# Table of Contents

- Table of Contents ................................................................. iii
- How to Use this Guide ............................................................. v

## Chapter 1

- Before you Begin ........................................................................ 1

## Chapter 2

- Installation Steps ........................................................................ 2
  - 2.1. Internet Information Services (IIS) ........................................ 2
  - 2.1.1. Enable ASP.NET 2.0 in IIS ................................................... 2
  - 2.2. Initial Reports Installation Steps ............................................ 3
  - 2.3. SharedObjects Installation .................................................... 6
  - 2.4. AccessServer Installation ..................................................... 9
  - 2.5. Final Reports Installation Steps .......................................... 14

## Chapter 3

- Post-Installation Adjustments .................................................. 15
  - 3.1. AccessServer Configuration ................................................ 15
  - 3.2. All Versions Of IIS ............................................................ 15
  - 3.3. For IIS 6 / Windows 2003 .................................................. 16
  - 3.4. For IIS 7 / Windows Vista .................................................. 17
Chapter 4

Starting Reports ................................................................. 22
  4.1. First Run ................................................................. 22
  4.2. Setting Database Connections ................................. 28

Appendices

Appendix A: Manual Configuration for Windows 2003 x64 .............. 29

Appendix B: Manual Configuration for Windows 2008 x64 and Vista x64 ................................................................. 30

Appendix C: How to Configure Machine Keys on ASP.NET When Installing on a Web Farm (Cluster) ........................................ 31
  C.1. Generating the Keys .................................................. 31
  C.2. Setting the Keys ....................................................... 31

Appendix D: Configuring SSL Connections .............................. 33
  D.1. IIS 6 ............................................................ 33
    D.1.1. Prepare a Certificate Signing Request (CSR) ........ 33
    D.1.2. Request a Certificate from a Certificate Vendor .... 35
    D.1.3. Install the Certificate .......................................... 36
  D.2. IIS 7 ............................................................ 37
    D.2.1. Prepare a Certificate Signing Request (CSR) ........ 37
    D.2.2. Request a Certificate from a Certificate Vendor .... 39
    D.2.3. Install the Certificate .......................................... 39

Appendix E: Configuring Mail Encryption Settings on Cluster Implementations ................................................................. 42

Appendix F: Further Information ........................................... 44
  F.1. Using Tango/04 PDF Documentation ........................ 44
  F.2. Tango/04 University ................................................. 44
  F.3. Contacting Tango/04 ................................................ 46

About Tango/04 Computing Group .......................................... 47

Legal Notice ........................................................................ 48
This chapter explains how to use Tango/04 User Guides and understand the typographical conventions used in all Tango/04 documentation.

Typographical Conventions

The following conventional terms, text formats, and symbols are used throughout Tango/04 printed documentation:

<table>
<thead>
<tr>
<th>Convention</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Boldface</strong></td>
<td>Commands, on-screen buttons and menu options.</td>
</tr>
<tr>
<td><em>Blue Italic</em></td>
<td>References and links to other sections in the manual or further documentation containing relevant information.</td>
</tr>
<tr>
<td><em>Italic</em></td>
<td>Text displayed on screen, or variables where the user must substitute their own details.</td>
</tr>
<tr>
<td><strong>Monospace</strong></td>
<td>Input commands such as System i commands or code, or text that users must type in.</td>
</tr>
<tr>
<td><strong>UPPERCASE</strong></td>
<td>Keyboard keys, such as CTRL for the Control key and F5 for the function key that is labeled F5.</td>
</tr>
<tr>
<td><img src="image" alt="Notes logo" /></td>
<td>Notes and useful additional information.</td>
</tr>
<tr>
<td><img src="image" alt="Tips logo" /></td>
<td>Tips and hints that will improve the users experience of working with this product.</td>
</tr>
<tr>
<td><img src="image" alt="Important logo" /></td>
<td>Important additional information that the user is strongly advised to note.</td>
</tr>
<tr>
<td><img src="image" alt="Warning logo" /></td>
<td>Warning information. Failure to take note of this information could potentially lead to serious problems.</td>
</tr>
</tbody>
</table>
Before you Begin

The following software must be installed before installing Reports:

- Microsoft .Net Framework 2.0
- Internet Information Services (IIS) version 5 or above

**Note**
The Reports Installer will install Microsoft .Net Framework if it is not already installed on your server. However, IIS must be installed manually.

**Important**
If you have previously installed IIS and then changed the name of your PC, it is strongly recommended that IIS is *re-installed* to avoid new web sites using an incorrect anonymous account user name.

VISUAL Message Center Reports requires:

- Microsoft Internet Explorer 7.0 or Microsoft Internet Explorer 8.0 in compatibility mode, or
- Mozilla Firefox 3.0 or 3.5.

Please check your browser for compatibility.

The following must be enabled before installing Reports:

- ASP.NET 2.0 enabled in IIS

If any of the prerequisites are not in place when you begin the installation process, the following message appears:

![Error Message](image)

*Figure 1 – Error message received if any of the prerequisites are not in place*

Possible causes for this message are:

- IIS is not installed on the computer
- Your IIS installation does not allow ASP.NET
Installing Reports is easy and most of the work is done automatically by the installer. This Installation Guide serves as a reference when installing Reports and explains the different steps in the process.

2.1 Internet Information Services (IIS)

IIS must be installed before installing Reports.

IIS is available on any Microsoft Windows installation disc. You will need a Microsoft Windows installation disc to install IIS.

**Note**
The version of IIS on a Microsoft Windows installation disc is only a limited version, it is not the full version of the product.

**Step 1.** Insert the Microsoft Windows installation disc

**Step 2.** Select Optional Components

**Step 3.** Select the **Internet Information Services** check-box to add it to the default selections

**Step 4.** Click **Next** to begin the installation

**Step 5.** When the installation is complete, click **Finish**

**Step 6.** Click **Exit**

2.1.1 Enable ASP.NET 2.0 in IIS

In IIS 6 (Windows 2003), ASP.NET 2.0 must be allowed (by default it is not allowed). This is achieved by editing the **Web Service Extensions** in the **IIS Manager**. Change the status of **ASP.NET v2.0** to **allowed**.
2.2 Initial Reports Installation Steps

To install Reports:

**Step 1.** Double-click the **ReportsInstaller.exe** installer file.

The installer will extract the necessary files to install.

The installer automatically installs C++ components.

The Welcome page appears. Click **Next** to continue.
Step 2. Choose the applications you want to install:

- **VMC Reports**: inside this section you will find the core (mandatory installation), and the set of reports you want to install.
- **Scheduler**: is intended to schedule reports and send them via e-mail.
- **AccessServer**: is mandatory, this application will be in charge of user validation for Reports; however, if you have already installed AccessServer on your network previously, you can omit this installation and use you current installation of AccessServer.
- **SharedObjects**: is an additional web application that will provide Reports with a CalendarService, it is a mandatory application.
- **NiceLink**: this application is needed in order to enter the keys for the product. If the installer detects that you have NiceLink already installed, it will automatically prevent NiceLink from being installed again, unless it is an older version.

Step 3. Indicate what features to install. By default all features are selected.

Click **Next** to continue.

The Web Configuration opens. Click **Next** to continue.
Step 4. You will be prompted for the kind of Web Site installation you desire for Reports.

- In Windows 2003 and Vista it is better to use the New Web Site option.
- In Windows XP, IIS does not support multiple web sites, so you have to use Virtual Directory.

Select an option and Click Next to continue.

Step 5. In this step you have to configure Reports Web Site settings. See Figure 9 below, for a common example of how to configure these parameters, as we have selected New web Site, the final Reports URL in this case would be:

http://server_ip_adress_or_server_name:8083

Click the Browse Button to change the destination path.
Step 6. Now you are ready to install Reports and the selected features, click **Next** to continue.

Click **Next** to continue.

### 2.3 SharedObjects Installation

The next stage of the Reports installation is the SharedObjects installation:

**Step 1.** The SharedObjects Installation Wizard automatically begins.
Step 2. The Web site configurator for SharedObjects appears.

You have to configure the Web site using exactly the same recommendations selected earlier for Reports.
Installation Steps

Step 3. Select a location. Click **Next**.

Step 4. Enter the Web Site information. Click **Next**.

Step 5. Click **Next** and the SharedObjects installation will start.
Step 6. The installation of the SharedObjects is completed. Click Finish, and the AccessServer Installation will start.

2.4 AccessServer Installation

The next feature to be installed is AccessServer:

Step 1. Click Next on the first AccessServer installation Screen to begin the installation.

Step 2. Select the location to install AccessServer to.
Installation Steps

Click **Next**.

**Step 3.** After copying a set of files, the AccessServer Data source selection form appears. Here you select the DSN where AccessServer will store its metadata (internal operation tables).
Once you have chosen the DSN click **Next**.

**Step 4.** Enter a User name and password for the data source.

Click **Next**.

**Step 5.** The AccessServer configuration screen appears, look carefully at each parameter in order to set them to the most suitable values for your installation.

**Tip**

We recommend you increase the session time-out value. Time values are expressed in seconds.

Step 7. In this step you will have to set up the user that will act as AccessServer security administrator, the user must be either a *local* user or a *domain* user, according to the authentication mode selected in the previous step.
Figure 24 – Set up the user that will act as the AccessServer security administrator

Click **Next**.

Figure 25 – Apply the configuration changes

Click **Next**.

When the installation is complete, click **Finish**.

Figure 26 – AccessServer installed successfully

Click **Finish** again. The Reports final installation steps will start.
2.5 Final Reports Installation Steps

The final steps of the installation automatically begin. All the selected features are installed.

Click **Finish**, and the installation of Reports is complete.

**Important**

Please read the next sections carefully, in some cases you will have to configure some settings manually before starting Reports.

![Final Reports Installation Steps](image)
Chapter 3
Post-Installation Adjustments

Once the installer has completed a few adjustments must be made, depending on the operating system of the server. This chapter describes the required adjustments.

### 3.1 AccessServer Configuration

For information on configuring AccessServer for a specific operating system, please refer to the *AccessServer Installation Guide*.

### 3.2 All Versions Of IIS

Add a new MIME Type for the `.rti` extension from the IIS Manager:

1. **Step 1.** Open the IIS Manager and select the Reports Site Properties.
2. **Step 2.** Click the HTTP Headers tab and click the MIME Types button.
3. **Step 3.** Select the `.rti` extension and click Edit.
4. **Step 4.** Change the MIME Type to `application/octet-stream`

**Important**

If the extensions `.DOC`, `.XLS` and `.CSV` do not have an associated MIME Type, you will have to repeat the previous steps for each of these extensions, otherwise you will have issues when exporting reports.
3.3 For IIS 6 / Windows 2003

Step 1. Disable Recycling in the Application Pool where Reports and SharedObjects are installed.

Step 2. Modify the Application Pool to work with only one process, as shown below:
3.4 For IIS 7 / Windows Vista

If you are using Windows Vista and IIS 7, you will need to

- set the web application path
- grant permission to share the Reports folder to Windows users
- set the application pool identity to Network Service
- change the managed pipeline mode of the application pool
- disable recycling in the application pool
- remove the StaticContent tag from XML in the web.config file.

To set the Web Application Path:

**Step 1.** Open IIS Manager.

**Step 2.** Browse to the created Web Site or Virtual Directory.

**Step 3.** In the side bar, under Actions click Basic Settings...

**Step 4.** In the Physical path field, enter the path you used during the installation. For Example:

```
C:\Inetpub\wwwroot\Reports
or
C:\program files\tango04\Reports
```

**Step 5.** Repeat the same steps for SharedObjects.
Figure 31 – Enter the Physical path

To grant permission to share the Reports folder to Windows users:

Step 1. Open IIS Manager.

Step 2. Open Sites.

Step 3. Select Reports from the list of sites and click Edit Permissions on the sidebar. The Reports Properties window appears.

Step 4. Select the Sharing tab and click the Advanced Settings button. The Advanced Sharing dialog box appears.

Step 5. Click the Share this folder check box. Reports appears in the Share name field. Click the Permissions button. The Permissions for Reports dialog box appears. By default, Everyone appears in the Group or user names list.

Step 6. Click Add. The Select Users or Groups dialog box appears. In the Enter the object names to select field, enter:

- Administrator, then click the Check name box. Once the name is found, click OK.
- User, then click the Check name box. Once the name is found, click OK.
- Network Service, then click the Check name box. Once the name is found, click OK.
- IIS_xxxxxx, then click the Check name box. Once the name is found, click OK.

To set the application pool identity to Network Service:

Step 1. Open IIS Manager.

Step 2. Open the Application Pools list.

Step 3. Select Reports and click Advanced Settings under Edit Application Settings on the sidebar. The Advanced Settings window appears.
Step 4. Click the (hidden) button in the field next to **Identity**. By default, it says **ApplicationPoolIdentity**. A dialog box appears.

![Application Pool Identity](image)

*Figure 32 – Changing Reports’ application pool identity in IIS*

**Step 5.** Click the **ApplicationPoolIdentity** drop-down list box and select **NetworkService**. Click **OK**.

To change the managed pipeline mode:

**Step 1.** Open IIS Manager.

**Step 2.** Open the Application Pools list.

**Step 3.** Set the Managed pipeline mode to **Classic**.
To disable recycling in the application pool:

**Step 1.** Open IIS Manager.

**Step 2.** Open the Application Pools list.

**Step 3.** Select Reports and click Recycling on the sidebar under Edit Application Pool. The Recycling Conditions window appears.

**Step 4.** Ensure that no recycling check boxes are selected, click Next, and then Finish.

To edit the web.config file:

**Step 1.** Open the Reports install directory (by default `C:\inetpub\wwwroot\Reports` or `c:\program files\tango04\Reports`) and edit the web.config file.

**Step 2.** Remove `StaticContent` tag from XML and Save the File:

```xml
<staticContent enableDocFooter="false" isDocFooterFileName="true">
    <clientCache cacheControlMode="NoControl"/>
</staticContent>
```
Step 3. Additionally if you have installed SharedObjects you will have to remove the same XML tag from the `web.config` files located at:

C:\program files\tango04\SharedObjects\and

C:\program files\tango04\SharedObjects\calendars
Now you are ready to start Reports. The first time you start Reports you will need to configure a few basic settings and create the database connections, as described here.

**Important**
Before you go to the Reports URL you will have to enter your product Key via NiceLink configurator, otherwise after the configuration tasks finish, you will get a message saying you have an Invalid Key and that the product is not installed.

Contact you customer representative for a definitive or temporary Key.

### 4.1 First Run

After installing VISUAL Message Center Reports there are several configuration screens which are automatically presented the first time that Reports is run which must be completed before reports can be used.

**Note**
The wizard will help you complete each stage of the initial configuration.

Keep in mind that the first time you run Reports, there are a series of tasks that can take several minutes to finish, laboratory tests has shown that a first run commonly takes 15-20 minutes depending on hardware.
Enter details regarding the database used for storing reports:

- **Engine**: type of database engine used to connect to the Reports database
- **Connector**: type of connection to the database
- **Driver**: driver used by the database
- **Server**: name of the server where the reports database is located
- **Database**: name of the reports database
- **User**: username used for access to the database
- **Password**: password for access to the database
After entering the correct details, click **Test Connection** to verify everything is correct.

![Connected Successfully](image)

*Connection was established successfully*

**Figure 39 – Connected to the Reports database successfully**

Access Server

Reports securely relies on AccessServer, the security solution of the VDAAS Message Center Suite. In order to use Reports securely, you must have AccessServer installed and working on a network connected with the Reports server.

User entries and configurations validated by AccessServer according to the settings configured through the Reports security settings.

If you do not have AccessServer installed, enabled with the Reports installation file you will test the AccessServer installed. Remember you will need a fixed IP address for AccessServer to function correctly. AccessServer can utilize user access via an active directory domain, or local Windows PC (\<computer\>\<username\>), depending on your choice when installing AccessServer.

To view in print when AccessServer is installed, you will be prompted for an AccessServer administrator user. The user who logs in will be defined as the AccessServer administrator and must be created before the installation.

The user will also use the AccessServer administrator user to log in to the AccessServer administrator user, which will be defined as the AccessServer administrator. The user will log in to an external reports via the **AccessServer** and will have access to the configurations and reports that have been configured for them. The user will be prompted for the correct details using the simple name (nsew\administrator, user\administrator) and the security administrator password (**pcname\administrator**).

- **AccessServer Admin**: select the type of user to be configured as the AccessServer administrator.
- **Domain \ User**: enter the name of the AccessServer administrator.
- **Reports Admin**: enter the name of the Reports administrator.

After entering the correct details, click **Test Authentication** to verify everything is correct.

![Authenticated Successfully](image)

*The given User was successfully authenticated*

**Figure 41 – Authenticated successfully with AccessServer**

Enter details regarding connecting to AccessServer:

- **Hostname**: name of the host where AccessServer is located (usually *localhost*)
- **Port**: port where AccessServer is listening (by default *18081*)
- **Domain / PC**: name of the computer where AccessServer checks user authentication
- **AccessServer administrator, Domain \ User**: local computer name followed by back-slash (\) and the security administration username (pcname\administrator)
- **Password**: password for the security administrator
- **Type of Reports Admin**: select the type of user to be configured as the Reports administrator
- **Reports Admin**: enter the name of the Reports administrator

After entering the correct details, click **Test Authentication** to verify everything is correct.
Enter the URL for the SharedObjects service, which is the IP address where the service is located followed by the name of the service or the port number where the service is listening:

- http://IP Address/SharedObjects/
- http://IP Address:Port/

After entering the correct details, click **Test Availability** to verify the URL is correct and SharedObjects is working.

The default settings should be sufficient.
Scheduler Client Settings

Reports will let you schedule actions called scans, which will run reports, export them, and send them to a user. Scheduler service is an independent service, with a part of the VSAM/Messaging solution.

Enter e-mail details scheduler. If you do not have scheduler running on a different network, you can leave the default parameters and continue with the report.

Figure 45 – Scheduler Client Settings

The default settings should be sufficient.

Mail Settings

This section lets you configure the SMTP parameters according to your company. This information will be used by reports when you decide to send reports by email or whether you choose to run a scan manually or using a scheduler.

Figure 46 – Mail Settings

Enter details of the e-mail account and mail server required to send messages with Reports.
After completing the configuration forms click **Save** to save the settings.

Enter the authentication details specified earlier to start using Reports.
4.2 Setting Database Connections

In the settings page you can indicate what database engine to use and select the type of connector to use. Various options are available, including Native connectors.

To use Native connectors, the .NET Driver must be installed. (SQL Server is included in MicroSoft Framework).

In order to install the .NET Driver:

**Step 1.** Go to the DB Engine site and download the installer.

**Step 2.** After installing the .net Driver, you will have to set some parameters in the `web.config` file in Web Application directory:

```
go to C:\Windows\assembly and find the corresponding assembly.
```

**Step 3.** Go to the `Web.config` file in the application directory and create an entry with the assembly data. For example like that located in the XML path `/configuration/runtime/assemblyBinding`.

```
<qualifyAssembly partialName="MySql.Data" fullName="MySql.Data, Version=5.0.8.1, Culture=neutral, PublicKeyToken=c5687fc88969c44d"/>
```

**Note**
The settings entered in the Wizard can be changed within the Reports application in the Management or Settings tabs. For further details please refer to the _VISUAL Message Center Reports User Guide_.

---

**Figure 51 – Find the corresponding assembly**

**Figure 52 – Create an entry with the assembly data**
Appendix A

Manual Configuration for Windows 2003 x64

When running in 32-bit mode on a 64-bit OS Microsoft Windows 2003 Server, once the application has been deployed, the following configurations may need to be performed:

**Step 1.** Run Internet Information Services (IIS) in 32-bit mode by running the following line in a command window:

```
Cscript %SystemDrive%\inetpub\AdminScripts\adsutil.vbs set w3svc/AppPools/Enable32bitAppOnWin64 1
```

*Tip*
Leave the command window open because it will be needed again

The last number in the above line is to set 32-bit to True. See the Microsoft Knowledge Base article 894435.

**Step 2.** Restart the IIS service. Type the following in the command window:

```
net stop w3svc /y & net start w3svc
```

The `net stop` and `net start` commands force IIS services to re-read the registry.

**Step 3.** Navigate to the Windows folder in the command window. Locate the `Microsoft.Net\Framework\v2.0.50727` folder.

**Step 4.** Run the `aspnet_regiis -i` command. This will register the 32-bit .NET subsystem.

**Step 5.** Open IIS Manager (`inetmgr`) and ensure that the web extension for ASP.NET (.Net Framework 2.0 32 bits) is allowed.

**Step 6.** Open IIS Manager (`inetmgr`) and ensure that your application is able to use ASP .NET framework version 2.0.

*Note*
The above will require all applications to run in 32-bit mode only. If there are other applications running on the IIS server that must run in 64-bit mode, then the 32-bit application should be run on a different server.
If you are running Windows 2008 x64 / Vista x64 (IIS7 for 64 bits), an extra modification step is required.

**To modify a Windows 2008 x64 / Vista x64 (IIS7 for 64 bits) system:**

**Step 1.** Open the IIS Manager, navigate to Application Pools, right-click in the DefaultAppPool, and select Advanced Settings.

**Step 2.** In the General section, change the property for the Enable 32-Bit Applications to True.
Appendix C: How to Configure Machine Keys on ASP.NET When Installing on a Web Farm (Cluster)

When installing a .NET web application on a Web Farm, it is important that all the servers of the farm generate the same machine key. This has to be done because when a web page is served by a server and then served by another in a further request, the engine fires an exception if the keys do not match. This happens because it thinks that someone might have tampered with the View State.

C.1 Generating the Keys

To generate the keys:

Step 1. Download the generateKey.exe program from:

http://www.tango04.info/products/generateKey.exe

Step 2. Run the program using the following command line argument:

generateKey.exe 24 64

Note

The two integer values 24 and 64 represent the size of the decryption and the validation keys respectively.

Because the code is using a random number generator, the output is different every time.

More detailed information on both the problem and the solution can be found in the following KB articles from Microsoft:

http://support.microsoft.com/default.aspx?scid=kb;en-us;323744
http://support.microsoft.com/kb/312906/EN-US/

C.2 Setting the Keys

To set the keys:

Step 1. After running the program, copy the output to the clipboard.

Step 2. Then open the file:

C:\Windows\Microsoft.NET\Framework\v2.0.50727\config\machine.config
Step 3. In the `machine.config` file, find the `<system.web>` XML tag and add the contents of the clipboard (the output of the program) inside the tag.

You will have to copy the same machine key to this file on every server of the cluster.

### Note
The path might be different if the system is a 64 bit OS.
Remember to make a backup of the file first!
This appendix explains how to configure a Secure Sockets Layer (SSL) connection for Internet Information Server (IIS).

D.1 IIS 6

D.1.1 Prepare a Certificate Signing Request (CSR)

To prepare a CSR:

Step 1. Open the Internet Information Services (IIS) Manager: Click Start > Administrative Tools > Internet Information Services (IIS) Manager.

Step 2. Expand the server (local computer) and Web Sites branches and right-click on the Web site on which you want to install the new certificate and select Properties.

Step 3. In the Web Site tab enter a port to be used for SSL in the SSL port field.

Tip
Make sure you use a port that is not already being used. You can check the properties of each configured Web site in the IIS Manager to see what ports are currently in use.

Figure 54 – Web site properties
Step 4. Click the Directory Security tab and click the **Server Certificate** button to open the Web Server Certificate Wizard.

**Note**
If the **View Certificate** button is not grayed out, you already have a certificate protecting this site. Check the certificate has not expired.

![Figure 55 – Directory Security tab, click the Server Certificate button to start the wizard](image)

Step 5. Click **Next** to continue, select the **Create a new certificate** selection box and click **Next**.

![Figure 56 – Create a new certificate](image)

Step 6. Accept the default options and complete the **organizational information** and **geographical information** fields as required until you reach the Certificate Request File Name window.
Step 7. Enter a file name and location for the certificate request to be saved in. Click Next to continue and view a summary of the certificate.

Click Next and then click Finish to complete the process.

D.1.2 Request a Certificate from a Certificate Vendor

After creating a CSR the next step is to apply for a certificate from the appropriate certification authority.

Important
The certificate request process varies for each certification authority, so we cannot provide details of the process in this document. Please contact the appropriate authority for further information.

The text file that contains the certificate request created in the steps above will be required in order to complete the certificate order form. Copy and paste the encrypted certificate request in the appropriate field in the order form.

Complete the vendor's certificate request form, return it complete with the required payment and wait for the SSL certificate to be delivered by e-mail.
D.1.3 Install the Certificate

When you receive the certificate ensure that your Web server has access to the certification authority’s response. Now you need to install the new certificate by completing the certificate process started in section D.1.1 - Prepare a Certificate Signing Request (CSR) on page 33.

To install the certificate:

**Step 1.** Open the Internet Information Services (IIS) Manager: Click Start > Administrative Tools > Internet Information Services (IIS) Manager.

**Step 2.** Expand the server (local computer) and Web Sites branches and right-click on the Web site on which you want to install the new certificate and select Properties.

**Step 3.** Click the Directory Security tab and click the **Server Certificate** button to open the Web Server Certificate Wizard.

**Step 4.** Select the **Process the pending request and install the certificate** selection box and click Next.

![Figure 59 – Process the pending request](image)

**Step 5.** Enter the path and the file name of the certificate file received from the certification authority.

![Figure 60 – Enter the path and file name of the file that contains the certification authority’s response](image)

Click Next to continue.

**Step 6.** Specify the SSL port to be used by the Web Site.
Click Next to continue.

**Step 7.** A summary window will display the information found in the certificate. Click Finish to complete the process.

---

**D.2 IIS 7**

**D.2.1 Prepare a Certificate Signing Request (CSR)**

To prepare a CSR:

- **Step 1.** Open the Internet Information Services (IIS) Manager: Click Start > Administrative Tools > Internet Information Services (IIS) Manager.

- **Step 2.** Select the server (local computer) and double-click Server Certificates to open.
Step 3. Click **Create Certificate Request** in the Actions pane.

Step 4. Enter the required information for the certificate and click **Next**.
**Step 5.** Enter a *file name* and *location* for the certificate request to be saved in and click **Finish** to complete the process.

![Certificate Request File Name](image)

**Figure 66 – Certificate Request File Name**

### D.2.2 Request a Certificate from a Certificate Vendor

After creating a CSR the next step is to apply for a certificate from the appropriate certification authority.

**Important**

The certificate request process varies for each certification authority, so we cannot provide details of the process in this document. Please contact the appropriate authority for further information.

The text file that contains the certificate request created in the steps above will be required in order to complete the certificate order form. Copy and paste the encrypted certificate request in the appropriate field in the order form.

Complete the vendor's certificate request form, return it complete with the required payment and wait for the SSL certificate to be delivered by e-mail.

### D.2.3 Install the Certificate

When you receive the certificate ensure that your Web server has access to the certification authority’s response. Now you need to install the new certificate by completing the certificate process started in **section D.2.1 - Prepare a Certificate Signing Request (CSR)** on page 37.

To install the certificate:

1. **Step 1.** Open the Internet Information Services (IIS) Manager: Click **Start** > **Administrative Tools** > **Internet Information Services (IIS) Manager**.
2. **Step 2.** Select the **server** (local computer) and double-click **Server Certificates** to open.
3. **Step 3.** Click **Complete Certificate Request** in the Actions pane.
Step 4. Enter the path and the file name of the certificate file received from the certification authority. Click OK.

Step 5. To associate the certificate with the site, click Bindings... in the Actions pane. Click Add... to create a new Web site connection for the certificate.
Enter the Web site *port* details and select the *certificate* from drop-down list box and click **OK**.

The new binding appears in the list. Click **Close** to complete the process.
In order to encrypt sensitive mail settings, Reports uses Framework.NET encryption tools that are prepared for Web.config files.

It uses an RSA Algorithm which stores the keys in a container in each computer. The container works only in the machine in which it was used.

Web.config section encryption allows specifying which Key Provider is going to be used. This enables us to create an exclusive container for the Reports application, export it and then import it into another machine in the Cluster which can then use the same container.

To configure mail encryption settings:

**Step 1.** Add the following XML node to the Reports Web.config file (inside the Configuration node):

```
<configProtectedData>
  <providers>
    <add keyContainerName="ReportsKeys"
         useMachineContainer="true"
         description="Uses RsaCryptoServiceProvider to encrypt and decrypt"
         name="ReportsProvider"
         type="System.Configuration.RsaProtectedConfigurationProvider, System.Configuration, Version=2.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a" />
  </providers>
</configProtectedData>
```

**Step 2.** Execute the `asp_regiis.exe` command, located by default in:

```
C:\Windows\Microsoft.NET\Framework\v2.0.50727
```

This will create a key container.

```
aspnet_regiis -pc "ReportsKeys" -exp
```
If using -exp is not valid, try removing it and executing the command again.

**Step 3.** Export the keys:

```
aspnet_regiis -px "ReportsKeys" "C:\ReportsKeys.xml" -pri
```

**Step 4.** Import the keys into another machine (other cluster node):

```
aspnet_regiis -pi "ReportsKeys" "C:\ReportsKeys.xml"
```

**Step 5.** In both machines, add permissions to the user running the ApplicationPool in IIS to use this key container:

```
aspnet_regiis -pa "ReportsKeys" "NT Authority\Network Service"
```

**Step 6.** Modify the `Settings.General.ProtectionProvider` node in the `Asterion.config` file to use the created key container (specifying the provider set in the `Web.config` file).

```
<ProtectionProvider>ReportsProvider</ProtectionProvider>
```

**Step 7.** Clean the `mailSettings` node in the `Web.config` in order to start using this new key container, then access the Reports configuration and save the configuration in order to verify everything is working properly.
Appendix F

Further Information

F.1 Using Tango/04 PDF Documentation

Tango/04 documentation is available directly from the Tango/04 solutions DVD.

To open the Tango/04 documentation that is provided in PDF files use Adobe Acrobat Reader. Acrobat Reader lets you view, search, and print the documentation. You can download Acrobat Reader for free from the Adobe Web site (http://www.adobe.com).

Tip
We advise printing PDF documentation for easy reference. Please ensure you familiarize yourself with a product’s user guide before attempting to use the product.

To access PDF documents on the DVD:

Step 1. Navigate to a product suite (VISUAL Message Center for example) and click on the Product Documentation link to open a list of all the User Guides available for that product suite. The list contains direct links to the documents in PDF format.

Step 2. Alternatively, you can navigate within the DVD menu to a particular product and click on the Product Documentation link to open the User Guide in PDF format for that product.

F.2 Tango/04 University

In a continuous effort to provide all users of Tango/04 technologies with high quality training and education, Tango/04 Computing Group presents the new training program open to partners and users worldwide.

Tango/04 University is aimed at providing Tango/04 users and partners with the most effective tools and knowledge to manage Tango/04 technologies and products and use them at their highest potential.

Attendance of the training course and passing the related exams is mandatory in order to qualify as Tango/04 Business Partner for the technology area covered by the course, and will offer you important benefits such as:

• Tango/04 Official Certifications - Tango/04 partners will be required to have a number of certified consultants, depending on the Business Partner Level
• Exploit the full potential of Tango/04 technologies - Solutions such as VISUAL Message Center and VISUAL Security Suite are very broad solutions that feature much functionality. Knowing all these functions and how to use them is key to getting the most out of the product.

• Integration with other solutions - Tango/04 is constantly growing: knowing the new products and agents may allow you to integrate other parts of the IT infrastructure into Tango/04 Solutions.

• Tango/04 Business Partners will learn how to effectively deploy a monitoring project in order to obtain the maximum effectiveness and customer satisfaction.

Participants’ profile: Consultants, System Administrators, operators and technical staff, with knowledge of Windows, iSeries, Linux and Unix systems who will be involved in managing or deploying Tango/04 technology.

Pre-requisites: Being Tango/04 Business Partner or Tango/04 Customer.
F.3 Contacting Tango/04

North America
Tango/04 North America
PO BOX 3301
NH 03458 Peterborough
USA
Phone: 1-800-304-6872 / 603-924-7391
Fax: 858-428-2864
sales@tango04.net
www.tango04.com

EMEA
Tango/04 Computing Group S.L.
Avda. Meridiana 358, 5 A-B
08027 Barcelona
Spain
Phone: +34 93 274 0051
Fax: +34 93 345 1329
info@tango04.net
www.tango04.com

Italy
Tango/04 Italy
Viale Garibaldi 51/53
13100 Vercelli
Italy
Phone: +39 0161 56922
Fax: +39 0161 259277
info@tango04.it
www.tango04.it

Sales Office in Switzerland
Tango/04 Switzerland
18, Avenue Louis Casaï
CH-1209 Genève
Switzerland
Phone: +41 (0)22 747 7866
Fax: +41 (0)22 747 7999
contact@tango04.net
www.tango04.fr

Latin American Headquarters
Barcelona/04 Computing Group SRL (Argentina)
Avda. Federico Lacroze 2252, Piso 6
1426 Buenos Aires Capital Federal
Argentina
Phone: +54 11 4774-0112
Fax: +54 11 4773-9163
info@barcelona04.net
www.barcelona04.com

Sales Office in Peru
Barcelona/04 PERÚ
Centro Empresarial Real
Av. Víctor A. Belaúnde 147, Vía Principal 140
Edificio Real Seis, Piso 6
L 27 Lima
Perú
Phone: +51 1 211-2690
Fax: +51 1 211-2526
info@barcelona04.net
www.barcelona04.com

Sales Office in France
Tango/04 France
La Grande Arche
Paroi Nord 15ème étage
92044 Paris La Défense
France
Phone: +33 01 40 90 34 49
Fax: +33 01 40 90 31 01
contact@tango04.net
www.tango04.fr

Sales Office in Chile
Barcelona/04 Chile
Nueva de Lyon 096 Oficina 702,
Providencia
Santiago
Chile
Phone: +56 2 234-0898
Fax: +56 2 2340865
info@barcelona04.net
www.barcelona04.com
About Tango/04 Computing Group

Tango/04 Computing Group is one of the leading developers of systems management and automation software. Tango/04 software helps companies maintain the operating health of all their business processes, improve service levels, increase productivity, and reduce costs through intelligent management of their IT infrastructure.

Founded in 1991 in Barcelona, Spain, Tango/04 is an IBM Business Partner and a key member of IBM's Autonomic Computing initiative. Tango/04 has more than a thousand customers who are served by over 35 authorized Business Partners around the world.

Alliances

- IBM Business Partner
- IBM Autonomic Computing Business Partner
- IBM PartnerWorld for Developers Advanced Membership
- IBM ISV Advantage Agreement
- IBM Early code release
- IBM Direct Technical Liaison
- Microsoft Developer Network
- Microsoft Early Code Release

Awards

- IBM All Star Award
- Products of the Year Award
- Apex Winner's Award
The information in this document was created using certain specific equipment and environments, and it is limited in application to those specific hardware and software products and version and releases levels.

Any references in this document regarding Tango/04 Computing Group products, software or services do not mean that Tango/04 Computing Group intends to make these available in all countries in which Tango/04 Computing Group operates. Any reference to a Tango/04 Computing Group product, software, or service may be used. Any functionally equivalent product that does not infringe any of Tango/04 Computing Group's intellectual property rights may be used instead of the Tango/04 Computing Group product, software or service.

Tango/04 Computing Group may have patents or pending patent applications covering subject matter in this document. The furnishing of this document does not give you any license to these patents.

The information contained in this document has not been submitted to any formal Tango/04 Computing Group test and is distributed AS IS. The use of this information or the implementation of any of these techniques is a customer responsibility, and depends on the customer's ability to evaluate and integrate them into the customer's operational environment. Despite the fact that Tango/04 Computing Group could have reviewed each item for accurateness in a specific situation, there is no guarantee that the same or similar results will be obtained somewhere else. Customers attempting to adapt these techniques to their own environments do so at their own risk. Tango/04 Computing Group shall not be liable for any damages arising out of your use of the techniques depicted on this document, even if they have been advised of the possibility of such damages. This document could contain technical inaccuracies or typographical errors.

Any pointers in this publication to external web sites are provided for your convenience only and do not, in any manner, serve as an endorsement of these web sites.

The following terms are trademarks of the International Business Machines Corporation in the United States and/or other countries: iSeries, iSeriese, iSeries, i5, DB2, e (logo)®, Server IBM®, Operating System/400, OS/400, i5/OS.

Microsoft, SQL Server, Windows, Windows NT, Windows XP and the Windows logo are trademarks of Microsoft Corporation in the United States and/or other countries. Java and all Java-based trademarks and logos are trademarks or registered trademarks of Sun Microsystems, Inc. in the United States and/or other countries. UNIX is a registered trademark in the United States and other countries licensed exclusively through The Open Group. Oracle is a registered trade mark of Oracle Corporation.

Other company, product, and service names may be trademarks or service marks of other companies.