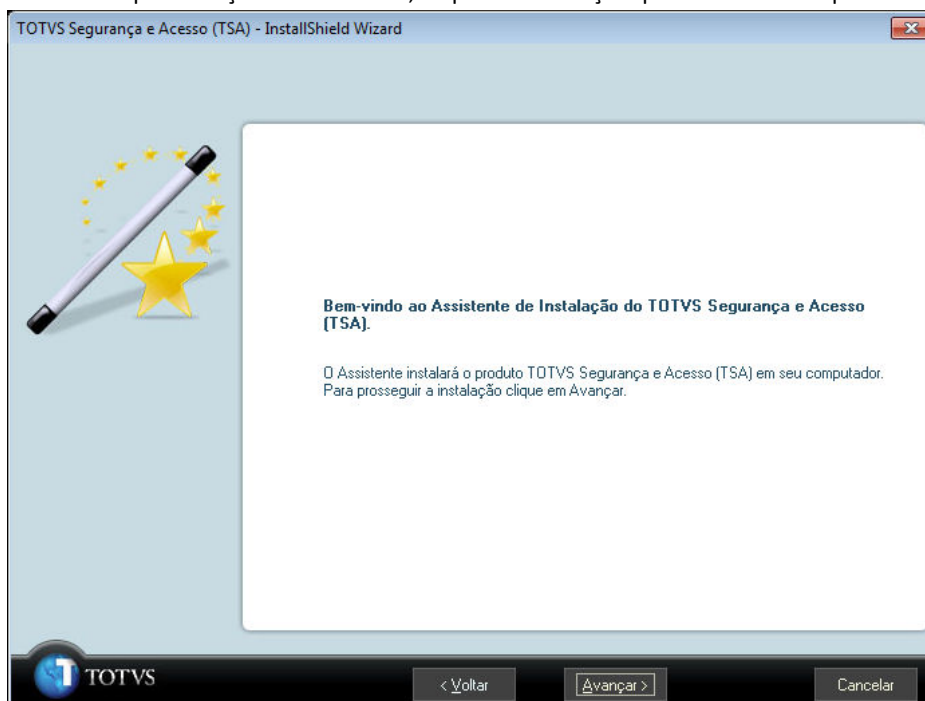
Inicie o JBoss através do serviço “**TOTVS Controle de Acesso (TSA) - 8080**” criado no “Services” do Windows. Após a conclusão destas etapas, o produto estará pronto para utilização.

4.3. Instalação do Servidor de Aplicação

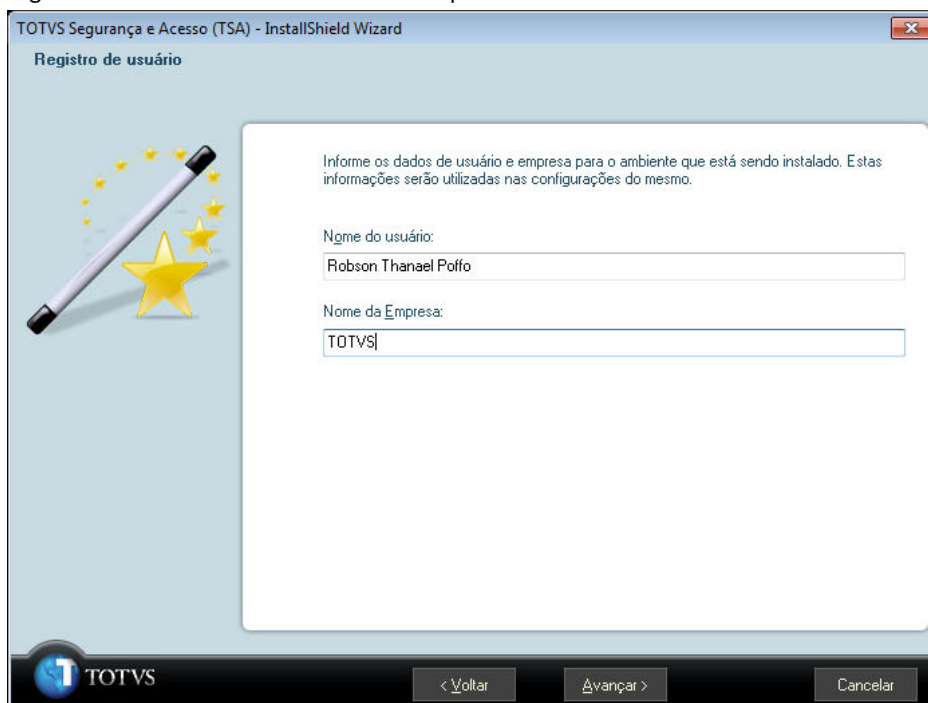
Execute o arquivo “setup.exe” para iniciar o processo de instalação.



Na tela de apresentação do instalador, clique em “Avançar” para dar início no processo de instalação do TSA:



Digite o nome do usuário e o nome da empresa onde esta sendo instalado o TSA:



TOTVS Segurança e Acesso (TSA) - InstallShield Wizard

Registro de usuário

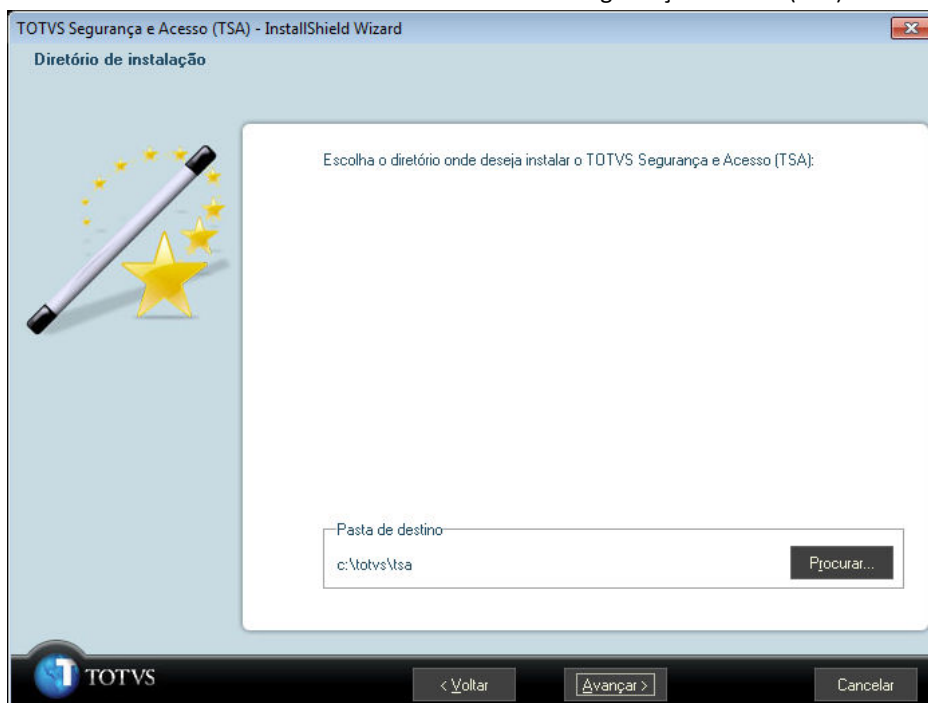
Informe os dados de usuário e empresa para o ambiente que está sendo instalado. Estas informações serão utilizadas nas configurações do mesmo.

Nome do usuário:
Robson Thanael Polfo

Nome da Empresa:
TOTVS

< Voltar Avançar > Cancelar

Na tela abaixo selecione onde será instalado o TOTVS Segurança e Acesso (TSA):



TOTVS Segurança e Acesso (TSA) - InstallShield Wizard

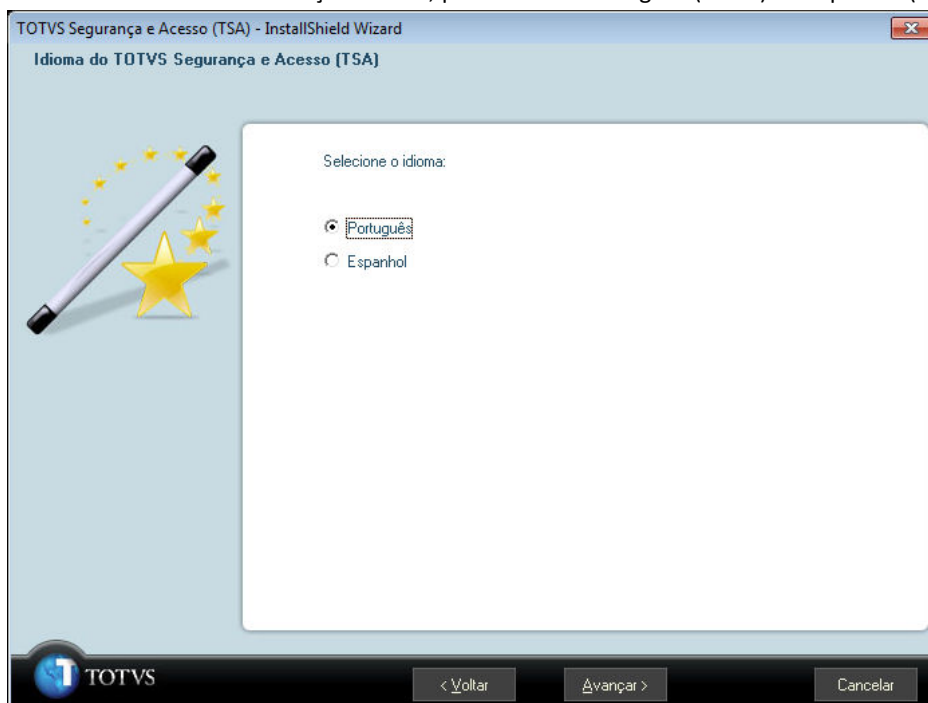
Diretório de instalação

Escolha o diretório onde deseja instalar o TOTVS Segurança e Acesso (TSA):

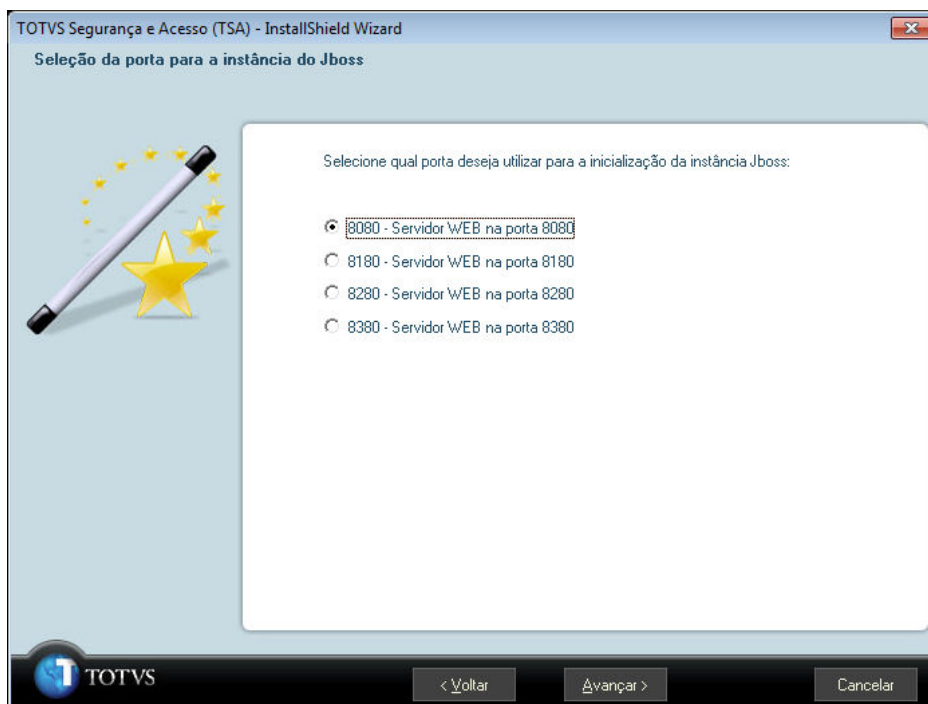
Pasta de destino:
c:\totvs\tsa Procurar...

< Voltar Avançar > Cancelar

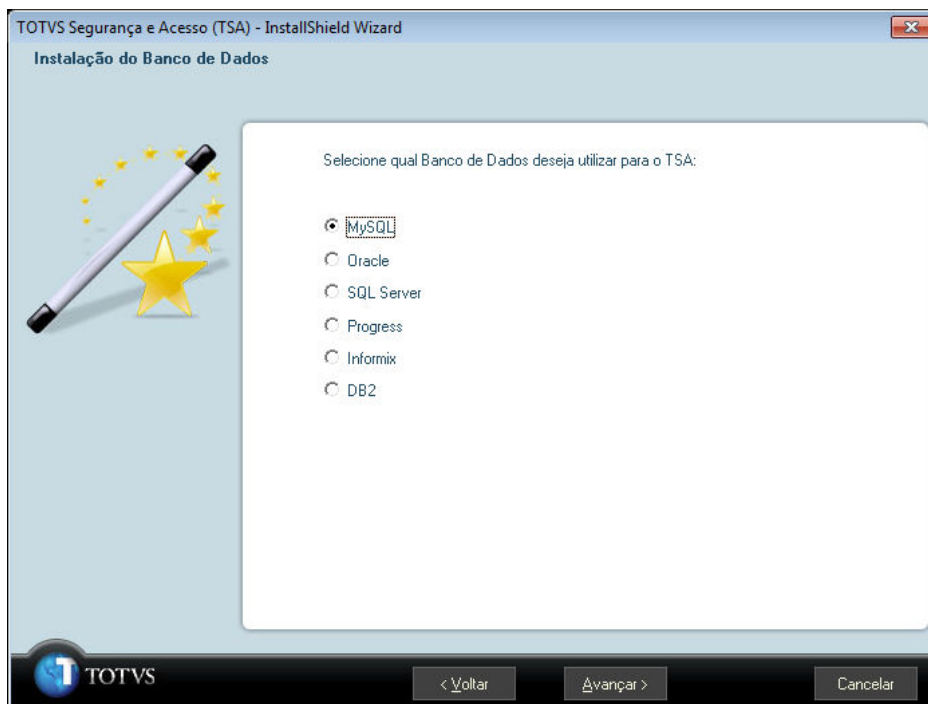
Selecione o idioma de instalação do TSA, podendo ser Português (Brasil) ou Espanhol (México):



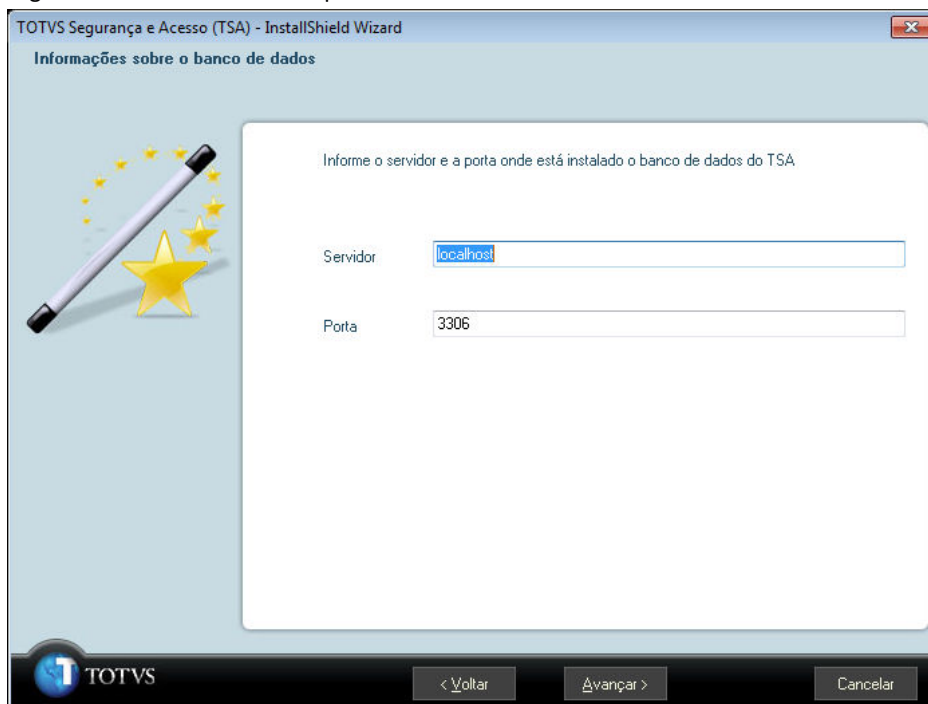
Na tela abaixo selecione em qual porta WEB o TSA estará disponível. Com essa opção é possível instalar até 4 instâncias do TSA no mesmo servidor.



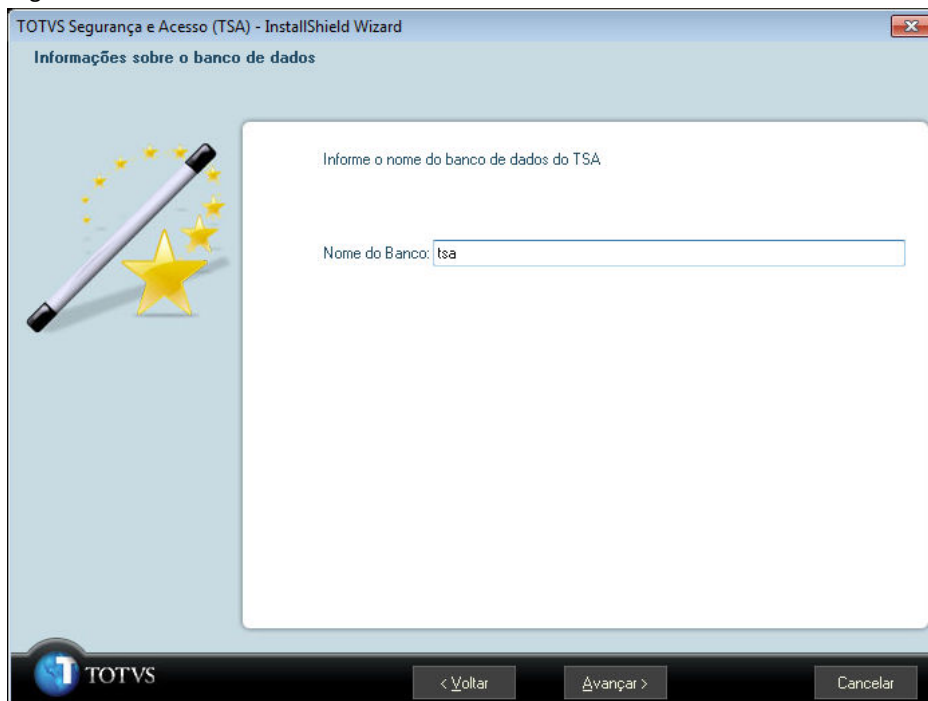
Selecione a base de dados na qual o TSA será executado dentro das opções disponíveis, nessa simulação escolheremos MySQL (posteriormente será questionado qual o banco de dados do sistema externo: Datasul, Protheus ou RM):



Digite o nome do servidor e a porta de conexão do servidor de banco de dados:



Digite o nome do banco de dados onde as tabelas do TSA estarão:



TOTVS Segurança e Acesso (TSA) - InstallShield Wizard

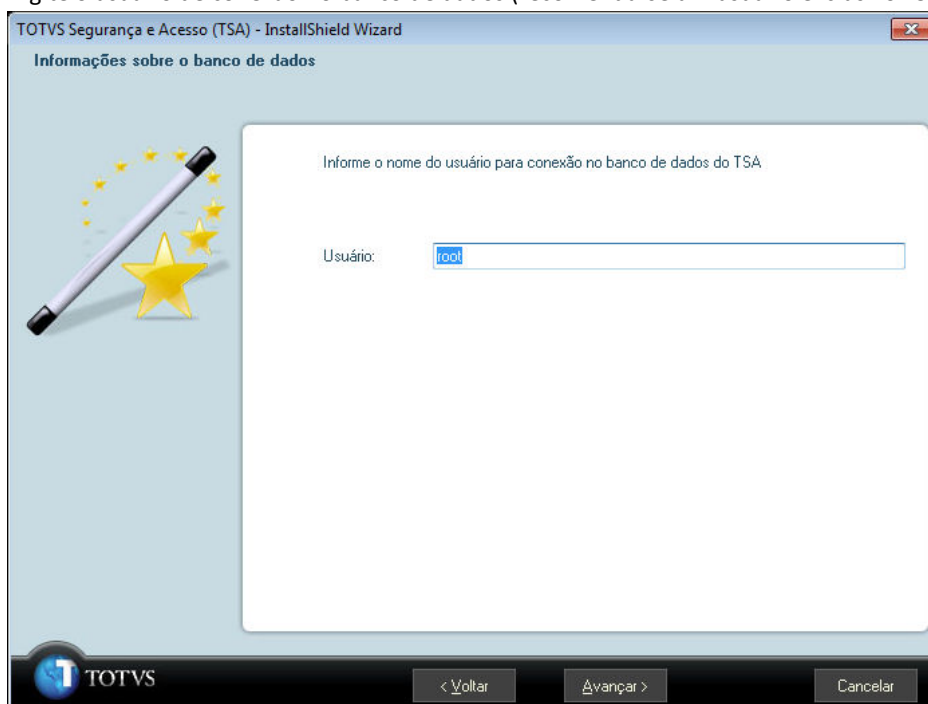
Informações sobre o banco de dados

Informe o nome do banco de dados do TSA.

Nome do Banco: tsa

< Voltar Avançar > Cancelar

Digite o usuário de conexão no banco de dados (recomenda-se um usuário exclusivo TSA):



TOTVS Segurança e Acesso (TSA) - InstallShield Wizard

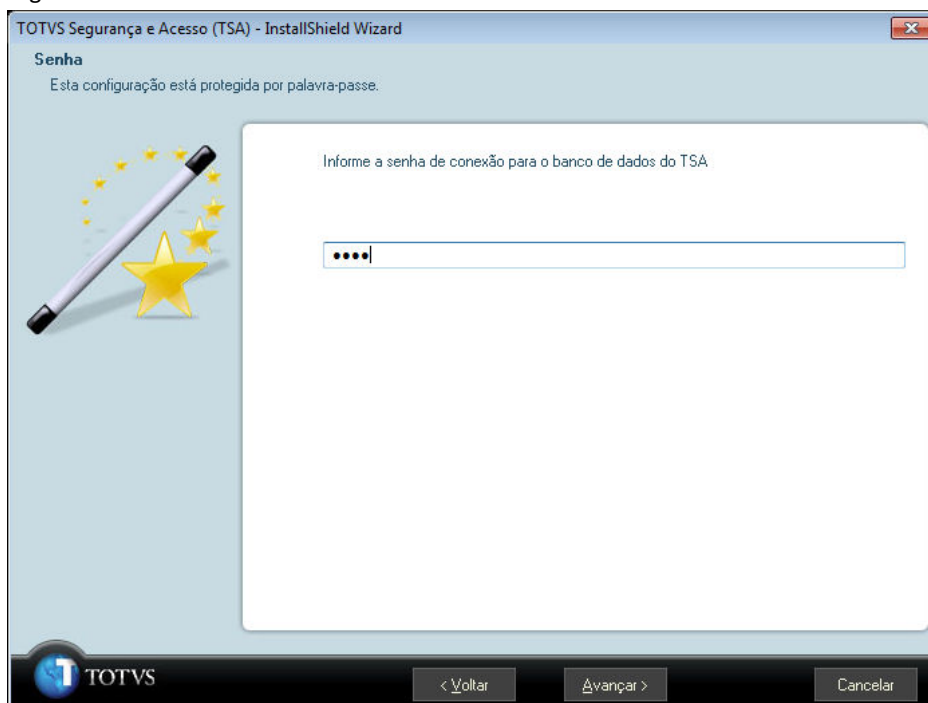
Informações sobre o banco de dados

Informe o nome do usuário para conexão no banco de dados do TSA.

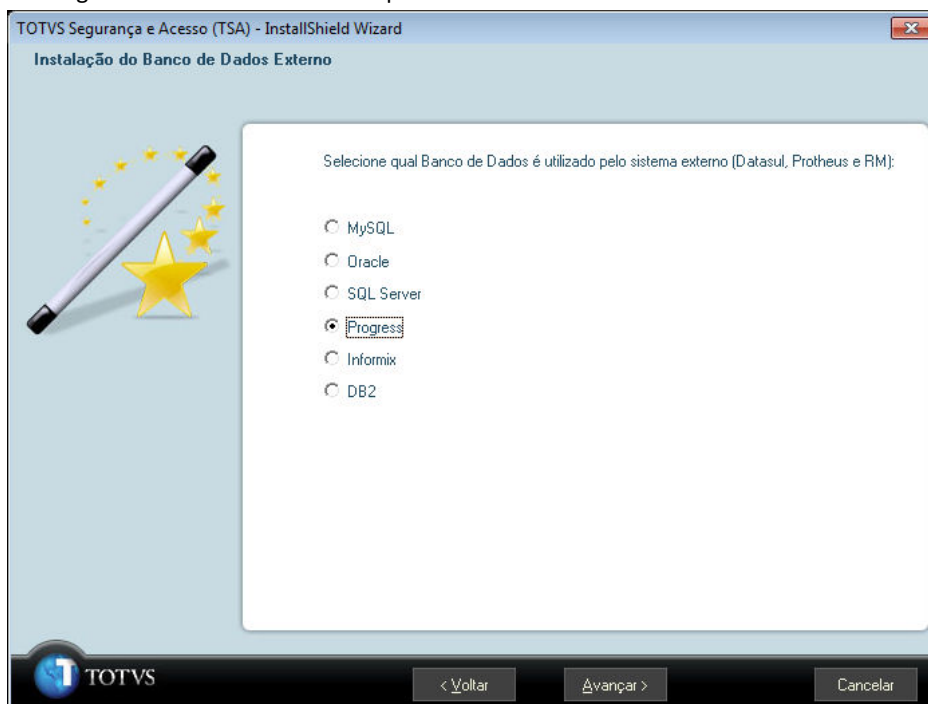
Usuário: root

< Voltar Avançar > Cancelar

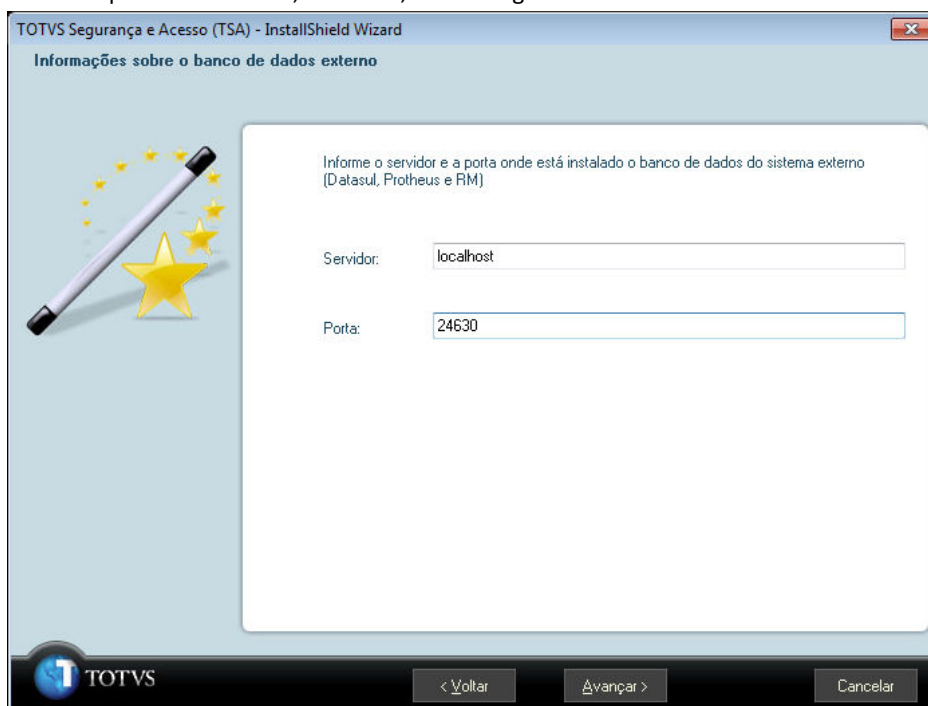
Digite a senha do usuário de conexão no banco de dados:



Selecione a base de dados que o sistema externo (Datasul, Protheus ou RM) utiliza. No exemplo abaixo será escolhido Progress utilizando como base o produto Datasul:



Informe o nome do servidor e a porta do servidor de banco de dados do sistema externo. O sistema externo é o produto de gestão de pessoas da TOTVS que fará o tratamento das marcações para o cálculo do ponto eletrônico. O sistema externo pode ser: Datasul, Protheus, RM ou Logix.



TOTVS Segurança e Acesso (TSA) - InstallShield Wizard

Informações sobre o banco de dados externo

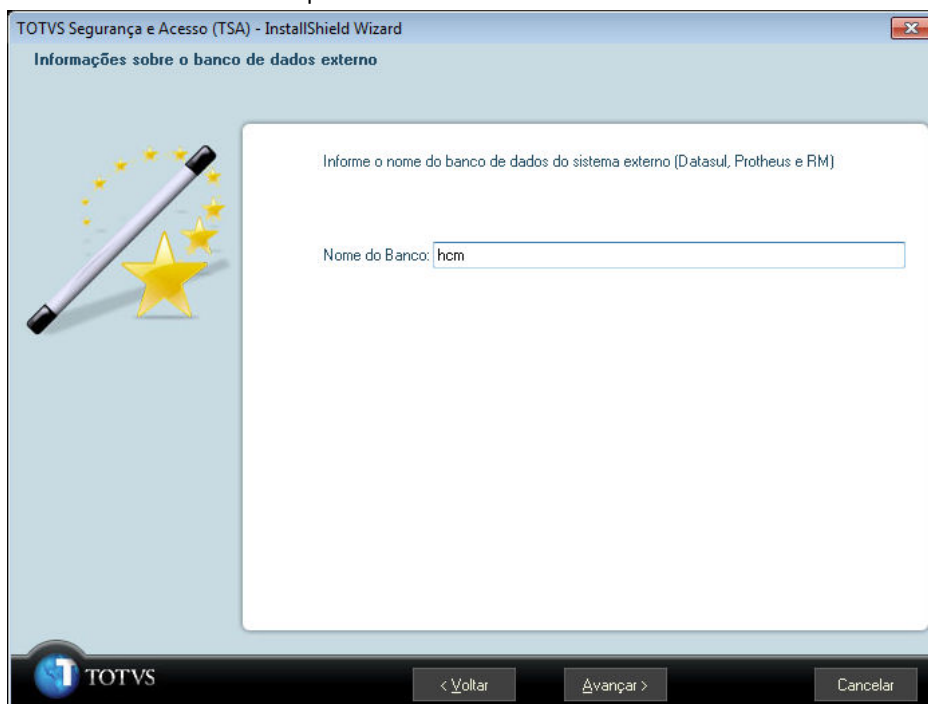
Informe o servidor e a porta onde está instalado o banco de dados do sistema externo (Datasul, Protheus e RM)

Servidor: localhost

Porta: 24630

< Voltar Avançar > Cancelar

Na tela abaixo é informado qual o nome do banco de dados do sistema externo:



TOTVS Segurança e Acesso (TSA) - InstallShield Wizard

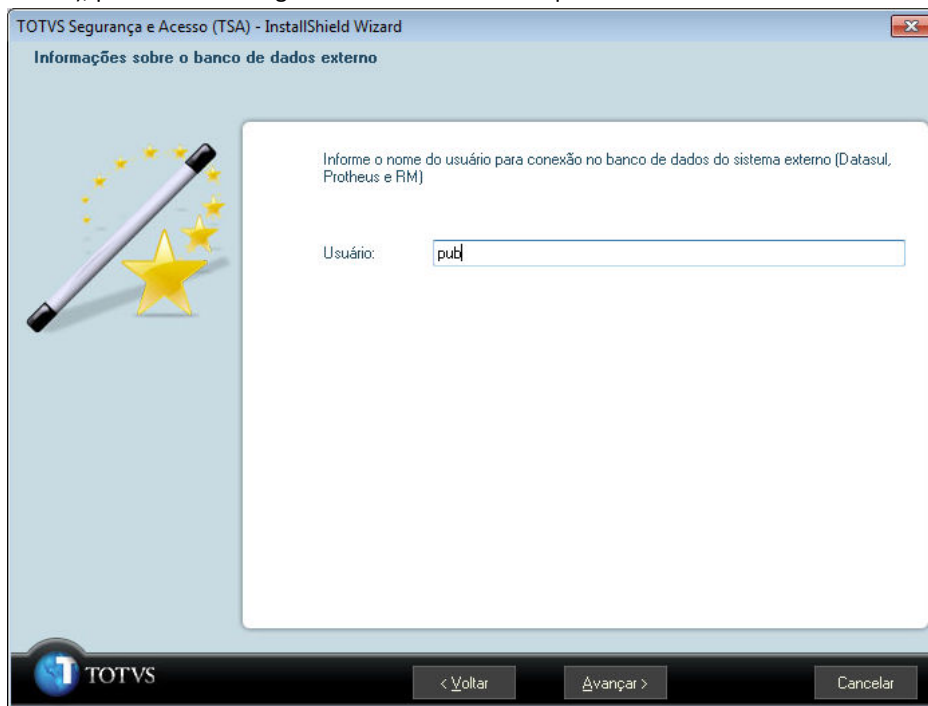
Informações sobre o banco de dados externo

Informe o nome do banco de dados do sistema externo (Datasul, Protheus e RM)

Nome do Banco: hcm

< Voltar Avançar > Cancelar

Na tela abaixo é informado o usuário de conexão no banco de dados do sistema externo (recomenda-se um usuário exclusivo TSA), para o banco Progress é utilizado o usuário pub:



TOTVS Segurança e Acesso (TSA) - InstallShield Wizard

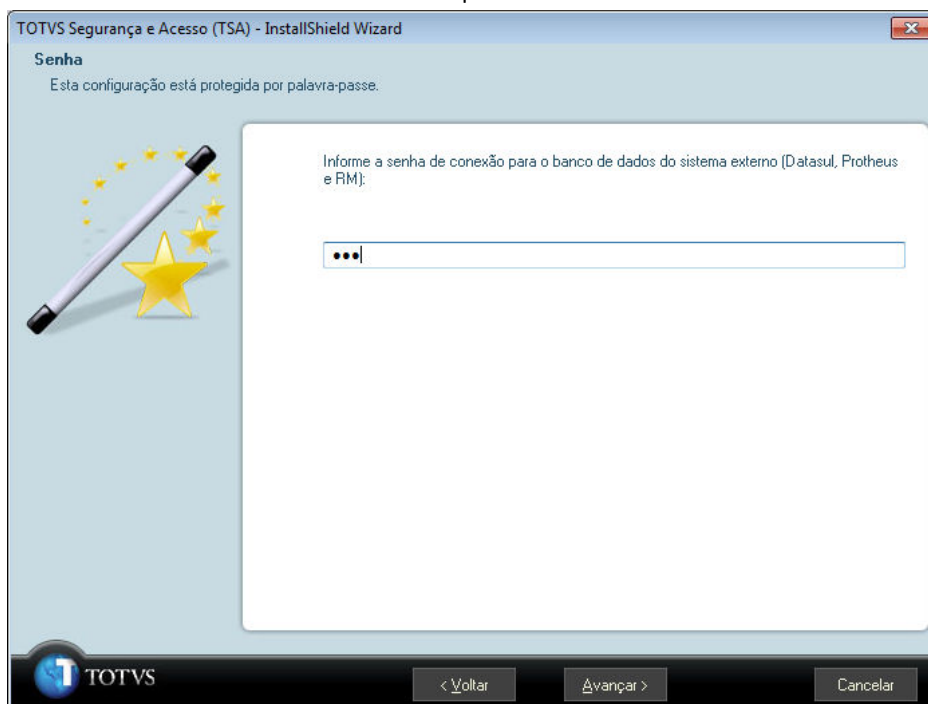
Informações sobre o banco de dados externo

Informe o nome do usuário para conexão no banco de dados do sistema externo (Datsul, Protheus e RM)

Usuário:

< Voltar Avançar > Cancelar

Na tela abaixo deve ser informado a senha para conexão no banco de dados do sistema externo.



TOTVS Segurança e Acesso (TSA) - InstallShield Wizard

Senha

Esta configuração está protegida por palavra-passe.

Informe a senha de conexão para o banco de dados do sistema externo (Datsul, Protheus e RM):

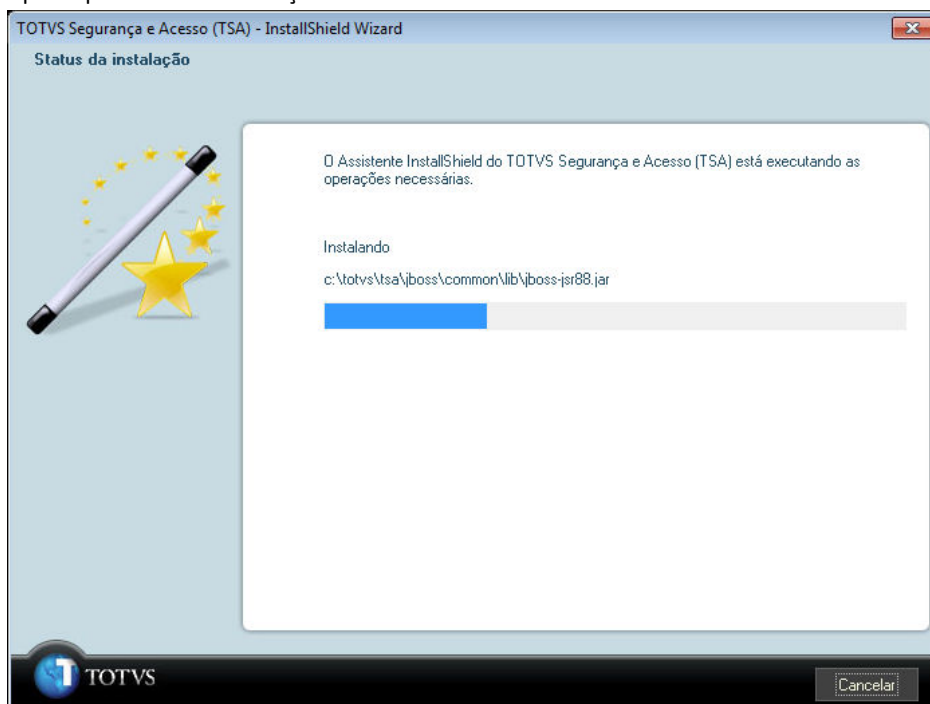
< Voltar Avançar > Cancelar

Após, o instalador irá preparar os dados para iniciar a instalação:

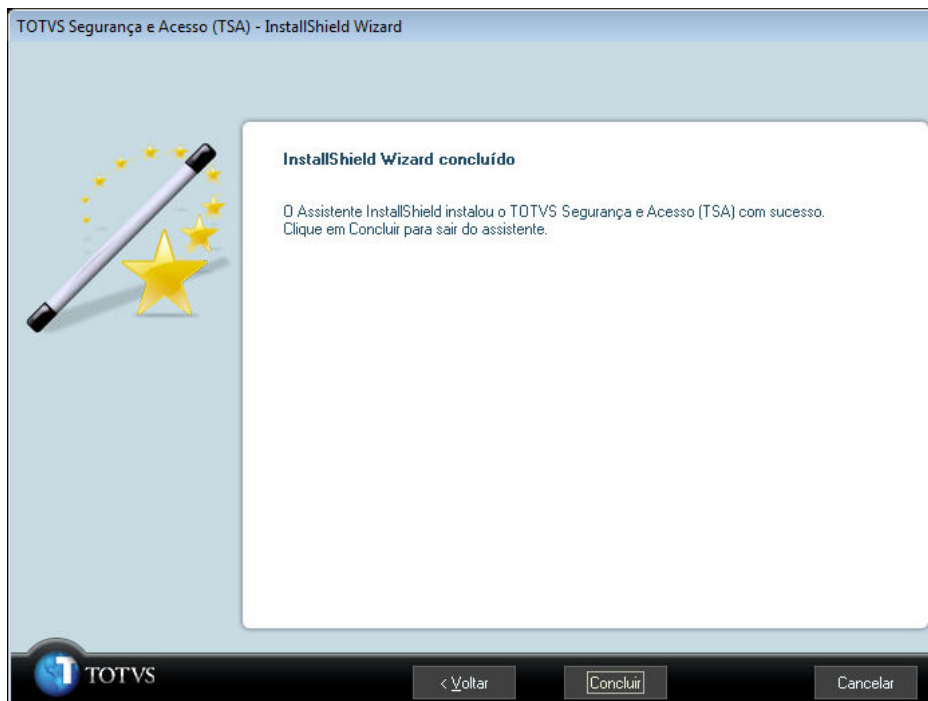


A seguir serão instalados os componentes necessários para o funcionamento do TOTVS Segurança e Acesso (TSA)...

Após o processo de instalação irá iniciar:



Após, o processo de instalação foi finalizado:



ATENÇÃO: Caso deseja-se instalar o TOTVS Segurança e Acesso em ambiente Linux, deve-se efetuar a instalação em ambiente Windows e após efetuar a cópia do diretório para o ambiente Linux.

4.3.1. Objetos Criados na Instalação do Servidor de Aplicação

Seguem os objetos importantes para administração do ambiente, criados na instalação do servidor de aplicação.

Localização	Descrição
<TSA_HOME>\ico	Diretório contendo o ícone do produto TOTVS.
<TSA_HOME>\integrador	Diretório da aplicação de integração com os equipamentos de Controle de Acesso e Ponto Eletrônico.
<TSA_HOME>\jboss	Diretório do servidor de aplicação JBoss.
<TSA_HOME>\jre	Diretório de instalação da máquina virtual do Java (JRE).
<TSA_HOME>\scripts	Diretório onde estão os scripts de carga da base de dados para os bancos de dados homologados e scripts de migração entre versões do TSA.

4.4. Instalação de Banco de Dados

A seleção do banco de dados no processo de instalação descrito no capítulo “4.3 Instalação do Servidor de Aplicação” é para que o JBoss seja configurado corretamente. O processo de instalação do banco de dados deverá ser executado manualmente e após, efetuada a carga dos dados do banco de dados.

Deverá ser carregado no banco de dados informado no processo de instalação o script “**databaseInitialization-TSA-*schema.sql**” localizado no diretório “<TSA_HOME>\scripts”. Substitua o asterisco (*) pelo fabricante do banco de dados que deve ser carregado (DB2, Informix, MySQL, Oracle, Progress ou SQL Server). Esse script fará a criação do ambiente do TOTVS Segurança e Acesso e a inicialização necessária do ambiente.

O script de criação da tabela externa (de marcações) deverá ser carregado no banco de dados informado no processo de instalação como “**Sistema Externo**” que corresponde ao software de gestão de pessoas utilizado, podendo ser: Datasul, Protheus ou RM. Os scripts estão localizados no diretório “TSA_HOME\scripts” e possuem o padrão de nomenclatura: “**databaseInitialization-TSA_EXT-*schema.sql**”, sendo que o asterisco (*) corresponde ao fabricante do banco de dados.



DICA: Para o produto Datasul não será necessário efetuar a carga do script “databaseInitialization-TSA-PROGRESS-schema.sql” (por esse motivo esse arquivo não está presente na mídia de instalação) pelo fato da tabela de marcações (MSA_CONTROL_MARCAC) ser expedida com o produto padrão.



ATENÇÃO Datasul: Para o produto Datasul apenas será necessário carregar o script do sistema externo (databaseInitialization-TSA_EXT-DATASUL-Oracle-schema.sql) quando o Datasul estiver instalado em banco de dados Oracle. Neste caso o script (databaseInitialization-TSA_EXT-DATASUL-Oracle-schema.sql) deverá ser carregado no banco de dados HCM/DTHRTMA. A tabela (MSA_CONTROL_MARCAC) necessária pelo TSA no produto Datasul já é expedida juntamente ao produto padrão para as versões homologadas do Datasul (versão igual ou superior a 11.2.2) no banco HCM/DTHRTMA.



ATENÇÃO Protheus, RM e Logix: É necessário executar o script “databaseInitialization-TSA_EXT-*schema.sql” para criação da entidade de marcações do TSA. Esse script deve ser executado no banco de dados do respectivo produto.

4.5. Inicializando o TOTVS Segurança e Acesso

Inicie o JBoss através do serviço “**TOTVS Controle de Acesso (TSA) - 8080**” criado no “Services” do Windows.

4.6. Acesso ao TOTVS Segurança e Acesso

Abra um navegador e acesse “**http://localhost:8080/tsa-web**” com os dados de *login* abaixo:

Login: **adm**

Senha: **123**

5. Reinstalação

A reinstalação pode ser executada para restaurar os programas originais, atente-se em informar os mesmos valores para as configurações de banco de dados. Recomenda-se que seja efetuado um backup do ambiente antes de prosseguir com um processo de reinstalação.

Arquivos de configurações importantes para backup:

- ✓ %TSA_HOME%\integrador\server\conf*
- ✓ %TSA_HOME%\jboss\server\tsa-web\deploy\properties-service.xml
- ✓ %TSA_HOME%\jboss\server\tsa-web\deploy\tsa-ds.xml

6. Desinstalação

O procedimento de desinstalação deve ser executado somente quando não é mais necessário os componentes instalados em cada servidor, sendo que essa rotina deve ser executada a partir do servidor onde foi instalado cada componente.

Para desinstalar o produto em ambiente Windows deve ser selecionada a opção “remover” do **“TSA * Controle de Acesso TOTVS”** em **“Iniciar > Configurações > Pannel de Controle > Adicionar ou Remover Programas”**.