CMWT Installation Guide

Configuration Manager Web Tools

For Build 2016.12.16.01

Overview

This document explains how to install and configure CMWT on a System Center Configuration Manager site system. Note that the site system must have the SMS Provider role. CMWT works with CAS and standalone primary site hierarchies.

CMWT has been tested on Windows Server 2012 R2, SQL Server 2014 and Configuration Manager 1610 (5.00.8458.1000), using Microsoft Internet Explorer, Microsoft Edge and Google Chrome web browsers. Note that features may not behave identically in different browsers. It should work equally as well on Windows Server 2016.

Installation Process

File System Preparation

1. Create a Folder on the Site Server named CMWT (e.g. F:\CMWT)
2. Extract the ZIP contents (files and folders) into the CMWT target folder

CMWT Configuration Settings

There are two (2) modes for configuring global settings for CMWT: Express and Manual. Express configuration uses a script to walk through the settings individually. Manual mode involves locating and editing the "_config.txt" settings file. For details about settings, refer to Appendix B, and C.

Express Mode

1. Double-click the script file "**config.vbs**" located in the CMWT installation folder.
2. Review and modify the values for each setting to suit your environment
3. When finished, the settings are written to the _config.txt file, and the original is backed up as _config.bak.

Manual Mode

1. Edit the file **_config.txt**" , located in the CMWT installation folder.
2. Review and modify the values for each setting to suit your environment

Permissions

1. Configure NTFS permissions on the CMWT folder
2. Refer to the following example for NTFS security settings. Essentially, make sure that whatever account is used by the IIS application pool to read the CMWT physical folder contents has Read permissions on the physical folder.
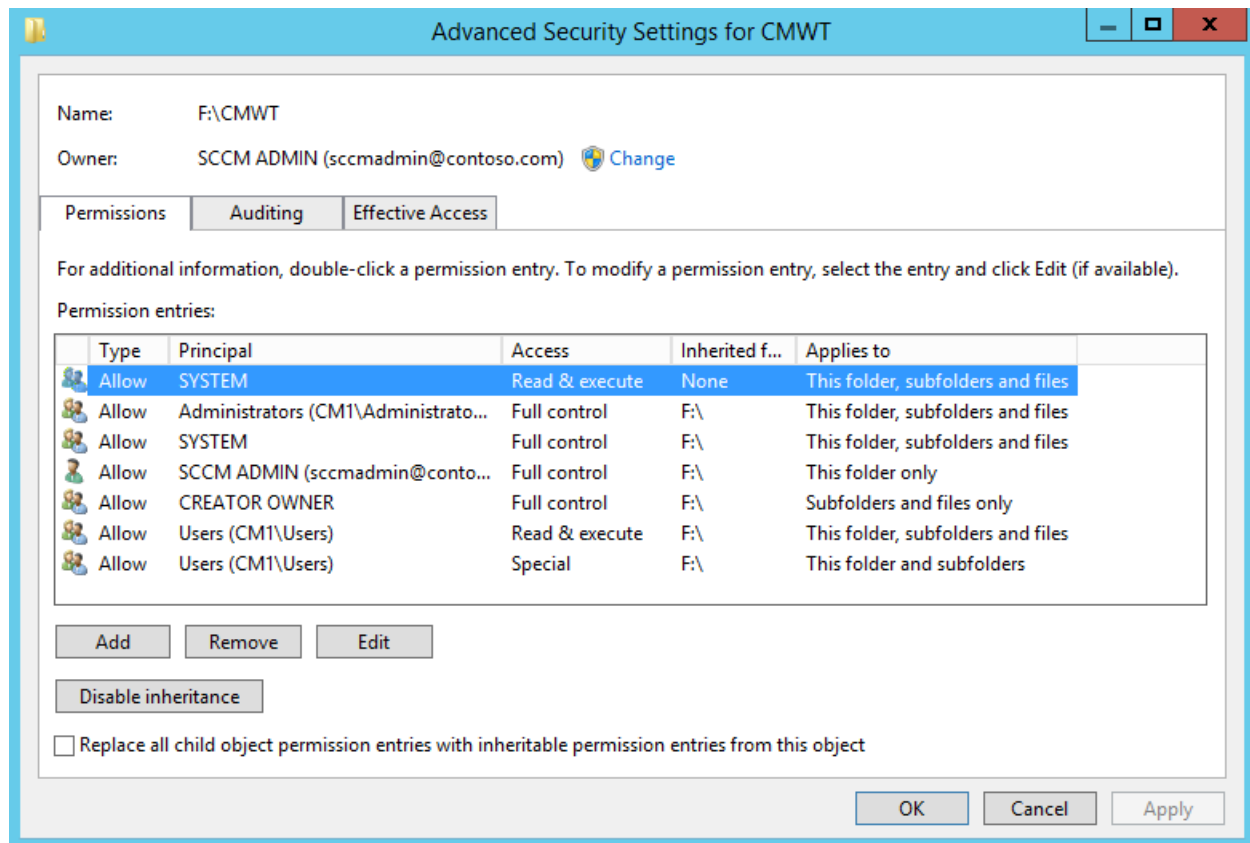
Database Preparation

<u>Note</u>: The CMWT database can reside on the same SQL Server instance as the ConfigMgr database, or under a separate instance, or on a separate SQL Server host altogether. If you choose to place the CMWT database on the same SQL Server instance as ConfigMgr, be sure to account for performance tuning to give ConfigMgr higher priority to resources.

- Open SQL Server Management Studio
- Connect to the CM database instance
- Create a new Database named "CMWT"
- Click File / Open
- Browse to locate the file "**cmwt_db_setup.sql**"
- When it opens in SSMS, click Run (or press F5)

Web Server Preparation

Add the following Windows Server roles to the site server, if they are not already present:

- ASP
    - Web Server / Application Development / ASP
- Windows Authentication
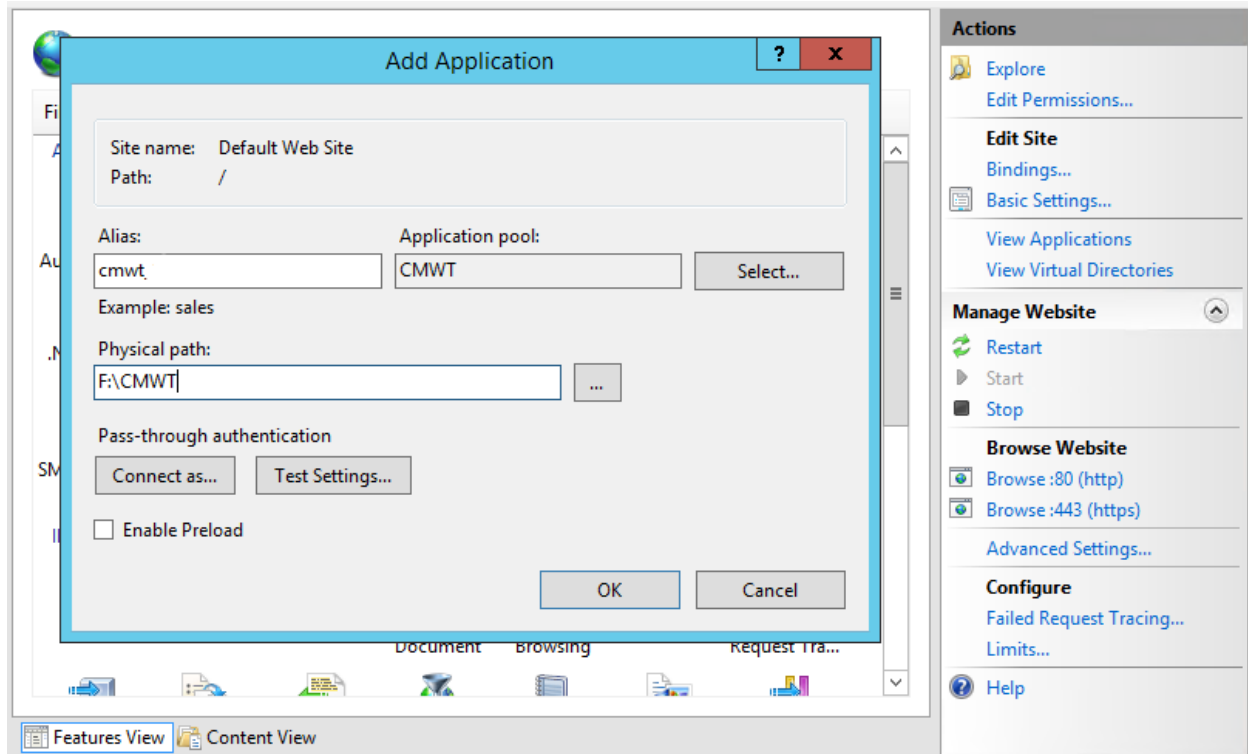   - Web Server / Security / Windows Authentication

Create a New Application Pool
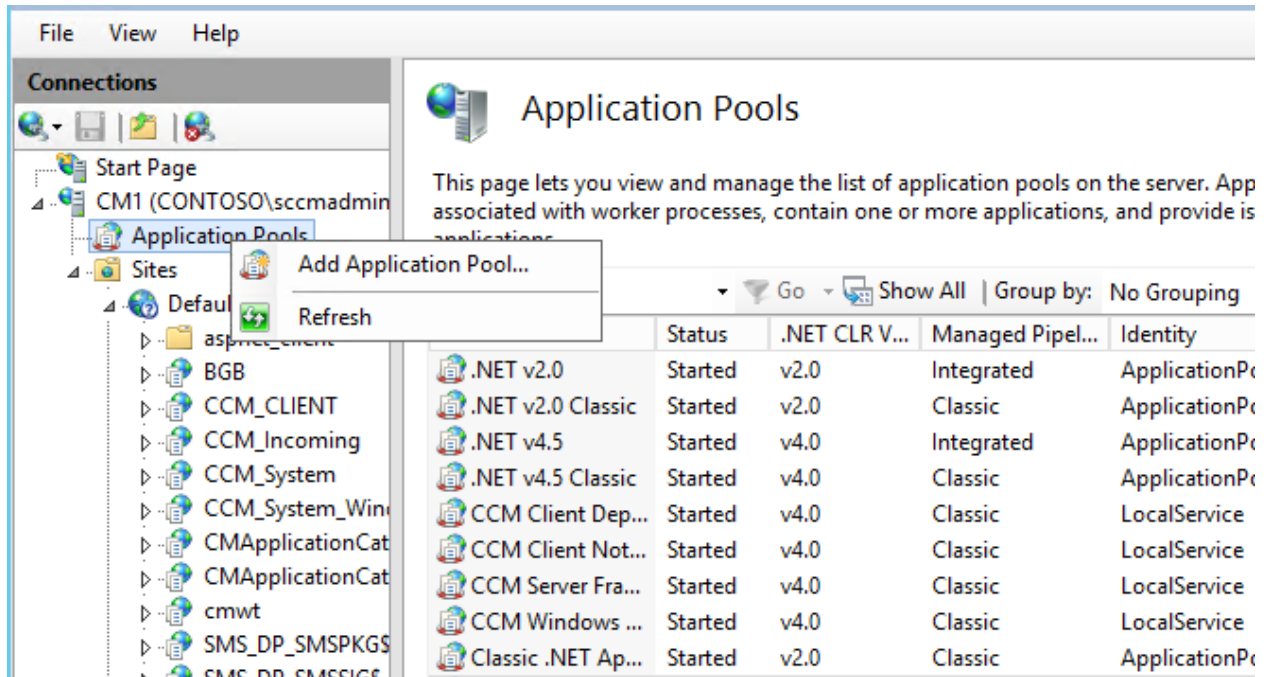
Name the new Application Pool "CMWT"

Add the CMWT Application

Right-click on the Default Web Site, and select Add Application. Fill in the Alias as "cmwt", click Select, and choose the "cmwt" application pool from the drop list, and select the CMWT physical install path. Then click OK

Configure IIS Permissions

CMWT requires **Windows Authentication** in order to work properly. **All other authentication options, including Anonymous Authentication, must be disabled.**

1. In the IIS Manager console, expand **Sites**, and click on the CMWT virtual folder object.
2. In the right-hand details panel, double-click "**Authentication**"
3. Right-click on **Windows Authentication** and select **Enable**
4. Right-click any other options in the list which show Status is "Enabled" and select Disable.

Authentication

Group by: No Grouping

Name	Status	Response Type
Anonymous Authentication	Disabled	
ASP.NET Impersonation	Disabled	
Forms Authentication	Disabled	HTTP 302 Login/Redirect
Windows Authentication	Enabled	HTTP 401 Challenge

Test Validation

After the site is installed and configured, there are several ways to confirm the site is properly configured and permissions are correctly configured.

To begin the testing process, open a web browser on the CMWT host server and go to the following URL: http://localhost/cmwt/test.htm

If the HTML test is successful, click the link to proceed to the ASP test page. If that is successful, continue to the CMWT home page. This indicates a successful configuration and CMWT is ready for use!

If you encounter issues with the HTML test, confirm the IIS virtual folder and application pool settings.

Appendix A – _Config.txt File Keys

Note that the values assigned to a given key should <u>not</u> be enclosed in quotations.

Key	Description
CMWT_DOMAIN	NETBIOS name of AD domain (e.g. "Contoso")
CMWT_DOMAINSUFFIX	FQDN of AD domain (e.g. "contoso.com")
CMWT_ADMINS	Comma-delimited list of usernames to have access to CMWT. Note that the usernames must also have explicit or implicit permissions granted within the associated Configuration Manager site.
DSN_CMDB	The DSN connection string to the Configuration Manager SQL database
DSN_CMWT	The DSN connection string to the CMWT SQL database
CMWT_PhysicalPath	The physical installation path to CMWT
CMWT_DomainPath	The LDAP domain label (e.g. "dc=contoso,dc=com")
CMWT_MailServer	SMTP or relay server address for sending alerts (not currently used)
CMWT_MailSender	Email address from which alerts will be sent (not currently used)
CMWT_SupportMail	Email address to send support requests, feature requests, comments (should be "ds0934@gmail.com")
CMWT_ENABLE_LOGGING	TRUE = Enable logging of console activities, FALSE = disabled logging
CMWT_MAX_LOG_AGE_DAYS	Number of days to maintain CMWT activity logs
CM_SITECODE	Configuration Manager site code (e.g. "PS1")
CM_AD_TOOLS	TRUE
CM_AD_TOOLS_SAFETY	TRUE
CM_AD_TOOLS_ADMINGROUPS	Comma-delimited list of AD security groups to protect from modification via CMWT
CM_AD_TOOLUSER	Domain user account used for reading and modifying AD accounts from the CMWT console. Enter as "domain\username" (e.g. "contoso\admin123")
CM_AD_TOOLPASS	Password for CM_AD_TOOLUSER account

Appendix B – _Config.txt File Variables

The default _config.txt file provided with a new CMWT installation is not intended for immediate use. It will contain variable entries which need to be replaced with actual values in order to configure the site properly.

Use Search/Replace to update the following keys to values that match your environment. For example, if your AD domain is "contoso.com" with NetBIOS name "contoso", replace "<<DOMAIN>>" with "CONTOSO" and "<<DOMSUFFIX>>" with "COM". The values are not case sensitive, so you can use "contoso" or "CONTOSO" or "Contoso".

Note: For nested or sub-level domains, such as "corp.contoso.com", you may need to add an additional FQDN label to the

<<DOMAIN>> = NETBIOS name of AD domain to connect to. Example "contoso"

<<DOMSUFFIX>> = FQDN Suffix of the AD domain to connect to. Example "com"

<<SITECODE>> = ConfigMgr 3-character site code. Example "PS1"

<<ALERTSENDER>> = Email address from which email alerts will be sent (optional). This is separate from the <<DOMAIN>> and <<DOMSUFFIX>> keys. You can assign this independent as well using a different domain and suffix than that of the site or ConfigMgr. Example "cmwtalerts"

<<DBSERVER1>> = NETBIOS server name of the SQL Server host for ConfigMgr

<<DBSERVER2>> = NETBIOS server name of the SQL Server host for CMWT

Appendix C – Examples

Example 1

```
;---------------------------------------------------------------------------
; filename....... _config.txt
; last updated... 11/30/2016
;---------------------------------------------------------------------------
CMWT_DOMAIN~CONTOSO
CMWT_DOMAINSUFFIX~CONTOSO.COM
CMWT_ADMINS~dstein,sccmadmin,user1,user2
DSN_CMDB~DRIVER=SQL Server;SERVER=CM01;DATABASE=CM_PS1;Trusted_Connection=True;
DSN_CMWT~DRIVER=SQL Server;SERVER=CM01;database=CMWT;Trusted_Connection=True;
CMWT_PhysicalPath~E:\CMWT
CMWT_DomainPath~dc=contoso,dc=com
CMWT_MailServer~smtp.contoso.com
CMWT_MailSender~cmwtalerts@contoso.com
CMWT_SupportMail~ds0934@gmail.com
CMWT_ENABLE_LOGGING~TRUE
CMWT_MAX_LOG_AGE_DAYS~90
CM_SITECODE~PS1
CM_AD_TOOLS~TRUE
CM_AD_TOOLS_SAFETY~TRUE
CM_AD_TOOLS_ADMINGROUPS~Domain Admins,Enterprise Admins,Schema Admins,Domain
Users,Authenticated Users,Protected Users,Domain Computers,Domain
Controllers,DnsUpdateProxy,Allowed RODC Password Replication Group,Denied RODC Password
Replication Group,Cloneable Domain Contollers,Cert Publishers,RAS and IAS
Servers,WinRMRemoteWMIUsers__,Read-only Domain Controllers
CM_AD_TOOLUSER~contoso\sccmadmin
CM_AD_TOOLPASS~P@ssw0rd123
```
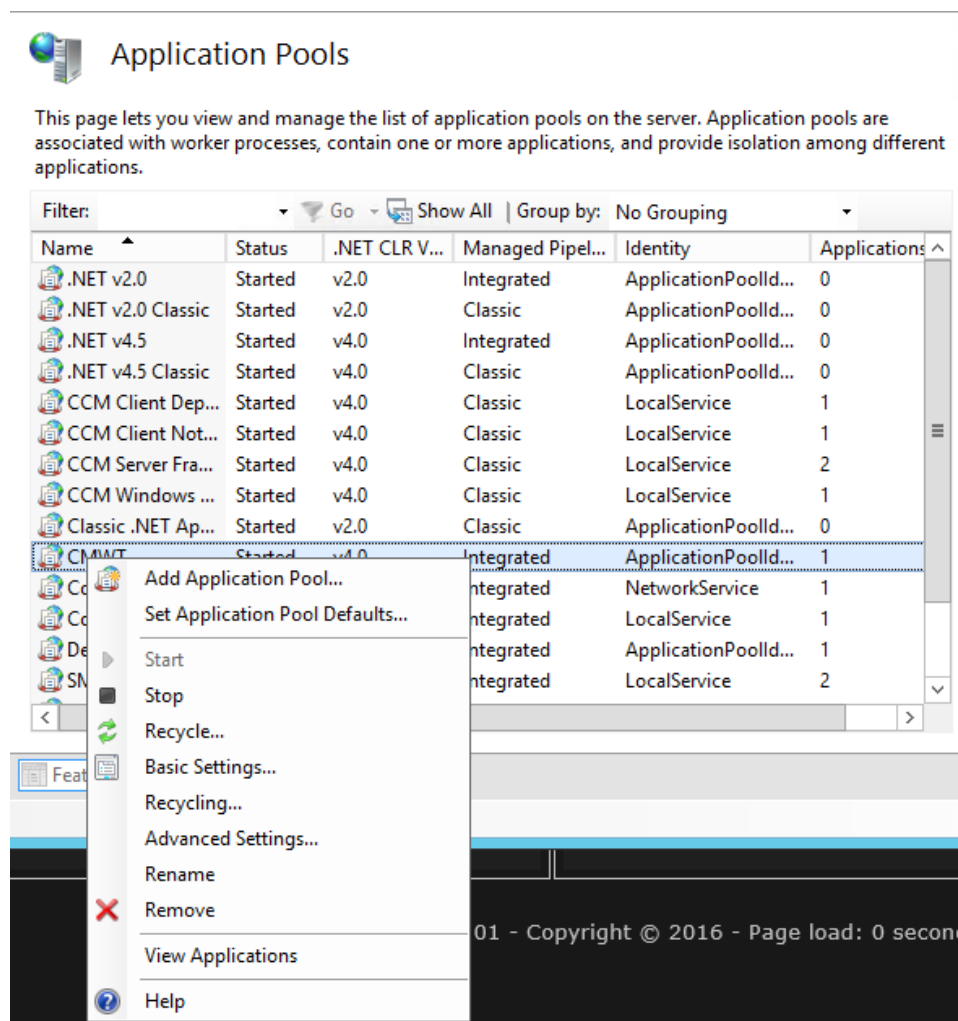
Example 2

```
;---------------------------------------------------------------------------
; filename....... _config.txt
; last updated... 11/30/2016
;---------------------------------------------------------------------------
CMWT_DOMAIN~CORP
CMWT_DOMAINSUFFIX~CORP.CONTOSO.COM
CMWT_ADMINS~dstein,sccmadmin,user1,user2
DSN_CMDB~DRIVER=SQL Server;SERVER=CM01;DATABASE=CM_PS1;Trusted_Connection=True;
DSN_CMWT~DRIVER=SQL Server;SERVER=CM01;database=CMWT;Trusted_Connection=True;
CMWT_PhysicalPath~E:\CMWT
CMWT_DomainPath~dc=corp,dc=contoso,dc=com
CMWT_MailServer~smtp.contoso.com
CMWT_MailSender~cmwtalerts@contoso.com
```

CMWT_SupportMail~ds0934@gmail.com
CMWT_ENABLE_LOGGING~TRUE
CMWT_MAX_LOG_AGE_DAYS~90
CM_SITECODE~PS1
CM_AD_TOOLS~TRUE
CM_AD_TOOLS_SAFETY~TRUE
CM_AD_TOOLS_ADMINGROUPS~Domain Admins,Enterprise Admins,Schema Admins,Domain
Users,Authenticated Users,Protected Users,Domain Computers,Domain
Controllers,DnsUpdateProxy,Allowed RODC Password Replication Group,Denied RODC Password
Replication Group,Cloneable Domain Contollers,Cert Publishers,RAS and IAS
Servers,WinRMRemoteWMIUsers__,Read-only Domain Controllers
CM_AD_TOOLUSER~contoso\sccmadmin
CM_AD_TOOLPASS~P@ssw0rd123

Appendix D – Notes

1. Whenever changes are made to the _config.txt file, the CMWT application pool must be recycled in order to reset the environment. This causes CMWT to re-read the _config.txt file and assign the updated values within the IIS application pool which updates the application behavior. If you modify the _config.txt, but do not see the changes reflected in the CMWT web interface, the most common causes are either that the _config.txt file was not saved, or it wasn't saved in the correct folder location (the root of the CMWT installation), or the IIS application pool wasn't recycled.

   To reset the application pool, open Application Pools in the IIS Manager console, right-click on the application pool and select "Recycle…"

2. In many cases, the best way to configure CMWT is to use the same AD user account which was involved with the installation of Configuration Manager. It will (should) typically have SA permissions in the associated SQL Server database, as well as full Administrator rights within the Configuration Manager site.

Appendix E – Enabling Console Tools

The CMWT console tools use client-side scripting to facilitate direct interfacing with remote computers on a common network environment (and domain credentials). This allows for browsing remote hard drives, registry and event log information and so on. This is only supported when using CMWT with Microsoft Internet Explorer, but also requires some security zone settings to be configured to allow the feature to work.
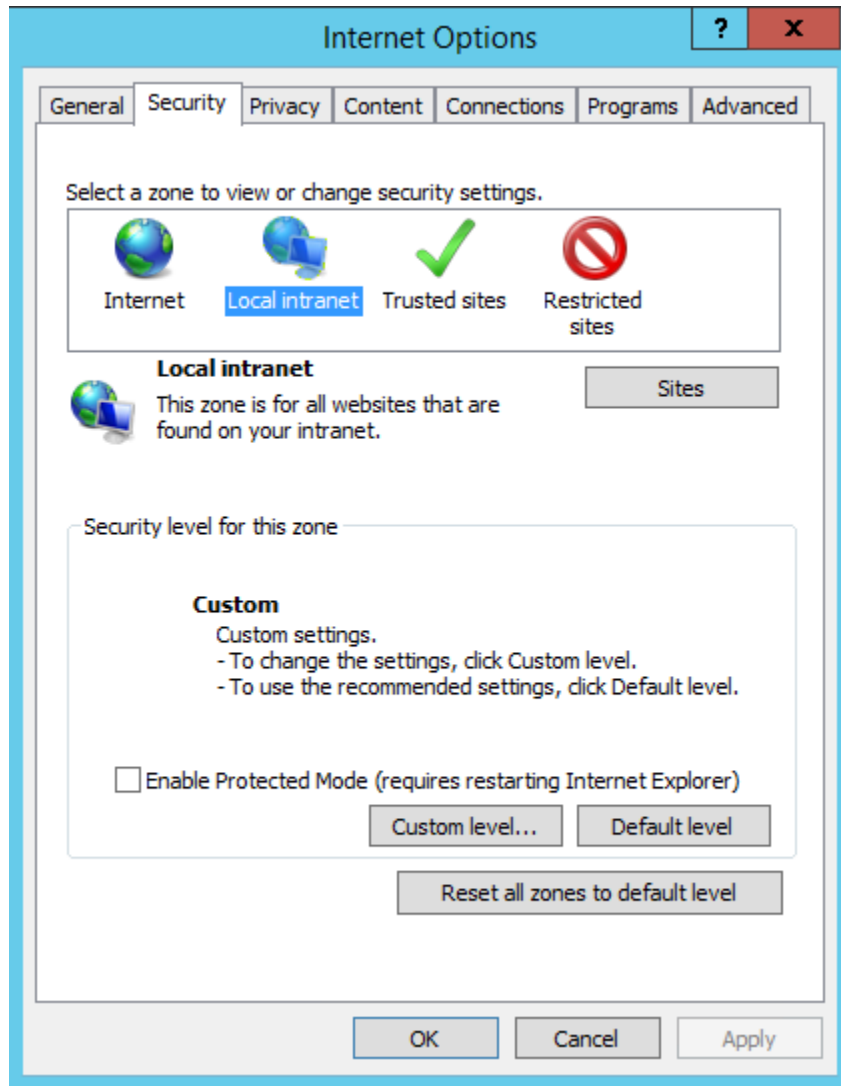

1. Assuming that the CMWT web site is set as an Intranet site, and that the Local Intranet security zone is set to the Medium-level (default), the remaining steps will enable this feature to work:
2. Open "Internet Options" in Internet Explorer by clicking on the small gear icon at top-right:

3. Select the Security tab
4. Select the Local Intranet zone

5. Click "Custom level…"
6. Scroll down to "Initalize and script ActiveX controls not marked as safe for scripting"
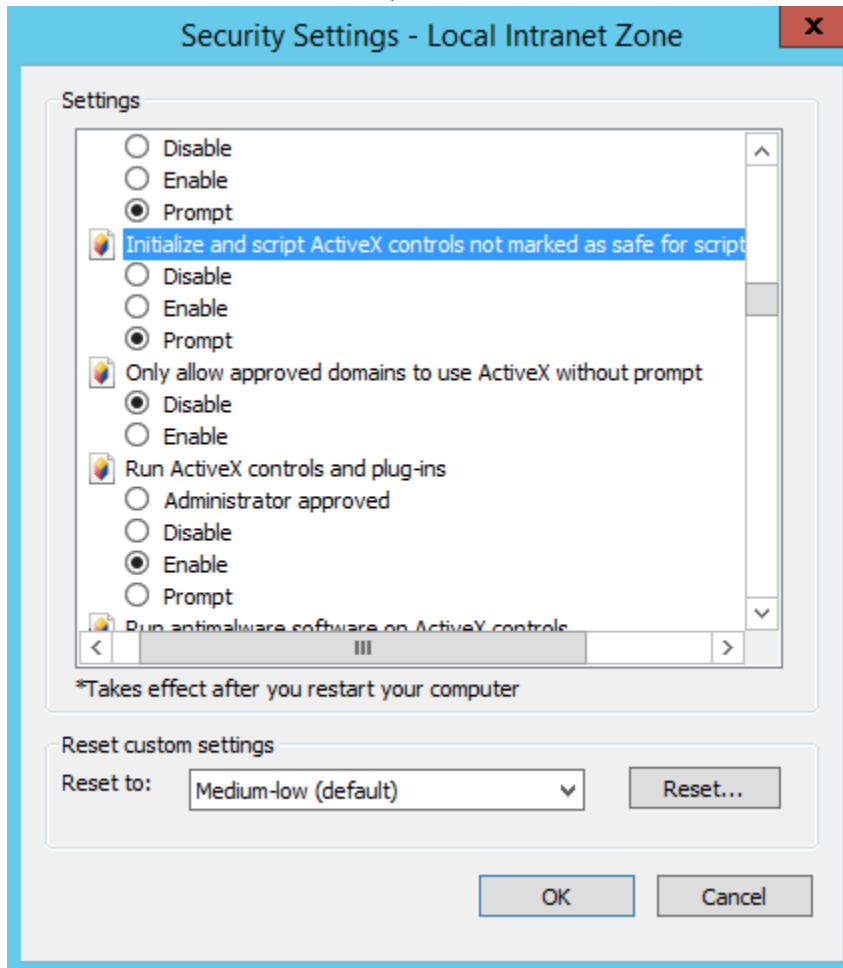
7. Change the setting from Disable to Prompt (or Enable, if you don't want to be prompted each time you use a CMWT tool feature)
8. Click OK