Deltek

Deltek Acumen Touchstone 8.11.3

Installation and Administration Guide

April 30, 2026

Deltek

While Deltek has attempted to verify that the information in this document is accurate and complete, some typographical or technical errors may exist. The recipient of this document is solely responsible for all decisions relating to or use of the information provided herein.

The information contained in this publication is effective as of the publication date below and is subject to change without notice.

This edition published April 2026.

Deltek

Contents

Deltek

Overview

This document is meant to serve as a guideline for hardware and software requirements and provides your firm's IT department with information about the technical deployment architecture.

It is important to note that the choices of hardware, relational database software, and operating system in these examples represent guidelines, are subject to change, and do not replace a needs analysis and site survey with a Deltek Technical Consultant. Contact a Deltek Technical Systems Engineer for suitability of legacy equipment.

Consulting

Deltek, Inc. can provide onsite consulting and training services as well as phone support on a contract or time-and-materials basis.

Additional Notes

The evolution of technology dictates the way IT professionals plan their network hardware and software environments. While this document does not account for all possible options in the deployment of Deltek software, it does provide specific recommendations based on testing metrics and years of experience working directly with Deltek customers.

Prior to making assumptions on how specific 3rd party technologies will perform with Deltek applications, Deltek recommends contacting your sales representative to arrange a discussion with a Deltek Technical Systems Engineer who can help you plan for a cost effective and optimally performing application environment.

Legal Disclaimer: The recommendations in this document are intended to convey general information and should not be relied upon as a substitute for a professional consultation with Deltek. All of the information in this document is provided "as is" and without warranties of any kind, either expressed or implied.

Deltek

Downloading Deltek Products using Deltek Software Manager

You can use Deltek Software Manager (DSM) to download complete Deltek products, hot fixes, cumulative updates, and sub-releases. You can access DSM through the Deltek Support Center or use Deltek Software Manager Lite to download Deltek products.

Accessing DSM from within the Deltek Support Center

To access DSM from within the Deltek Support Center:

1. In your Web browser, go to https://deltek.custhelp.com.
2. Enter your Deltek Support Center **Username** and **Password** and click **Login.**
3. When the Deltek Support Center page displays, click **Product Downloads**.
4. On the Deltek Software Manager screen, click **Launch Deltek Software Manager**.
5. Click **Settings** at the top right of the dialog box to use the Settings dialog box to specify the folder where you want to download Deltek products and click **OK**.

   > **Note:** When you log on for the first time, DSM asks you to select a default folder where Deltek products are to be downloaded.
   >
   > You can change this folder anytime in the Settings dialog box.

6. In the left pane, expand the Deltek product that you want to download, if it is not already expanded.
7. Select the product type that you want to download.

   Options include:

   - **Complete**
   - **Cumulative Updates**
   - **HotFixes**
   - **Sub-Release**

8. In the table, select the check box that corresponds to the Deltek product that you want to download.

   The right pane displays a message stating that the product has been added to the download queue.

   > **Note:** To view the items in the download queue, click **View Download Queue** at the bottom of the left pane.

9. Click **Download** at the bottom of the left pane to download the product to the folder that you selected.

Deltek

Accessing DSM Lite

To access Deltek Software Manager Lite:

1. In your Web browser, go to https://dsm.deltek.com/DeltekSoftwareManagerLite.
2. Enter your Deltek Support Center **Username** and **Password** and click **Logon.**
3. When the Deltek Software Manager Lite page displays, select a product from the drop-down list.
4. Click the product type that you want to download.

> **Note:** The download behavior and download folder may differ depending on the browser and browser settings that you are using.

DSM Documentation and Troubleshooting

- To view the online help for Deltek Software Manager, click here.
- To view a tutorial on how to use Deltek Software Manager, click here.
- To view more information on troubleshooting Deltek Software Manager, click here.

> **Note:** When you click a link, you will be asked to log into DSM if you aren't already logged in.

Deltek

Before You Begin Deployment

Logical Tiers

Before you install Touchstone, you should carefully consider the server architecture that best fits your company's needs. Touchstone uses a multi-tier architecture. Various components of the Touchstone application are distributed to logical tiers for performance and scalability.

Tier	Description
Web/Application Server	This tier hosts the Touchstone application in IIS and handles all web requests and processing for Touchstone. When a request is sent, this Web/Application server tier processes that request (such as retrieving stored data or performing a specific function) and returns the result. Internet accessibility is not required but makes installations and upgrades easier.
Database	This tier hosts the Database Server(s) where Touchstone data is stored. Touchstone supports Oracle and Microsoft SQL Server databases.

Installation/Deployment Models

Touchstone supports multiple deployment models. The model that you choose depends on several factors including the number of application users, the application data storage requirements, cost considerations, security requirements, and fault tolerance.

Deployment Model	Description	Use this model if...
Single-Server	Install the Touchstone Web/Application and Database tiers on the same machine.	▪ Deployment needs are simple. For example, you are installing Touchstone on a test machine. ▪ All users are at a single location and will access Touchstone in the office or over a Virtual Private Network (VPN) connection to the company network. ▪ Users will not access the application over the internet. ▪ Deltek does not recommend using a single server deployment if the server is accessible from the internet. With this deployment model, the Database Server is hosted on the Application Server and exposes the Database Server to the internet. This may create security risks for your application data. ▪ If you want to access Touchstone from the internet, a two-tier configuration is a more secure option.

Dual-Server (Two-Tier)	Install the Touchstone Web/Application and Database tiers on separate machines.	▪ All users are at a single location and will access Touchstone in the office or over a Virtual Private Network (VPN) connection to the corporate network. ▪ Users will access the application over the internet.
Multiple Server (Two Tier)	Install the Touchstone Web/Application and Database tiers on separate machines.	▪ All users are at a single location and will access Touchstone in the office or over a Virtual Private Network (VPN) connection to the corporate network. ▪ Users will access the application over the internet. ▪ User access can be distributed across multiple Application Servers, with or without load balancing. ▪ Suitable for organizations with complex deployment requirements and proficient firewall management.

Service Accounts

Deltek recommends that you use domain accounts for the Touchstone IIS Application Pool and for connections to the Touchstone database; however, you can use local accounts. During installation, the Touchstone installer prompts for the IIS Application Pool service account name. If you enter a service account name that does not exist, the installer can create the account during the installation.

Note: Deltek recommends that you do not share the Touchstone application service account with any other applications.

Supported Deployment Scenarios

- Touchstone supports single server and multi-server installations.
- Touchstone supports advanced deployments such as DMZ and multiple Web Servers.
- Touchstone supports non-standard HTTPS ports.
- Touchstone supports Microsoft SQL Server and Oracle databases.
- The installation directory for Touchstone is determined by the drive from which you run the installation script. Touchstone supports installing to a drive other than C; however, the installation directory must be <drive>:\Program Files\Deltek\Acumen Touchstone. For example, if you want to install Touchstone on the D:\ drive, download the **DeltekAcumenTouchstone.ps1** file to a temporary folder on the D:\ drive.
- Each server must be a member of the same domain or domains with a trusted relationship.

Deltek

Unsupported Scenarios

The Touchstone installation does not support installing any Touchstone tiers on any of the following servers:

- Domain Controller
- Microsoft Exchange Server
- Proxy, Firewall, or ISA Server
- Microsoft SharePoint Portal Server
- Terminal Services
- Citrix Server

Using these services/servers can cause significant issues in the performance, reliability, and functionality of Touchstone and the other applications on your network.

Permissions Required to Install Touchstone

In order to perform a Touchstone installation, you must have the appropriate rights and privileges on your Web/Application tier. Your Windows account must be a member of the Local Administrator group on the server.

Security

- All servers/tiers must be a member of the same domain or domains with a trusted relationship (that is, not in a workgroup).
- TLS 1.2 is required. SSL 2.0/3.0 and TLS 1.0/1.1 must be disabled on all tiers.
- SSL (HTTPS) is required. A valid SSL certificate with accessible FQDN is required on all Web Servers (IIS). A self-signed certificate is sufficient for local single-server installation testing only.
- Touchstone recommends that data sources use Integrated Security when creating a connection to the database. To disable this requirement, update **RequireWinAuthForDatabase** in C:\Program Files\Deltek\Acumen Touchstone\web\PPMAPI\config to a value of 0.
- All installation scripts are digitally signed by the Deltek code signing certificate. If a script is edited or tampered with, an error displays and the script process ends.
- Each time you run the **DeltekAcumenTouchstone.ps1** script, you are prompted for your customer support username and password, which is encrypted and sent to Deltek to authenticate. If you do not know your credentials, contact Deltek using the Deltek Support Center.

  > **Note:** You must have opened a browser with this user profile before running the script.

- When you specify a password (for example, Application Pool Identity, Database login), the script checks it against a list of known insecure passwords that may not be used. Deltek maintains the list and it is set in the **DeltekAcumenTouchstoneConfiguration.xml** file that the script downloads to the installation directory.

- Passwords must meet domain policy requirements (upper case, lower case, a number, and a special character).
- Passwords are masked in the log.

Deltek

System Requirements

Your organization has made a substantial commitment to project management. To support that commitment, Deltek recommends that you carefully consider the hardware requirements necessary to run Touchstone properly.

Platform Virtualization

Virtual environment software, such as VMware®, resides in the hardware layer underneath the operating system and is used to partition a single server into a multiple server/multiple operating system environment. Deltek's product development makes limited use of virtual environments.

> **Attention:** See the *Virtual Environments Statement* document on the Deltek Customer Care Connect site (http://support.deltek.com) for more information.

Display Settings

Deltek recommends display resolution of 1920 × 1080 with a minimum resolution of 1024 × 768.

Hardware Sizing Considerations

There are several factors that go into sizing an appropriate server infrastructure. The number of concurrent users accessing the system at any given time, the amount of data being analyzed, the number of code and other user-defined fields loaded from schedules, customizations, and growth expectations all have an impact on the initial sizing plans. The hardware profiles are intended as a starting point for deployment. Further in-depth discussion of the business needs of the solution during implementations of application will provide final guidance on hardware requirements.

Hardware Requirements

The number of people using Touchstone, the Touchstone processes they are using, and the size of the projects all have an effect on the server hardware and software requirements.

Stand-Alone Deployment

> **Note: For Touchstone, the initial database size estimate is around 69 MB (Touchstone 8.10.1).**
>
> This is in addition to any memory needed for each project that is uploaded since these file contents are stored in the database. Use the **DeltekAcumenTouchstone810DatabaseSizeEstimator.xls** spreadsheet to help estimate your database size.

The following table lists the recommended minimum hardware requirements for a deployment of Touchstone in a stand-alone workstation environment.

Tier	Hardware Required	Determining Factors

Client/Server Deployment	**Database** ▪ 2.8 GHz or faster CPU, 8x Logical cores ▪ 8+ GB physical memory, additional space for each project that is uploaded file content is stored in the database ▪ Database instance memory should be 10%–15% of the database size **Application Server** ▪ 8x Logical Cores 2.5 GHz or faster CPU ▪ 16+ GB physical memory ▪ 300 MB of available disk space for application ▪ Client ▪ 2.0 GHz or faster CPU ▪ Recommended 4 GB physical memory	▪ **Medium Installation:** 25–50 concurrent users ▪ **Large Installation:** 50+ concurrent users

Software Requirements

For a complete list of the recommended minimum software requirements, see the *Deltek Product Support Compatibility Matrix* document that you can download from the Deltek Customer Care Connect site.

Supported Deployment Technology

Note: Supported versions are the currently actively tested versions of technologies used to deploy Acumen Touchstone. Except for the Deltek Integrated Products, these technologies are not directly supported by Deltek. Changes to these technologies occur at the discretion of the individual technology vendors.

Category	Supported Deployment Technology
Operating Systems	**Windows Server** ▪ Windows Server 2019 ▪ Windows Server 2022 ▪ Windows Server 2025

	▪ Microsoft Windows Server 2022 Azure Edition
Web Server	**Microsoft Internet Information Server (IIS)** ▪ IIS 10 (Win Svr 2019) ▪ IIS 10 (Win Svr 2022) **Note:** For the Web Server, Touchstone supports **Region and Language** set to **English (United States)** only.
Database Platform	**Azure SQL** **Microsoft SQL Server** ▪ SQL Server 2019 ▪ SQL Server 2022 SQL Server is supported on Linux and Unix. **Oracle** ▪ Oracle 19.3 Oracle is supported on Linux, Unix, and Exadata. **Note:** For both the SQL Server and Oracle database, Touchstone supports **Region and Language** set to **English (United States)** only.
Database Driver	▪ Oracle Provider for OLE DB ▪ Oracle Data Provider for .NET (ODP.NET) ▪ MS SQL Server Native Client 11.0 (SQL Server 2012 Native Client, version 11.4.7001.0 or higher) **Note:** For information about this support matrix, see Support Policies for SQL Server Native Client. ▪ MS OLE DB Driver for SQL Server, version 18.2.2.0 or higher

Scheduling Tools	Touchstone integrates with multiple project management platforms. Projects can be from any of the following platforms:
	Microsoft Project
	▪ **Microsoft Project Standard**
	  ▪ Microsoft Project Standard 2021
	  ▪ Microsoft Project Standard 2024
	▪ **Microsoft Project Professional**

	▪ Microsoft Project Professional 2021 ▪ Microsoft Project Professional 2024 **Oracle** ▪ **Primavera P6 (XML)** ▪ Primavera P6 17.12 ▪ Primavera P6 18.8 ▪ Primavera P6 19.12 ▪ Primavera P6 20.12 ▪ Primavera P6 21.12 ▪ Primavera P6 22.12 ▪ Primavera P6 24.12 ▪ **Primavera P6 (XER)** ▪ Primavera P6 15.2 ▪ Primavera P6 17.12 ▪ Primavera P6 18.8 ▪ Primavera P6 19.12 ▪ Primavera P6 20.12 ▪ Primavera P6 21.12 ▪ Primavera P6 22.12 ▪ Primavera P6 24.12
Deltek Integrated Products	**Deltek Acumen** ▪ 8.7 ▪ 8.8 ▪ 8.9 ▪ 8.10 ▪ 8.11 **Deltek EPM Security Administrator** ▪ Deltek EPM Security Administrator 8.6 **Deltek Open Plan** ▪ Deltek Open Plan 8.6 ▪ Deltek Open Plan 8.7 ▪ Deltek Open Plan 8.8 **Deltek PPM Administrator**

	▪ Deltek PPM Administrator 1.0
Web Browser	▪ Chrome ▪ Edge ▪ Firefox ▪ Safari
.NET Framework	▪ .Net F/W 4.8 ▪ .Net F/W 4.8.1
Microsoft Office	**Microsoft Excel** ▪ Microsoft Excel 2021 ▪ Microsoft Excel 2024
Embedded Technologies	▪ Visual C++ 2015-2022 Redistributable Package (x86) ▪ Visual C++ 2015-2022 Redistributable Package (x64)

Compatible Deployment Technology

Note: Compatible versions are the recent previously supported and tested technologies used to deploy Acumen Touchstone. These are not actively being tested but are believed to be compatible with Acumen Touchstone. Deltek does not recommend these technologies for new deployments but will make its best effort to answer questions concerning these technologies. These technologies may not be available for troubleshooting at Deltek.

Category	Compatible Deployment Technology
Operating System	**Windows Server** ▪ Windows Server 2016 **Web Server** ▪ IIS 10 (Win Svr 2016)
Database Platform	**Microsoft SQL Server** ▪ SQL Server 2016 ▪ SQL Server 2017 (This is also supported on Linux and Unix.) **Oracle** ▪ Oracle 12.2 ▪ Oracle 18.3

Deltek

Open-Source Software Included with Touchstone

Touchstone includes the following open-source software:

Software	Company
Microsoft.Office.Interop.MSProject v15.0.0.0	Microsoft
Microsoft.Office.Interop.Excel v15.0.0.0	Microsoft
CsvHelper v33.0.1	Josh Close
JamesNK/Newtonsoft.Json 13.0.3	Newtonsoft, James Newton-King
NLog - Advanced .NET Logging v5.3.3	Jarek Kowalski, Kim Christensen, Julian Verdurmen
System.ValueTuple v4.5.0	Microsoft
StyleCop.Analyzers v1.1.118	Tunnel Vision Laboratories, LLC, Sam Harwell
Oracle Data Provider for .Net, Managed Driver v4.112.4.3	Oracle
Microsoft.Web.Infrastructure v1.0.0	Microsoft
Microsoft.IO.RecyclableMemoryStream v3.0.1	Microsoft
System.Buffers vv4.6.0	Microsoft
System.Memory v4.6.0	Microsoft
System.Numerics.Vectors v4.6.0	Microsoft
System.Runtime.CompilerServices.Unsafe v6.1.0	Microsoft
Aspose.Tasks for .NET v24.11.0 (Nuget)	Aspose
ServiceStack v8.7.0 (Nuget)	ServiceStack
SpreadsheetGear 2023 for .NET Framework v9.2.9.102	SpreadsheetGear
Microsoft.Csharp v4.7.0 (Nuget)	Microsoft
System.Threading.Tasks.Extensions v4.6.0 (NuGet)	Microsoft
Microsoft.Bcl.AsyncInterfaces v9.0.0 (Nuget)	Microsoft
Microsoft.Bcl.HashCode v1.1.1 (Nuget)	Microsoft

Microsoft Visual Studio Enterprise 2022	Microsoft
Microsoft.Extensions.DependencyInjection v8.0.0 (NuGet)	Microsoft
Microsoft.Extensions.DependencyInjection.Abstractions v8.0.1 (NuGet)	Microsoft
System.Text.Encodings.Web v9.0.0 (NuGet)	Microsoft
System.Text.Json v9.0.0 (NuGet)	Microsoft
System.IO.Pipelines v9.0.0 (NuGet)	Microsoft
CmdLine v1.0.7.509 (NuGet)	Ron Jacobs
Moq v4.2.1510.2205 (NuGet)	Daniel Cazzulino, kzu
Python v2.7.18	Python
NodeJS v14.15.1	NodeJS
NPM v6.14.8	NPMJS
MSTest.TestAdapter v3.6.1	Microsoft
MSTest.TestFramework v3.6.1	Microsoft
VS.QualityTools.UnitTestFramework - 15.0.27323.2	Microsoft
Azure.Core v1.38.0	Microsoft
Azure.Identity v1.11.4	Microsoft
Microsoft.Data.SqlClient v5.2.2	Microsoft
Microsoft.Data.SqlClient.SNI v5.2.0	Microsoft
Microsoft.Extensions.Logging v8.0.0	Microsoft
Microsoft.Extensions.Logging.Abstractions v8.0.1	Microsoft
Microsoft.Extensions.Options v8.0.0	Microsoft
Microsoft.Extensions.Primitives v8.0.0	Microsoft
Microsoft.Identity.Client v4.61.3	Microsoft
Microsoft.Identity.Client.Extensions.Msal v4.61.3	Microsoft

Microsoft.IdentityModel.Abstractions v6.35.0	Microsoft
Microsoft.IdentityModel.JsonWebTokens v6.35.0	Microsoft
Microsoft.IdentityModel.Logging v6.35.0	Microsoft
Microsoft.IdentityModel.Protocols v6.35.0	Microsoft
Microsoft.IdentityModel.Protocols.OpenIdConnect v6.35.0	Microsoft
Microsoft.IdentityModel.Tokens v6.35.0	Microsoft
System.ClientModel v1.0.0	Microsoft
System.Configuration.ConfigurationManager v6.0.1	Microsoft
System.Data.Common v4.3.0	Microsoft
System.Data.Odbc v8.0.0	Microsoft
System.Data.OleDb v8.0.0	Microsoft
System.DirectoryServices v8.0.0	Microsoft
System.IdentityModel.Tokens.Jwt v6.35.0	Microsoft
System.IO.FileSystem.AccessControl v5.0.0	Microsoft
System.Memory.Data v1.0.2	Microsoft
System.Runtime.InteropServices.RuntimeInformation v4.3.0	Microsoft
System.Security.AccessControl v6.0.0	Microsoft
System.Security.Cryptography.ProtectedData v4.7.0	Microsoft
System.Security.Permissions v6.0.0	Microsoft
System.Security.Principal.Windows v5.0.0	Microsoft
System.Text.Encoding v4.3.0	Microsoft
BouncyCastle.Cryptography v2.5.1	
MailKit v4.13.0	
MimeKit v4.13.0	
System.Formats.Asn1 v8.0.1	Microsoft

Deltek

Database Requirements

Touchstone data can be stored in a Microsoft SQL Server database or an Oracle database. The database that you choose depends on several factors, including the number of application users, the application data storage requirements, cost considerations, security requirements, and fault tolerance.

Note: Before starting your installation, review the appendix that is applicable to your environment for information about storing Touchstone data and other database requirements.

- Appendix A: Using Microsoft SQL Server with Touchstone
- Appendix B: Using Oracle with Touchstone

Database Sizing Utility

Use the **Deltek Acumen Touchstone Database Size Estimator** spreadsheet to estimate the database size required to support your use of Touchstone. You can download the spreadsheet from the Touchstone Documentation folder in Deltek Software Manager (DSM).

PPM Suite Shared Database

Deltek recommends as a best practice that all applications in the PPM suite of applications are installed into the same database and schema. If you are installing Touchstone into an existing database containing other PPM applications, it will be necessary to apply schema changes (tables, views, stored procedures, and so on) to your existing database in order to support the Touchstone application.

Database Maintenance Activities

Deltek recommends completing the following activities on your database daily:

1. Check database integrity.
2. Rebuild indexes. (Doing this daily is not required, but it should be done at regular intervals.)
3. Update statistics.
4. Make a complete backup.

Deltek

Pre-Installation Checklists

You Should Know...

Before you start your installation, you should know:

- The fully qualified domain names for your Web/Application servers.
- The service account that you will use for the Touchstone IIS Application Pool Identity. This account will also be used by Touchstone to connect to the SQL Server or Oracle databases. The databases must be configured to allow the service account to connect to the database using Windows Authentication.
- The SQL Server account/Oracle schema that you will use to run the database scripts to create the Touchstone database tables.

Database Tier

Touchstone does not require any installation to be performed on the database tier if it is on its own server. Connections are made to the database tier when you run the installer on your Web/Application Server.

Step	Description	Related Topics
1	Verify that the Microsoft SQL Server or Oracle database version is supported and meets the system requirements.	Software Requirements
2	Verify that TLS 1.2 is enabled. Verify that the following are disabled: ▪ SSL 2.0/3.0 ▪ TLS 1.0/1.1 **Tip:** You can use the IISCrypto tool by Nartac Software to disable older protocols. Deltek recommends using the Strict Template to fulfill these requirements.	Microsoft article about disabling PCT 1.0, SSL 2.0, SSL 3.0, or TLS 1.0 in Internet Information Services: https://support.microsoft.com/en-us/help/187498/how-to-disable-pct-1-0-ssl-2-0-ssl-3-0-or-tls-1-0-in-internet-informat External link: https://www.nartac.com/Products/IISCrypto
3	The Touchstone installation script connects to the database server from the web server to verify the servers TLS/SSL configuration. Ensure that the user performing the installation on the Web/Application tier is a member of the Local Administrator group on the Database Server in order to complete this verification step during the installation.	

Deltek

Web/Application Tier

Step	Description	Related Topics
1	Verify that the server operating system is supported.	Software Requirements
2	Confirm that you have installed and configured the database client software in order to connect to the Database tier. **SQL Server** ▪ Download and install the MSL OLEDB **driver**. **Oracle** ▪ Install the 64-bit Oracle Database Client (Administrator installation type).	Appendix A: Using Microsoft SQL Server with Touchstone Appendix B: Using Oracle with Touchstone
3	Verify that TLS 1.2 is enabled. Verify that the following are disabled: ▪ SSL 2.0/3.0 ▪ TLS 1.0/1.1 **Tip:** You can use the IISCrypto tool by Nartac Software to disable older protocols. Deltek recommends using the Strict Template to fulfill these requirements.	Microsoft article about disabling PCT 1.0, SSL 2.0, SSL 3.0, or TLS 1.0 in Internet Information Services: https://support.microsoft.com/en-us/help/187498/how-to-disable-pct-1-0-ssl-2-0-ssl-3-0-or-tls-1-0-in-internet-informat External link: https://www.nartac.com/Products/IISCrypto
4	Install Microsoft Internet Information Services (IIS) with ASP .NET and the Microsoft .NET Framework enabled. Verify that you have a resolvable, fully qualified domain name (FQDN) and test FQDN URL access.	Microsoft Internet Information Server (IIS) Installation on Windows Server
5	Install the supported Microsoft .NET Framework version.	Software Requirements
6	Install a valid HTTPS (SSL) certificate. If Touchstone is only used internally, the certificate can be generated by an internal certificate authority. If Touchstone is used externally, the certificate must be generated by a third-party certificate authority, such as Verisign or DigiCert.	Configure Secure Sockets Layer (SSL)
7	Enable, configure, and test PowerShell Remoting.	Appendix E: PowerShell Script and Console

Deltek

Installation Overview

Follow these steps to install Touchstone.

Step	Description	Read this section:
1	Make sure that you have all the prerequisites in place.	Pre-Installation Checklists
2	Download the **DeltekAcumenTouchstone.ps1** PowerShell script.	Download the PowerShell Script from DSM
3	Run the **DeltekAcumenTouchstone.ps1** script, using no switches, to set up the installation environment and to check that the script prerequisites are in place.	Set Up the Environment and Verify Script Prerequisites (No Switches)
4	Re-run the **DeltekAcumenTouchstone.ps1** script, using the **-CheckPreReq** switch, to make sure that the product/software prerequisites are in place.	Verify Software Prerequisites (-CheckPreReq Switch)
5	Re-run the **DeltekAcumenTouchstone.ps1** script using **-Setup** to install Touchstone.	Install Touchstone (-Setup Switch)
6	Run the post-installation scripts to create the Touchstone tables in the database.	Create the Touchstone Tables in the Database
7	Set up PPM Administrator.	Set Up PPM Administrator
8	Set up EPM Security Administrator. **Note:** This is an alternative step to "Step 7: Set Up PPM Administrator."	Set Up EPM Security Administrator
9	Begin Touchstone set up.	Set Up Touchstone

Deltek

Install Touchstone on a Server with No Internet Access

To install Touchstone on servers that do not have an internet connection, you need a server with internet access to act as a Download Server. Download setup files to your Download Server and then copy the files to your non-internet-accessible servers. All authentication, acknowledgement, and licensing prompts occur only on the Download Server, regardless of the switches you use.

> **Note:** If the setup detects an installed version earlier than 8.2, it prompts you to uninstall and run the setup again. For more information, see the Uninstall Switch section in this document.

When you install on a server without an internet connection, you will see the following differences:

- There is no prompt to authenticate to DSM. This step is handled on the Download Server using the **-DownloadSetupPrep** switch.
- There are no acknowledgements that require internet calls.
- There are no downloads performed. The files are already downloaded.

> **Note:** The non-internet setup checks for an internet connection. If one exists, you are required to run the regular setup.
>
> The machine must have all prerequisites installed and configured before the switch can be used.

To install Touchstone on a machine that does not have internet access:

> **Note:** You need to enable TLS 1.2 and disable TLS 1.0 and 1.1 on all servers whether the machine has internet or not.

1. Using a machine that does have internet access, complete Step 1: Download the PowerShell Script from DSM in "Install Touchstone on a Server with Internet Access" and run it in PowerShell (as Administrator). This step will copy the file to the correct location in the server, specifically C:\Program Files\Deltek\Acumen Touchstone\Scripts.
2. From the C:\Program Files\Deltek\Acumen Touchstone\Scripts folder, run the **DeltekAcumenTouchstone.ps1** script with the **-DownloadSetupPrep** switch. This step downloads the script files to a folder on the machine and runs the self-updater.
3. Run **.\DeltekAcumenTouchstone.ps1 -DownloadSetupPrep** again.

   > **Note:** This will have the **DeltekAcumenTouchstone.ps1** script run the **-DownloadSetupPrep** switch and download the .exe files. This step also creates two .xml files in the C:\Program Files\Deltek\Acumen Touchstone root folder. These files are the following:
   >
   > - DeltekAcumenTouchstoneConfiguration.xml
   > - DeltekAcumenTouchstoneSettings.xml

4. Copy the entire C:\Program Files\Deltek folder to the machine that does not have internet to the same location.

   > **Note:** If you are upgrading Touchstone, copy the folder to the machine with no internet access. Replace any file, if prompted. Then, complete the remaining steps.

5. From the C:\Program Files\Deltek\Acumen Touchstone\Scripts folder, run **.\DeltekAcumenTouchstone.ps1 -CheckPreReq** in PowerShell (as Administrator).

   > **Note:** This step should not ask you for any username or password information.

6. Run **.\DeltekAcumenTouchstone.ps1 -Setup** to install Acumen Touchstone.

Deltek

Install Touchstone on a Server with Internet

Note: You need to enable TLS 1.2 and disable TLS 1.0 and 1.1 on all servers whether the machine has internet or not.

Step 1: Download the PowerShell Script from DSM

When you are sure that your prerequisites are in place, download the **DeltekAcumenTouchstone.ps1** PowerShell script from Deltek Software Manager (DSM) to a temporary location on your Touchstone Web/Application server.

Note: You only download this deployment script from DSM the first time you install Touchstone. When you run the script in the future, it automatically applies any updates.

To access DSM from within the Deltek Support Center:

1. In your Web browser, go to https://deltek.custhelp.com.
2. Enter your Deltek Support Center **Username** and **Password**, and click **Login.**
3. When the Deltek Support Center page displays, click **Product Downloads**.
4. On the Deltek Software Manager screen, click **Launch Deltek Software Manager**.
5. Click **Settings** at the top right of the dialog box to use the Settings dialog box to specify the folder to which you want Touchstone to download, and click **OK**.

   Note: The installation directory for Touchstone is determined by the drive from which you run the installation script. Touchstone supports installing to a drive other than C; however, the installation directory must be <drive>:\Program Files\Deltek\Acumen Touchstone. The system automatically creates this folder the first time you run the installation.

   For example, if you want to install Touchstone on the D:\ drive, download the **DeltekAcumenTouchstone.ps1** file to a temporary folder on the D:\ drive.
6. In the left pane, expand the Deltek Acumen Touchstone folder if it is not already expanded.
7. Select the checkbox next to the **DeltekAcumenTouchstone.ps1** PowerShell script.

   The right pane displays a message stating that the script has been added to the download queue.

   Note: You can also download the **Deltek Acumen Touchstone Database Size Estimator** spreadsheet and Touchstone documentation while you are on DSM.
8. Click **Download** at the bottom of the left pane to download the script to the folder that you selected.

Step 2: Set Up the Environment and Verify Script Prerequisites (No Switches)

After you download the **DeltekAcumenTouchstone.ps1** PowerShell script, you can begin installing Touchstone.

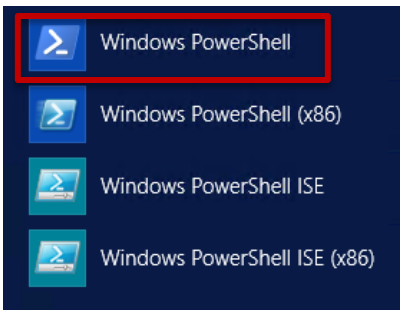
> **Attention:** For more information about the PowerShell console, entering commands, and performance, see Appendix E: PowerShell Script and Console.

Run the script the first time using no switches to:

- Set up the installation environment, including creating the installation directory and copying the script to the installation directory \Scripts folder.
- Verify that the prerequisites are in place to run the script with switches. (These script prerequisites are different from the product/software prerequisites, which are validated when you run the script using the **-CheckPreReq** switch.)

To run the script with no switches:

1. On the operating system **Start** menu, launch the Windows PowerShell Console:



> **Warning:** DO NOT attempt to run the **DeltekAcumenTouchstone.ps1** installation script using the Windows PowerShell ISE.

2. Run the console using the **Run as Administrator** option on the right-click context menu.

   The **DeltekAcumenTouchstone.ps1** script includes a #Requires statement that checks that you are running the PowerShell Console using the **Run as Administrator** option. If you are not, an error message displays.

3. In the PowerShell Console, which is similar to the command prompt, you may need to change the default directory (c:\windows\system32) to the directory where you stored the **DeltekAcumenTouchstone.ps1** script.

4. To run the script, enter **.\DeltekAcumenTouchstone.ps1** and press ENTER.

> **Note:** The default Execution Policy (get-executionpolicy) for the Touchstone supported operating systems is RemoteSigned. Your company may require a tighter policy (for example, Restricted). If you see an error, you may need to change the policy. For more information and steps, see PowerShell Execution Policy in Appendix E.

5. Enter your Deltek Support username and password.

   The script downloads and extracts the PowerShell modules and checks for any updates to the script. If updates are found, a message displays letting you know that the update is complete and to run the script again.

6. Re-run the script by entering **.\DeltekAcumenTouchstone.ps1** or clicking the **Up** arrow on your keyboard.

7. Enter your username and password again.

   The script downloads and extracts the PowerShell modules and checks for any updates to the script. Since you just completed an update, it shouldn't find any this time around.

   The script:

   - Checks that the correct versions of the following prerequisites are installed:
     - Operating system
     - .NET Framework
     - PowerShell
   - Checks that SSL 2.0/3.0 and TLS 1.0/1.1 have been disabled.
   - Downloads the **DeltekAcumenTouchstoneConfiguration.xml** file and overwrites any existing version of this file. The file stores meta-information about releases that are used to derive release, version, configuration, and dependency information. You should not change this file unless Deltek support asks you to change it.

     > **Attention:** For more information about the DeltekAcumenTouchstoneConfiguration.xml file, see Appendix F: Installation .XML Files.

   - Checks the system prerequisites.

   If any third-party software prerequisites are missing, they display in red in the script messages. The script automatically downloads the required installers to the following location and opens the folder: <drive>:\Program Files\Deltek\Acumen Touchstone\Support\PreReq. Resolve the problem before continuing with the setup process.

Step 3: Verify Software Prerequisites (-CheckPreReq Switch)

Run the **DeltekAcumenTouchstone.ps1** PowerShell script with the -**CheckPreReq** switch to verify that the product/software prerequisites are correct.

To run the script with the -CheckPreReq switch:

1. Run the script from the Touchstone installation \Scripts directory with the CheckPreReq switch appended: **.\DeltekAcumenTouchstone.ps1 -CheckPreReq**.

2. Enter your Deltek Support username and password.

   The script displays the username that was used when you ran the script with no switches. If it is the same username, you don't need to enter it again. If you need to change the username, enter the correct one.

   The script:

   - Downloads the PowerShell modules.
   - Checks for any updates to the script.
   - Checks that the correct versions of the following prerequisites are installed:
     - Operating system
     - .NET Framework
     - PowerShell
   - Downloads the Deltek Acumen Touchstone configuration file.
   - Checks system prerequisites.
   - Checks that all required IIS features are enabled. If any are not enabled, install them using Windows Server Manager or Deployment Image Servicing and Management (DISM), or use the EnableIISRequiredFeatures switch discussed in Microsoft Internet Information Server (IIS) Installation on Windows Servers.

3. Press ENTER if the default URL for your Web Server is correct, or enter the URL to your Web Server and press ENTER.

   The script tries to connect to the server and checks that a valid SSL certificate is installed. If it cannot make a valid HTTPS connection, an error message displays.

   If you see the error message, check that the URL is correct, that you are using HTTPS (not HTTP), and that an SSL certificate has been installed, and then re-try the connection. In most instances, your SSL certificate is assigned to a custom DNS value, not the DNS name of the server, even though the DNS name of the server displays in brackets at the prompt.

If everything is successful, continue with the next step.

Step 4: Install Touchstone (-Setup Switch)

Use the **DeltekAcumenTouchstone.ps1** PowerShell script with the **-Setup** switch to install Touchstone. You can perform different tier installations with the Setup switch.

Whether you are installing Touchstone on one server or multiple servers, all installation functions are performed from the Web/Application server where the Touchstone PowerShell Installation script is run.

> **Note:** You do not need to run this on the Database tier.

After you run the script, a log is created. Deltek recommends that you review the log files if you encounter any errors during the installation. If you find any errors, contact Deltek Customer Care with the contents of the log file. Setup logs are written to the installation directory Logs folder and stamped with the date and time that the setup script was executed.

> **Note:** If the setup detects an installed version earlier than 8.2, it prompts you to uninstall and run the setup again. For more information, see the Uninstall Switch section in this document.

To run the script with the -Setup switch:

1. Navigate to the Web/Application Server's installation directory Scripts folder and enter: **\DeltekAcumenTouchstone.ps1 -Setup**.
2. Enter your Deltek Support username and password.

   The script displays the username that was used when you ran the script with no switches. If it is the same username, you don't need to enter it again. If you need to change the username, enter the correct one.

   The script:

   - Downloads the PowerShell modules.
   - Checks for any updates to the script.
   - Checks that the correct versions of the following prerequisites are installed:
     - Operating system
     - .NET Framework
     - PowerShell
   - Downloads the Deltek Acumen Touchstone configuration file.
   - Checks system prerequisites.
   - Validates your access to Deltek Acumen Touchstone.
   - Verifies that all required IIS features are enabled.

   The script displays this message:

   "Touchstone requires resolvable FQDN using a valid SSL certificate being installed on the Web Server (IIS). TLS 1.2 is required. SSL 2.0/3.0 must be disabled. PowerShell Remoting is used so ensure it is enabled on all your tiers.

   The installation scripts are signed and should not be changed.

   Please read the installation documentation (that explains all above in more detail) before continuing."

   > **Note:** If you are installing Touchstone on a machine with no internet access, and you used the **DownloadSetupPrep** switch to download and copy the files, the script will not prompt you to acknowledge that you have read the installation documentation. In this case, skip the documentation acknowledgement steps.

   > **Note:** The server, whether the machine has internet or not, needs to be part of a Windows Domain for the **DownloadSetupPrep** switch to download and copy the files.

3. If you read and understand the message, enter **Yes**.

4. The script displays the fully qualified domain name of the Web server, with the prefix HTTPS.

   Either press ENTER to accept the displayed value or, if your web server SSL certificate is registered to a custom DNS value, enter the fully qualified URL for the web server.

   - The URL (FQDN) must start with **https://**.

5. The script prompts you for the account to be used as the IIS Application Pool identity. The Application Pool Identity can either be a domain account (preferred) or a local account. The default value is a local account called **[DeltekTouchstone]**.

   If you choose to have the default domain account installation, create the **[DeltekTouchstone]** account. After its creation, you will have to add this account to the domain.

   Either press ENTER to accept the default value or enter an existing domain account and press ENTER.

6. Enter a password.

   The script checks that the password entered is a secure password so that it will pass standard Domain Group Policy password tests.

7. When the password passes the check, enter the password again to confirm it and press ENTER.

   If you chose a local account and it does not exist, the script creates it. Regardless of whether you entered a local or domain account, the script adds the account to the local Administrator group.

   After you enter all of the information, the script:

   a. Downloads and extracts the following Touchstone installation files to <drive>\Program Files\Deltek\Acumen Touchstone:

      - DeltekAcumenTouchstone<version>.exe

   b. Creates IIS Virtual Directories/Applications and associates them with the DeltekAcumenTouchstone Application Pool:

      - **DeltekAcumenTouchstone:** <drive>:\Program Files\Deltek\Acumen Touchstone\Web
      - **DeltekAcumenTouchstone\App:** <drive>:\Program Files\Deltek\Acumen Touchstone\Web\app
      - **PPMAPI:** <drive>\Program Files\Deltek\Acumen Touchstone\web\PPMAPI

      > **Note:** If you have more than one website, the installer displays a list of the sites and asks you to enter the site ID where you would like Touchstone installed.

   c. Updates the Deltek Acumen Touchstone Settings file.

   d. Copies and updates the config files for the installation.

   e. Creates three Touchstone scheduled tasks that run every 15 minutes:

      - **Reset Submittal Process:** This scheduled task periodically scans for Submittals that may have prematurely terminated prior to the process completion or are taking an excessive amount of time to complete. It sets the Submittal Status to **Failed** when it finds submittals that meet either of these conditions.

- **Touchstone Clear Expired Sessions:** This scheduled task periodically scans for and removes inactive user sessions. These typically occur when a user does not log out of Touchstone prior to closing the Touchstone application session in their web browser.
- **Cleared Reports:** This scheduled task periodically scans for reports stuck in submitted/processing statuses and sets the Report Status to **Failed**.

> **Note:** When the installation script is complete, the Acumen Touchstone folder is created under:
>
> - <drive>\Program Files\Deltek\
>
> To see details of the scripts that ran during the installation, navigate to the *Acumen Touchstone\Scripts* folder. You can open and view any of the scripts but cannot edit them.

8. Run the **TouchstoneSnapshotPersistJsonDataProcess.ps1** PowerShell script as needed.

   This script will update the snapshots created before Touchstone version 8.10 to include the JSON metadata across all Touchstone databases.

9. Run the **MigrateEmailSettings.ps1** PowerShell script.

   This script will update the email settings to prepare its migration to PPM Administrator.

10. When the installation script is finished running, verify that the installation was successful.

Step 5: Create the Touchstone Tables in the Database

The next step is to run the database scripts on your database server to create the necessary Touchstone database tables and data.

> **Note:** If you have not already created the database, create it before you continue with this step.

> **Additional Note:** If you will open the scripts in a text editor, make sure the editor supports Unicode characters.

The scripts that you run depend on whether you have a new database or an existing Deltek PPM database, and whether you are using SQL Server or Oracle.

Touchstone includes database scripts for both SQL Server and Oracle databases. The scripts for each database type are located in subfolders in the Acumen Touchstone\Databases\Scripts folder.

- **Touchstone_Tables_*:** This script creates all necessary database tables required by Touchstone. You run it when you create a new Touchstone database or when you add Touchstone to an existing PPM database.
- **Touchstone_Upgrade_*:** This script upgrades tables in an existing PPM database with the necessary changes that are required to support Touchstone. You run it when you add Touchstone to an existing PPM database.
- **Touchstone_Data_*:** This script adds the necessary data to the Touchstone database tables that is required by Touchstone. You run it when you create a new Touchstone database or when you add Touchstone to an existing PPM database.

- **Touchstone_Oracle_CI_Indexes:** This Oracle script provides support for case-insensitive index in Oracle databases when you install Touchstone in a Deltek PPM database that is used by Cobra or PM Compass. You must run it when you add Touchstone to a PPM database that is used by Cobra or PM Compass.
- **WST_Tables_*:** This script creates the PPM common tables that are shared by multiple Deltek PPM products. You run it when you create a new Touchstone database.
- **WST_Upgrade_*:** This script upgrades PPM common tables, that are shared by multiple Deltek PPM products, in an existing PPM database with the necessary changes required to support the various PPM products.
- **WST_Data_*:** This script adds the default data to common tables that are shared by multiple Deltek PPM products. You run it when you create a new PPM product database for Touchstone.
- **WST_Oracle_ CI_Indexes_*:** This script creates case-insensitive indexes on WST tables for integration with Cobra and PM Compass. This is run when you install any PPM product in a database that is used by Cobra or PM Compass.

SQL Server Scripts

New Database	Existing PPM Database
▪ WST_Tables_SQLServer.sql ▪ WST_Data_SQLServer.sql ▪ WST_Upgrade_SQLServer.sql ▪ Touchstone_Tables_SQLServer.sql ▪ Touchstone_Data_SQLServer.sql	▪ WST_Upgrade_SQLServer.sql ▪ Touchstone_Upgrade_SQLServer.sql

Oracle Scripts

New Database	Existing PPM Database
▪ WST_Tables_Oracle.sql ▪ WST_Data_ Oracle.sql ▪ WST_Oracle_ CI_Indexes.sql ▪ WST_Upgrade_Oracle.sql ▪ Touchstone_Tables_Oracle.sql ▪ Touchstone_Data_Oracle.sql ▪ Touchstone_Oracle_CI_Indexes.sql	▪ WST_Upgrade_Oracle.sql ▪ WST_ Oracle_ CI_Indexes.sql ▪ Touchstone_Upgrade_Oracle.sql ▪ Touchstone_Oracle_CI_Indexes.sql

Step 6: Set Up PPM Administrator

The Deltek PPM Administrator is a security tool that the Touchstone Administrator can use to define and manage licenses, users, and security.

Deltek

Note: Make sure to download the most recent version of PPM Administrator from DSM before starting the setup process.

It is the next-generation replacement for the Deltek EPM Security Administrator. PPM Administrator consolidates the legacy desktop and Smart Client versions into a modern, web-based tool that strengthens security management across the Deltek PPM suite. It offers enhanced usability, centralized access control, and improved integration with Touchstone. PPM Administrator also offers a full Rest API to allow integration with other systems.

Attention: For detailed information about setting up PPM Administrator, see the PPM Administrator online help.

Before you can log into new installations of Touchstone, you must use PPM Administrator to:

- Add a data source for Touchstone.
- Add a Touchstone product license.
- Add Touchstone users.

Add the Data Source

To add the data source:

1. Log into PPM Administrator.
2. Launch the PPM Datasource Management Tool.
3. Click **Add**.
4. In the Add Data Source dialog box, click the General tab and enter or select the values in the **Name**, **Schema**, and **Provider** fields.
5. Click the **Configure** button.
6. In the Data Link Properties dialog box, enter or select the values in the appropriate fields on each tab.
7. Click the **Test Connection** button to verify if the connection information is correct.

Note: If you are using Oracle ODP.NET as your provider, you must specify the Oracle connection details in the format **ServerName/Instance**. For example, if your Oracle server is named **ServerA** and the Oracle instance is **ORCL**, then your Data Source value would be **ServerA/ORCL**.

Microsoft made their SQL Server providers connect only to database servers that are configured with SSL/TLS by default, as using database servers without SSL/TLS poses security risks.

To make SQL Server providers connect to unsecured database servers, the encryption of the data must be disabled when configuring providers:

- For Microsoft OLE DB Driver 19 for SQL Server, on the Advanced tab, set the **Connection encryption** field to **Optional**.
- For Microsoft OLE DB Driver for SQL Server, on the Connection tab, remove the checkmark in **Use strong encryption for data** option.
- For Microsoft OLE DB Provider for SQL Server or SQL Server Native Client, on the All tab, set the **Use Encryption for Data** field to **False**.
- For SQL Server .NET Framework, on the Advanced tab, set the **Encrypt** field to **False**.

Add the Touchstone Product License

When you purchase a Touchstone license, Deltek sends you an email with a new license key. The email includes the client ID number, activation key, and number of users who can log on to Acumen Touchstone. Touchstone supports both Named and Submitter licenses.

- A **Named** license provides access to the full functionality of the product but does not allow more users to be assigned to the license than the license allows.
- A **Submitter** license is a limited license that only provides access to the Submittals hub to allow users to submit schedules for projects to which they have been assigned. This license, like the named license, only allows the licensed number of users to be assigned to the license.

To add a Touchstone product license to PPM Administrator:

1. Log into PPM Administrator.
2. In the Navigation pane, select **SECURITY » Licenses**.

   By default, **Licenses Detail View** displays.
3. At the upper right part of the **Licenses Detail View**, click **+ New License**.
4. On the **Licenses Detail View**, enter the necessary information.

   Note: For Touchstone, the client ID is required.
5. When you are done, click **Save**.

Add Touchstone Users

The primary task of the system administrator is to provide a potential user with access to one or more supported Deltek application. The first step in providing this access is to create a user record.

To add a user:

1. Log into PPM Administrator.
2. In the Navigation pane, select **SECURITY » Users**.

   By default, **Users Detail View** displays.
3. On the **Users Detail View**, click **+ New User**.

   Note: You can only add users when the authentication mode is set to **Basic**, **Windows**, or **Mixed** on the System Authentication tab. In addition, all installed products should be compatible with PPM Administrator. Otherwise, the **+ New User** button will be disabled.
4. On the GENERAL tab, complete the necessary fields.
5. On the other tabs of the created record, enter the necessary information for the user.
6. When you are done, click **Save**.

   When adding new users, PPM Administrator automatically sends them a temporary password email. New users must change their password before logging in to PPM Administrator. The new password must adhere to the established password policies, and blank passwords are not allowed.

   Note: A product license must be assigned to the users before a temporary password can be sent to their email addresses.

Step 7: Set Up EPM Security Administrator

Attention: With the release of Acumen Touchstone 8.11.3, EPM Security Administrator will no longer be bundled with the Acumen Touchstone installer. You will have to download it separately from the DSM. In addition, EPM SA versions downloaded prior to Acumen Touchstone 8.11.3 are incompatible with the latest version and will no longer function.

Note: This is an alternative step in the installation process. If you have already completed “Step 6: Set Up PPM Administrator,” you do not have to complete this step.

The Deltek EPM Security Administrator (EPM SA) is a security tool that the Touchstone Administrator can use to define and manage licenses, users, and security.

The Touchstone security features enable the System Administrator to grant or restrict access to views and processes in Touchstone. To define rights to the application, the System Administrator uses EPM SA to create user "roles" that reflect your organization's business rules. The System Administrator then assigns each user or a group of users to a role.

EPM SA allows you to define the security rights for all PPM applications, such as Touchstone, PM Compass, Cobra, and Open Plan. These applications offer different options, but they all follow the same premise.

You use EPM SA to perform tasks such as:

- Define groups and users

- Define roles and permissions
- Disable or enable user logins
- Terminate current sessions in Touchstone

> **Attention:** For detailed information about setting up security in EPM SA, see the EPM Security Administrator online help.

Before you can log into Touchstone, you must use EPM SA to:

- Add a data source for Touchstone.
- Update the Touchstone URL.
- Add a Touchstone product license.
- Add Touchstone users.

Add the Data Source

To add the data source:

1. Launch the EPM SA.

   Navigate to <install drive>\Program Files\Deltek\EPMSecAdmin
   SQL Server: Select **Microsoft OLE DB Driver for SQL Server**. Do not select the older Microsoft OLEDB Provider for SQL Server as it does not support the newer TLS 1.2 protocol.

   > **Note:** Always select the option with Driver in the label. An error will occur when you select the option with Provider in the label.

   - **Oracle:** Select **Oracle Provider for OLEDB**. Do not select the older Microsoft OLEDB Provider for Oracle as it does not support the newer TLS 1.2 protocol.
2. On the Connection tab, enter all required information, test the connection, and click **OK**.
   - **SQL Server:** Choose **Windows Authentication** from the **Enter information to log on to the server** drop-down list.

     > **Note:** Touchstone requires Windows Authentication when you create datasources. EPM SA will not let you proceed in creating a datasource when the new datasource is not set for Windows Authentication.

   - **Oracle:** A Windows Authenticated connection is enabled when you enter a forward slash (/) for the username and leave the password blank.
3. On the Edit Data Source dialog box:
   - In the **Name** field, enter a name for the Touchstone data source.
   - In the **Database Name (Schema)** field:
     - **SQL Server:** Enter **dbo**.
     - **Oracle:** Enter the schema name that owns the database.

- Select **Database is Unicode**.

4. Click **OK**.
5. On the Data Sources dialog box, select the newly created data source and click **OK**.

You can now log into EPM Security Administrator and add your product licenses.

> **Note:** The default user name for first time login is "SYSADMIN" and the default password is "password". Deltek strongly recommends that you change the "SYSADMIN" account password after you have logged in.
>
> In addition, when you create a new password for a database, make sure not to use the semicolon (;) character. If you use the semicolon (;) character in a password, you will have to place a single quotation mark before and after the password.

Update the Touchstone URL

> **Note:** The **URL** field remains available in EPM SA. However, if you are using the PPM Administrator website, you will have to follow the process below.

By default, when the product URL in Touchstone is not set or is empty, the system automatically assigns the current browser path as the product URL upon user login.

To update a Touchstone URL:

1. Log into Touchstone.
2. In the Navigation pane, select **Settings » General**.
3. In the Email Footer Template tab, go to **URL**.
4. Change the URL.

   The chosen URL should begin with a valid protocol, such as http or https.

Add the Touchstone Product License

When you purchase a Touchstone license, Deltek sends you an email with a new license key. The email includes the client ID number, activation key, and number of users who can log on to Acumen Touchstone. Touchstone supports both **Named** and **Submitter** licenses.

- A **Named** license provides access to the full functionality of the product but does not allow more users to be assigned to the license than the license allows.
- A **Submitter** license is a limited license that only provides access to the Submittals hub to allow users to submit schedules for projects to which they have been assigned. This license, like the named license, only allows the licensed number of users to be assigned to the license.

To add a Touchstone product license to EPM SA:

1. In EPM SA, expand the Products folder and select **Acumen Touchstone**.
2. In the right pane, select **Manage Licenses**.
3. On the Manage Touchstone Licenses dialog box, click **Add.**

4. Enter the **Client Number**, **Activation Key**, and **Organization**.
5. Click **OK**.

Add Touchstone Users

In order for users to have access to different areas of Touchstone, they must be added to EPM Security Administrator and/or PPM Administrator and assigned to a Named or Submitter license. In addition to adding them manually, you can also import users from an active directory, Outlook, or a text file.

Users might be Touchstone Administrators, Project Managers, or Subcontractors (Submitters).

> **Note:** When you create a new user, the username is **new user** by default. In addition, you will be sent a temporary password via email. Deltek recommends changing the user name and password upon first login.
>
> When you create a new username and new password, make sure not to use the semicolon (;) character. If you use the semicolon (;) character in a username and/or password, you will have to place a single quotation mark before and after the username and/or password.
>
> See the *Touchstone Workflow* topic in the Touchstone online help (**Getting Started » Touchstone Workflow**) for more info on setting up the new user.

In EPM SA, you can create roles that grant or deny access to certain areas of Touchstone. These roles define the type of operations a user can perform, such as submit schedules, add projects, and create templates. When you create a user, you assign them to a role. For example, if you disable Settings for a role, the users assigned to that role won't see the Settings group in the Touchstone Navigation pane.

You can override the primary role if a user has a different role on another project. You can also override a user's primary role via group settings. For example, you can give a group called the PMO (project management office) a role with a high degree of access. This simplifies the process of granting access to all members of a group. For a group of project managers (PMs), the role assigned to the group might not allow access to Acumen Touchstone Settings options like Benchmark Attributes or Metrics.

Security in Touchstone uses the most permissive access. For example, if a user has read-only access to a project but is a member of a group that has full access to the same project, the user will have full access.

Step 8: Verify That the Installation Was Successful

Verify the installation to confirm that all prerequisite software is installed and all installation steps have been completed.

To verify that the installation was successful:

1. Open a supported browser and enter the URL to Acumen Touchstone:

   https://<Web Server>/**acumentouchstone/app/**.
2. On the Logon screen, enter your **User ID** and **Password**.
3. Use the drop-down list to select the **Database**.

   If more than one datasource is available, a list box displays on the login screen that allows you to select the data source that you would like to use. If only one datasource is available, the list box does not display.

4. Click **Login**. If Touchstone opens, your installation is successful.

> **Note:** Any errors that occur during the installation process will be listed in the installation log.

Step 9: Initial Setup in Touchstone

> **Note:** You only need to complete this step if you are performing a new Touchstone installation.

For information and steps about the tasks that need to be performed for the initial Touchstone setup, see the *Touchstone Workflow* topic in the Touchstone online help (**Getting Started » Touchstone Workflow**). The help topic includes the following information:

- **IT Administrator:** Create User Accounts in EPM Security Administrator
- **Touchstone Administration:** Initial Touchstone Setup
- **Project Manager:** Create a Program
- **Project Manager:** Create Projects
- **Project Manager:** Send Submitter Login Details
- **Submitter:** Log Into Touchstone for the First Time
- **Submitter:** Upload a Schedule Snapshot
- **Project Manager:** Select and View Benchmark Attributes

Deltek

Upgrade Touchstone

Step 1: Upgrade Touchstone Application (-Upgrade Switch)

Use the **DeltekAcumenTouchstone.ps1** PowerShell script with the **-Upgrade** switch to upgrade the Touchstone application.

Whether you are installing Touchstone on one server or multiple servers, all installation functions are performed from the Web/Application server where the Touchstone PowerShell Installation script is run.

> **Note:** The script:
>
> 1. Stops the W3SVC (IIS).
> 2. Downloads and extracts the new Acumen Touchstone build and removes the prior build.
> 3. Restarts the services stopped in Step 1.
>
> When you install on a server without an internet connection, any acknowledgement and licensing prompts and file downloads occur only on the Download Server.

Deltek recommends that you upgrade to the latest version of Acumen Touchstone because:

- New features are added only to the latest version.
- Except in critical situations, Deltek resolves software issues only in the latest version.
- Deltek support is typically available only for the latest and the next previous versions.
- The latest version incorporates the newest technologies and tools.

> **Note:** Before upgrading, review the Acumen Touchstone Release Notes and perform a test conversion and test installation of the new version to ensure that your business processes are working correctly in the new version.

After you run the script, a log is created. Deltek recommends that you review the log files if you encounter any errors during the installation. If you find any errors, contact Deltek Customer Care with the contents of the log file. Setup logs are written to the installation directory Logs folder and stamped with the date and time that the setup script was executed.

> **Note:** If the setup detects an installed version earlier than 8.2, it prompts you to uninstall and run the setup again. For more information, see the Uninstall Switch section in this document.

To run the script with the -Upgrade switch:

1. Navigate to the Web/Application Server's installation directory Scripts folder and enter: **.\DeltekAcumenTouchstone.ps1 -Upgrade**.
2. Enter your Deltek Support username and password
3. When prompted to upgrade Touchstone to the latest version, enter **Yes**.
4. When the upgrade script is finished running, verify that the installation was successful.

5. Upgrade your database.

> **Note:** When you initially run the Setup switch to set up your Acumen Touchstone environment, the setup prompts you for information about your servers and validates that information. After it is validated, the information is written to the DeltekAcumenTouchstoneSettings.xml file at the root of the Acumen Touchstone installation directory.
>
> The Upgrade switch attempts to retrieve the server information so that you are not prompted for the same information again. If the information in the settings file is not accurate, you must edit that file prior to running the Upgrade switch.

Step 2: Upgrade the Touchstone Database

After you run the deployment script to upgrade Touchstone, you must manually run a script to upgrade the database.

- **Oracle:** Run the **Touchstone_Upgrade_Oracle**, **WST_Upgrade_Oracle**, and all **CI_Indexes** scripts on your Touchstone Databases.
- **MS SQL Server:** Run the **Touchstone_Upgrade_SQLServer** and **WST_Upgrade_SQLServer** scripts on your Touchstone Databases.
- **PowerShell:** If you have snapshots prior to Touchstone version 8.10, run the **TouchstoneSnapshotPersistJsonDataProcess.ps1** script in C:\Program Files\Deltek\Acumen Touchstone\Support\. This script generates JSON metadata for all databases listed in datasources.dat.

  > **Note:** For more information on the **TouchstoneSnapshotPersistJsonDataProcess.ps1** PowerShell script, see Appendix E: PowerShell Script and Console.

  If you are upgrading Touchstone, run the **MigrateEmailSettings.ps1** script in C:\Program Files\Deltek\Acumen Touchstone\Support\. This script will update your email settings for its migration to PPM Administrator.

You can find the scripts in the installation folder under **Deltek\Acumen Touchstone\Databases\Scripts**.

> **Attention:** For more information on the database scripts, see Step 5: Create the Touchstone Tables in the Database section in this document.

Deltek

Touchstone Logs

The installation creates a logs subfolder that contains the installation log. The logs are located in the **\Program Files\Deltek\Acumen Touchstone\Logs** folder. You cannot change this folder location.

Every time you run the **DeltekAcumenTouchstone.ps1** script, the installer creates a log with the date and time that the script was executed.

Passwords are not stored in the log. They display as **<Password>**.

Deltek

Optional Switches

This table lists all of the optional switches that you can run with the **DeltekAcumenTouchstone.ps1** PowerShell script.

Switch	Use this switch to...	Read this section...
DownloadSetupPrep	Download all setup files needed to install Touchstone on servers that are not connected to the internet.	DownloadSetupPrep Switch
Upgrade	Apply software updates to your Touchstone installation.	Step 1: Upgrade Touchstone Application (-Upgrade Switch)
Uninstall	Remove Touchstone from the Web/Application server.	Uninstall Switch
SendLogsToDeltek	Compress all of the logs in the \Logs folder and send them in an email to Deltek.	SendLogsToDeltek Switch
ConfigureWindowsAuthentication	Configure Windows Authentication for Touchstone.	ConfigureWindowsAuthentication Switch

DownloadSetupPrep Switch

Use the DownloadSetupPrep switch if you are installing Touchstone on servers that do not have an internet connection. Download the setup files to a Download Server and then copy the files to your non-internet-accessible servers.

- The Download Server cannot contain a build or installation of Touchstone.
- After you run the **DownloadSetupPrep** switch on the Download Server, you cannot run any other switches on this server.

To run the installation script with the -DownloadSetupPrep switch:

1. From the installation directory Scripts folder, enter **.\DeltekAcumenTouchstone.ps1 -DownloadSetupPrep**.
2. Enter your Deltek Support username and password.

   The script checks prerequisites and verifies your access to Touchstone.

   The script displays a message indicating that it will download files for installation/upgrade in a non-Internet connected environment and provides information on the currently downloaded build (if applicable) and the build version being downloaded.

   The script downloads the following files to the installation directory:

   - DeltekAcumenTouchstoneConfiguration.xml

- DeltekAcumenTouchstoneSettings.xml (The file extension is renamed to .bak on the Download Server to avoid overwriting the file on your installation servers)
- Updated PowerShell script and associated modules:
- SQL Server PowerShell Module
- Visual C++ components
- DeltekAcumenTouchstone<build>.exe
- Acumen Touchstone license file script

The script creates a new **DeltekAcumenTouchstoneSettingsInternet.xml** file to track the build version and download date.

After the script operations are completed, the script prompts you to copy the full Deltek folder under Program Files to the Program Files directory on your Web/Application server.

4. After the files are copied to your non-internet servers, install Touchstone, starting with Step 3: Verify Software Prerequisites (CheckPreReq Switch).
5. Run the appropriate Setup switch for your chosen Web/Application server.
6. When a new build is available, run the **DownloadSetupPrep** switch again on the Download Server to download the updated build files. Copy the files to your existing server(s), overwriting existing files as necessary, and run the appropriate upgrade switches.

Uninstall Switch

Use the Uninstall switch to remove Touchstone from your Web/Application server. The script:

- Removes the Touchstone/PPMAPI IIS applications.
- Removes the DeltekAcumenTouchstoneApplicationPool IIS application pool.
- Checks to see if the local DeltekTouchstone account exists and, if it does, asks you if you want to delete the account.
- Removes the installation files, except for the \Scripts and \Logs folders.

To run the installation script with the -Uninstall switch:

1. From the installation directory Scripts folder, enter **.\DeltekAcumenTouchstone.ps1 -Uninstall**.

   The script checks for prerequisites and asks if you want to continue with the uninstall process.
2. Enter **Yes** to start the uninstall process.

SendLogsToDeltek Switch

Use this switch to compress and send installation logs via email to Deltek. Run this switch anytime Deltek requests log files for review.

To run the installation script with the -SendLogsToDeltek switch:

1. From the installation directory Scripts folder, enter **.\DeltekAcumenTouchstone.ps1 –SendLogsToDeltek**.

   The switch compresses and sends all logs in the \Logs folder via email.

Deltek

ConfigureWindowsAuthentication Switch

Use this switch to configure Windows Authentication for Touchstone.

To run the installation script with the -ConfigureWindowsAuthentication switch:

1. From the installation directory Scripts folder, enter **.\DeltekAcumenTouchstone.ps1 -AdvancedSetupOption ConfigureWindowsAuthentication**.

   The switch enables the IIS Windows Authentication module (if it is not already enabled), configures Windows Authentication, and updates the necessary configuration files to enable Windows Authentication.

2. To complete the Windows authentication configuration in EPM Security Administrator, perform the steps outlined in the Configure Touchstone for Windows Integrated Authentication.

Deltek

Troubleshooting

Installation Issues

If you encounter issues during the Touchstone installation and are unable to continue, contact Deltek Customer Care for assistance and include the following information:

- The timestamped setup log stored in the **\Program Files\Deltek\Acumen Touchstone\Logs** folder on the Touchstone server.
- Screenshots and details about the errors received.

> **Note:** A Deltek Customer Care analyst might ask you to use the SendLogsToDeltek switch, which zips and sends the logs directly to Deltek via email. This information helps Deltek to resolve your issue as quickly as possible.

Touchstone Window Is Empty

Issue: After you install Touchstone, if you launch the browser and navigate to the Touchstone URL before you connect to a database, the Touchstone window displays an empty page (no login dialog box).

Solution: You must log in to EPM Security Administrator and add a data source before you can log into Touchstone. For more information, see Step 6: Set Up EPM Security Administrator.

Azure-Hosted SQL Server and Windows Authentication

Touchstone requires Windows Authentication to be enabled when you create datasources. When you do not enable Windows Authentication, the EPM SA desktop tool will not allow you to proceed in creating a datasource. However, this adds the connection string attribute Integrated Security=SSPI to the connection string, which is not valid when you connect to Azure-hosted SQL databases.

As a workaround, you will have to manually remove the Integrated Security=SSPI connection string attribute from the datasources.dat file.

> **Note:** For additional assistance, contact the Deltek Support Center.

Deltek

Appendix A: Using Microsoft SQL Server with Touchstone

Database Platform Options for Microsoft SQL Server Databases

The procedure in this section is for Administrators performing the Touchstone installation on a Microsoft SQL Server database.

> **Note:** If you are unable to connect to your SQL Server or have not yet performed the requirements, see the Database Requirements section in this guide.

Storing Touchstone Data in a Microsoft SQL Server Database

Touchstone supports Microsoft SQL Server Standard and Enterprise Edition. The following Microsoft link lists the features supported by the different editions of Microsoft SQL Server. Click **Other Versions** and select the version that you are using: https://learn.microsoft.com/en-us/mem/configmgr/core/plan-design/configs/support-for-sql-server-versions.

Touchstone requires a Windows Authenticated connection to the database. You must give the Touchstone Application Pool Service Account Login rights to Microsoft SQL Server. It must be an existing Windows account. The account must be given the **db_owner** database role membership to the database in the Login Properties and User Mapping dialog box.

Create a Login in SQL Server for the Touchstone Application Pool Service Account and Assign It to the Database

To create a SQL Server Login for the Touchstone Application Pool Service Account that runs the Touchstone IIS Application Pool and give it access to the Touchstone database in Microsoft SQL Server:

1. Launch Microsoft SQL Server management Studio and connect to the Touchstone database server.
2. Expand the **Security » Logins** folder.
3. Right-click the Logins folder and select **New Login**.
4. Enter the account that is used to run the Touchstone Application Pool and select **Windows authentication**.
5. Click **User Mapping** and select the **Touchstone database** checkbox in the **Users mapped to this login** section.
6. In the **Database role membership for the Touchstone database** section, select the **db_owner** checkbox to add the login to the db_owner role for the database.
7. Click **OK**.

Install the Microsoft OLE DB Driver for SQL Server

The Microsoft OLE DB Driver supports TLS 1.2 secure communications and is needed for connecting to the SQL Server database from the Touchstone server.

Enable the TCP/IP and Shared Memory Network Protocols

Enable the "TCP/IP" and "Shared Memory" Network Protocols in SQL Server Configuration Manager on the Microsoft SQL Server. All network protocols are installed by SQL Server Setup but may or may not be enabled. Use SQL Server Configuration Manager to enable "TCP/IP" and "Shared Memory" to allow Touchstone to connect to the database.

> **Attention:** For details, see the article on Microsoft's website titled *How to: Enable or Disable a Server Network Protocol (SQL Server Configuration Manager)*—http://msdn.microsoft.com/en-us/library/ms191294.aspx

SQL Server Connection (Port 1433)

If your SQL Server is configured to listen on a port other than TCP 1433, and the SQL Server Browser service is disabled, Touchstone will not be able to connect to your database server.

> **Note:** If you disable the SQL Server browser service on your Database Server, and you are not using TCP port 1433, Deltek strongly recommends that you use the SQL Server Client Network Utility (part of the Windows operating system) on the Touchstone server to tell it how to connect to the Database Server using the correct port without having to specify the port number each time you make a connection.
>
> Background information: When you make connections to the SQL Server, the Touchstone Server tries to connect using TCP port 1433. If SQL Server was installed using a different port, the SQL Server browser service on the Database Server directs the connection to the correct port number. If this service is disabled, the Touchstone server does not know how to connect unless you specify the port number each time you make a connection (for example, DBServerA,2325).

You can do one of the following (not both):

- Enable the SQL Server Browser service on the Database server.
- Run the SQL Server Client Configuration Utility on every Web/Application server to create a SQL Server connection alias that contains the SQL Server name/instance along with the port number.
    1. Navigate to the Configuration Utility:
        - %SystemRoot%\system32\cliconfg.exe
    2. On the SQL Server Client Network Utility dialog box General tab, enable **TCP\IP**.
    3. On the Alias tab, click **Add**.
    4. On the Edit Network Library Configuration dialog box:
        a. In the **Server alias** field, enter a name for the alias. For example, the SQL Server name or instance to which you are connecting.
        b. In the Network Libraries group, click **TCP\IP**.
        c. In the **Server name** field, enter a server name.
        d. Deselect **Dynamically determine port**.

e. In the **Port number** field, enter the port number that you configured SQL Server to listen on.

f. Click **OK**.

g. Click **Apply**.

Your Touchstone connection should now be successful.

SQL Server Instance Name

Verify the name of your SQL Server Instance. During the installation of Microsoft SQL Server, Microsoft gives you the option to install the Database engine to the default instance (named MSSQLSERVER) or to a named instance that you specify. The default Touchstone installation uses the server name for the connection and installs as an instance named MSSQLSERVER.

Note:

- When connecting to the Default SQL Server Database Engine instance, you use the name of your Database server. SQL Server automatically maps the Default Instance of the Database Engine to the Server Name when accepting connections.
- When connecting to a named instance of SQL Server Database Engine, you must specify the name of the SQL Server plus the instance in the connection in the format of SERVERNAME\INSTANCENAME.

  For example, if your SQL Server is named SQLSERVER1 and you installed to an instance named SQL2008, you would specify the server connection information in the format of SQLSERVER1\SQL2008.

If you do not know the name of your SQL Server instance, or you are unable to connect to your database server after installation, see the article on Microsoft's website titled *How to: Determine Whether the Database Engine Is Installed and Started*: http://msdn.microsoft.com/en-us/library/ms366339.aspx.

SQL Server and Windows Authentication

Touchstone requires **Windows Authentication Only** to connect to the SQL Database Server.

Download the Microsoft OLE DB Driver

The Microsoft OLE DB driver 19.3.5 for SQL Server allows Touchstone to access the data source when the server has been configured to use a secure TLS connection.

Before connecting to your data source, download and install the Microsoft OLE DB driver for SQL Server.

To download and install the Microsoft OLE DB driver for SQL Server:

1. Navigate to: https://learn.microsoft.com/en-us/sql/connect/oledb/download-oledb-driver-for-sql-server?view=sql-server-ver16.
2. Select **Download Microsoft OLE DB Driver 19 for SQL Server (x64)**.
3. Download and install.

> **Note:** On the Feature Selection screen, you only need to select **Client Components**.

Microsoft SQL Server Edition and Version Information

Use these links to learn about recommended SQL Server service packs and cumulative updates.

- **Microsoft SQL Server 2016 Service Pack 1 (SP1):** Microsoft SQL Server 2016 SP1 Update. This package contains the Microsoft SQL Server 2016 Service Pack 1 update to be applied to existing SQL Server 2016 installations:

  https://www.microsoft.com/en-us/download/details.aspx?id=54276

- **Microsoft SQL Server 2017 Cumulative Update:** Cumulative update package 6 for SQL Server 2017 RTM:

  http://catalog.update.microsoft.com/v7/site/Search.aspx?q=SQL%20Server%202017%20RTM%20Cumulative%20Update%20(CU)%206%20KB4101464%20

- **Microsoft SQL Server 2016 Cumulative Update:** Cumulative update package 6 for SQL Server 2016 SP1:

  http://catalog.update.microsoft.com/v7/site/Search.aspx?q=SQL%20Server%202016%20Service%20Pack%201%20Cumulative%20Update%20(CU)%206%20KB4037354%20

- **Microsoft SQL Server 2016 Express Edition with Advanced Services**
  - If you are using the free edition of SQL Server as your database, download and install Microsoft SQL Server 2016 with Advanced Services:

    https://download.microsoft.com/download/9/0/7/907AD35F-9F9C-43A5-9789-52470555DB90/ENU/SQLEXPRADV_x64_ENU.exe

  - You must also download and install SQL Server Management Studio, which does not come as part of SQL Express:

    http://go.microsoft.com/fwlink/?LinkID=840946

Deltek

Appendix B: Using Oracle with Touchstone

Note: Deltek provides several deployment models. For all models, Deltek assumes that your Oracle Database Server is a separate machine. No installations are performed on this machine. All connections to your Database Server are made from the Touchstone Web/Application server.

Storing Touchstone Data in an Oracle Database

To store the Touchstone data in an Oracle database, the following is required:

- Oracle database Standard or Enterprise editions.
- Contact your Oracle DBA to obtain the Oracle server name/SID and the user credentials for the Touchstone database schema. Your DBA will need the following information in order to configure the account:

  Touchstone requires that the user credentials use Windows Authentication for connecting to the Oracle Database. The user requires the following grant: GRANT CONNECT, RESOURCE TO <USER>.

  Note: The Touchstone installation queries the **session_privs** and **user_role_privs** tables to validate that all of these grants have been applied.

- You must install the Administrator version of the Oracle client on the Application tier.
- The Oracle client on the Web/Application servers must be 64-bit.

The Touchstone database is Unicode only and uses case-insensitive indexes.

Create a Windows Login for Oracle and Assign it Privileges

Step 1: Create the user (the account specified must all be in UPPERCASE and the NETBIOS domain name must not contain a period)

CREATE USER “OPS$<DOMAIN_NAME>\<USER_NAME>" IDENTIFIED EXTERNALLY;

Step 2: Give the user access to the Oracle database (the account specified all be in UPPERCASE)

GRANT CONNECT TO “OPS$<DOMAIN_NAME>\<USER_NAME>”;

Step 3: Grant the user access to the tables:

GRANT “DBA” TO “OPS$VCAC\DELTEKSERVICEACCOUNT”;

Note: When you run the PowerShell script installer, the Deltek Touchstone Service Account is created. For more information, see Appendix E: PowerShell Script and Console.

Deltek

Add Oracle Policy Files to the Global Assembly Cache (GAC)

Running the Touchstone Web/Application server and connecting to an Oracle database requires the installation of the 64-bit Oracle clients (using the "Administrator" Installation Type) on the Web/Application server.

The Oracle client installation does not register the .NET assembly files into the Global Assembly Cache (GAC) that Touchstone needs to connect to the Oracle database. After installing the Oracle Client, you must run the commands below to register the DLLs.

> **Note:** You must register the Oracle .NET Assemblies every time you install, add, or modify an Oracle client or after applying an Oracle client patch. You must run these steps to register both new and existing clients.
>
> **Example 1:** If you have already the 32-bit client installed and you add the 64-bit client, after the installation, you must register both the 32-bit and 64-bit clients.
>
> **Example 2**: You have an Oracle 64-bit client installed and are using Touchstone. You install a new Oracle client version (32-bit or 64-bit). If you are going to use the old and new Oracle client versions, after you install the new version, you must register both versions. If you are only going to use the new Oracle version, after the installation, you must register the new version.

Register the Oracle .NET Assemblies (12c R2 and Higher Versions)

These steps must be performed on your Web/Application server.

1. Click **Start » All Programs » Accessories**.
2. Right-click the Command Prompt and select **Run as administrator**.
3. On the Administrator Command Prompt window, enter or paste the following lines:

   Echo Register the ODP.NET 4 Managed assembly into the GAC

   "<Oracle_client_home_path>\ODP.NET\managed\x64\OraProvCfg.exe" /action:gac /providerpath:"<Oracle_client_home_path>\ODP.NET\managed\common\Oracle.ManagedDataAccess.dll"

   Echo Register the ODP.NET 4 Managed Publisher Policy assembly into the GAC

   "<Oracle_client_home_path>\ODP.NET\managed\x64\OraProvCfg.exe" /action:gac /providerpath:"<Oracle_client_home_path>\ODP.NET\managed\PublisherPolicy\4\Policy.4.121.Oracle.ManagedDataAccess.dll"

   "<Oracle_client_home_path>\ODP.NET\managed\x64\OraProvCfg.exe" /action:gac /providerpath:"<Oracle_client_home_path>\ODP.NET\managed\PublisherPolicy\4\Policy.4.122.Oracle.ManagedDataAccess.dll"

   Echo Configure the Machine.config for .NET 4 Framework with proper section Handler

   "<Oracle_client_home_path>\ODP.NET\managed\x64\OraProvCfg.exe" /action:config /product:odpm /frameworkversion:v4.0.30319 /providerpath:"<Oracle_client_home_path>\ODP.NET\managed\common\Oracle.ManagedDataAccess.dll" /set:settings\TNS_ADMIN:"<Oracle_client_home_path>\network\admin"

4. Close the Administrator Command Prompt window.

> **Note:** Oracle client home path refers to the location where the Oracle client binaries are stored. For example, C:\app\oracle\product\12.2.0\client_1.

You may encounter one or more of these errors if the Oracle file registration steps are not performed:

Error	Description
"Invalid Identifier" error encountered when using Oracle 12c R2 or Oracle 18c client	This happens with the 64-bit version of the Oracle client. The Oracle client installation failed to add the Oracle.DataAccess assemblies (dll and Policy files) to the Global Assembly Cache (GAC).
Unable to find the requested .NET Framework Data Provider. It may not be installed.	This happens with the 64-bit version of the Oracle client. The Oracle client installation failed to add the Oracle.DataAccess assemblies (dll and Policy files) to the Global Assembly Cache (GAC).
Unable to load dll 'OraOps12.dll': This specified module cannot be found (Oracle.DataAccess.Client.OpsInit)	The Oracle client installation failed to add the Oracle.DataAccess assemblies (dll and Policy files) to the Global Assembly Cache (GAC).
Unable to load dll 'OraOps18.dll': This specified module cannot be found (Oracle.DataAccess.Client.OpsInit)	The Oracle client installation failed to add the Oracle.DataAccess assemblies (dll and Policy files) to the machine.config.

Deltek

Appendix C: Touchstone Application Configuration Settings

Touchstone application configuration settings are stored in the PPM API configuration file named config.dat in the location <drive>\Program Files\Deltek\Acumen Touchstone\web\PPMAPI\config.

Session Timeout Value

By default, Touchstone implements a session timeout that will log a user out of the system after 30 minutes of inactivity. You can change the default timeout value in PPM Administrator. When you go to **System » Polling**, enter your new timeout value in the **Max Time of Inactivity** field.

Submittal Processing Timeout Value

If a submittal takes too long to process, the Status changes to **Failed** and you have to submit the schedule again. The default timeout value is 30 minutes.

You can configure the timeout period in the [PPM.WebService] section of the config.dat file:

[PPM.WebService]

SubmittalProcessingTimeout=30

Benchmark Report Generation Timeout Value

If you are generating a benchmark report, the Status changes to **Failed** when the process takes too long. Touchstone has a default timeout value of 60 minutes for the report generation process.

You can configure the timeout period in the [PPM.WebService] section of the config.dat file:

[PPM.WebService]

ReportGenerationTimeout=60

Project File Submittal Number of Threads

This setting allows multiple users to upload schedule files simultaneously and optimizes the file submission process to run asynchronously.

Touchstone allows each message queue handler to get the thread count from the [PPM.Webservice.MQ] section in config.dat. There are eight message queue handlers in Touchstone, in the File Submittal process:

[PPM.WebService.MQ]

SnapshotQueueRequestThreads=<count>

SnapshotQueueResponseThreads=<count>

- The number of threads allocated for running the scoring analysis

PersistJsonObjectRequestThreads=<count>

PersistJsonObjectResponseThreads=<count>

- The number of threads allocated for storing the metadata of the submitted file

GenerateExcelScoreReportRequestThreads=<count>

GenerateExcelScoreReportResponseThreads=<count>

- The number of threads allocated for generating the excel score report

SendEmailNotificationRequestThreads=<count>

SendEmailNotificationResponseThreads=<count>

- The number of threads allocated for sending the email to the SMTP server

The count range of values goes from [1] to [2 x processor count]. If the count is not set in the config.dat file, the default value of the count is 1. If the count is set in the config.dat file, then the value in the config.dat file is used, not exceeding twice the processor count. If the current machine contains multiple processor groups, this equates to the number of logical processors that are available for use by the common language runtime (CLR).

Attention: For more information, see https://docs.microsoft.com/en-us/dotnet/api/system.environment.processorcount?view=netframework-4.8.

Benchmark Report Generation Number of Threads

This setting allows multiple users to generate reports simultaneously and optimizes the report generation process to run asynchronously.

Touchstone allows each message queue handler to get the thread count from the [PPM.Webservice.MQ] section in config.dat. There are two message queue handlers in Touchstone, in the Report Generation process:

[PPM.WebService.MQ]

ReportProjectSummaryDataRequestThreads=<count>

ReportProjectSummaryDataResponseThreads=<count>

The number of threads are allocated for generating the benchmark report data. These threads are displayed on your browser.

- The count range of values goes from [1] to [2 x processor count].
- If the count is not set in the config.dat file, the default value of the count is 1.
- If the count is set in the config.dat file, then the value in the config.dat file is used, not exceeding twice the processor count. If the current machine contains multiple processor groups, this equates to the number of logical processors that are available for use by the common language runtime (CLR).

Attention: For more information, see https://docs.microsoft.com/en-us/dotnet/api/system.environment.processorcount?view=netframework-4.8.

Enable/Disable Windows Authentication

Use this setting to enable or disable windows authentication support in the Touchstone application.

[PPM.WebService]

WindowsAuthentication=1

1 = Enabled; 0 = Disabled

In addition to this setting, you must run the **.\DeltekAcumenTouchstone.ps1** script with the **-AdvancedSetupOption ConfigureWindowsAuthentication** switch. You must also configure specific data sources to enable Windows Authentication.

Attention: For more information and steps to configure windows authentication, see Configure Touchstone for Windows Integrated Authentication.

Using Redis for Session State and Queueing

Note: When you enable Redis, issues can occur when you run the benchmark report generation process. Disable Redis by removing the config.dat settings mentioned below.

Touchstone supports the use of Redis for shared caching of Touchstone user session state, for queueing of project submittals, for scoring for fault tolerance, and for load balanced environments.

If you choose not to use Redis for caching Touchstone user session state in a load balanced environment, the load balancer must be configured with client affinity to ensure that users are routed to the same server that they initially are connected to when they log into the application.

For more information about Redis, see the following article: https://redis.io/topics/introduction.

Configuring Touchstone to Use Redis

By default, the PPM API is configured to store session state in memory, and all background MQ processes are executed as background threads in process. You can configure both session state and MQ independently via PPM API's config.dat file. No further configuration is required after installing Redis and configuring PPM API's config.dat.

Session State

To enable the use of Redis for user session state, add the following to the config.dat file to specify the IP address and port of the Redis server:

[PPM.WebService.Session]

RedisHost=[IP address:port]

Handling the Publish/Subscribe Process

You can enable the use of Redis in handling the publish/subscribe process related to Server Sent Events in ServiceStack. Add the following to the config.dat file:

[PPM.WebService.SSE]

RedisHost=127.0.0.1:6379

In addition, you can include session information in the HTTP headers on the Server Sent Events (SSE) channel using the following:

AllowSessionIdsInHttpParams=true

Queuing of Project Submittals

To enable the use of Redis for queuing of project submittals, add the following to the config.dat file to specify the IP address and port of the Redis server:

[PPM.WebService.MQ]

RedisHost=[IP address:port]

The RedisHost key allows you to point to an IP address/port combo of a running Redis server.

Configuring the RedisHost With a Password

In some cases, the RedisHost IP address will require a password. Regardless of the platform you use for Redis, you can configure the provided password. For example:

Redis IP Address: AcumenTSBeta.resid.cache.windows.net

Redis Port: 6379

Redis Password: G5PiV7BgGRtaUehUge4PX9UZyaIN3JaahAzCaBZoPQk=

The value for the RedisHost key will look like the following:

[PPM.WebService.MQ]

RedisHost=G5PiV7BgGRtaUehUge4PX9UZyaIN3JaahAzCaBZoPQk=@AcumenTSBeta.redis.cache.windows.net:6379

Note: In case a password is unnecessary, simply omit the part before the @ symbol as well as the symbol itself. For example:

[PPM.WebService.WQ]

RedisHost=AcumenTSBeta.redis.cache.windows.net:6379

Deltek

Appendix D: Touchstone Website Configuration Settings

Maximum Web Request Length and Timeout

You can configure the maximum length and timeout for web requests that are accepted and processed by Touchstone.

Touchstone supports separate values for metric file upload requests, project submittal upload requests, and all other application requests. If a request size is too large or takes too long to process, Touchstone displays an error message.

The default values for maximum request length and timeouts are as follows:

- **General:** 20KB or 300 seconds
- **Metric file upload:** 10MB or 300 seconds
- **Project submittal upload:** 750MB or 300 seconds

In addition, Touchstone has maximum request length and timeouts for email attachments and templates. These default values are as follows:

- **Email attachments upload:** 10MB or 300 seconds
- **Email footer templates upload:** 10MB or 300 seconds

There are two web.config files on the Touchstone Server and the timeout values must be the same in both. The files are located in the following folders:

- The **PPM API web.config** file is in the <drive>\Program Files\Deltek\Acumen Touchstone\Web\PPMAPI\config folder.
- The **Touchstone web.config** file is in the <install drive>\Program Files\Deltek\Acumen Touchstone\Web\App folder.

General

To set the maximum request length, change the value of the **maxRequestLength** option in the **<httpRuntime>** element in the **<system.web>** section of both web.config files.

To set the timeout, change the value of the **executionTimeout** option in the **<httpRuntime>** element in the **<system.web>** section of both web.config files.

The example below shows a maximum request length of 20kb and a timeout value of 300 seconds:

```
<configuration>
  <system.web>
   <httpRuntime targetFramework="4.8" maxRequestLength="20"
executionTimeout=”300”/>
  </system.web>
</configuration>
```

Deltek

Metric File Upload

To set the maximum request length for a metric file upload, change the value of the **maxRequestLength option in the <httpRuntime>** element in the **<system.web>** section of the <location path="benchmark/metricfileuploads"> section in both web.config files.

To set the timeout for a metric file upload, change the value of the **executionTimeout** option in the **<httpRuntime>** element in the **<system.web>** section of the <location path="benchmark/metricfileuploads"> section in both web.config files.

If you change the **maxRequestLength** option, you must also change the value of the **MaxMetricFileSize** option in the **<appSettings>** section to match the **maxRequestLength** value.

The example below shows a maximum request length of 10MB and a timeout value of 300 seconds:

```
<configuration>
  ...  <location path="benchmark/metricfileuploads">
    <system.web>
      <httpRuntime maxRequestLength="10240" executionTimeout="300" />
    </system.web>
  </location>
  ...

  ...
  <appSettings>
    <add key="MaxMetricFileSize" value="10240"/>
  </appsettings>
  ...
</configuration>
```

Project Submittal Upload

To set the maximum request length for the project submittal upload, change the value of the **maxRequestLength** option in the **<httpRuntime>** element in the **<system.web>** section of the <location path="benchmark/ projects/snapshotfileupload "> section in both Web.config files.

To set the timeout for the project submittal upload, change the value of the **executionTimeout** option in the **<httpRuntime>** element in the **<system.web>** section of the <location path="benchmark/ projects/snapshotfileupload "> section in both web.config files.

If you change the **maxRequestLength** option, you must also change the value of the **MaxSubmittalFileSize** option in the **<appSettings>** section to match the **maxRequestLength** value.

The example below shows a maximum request length of 750MB and a timeout value of 300 seconds:

```
<configuration>
...  <location path="benchmark/projects/snapshotfileupload">
    <system.web>
      <httpRuntime maxRequestLength="768000" executionTimeout="300" />
    </system.web>
  </location>
...

  ...
```

```
  <appSettings>
    <add key=" MaxSubmittalFileSize" value="768000"/>
  </appsettings>
  ...
</configuration>
```

Deltek

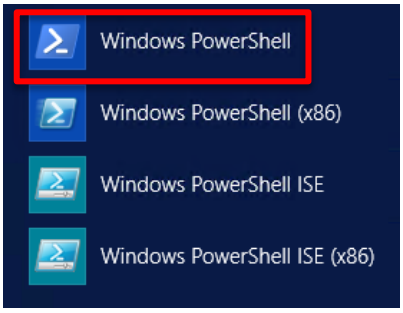
Appendix E: PowerShell Script and Console

The Touchstone installation is built using PowerShell scripts. PowerShell is a command-line shell and scripting language, designed specifically for system administrators and power users. PowerShell leverages new technologies, provides enhanced automation, and provides complete visibility and transparency into what is being deployed, run, and executed, including all changes that the installation makes to your servers.

> **Attention:** For more information on PowerShell and its capabilities, see: https://learn.microsoft.com/en-us/training/modules/script-with-powershell/.

PowerShell Console

The **DeltekAcumenTouchstone.ps1** installation script runs from the PowerShell Console window. Launch the PowerShell console from the operating system **Start** menu:



> **Warning:** Do NOT attempt to run the **DeltekAcumenTouchstone.ps1** installation script using the Windows PowerShell ISE.

Entering Commands

- As you respond to prompts, you may see default values in brackets. If the default value is correct, press ENTER to accept the default.
- PowerShell remembers a list of the most recent commands entered. Even if you close the console and re-open it, you can use the up and down arrows to navigate through previously entered commands. This functionality is enabled by default in Windows Server 2016 but may require you to install the PSReadLine module to function properly in Windows Server 2012 R2.

  > **Attention:** For more information about PSReadLine, see this article: https://github.com/lzybkr/PSReadLine.

- You must run all scripts with the period and backslash characters before the script name (for example, **.\DeltekAcumenTouchstone.ps1**).
- You can begin entering the name of a file and then press TAB to auto-complete the entry. For example, to enter the filename **DeltekAcumenTouchstone.ps1**, enter **Del** and press TAB. If

multiple options exist, tab through them until you find the correct one. The auto-completion places the characters **.** in front of the filename (for example, **.\DeltekAcumenTouchstone.ps1**).

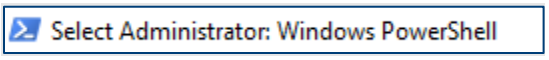
Performance

- If scripts or executables are running very slowly on Windows Server 2016, try running the following command to temporarily disable Windows Defender real-time monitoring:

  Set-MpPreference -DisableRealTimeMonitoring $true

  To re-enable real-time monitoring, run the same command but use **$false** instead of **$true**.

- If the console appears to be hung, check to see if the word **Select** is displayed in the console window:

  If it is, click the top bar of the console and press ENTER.

Install SqlServer PowerShell Module

You need to install the SqlServer PowerShell module if you do not have it already installed. This module is necessary in running the Touchstone installation script. The SqlServer PowerShell module includes cmdlets that support the latest SQL features.

To check if the module is installed, run the following command in a PowerShell session as an administrator:

Get-Module -ListAvailable -Name SqlServer

If this command does not return anything, it means the module is not installed.

To install the SqlServer module:

1. Go to the PowerShell Gallery.
2. Start a PowerShell session.
3. Run **Install-Module SQLServer**.

Installing the SqlServer Module for All Users

To install the SqlServer module for all users, run the following command in a PowerShell session as an administrator:

Install-Module -Name SqlServer

Installing the SqlServer Module to a Machine with No Internet Access

To install the SqlServer Module to a machine with no internet access:

1. Using a machine that does have internet access, download the SQLServer PowerShell module. This step saves the files in the sample **$env:TEMP\SQLServer\<SomeVersion>** folder which is defined in the **-Path** parameter.

2. Copy the **$env:TEMP\SQLServer\<SomeVersion>** folder to the **%ProgramFiles%\WindowsPowerShell\Modules\SqlServer** folder in the machine with no internet access.
3. Run **Get-Module SqlServer -ListAvailable** to confirm the SqlServer Powershell module is available on the machine with no internet access.

Digital Signature

The Touchstone PowerShell installation script is digitally signed by Deltek and will not execute if modified in any way.

Firewall Rules for PowerShell Remoting

The Touchstone installation process uses PowerShell remoting several times to:

- Create local accounts on remote servers (if a local account is selected as the service account).
- Obtain remote server information needed for setup.

Remoting is enabled by default and uses the Windows Remote Management framework service, which listens on port 5985. Oracle, by default, listens for database connections on port 1521; therefore, Touchstone requires that you open port 1521.

> **Attention:** Read this article to learn how to enable PowerShell remoting: https://docs.microsoft.com/en-us/powershell/module/microsoft.powershell.core/enable-psremoting?view=powershell-5.1
>
> If you are using dynamic ports for your SQL Server, read this article to learn about correct firewall configuration: https://docs.microsoft.com/en-us/sql/database-engine/configure-windows/configure-a-windows-firewall-for-database-engine-access.

PowerShell Execution Policy

The default execution policy (get-executionpolicy) for the Touchstone-supported operating systems is RemoteSigned. Your organization may require a tighter policy (for example, Restricted), in which case you may see an error message when you try to run the script.

Run the following command from the PowerShell console to temporarily change the execution policy to RemoteSigned:

Set-ExecutionPolicy -Scope Process -ExecutionPolicy RemoteSigned

This command changes the policy for this console session only, meaning that if you close the console and re-open it, you will need to run the **Set-ExecutionPolicy** command again.

DeltekAcumenTouchstone.ps1 PowerShell Script

The first time you install Touchstone, you have to download the **DeltekAcumenTouchstone.ps1** PowerShell script from Deltek Software Manager (DSM). When you run the script again, it automatically pulls any needed updates from DSM without you logging into DSM and downloading a new file.

When you run the **DeltekAcumenTouchstone.ps1** script, it does the following:

1. Verifies that you own the product
2. Downloads and extracts the latest build from DSM
    a. Downloads AcumenTouchstone.exe and extracts it to the installation directory
3. Creates a DeltekTouchstone account
4. Creates the IIS application pools and virtual directories for AcumenTouchstone, AcumenTouchstone\app, and PPM.API
5. Lays down the database scripts
6. Enables Windows Authentication

    Attention: For more information on this authentication and its command line argument, see Configure Touchstone for Windows Integrated Authentication in this document.

7. Configures the PPMAPI web.config file
8. Creates three scheduled tasks

Attention: If you want to generate all of the actions listed above, you will have to manually trigger them using specific switches.

The script does not:

- Create the database
- Run database scripts
- Configure datasources.dat

Generate JSON Metadata for Project Snapshots Submitted Before Touchstone 8.10

If you submitted project snapshots before the release of Touchstone version 8.10, you must run a batch process to update those snapshots to ensure accurate benchmark reporting. This process adds the necessary data required to support benchmark functionality. If your snapshots were submitted prior to version 8.10, it is essential that you run the provided script to enable benchmark reporting.

To generate JSON metadata for project snapshots submitted before Touchstone 8.10:

1. Navigate to C:\Program Files\Deltek\Acumen Touchstone\Support\.
2. Find the **TouchstoneSnapshotPersistJsonDataProcess.ps1** script.
3. Before running the script, open it in a text editor and update the following values:
    a. Update LogFilePath
        i. **Original value:** $global:LogFilePath = "LOGPATH\TouchstoneSnapshotPersistJsonDataProcess.txt"
        ii. **Updated value (sample):** $global:LogFilePath = "C:\Program Files\Deltek\Acumen Touchstone\Support\TouchstoneSnapshotPersistJsonDataProcess.txt"

b. Update TASKURL

i. **Original value:** "TASKURL/ppmapi/benchmark/generate-json-metadata"

ii. **Updated value (sample):** "https://acumentouchstone.deltek.com/acumentouchstone/ppmapi/benchmark/generate-json-metadata"

4. Run the script.

Update Email Settings to Migrate to PPM Administrator

Touchstone is migrating its email settings to PPM Administrator. If you are upgrading from Touchstone version 8.10, you must run the PowerShell script to update your email settings to be compatible with the migration changes.

To update email settings to migrate to PPM Administrator:

1. Navigate to C: \Program Files\Deltek\Acumen Touchstone\Support\.
2. Find the **MigrateEmailSettings.ps1** script.
3. Before running the script, open it in a text editor and update the following values:

a. Update TASKURL

i. **Original value:** TASKURL/PPMAPI/benchmark/email-settings-migration

ii. **Updated value (sample):** https://localhost/AcumenTouchstone/PPMAPI/benchmark/email-settings-migration

4. Run the script.

Deltek

Appendix F: Installation .XML Files

DeltekAcumenTouchstoneConfiguration.xml

The installation script creates the **DeltekAcumenToucstoneConfiguration.xml** file during the Touchstone installation. It contains metadata and default information for all Deltek Acumen Touchstone versions. It is maintained by Deltek and updated and deployed with each release. An updated file is downloaded each time you run the **DeltekAcumenTouchstone.ps1** script. The file is located in <install drive>\Program Files\Deltek\Acumen Touchstone.

It includes the following information:

- The DSM Release ID
- The License Agreement URL
- The product version (for example, 8.2.0.824)
- The File name (for example, DeltekAcumenTouchstone810824.exe)
- Compatibility information
- Server information for upgrades
- Identities used (usernames only)

The file is stored in the root of the installation directory.

Warning: Do not delete this file. You will need it for future upgrades.

DeltekAcumenTouchstoneSettings.xml

The file is located in <install drive>\Program Files\Deltek\Acumen Touchstone and includes:

- Configuration information
- Usernames
- Installation directory
- Installed version
- Mode
- Branch
- Debug
- Hosted
- Web URL

Deltek

Appendix G: PPM Encryption Conversion Utility

Overview

The PPM Encryption Conversion Utility is designed to scan a computer for all copies of installed PPM products and validate if the PPM products have been upgraded to compatible versions that support the new protocols. It also validates any configuration files (such as the datasources.dat file) and databases that are shared by the PPM products are eligible to be upgraded to support the new protocols.

These validations are designed to ensure that the upgrade is only performed when all installed PPM products are compatible with the new protocols, which guarantees that environments with a mix of new PPM products and older PPM products will continue to function properly until all installed versions of PPM products are compatible with the new protocols.

If configuration files and databases that are shared by PPM products are eligible to be upgraded, the PPM Encryption Conversion Utility performs the necessary upgrades to the configuration files and databases to enable the use of the new protocols.

Note: The PPM Encryption Conversion Utility must be run on all computers that have PPM product configuration files on them to upgrade the configuration files to support the new protocols. For Acumen Touchstone, this is the file datasources.dat.

Attention: Each PPM product is shipped with this tool (**PPMEncryptionConverter.exe**) and its location may vary per product. For more information, see the Run the PPM Encryption Conversion Utility section in this document.

Upgrading from Older Versions

When you upgrade from older versions of PPM Products to new versions, PPM Products will continue to use the previous protocols by default to ensure compatibility with older versions of PPM Products. Therefore, a separate conversion process is required to upgrade existing PPM Product configuration files and data sources to enable the use of the new protocols.

To support the conversion process, PPM products include a new PPM Encryption Conversion Utility application that is designed to perform the upgrade of existing PPM Product configuration files and data sources to enable the use of the new protocols.

Note: Deltek strongly recommends that you run the new PPM Encryption Conversion Utility application to upgrade existing PPM product configuration files and data sources to enable the use of the new protocols.

Note: New installations of PPM products and data sources are pre-configured to use the new protocols by default. New installations do not need to run the PPM Encryption Conversion Utility.

Upgrading from Touchstone 8.1 to 8.2 and 8.10

If you currently use Touchstone 8.1 to 8.2 or 8.10, you will need to complete the following steps to upgrade smoothly to Touchstone 8.11.3.

To upgrade to Touchstone 8.11.3:

1. Navigate to the following folders:
   - C:\Program Files\Deltek\Acumen Touchstone\Databases\Scripts\Oracle
   - C:\Program Files\Deltek\Acumen Touchstone\Databases\Scripts\SQLServer
2. Run the 8.11.3 Database Upgrade scripts.

   Update your database schema to the latest version to support new features and protocol changes.
3. Run the **MigrateEmailSettings.ps1** PowerShell script.

   This script migrates the legacy EMAILSETTINGS configuration into individual fields to support PPM Administrator. In addition to related email configuration parameters, the fields include:
   - EMAIL_HOST
   - EMAIL_DEFAULT_SENDER
   - EMAIL_AUTH_USERNAME
   - EMAIL_AUTH_PASSWORD
   - EMAIL_PORT
   - EMAIL_USE_TLS
4. Run the PPM Encryption Conversion Utility.

   Use this utility to convert existing configuration files and data sources to enable the new encryption and password hashing protocols.

Run the PPM Encryption Conversion Utility

You need to run this tool under the following conditions:

- You have an environment with existing PPM products.
- All PPM products have been upgraded to a version that supports the new hashing and encryption protocols.

To run the conversion utility tool:

1. Navigate to the location of the PPM Encryption Conversion Utility.

   Note: The location may vary for each PPM product. See the *Deltek PPM Encryption Conversion Utility Conversion Guide*.
2. Double-click **PPMEncryptionConverter.exe** or click the corresponding shortcut from the **Start** menu.

It automatically detects all installed PPM products in your machine and determines whether the installed products are compatible (meet minimum supported version) to determine if their files and databases are eligible for upgrade.

> **Note:** Upon launching the conversion utility, it creates the PPM Encryption Converter folder for the backup files in the C:\Users\<User Name>\Documents\Deltek\PPM Encryption Converter\. This folder contains <Backup> folders using the **yyyymmdd_hhmmss** name format, which refers to the date and time when the conversion utility is launched (for example, 20221116_194029). Each <Backup> folder contains the Backup subfolder and the PPMEncryptionConverter.log (which is created after the conversion process).

3. On the first screen of the PPM Encryption Conversion Utility dialog box, click **Next**.

> **Note:** This screen contains the **Products** grid, which displays all installed PPM products in your machine. The grid is read-only.
>
> - The corresponding version and compatibility status of each installed product also display. Products with the **Compatible** column set to **Yes** indicate that they meet the minimum compatible version.
> - When you hover your mouse cursor over a product in the list, it displays the installation location of the product.

4. On the second screen, select the database configuration files and data sources you need to upgrade.

   Selecting a configuration file in the **Files** grid displays all the databases in the **Datasources** grid and checks whether they can be converted. Alternatively, you can click the **Check all datasources** button to verify the status of all data sources in all of the files instead of selecting the files one by one.

> **Note:** You cannot select and upgrade the configuration files and data sources of those PPM products that do not meet the minimum compatible version.

> **Attention:** Different icons display beside the available files and data sources to indicate their conversion status. For more information, see the "Conversion Status Icons" section of the *Deltek PPM Encryption Conversion Utility Conversion Guide*.

   If you need to add more encrypted files to convert, click **Add**.

> **Attention:** PPM products have different locations (or containers) where encrypted and hashed data is stored. For more information, see the Updated Files and Data section in this document.

5. Click **Process**.

Deltek

Note: During the conversion process, the PPM Encryption Conversion Utility creates a copy of the database configuration files in the Backup folder. The backup name has the **<n>.<filename>** format, where **<n>** represents a number starting from 1 to make the backup fiels unique (such as, 1.datasources.dat, 2.ideablade.ibconfig, and 3.databases.enc).

It also creates a file named FileMapping.txt, which contains the mappings of both the backup and original files. The mapping follows the **<backup file> (<original file>)** format. For example, 1.datasources.dat (C:\Program Files (x86)\Deltek\Acumen Touchstone\datasources.dat).

After the conversion process, the WST_UPD (for all products) and WST_UPF (for Acumen Touchstone) tables are updated.

Updated Files and Data

PPM products use different files to store encrypted and hashed data. For Acumen Touchstone, the updated files are Datasources.dat and Databases.

Attention: For more information, see the *Updated Files and Data* section of the Deltek PPM Encryption Conversion Utility Conversion Guide.

Change Passwords

After a PPM data source has been upgraded by the PPM Encryption Conversion Utility, you are prompted to update your password the very first time you log on to the converted data source using a PPM product. This is a necessary step to update the stored password to use the new password protocol for storing your passwords.

New passwords are case sensitive, so you must remember the case they were entered in.

Note: You are permitted to enter your existing password again, if desired. It is not necessary to create an entirely new password.

Note: You must complete the Change Password step to use the PPM product with the converted data source. If you choose to cancel the Change Password step, you will return to the Login dialog box.

Note: In EPM SA, there is an option to generate a temporary password. When you click **Send Email**, EPM SA sends you an email that contains a new temporary password that uses the new password protocol. This temporary password allows you to log on to Acumen Touchstone, where a dialog box displays where you can change your temporary password.

Deltek

Appendix H: If You Need Assistance

If you need assistance installing, implementing, or using Touchstone, Deltek makes a wealth of information and expertise readily available to you.

Customer Services

Deltek has always maintained close relationships with client firms, helping with their problems, listening to their needs, and getting to know their individual business environments. A full range of customer services has grown out of this close contact, including the following:

- Extensive self-support options through the Deltek Support Center
- Phone and email support from Deltek Support Services analysts
- Technical services
- Consulting services
- Custom programming
- Classroom, on-site, and Web-based training

Attention: Find out more about these and other services from the Deltek Support Center.

Deltek Support Center

The Deltek Support Center is a support Web site for Deltek customers who purchase an Ongoing Support Plan (OSP).

The following are some of the many options that the Deltek Support Center provides:

- Search for product documentation, such as release notes, install guides, technical information, online help topics, and white papers
- Ask questions, exchange ideas, and share knowledge with other Deltek customers through the Deltek Support Center Community
- Access Cloud-specific documents and forums
- Download the latest versions of your Deltek products
- Search Deltek's knowledge base
- Submit a support case and check on its progress
- Transfer requested files to a Deltek Support Services analyst
- Subscribe to Deltek communications about your products and services
- Receive alerts of new Deltek releases and hot fixes
- Initiate a Chat to submit a question to a Deltek Support Services analyst online

Attention: For more information regarding Deltek Support Center, refer to the online help available from the Web site.

Deltek

Access Deltek Support Center

To access the Deltek Support Center:

1. Go to https://deltek.custhelp.com.
2. Enter your Deltek Support Center **Username** and **Password**.
3. Click **Login**.

> **Note:** If you forget your username or password, you can click the **Need Help?** button on the login screen for help.

Microsoft Internet Information Server (IIS) Installation on Windows Server

A prerequisite for installing Touchstone is that Microsoft Information Server (IIS) must be installed on the Web/Application server. The setup script checks that all required IIS features are installed on the server. If not, the script prompts you to install them.

Required IIS Features

The following features are prerequisites for Touchstone installation. Enable them on the Select Role Services screen.

Area	Feature
Common HTTP Features	▪ Default Document ▪ Directory Browsing ▪ HTTP Errors ▪ Static Content ▪ HTTP Redirection
Health and Diagnostics	▪ HTTP Logging ▪ Request Monitor (recommended) ▪ Tracing (recommended)
Performance	▪ Static Content Compression
Security	▪ Windows Authentication (only necessary if you will be using it) ▪ Request Filtering
Application Development	▪ .NET Extensibility 4.6 ▪ ASP.NET 4.6 (Add Roles and Features Wizard dialog box displays when you select this option. Click **Add Features** button.) ▪ ISAPI Extensions ▪ ISAPI Filters
Management Tools	▪ IIS Management Console ▪ IIS Management Scripts and Tools

Deltek

Install IIS Features Using PowerShell (Admin)

Use the steps below to install the IIS prerequisites for Touchstone.

To install IIS features:

1. Open Windows PowerShell (Admin).
2. Run the following command to install features:

   Install-WindowsFeature -Name Web-Server,Web-Http-Redirect,Web-Request-Monitor,Web-Http-Tracing,Web-Windows-Auth,Web-Net-Ext45,Web-Asp-Net45,Web-ISAPI-Ext,Web-ISAPI-Filter,Web-Scripting-Tools -IncludeManagementTools
3. Run the following command to verify installed features:

   get-WindowsFeature -name Web-*

Configure the Idle Time-out Field

To configure the Idle Time-out (minutes) field in the Application Pool Setting:

1. Click **Administrative Tools » Internet Information Services » Application Pools** and change the application pool identity.
2. Right-click **DeltekTouchstoneAppPool**, and click **Advanced Settings**.
3. In the **Process Model » Idle Time-out (minutes)** field, enter 0.
4. Click **OK**.

> **Note:** If the **Idle Time-out (minutes)** field is set to 0 in IIS, the session timeout in the coding.dat file in the PPM API dictates the duration of inactivity before the session expires. This is where you should adjust the **Idle Time-out (minutes)** field.
>
> If the **Idle Time-out (minutes)** field is set to > 0, the duration of inactivity before the session expires is dictated by the smaller of the two values between the IIS setting and the config.dat setting.

Deltek

Configure Secure Sockets Layer (SSL)

You must have properly configured SSL certificates installed and the necessary bindings created on all web/application servers in your Touchstone configuration. You cannot run the setup script and the various switches without them.

Secure the Touchstone Web Server

To configure Touchstone for use with SSL, you must either:

- Obtain an SSL certificate from an online certificate authority such as Verisign, Thawte, or Comodo, *or*
- Have access to a domain or stand-alone certificate authority on your network.

Request a Server Certificate

To request the certificate:

1. Log on to the web server.
2. From Administrative Tools, open Internet Information Services Manager.
3. From the navigation pane, select your server navigation menu.
4. Double-click **Server Certificates** to display the Server Certificates window.
5. In the Actions pane, select one of the following options:
   - **Import**: If you already have a certificate for your server, select this action to import that certificate.
   - **Create Certificate Request**: Select this action to launch a wizard that guides you in creating a text file to submit to your Certificate Authority (CA) to obtain the actual SSL certificate for your web server.
   - **Complete Certificate Request**: If you used **Create Certificate Request** to request a certificate, select this action to complete your request and install your certificate.
   - **Create Domain Certificate**: If you have a Certificate Authority on your domain, select this action to request your certificate.
   - **Create Self-Signed Certificate**: Select this action to test SSL functionality or troubleshoot SSL certificate issues.

     After you obtain and import your SSL Certificate, you must create an SSL binding for your web server.
6. Expand **Sites**, and select your website.
7. In the Actions pane, click **Bindings**.
8. On the Site Bindings dialog box, click **Add**.
9. On the Add Site Binding dialog box, in the **Type** drop-down list, select **https**.

   The **Port** value automatically changes to **443**.

10. From the **IP address** drop-down list, select your IP address or use the default setting **All Unassigned**.
11. From the **SSL Certificate** drop-down list, select your certificate.
12. Click **OK**.

Test the SSL Certificate and Binding

To test your new SSL certificate and binding, access your website using **https://** as the URL prefix and make sure that everything is working correctly.

Deltek

Configure Integrated Security for Touchstone

You can use Windows Integrated Authentication with Touchstone, which allows users to log in one time for both Windows and Touchstone.

To do this, you configure Windows Integrated Security for each user's Touchstone account using the Windows Domain network login as the username for that user. This allows the user to be automatically logged in to Touchstone as long as they are logged in to the domain. If the user is not properly logged in to the domain, the user is prompted for network credentials to log in to Touchstone. For example, non-domain workstation users, as well as users connecting to the network via an internet connection, receive a domain authentication challenge before they are logged in to Touchstone.

The use of Integrated Security in IIS **requires** a CAL (Client Access License) for each user who will access the web server. This is a Microsoft, not Deltek, licensing requirement.

Required Configuration Changes

To configure Windows Integrated Authentication, you must make several changes at the domain level and in IIS, in addition to configuring your domain user accounts in Touchstone:

- You must configure a domain user account as the IIS Application Pool identity for the DeltekTouchstoneAppPool in IIS. The domain account does not require domain administrative rights. Optionally, the Touchstone installation creates a local Windows account, DeltekTouchstone, to serve this function. However, a domain account is required to support trusted domains as well as the default IIS Windows Integrated Security configuration of using Kernel Mode Authentication.
- The domain account used for the Application Pool Identity needs the following rights on the Touchstone web/application server:
  - The account must be a member of the following local groups:
    - Administrators group
    - IIS_IUSRS group
  - The account requires the following local security policy rights:
    - Allow log on locally
    - Log on as a service
    - Log on as a batch job
- You must change the Touchstone IIS Application (virtual directory) from using Anonymous Access to using Windows Integrated Security.
- If you do not wish to use the default of Kernel Mode Authentication, you must create a Service Principal Name (SPN) for the domain user account that is the Application Pool Identity. You must have domain administrative rights to create the SPN.

  Attention: See Configure a Service Principal Name for more information.

Deltek

Configure the Application Pool Identity

To configure the Application Pool Identity to be a domain account:

1. Click **Server Manager » Configuration » Local Users and Groups » Groups** and add the domain user to the local Administrators and IIS_IUSRS group.
2. In Administrative tools, click **Security Settings » Local Policies » User Rights Assignment** to grant the domain user the necessary rights.
3. Click **Administrative Tools » Internet Information Services » Application Pools** and change the application pool identity.
4. Right-click **DeltekTouchstoneAppPool**, and click **Advanced Settings**.
5. In the **Process Model » Identity** field, click the ellipses (**...**).
6. On the Application Pool Identity dialog box, select **Custom Account**.
7. Click **Set**.
8. On the Set Credentials dialog box, in the **Username** field, enter the domain and user name in the following format: **Domain\Username**. Click **OK**.
9. Launch Touchstone on the web/application server to ensure that the application launches correctly.

   If not, review the application event logs to look for a problem.

Configure IIS to Use Windows Integrated Authentication

To configure IIS to use Windows Integrated Authentication:

1. From within Internet Information Services, expand the website where the Touchstone application is installed.
2. Select the Touchstone application.
3. Double-click the **Authentication** icon under IIS.
4. Select **Anonymous Authentication**, and click **Disable** on the Actions pane.
5. Select **Windows Authentication**, and click **Enable** on the Actions pane.
6. With Windows Authentication still selected, click **Advanced Settings**. Ensure that the **Enable Kernel-mode authentication** option is selected, and click **Cancel**.

   The default configuration is to have **Enable Kernel-mode authentication** selected. If you clear **Enable Kernel-mode authentication**, you must create a Service Principal Name. The default setting is acceptable for application authentication; however, if you wish to use Windows Integrated Authentication for your database connection, you must complete the Configure Windows Integrated Authentication for Internet Users (and Non-Domain Workstations) procedure.

7. Launch the Touchstone application.

Configure Touchstone for Windows Integrated Authentication

For security, Windows Authentication support for user logins in Touchstone is disabled by default. If you wish to use Windows Authentication with Touchstone on your Web Server, you must run the installation script with the **ConfigureWindowsAuthentication** switch to enable Windows Authentication support on the Touchstone Web/Application Server and then use the EPM Security Administrator to enable Windows Authentication for a data source.

To configure Touchstone for Windows Integrated Authentication:

1. From the installation directory Scripts folder, enter **.\DeltekAcumenTouchstone.ps1 -AdvancedSetupOption ConfigureWindowsAuthentication**.

   The switch enables the IIS Windows Authentication module (if it is not already enabled), configures Windows Authentication, and updates the necessary configuration files to enable Windows Authentication and perform the needed windows authentication configuration in EPM Security Administration.

2. Log into EPM Security Administration and configure specific data sources to enable Windows Authentication:

   a. Click **Tools » Change Data source**.

   b. On the Data Source dialog box, select the data source for which you want to enable Windows Authentication and click **OK**.

   c. Click **Products » Acumen Touchstone**.

   d. Click **Tools » Authentication Options**.

   e. In the Authentication Options dialog box **Authentication Mode** field, select **Mixed** or **Windows Authentication**.

   > **Note:** When you add Touchstone users in EPM SA, make sure that you specify the **Domain**. For steps to add the product license and users, see Step 6: Set Up EPM Security Administrator.

Configure Windows Integrated Authentication for Internet Users (and Non-Domain Workstations)

A different authentication process applies to domain users who are configured for Windows Integrated Authentication but are accessing the application from a non-domain workstation or via the internet.

To configure Integrated Authentication for internet users:

1. Launch the Touchstone application.

   The browser security prompt displays because the user is not authenticated to the domain and IIS is configured for Windows Integrated Authentication, meaning that only authenticated users can access without a challenge.

2. Select the **Remember my credentials** option if you want to save your credentials for both the browser and the WinForms application.

   In the future, you will not be prompted for credentials.

3. Enter the domain credentials, and click **OK**.
4. Enter values in the **Username**, **Password**, and **Domain** fields on the Windows Login Credentials dialog box.

   This step is necessary because the client side WinForms application is not able to use the previous credentials requested by and processed by the browser.

Configure a Service Principal Name

To disable Kernel Mode Authentication, you must create a Service Principal Name (SPN) for the domain user account that is the Application Pool Identity. The creation of the SPN requires domain administrative rights.

IIS Kernel Mode Authentication

When you use Windows Integrated Authentication, the default configuration of IIS is to use Kernel Mode Authentication. If you must disable Kernel Mode Authentication, follow the steps in this section to establish a Service Principal Name (SPN) for the Application Pool Identity. In a default configuration of IIS, Kernel Mode Authentication is enabled.

To see if Kernel Mode Authentication is enabled:

1. Using an Administrator account, log on to the Touchstone web/application server domain.
2. To open Internet Information Services, click **Start » All Programs » Administrative Tools » Internet Information Services (IIS) Manager**.
3. Expand the server name, expand **Sites**, and select **Default Web Site** (or the site where Touchstone is installed).
4. Select the Touchstone virtual directory, and double-click **Authentication** in the Features view.
5. Select **Windows Authentication** and verify that the status is **Enabled** (Anonymous Access should be **Disabled**). If it is not, select **Enable** from the **Actions** menu.
6. With **Windows Authentication** still selected, click **Advanced settings** on the **Action** menu.
7. On the Advanced Settings dialog box, if the **Kernel Mode Authentication** checkbox is selected, Kernel Mode Authentication is enabled.

Kernel Mode Authentication Implementation

The default configuration works for the Touchstone Windows Integrated Authentication application and database connections.

To disable Kernel Mode Authentication, clear the **Enable Kernel Mode Authentication** selection under the Advanced Settings of the Windows Authentication feature for the Touchstone virtual directory. Disabling Kernel Mode Authentication requires that a Service Principal Name be established for the Application Pool Identity.

Service Principal Names

Under the default configuration with Kernel Mode Authentication enabled, it is not necessary to create a Service Principal Name for the Application Pool Identity. The default SPNs created are sufficient.

If you do create an SPN for the Application Pool Identity, you will cause a duplicate SPN issue that prevents Windows Integrated Security from authenticating anyone to the web site.

When Kernel Mode Authentication is disabled, complete the following steps to create a Service Principal Name for the Application Pool Identity of the DeltekTouchstoneAppPool.

To create the Service Principal Name:

1. Log on to the server with domain administrative rights.
2. Run the following commands:
   - setspn –A http/<name of server> ApplicationPoolIdentity (Domain\Username)
   - setspn –A http/<fully qualified name of server> ApplicationPoolIdentity (Domain\Username)

   Or, if appropriate, use the DNS name of the server:
   - setspn –A http/<DNS name of server> ApplicationPoolIdentity (Domain\Username)

> **Attention:** See the following related Microsoft Knowledge Base article if you need additional details: You receive an "HTTP Error 401.1 - Unauthorized: Access is denied due to invalid credentials" error message when you try to access a Web site that is part of an IIS 6.0 application pool.

Configure Authentication Persistence

When you use Windows Integrated Authentication in IIS, every request made by the client is authenticated, by default, using one of two Windows Integrated Authentication providers: Negotiate or NTLM. This repeated authentication causes extra round trips between the client and server for each request and can impact performance, especially on latent connections.

However, if you use Authentication Persistence, the server authenticates only the initial request from the client and does not perform authentication on subsequent requests on the same connection, thus improving performance.

Source of Extra Round Trips

The default Windows Integrated Authentication provider is Negotiate, which causes the client and server to “negotiate” an authentication method that both can support.

- On a typical Active Directory network, the default authentication method is Kerberos.
- On non-domain, or more specifically, internet-based connections, the default authentication method is NTLM.

If you view the connections for a single user in IIS logs, you see something like this:

NTLM:

2016-01-05 16:24:51 10.5.12.16 POST /Touchstone/MethodCall.aspx - 81 - 10.5.4.5 - - 401 2 5 484

2016-01-05 16:24:51 10.5.12.16 POST /Touchstone/MethodCall.aspx - 81 - 10.5.4.5 - - 401 1 2148074254 15

2016-01-05 16:24:51 10.5.12.16 POST /Touchstone/MethodCall.aspx - 81 DOMAIN\user 10.5.4.5 - - 200 0 0 501

2016-01-05 16:24:51 10.5.12.16 POST /Touchstone/MethodCall.aspx - 81 - 10.5.4.5 - - 401 2 5 15

2016-01-05 16:24:51 10.5.12.16 POST /Touchstone/MethodCall.aspx - 81 - 10.5.4.5 - - 401 1 2148074254 0

2016-01-05 16:24:51 10.5.12.16 POST /Touchstone/MethodCall.aspx - 81 DOMAIN\user 10.5.4.5 - - 200 0 0 15

2016-01-05 16:24:51 10.5.12.16 POST /Touchstone/MethodCall.aspx - 81 - 10.5.4.5 - - 401 2 5 0

2016-01-05 16:24:51 10.5.12.16 POST /Touchstone/MethodCall.aspx - 81 - 10.5.4.5 - - 401 1 2148074254 0

2016-01-05 16:24:51 10.5.12.16 POST /Touchstone/MethodCall.aspx - 81 DOMAIN\user 10.5.4.5 - - 200 0 0 15

2016-01-05 16:24:54 10.5.12.16 POST /Touchstone/MethodCall.aspx - 81 - 10.5.4.5 - - 401 2 5 15

2016-01-05 16:24:54 10.5.12.16 POST /Touchstone/MethodCall.aspx - 81 - 10.5.4.5 - - 401 1 2148074254 0

2016-01-05 16:24:54 10.5.12.16 POST /Touchstone/MethodCall.aspx - 81 DOMAIN\user 10.5.4.5 - - 200 0 0 140

Kerberos:

2016-01-05 17:37:46 10.5.12.16 POST /Touchstone/MethodCall.aspx - 81 - 10.5.4.5 - - 401 2 5 0

2016-01-05 17:37:47 10.5.12.16 POST /Touchstone/MethodCall.aspx - 81 DOMAIN\user 10.5.4.5 - - 200 0 0 93

2016-01-05 17:37:47 10.5.12.16 POST /Touchstone/MethodCall.aspx - 81 - 10.5.4.5 - - 401 2 5 0

2016-01-05 17:37:47 10.5.12.16 POST /Touchstone/MethodCall.aspx - 81 DOMAIN\user 10.5.4.5 - - 200 0 0 15

2016-01-05 17:37:47 10.5.12.16 POST /Touchstone/MethodCall.aspx - 81 - 10.5.4.5 - - 401 2 5 0

2016-01-05 17:37:47 10.5.12.16 POST /Touchstone/MethodCall.aspx - 81 DOMAIN\user 10.5.4.5 - - 200 0 0 15

2016-01-05 17:37:50 10.5.12.16 POST /Touchstone/MethodCall.aspx - 81 - 10.5.4.5 - - 401 2 5 0

2016-01-05 17:37:50 10.5.12.16 POST /Touchstone/MethodCall.aspx - 81 DOMAIN\user 10.5.4.5 - - 200 0 0 144

For NTLM, note that there are two 401 (unauthorized) HTTP status codes (401.2 and 401.1) for each HTTP 200 (success) status code. Each of these 401/401/200 codes represents a single request from the client.

With Kerberos, there is only one 401 HTTP status code for each 200 status code.

Each 401 represents an extra round trip between the client and server, which can decrease overall performance, especially on latent connections, such as from remote offices over a slower WAN link or via the Internet.

Use IIS Logs to Confirm Authentication Persistence

You can review IIS logs using Excel to see if authentication persistence is configured properly.

Fiddler is a great tool for debugging HTTP issues. However, to determine if authentication persistence is enabled and working, use IIS logs. Examining IIS logs lets you see what is occurring from the perspective of the server rather than the client.

To review IIS logs to confirm authentication persistence:

1. Copy the log to your desktop or to another working location.
2. Open the log in Notepad.

3. Remove all of the header information or the log will not parse properly:
   a. At the top of the log, note the first four rows:

      #Software: Microsoft Internet Information Services 8.0

      #Version: 1.0

      #Date: 2016-01-05 16:24:50

      #Fields:

   b. After #Fields, find the word **date** followed by all of the other column headers.
   c. In Notepad, place your cursor just before the **d** in **date**, press ENTER, and then delete the first four rows.
   d. Search through the log for additional instances of this header information, because IIS restarts will cause the header information to repeat in the log. Delete any additional instances that you find.
4. Open the log with Excel:
   a. Browse to the location where you edited the log file.
   b. On the Open File dialog box, select **All Files** from the **File Type** drop-down list. By default, you will only see Excel files.
   c. When the Text Import Wizard starts, select the **Delimited** option and click **Next**.
   d. Select **Space** as the delimiter and click **Finish**.
5. When the file displays in Excel, locate the **c-ip** column and filter on unique client IP addresses.
6. Examine the requests.

   If persistence is configured properly, you will see a few 401s at the beginning of the user's session, but the majority of requests will display as 200s.

   It is normal to see other 401s. As long as they are not repetitive, persistence is configured properly.

Deltek

Securing Your Touchstone Deployment

When you install Touchstone, the installation script optionally creates a local Windows Service account on the Touchstone physical Web/Application tier. Deltek recommends using a domain account for the service account.

To secure your Touchstone deployment, you must change this account so that it is unique to your firm and does not include any Deltek default user accounts or passwords.

Most of these changes require administrative rights to your servers, so be sure to log in with the proper account to make these changes. **Do not** log in using the DeltekTouchstone local account because you will subsequently delete or disable this account on all Touchstone servers.

If You Have Multiple Servers

If you have multiple Web/Application servers, make sure that you repeat the same steps on each physical server, using the same user account information that you used on the first server for that tier.

If You Have Deployed Several Logical Tiers with the Same Windows Account

You may have deployed several logical tiers, all using the same Windows account and all located on the same physical server. For example, in a single-server installation, the DeltekTouchstone local Windows account is used as the Application Pool Identity and Windows SQL Login account.

If the account is serving multiple roles, you may not need to delete or disable the accounts as many times as indicated in these instructions.

Web/Application Tier

By default, the Web/Application tier installation creates a local Windows user account named **DeltekTouchstone**. (You can opt to use a domain account instead.)

This account is also added to the Local Administrators group and the IIS_IUSRS group and is configured as the Application Pool Identity of the DeltekTouchstoneAppPool.

To secure the web/application tier and customize the Application Pool Identity:

1. Begin by changing the Application Pool Identity. Select one of the following actions:
   - If you are using a Windows domain, create a domain user account, or use an existing one. Then, add this user to the Local Administrators group and IIS_IUSRS group on the web/application server.
   - If you are not using a Windows domain, create a new local Windows user account and add that user to the same Windows groups.
2. Log on to the domain on the Touchstone web/application server using an Administrator account.
3. Click **Start » All Programs » Administrative Tools » Internet Information Services (IIS) Manager** to open Internet Information Services.
4. Expand the Server name, and click **Application Pools**.

5. Select the **DeltekTouchstoneAppPool**, and select **Advanced Settings** from the Action pane on the right side.
6. Place your mouse pointer in the **Identity** field, and click the ellipses (…) button to set the identity.
7. Select the **Custom account** option, and click **Set**.
8. In the **User name** field on the Set Credentials dialog box, enter the Application Pool Identity in the form <Domain>\<Username>.
9. In the **Password** and **Confirm password** fields, enter the user's password.
10. Click **OK** three times to set the identity.

    After this process is completed, if you are using Windows Integrated Authentication for the SQL Server connection, add the Domain user to the Local User (not Administrators) group on the SQL Server and grant this new Domain user dbo (database owner) rights to your Touchstone database(s).

    > **Attention:** See Database Tier for more information.

11. Click **Computer Management » Local Users and Groups » Users** and delete or disable the local DeltekTouchstone Windows user account on the web/application server.

Deltek

Configure HTTP Compression

Configuring HTTP Compression for Touchstone can greatly reduce the size of HTTP (hypertext transfer protocol) requests and responses between the client and web server, which improves application response time. HTTP Compression functionality is built into Internet Information Services (IIS) but is not enabled by default. This section explains how to install and configure HTTP Compression.

Three Configuration Methods for HTTP Compression

You can configure HTTP Compression using one of three methods:

- Use the appcmd IIS command line administrative utility. You must run this utility via an elevated command prompt such as **Run as Administrator**.
- Modify the applicationhost.config file directly. Deltek does **not** recommend that you modify the applicationhost.config file directly unless you are familiar with XML formatting. Be sure to make a backup of applicationhost.config before you make any changes.
- Use the Configuration Editor via the Internet Information Services administrative utility.

This document focuses on the first of the three methods. However, if you want to use the other methods, you can use the modified entries and settings from applicationhost.config, described at the end of this section.

Install HTTP Compression IIS Role Services

To install HTTP Compression IIS Role Services:

1. Launch the Server Manager.
2. Click **Roles**.
3. Under Web Server (IIS), locate **Role Services** and check to see that the Static and Dynamic Content Compression role services have been installed.
4. If not, select **Add Role Services** and install both role services.

Alternative Procedure

Alternatively, you can install these role services using the Windows Package Manager (pkgmgr) from an administrative command prompt (for example, **Run as Administrator**). Run this command:

```
start /w pkgmgr /iu:IIS-WebServerRole;IIS-Performance;IIS-HttpCompressionStatic;IIS-HttpCompressionDynamic
```

Configure HTTP Compression

To configure HTTP Compression:

1. Select one of the following actions:
   - If you want to enable compression at the server level, ensure that both static and dynamic compression are enabled via an elevated command prompt:

     ```
     C:\Windows\System32\Inetsrv\Appcmd.exe set config -section:urlCompression -doStaticCompression:true -doDynamicCompression:true
     ```

- If you want to enable compression for a particular web site, use the following command and replace **"Site Name"** with the name of the web site:

  ```
  C:\Windows\System32\Inetsrv\Appcmd.exe set config "Site Name" -
  section:urlCompression -doStaticCompression:true -doDynamicCompression:true
  ```

2. Set the static and dynamic compression levels via an elevated command prompt:

   ```
   C:\Windows\System32\Inetsrv\Appcmd.exe set config -section:httpCompression -
   [name='gzip'].staticCompressionLevel:9 -
   [name='gzip'].dynamicCompressionLevel:4
   ```

   The default dynamic compression level is zero.

   > **Note:** Dynamic compression can significantly impact CPU resources. For information and recommendations on setting compression levels, see the blog post IIS 7 Compression. Good? Bad? How much?. The command above uses recommendations from this blog post.

3. Configure the content types that you want to compress.

   The default configuration compresses most static and dynamic content types used by the application.

Additional Settings that May Impact HTTP Compression

You should test to ensure that HTTP Compression is working as expected before modifying these settings. Follow the instructions in the next section to determine if these settings are necessary in your environment.

The following additional settings may impact the functionality of HTTP Compression:

```
C:\Windows\system32\inetsrv\appcmd.exe set config -
section:system.webServer/serverRuntime /frequentHitThreshold:1 /commit:apphost
```

```
C:\Windows\system32\inetsrv\appcmd.exe set config -
section:system.webServer/serverRuntime /frequentHitTimePeriod:00:01:00 /commit:apphost
```

The default values are **2** and **00:00:10**, respectively.

> **Attention:** For more information, see the article Server Runtime.

Test the HTTP Compression Configuration

Consider using Telerik Fiddler HTTP Debugging Proxy to determine that HTTP Compression is working as expected.

HTTP Compression Sections/Settings in applicationhost.config

The configuration of HTTP Compression described above modifies the three primary sections in applicationhost.config shown below. The specific settings that you modify are displayed in red:

- `<urlCompression doStaticCompression="true" doDynamicCompression="true" />`
- `<httpCompression directory="%SystemDrive%\inetpub\temp\IIS Temporary Compressed Files">`

```
<scheme name="gzip" dll="%Windir%\system32\inetsrv\gzip.dll"
staticCompressionLevel="9" dynamicCompressionLevel="4" />
          <staticTypes>
              <add mimeType="text/*" enabled="true" />
              <add mimeType="message/*" enabled="true" />
              <add mimeType="application/x-javascript" enabled="true" />
              <add mimeType="application/atom+xml" enabled="true" />
              <add mimeType="application/xaml+xml" enabled="true" />
              <add mimeType="*/*" enabled="false" />
          </staticTypes>
          <dynamicTypes>
              <add mimeType="text/*" enabled="true" />
              <add mimeType="message/*" enabled="true" />
              <add mimeType="application/x-javascript" enabled="true" />
              <add mimeType="application/octet-stream" enabled="true" />
              <add mimeType="application/x-ms-application" enabled="true" />
              <add mimeType="application/x-ms-manifest" enabled="true" />
              <add mimeType="*/*" enabled="false" />
          </dynamicTypes>
      </httpCompression>
```

- `<serverRuntime frequentHitThreshold="1" frequentHitTimePeriod="00:01:00" />`

Deltek

Web/Application Server Load Balancing

Touchstone supports the use of multiple Web/Application servers in a load balanced configuration. Configure load balancing according to your vendor's recommendations.

To better support fault tolerance and load balanced configurations, Touchstone supports the use of Redis for sharing Touchstone user session state, queueing of project submittals for scoring, and queueing between the load balanced Web/Application servers.

If you choose not to use Redis for caching Touchstone user session state in a load balanced environment, the load balancer must be configured with client affinity to ensure that users are routed to the same server that they initially are connected to when they log into the application.

For more information about Redis, see the following article: https://redis.io/topics/introduction.

Configuring Touchstone to Use Redis

> **Note:** When you enable Redis, issues can occur when you run the benchmark report generation process. Disable Redis by removing the config.dat settings mentioned below.

For information about the settings needed to enable the use of Redis for Touchstone, see Using Redis for Session State and Queueing in Appendix C.

Deltek

Schedule File Types and Maximum File Size

Schedule File Types

Touchstone integrates with different types of schedule projects. You can upload a schedule to Touchstone from one of the following schedule types:

- Deltek Open Plan (.bk3)
- Microsoft Project (.mpp)
- Primavera P6 (.xer and .xml)

Maximum File Size for Uploaded Files

You can configure the maximum file size for uploaded files to limit the maximum size of a schedule that can be submitted to Touchstone. Touchstone has two web.config files—one for the PPM.API and one for the Touchstone API. The file size must be set to the same value in both.

For more information about these settings, see Metric File Upload and Project Submittal Upload in Appendix D: Touchstone Website Configuration Settings.