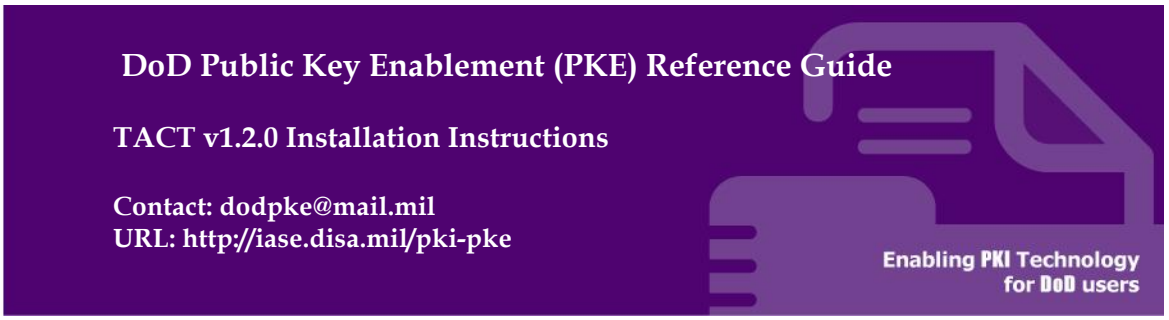


Trust Anchor Constraint Tool (TACT) v1.1.2 Installation Instructions

16 June 2014

Version 1.2.0

DoD PKE Team

Revision History

Issue Date	Revision	Change Description
01/27/2012	1.0	Initial release
06/22/2012	1.0.3	Added statement to section on IIS6 activation steps clarifying that similar steps are not required in IIS7 and later
12/29/2012	1.1	Updated for TACT 1.1. Add section on Apache/Windows. Add advice for integrated app pool usage.
2/21/2013	1.1.1	Updated for TACT 1.1.1 platforms.
3/20/2013	1.1.2	Add Windows 8/Server 2012, update versions to 1.1.2
6/16/2014	1.2.0	Updated for TACT 1.2.0. Add section on new features for mod_nss

Contents

Overview

This guide is intended to provide step-by-step instructions for installing the Trust Anchor Constraint Tool (TACT) software onto a web server, or for installing the TACT utilities onto a server or workstation. The guide assumes that the server is already configured for https client certificate authentication prior to installation.

Supplemental Information

The DoD Public Key Enabling (PKE) web site located at http://iase.disa.mil/pki-pke contains many informational documents and best practice guides related to PK-enablement and certificate validation implementation in the DoD. Guidance for the full configuration of Microsoft Internet Information Services (IIS) 6, IIS 7 and the Apache web server with both mod_ssl and mod_nss is available on the site.

Installation Overview

TACT components are divided into groups that can be installed together or separately. All TACT utilities can function independently of each other, although the installers on different platforms may group them slightly differently in order to most efficiently use the platform's native package management features.

Available Packages

There are different TACT installers for different platforms:

- **TACT for 64-bit Windows platforms**: This msi can be installed on Windows 7, Windows 8, Windows Server 2003, Windows Server 2008, Windows Server 2008R2 and Windows Server 2012.
- **TACT for 32-bit Windows platforms**: This msi can be installed on 32-bit editions of Windows 7, Windows Server 2003 and Windows Server 2008.
- **TACT for 64-bit Windows platforms with apache**: This msi can be installed on Windows 7, Windows Server 2003, Windows Server 2008 and Windows Server 2008R2 where apache is being used as the web server.
- **TACT for 32-bit Windows platforms with apache**: This msi can be installed on 32-bit editions of Windows 7, Windows Server 2003 and Windows Server 2008 where apache is being used as the web server.
- **TACT for 64-bit RHEL 5 platforms:** This package can be installed on Red Hat Enterprise Linux 5.8.
- **TACT for 64-bit RHEL 6 platforms:** This package can be installed on Red Hat Enterprise Linux 6.3.
- **TACT for 32-bit RHEL 5 platforms:** This package can be installed on Red Hat Enterprise Linux 5.8.
- **TACT for 32-bit RHEL 6 platforms:** This package can be installed on Red Hat Enterprise Linux 6.3

Each installer can install platform-appropriate plug-ins and/or management applications.

TACT Management Applications

The TACT management applications can be installed independent of the plug-ins on all platforms. This enables easy creation of configuration files which can then be transferred to a server with the plug-in, as well as offline analysis of server configurations.

The TACT archive contains two installation scripts: `installtact.sh` and `installtact-nonstandard.sh`. Both scripts are identical with regard to the management applications. The only differences between the two are related to plugin installation.

Installing TACT Management Applications on Linux

The default installation procedure should suffice in all cases for the TACT management applications on Linux systems. Note that you must have root privileges in order to complete the installation.

Step	Explanation	Example
1.	Unpack the archive.	`$ tar jxf tact-1.0.0-linux.tar.bz2`
2.	Become the super-user.	`$ su`
3.	Change into the extracted directory	`# cd install-tact`
4.	Execute the installation script	`# bash ./installtact.sh`

Once the installation script begins, there will be a series of prompts. In all cases, the defaults are acceptable for the Graphical User Interface (GUI) and command-line utilities.

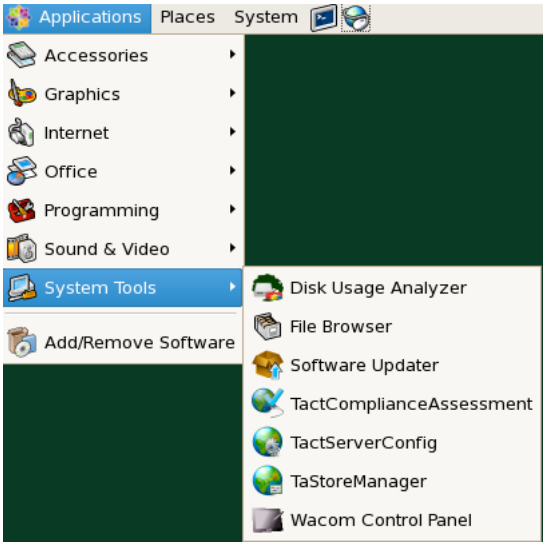
```
Select an installation type:
[A]ll, [G]UI utilities only, [C]ommand-line utilities only, [P]lug-in only, E[x]it
[A] G
Installing TACT GUI utilities
Where should TACT configuration data be stored? [/etc/tact]
Where should TACT TA databases be stored [/etc/tact/tas]
Where should TACT Policy databases be stored [/etc/tact]
Where should server log files be written? [/var/log/tact]
Where should the TACT PKI log database be written? [/var/log/tact/pkilog.db]
```

Sample Installation Session

If both the GUI and command-line utilities are needed, re-run the script to select the other option.

Once installed, the GUI tools can be found in the applications menu or launched via the command line. Symbolic links to the GUI tools are placed in /usr/local/bin. Default configurations for the tools are found in /etc/tact and may be changed by a system administrator. The default configurations in the installer archive may also be changed prior to installation if necessary.

Upon first execution of each management application, open the options dialog and navigate to the desired settings files to prepare the application for use.

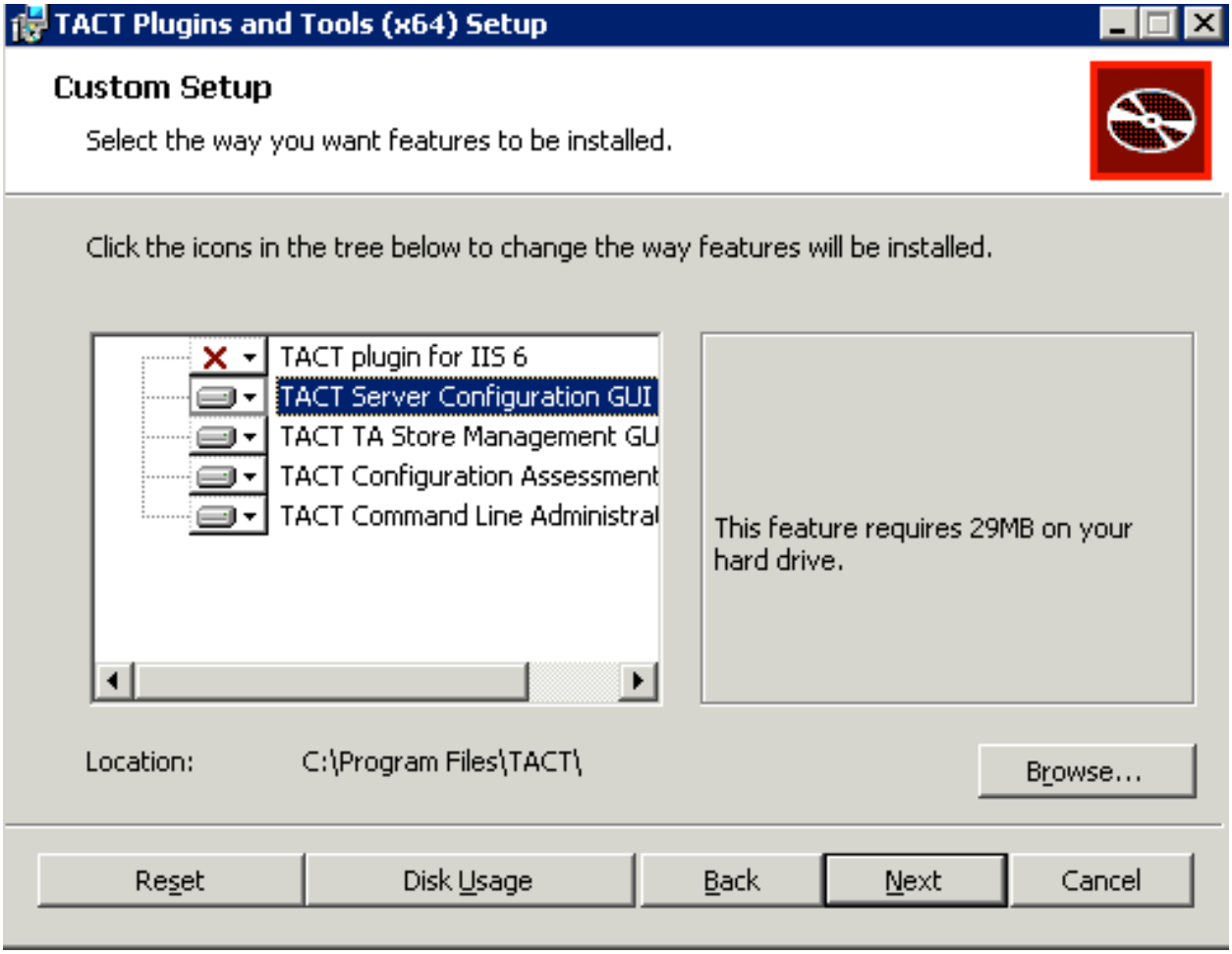


Installing TACT Management Applications on Windows

Special note for Windows Server 2003: A bug on server 2003 can prevent the standard TACT windows installer from completing if IIS is not installed on the system. If TACT management applications are needed on a Server 2003 system that does not have IIS installed, a separate installer **tacttools-version-platform.msi** is available from the TACT download site. This separate installer is only necessary on Server 2003 systems that do not have IIS installed.

To begin installation, make sure to select the appropriate msi file for your platform. 64-bit editions of Windows should use the msi with x64 in the name, and 32-bit editions of Windows should use the msi with x86 in the name. If the wrong msi is used, an error will be displayed prior to installation, and installation will not proceed.

In most cases, simply double-click the msi to begin installation.



To install the management utilities alone, ensure that the plug-in is not selected in the feature tree. (Note that the exact contents of the feature tree may differ depending on the capabilities of the target system.)

Click next to see various configuration options. There is no reason to change any of these unless the plug-in is being installed. After clicking Finish, the utilities will be available from the Windows start menu.

Upon first execution of each management application, open the options dialog and navigate to the desired settings files to prepare the application for use.

TACT Plug-in

The TACT plug-in is contained within the same install archives as the TACT management applications. It's simply a matter of selecting different options during the install process. In most cases, it is advisable to install the management utilities along with the plug-in for ease of maintenance.

Installing the TACT Plug-in on Linux

The TACT plug-in is contained within the same installation package as the administration utilities. There are two different scripts for plugin installation on Linux. `installtact.sh` is for systems which use as standard Red Hat-supplied apache installation, with either mod_nss or mod_ssl. `installtact-nonstandard.sh` is for systems which use a custom apache installation (which is required for apache 2.0 or 2.4, as Red Hat does not supply a standard installation for those server versions as of this writing).

Some additional considerations may apply when installing the plug-in, as opposed to only the management utilities:

1. The default locations for configuration files are typically the best locations, particularly on systems where SELinux is enabled. If other locations are chosen, manual relabeling of the file system objects may be necessary before the server will function, depending on the SELinux configuration and policies.
2. The log files and the log database will need to reside in a location that is readable and writable by the web server account. They should also be on a file system that is separate from the root to prevent a log file that grows too rapidly from negatively impacting the system.
3. The configuration locations should be readable but not writable by the web server.

For standard, Red Hat-supplied Apache installations, always use installtact.sh.

```
Select an installation type:
[A]ll, [G]UI utilities only, [C]ommand-line utilities only, [P]lug-in only, E[x]it
[A]

Installing all TACT packages
Where should TACT configuration data be stored? [/etc/tact]
Where should TACT TA databases be stored [/etc/tact/tas]
Where should TACT Policy databases be stored [/etc/tact]
Where should server log files be written? [/var/log/tact]
Where should the TACT PKI log database be written? [/var/log/tact/pkilog.db]
Saving selected options to /tmp/install-tact/install.cf
Proceed with installation? (y/n) [Y]
```

For mod_nss systems, once the plug-in has been installed by the script, all that remains to be done is to configure it and activate it. Simply edit the configuration database and

Trust Anchor (TA) store as outlined in the user guide, restart httpd, and TACT will be active.

For mod_ssl systems, one additional step is required. In the mod_ssl configuration file, the server was configured with a list of trusted CAs using either or both of the `SSLCACertificatePath` directive or the `SSLCACertificateFile` directives. Before starting TACT, the value of this directive must be copied to tact.conf as either `CTModSSLCACertificatePath` or `CTModSSLCACertificateFile`, respectively. TACT will not start successfully if mod_ssl is present until one of these directives is updated to match the corresponding entry in mod_ssl's configuration file.

```
CTModSSLCACertificateFile /etc/pki/tls/certs/ca_certs/alldodcerts.pem
```

Non-standard Apache Installations

On systems where Apache 2.2 has been custom compiled, where Apache 2.0 is in use, or where Apache 2.4 is in use, the standard installation script's attempts at automated configuration are unlikely to match the apache installation. For these systems, use installtact-nonstandard.sh instead. This script will generate a configuration file and offer guidance for how to find the correct location for installation. Generally, custom apache installations are an advanced configuration item and administrators who maintain them are expected to understand where the installed httpd needs to find configuration files and loadable modules.

Once the script finishes, it prints output similar to the following:

```
**************************************************************
**************************************************************
**************************************************************
**************************************************************
In order to complete the TACT plug-in installation, you'll need to:
1. Make certain that the TACT plugin can write to its log file in /var/log/tact
2. Make certain that the user account used by the service can create files in
/var/log/tact
3. If a custom SELinux policy is in place, make sure that these locations are
writable by the apache user account under that policy as well.
4. Create a symbolic link to the appropriate TACT plugin in your apache
installation's
modules directory.
For example:
ln -s /usr/local/redhound/lib/mod_auth_tact20.so
/usr/local/apache2/modules/mod_auth_tact.so
is necessary for Apache 2.0. See the installation guide for more information.
5. Copy the generated tact.conf file from this directory to your appache
installation's
configuration directory and make sure that it gets included by one of the other files
after your SSL module loads. Usually this can be accomplished by copying the conf
file
to conf.d
If you\'re using mod_ssl, do not forget to configure the
CTModSSLCACertificateFile or CTModSSLCACertificatPath
directive in tact.conf.
```

```
************************************************************
************************************************************
************************************************************
************************************************************
```

In particular, note the need to create a symbolic link into the apache modules directory. The command to do so will differ depending on the apache version. From a shell prompt within the modules directory, (frequently `/etc/httpd/modules` or `/usr/local/apache2/modules`), issue one of the following commands.

Apache 2.0

```
ln -s /usr/local/redhound/mod_auth_certtrust20.so mod_auth_certtrust.so
```

Apache 2.2

```
ln -s /usr/local/redhound/mod_auth_certtrust.so mod_auth_certtrust.so
```

Apache 2.4

```
ln -s /usr/local/redhound/mod_auth_certtrust24.so mod_auth_certtrust.so
```

This will allow apache to find the module when it's reference from a configuration file. Once the link is created, the plug-in needs to be enabled within the apache configuration system. For most servers, this means copying tact.conf to the apache server root config directory, then adding an include directive in httpd.conf to load it. Note that mod_auth_certtrust.so must be loaded **after** mod_nss or mod_ssl within httpd.conf or the server will not start.

Finally, appropriate permissions must be established for log and configuration files. The TACT log directory must be readable and writable by the user account that the apache service runs under (frequently nobody, apache, daemon or httpd). The TACT PKI log database must be readable and writable by httpd's user account. That account must also have permission to create files in the directory containing the PKI log database. The TACT configuration directory must be readable by that same user.

Note: On certain apache custom configurations, TACT's pki log database can be created before httpd drops privileges. If TACT detects the prefork mpm and can determine the user and group child process will run as, TACT will attempt to change permissions on the log directory and database directory appropriately. If a different mpm is in use or TACT can't detect the user and group, depending on the account's umask, the permissions of the directory containing the database, the SELinux status, and the filesystem, the database created before httpd drops privileges may not be writable to later child processes. If this happens, TACT will return HTTP error 403 (forbidden) for all requests and write a message to its log file indicating that the database could not be updated. To remedy this, the administrator simply needs to edit the permission on the database file so that the lower-privileged apache account can read and write to that file.

Enabling Full Path Building for mod_nss

As of TACT 1.2.0, an additional mode of operation is supported for mod_nss on Apache 2.2. TACT can build certification paths itself, rather than relying on the path returned by mod_nss, and can use CRLs or OCSP responses to check revocation status. When TACT is operating in this mode, it is safe to disable mod_nss path processing.

There are two mechanisms for disabling this. With the default mod_nss, as shipped by Red Hat, the only option is to mark every certification authority that may issue client certificates as trusted (trust flags "CT,C,C") within the NSS database. While this is effective, there are two significant limitations:

1. All intermediate certification authorities must be known to the server operator and installed in the server's NSS database proactively.
2. If this list grows too large, users with Internet Explorer will become unable to access the site. The threshold is not documented.[1]

To address these limitations, a patched version of mod_nss is included with TACT.[2] To install the patched mod_nss, the following steps are necessary when using the system-installed httpd. For other configurations, see Appendix E for building the patch from source and overwrite `libmodnss.so` within the configuration's modules location.

Once the patch is installed, two new directives are available for mod_nss. `NSSVerifyClient` will now accept a value of `external`. When configured for external verification, mod_nss will query TACT to ensure that it is active, then defer all path processing to TACT. Additionally, `NSSSendNullCaList` will, if set to `on`, cause mod_nss to send an empty list of client CA names during the handshake. As a result, browsers will prompt the user to select any certificate with acceptable key usage for authentication.

Once mod_nss is configured either with a set of trusted intermediate CAs or with the patches supplied with TACT, some additional configuration is required within TACT to enable full path building. The following directives must be added to tact.conf:

```
CertTrustCertStoreLocation      /var/tact/certs
CertTrustCrlStoreLocation       /var/tact/crls
CertTrustEnablePathBuilder
```

[1] Through testing, it was determined that the threshold is based on the size of the list of names sent from the server to the client. As of this writing, for Internet Explorer 11 the limit was between 32215 and 32341 bytes of names, which, in the tested configuration, was 262 Certification Authorities. Because the threshold is neither documented by Microsoft nor specified in the relevant standards, it may go up or down at any time. Microsoft servers will send a documented maximum 16384 bytes of names, so careful testing should be performed any time a hint list sent to a Microsoft client exceeds this size.

[2] The published mod_nss build will run on 32-bit RHEL 5 with the vendor-supplied apache installation. For other configurations, see Appendix X for instructions on building the patch.

CertTrustCertStoreLocation is the location where TACT will redirect any folder-based certificate stores configured within the .sdb file. It must be writable to the unprivileged user used by apache and must exist.

CertTrustCrlStoreLocation is the location where TACT will redirect any folder-based CRL stores configured within the .sdb file. It must be writable to the unprivileged user used by apache and must exist. It is best to indicate the same path in the .sdb file as wil be arrived at in TACT in order to browse contents using the configuration utilities. For example, if /var/tact/crls is entered in tact.conf, enter /var/tact/crls/crls in the .sdb file. This is only relevant if browsing the folder contents through the configuration utilities is desired. The same applies to the certificate store values as well.

These two locations may be the same, provided that the path settings in the .sdb file are configured to use different folders for certificates and CRLs.

CertTrustEnablePathBuilder, if present, will cause TACT to use the certification path building and revocation status checking options configured within the .sdb file.

Step	Explanation	Example
1.	Become the super-user.	`$ su`
2.	Stop the http server.	`# /sbin/service httpd stop`
3.	Replace mod_nss	`# cp libmodnss.so /etc/httpd/modules/`
4.	Edit nss.conf to enable the new features	`NSSVerifyClient external` `NSSSendNullCaList on`

5.	Edit tact.conf to enable the new features	`CertTrustCertStoreLocation /var/tact/certs`
		`CertTrustCrlStoreLocation /var/tact/crls`
		`CertTrustEnablePathBuilder`

6.	Start the http server.	`# /sbin/service httpd start`

Disabling an Installed Plug-in

To temporarily deactivate the TACT plug-in on a Linux system, apache needs to be prevented from loading the plug-in when it starts. Note that once TACT is disabled, any Trust Anchor (TA) constraints established in its TA store will not be enforced until it is re-enabled and Apache is restarted. On a default apache installation, renaming tact.conf is sufficient. Custom installations may require other steps. Consult these systems' build documentation for further guidance.

Step	Explanation	Example
1.	Become the super-user.	`$ su`
2.	Stop the http server.	`# /sbin/service httpd stop`

3.	Rename the configuration file so that apache will ignore it upon restart.	`# mv /etc/httpd/conf.d/tact.conf /etc/httpd/conf.d/tact.conf.disabled`
4.	Start the http server.	`# /sbin/service httpd start`

When it's time to re-enable the plug-in, simply rename tact.conf.disabled to tact.conf and restart the server again.

SELinux

On systems where SELinux is enabled, set to "enforcing" mode, and configured with targeted policies defined for httpd, additional steps may be necessary to label TACT's items with appropriate context.

The installation script attempts to detect this, and prints information to the console along with an example script containing suggested commands. On some systems, the script may not be able to detect the SELinux status, or management tools may be missing. On these systems, the script will print an alert once TACT has been installed, reminding the administrator to ensure that the SELinux profile is adjusted before running TACT.

The install script writes out the specific commands necessary on a typical RHEL 5.8 or 6.3 installation in a form suitable for copy-and-paste into the command prompt, as well as a sample bash script.

For custom installations that use targeted enforcement, consult the documentation for the targeted policies installed on the system. The labels need to permit httpd read/write access to the PKI log database, read/write/create access for the directory containing that database, read access to the TACT configuration files, and read/write access to the TACT log file. Additionally, mod_auth_certtrust.so (or mod_auth_certtrust20.so or mod_auth_certtrust24.so, as applicable to the apache version in question) must be loadable by the apache httpd process.

Removing the TACT Plug-in on Linux

To permanently remove the TACT plug-in, simply uninstall the rpm containing it.

```
# rpm –e tactplugin
```

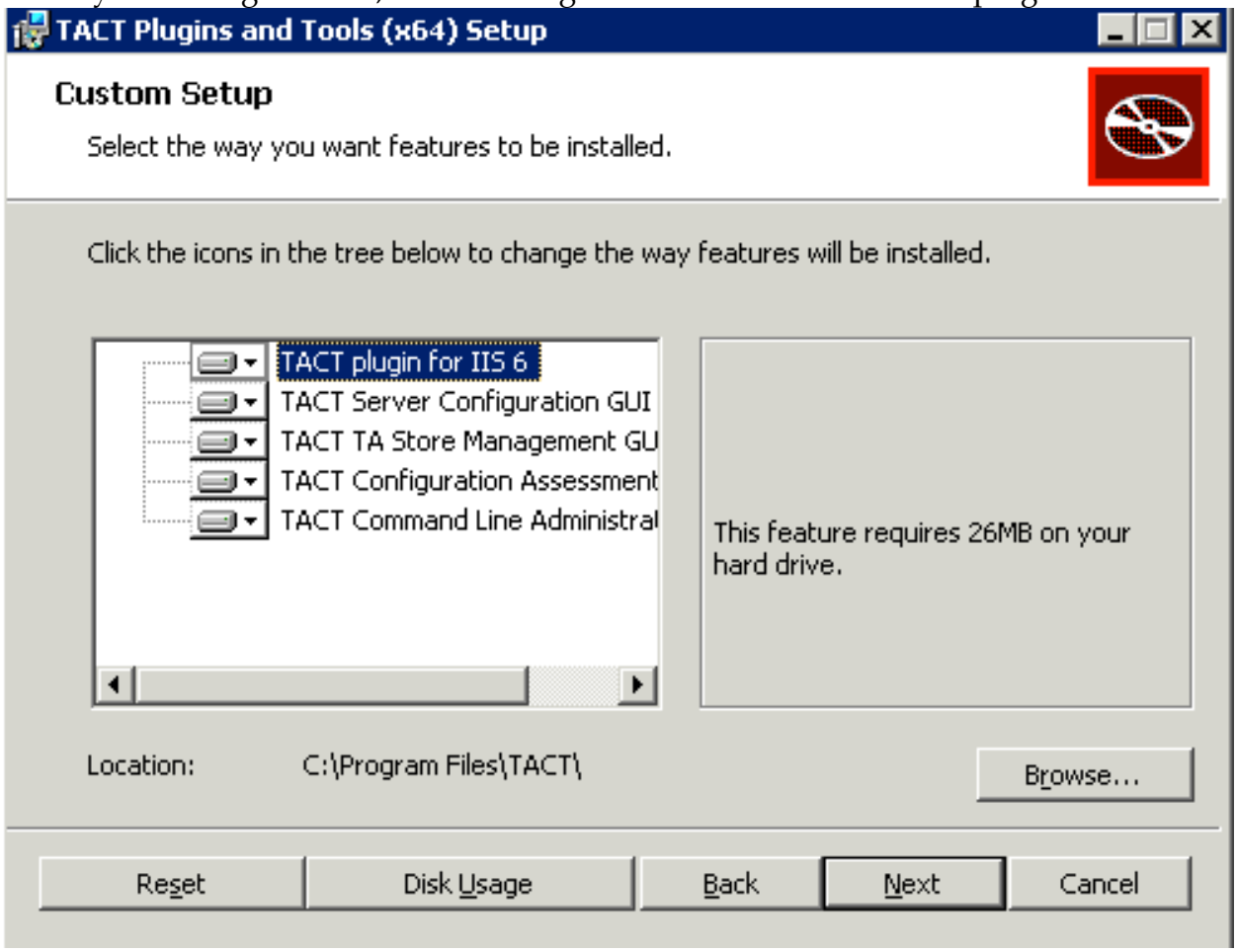
This will not remove any of the configuration or log files you've created on the system. Those must be removed manually, either from the custom selected locations or from the default /etc/tact and /var/log/tact.

Installing the TACT plug-in for IIS on Windows

As on Linux, the TACT plug-in on Windows is contained within the same archive as the management tools. Similarly, it is usually advisable to perform a complete installation on systems that will run the plug-in.

When installing the plug-in, there may be more reason to pay attention to the default settings than when installing the management applications alone. In particular, the log files and log database will need to be writable by the web server's service account (or application pool account on Server 2008). The log files and database should also be stored on a drive that can sustain substantial file growth without jeopardizing the system.

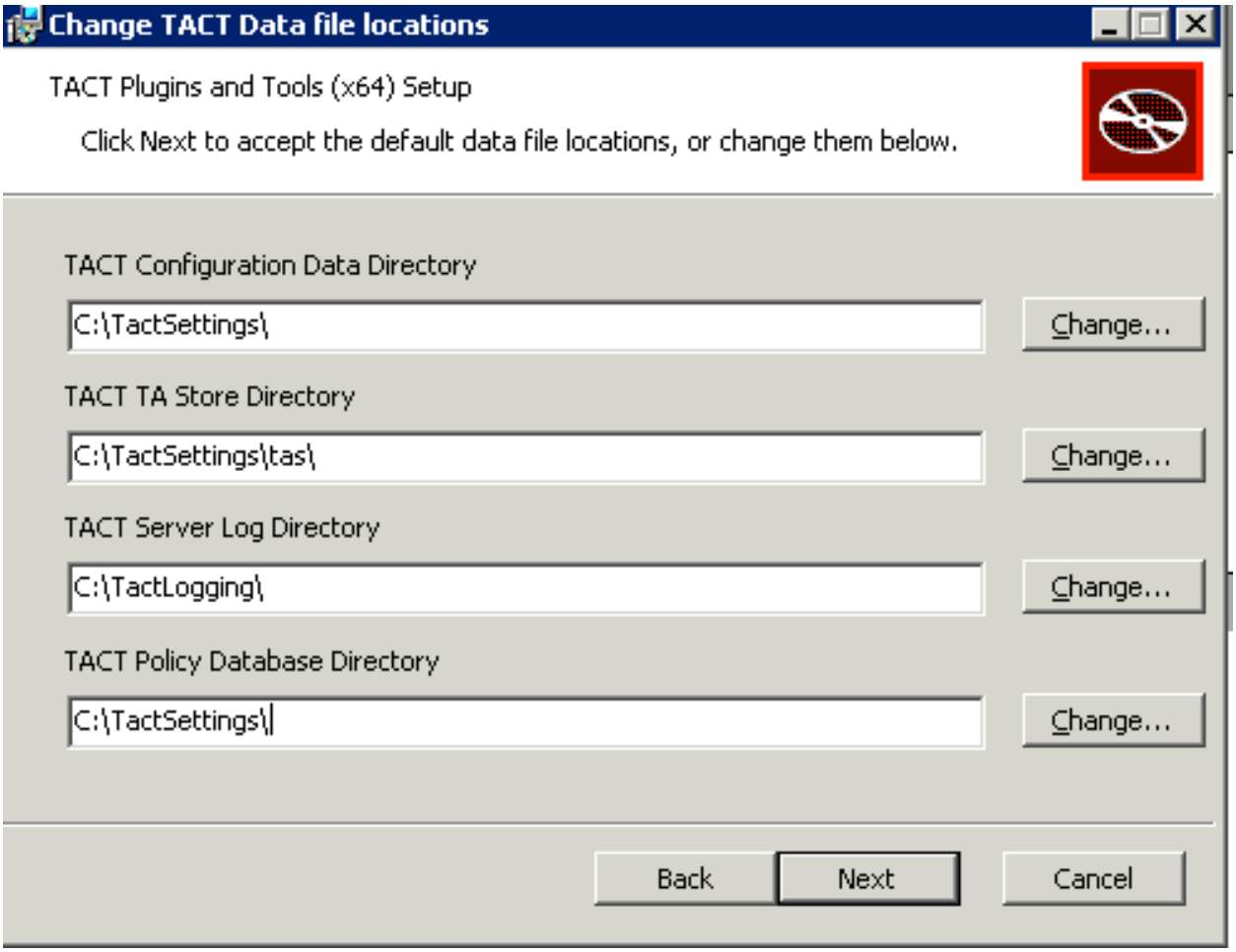
Start by launching the .msi, and selecting a feature set that includes a plug-in.



Note: The plug-in will only appear on the list of features if a compatible web server is detected on the system. If no plug-in is available, ensure that the web server role is configured and active.

Make certain to change any directories that are inappropriate for the target system. The installer will create custom directories here, and copy initial configurations into them.

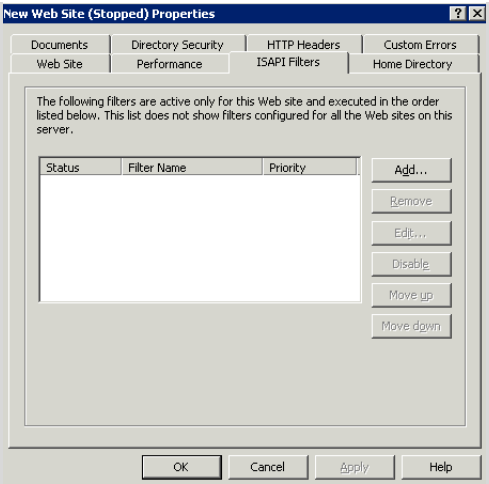
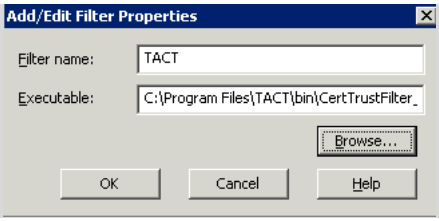
Note that directories or configurations created on this screen will not be removed by the uninstaller, to prevent the loss of user-created or modified configuration data.



Once the installer completes, stop IIS if it's running, edit TACT configurations, start IIS, and confirm that TACT is enabled by looking at the logs.

Activating TACT for a site on IIS 6.0

On IIS 6.0 (on Windows Server 2003), TACT must be activated on a per-site basis. Similar steps are not required for IIS7 and later. The following steps explain how to load it for each site where trust anchor constraints are required.

Step	Explanation	Example
1.	Launch the IIS Management Console.	
2.	Right-click on the new web site and choose "Properties…"	
3.	Select ISAPI filters.	
4.	Click "Add…"	
5.	Enter a name you'll recognize and select CertTrustFilter_ISAPI.dll from the TACT install location	
6.	Click OK, then restart IIS.	

Disabling an Installed Plug-in

For Windows, it is currently recommended to uninstall the plug-in in order to disable it. All configuration data will be left intact and can be used upon reinstallation.

Uninstalling TACT

To uninstall TACT, use the Add/Remove Programs control panel. The uninstaller will not remove operator-created configuration data.

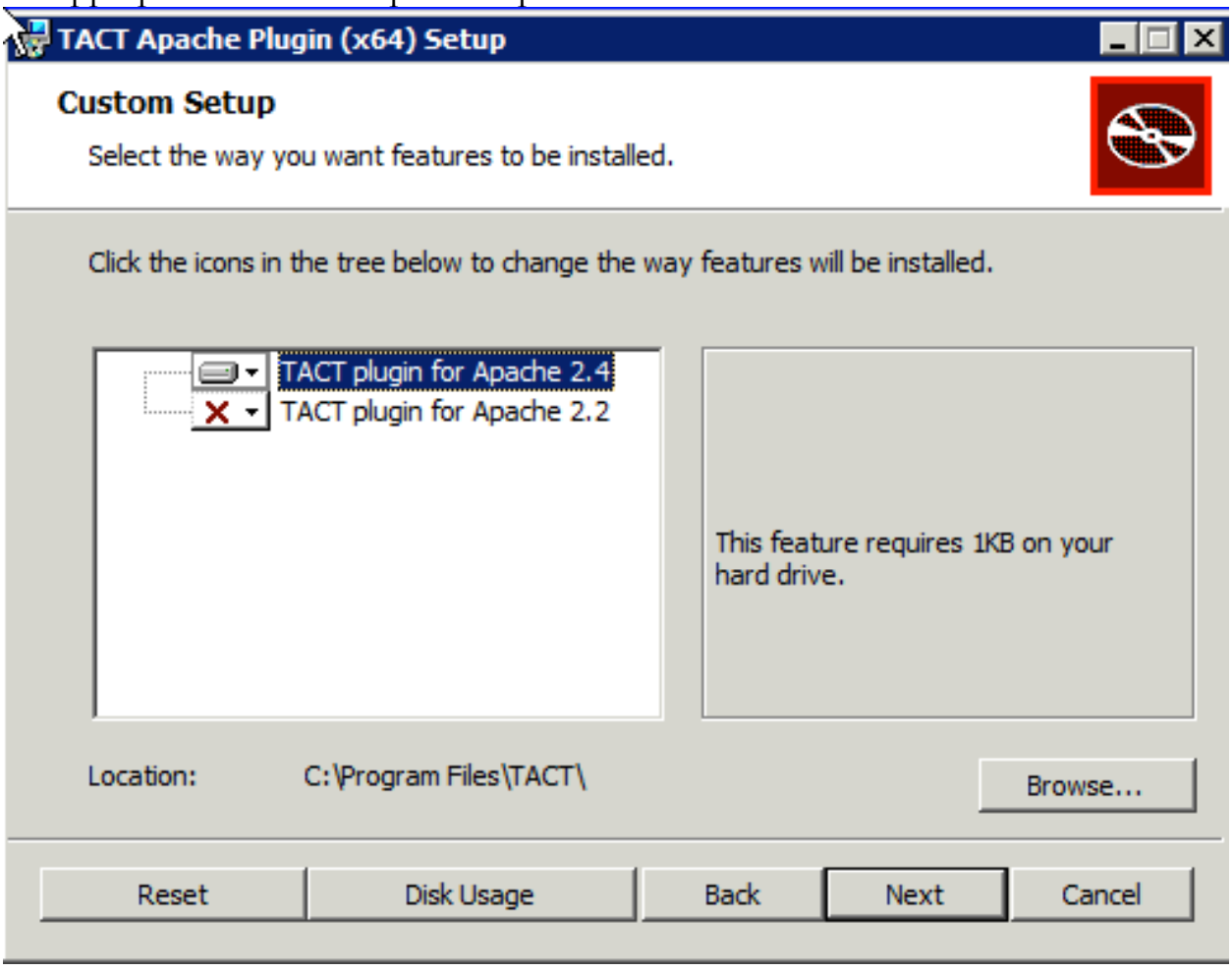
Installing the TACT plug-in for Apache on Windows

On Windows, the TACT plug-in for Apache httpd is provided in a separate installer. This separate installer contains only the plug-in and sample files; to install the management tools, see the instructions above in the section labeled **Installing TACT Management Applications on Windows**.

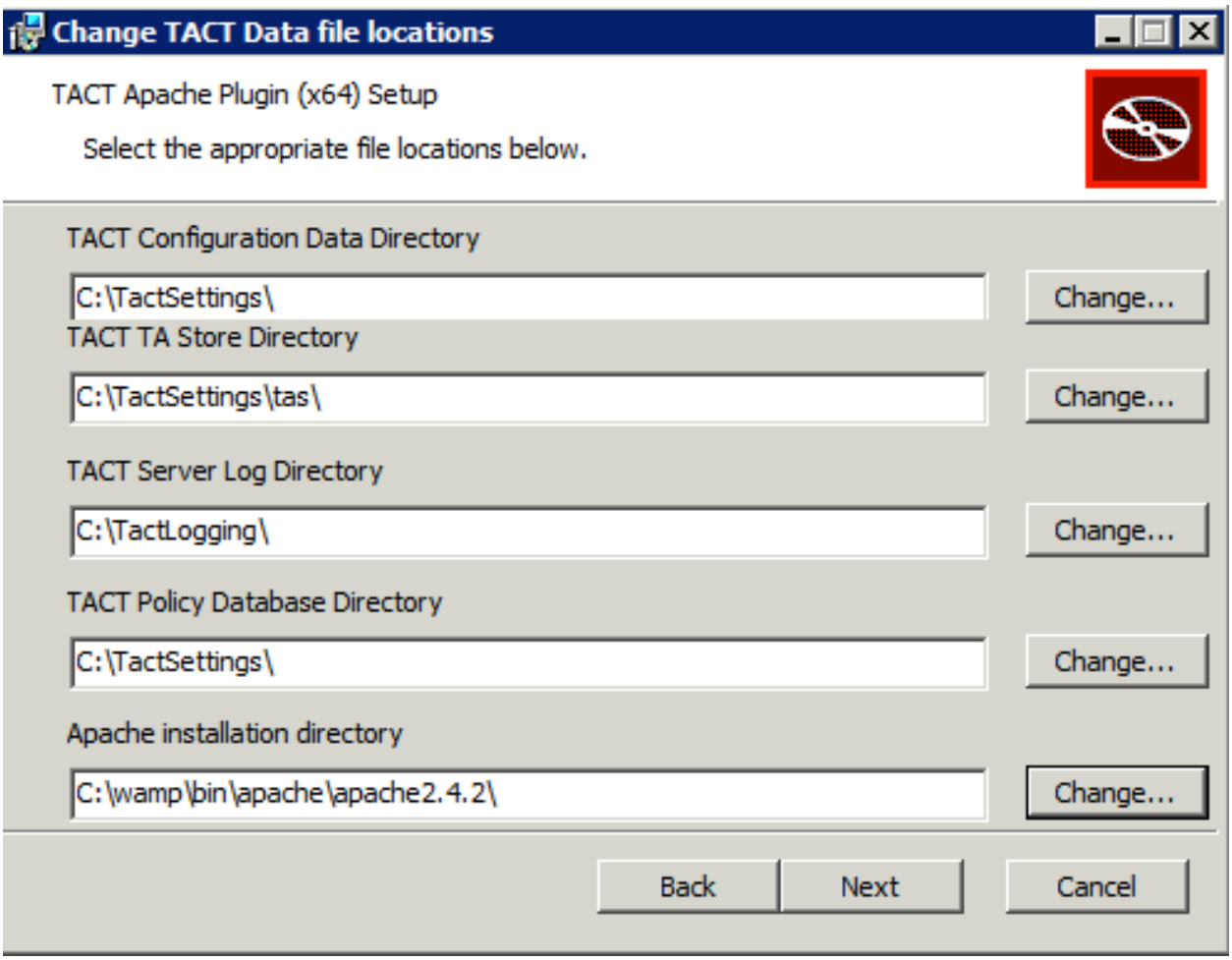
The TACT plug-in for Apache httpd on Microsoft Windows can be installed into Apache 2.2 and 2.4. It has been tested for compatibility with httpd distributions built from the Apache Software Foundation source code as well as with popular third-party distributions including WampServer, xampp and the Bitnami stack. In order to support as many different configurations of Apache httpd on Windows as possible, the installer relies on the system administrator to provide two details about the system:

- httpd version
- httpd installation location

Start by launching the TACT apache Microsoft Installer (MSI) and ensuring that only the appropriate version of apache httpd is selected:



Then select the appropriate directories:



The **Apache installation directory** is the directory containing bin, conf and modules for your system's Apache httpd.

Activating TACT for Apache on Windows

Once the installer completes, two additional steps are required to enable TACT in the running httpd:

1. Add an include line for the TACT configuration file.
2. Configure TACT so that it has access to the mod_ssl certificate store file or directory.

TACT needs to be loaded after mod_ssl. The easiest way to be certain that this happens is to place the line

```
Include conf/tact.conf
```

immediately following the line that includes mod_ssl's configuration file.

Within tact.conf, it is necessary to alter either the `CTModSSLCACertificateFile` or `CTModSSLCACertificatePath` directives so that they point to the `CACertificateFile` or `CACertificatePath` used by mod_ssl.

Once that is complete, TACT should be active the next time Apache httpd is stopped and started.

Disabling an Installed Apache Plug-in

Remove the line that includes conf/tact.conf from the httpd configuration file.

Uninstalling the Apache Plug-in

Remove the line that includes conf/tact.conf from the httpd configuration file, then use Add/Remove Programs to remove the TACT plugin for Apache.

Appendix A: Support

Web Site

Please visit the URL below for additional information.
http://iase.disa.mil/pki-pke

Technical Support

Contact technical support at the email address below.
dodpke@mail.mil

Appendix B: Customizing the TACT installer

The Linux installer will save all custom options selected in a file within the archive called install.cf. These selections will become the default when the installer is re-run. Additionally, default configuration files stored within the defaultconfigs subdirectory may be edited. To produce a custom distribution, simply use the system's tar utility to archive the install-tact directory containing the desired custom selections and default configurations.

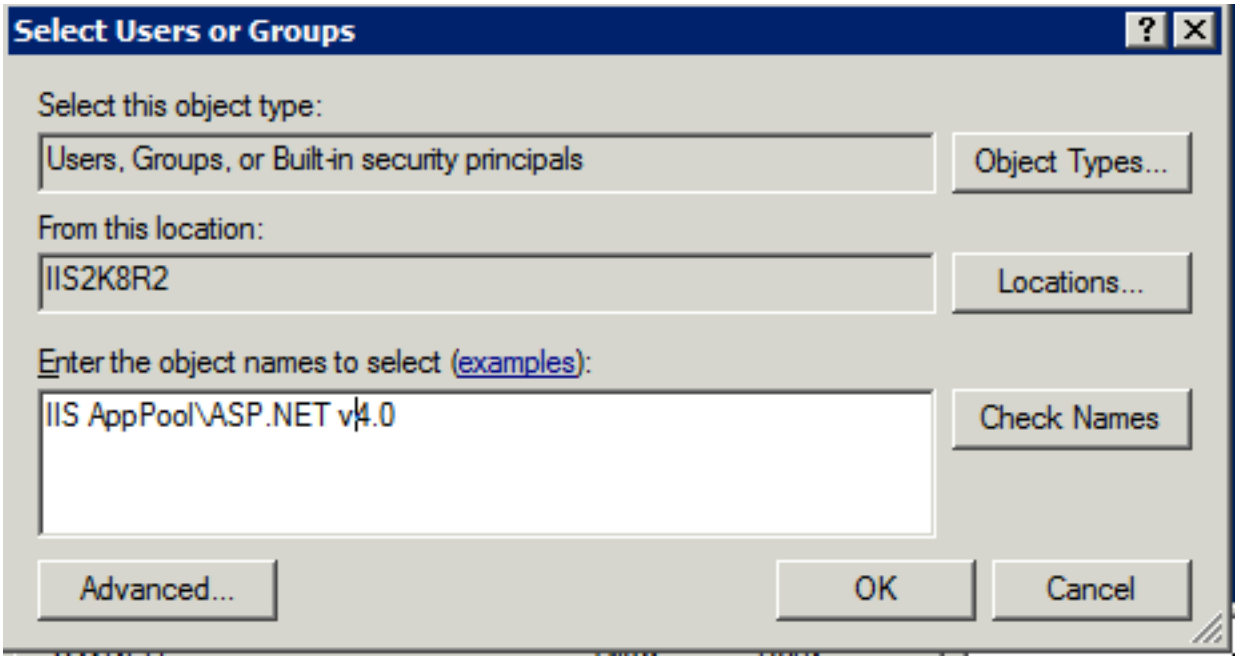
The Windows installer may be customized using an mst file, which can be applied using the msiexec tool from the command line.

Appendix C: Scripted IIS 6 Plugin Activation

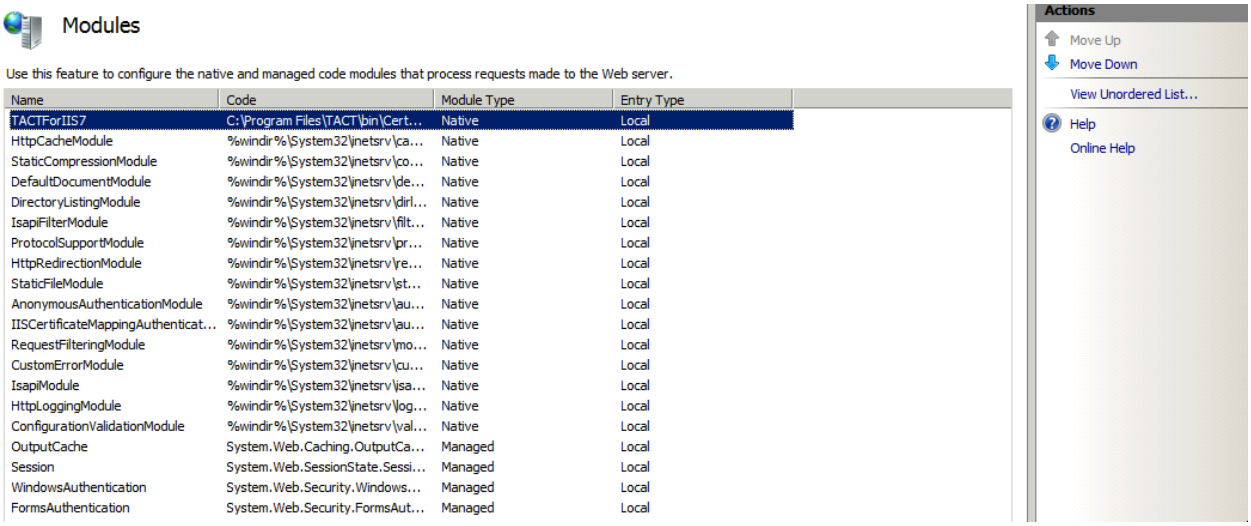
```
' This script will add the TACT filter to all sites on a server.
Dim FiltersObj
Dim FilterObj
Dim LoadOrder
Dim FilterName
Dim FilterPath
Dim FilterDesc

FilterName = "TACT Filter for ISAPI"
FilterPath = "C:\Program Files\TACT\certtrustfilter.dll"
FilterDesc = "TACT Filter for ISAPI"

'get IIS instance
Set IISOBJ = getObject("IIS://LocalHost/W3SVC")

'enumerate over objects
For each Object in IISOBJ
       'act upon web sites
    if (Object.Class = "IIsWebServer") then
                     serverFilters = "IIS://LocalHost/W3SVC/" & Object.Name & "/Filters"
                     'by getting the filters instance
                     Set FiltersObj = GetObject(serverFilters)

                     'saving its load order
                     LoadOrder = FiltersObj.FilterLoadOrder
                     If LoadOrder <> "" Then
                      LoadOrder = LoadOrder & ","
                     End If

                     'augmenting its load order
                     LoadOrder = LoadOrder & FilterName
                     FiltersObj.FilterLoadOrder = LoadOrder
                     FiltersObj.SetInfo

                     'and creating a new filter object with TACT info
                     Set FilterObj = FiltersObj.Create("IIsFilter", FilterName)
                     FilterObj.FilterPath = FilterPath
                     FilterObj.FilterDescription = FilterDesc
                     FilterObj.SetInfo
    end if
next
```

Appendix D: Integrated ASP.NET Application Pools on IIS 7.5

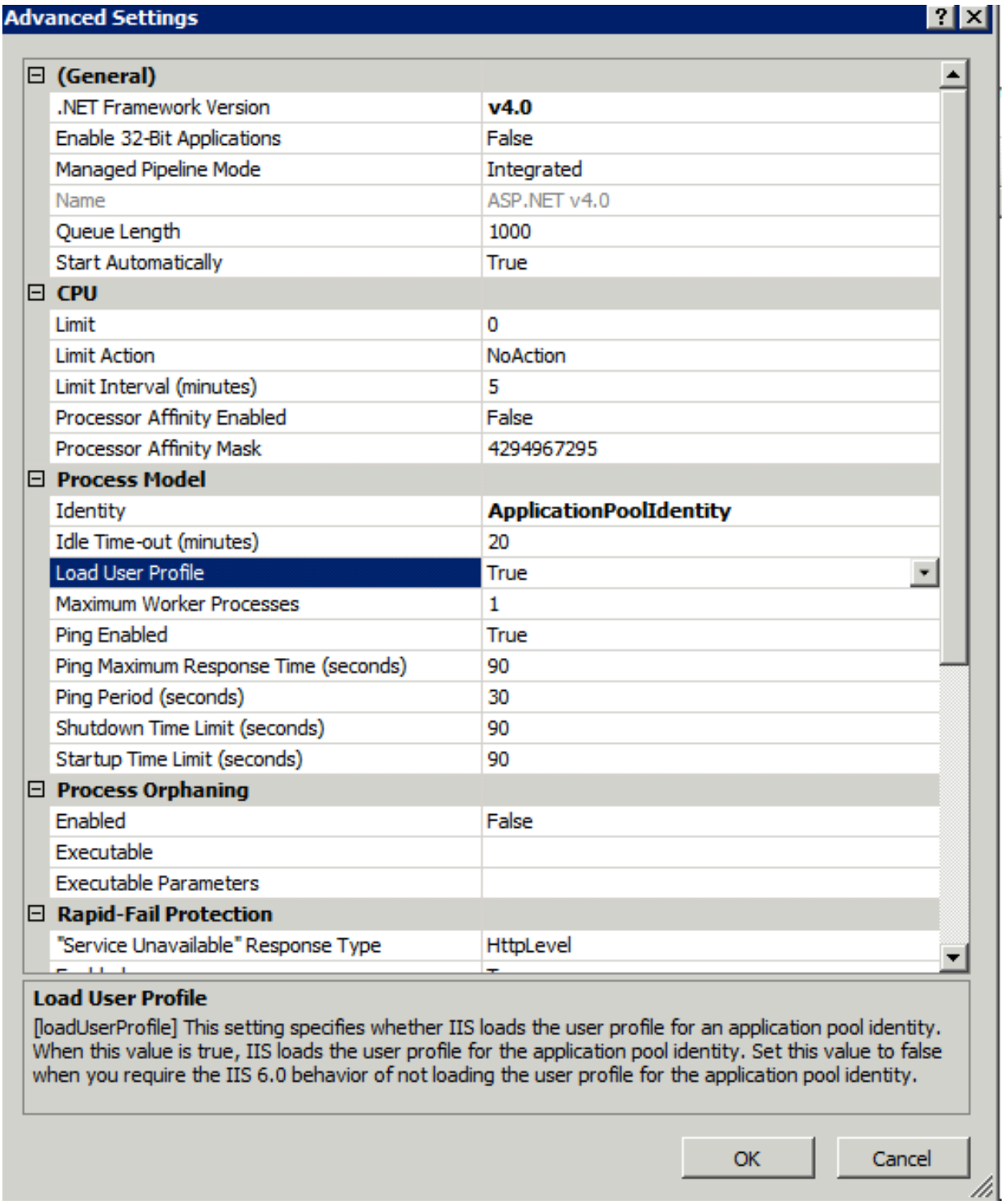
Access Control Lists (ACLs) need to be set to match the App Pool user. Note that this doesn't show up in the GUI and will need to be redone if the .NET application is installed after TACT is already installed, or if more than one Application Pool uses TACT.



It's important to move TACT to the top of the modules list in IIS manager:



The Application pool identity needs to be configured to load its user profile:



Appendix D: Acronyms

ACL	Access Control List
DoD	Department of Defense
GUI	Graphical User Interface
HTTP	Hyper Text Transfer Protocol
IIS	Internet Information Services
MSI	Microsoft Installer
PKE	Public Key Enablement
PKI	Public Key Infrastructure
RHEL	Red Hat Enterprise Linux
TA	Trust Anchor
TACT	Trust Anchor Constraint Tool

Appendix E: Patching mod_nss

The patch supplied with TACT for mod_nss is intended to be applied to a Red Hat source tree. To obtain the Red Hat source tree, download mod_nss-1.0.8-8.el5_10.src.rpm and use the command rpmbuild –bp to process it. Then, within the resulting source tree, run patch –p1 <pke_features.patch. Configure and compile the build according to the settings used with the apache build for that server.