

IBM Tivoli Composite Application Manager for Transactions V7.3

Configuring a Web Response Time agent to monitor
HTTPS transactions



© 2012 IBM Corporation

IBM Tivoli® Composite Application Manager for Transactions V7.3, Configuring a Web
Response Time agent to monitor HTTPS transactions

Assumptions

Before you proceed, the module designer assumes that you have these skills and knowledge:

- Create a keystore
- Import certificates
- Configure the Web Response Transactions agent

The module developer assumes that you can create a keystore, import certificates, and configure the Web Response Transactions agent.

Objectives

When you complete this module, you can perform these tasks:

- Create a keystore for use by the Web Response Transaction agent
- Import a certificate into the keystore
- Configure the Web Response Transaction agent to monitor HTTPS transactions

When you complete this module, you can perform these tasks:

- Create a keystore for use by the Web Response Transaction agent
- Import a certificate into the keystore
- Configure the Web Response Transaction agent to monitor HTTPS transactions

Export the certificate from the web server

- Steps to export the certificate
 - Start the ikeyman utility and choose the correct certificate
 - Export the certificate to a .p12 file
- Note: The certificate might already be available from the certificate authority, in which case skip exporting the certificate

These are the steps to export the certificate from the web server:

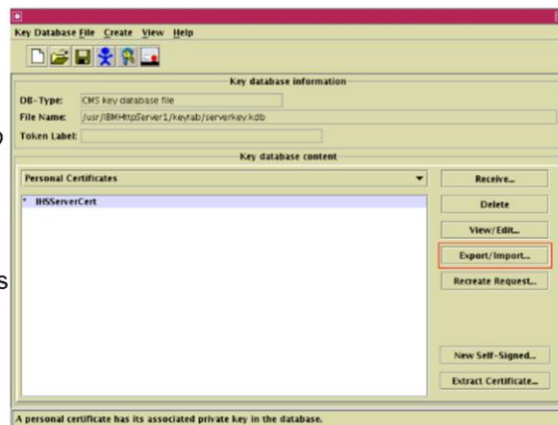
- Start the ikeyman utility and choose the correct certificate
- Export the certificate to a .p12 file

Note: The certificate might already be available from the certificate authority, in which case skip exporting the certificate.

Start ikeyman and choose the certificate

Example:

- Web server is on *iago.tivlab.austin.ibm.com*
 - IBM HTTP Server is configured to use the keystore */usr/IBMHttpServer1/keytab/serverkey.kdb*
1. Start the **ikeyman** utility and open the keystore that the web server uses
 2. Select the **Personal Certificate** view and highlight the certificate that the server uses to authenticate the application you want to monitor
 3. Highlight the certificate
 4. Click **Export/Import**



5

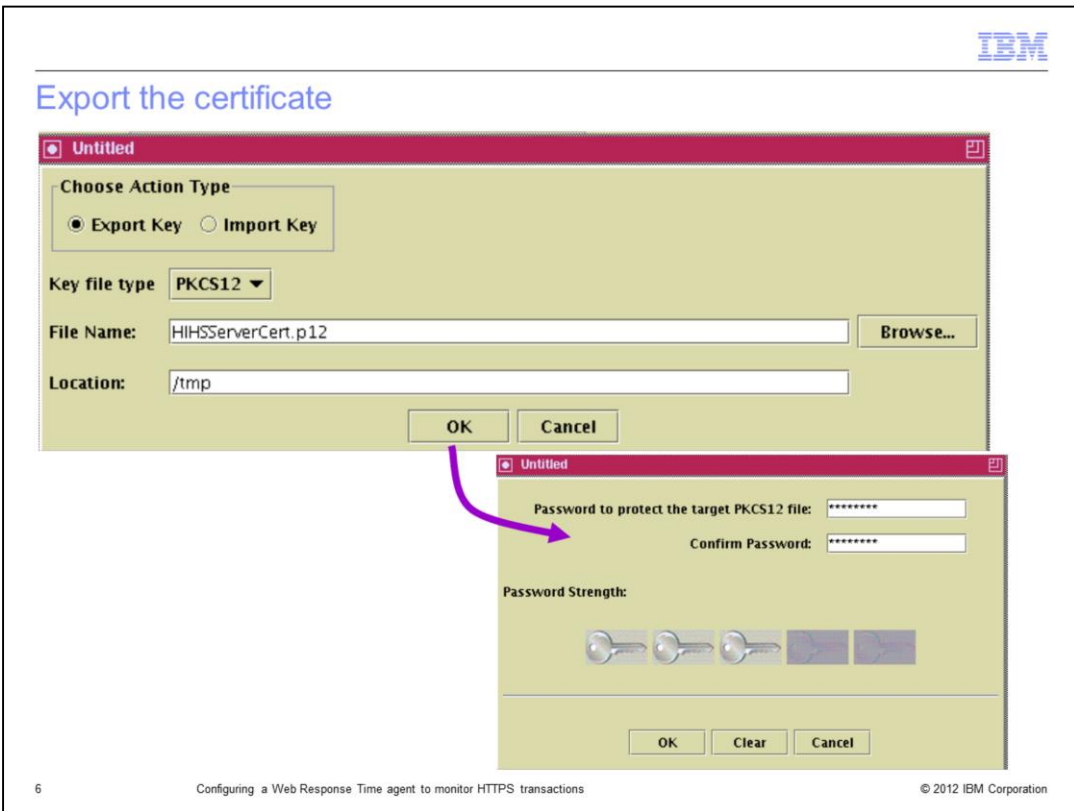
Configuring a Web Response Time agent to monitor HTTPS transactions

© 2012 IBM Corporation

In this example, the web server located at **iago.tivlab.austin.ibm.com** and the IBM HTTP Server is configured to use the keystore **/usr/IBMHttpServer1/keytab/serverkey.kdb**.

1. Start the **ikeyman** utility and open the keystore that the web server uses.
2. Select the **Personal Certificate** view and highlight the certificate the server uses to authenticate the application you want to monitor.
3. Click the certificate to highlight it.
4. Click **Export/Import**.

Export the certificate



Export the certificate.

1. From the **Key file type** menu, select **PKCS12**.
2. Type a **File name** for the certificate.
3. Click **OK**. The password prompt window opens.
4. Type the certificate password in the two fields.
5. Click **OK**. The password prompt window closes.

Create a keystore for the WRT agent to use

Steps to create the WRT keystore

1. Copy the certificate file to the WRT system
2. Create a keystore
3. Import the certificate into the keystore
4. Save the keystore

The steps to create the Web Response Transaction (WRT) keystore are:

1. Copy the certificate file to the WRT system.
2. Create a new keystore.
3. Import the certificate into the keystore.
4. Save the keystore.

Copy the certificate

- Copy the **.p12** file to the system where the WRT agent is installed
- Example
Copy the certificate to **/opt/IBM/ITM/keyfiles/IHSServerCert.p12**

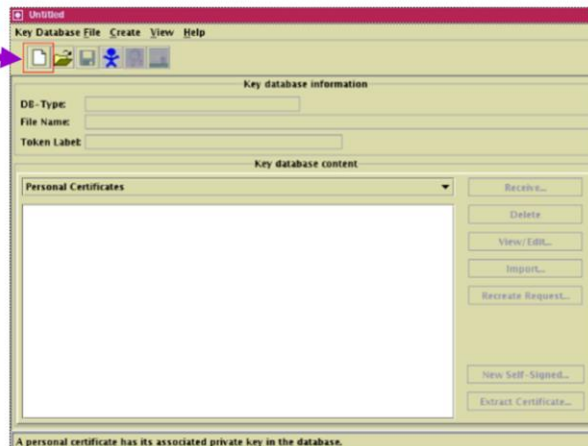
Copy the **.p12** file to the system where the WRT agent is installed.

For this example, copy the certificate to the **/opt/IBM/ITM/keyfiles/IHSServerCert.p12** directory.

Create keystore (1 of 2)

On the WRT system, create a keystore for the WRT agent to use to decrypt SSL packets sent to and from the server **iago.tivlab.austin.ibm.com**, IP address **9.48.205.152**.

1. Find the program **gsk7ikm** that is distributed with the WRT agent
2. Start **gsk7ikm**
3. Click the **Create a new key database file** icon



9

Configuring a Web Response Time agent to monitor HTTPS transactions

© 2012 IBM Corporation

On the WRT system, create a keystore for the WRT agent to use to decrypt SSL packets sent to and from the server **iago.tivlab.austin.ibm.com**, IP address **9.48.205.152**.

1. To find the program **gsk7ikm** distributed with the WRT agent, run these three commands:

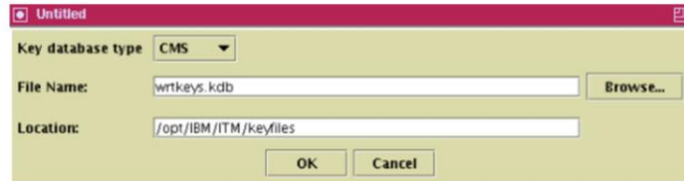
```
cd /opt/IBM/ITM/iago@/opt/IBM/ITM
find . -name gsk7ikm ./aix523/gs/bin/gsk7ikm
cd aix523/gs/bin/iago@/opt/IBM/ITM/aix523/gs/bin
```

2. Start **gsk7ikm**.

3. Click the **Create a new key database file** icon; it is the first icon in the icon list. A window opens.

Create new keystore (2 of 2)

5. From the **Key database type** menu, click **CMS**.
6. Type the keystore name and location.
7. Click **OK**.
8. Give the keystore a password
9. Select the **Stash the password to a file** check box.
10. Click **OK**.



Key database type: CMS

File Name: wrtkeys.kdb

Location: /opt/IBM/ITM/keyfiles

OK Cancel



Password: *****

Confirm Password: *****

Set expiration time? 60 Days

Stash the password to a file?

Password Strength:

OK Reset Cancel

10

Configuring a Web Response Time agent to monitor HTTPS transactions

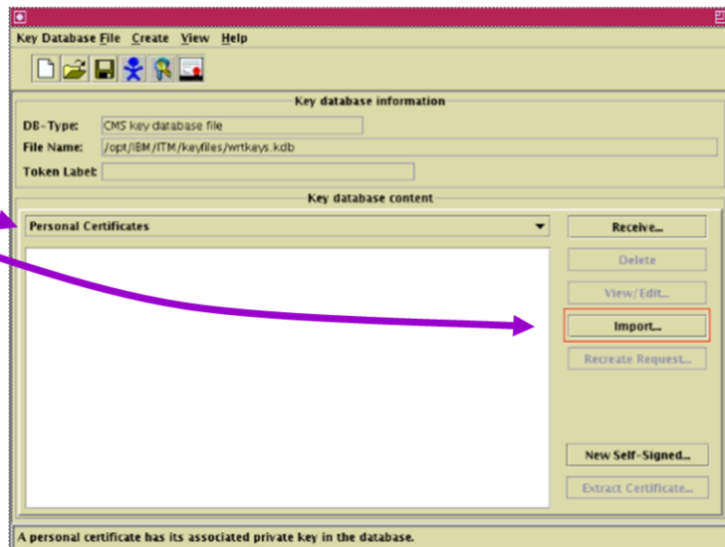
© 2012 IBM Corporation

5. From the **Key database type** menu, click **CMS**.
6. Type the keystore name and location. In this example, the keystore is named **wrtkeys.kdb**.
7. Click **OK**. A password window opens.
8. Type a password for the keystore.
9. Select the **Stash the password to a file** check box.
10. Click **OK**. The password window closes.

Import the certificate (1 of 3)

Import the **.p12** web server certificate into the keystore

1. Click **Personal Certificates**
2. Click **Import**
3. Type the **File name** and **Location** for the **.p12** certificate file
4. Click **OK**
5. Enter the password and click **OK**



11

Configuring a Web Response Time agent to monitor HTTPS transactions

© 2012 IBM Corporation

Import the **.p12** web server certificate into the keystore.

1. From the **Key database content** menu, click **Personal Certificates**.
2. Click the **Import** button. A new window opens.
3. Type the **File name** and **Location** for the **.p12** certificate file.
4. Click **OK**. A password prompt window opens.
5. Enter the password and click **OK**. The password prompt window closes and another window opens.

Import the certificate (2 of 3)

6. Type the **New label** for the certificate if required and click **OK**

7. Click the **Save** icon

8. Click a certificate name to highlight it

9. To examine the certificate, click **View/Edit**

12

Configuring a Web Response Time agent to monitor HTTPS transactions

© 2012 IBM Corporation

6. Type the new label for the certificate, if required, and click **OK**. The window closes.
7. Click the **Save** icon. The certificate is now saved in the keystore and can be examined.
8. Click a certificate name to highlight it.
9. Click the **View/Edit** button to examine the certificate.

Import the certificate (3 of 3)



The certificate is displayed. You can click **View Detail** for more information or **OK** to close the certificate window.

Configure WRT to use the new key database

1. Configure the T5 agent
2. Select the **Monitor HTTPS** option
3. Add **Certificate to Server** mapping
4. Stop and start the T5 agent

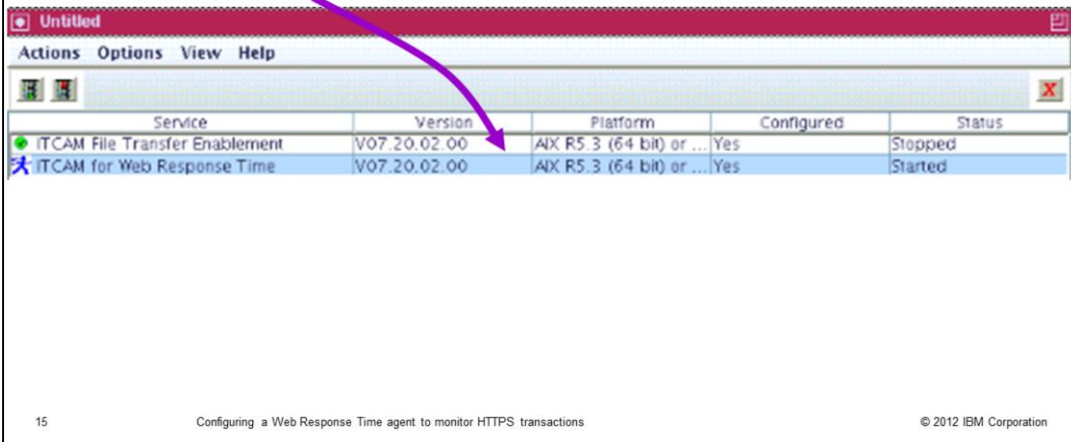
These are the steps to configure WRT to use the new key database:

1. Configure the T5 agent.
2. Select the **Monitor HTTPS** option.
3. Add **Certificate to Server** mapping.
4. Stop and start the T5 agent.

Configure the T5 agent

The keystore is saved in the Tivoli Monitoring directory `<ITM_HOME>/keyfiles` on the WRT agent system, so it is ready for use

1. Start Manage Tivoli Enterprise Monitoring Services (MTEMS)
2. Right-click the T5 agent and click **Configure**



The keystore has been saved in the ITM directory `<ITM_HOME>/keyfiles` on the WRT agent system, and it is ready for use.

1. Start **Manage Tivoli Enterprise Monitoring Services** (MTEMS).
2. Right-click the T5 agent and click **Configure** from the menu.

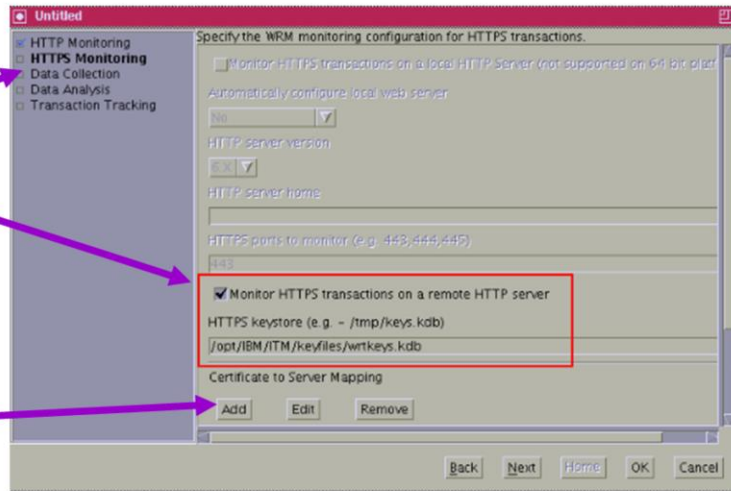
Configure the agent to monitor HTTPS

1. Click the **HTTPS Monitoring** dialog box

2. Select **Monitor HTTPS on a remote HTTP server** check box

3. Type the path to the keystore

Start to add the certificate to server mapping by clicking **Add**



16

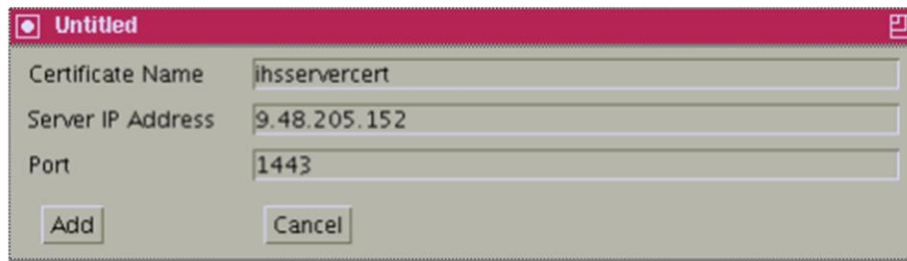
Configuring a Web Response Time agent to monitor HTTPS transactions

© 2012 IBM Corporation

To configure the agent to monitor HTTPS, perform these steps:

1. Navigate to the **HTTPS Monitoring** dialog box.
2. Select the **Monitor HTTPS on a remote HTTP server** check box.
3. Type the path to the keystore. Start to add the certificate to server mapping by clicking the **Add** button. A new window opens.

Configure certificate to server mapping (1 of 2)



The screenshot shows a dialog box titled "Untitled" with a red header bar. It contains three input fields: "Certificate Name" with the value "ihsservercert", "Server IP Address" with the value "9.48.205.152", and "Port" with the value "1443". At the bottom of the dialog are two buttons: "Add" and "Cancel".

17

Configuring a Web Response Time agent to monitor HTTPS transactions

© 2012 IBM Corporation

If the web server listens on more than one port, add a certificate mapping for each port. To configure certificate to server mapping, perform these steps:

1. In the **Certificate Name** field, type the label name.
2. In the **Server IP Address** field, type the address of the web server where the certificate was extracted. This is the destination IP address in the request to the web server.
3. Type the port number that the web server listens to for HTTPS traffic. This is the destination port in the request to the web server.
4. Click **Add**. The window closes.

Configure certificate to server mapping (2 of 2)

Specify the WRM monitoring configuration for HTTPS transactions.

HTTP server home

HTTPS ports to monitor (e.g. 443,444,445)

443

Monitor HTTPS transactions on a remote HTTP server

HTTPS keystore (e.g. - /tmp/keys.kdb)

/opt/IBM/ITM/keyfiles/wrtkeys.kdb

Certificate to Server Mapping

Add Edit Remove

Certificate Name	Server IP Address	Port
ihsservercert	9.48.205.152	1443

Back Next Home OK Cancel

18

Configuring a Web Response Time agent to monitor HTTPS transactions

© 2012 IBM Corporation

The window updates with the information, showing that the WRT agent uses the **Certificate Name** labeled **ihsservercert** in the SSL handshake for any HTTPS requests bound for **IP Server Address** and **Port 9.48.205.152:1443**.

At the bottom of the window, click **OK**.

Stop and start the T5 agent

1. Stop and start the T5 agent to read the configuration changes
2. Ensure that an appropriate profile is distributed to the T5 agent
3. Generate some traffic on the web server that the T5 agent monitors

The Tivoli Enterprise Portal now lists the application

Application Current Status Details			
Application	Importance	Percent Available	Per
9.48.205.152	Medium	100.000	
iago.tivlab.austin.ibm.com:1443	Medium	100.000	

19

Configuring a Web Response Time agent to monitor HTTPS transactions

© 2012 IBM Corporation

1. Stop and start the T5 agent to read the configuration changes. Run these two commands:

```
/opt/IBM/ITM/bin/itmcmd agent stop t5
```

```
/opt/IBM/ITM/bin/itmcmd agent start t5
```

Note: The Certificate to Server mapping is stored in `<ITM_HOME>/tmaitm6/wrm/keystore/servermap.csv`. If needed, you can run this command to catalog the file:

```
cat /opt/IBM/ITM/tmaitm6/wrm/keystore/servermap.csv
9.48.205.152, 1443, ihservercert
```

2. Ensure that an appropriate profile is distributed to the T5 agent.
3. Generate traffic on the web server being monitored by the T5 agent. In this example, you can access the URL <https://iago.tivlab.austin.ibm.com:1443/readme.html>.

The Tivoli Enterprise Portal lists the application.

Summary

Now that you completed this module, you can perform these tasks:

- Create a keystore for use by the Web Response Transaction agent
- Import a certificate into the keystore
- Configure the Web Response Transaction agent to monitor HTTPS transactions

Now that you have completed this module, you can perform these tasks:

- Create a keystore for use by the Web Response Transaction agent
- Import a certificate into the keystore
- Configure the Web Response Transaction agent to monitor HTTPS transactions

Trademarks, disclaimer, and copyright information

IBM, the IBM logo, ibm.com, and Tivoli are trademarks or registered trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of other IBM trademarks is available on the web at "[Copyright and trademark information](http://www.ibm.com/legal/copytrade.shtml)" at <http://www.ibm.com/legal/copytrade.shtml>

THE INFORMATION CONTAINED IN THIS PRESENTATION IS PROVIDED FOR INFORMATIONAL PURPOSES ONLY. WHILE EFFORTS WERE MADE TO VERIFY THE COMPLETENESS AND ACCURACY OF THE INFORMATION CONTAINED IN THIS PRESENTATION, IT IS PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. IN ADDITION, THIS INFORMATION IS BASED ON IBM'S CURRENT PRODUCT PLANS AND STRATEGY, WHICH ARE SUBJECT TO CHANGE BY IBM WITHOUT NOTICE. IBM SHALL NOT BE RESPONSIBLE FOR ANY DAMAGES ARISING OUT OF THE USE OF, OR OTHERWISE RELATED TO, THIS PRESENTATION OR ANY OTHER DOCUMENTATION. NOTHING CONTAINED IN THIS PRESENTATION IS INTENDED TO, NOR SHALL HAVE THE EFFECT OF, CREATING ANY WARRANTIES OR REPRESENTATIONS FROM IBM (OR ITS SUPPLIERS OR LICENSORS), OR ALTERING THE TERMS AND CONDITIONS OF ANY AGREEMENT OR LICENSE GOVERNING THE USE OF IBM PRODUCTS OR SOFTWARE.

© Copyright International Business Machines Corporation 2012. All rights reserved.