


Deltek Vantagepoint

Installation and Maintenance Guide

September 10, 2021



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 publication contains proprietary information that is protected by copyright. All rights are reserved. No part of this document may be reproduced or transmitted in any form or by any means, electronic or mechanical, or translated into another language, without the prior written consent of Deltek, Inc.

This edition published September 2021.

© Deltek, Inc.

Deltek's software is also protected by copyright law and constitutes valuable confidential and proprietary information of Deltek, Inc. and its licensors. The Deltek software, and all related documentation, is provided for use only in accordance with the terms of the license agreement. Unauthorized reproduction or distribution of the program or any portion thereof could result in severe civil or criminal penalties.

All trademarks are the property of their respective owners.

Contents

Overview.....	1
What's New	1
Related Vantagepoint Documentation	1
If You Need Assistance	2
Customer Services.....	2
Deltek Support Center	2
Access Deltek Support Center	3
Adding Custom Notes to This Guide	3
Install the Vantagepoint Software.....	4
Before You Begin Deployment	4
Logical Tiers Overview.....	4
Logical Tiers	4
Installation/Deployment Models	5
Logical Tier Model	7
Logical Tier Model with Reverse Proxy	8
Logical Tier Model with Three or More Servers	9
Passwords	9
Password Complexity Rules	9
Supported Deployment Scenarios	10
Install without an Internet Connection.....	10
Access to Weblink.....	10
Permissions Required to Install Vantagepoint.....	11
Vantagepoint Service Account Requirements	11
PowerShell Script and Console.....	12
PowerShell Console.....	12
Navigation and Data Entry Tips	12
Performance.....	14
Digital Signature.....	14
Firewall Rules for PowerShell Remoting	14
PowerShell Execution Policy	15
Prompts for Deltek Support Username and Password.....	15
Log Files	15
Log Files Generated During the Report-Loading Process.....	15

Conversion Log	16
Troubleshoot Installation Problems	16
System Requirements	17
Platform Virtualization	17
Software Requirements	17
Supported Versions and Compatible Versions	17
Prerequisite Checks Run Automatically.....	19
SQL Server Database Requirements	20
SQL Server Standard or Enterprise Edition	20
SQL Server Express Edition with Advanced Services	21
SQL Server Express Edition Requirement.....	21
Communication between Vantagepoint and the SQL Server Database.....	21
Multiple Languages	22
Database Maintenance Activities	23
.NET Architecture.....	23
Upgrade Scenarios for Vantagepoint 4.5	25
Upgrading from Vision, GovWin CM, or Ajera CRM 7.6	25
Upgrading from Vantagepoint 2.0.x through 4.0.x	25
Upgrade Scenarios for Vantagepoint 4.0	26
Upgrading from Vision, GovWin CM, or Ajera CRM 7.6	26
Upgrading from Vantagepoint 2.0.x through 3.5.x	26
Important Note for Vantagepoint 4.0 Upgrades	27
Upgrade Scenarios for Vantagepoint 3.5	28
Upgrading from Vantagepoint 2.0.x and 3.0.x	28
Pre- and Post-Installation Checklists.....	29
Pre-Installation General Checklist	29
Pre-Installation Server Checklists	30
Single-Server.....	30
Dual-Server (Two-Tier) Configuration 1	31
Dual-Server (Two-Tier) Configuration 2.....	33
Three or More Servers	34
Post-Installation Checklist (New Installations)	37
Web Server	37
Dedicated Process Server	38
Client Tier (Workstation)	38
Post-Installation Checklist (Upgrades).....	38

Web Server	39
Dedicated Process Server	39
Installing Vantagepoint	40
Overview	40
Step 1: Download the PowerShell Script	40
Download the Script via the Deltek Support Center	41
Download the Script via DSM Lite	41
DSM Documentation and Troubleshooting	42
Step 2: Run the Script with No Switches	42
Step 3: Run the Script with the CheckPreReq Switch	43
Step 4: Run the Script with the Setup or SetupAndMigrate Switch	45
Setup Steps for Non-Internet Server	46
Run the Script with the Setup Switch	46
Run the Script with the SetupAndMigrate Switch	50
Step 5: Rerun the Script Using Optional Switches	54
Step 6: Verify That the Installation Was Successful	55
First-Time Installation	55
Migration from Another Deltek Product	55
Step 7: Optimize Database	55
Optional Switches	56
Primary Switches	56
Additional Setup Switches	58
Advanced Setup Switches	59
Support Setup Switches	60
Intelligence Setup Switches	61
SetupDatabaseNew Switch	62
MigrateDatabase Switch	64
UpgradeDatabase Switch	65
ValidateDatabases Switch	67
CreateDatabaseEntry Switch	68
RemoveInvalidWeblinkEntries Switch	70
SetupWebApp Switch	71
SetupProcessServer Switch	73
SetupCustom Switch	74
Procedure	74
Download, DownloadAndExtract, DownloadDatabases, and DownloadSetupPrep Switches	75

DownloadAndExtract.....	75
DownloadSetupPrep	75
Procedure.....	76
Setup Steps Performed by the Script.....	76
DownloadVantagepointIntelligence Switch.....	78
Procedure.....	78
Setup Steps Performed by the Script.....	79
SetVersion Switch.....	79
Procedure.....	79
Setup Steps Performed by the Script.....	79
Upgrade Switches.....	79
Upgrade Switch	80
Procedure.....	80
Setup Steps Performed by the Script.....	82
UpgradeWebApp Switch.....	82
Procedure.....	83
Setup Steps Performed by the Script.....	83
UpgradeProcessServer Switch.....	84
Procedure.....	84
Setup Steps Performed by the Script.....	84
UpgradeDatabases Switch	85
Procedure.....	85
Setup Steps Performed by the Script.....	86
RunSQLScriptOnSelectedDatabases Switch	86
Procedure.....	86
Setup Steps Performed by the Script.....	86
Uninstall Switch.....	86
Procedure.....	87
Setup Steps Performed by the Script.....	87
InstallProcessServerService and RemoveProcessServerService Switches	87
Procedure.....	88
SetServiceAccounts Switch	88
Procedure.....	88
LoadReports Switch.....	89
Procedure.....	89
Setup Steps Performed by the Script.....	90

LoadReportsCustom Switch	90
Procedure	90
Setup Steps Performed by the Script.....	90
EnableIISRequiredFeatures Switch	91
Procedure	91
Setup Steps Performed by the Script.....	91
GetLicenseFile Switch	91
Procedure	92
Setup Steps Performed by the Script.....	92
UpdateLicenseFile Switch.....	92
Procedure	92
Setup Steps Performed by the Script.....	92
EnableWindowsExplorerPowerShellIntegration Switch.....	92
Procedure	92
Setup Steps Performed by the Script.....	92
CreateDeltekVantagepointCMDFile Switch	93
Setup Steps Performed by the Script.....	93
Procedure	93
Cleanup Switch	93
Procedure	93
Setup Steps Performed by the Script.....	93
ChangeWeblinkPassword Switch	93
Procedure	93
Setup Steps Performed by the Script.....	94
ConfigureARR Switch	94
Procedure	94
Setup Steps Performed by the Script.....	94
ConfigureIISCompression Switch	94
Procedure	94
Setup Steps Performed by the Script.....	94
ConfigureWindowsAuthentication Switch	94
Procedure	94
Setup Steps Performed by the Script.....	94
ConfigureAuthenticationPersistence Switch	95
Procedure	95
Setup Steps Performed by the Script.....	95

ConfigureDatabaseSessionState Switch	95
Procedure	95
Setup Steps Performed by the Script.....	95
EnableFailedRequestTracing Switch	95
Procedure	95
Setup Steps Performed by the Script.....	95
DisableFailedRequestTracing Switch	96
Procedure	96
Setup Steps Performed by the Script.....	96
GetConfigFiles Switch.....	96
Procedure	96
Setup Steps Performed by the Script.....	96
GetAllLogs Switch	97
Procedure	97
Setup Steps Performed by the Script.....	97
GetSetupLogs Switch	97
Procedure	97
Setup Steps Performed by the Script.....	97
GetSSRSLogs Switch	98
Procedure	98
Setup Steps Performed by the Script.....	98
GetIISLogs Switch	98
Procedure	98
Setup Steps Performed by the Script.....	98
GetEventLogs Switch.....	99
Procedure	99
Setup Steps Performed by the Script.....	99
GetSQLErrorLogs Switch.....	99
Procedure	99
Setup Steps Performed by the Script.....	99
GetAppUserInQuery Switch.....	100
Procedure	100
Setup Steps Performed by the Script.....	100
GetActiveRunningReports Switch.....	100
Procedure	101
Setup Steps Performed by the Script.....	101

GetActiveWebRequests Switch	101
Procedure	101
Setup Steps Performed by the Script.....	101
Analysis Cubes Switches.....	101
GenerateMachineKey Switch	101
Procedure.....	102
Setup Steps Performed by the Script.....	102
Insert the <machinekey> element into web.config file.....	102
Optional Sub-Switches	104
Vantagepoint URLs	105
Set Up Single Sign-On for Vantagepoint with Microsoft Azure Active Directory	105
Mobile Applications and Vantagepoint.....	106
Touch Server URL Setup in Email.....	106
Touch Server URL Format	106
ProductApplication.php	106
Link for Customers	106
Create the Link to Email Users	106
Configure Vantagepoint.....	108
Back Up Your Vantagepoint Database.....	109
Set Up Silent Installation	110
Basic Setup Steps.....	110
Generate Password Files.....	110
Optional: Edit the Create Passwords Script.....	111
Generate the Response File	112
Switches.json and Parameters.json Files	112
Use the ResponseGenerator.ps1 Script	113
Run DeltekVantagepoint.ps1 with the SilentInstall Switch	116
Take Screenshots	116
Test the Silent Installation.....	116
Flowcharts and Samples.....	118
Relationship of Files Used with the SilentInstall Switch.....	118
Relationship of Switches.json and Parameters.json Values.....	119
Sample Response File (for CheckPreReq.xml)	119
Sample Elements/Prompts.....	120
Sample Excerpt from the Switches.json File.....	123
Sample Excerpt from the Parameters.json File	123

System Constants	125
Advanced Administrator Topics.....	126
Microsoft Internet Information Server (IIS) Installation on Windows Server	127
Required IIS Features.....	127
Microsoft SQL Server Edition and Version Information.....	128
Microsoft SQL Server 2019 Express Edition with Advanced Services	128
Microsoft SQL Server Reporting Tools.....	128
Microsoft SQL Server Reporting Services.....	129
Overview of SQL Server Reporting Services.....	129
More Information about Reporting Services	130
Report Server Licensing Requirements.....	130
Features Supported by Different SQL Server Editions	130
Custom Reports and Custom Invoices	131
Supported Report Writing Tools.....	131
Upgrade Custom Reports and Custom Invoices.....	131
Summary of Upgrading Custom Reports and Invoices.....	131
Extra Space in Invoice Header.....	132
Configure Microsoft SQL Server Reporting Services	132
Important Information about Configuring Reporting Services.....	132
Initial Setup Steps	133
Connect to the Report Server Web Service.....	134
Specify the Report Server Host Name and URL.....	134
SQL Report Server Database Prompt During Setup	136
Give Your Account Proper Rights and Privileges in Reporting Services Web Services	137
Prerequisite Report Server and SQL Server Database Credentials.....	138
Configure Transaction Document Management	139
Prerequisites	139
FileStream Best Practices.....	139
Identify the SQL Server to Host the FileStream Database	140
Enable FileStream on SQL Server	140
Enable FileStream during SQL Server Installation	140
Enable FileStream after SQL Server is installed.....	140
Configure and Validate the FileStream Database with Weblink	141
Files Administration Utility in Vantagepoint.....	141
“Databases Out of Sync” Issue	142
Troubleshooting FileStream.....	142

Weblink Cannot Create FileStream Database Objects.....	142
Error: "FILESTREAM data cannot be placed on empty filegroup"	142
Not Configured to Upload Supporting Documents.....	143
FILESTREAM Database Cannot be Opened.....	143
Using FileStream with Other SQL Server Features.....	143
How to Use FileStream in a Firewall-Protected Environment.....	144
Queries to Join the Vantagepoint Transaction DB and FILES DB	144
Configure a Shared Location for Databases.enc	145
Alternative to a Shared Databases.enc File	145
Configure Secure Sockets Layer (SSL)	146
Important Information on SSL Configurations	146
How the Reporting Framework Handles SSL.....	146
Non-Standard SSL Ports	146
Secure the Vantagepoint Web Server	147
Request a Server Certificate	147
Test the SSL Certificate and Binding	148
Secure SQL Server Reporting Services	148
Test the SSL Configuration.....	149
Reload Reports into Vantagepoint	150
Connection Errors	150
Identify the Error	150
Test the Report Server Settings in Weblink	150
Reload Reports into Vantagepoint	150
Create a Reverse Proxy for SQL Reporting Using Application Request Routing (ARR).....	152
Do I Need a Reverse Proxy?	152
Important Information on the Use of Non-standard Ports.....	152
Prerequisites	152
Install Application Request Routing (ARR)	153
Configure Application Request Routing (ARR).....	153
Test the Proxy Server	155
Configure Vantagepoint to Use the Reverse Proxy	155
Troubleshooting	156
Configure HTTP Compression	157
Three Configuration Methods for HTTP Compression	157
Install HTTP Compression IIS Role Services	157
Alternative Procedure.....	157

Configure HTTP Compression.....	157
Additional Settings that May Impact HTTP Compression.....	158
Test the HTTP Compression Configuration.....	159
HTTP Compression Sections/Settings in applicationhost.config.....	159
Pre-Deploy Vantagepoint Smart Client to User Workstations.....	160
ClickOnce Deployment Features	160
Files to be Deployed	160
Deploy Files to a Workstation	161
Configure Integrated Security for Vantagepoint	162
Required Configuration Changes	162
Configure the Application Pool Identity.....	163
Configure IIS to Use Windows Integrated Authentication	163
Configure Vantagepoint for Windows Integrated Authentication.....	164
Configure Windows Integrated Authentication for Internet Users (and Non-Domain Workstations).....	165
Configure Windows Integrated Authentication for the Vantagepoint Database Connection	165
Configure a Service Principal Name.....	166
IIS Kernel Mode Authentication.....	166
Kernel Mode Authentication Implementation	167
Service Principal Names	167
Configure Authentication Persistence.....	167
Source of Extra Round Trips.....	168
Configuration Options for Authentication Persistence	169
Use IIS Logs to Confirm Authentication Persistence	169
Important Configuration Changes for Vantagepoint API	170
Modify IIS Feature Delegation.....	170
Modify Vantagepoint Web.config File	171
Configure Database Session State for Vantagepoint.....	174
Create the Session State Database (Optional)	174
Configure Vantagepoint for Database Session State	174
Securing Your Vantagepoint Deployment	176
If You Have Multiple Servers	176
If You Have Deployed Several Logical Tiers with the Same Windows Account	176
Web/Application Tier.....	176
Database Tier	177
Windows Integrated Authentication	178
Mixed Mode Authentication.....	179

Report Tier	179
Process Server Tier	180
Configure Reporting Services Logging.....	181
Enable Reporting Services Trace Logging	181
Rules for Tracing	181
Components that Can Be Traced Library	181
Changes to the ReportServer\bin\ReportServerService.exe.config File.....	182
Errors in the Reporting Services Log File	183
Enable Reporting Services HTTP Logging	183
Configure an Alternate Database for Vantagepoint Reporting.....	184
Alternate Database for Reporting	184
Configure the Alternate Database for Reporting in WebLink.....	185
Identify the Connection String Used in a Report	186
Configure Basic Availability Groups Using Microsoft SQL Server Standard Edition.....	187
Differences in SQL Server Standard and Enterprise Features.....	187
Multi-subnet Failover	188
Install and Configure Windows Server Failover Cluster (WSFC)	188
Install the Failover Clustering Feature	189
Configure Failover Clustering using Failover Cluster Manager	189
Install SQL Server on Each Cluster Node	190
Installation Requirements and Notes	190
Configure Database Login	191
Create Availability Groups	192
Configure Vantagepoint and Reporting Services to Use Availability Group Listener	194
Configure Vantagepoint to Use the Availability Group Listener.....	194
Configure Reporting Services to Use the Availability Group Listener.....	195
Flexible Failover Policy	196
Failover Condition Level and Health Check Timeout.....	196
Monitoring Availability Groups	196
Availability Group Dashboard.....	197
System and Dynamic Management Views (DMVs)	197
System Monitor (PerfMon)	197
Windows PowerShell	197
Troubleshooting	197
Use Availability Groups Check Box Does Not Display	197
System Health Check.....	197

Framework Exception: The User Does Not Have Permission to Perform this Action	198
Configure Availability Groups Using Microsoft SQL Server Enterprise Edition.....	199
Differences in SQL Server Standard and Enterprise Features.....	199
More Information.....	199
Prerequisites	200
Installation Overview.....	200
Create the Windows Server Failover Cluster (WSFC)	200
Multi-subnet Clustering	201
Install and Configure WSFC	201
Install the Failover Clustering Feature	201
Configure Failover Clustering using Failover Cluster Manager	202
Install SQL Server on Each Node.....	202
Installation Requirements and Notes	202
Configure Database Login	203
Create Availability Groups	204
Read Only Routing Configuration	206
Read Only Routing Queries	207
Configure the Read Only Routing URL.....	207
Configure Read Only Routing Lists.....	208
Configure Vantagepoint and Reporting Services to Use Availability Group Listener	209
Configure Vantagepoint to Use the Availability Group Listener.....	209
Configure Reporting Services to Use the Availability Group Listener.....	210
Flexible Failover Policy	210
Failover Condition Level and Health Check Timeout	211
Monitoring Availability Groups	211
Availability Group Dashboard.....	211
System and Dynamic Management Views (DMVs)	212
System Monitor (PerfMon)	212
Windows PowerShell	212
Troubleshooting	212
Use Availability Groups Check Box Does Not Display	212
System Health Check.....	212
Framework Exception: The user does not have permission to perform this action	213
Identify the Connection String Used by the Application or Process Server	213
Identify the Connection String Used in a Report.....	214

Overview

This guide explains how to install Deltek Vantagepoint software on your servers. This guide is divided into the following sections:

Title	Purpose
Install the Vantagepoint Software	This part of the guide walks you through the process of installing Vantagepoint software on your servers, creating new Vantagepoint databases or migrating existing Vision databases, and performing related steps. This section begins with an overview of Vantagepoint server architecture.
Advanced Administration Topics	This part of the guide covers advanced configuration options that you may want to consider, especially if you have a large-scale Vantagepoint implementation.

What's New

Version 4.5

- Added [Upgrade Scenarios for Vantagepoint 4.5](#).
- Made the following changes to the GenerateMachineKey Switch:
 - Added information on how to insert the <machinekey> switch into web.config files.
 - Added to the list of steps that the script completes.
 - Added a new procedure: [Insert the <machinekey> switch into web.config files](#).

Related Vantagepoint Documentation

Go to the Deltek Support Center to access the following:

- Online help
- What's new? / release notes
- How-to videos
- Settings and Configuration guide
- Product Support Compatibility Matrix

If You Need Assistance

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

Customer Services

For over 30 years, Deltek has 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 Customer Care analysts
- Technical services
- Consulting services
- Custom programming
- Classroom, on-site, and Web-based training

Note: 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 Customer Care 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 Customer Care analyst online

Attention: For more information regarding Deltek Support Center, see the online help available from the [Web site](#).

Access Deltek Support Center

To access the Deltek Support Center:

1. Go to <http://support.deltek.com>.
2. Enter your Deltek Support Center **Username** and **Password**.
3. Click **Login**.

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

Adding Custom Notes to This Guide

If you would like to add custom notes to this guide that are specific to your company, Adobe® Reader® X provides this ability. If you do not already use Adobe Reader X, you can download it [here](#) free from Adobe.

To add a custom note using Adobe Reader X:

1. On the Reader toolbar, click **Comment** at the far right.
2. In the **Annotations** pane that displays, click the **Sticky Note**. The cursor changes to match the button.
3. Position the cursor at the location in the guide where you want the note to appear, and click. A note icon is inserted at the location and a text box pops up.
4. Enter your information in the text box.
5. Continue adding notes as needed.

Note: Deltek recommends that you save the document to a slightly different filename so as to keep the original from being overwritten.

When reading the document, cursor over a note icon to see the information. Double-click a note icon to edit the information.

Install the Vantagepoint Software

Before You Begin Deployment

Before you begin deployment, it is important to understand the following:

- Logical Tiers
- Installation / Deployment Models
- Hardware and Software Requirements

Logical Tiers Overview

Before you install Vantagepoint, you should carefully consider the server architecture that best fits your company's needs. You can choose from several architecture models

Logical Tiers

Vantagepoint uses a multi-tier architecture. Various components of the Vantagepoint application are distributed to logical tiers for performance and scalability. The logical tiers are as follows:

Tier	Description
Client	<p>This is the user interface layer for Vantagepoint. It presents input data to the application/web server tier and displays the returned result in a format that you can understand. The client tier is installed on a workstation.</p> <p>Vantagepoint uses two technologies in the client tier:</p> <ul style="list-style-type: none"> ▪ The primary technology is a web-based interface (web client). ▪ The secondary technology is a smart client that uses the ClickOnce deployment technology for delivering Windows-based applications to the user. The smart client application checks for new updates on the web/application server each time the application is launched and automatically installs them into the local user's profile (%USERPROFILE%\Local Settings\Apps\2.0\...). <p>The smart client technology will be phased out prior to the release of Vantagepoint 3.0.</p>
Web/Application Server	<p>This tier performs functional process logic for Vantagepoint. When a request is sent by the client tier, this the web/application server tier processes that request (such as retrieving stored data or performing a specific function) and then returns the result to the client tier. This tier also uses IIS to host Vantagepoint applications.</p>
Process Server	<p>This tier lets the user schedule processes and profiles to run automatically in the background. Examples of processes that can run on the process server are:</p> <ul style="list-style-type: none"> ▪ All reports ▪ All scheduled alerts ▪ Large batch jobs (for example, billing, revenue generation)

Tier	Description
Report Server	This tier handles all reporting requests. It uses Microsoft SQL Server Reporting Services.
Database	This tier consists of SQL Server Database Server(s) where Vantagepoint data is stored and retrieved.

Installation/Deployment Models

You can choose one of three different tier models to deploy Vantagepoint. The model that you choose depends on your organization's size needs, cost considerations, security requirements, and fault tolerance.

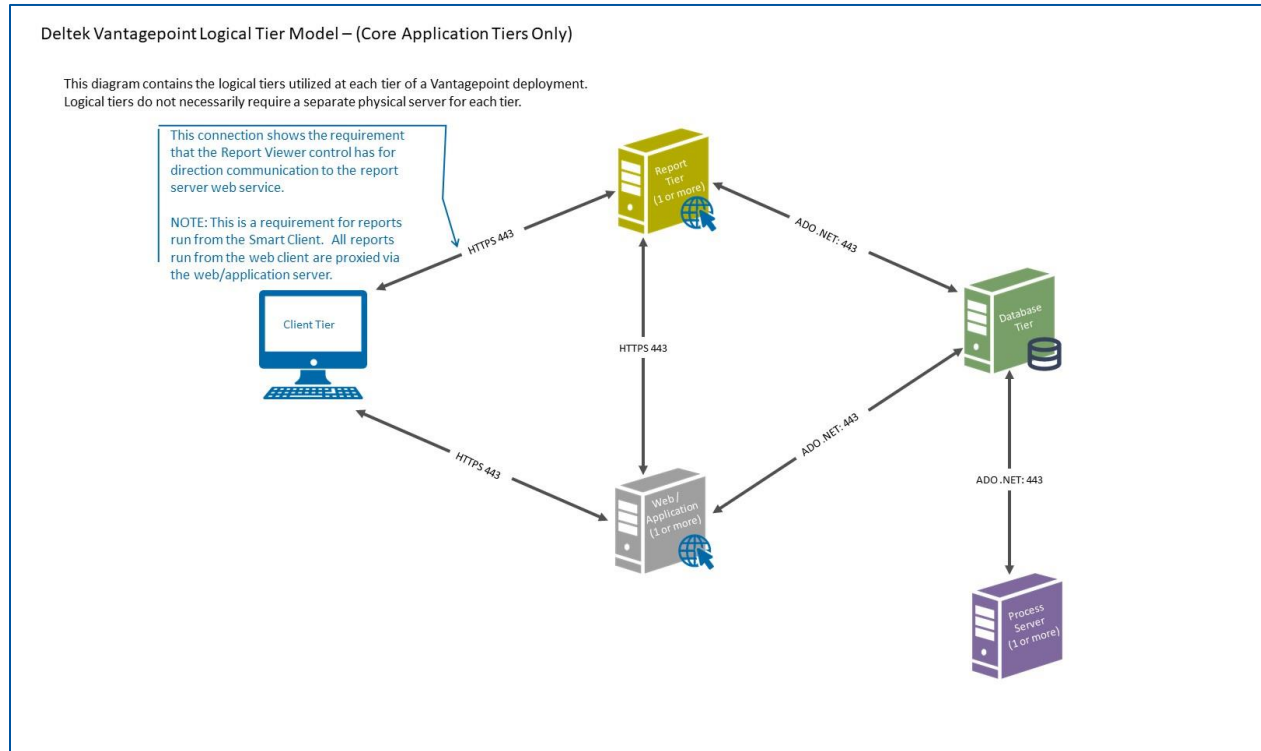
Note: Regardless of the deployment model you choose, you install all components from the web/application tier, except a dedicated process server.

Deployment Model	Description	Use this model if...
One-Server (Single Server)	<p>Install Vantagepoint tiers (web, application, process server, report components, and database) on the same machine.</p> <p>Infrastructure security is not a concern with this model because all application use is internal to the organization.</p>	<ul style="list-style-type: none"> Your organization is small (fewer than 50 employees). Deployment needs are simple. For example, you are installing Vantagepoint on a test machine. All users are at a single location and will access Vantagepoint in the office or over a Virtual Private Network (VPN) connection to the corporate network. Users will not access the application over the internet.
Dual-Server (Two-Tier) Configuration 1	<p>Install the database and report components on a server machine and the web/application and process server components on a separate server machine.</p> <p>In this configuration, the Vantagepoint client application needs a direct connection to the report server to run and view reports.</p> <p>Infrastructure security is not a concern with this model because all application use is internal to the organization.</p>	<ul style="list-style-type: none"> You have a small to medium sized organization that may not have a technical staff. Your organization has one SQL Server license. All users are at a single location and will access Vantagepoint in the office or over a Virtual Private Network (VPN) connection to the corporate network. Users will not access the application over the internet. Because the database server and the report server are on the same server machine, this model is not suitable for

Deployment Model	Description	Use this model if...
		<p>an environment in which users access the application over the internet. To address the security issue of having the report/database server exposed to the internet, consider using the IIS ARR Reverse Proxy for the web server to act as a proxy for handling requests to the report server. See Create a Reverse Proxy for SQL Reporting Using Application Request Routing for details.</p>
<p>Dual-Server (Two-Tier) Configuration 2</p>	<p>Install the database component on a server machine and the web/application, process server, and report components on a separate server machine.</p> <p>Split the report server (web service) from the database server hosting the report server database.</p> <p>Install reporting services on a server separate from the database engine.</p>	<ul style="list-style-type: none"> You have a small to medium sized organization that may not have a technical staff. Your organization has more than one Microsoft SQL Server license. Users will access Vantagepoint over the internet.
<p>Three or More Servers</p>	<p>Install any of the following:</p> <ul style="list-style-type: none"> A single database server One or more report servers One or more web/application servers One or more process servers, each on its own machine 	<ul style="list-style-type: none"> You have a large organization that has multiple locations, can afford multiple SQL Server licenses, and will use Vantagepoint on an internal Wide Area Network (WAN). You need additional report, web/application, or process servers for load balancing, performance, security, or fault tolerance reasons. You have complex deployment and firewall requirements.

Logical Tier Model

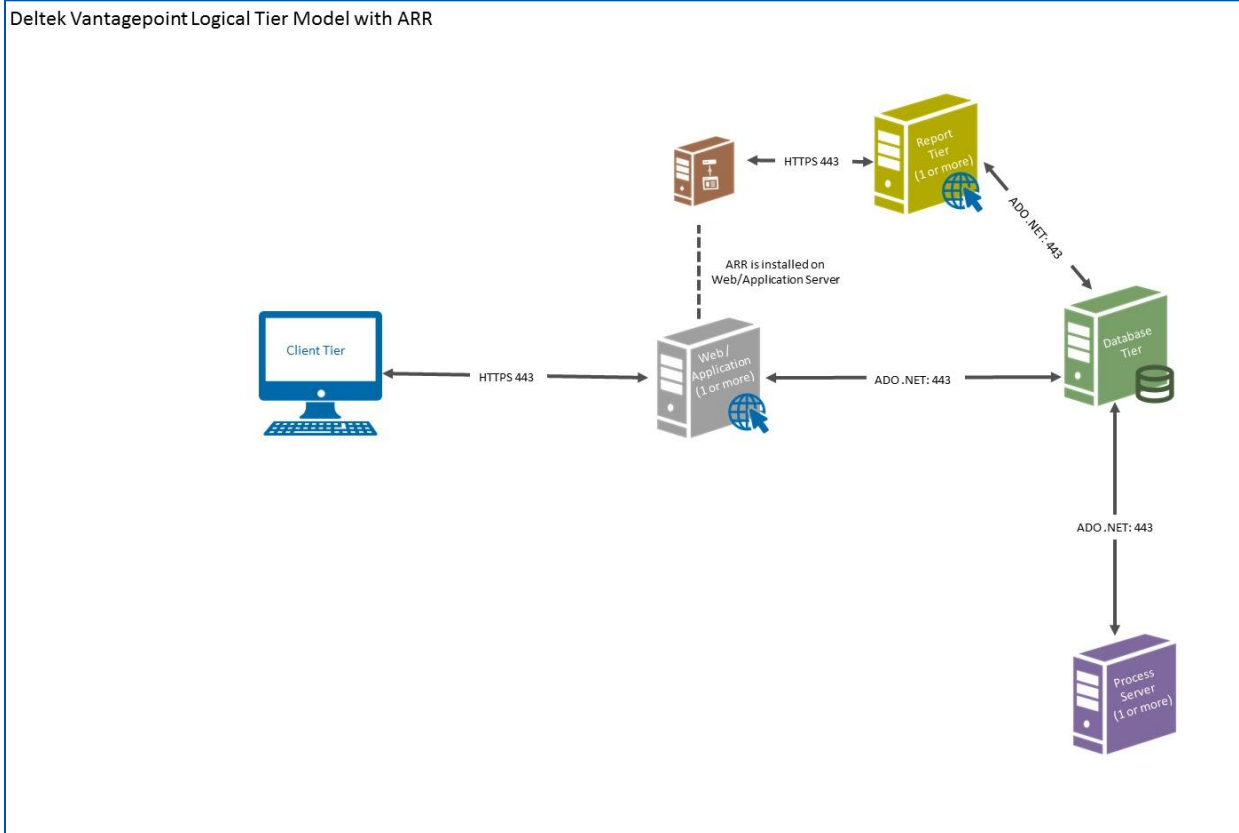
This diagram shows the logical tiers and technologies used at each tier of a Vantagepoint deployment. You do not necessarily need a separate physical server for each logical tier. If you use a single-server deployment model, you install and configure each tier on a single server.



Logical Tier Model with Reverse Proxy

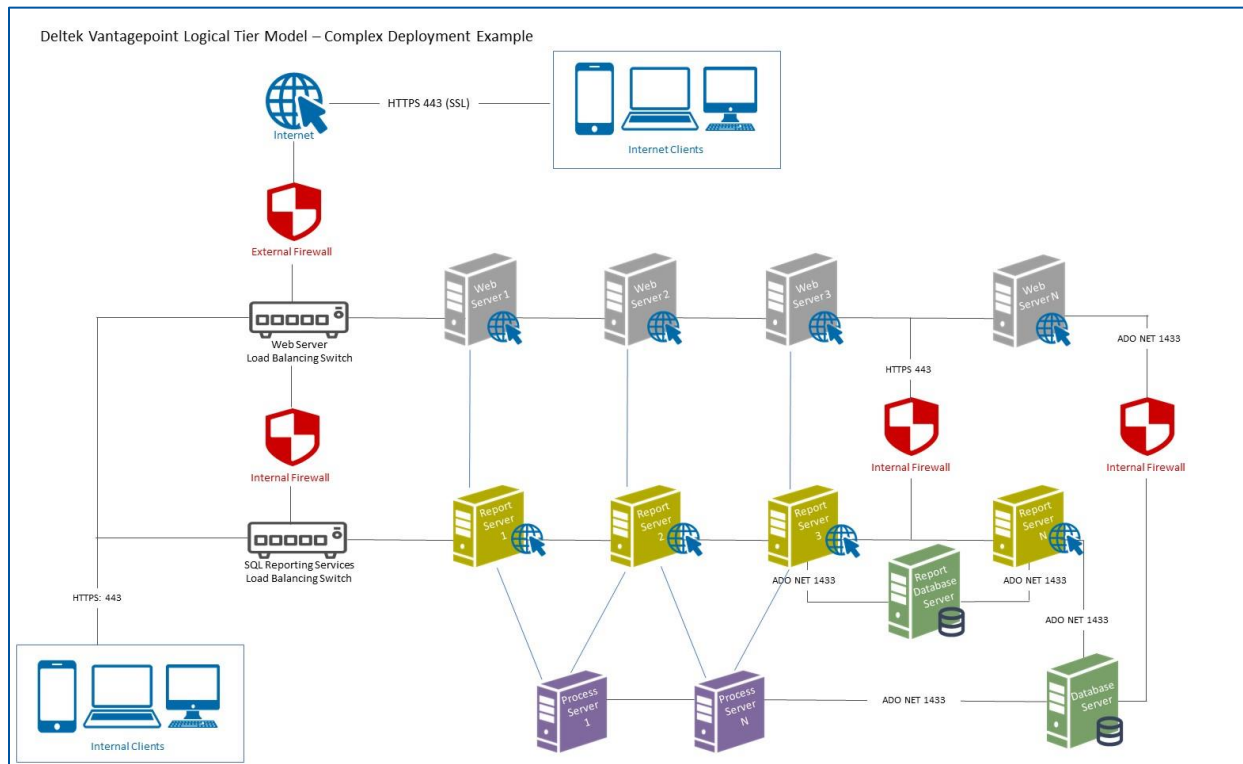
This diagram shows how the IIS [ARR Reverse Proxy](#) has been implemented on a web server to serve as a proxy for handling requests to the report server. This configuration addresses the security issue of having the report/database server exposed to the internet.

This diagram shows the logical tiers and technologies used at each tier of a Vantagepoint deployment. You do not necessarily need a separate physical server for each logical tier.



Logical Tier Model with Three or More Servers

This diagram shows a Vantagepoint deployment that uses three or more servers.



Passwords

When you specify a password (for example, for the Application Pool Identity or database logon), the setup script checks to make sure that your password is strong. These checks apply to any local Windows accounts and any SQL logins created by the setup. The script:

1. Checks the password against a list of known insecure passwords. If the password is in the list, the script prompts you to choose a different password.
2. Checks the password against password complexity rules.

Password Complexity Rules

The DeltekVantagepointSettings.xml file includes default password complexity rules, which you can modify to suit your needs. Because all passwords must meet domain policy requirements, you may need to modify the password complexity rules to overcome conflicts.

Rule	Settings	Default Settings
Require a minimum password length?	True or False	True
If you require a minimum password length, how many characters are required?	Number of characters	8

Rule	Settings	Default Settings
Require uppercase characters in the password?	True or False	True
Require lowercase characters in the password?	True or False	True
Require numbers in the password?	True or False	True
Require special characters in the password?	True or False	True

For example, if you try to use a password of **password**, you will receive an error message saying that the password does not include an uppercase character, number, or special character.

Supported Deployment Scenarios

- Vantagepoint supports single server, dual server, or multi-server installations.
- Vantagepoint supports advanced deployments, such as the use of DMZ, multiple web servers, and dedicated process servers.
- Vantagepoint supports non-standard HTTPS ports.
- Vantagepoint supports installing to a drive other than C:\Program Files\Deltek\Vantagepoint.
- Each server must be a member of the domain.
- Vantagepoint cannot be installed on domain controllers, Exchange servers, SharePoint servers, terminal services, or Citrix servers.
- Vantagepoint cannot upgrade an existing Deltek for Professional Services installation. Deltek for Professional Services must be uninstalled before Vantagepoint can be installed.
- Vantagepoint cannot be installed on existing Deltek Vision/GovWin CM/Ajera CRM or Deltek for Professional Services web/application servers. However, Vantagepoint can use the same database and report servers as Deltek Vision/GovWin CM/Ajera CRM.
- Vantagepoint supports SQL Server instances and multiple SQL Server instances on the same server.
- Vantagepoint supports using a different SQL Server instance for the Vantagepoint and Report Server databases.

Install without an Internet Connection

You can install Vantagepoint on servers without an Internet connection. Use the [DownloadSetupPrep](#) switch to download the installation files, copy the files to the server(s), and run the regular setup/upgrade switches.

Access to Weblink

To run Weblink, use the weblink.lnk shortcut in the Vantagepoint installation directory, <drive>:\Program Files\Deltek\Vantagepoint.

Permissions Required to Install Vantagepoint

If you plan to perform a Vantagepoint installation, you must have the appropriate rights and privileges.

Attention: For more information, see [How to Give Your Account Proper Rights and Privileges in Reporting Services](#).

Tier	Permissions Required
Web/Application Tier	<ul style="list-style-type: none"> Your Windows account must be a member of the Local Administrator group on the server. Your Windows account must be a member of the System Administrator group and Content Manager Roles in SQL Server Reporting Services on the report server. The setup script requires that you have a user account with sysadmin rights to connect to the database server. This can be the account that you are using to run the setup script or can be another SQL login account with sysadmin rights.
Process Server Tier	<ul style="list-style-type: none"> Your Windows account must be a member of the Local Administrator group on the server.
Report Server Tier	<ul style="list-style-type: none"> Your Windows account must be a member of the Local Administrator group on the server. Your Windows account must be a member of the System Administrator group and Content Manager Roles in SQL Server Reporting Services on the report server.
Database Server Tier	<ul style="list-style-type: none"> Your Windows account must be a member of the Local Administrator group on the server and a member of the SYSADMIN role in SQL Server.

Vantagepoint Service Account Requirements

Deltek recommends that you use domain accounts for IIS Application Pool, Vantagepoint Process Server, and database access. However, you can use local accounts. If an account doesn't exist, the Vantagepoint setup script creates a local account with a username and password that you specify.

You can choose to have the Vantagepoint installation create a local account and use that account to set up Vantagepoint server components, including configuring IIS Web Server settings, creating and launching the Vantagepoint Process Server Windows service, and running Vantagepoint reports. However, Deltek recommends that you use a domain account instead of a local account.

If you have a domain or local account policy that has stringent password requirements, the Vantagepoint installation will be unable to create the local account and you will need to manually configure the Vantagepoint server components before users can launch the application. If this happens, you will not be able to run reports.

PowerShell Script and Console

The Vantagepoint on-premises installation is built using PowerShell scripts. PowerShell is a command-line shell and scripting language, designed specifically for system administrators and power-users.

Using PowerShell as the technology for installing and deploying Vantagepoint provides a number of benefits. 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://docs.microsoft.com/en-us/powershell/scripting/powershell-scripting?view=powershell-5.1>

You will run the PowerShell script, named **DeltekVantagepoint.ps1**, multiple times, using different switches to achieve the required results. The steps that you follow depend on whether you are installing Vantagepoint from scratch or migrating to Vantagepoint from Deltek Vision, GovWin CM, or Ajera CRM.

PowerShell Console

You will run the DeltekVantagepoint.ps1 installation script from the PowerShell Console window. Launch the PowerShell console from the operating system Start menu. The location of the program in the Start menu depends on the operating system you use.

Note: DO NOT attempt to run the DeltekVantagepoint.ps1 installation script using the Windows PowerShell ISE.

Navigation and Data Entry Tips

General

- Maximize the size of the PowerShell Console for easier reading and formatting.
- Create a batch file (or use the CreateDeltekVantagepointCMDFile switch to create a batch file) that automatically launches the PowerShell Console.
- Use the [EnableWindowsExplorerPowerShellIntegration](#) switch to add a PowerShell Console right-click context menu to Windows Explorer. Do not use the **Run with PowerShell** option on the default right-click context menu to run the setup script. This option does not run commands with Administrator rights. If you use the **Run with PowerShell** option, an error message will flash quickly and the PowerShell console window will close.
- To copy/paste in the PowerShell console:
 1. Use your mouse to highlight the text that you want to copy.
 2. With the text highlighted, right-click and select **Copy**.
 3. Place the cursor where you want to paste the text, right-click and select **Paste**.

Running Scripts and Switches

- You must run a script with the period and back-slash before the script name; for example:
.\DeltekVantagepoint.ps1

- To add a switch to the script:
 - Enter a space and then a dash after **\DeltakVantagepoint.ps1**. For example:
`.\DeltakVantagepoint.ps1 -`
 - Use the Tab key to scroll through the list of available switches, or enter the switch name manually. For example:
`.\DeltakVantagepoint.ps1 --upgrade`
 - When you use the `AdditionalSetupOption`, `AdvancedSetupOption` or `SupportSetupOption` switches, you can tab through the additional setup switches. Do not enter a dash before the additional setup switch. For example, do not enter a dash before **SetServiceAccounts** here:

.\DeltakVantagepoint.ps1 --AdditionalSetupOption SetServiceAccounts

- 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 can begin entering the name of a file and then press TAB to auto-complete the entry. For example, to enter the filename **DeltakVantagepoint.ps1**, type **Del** and press TAB. If multiple options exist, tab through them until you find the correct one. The auto-completion process places the characters `.\` in front of the filename (for example, `.\DeltakVantagepoint.ps1`).
- You can also auto-complete switches. After you auto-complete the filename `.\DeltakVantagepoint.ps1`, enter a dash (-) and then press TAB to scroll through the available switches.
- If you run multiple scripts without closing the PowerShell console window, you might encounter errors or incorrect script results. To prevent this problem, the installation process checks to make sure that you close the window between scripts. If you do not, the installation process displays a message indicating that the console was not closed between setup operations and starts a new PowerShell session in the current window.

Sub-switches for Specific Configurations

- You may need to install a specific build that is different from the latest build. This might happen, for example, if you install a secondary web/app server or dedicated process server months after your initial deployment and later Vantagepoint builds have been released. You may want to install the build from your initial deployment instead of the latest one.

You can add a **--VersionToInstall** secondary switch to the `Setup`, `SetupAndMigrate`, `SetupWebApp` or `SetupProcessServer` switch, and then specify the build to install. For example:

.\DeltakVantagepoint.ps1 --Setup --VersionToInstall <version>

You do not need this secondary switch if you installed the latest build.

- Before deploying a newer build to production, you may want to setup a development or testing environment to test it, but you may want to use the same database and report servers for both

environments. Because the Vantagepoint setup routines do not have the option of specifying a report server root folder, a secondary script is needed to avoid overwriting the reports on the production report server.

You can add a **–SkipLoadReports true** parameter when running Setup, SetupAndMigrate or Upgrade switch in your development or testing environments. These switches will run all setup routines except for loading reports. After completing the the initial Setup or SetupAndMigrate switches, you can then run the LoadReports switch which will prompt you to specify the report server root folder for the development installation. Enter a different name for the root folder (not “Vantagepoint”, the default in production installation’).

Finally, once reports are loaded for your development environment, you can run the Weblink utility and change the Report Server Root entry for all databases to be the root folder specified for the development environment.

.\DeltekVantagepoint.ps1 –Setup –SkipLoadReports true

You only need this secondary switch if you have multiple environments that utilize the same report and database tiers.

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 have hung, check to see if the word **Select** is shown in the top banner of the console window (for example, **Select** Administrator: Windows PowerShell).

If you see the word **Select**, click the top bar of the console and press ENTER.

Digital Signature

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

Firewall Rules for PowerShell Remoting

The Vantagepoint 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. Remoting uses the Windows Remote Management framework service, which listens on port 5985.

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 Vantagepoint-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 a script, indicating that running scripts is disabled on your system.

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.

Prompts for Deltek Support Username and Password

Whenever you run the DeltekVantagepoint.ps1 script, the script prompts you for your Deltek Support username and password. When you enter these credentials, the script:

- Checks to see if you have rights to access Deltek Software Manager, where installation files are stored.
- Downloads any newer versions of the Vantagepoint PowerShell modules and configuration files.

You will receive an error message if you have not launched Internet Explorer for the first time for your user profile before you enter your username and password. This step is required before PowerShell can make any Invoke-WebRequest calls. To resolve the error, start Internet Explorer, complete the initialization process, and re-run the script.

Log Files

The installation creates a logs subfolder, located in the \Program Files\Deltek\Vantagepoint folder, to house the installation log and the conversion log files created for each database that was upgraded during the installation.

The logs folder contains a timestamped sub-folder for each execution of the installation script. Each subfolder includes an installation log named Vantagepoint_<date>_<time>.txt.

You may also see additional logs in each timestamped directory such as database conversion logs and logs for reloading reports.

To see which installation switch was used in a log file, search for the word **arguments** in the log file.

To find errors in the log file, select one of the following actions:

- **Server installations:** Search for the word **error** in the log file.
- **Database Upgrades:** Search for “**msg**” in the log file.

Log Files Generated During the Report-Loading Process

If there are any errors during the installation process when reloading reports, they are logged in the installation log. Resolve any errors and reload your reports manually through the application.

If there are errors, you can reload your reports by accessing the Smart Client application **Utilities » Report Administration** and clicking **Load Report Files** or by using the LoadReports switch which will load reports for all languages for the entered database.

Conversion Log

If you upgraded any databases during the installation process, the installation creates database conversion log files, which are saved in the same timestamp folder as the setup logs.

Troubleshoot Installation Problems

If you encounter problems during the Vantagepoint installation on the server and are unable to continue, contact Deltek Customer Care for assistance and include the following information:

- The timestamped setup log stored in the **installation directory\logs** folder on the Vantagepoint server.
- Screenshots and details about the errors received.

Note: A Deltek Customer Care analyst might ask you to use the [SendLogsToDeltek](#) switch, which will zip and email the logs directly. This information will help Deltek resolve your issue as quickly as possible.

System Requirements

Some parts of the Vantagepoint application are distributed to logical tiers for performance, scalability, and security purposes. These logical tiers are distinct technologies required to run Vantagepoint, such as report server software or web server software. They may or may not be hosted on the same machine. The method that you use to distribute the Vantagepoint logical tiers across physical tiers or actual machines depends on your organization's needs.

Note: The software requirements for each logical tier are listed in the [Deltek Support Compatibility Matrix](#).

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.

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

Software Requirements

Before you install Vantagepoint, you must have the following software and configurations in place. Although every attempt is made to keep these prerequisites up to date, Deltek recommends that you verify them against the Deltek Platform Compatibility Matrix, which always has the latest compatibility information:

https://deltek.custhelp.com/app/answers/detail/a_id/38499

Supported Versions and Compatible Versions

The Platform Compatibility Matrix list both supported versions and compatible versions. Supported versions are the most current, actively tested technologies used to deploy Vantagepoint.

Compatible versions are recent technologies that have been tested and used for deploying Vantagepoint in the past, but are not currently being tested. Deltek believes that they are still compatible with Vantagepoint.

Component	Requirements
Operating System	<ul style="list-style-type: none">Windows Server 2019,Windows Server 2016, orWindows Server 2012 R2 (Windows Server 2012 is not supported.)

Component	Requirements
SQL Server	<ul style="list-style-type: none"> SQL Server 2019 plus currently supported SQL Cumulative Update* SQL Server 2017 plus currently supported SQL Cumulative Update* or SQL Server 2016 SP2 plus currently supported SQL Cumulative Update* <p>* See Deltek's Platform Support Compatibility Matrix for currently supported SQL Server Cumulative Updates.</p>
SQL Server Reporting Services	<ul style="list-style-type: none"> SQL Server Reporting Services 2019 SQL Server Reporting Services 2017 Beginning with the release of SQL Server 2017, Microsoft is shipping Reporting Services as a stand-alone product. SQL Server Cumulative Updates no longer apply to Reporting Services. Microsoft distributes only the most recent full release, which include all fixes and updates. <p>Note that there are separate downloads for the 2017 and 2019 versions of Reporting Services.</p>
SQL Server FileStream	<ul style="list-style-type: none"> SQL Server FileStream must be installed and configured. <p>See Configure Transaction Document Management for more information.</p>
PowerShell	<ul style="list-style-type: none"> PowerShell Version 5.1 (installed by default on Server 2016). Download Version 5.1 for Windows Server 2012 from: https://www.microsoft.com/en-us/download/details.aspx?id=54616 To check your version, run the PowerShell Console as an administrator and enter <code>\$PSVersionTable.PSVersion</code> PowerShell 6.x or 7 is not supported. The Deltek Vantagepoint PowerShell installation must be run using the Windows PowerShell Console, not the Windows PowerShell ISE (Integrated Scripting Environment). See Considerations for Running the PowerShell Script for more information. Do not use the Run with PowerShell option on the default right-click context menu to run the script. This option does not run commands with Administrator rights. If you want to add a Windows Explorer right-click option, use the EnableWindowsExplorerPowerShellIntegration switch to enable the Open Windows PowerShell Here as Administrator menu option. This option displays in the right-click menu in Windows Explorer.
.NET Framework	<ul style="list-style-type: none"> .NET 4.7.2 or higher (.NET Core is not supported.)
Internet Information Services (IIS)	<ul style="list-style-type: none"> IIS is required only on the web/application server. <p>See Microsoft Internet Information Server (IIS) Installation on Windows Server for more information</p>

Component	Requirements
Secure Sockets Layer (SSL)	<ul style="list-style-type: none"> A valid SSL certificate with resolvable fully qualified domain name must be installed and configured on both the web server (IIS) and the report server for the installation to proceed. You can use a self-signed certificate for local single server installation testing only. <p>See Configure Secure Sockets Layer (SSL) for more information.</p>
Transport Layer Security (TLS)	<ul style="list-style-type: none"> TLS 1.2 is required. Older TLS/SSL protocols must be disabled on all Vantagepoint tiers: <ul style="list-style-type: none"> TLS 1.1/1.0 must be disabled. SSL 2.0/3.0 must be disabled. Once these protocols are disabled, you must restart your server. You can also use the IISCrypto tool by Nartac Software to disable these older protocols. <p>For more information on why Deltek is requiring these protocols to be disabled, see the following article: https://blog.pcisecuritystandards.org/are-you-ready-for-30-june-2018-sayin-goodbye-to-ssl-early-tls</p> <p>See this article for more information about disabling protocols: 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</p>
Visual C++ Runtime	<ul style="list-style-type: none"> Necessary for mobile applications.

Prerequisite Checks Run Automatically

Every time that you run the setup script, regardless of the switches that you use, the script checks that prerequisites are in place. The script performs the following prerequisite checks:

- The script verifies that the installation directory is valid.
- The script prompts you for your support username and password and validates them before continuing.
- The script downloads the DeltekVantagepointSettings.xml file, if it is missing.
This file stores information about the setup, is server-specific, and is persistent from release to release. You should **not** change this file unless Deltek support asks you to change it.
- The script downloads the latest Vantagepoint PowerShell Modules.
- The script checks to ensure that the latest DeltekVantagepoint.ps1 script is being used. If not, it downloads the latest script and prompts you to restart setup.
- The scripts checks script prerequisites, including:
 - Operating system
 - .NET Framework

- PowerShell
 - Windows Remote Management service is running
 - TLS configuration
 - SSL 2.0/3.0 and TLS 1.0/1.1 have been disabled
 - Microsoft Visual C++ Runtime
7. If any third-party software prerequisite 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\Vantagepoint\Support\PreReq
8. Every time the script is run, it downloads the DeltekVantagepointConfiguration.xml file and overwrites any existing version of this file. The file stores meta-information about releases that the script uses to derive release, version, configuration, and dependency information. You should not change this file unless Deltek support asks you to change it.
9. The script gathers information about the user running the script, the server, and the domain.
10. The script checks for an existing installation of Vantagepoint and provides information about the currently available software version.

SQL Server Database Requirements

You must have a Microsoft SQL Server database engine to run Vantagepoint. The Microsoft SQL Server edition that you choose to deploy with Vantagepoint depends on a number of factors, such as the size of your database and the number of employees actively using the application, which can impact database server performance.

- For firms with fewer than 50 employees, Vantagepoint supports Microsoft SQL Server Express Edition with Advanced Services, which has a database size limitation of 10 GB, 1 GB maximum utilized RAM, and is limited to the lesser of 1 CPU socket or four cores.

See this Microsoft article to learn about other limitations of this edition:

[https://msdn.microsoft.com/en-us/library/cc645993\(v=sql.120\).aspx](https://msdn.microsoft.com/en-us/library/cc645993(v=sql.120).aspx)

- For firms with more than 50 employees, Vantagepoint supports Microsoft SQL Server Standard and Enterprise Edition.

The machine on which you install Microsoft SQL Server depends on your firm's deployment model.

SQL Server Standard or Enterprise Edition

- If you decide to split the report server (web service) from the database server hosting the report server database, you need an additional Microsoft SQL Server license.
- Report server scale-out deployment is only available in Enterprise Edition. A scale-out deployment is an installation configuration that has multiple report server instances sharing a single report server database.
- 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://msdn.microsoft.com/en-us/library/cc645993\(v=sql.120\).aspx](https://msdn.microsoft.com/en-us/library/cc645993(v=sql.120).aspx)

SQL Server Express Edition with Advanced Services

Owners of SQL Server Express Edition with Advanced Services (SQL Server Express) should note the following:

- The report server database must be hosted on the local machine running the SQL Server database engine instance. You cannot use a remote SQL Server instance to host the report server database.
- Any data sources that you use for reporting must be SQL Server databases that run on the same local machine that runs the SQL Server database engine instance. You cannot use remote data sources or other data source types. To use additional data source types, you must use a different edition of Reporting Services. This means that your Vantagepoint database must reside on the same machine as your report server databases.
- Use the Single Server Deployment Model or Configuration 1 of the Two Server Deployment Model.

SQL Server Express Edition Requirement

If you are implementing SQL Server Express Edition, Deltek requires that you use SQL Server Express Edition with Advanced Services as the database and report server for your Vantagepoint implementation. It contains the database engine and reporting services required to manage the database and run reports.

The other SQL Express Edition installers do not have all the components needed to support Vantagepoint.

Communication between Vantagepoint and the SQL Server Database

See the notes below about how to set up Vantagepoint to communicate with the SQL Server database.

- The Vantagepoint installer creates a Microsoft SQL Server logon account for the Vantagepoint database. The account requires the db_owner database role membership in the Login Properties and User Mapping dialog box for the following databases:
 - Vantagepoint database
 - ReportServer and ReportServerTempDB databases

Attention: For more information and guidance on configuring rights, see [How to Give Your Account Proper Rights and Privileges in Reporting Services Web Services](#).

- Use SQL Server Configuration Manager to enable the TCP/IP and Shared Memory network protocols on the Microsoft SQL Server to allow Vantagepoint to connect to the database. All network protocols are installed by SQL Server Setup, but may or may not be enabled.

Attention: For details, see the article [Enable or Disable a Server Network Protocol \(SQL Server Configuration Manager\)](#).

- Verify the name of your SQL Server Instance. The default installation uses the server name for the connection and installs as an instance named MSSQLSERVER. Sometimes SQL Server is installed using an instance name other than the default (MSSQLSERVER). The SQL Server Express Edition installer from Microsoft installs as the named instance SQLEXPRESS.

Note:

- When you connect to the default SQL Server database engine instance, you use the name of your database server. When accepting connections, SQL Server automatically maps the default instance of the database engine to the server name.
- When connecting to a named instance of the SQL Server database engine, you must specify the name of the SQL Server plus the instance in the connection in the format **SERVERNAME\INSTANCENAME**.

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

- 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 [Determine Whether the Database Engine Is Installed and Started](#).
- Vantagepoint supports both SQL Server authentication modes: **Windows Authentication Only** or **SQL Server and Windows Authentication** (also known as Mixed Mode).

If you are unable to connect to your SQL database server and you have already performed the steps in the first two bullets of this list, you should verify that the SQL Server security settings are properly configured.

Attention: For details, see the article [Change Server Authentication Mode](#).

- If you experience connection errors to your database or report server and have verified the previous steps, verify that Windows (or your) firewall is not blocking access to the SQL Server database engine and reporting services.

Attention: See the following Microsoft article for detailed steps:

- [Configure a Firewall for Report Server Access](#)
- [Configure a Windows Firewall for Database Engine Access](#)

Multiple Languages

You can install a blank Vantagepoint database on your database server. By default, all languages are enabled and available via the Vantagepoint login. You can select your desired language from the login page language drop-down list. Reports for all languages are installed by default.

You can select from these languages:

- English (United States or International)
- France (Canada or France)
- Spanish
- Dutch (Netherlands)
- Portuguese (Brazil)
- German

Database Maintenance Activities

Deltek recommends that you complete the following activities on your database on a regular basis (daily or weekly):

1. Check the integrity of the database.
2. Optimize the database by doing the following:
 - a. Defragment heap tables.
 - b. Rebuild indexes. You cannot rebuild indexes daily, but it is recommended that you do so on a regular basis.
 - c. Update statistics.

You can download a script from the Deltek Support Center to help you with this step. For more information, refer to this [KB article](#).
3. Make a complete back up of the database.

Note: In addition to regular intervals, you should perform the maintenance activities after large data imports that include major changes to the data. This includes application migration or major releases of the software that require you to apply database update scripts to the database.

Research the following topics in Microsoft Support and other relevant sources when creating your maintenance plans:

- [Microsoft SQL Server Maintenance Plans](#)
- [SQL Server Maintenance Solution](#)

Users of SQL Server Express Edition

If you are using SQL Server Express Edition, you cannot use SQL Maintenance Studio to create maintenance jobs or schedule jobs because it does not include the SQL Server Agent service.

Refer to the following to create stored procedures and scripts to accomplish maintenance plan activities:

- [Microsoft SQL Server Maintenance Plans](#)
- [SQL Server Maintenance Solution](#)
- Articles on Microsoft Support about creating a Windows scheduled task that works with SQL stored procedures
- [How to Schedule and Automate Backups of SQL databases in SQL Server Express](#)
- A [KB article](#) on Deltek Support Center about using a script to optimize the database.

.NET Architecture

The Vantagepoint server-side architecture uses the Microsoft .NET Framework, a set of software technologies developed to connect information, people, systems, and devices.

.NET allows Deltek developers and your in-house IT staff to extend the Vantagepoint workflow capabilities by calling outside web services from within Vantagepoint. For example, you may send real-time, updated project information from Vantagepoint to an external collaboration web site so that your clients can view current project information.

System Requirements

.NET makes it possible for you to develop applications that integrate with Vantagepoint, call web services from within Vantagepoint, and communicate with Vantagepoint through mobile devices.

Vantagepoint requires the Microsoft .NET Framework version specified in the [Software Requirements](#) section.

Upgrade Scenarios for Vantagepoint 4.5

Upgrading from Vision, GovWin CM, or Ajera CRM 7.6

Use the -SetupandMigrate and -MigrateDatabases switches to upgrade Vision, Ajera CRM, or GovWin CM 7.6 databases to Vantagepoint 4.5.

Upgrading from Vantagepoint 2.0.x through 4.0.x

- Use the -Upgrade switch to migrate directly from Vantagepoint 4.0.x to 4.5.
- Use the -Upgrade switch and the -UpgradeDatabase switch to migrate Vantagepoint 3.0.6 or higher databases to Vantagepoint 4.5. This upgrade has a three-step process:
 1. Upgrade the database from Vantagepoint 3.0.6 to 3.5.
 2. Upgrade the database from Vantagepoint 3.5 to 4.0.
 3. Upgrade the database from Vantagepoint 4.0 to 4.5.
- Use the -Upgrade switch and the -UpgradeDatabase switch to upgrade all other databases at a version lower than Vantagepoint 3.0.6 (Vantagepoint 2.0.x through 3.0.5). This upgrade has a four-step process:
 1. Upgrade the database to Vantagepoint 3.0.6
 2. Upgrade the database from Vantagepoint 3.0.6 to 3.5.
 3. Upgrade the database from Vantagepoint 3.5 to 4.0.
 4. Upgrade the database from Vantagepoint 4.0 to 4.5.
- Use the -ValidateDatabases switch to view a summary of the required steps for each database in databases.enc.

The same summary is displayed after you run the -Upgrade and -UpgradeDatabases switches.

The following table provides specific steps for upgrading to Vantagepoint 4.5:

Scenario	DeltekVantagepoint.ps1 Switch
Migrating from Vision / GovWin CM / Ajera CRM 7.6	Use -SetupAndMigrate or --MigrateDatabase
Upgrading from Vantagepoint 3.0.5 or earlier maintenance release	1. -Upgrade 2. -UpgradeDatabase for each database that needs to be upgraded to Vantagepoint 4.5
Upgrading from Vantagepoint 3.0.6 or higher or Vantagepoint 3.5 or higher maintenance release	3. -Upgrade 4. -UpgradeDatabase for each database that needs to be upgraded to Vantagepoint 4.5
Upgrading from Vantagepoint 4.0.x	-Upgrade or -UpgradeDatabases

Upgrade Scenarios for Vantagepoint 4.0

Upgrading from Vision, GovWin CM, or Ajera CRM 7.6

Use the -SetupandMigrate and -MigrateDatabases switches to upgrade Vision, Ajera CRM, or GovWin CM 7.6 databases to Vantagepoint 4.0.

Upgrading from Vantagepoint 2.0.x through 3.5.x

- Use the -Upgrade switch to directly migrate from Vantagepoint 3.5x to 4.0.
- Use the -Upgrade switch and the -UpgradeDatabase switch to migrate Vantagepoint 3.0.6 or higher databases to Vantagepoint 4.0. This upgrade has a two-step process:
 5. Upgrade the database from Vantagepoint 3.0.6 to 3.5.
 6. Upgrade the database from Vantagepoint 3.5 to 4.0.
- Use the -Upgrade switch and the -UpgradeDatabase switch to upgrade all other databases at a lower version than Vantagepoint 3.0.6 (Vantagepoint 2.0.x through 3.0.5). This upgrade has a three-step process:
 7. Upgrade the database to Vantagepoint 3.0.6
 8. Upgrade the database from Vantagepoint 3.0.6 to 3.5.
 9. Upgrade the database from Vantagepoint 3.5 to 4.0.
- Use the -ValidateDatabases switch to view a summary of the required steps for each database in databases.enc.

The same summary is displayed after you run the -Upgrade and -UpgradeDatabases switches.

The following table provides specific steps for upgrading to Vantagepoint 4.0:

Scenario	DeltekVantagepoint.ps1 Switch
Migrating from Vision / GovWin CM / Ajera CRM 7.6	Use -SetupAndMigrate or --MigrateDatabase
Upgrading from Vantagepoint 2.0.x (any maintenance release)	<ol style="list-style-type: none"> 1. -Upgrade 2. -UpgradeDatabase for each database that needs to be upgraded to Vantagepoint 4.0
Upgrading from Vantagepoint 3.0.5 or earlier maintenance release	<ol style="list-style-type: none"> 5. -Upgrade 6. -UpgradeDatabase for each database that needs to be upgraded to Vantagepoint 4.0
Upgrading from Vantagepoint 3.0.6 or higher maintenance release	<ol style="list-style-type: none"> 7. -Upgrade 8. -UpgradeDatabase for each database that needs to be upgraded to Vantagepoint 4.0
Upgrading from Vantagepoint 3.5.x	-Upgrade or -UpgradeDatabases

Important Note for Vantagepoint 4.0 Upgrades

With the release of Vantagepoint 4.0, the current web configuration file in <drive>:\Program Files\Deltek\Vantagepoint\Web is replaced with a new version. During the upgrade, your current web configuration file is backed up and assigned this filename: web<date_timestamp>.config.

In addition, Vantagepoint looks for changes on standard configuration options after installation and notifies you of such changes, specifically:

- The addition of a **<machineKey>** tag in the <system.web> section. This tag only exists for customers that are balancing load across multiple Vantagepoint web servers. After the upgrade, copy the tag from the generated backup file to avoid errors.
- The addition of the DatabasesEncDirectory <appSetting> tag. This tag is commented out unless you have configured a Shared Databases Enc Path. After the upgrade, copy the tag from the generated backup file to allow users to login to Vantagepoint.
- Changes to the <httpRuntime> tag for the executionTimeout (default value is 900) and maxRequestLength (default value is 128,000). The current values of these configuration settings are pointed out during the upgrade.

Upgrade Scenarios for Vantagepoint 3.5

Use the -SetupandMigrate and -MigrateDatabases switches to upgrade databases to Vantagepoint 3.5.

Upgrading from Vantagepoint 2.0.x and 3.0.x

- Before upgrading to a major version of Vantagepoint (for example, from Vantagepoint 3.0 to 3.5), you must first run the SetVersion switch before running the Upgrade switches.
- Use the -Upgrade switch to directly migrate Vantagepoint 3.0.6 or higher databases to Vantagepoint 3.5 during the upgrade process.
- Use the new -UpgradeDatabase switch to upgrade all other databases at a lower version than Vantagepoint 3.0.6 (Vantagepoint 2.0.x through 3.0.5).

The switch has a two-step process:

- Upgrade the database to Vantagepoint 3.0.6
- Upgrade the Vantagepoint 3.0.6 database to 3.5.
- Use the new -ValidateDatabases switch to view a summary of the required steps for each database in databases.enc.

The same summary is displayed after you run the -Upgrade and -UpgradeDatabases switches.

The following table provides specific steps for upgrading to Vantagepoint 3.5:

Scenario	DeltekVantagepoint.ps1 Switch
Migrating from Vision / GovWin CM / Ajera CRM 7.6	Use -SetupAndMigrate or --MigrateDatabase
Upgrading from Vantagepoint 2.0.x (any maintenance release)	<ol style="list-style-type: none"> 1. -SetVersion 2. -Upgrade 3. -UpgradeDatabase for each database that needs to be upgraded to Vantagepoint 3.5
Upgrading from Vantagepoint 3.0.5 or earlier maintenance release	<ol style="list-style-type: none"> 1. -SetVersion 2. -Upgrade 3. -UpgradeDatabase for each database that needs to be upgraded to Vantagepoint 3.5
Upgrading from Vantagepoint 3.0.6 or later	<ol style="list-style-type: none"> 1. -SetVersion 2. -Upgrade or -UpgradeDatabases

Pre- and Post-Installation Checklists

Pre-Installation General Checklist

Before starting with your server checklist, review the following:

- All tiers must have a resolvable, fully qualified domain name (FQDN).
- A valid SSL certificate must be installed on the web/application server and report server. If Vantagepoint is only used internally, the certificate can be generated by an internal certificate authority. If Vantagepoint is used externally, the certificate must be generated by a third-party certificate authority, such as Verisign or DigiCert.
- HTTPS and TLS 1.2 are required. SSL 2.0/3.0 and TLS 1.0/1.1 must be disabled. For more information about disabling SSL 2.0/3.0 and TLS 1.0/1.1, read this article:
<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>
You can also use the [IISCrypto](#) tool by Nartac Software to disable older protocols.
- [PowerShell Remoting](#) must be enabled on all tiers.
- The Vantagepoint setup scripts are signed and will not run if they are changed.
- If you are migrating from Deltek Vision, GovWin CM, or Ajera CRM, make sure that you have a valid backup and have tested a restore of your Vision/GovWin CM/Ajera CRM database. Perform a test migration before your final migration. Before proceeding, see [Upgrade Scenarios for Vantagepoint 4.5](#).

Note: Before you begin migrating, you must remove all custom database objects (indexes, triggers, and so on).

- If you are migrating from Deltek Vision, GovWin CM, or Ajera CRM, you must be on version 7.6 (CU9) or later. Before proceeding, see [Upgrade Scenarios for Vantagepoint 4.5](#).
- Vantagepoint supports both SQL Server authentication modes: **Windows Authentication Only** mode or **SQL Server and Windows Authentication** mode (also known as "Mixed Mode").
- Set up a dedicated web/application server. You can use an existing report and database server if they meet operating system and SQL requirements.
- You should know:
 - The fully qualified domain names for your web/application and report servers.
 - The service accounts that you will use for your IIS Application Pool Identity and Vantagepoint process server.
 - How you will connect to your database server (Windows Integration or SQL logon) with sysadmin rights.
 - What SQL logon you will use for Vantagepoint access.

Pre-Installation Server Checklists

Follow the appropriate checklist to configure your Vantagepoint servers, depending on your installation model:

- [Single Server](#)
- [Dual-Server \(Two Tier\) Configuration 1](#)
- [Dual-Server \(Two Tier\) Configuration 2](#)
- [Three or More Servers](#)

Single-Server

Step	Description	Related Topics
1.	Verify that the server operating system is supported.	▪ System Requirements
2.	Verify that you have at least 2 GB of disk space available for this installation.	
3.	Verify that the user account performing the installation is a member of the local Windows System Administrators group.	
4.	Verify that your SQL Server Database Engine and Reporting Services installations meet the system requirements.	▪ Database Requirements
5.	Verify that the user account performing the installation is a member of the sysadmin role in SQL Server security settings, or make sure that you have valid SQL Server credentials available for use during the installation.	
6.	Use SQL Server Configuration manager to ensure that the TCP/IP and Shared Memory protocols are enabled.	▪ Enable or Disable a Server Network Protocol (SQL Server Configuration Manager)
7.	Install Microsoft .NET Framework.	▪ .NET Architecture
8.	Install Microsoft Internet Information Services (IIS) with ASP .NET enabled.	▪ Microsoft Internet Information Server (IIS) Installation on Windows Server
9.	Configure Reporting Services with native mode.	▪ Microsoft SQL Server Reporting Services
	If Reporting Services is already configured, you will need to know the Web Service URL and the name of the Report Server databases.	▪ How to Connect to the Report Service Web Service

Step	Description	Related Topics
10.	Verify that the user account has the proper rights and privileges in Reporting Services.	<ul style="list-style-type: none"> ▪ How to Give Your Account Proper Rights and Privileges in Reporting Services Web Services
11.	If you experience connection errors to SQL Reporting Services and have verified the previous steps, check that access is not being blocked by Windows or your firewall.	<ul style="list-style-type: none"> ▪ Configure a Firewall for Report Server Access ▪ Configure a Windows Firewall for Database Engine Access
12.	Review the Web Server Post-Installation checklist .	

Dual-Server (Two-Tier) Configuration 1

Database and Report Tier

Step	Description	Related Topics
1.	Verify that the server operating system is supported.	<ul style="list-style-type: none"> ▪ System Requirements
2.	Verify that you have at least 2 GB of disk space available for this installation.	
3.	Verify that the user account performing the installation is a member of the local Windows System Administrators group.	
4.	Verify that your SQL Server Database Engine and Reporting Services installations meet the system requirements.	<ul style="list-style-type: none"> ▪ System Requirements
5.	Verify that the user account performing the installation is a member of the sysadmin role in SQL Server security settings, or make sure that you have valid SQL Server credentials available for use during the installation.	
6.	Use SQL Server Configuration manager to ensure that the TCP/IP and Shared Memory protocols are enabled on your report server and database server.	<ul style="list-style-type: none"> ▪ Enable or Disable a Server Network Protocol (SQL Server Configuration Manager)
7.	Configure Reporting Services with native mode.	<ul style="list-style-type: none"> ▪ Microsoft SQL Server Reporting Services
	If Reporting Services is already configured, you will need to know the Web Service URL and the name of the Report Server databases.	<ul style="list-style-type: none"> ▪ How to Connect to the Report Service Web Service

Step	Description	Related Topics
8.	Verify that the user account performing the installation has the proper rights and privileges in Reporting Services.	<ul style="list-style-type: none"> How to Give Your Account Proper Rights and Privileges in Reporting Services Web Services
9.	If you experience connection errors to your database or report server and have verified the previous steps, check that access is not being blocked by Windows or your firewall.	<ul style="list-style-type: none"> Configure a Windows Firewall for Database Engine Access

Web Application and Process Server Tier

Step	Description	Related Topics
1.	Verify that the server operating system is supported.	<ul style="list-style-type: none"> System Requirements
2.	Verify that you have at least 2 GB of disk space available for this installation.	
3.	Install Microsoft .NET Framework.	<ul style="list-style-type: none"> .NET Architecture
4.	Install Microsoft Internet Information Services (IIS) with ASP .NET enabled.	<ul style="list-style-type: none"> Microsoft Internet Information Server (IIS) Installation on Windows Server
5.	Verify that the user account performing the installation has the proper account credentials as stated in the database and report tier steps.	
6.	Ensure that you have the following information prior to starting your installation: <ul style="list-style-type: none"> Database Server\SQL instance name Report Server database names Report Server Web Service URL 	<ul style="list-style-type: none"> Database Requirements
7.	Review the Web Server Post-Installation checklist .	

Dual-Server (Two-Tier) Configuration 2

Database Tier

Step	Description	Related Topics
1.	Verify that the server operating system is supported.	<ul style="list-style-type: none"> System Requirements
2.	Verify that you have at least 2 GB of disk space available for this installation.	
3.	Verify that the user account performing the installation is a member of the local Windows System Administrators group.	
4.	Verify that your SQL Server Database Engine and Reporting Services installations meet the system requirements.	<ul style="list-style-type: none"> System Requirements
5.	Verify that the user account performing the installation is a member of the sysadmin role in SQL Server security settings, or make sure that you have valid SQL Server credentials available for use during the installation.	
6.	Use SQL Server Configuration manager to ensure that the TCP/IP and Shared Memory protocols are enabled on your report server and database server.	<ul style="list-style-type: none"> Enable or Disable a Server Network Protocol (SQL Server Configuration Manager)
7.	If you experience connection errors to your database and have verified the previous steps, check that access is not being blocked by Windows or your firewall.	<ul style="list-style-type: none"> Configure a Windows Firewall for Database Engine Access

Web Application and Report Tier

Step	Description	Related Topics
1.	Verify that the server operating system is supported.	<ul style="list-style-type: none"> System Requirements
2.	Verify that you have at least 2 GB of disk space available for this installation.	
3.	Install Microsoft .NET Framework.	<ul style="list-style-type: none"> .NET Architecture
4.	Install Microsoft Internet Information Services (IIS) with ASP .NET enabled.	<ul style="list-style-type: none"> Microsoft Internet Information Server (IIS) Installation on Windows Server

Step	Description	Related Topics
5.	Ensure that you have the SQL Server username and password that you created for Reporting Services.	<ul style="list-style-type: none"> Prerequisite Report Server and SQL Server Database Credentials
6.	Configure Reporting Services with native mode.	<ul style="list-style-type: none"> Microsoft SQL Server Reporting Services
	If Reporting Services is already configured, you will need to know the Web Service URL and the name of the Report Server databases.	<ul style="list-style-type: none"> How to Connect to the Report Service Web Service
7.	Verify that the user account has the proper rights and privileges in Reporting Services.	<ul style="list-style-type: none"> How to Give Your Account Proper Rights and Privileges in Reporting Services Web Services
8.	Verify that the user account performing the installation is a member of the sysadmin role in SQL Server security settings.	
9.	Verify that your SQL Server Reporting Services installation meets the system requirements.	<ul style="list-style-type: none"> System Requirements
10.	Use SQL Server Configuration manager to ensure that the TCP/IP and Shared Memory protocols are enabled on your report server and database server.	<ul style="list-style-type: none"> Enable or Disable a Server Network Protocol (SQL Server Configuration Manager)
11.	If you experience connection errors to your database or report server and have verified the previous steps, check that access is not being blocked by Windows or your firewall.	<ul style="list-style-type: none"> Configure a Firewall for Report Server Access Configure a Windows Firewall for Database Engine Access
12.	Review the Web Server Post-Installation checklist .	

Three or More Servers

Database Tier

Step	Description	Related Topics
1.	Verify that the server operating system is supported.	<ul style="list-style-type: none"> System Requirements
2.	Verify that you have at least 2 GB of disk space available for this installation.	

Pre- and Post-Installation Checklists

Step	Description	Related Topics
3.	Verify that the user account performing the installation is a member of the local Windows System Administrators group.	
4.	Verify that your SQL Server Database Engine and Reporting Services installations meet the system requirements.	<ul style="list-style-type: none"> ▪ System Requirements
5.	Verify that the user account performing the installation is a member of the sysadmin role in SQL Server security settings, or make sure that you have valid SQL Server credentials available for use during the installation.	
6.	Use SQL Server Configuration manager to ensure that the TCP/IP and "Shared Memory" protocols are enabled on your report server and database server.	<ul style="list-style-type: none"> ▪ Enable or Disable a Server Network Protocol (SQL Server Configuration Manager)
7.	If you experience connection errors to your database and have verified the previous steps, check that access is not being blocked by Windows or your firewall.	<ul style="list-style-type: none"> ▪ Configure a Windows Firewall for Database Engine Access

Report Tier

Step	Description	Related Topics
1.	Verify that the server operating system is supported.	<ul style="list-style-type: none"> ▪ System Requirements
2.	Verify that you have at least 2 GB of disk space available for this installation.	
3.	Verify that the user account performing the installation is a member of the local Windows System Administrators group.	
4.	Verify that the user account has the proper rights and privileges in Reporting Services.	<ul style="list-style-type: none"> ▪ How to Give Your Account Proper Rights and Privileges in Reporting Services Web Services
5.	Verify that the user account performing the installation is a member of the sysadmin role in SQL Server security settings.	
6.	Verify that your SQL Server Database Engine and Reporting Services installations meet requirements.	<ul style="list-style-type: none"> ▪ System Requirements

Step	Description	Related Topics
7.	Use SQL Server Configuration manager to ensure that the TCP/IP and Shared Memory protocols are enabled on your report server and database server.	<ul style="list-style-type: none"> ▪ Enable or Disable a Server Network Protocol (SQL Server Configuration Manager)
8.	Configure Reporting Services with native mode.	<ul style="list-style-type: none"> ▪ Microsoft SQL Server Reporting Services
	If Reporting Services is already configured, you will need to know the Web Service URL and the name of the Report Server databases.	<ul style="list-style-type: none"> ▪ How to Connect to the Report Service Web Service
9.	If you experience connection errors to your report server and have verified the previous steps, check that access is not being blocked by Windows or your firewall.	<ul style="list-style-type: none"> ▪ Configure a Firewall for Report Server Access

Web / Application Tier

Step	Description	Related Topics
1.	Verify that the server operating system is supported.	<ul style="list-style-type: none"> ▪ System Requirements
2.	Verify that you have at least 2 GB of disk space available for this installation.	
3.	Install Microsoft .NET Framework.	<ul style="list-style-type: none"> ▪ .NET Architecture
4.	Install Microsoft Internet Information Services (IIS) with ASP .NET enabled.	<ul style="list-style-type: none"> ▪ Microsoft Internet Information Server (IIS) Installation on Windows Server
5.	Verify that the user account performing the installation has the proper account credentials as stated in the database and report tier steps.	
6.	Ensure that you have the following information prior to starting your installation: <ul style="list-style-type: none"> ▪ Database Server\SQL instance name ▪ Report Server database names ▪ Report Server Web Service URL 	<ul style="list-style-type: none"> ▪ Database Requirements
7.	Note the Vantagepoint installation location on your web server. You will need this information for the Process Server tier.	
8.	Review the Web Server Post-Installation checklist .	

Process Server Tier

Step	Description	Related Topics
1.	Verify that the server operating system is supported.	<ul style="list-style-type: none"> ▪ System Requirements
2.	Verify that you have at least 2 GB of disk space available for this installation.	
3.	Install Microsoft .NET Framework.	<ul style="list-style-type: none"> ▪ .NET Architecture
4.	Verify the location (path) of the existing databases.enc file on your web server. During the installation, you will need to provide the Shared Path to Databases.enc or you will need to copy this file from the web/application server after installation. The default location of this file is: <drive>:\Program Files\Deltek\Vantagepoint\.	
5.	Review the Dedicated Process Server Post-Installation checklist .	

Post-Installation Checklist (New Installations)

After you finish installing Vantagepoint for the first time, follow these steps.

If you just finished installing an update, follow the steps in [Post-Installation Checklist \(Upgrades\)](#) instead.

Web Server

Step	Description
1.	Use Weblink to test your database and reporting services connections. Launch and log in to the Weblink utility on the Vantagepoint web/application server, using the shortcut created in the Vantagepoint installation folder.
2.	In Weblink, click the System Settings tab and review the Polling Interval and Max Concurrent Jobs field settings to confirm that they meet your needs.
3.	<p>If you have a dedicated process server machine:</p> <ol style="list-style-type: none"> On the web server, navigate to Control Panel » Administrative Tools and disable the Deltek Vantagepoint Process Server service. Launch Vantagepoint, add the name of the process server, and then assign queues to the server that you inserted. Click Configuration » System Settings. On the Servers tab, add the name of your process server. Assign the process queues to that process server.

Step	Description
4.	<ul style="list-style-type: none"> For new installations, perform the post-installation steps for new installations. For upgrade installations, perform the post-installation steps for upgrades.
5.	Verify that you can perform Database Maintenance Activities. See Database Maintenance Activities for more information.

Warning: Deltek recommends that the total of all of the process queues (per server) does not exceed the number in the **Max Concurrent Jobs** field.

Set the process queue maximum in the Max field in the Process Queues grid in **Settings » General » Process Servers**.

If the total of all of your process queues (per server) exceeds the number in the **Max Concurrent Jobs** field, only the number of jobs as specified in that field run concurrently. If you run too many concurrent jobs, you will add load to your database server and/or report server.

Dedicated Process Server

See Step 2 of the **Web Server Post-installation Checklist** above to add and configure dedicated process servers in Vantagepoint.

Client Tier (Workstation)

Step	Description
1.	Supply Vantagepoint users with the Vantagepoint URL: https://servername/Vantagepoint . Replace servername in the URL with your server name.
2.	<p>When you launch Vantagepoint, the credentials for new production databases are:</p> <ul style="list-style-type: none"> Username: SETUP Password: <no password> <p>When you enter these credentials, the Vantagepoint activation process begins automatically.</p> <p>The credentials for sample databases are:</p> <ul style="list-style-type: none"> Username: ADMIN Password: <no password>

Post-Installation Checklist (Upgrades)

After you finish installing an update to Vantagepoint, follow these steps.

If you have just finished installing Vantagepoint for the first time, follow the steps in [Post-Installation Checklist \(New Installations\)](#) instead.

Web Server

Step	Description
1.	Verify that you can view VisionServices (http://localhost/Vantagepoint/VisionServices.aspx).
2.	Verify that you can launch and run Weblink.
3.	Verify that you can launch and run Vantagepoint.
4.	Verify that the Process Server Windows Service is running.
5.	Verify that you can perform Database Maintenance Activities. See Database Maintenance Activities for more information.

Dedicated Process Server

See Steps in the [Web Server Post-installation Checklist \(Upgrades\)](#) to add and configure dedicated process servers in Vantagepoint.

Installing Vantagepoint

Overview

Note: If you are installing Vantagepoint on servers that do not have Internet access, download the DeltekVantagepoint.ps1 Powershell script to your Download Server, run the DownloadSetupPrep switch, copy the files to your installation servers, and perform the remaining steps to complete the setup or upgrade. See the [DownloadSetupPrep switch](#) instructions for more information.

Follow these steps to install Vantagepoint.

Step	Description	Read this section:
1.	Make sure that you have all prerequisites in place.	Prerequisites
2.	Download the DeltekVantagepoint.ps1 PowerShell script.	Download the PowerShell Script
3.	Run the script, using no switches, to set up the installation environment and to check that the script prerequisites are in place.	Considerations for Running the PowerShell Script Run the Script with No Switches
4.	Re-run the script, using the CheckPreReq switch, to make sure that the product/software prerequisites are in place	Run the Script with the CheckPreReq Switch
5.	Re-run the script, using one of the following switches: <ul style="list-style-type: none"> ▪ Setup: If you are installing Vantagepoint and creating a completely new Vantagepoint database. ▪ SetupAndMigrate: If you are installing Vantagepoint and migrating your existing Deltek Vision, GovWin CM, or Ajera CRM database to Vantagepoint. For more information, see Upgrade Scenarios for Vantagepoint 4.5. 	Run the Script with the Setup or SetupAndMigrate Switch <ul style="list-style-type: none"> ▪ Run the Script with the Setup Switch ▪ Run the Script with the SetupAndMigrate Switch
6.	Re-run the script as many times as needed, using the optional switches. Use only those switches that are relevant to your situation; skip those that are not.	Optional Switches

Step 1: Download the PowerShell Script

When you are sure that your prerequisites are in place, download the PowerShell script, DeltekVantagepoint.ps1, to a temporary location on your Vantagepoint web/application server.

Download it from Deltek Software Manager (DSM), the tool that Deltek uses to distribute new software and updates. You can access DSM through the Deltek Support Center or use Deltek Software Manager Lite to download Deltek products.

Note: The installation directory for Vantagepoint is determined by the drive from which you run the installation script. For example, if you want to install Vantagepoint on the D:\ drive, download the DeltekVantagepoint.ps1 file to a temporary folder on the D:\ drive.

Download the Script via the Deltek Support Center

To download the script via the Deltek Support Center:

1. In your Web browser, go to <http://support.deltek.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. On the Application Run dialog box, click **Run** to download the software manager.
6. Open Deltek Software Manager from the new icon at the bottom of your screen.
7. 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 at any time on the Settings dialog box.

8. In the left pane, scroll to Vantagepoint (1) and expand the folder structure.
9. Select the most recent version of Vantagepoint.

The right pane displays a message stating that the setup files have 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.

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

Download the Script via DSM Lite

To download the script via 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 **Vantagepoint 4.0 GA** from the drop-down list.
4. Under Complete Releases, click the most recent version of Vantagepoint.

Deltek Software manager prompts you to run or save the setup script. Rename the downloaded file to `DeltekVantagepoint.ps1` if it has a different filename.

5. Save the file to a folder.

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

DSM Documentation and Troubleshooting

Refer to the following links for additional information:

- [Deltek Software Manager online help](#)
- [Troubleshooting Deltek Software Manager](#)

Note: When you click a link, you will be asked to log into DSM if you are not already logged in.

Step 2: Run the Script with No Switches

After you download the PowerShell script, **DeltekVantagepoint.ps1**, to a temporary location on your Vantagepoint web/application server, you can begin installing Vantagepoint. Make sure to execute the script from a temporary location on the drive where you wish to install Vantagepoint.

First, run the script 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 `-CheckPreReq` switch.)

Procedure

To run the script with no switches:

1. On the operating system Start menu, locate the Windows PowerShell Console:
2. Run the console using the **Run as Administrator** option on the right-click context menu.
The **DeltekVantagepoint.ps1** script includes a `#Requires` statement that checks that you are running the PowerShell Console using the **Run as Administrator** option. If you do not use Run as Administrator, you will receive an error message indicating that the script contains a `#Requires` statement requiring that you run it as an administrator.
3. From the PowerShell Console, which is similar to the command prompt, change the default directory (`c:\windows\system32`) to the temporary location where you stored the **DeltekVantagepoint.ps1** script (for example, `c:\temp`).
4. To run the script, enter **DeltekVantagepoint.ps1** and then press TAB to autocomplete the entry.
The auto-completion places the characters `.\` in front of the filename (`.\DeltekVantagepoint.ps1`).
The script runs and performs these steps:
 - a. The script identifies the directory from which the script was executed.
 - b. If this is not the supported installation directory (for example, `<drive>:\Program Files\Deltek\Vantagepoint`), the script creates the supported installation directory.

- c. The script copies the DeltekVantagepoint.ps1 file to the installation directory \Scripts folder.
- d. The script prompts you to re-run the script.
5. To re-run the script, enter **DeltekVantagepoint.ps1** and then press TAB, or use the up and down arrow keys to browse through previously entered commands and choose **DeltekVantagepoint.ps1**.

Now, and whenever you run the script in the future, the script prompts you for your Deltek Support username and password. When you enter these credentials, the script:

- Checks to see if you have rights to access the software.
- Downloads any newer versions of the Vantagepoint PowerShell modules and configuration files.
- Checks to see if there is an updated version of DeltekVantagepoint.ps1. If there is, the new script is downloaded and you are prompted to re-run DeltekVantagepoint.ps1.

Note: If you are installing Vantagepoint on servers that do not have Internet access, you will receive these authentication prompts only on the Download Server.

6. Enter your Deltek Support username and password.

Setup Steps Performed by the Script

1. The script prompts for your Deltek support username and password.
2. The script checks for the presence of prerequisites. See [Prerequisite Checks Run Automatically](#).
3. If any prerequisites are missing, the script displays a red error message. You must resolve any issues before continuing with the setup process.
4. The script validates your access to Vantagepoint before continuing with the setup.
5. The script displays a list of available switches.

Step 3: Run the Script with the CheckPreReq Switch

The next time that you run DeltekVantagepoint.ps1, run it with the CheckPreReq switch to ensure that the necessary prerequisites, such as a supported version of SQL Server, are in place for the script to run.

Procedure

To run the script with the CheckPreReq switch:

1. Run the script from the Vantagepoint installation \Scripts directory with the CheckPreReq switch appended:

DeltekVantagepoint.ps1 –CheckPreReq

The script runs and checks that all [required IIS features](#) are enabled.

2. If any of these features are not enabled, install them using the EnableIISRequiredFeatures switch discussed in [Microsoft Internet Information Server \(IIS\) Installation on Windows Servers](#).

If the IIS features are enabled, the script prompts you for the web, database, and report servers to which you are installing Vantagepoint.

3. Enter the URL to your web server.

The script tries to connect to the server and checks that a [valid SSL certificate](#) is installed on it.

If you receive an error message, check that the URL is correct and that an SSL certificate has been installed. 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 the connection is successful, the script prompts you for your database server.

4. Identify your database server.

- Enter the name of your database server. If you are using a named SQL instance, identify the server in the form Server\Instance.
- The script attempts, via Windows Management Instrumentation (WMI), to obtain the port on which your SQL Server instance is listening and validate that a connection can be made. If the script cannot determine the port, the connection attempt is made on TCP port 1433. If a connection still cannot be made, the script prompts you for the port on which your SQL Instance is listening. If a connection still cannot be made, the script prompts you to check that the server name is correct and that the necessary ports are open in the firewall.
- If you are using dynamic ports, see the [firewall information](#) in this document.

If the connection is successful, the script prompts you for your SYSADMIN user account.

5. Identify your SYSADMIN user account to connect to the database server.

- If your domain account is a member of the sysadmin role, press ENTER at the [WI] prompt (for Windows Integrated). If not, enter a SQL login with sysadmin rights.
- Once a connection is made to the database server, the script checks that [SSL 2.0/3.0 and TLS 1.0/1.1 have been disabled](#) on the remote server.
- If necessary, disable the SSL and TLS protocols, reboot the server, and re-run the script. The script checks that a currently supported version of SQL Server is installed and that SQL FileStream has been configured properly.

If the connection is successful, the script displays the required and installed versions of SQL Server.

- If the installed version meets requirements, the script displays a note to check the Platform Compatibility Matrix for the currently supported SQL Server Cumulative update and then prompts you for your report server.
- If the installed version does not meet requirements, the script displays a message that the installed version is not supported and exits.

6. Enter the hostname of your report server and press ENTER. This must be the machine name, not the FQDN or the IP address.

The script checks that a [valid SSL certificate](#) is installed on the report server.

The script creates the default report server URL.

7. If the URL is correct, press ENTER; otherwise, enter the correct URL.

For example, you may use a custom DNS record for the server that does not match the hostname, or you may use a SQL instance, which will typically create the default report server virtual directory in the form ReportServer_<InstanceName>.

8. Enter the report server URL.

Once a connection is made to the report server, the script checks that an SSL (https) connection can be made.

If the connection is successful, the script displays the required and installed versions of SQL Server.

- If the installed version meets requirements, the script displays a note to check the Platform Compatibility Matrix for the currently supported SQL Server Cumulative update and then prompts you for your report server.
- If the installed version does not meet requirements, the script displays a message that the installed version is not supported and exits.

Step 4: Run the Script with the Setup or SetupAndMigrate Switch

The next time that you run the PowerShell script, DeltekVantagepoint.ps1, run it with one of the two Setup switches:

Switch	Use this switch...	Read this section...
Setup	If you are installing Vantagepoint and creating a completely new Vantagepoint database.	Run the Script with the Setup Switch
SetupAndMigrate	If you are migrating to Vantagepoint from Deltek Vision, GovWin CM, or Ajera CRM. Before proceeding, see Upgrade Scenarios for Vantagepoint 4.5 .	Run the Script with the SetupAndMigrate Switch

Whether you are installing Vantagepoint on one server or multiple servers, all installation functions are performed from the primary web/application server where the Vantagepoint PowerShell Installation script is run.

The only exceptions are when you use one of these switches:

- DownloadDatabases
- DownloadSetupPrep: This is performed on the Download server. See [Setup Steps for Non-Internet Server](#) for more information.
- SetupWebApp / SetupProcessServer: These are performed on the WebApp and Process Servers.
- Download
- DownloadAndExtract, followed by MigrateDatabase
 - The MigrateDatabase switch is used primarily with the DownloadAndExtract switch to test migrations from Ajera CRM, GovWin CM, or Vision 7.6 (CU 9 or later). Run the DownloadAndExtract switch, and then run the MigrateDatabase switch against a test copy of your production database. After you validate your database migration, use the SetupAndMigrate switch on the same server to make your installation production-ready and

perform your go-live migration at the same time. Before proceeding, see [Upgrade Scenarios for Vantagepoint 4.5](#).

- Alternatively, you can use the Setup switch (which will, by default, install a blank Vantagepoint database) to make the installation production-ready, and then use the MigrateDatabase switch to perform your go-live migration. When you use the MigrateDatabase switch, the script does not create a Weblink entry. Use the CreateDatabaseEntry switch to add the migrated database to Weblink.

After you run the installation script with any of the available switches, 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, stamped with the date and time that the setup script was executed. To gather and email the setup logs, use the GetSetupLogs switch after the SupportSetupOption switch.

Setup Steps for Non-Internet Server

To install Vantagepoint 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.

You will see the following differences when you install on a server without an Internet connection:

- 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.
- The non-Internet setup checks for an Internet connection. If one exists, you are required to run the regular setup.

Run the Script with the Setup Switch

Use the PowerShell script, DeltekVantagepoint.ps1, with the Setup switch to install Vantagepoint and create a completely new Vantagepoint database. If you are migrating from to Vantagepoint from Deltek Vision, GovWin CM, or Ajera CRM, use the [SetupAndMigrate switch](#) instead.

You can perform a one, two, or three tier installation with the Setup switch.

Procedure

To run the script with the Setup switch:

1. From the installation directory Scripts folder, enter **.\DeltekVantagepoint.ps1 -Setup**.
The script prompts you for your Deltek Support username and password.
2. Enter your Deltek Support username and password.
The script checks prerequisites, verifies your access to Deltek Vantagepoint, checks your IIS prerequisites, and then displays the following message:

Installing Deltek Vantagepoint <version>

Deltek Vantagepoint requires resolvable FQDN using a valid SSL certificate being installed on both the Web Server (IIS) and the Report Server. TLS 1.1/1.2 are 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.

3. Select **Yes** if you have read the installation documentation.

A new browser window opens, containing Deltek's licensing terms.

4. Read the licensing terms and, if you agree with them, return to the PowerShell console and select **Yes**.

The script prompts you for the URL for your web server. As the default, it displays the fully qualified domain name of the server, with the prefix HTTPS.

5. 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 script prompts you for the account to be used as the IIS Application Pool identity. The default value is a local account called [DeltekVantagepoint], which is a local Windows account. Deltek recommends that you use a domain account instead.

This account is used for the following service roles:

- Application Pool Identity
- Process Server service account
- Report Server Content Manager account

(Use the [SetServiceAccount switch](#) if you need to change these settings at a later time.)

6. Either accept the default value of [DeltekVantagepoint] or use an existing domain account.

The script prompts you for a password for this account. If you use a local account, [Password Complexity Rules](#) apply.

7. Enter and confirm the password.

If you entered a local account, the script uses the account value to create a local user account. Regardless of whether you entered a local or domain account, the script adds the account to the local administrator group. The script checks that the password entered is a secure password so that it will pass standard Domain Group Policy password tests.

The script prompts you for a password for Weblink.

8. Enter and confirm the password.

The script checks that the password is a secure password.

The script asks if you are using a [shared path for databases.enc](#).

9. Enter **Yes** or **No**.

If you enter **Yes**, the script creates a shared directory to eliminate the need to synchronize changes made to databases.enc across your servers.

The script prompts you for the name of your report server.

10. Enter the hostname of your report server and press ENTER. This must be the machine name, not the FQDN or the IP address.

When you enter the hostname, the script uses it to build a URL to the report server, which is the default value you will see in brackets. Your actual FQDN will likely be different and must be tied to the SSL certificate. The server URL must be SSL secured.

If the script cannot connect to the server, it prompts you to confirm this information:

- Report server name (the default is [HostName])
- Report server URL, in the format [https://FQDN/ReportServer]

If you are using a named instance for your Reporting Services installation (for example, if you are performing a SQL Express installation), your virtual directory is probably in the format: ReportServer_<InstanceName>. Your report server databases is probably in the form ReportServer\$<InstanceName>. The script checks for your report server database names and prompts you if a connection cannot be made. Because you may have your Report Server databases on a different SQL Server instance, you will be prompted for the name of the Report database server as well as the Report Server database name.

11. If the Report Server URL presented in brackets is correct, press ENTER to use it. If not, change the value to the correct URL for your Report Server and then press ENTER.

The script connects to the report server and validates the server's TLS configuration.

Then it prompts you for the information needed to connect to your database server.

12. Identify your database server.

- Enter the name of your database server. If you are using a named SQL instance, identify the server in the form Server\Instance.
- The script attempts, via Windows Management Instrumentation, to obtain the port that your SQL Server instance is listening on and validate that a connection can be made. If a port cannot be determined, the connection attempt is made on TCP port 1433. If a connection still cannot be made, the script prompts you for the port on which your SQL Instance is listening. If a connection still cannot be made, the script prompts you to check that the server name is correct and that the necessary ports are open in the firewall.
- If you are using dynamic ports, see the [firewall information](#) in this document.

If the connection is successful, the script prompts you for your database username.

13. Enter your database username. This should be either a SQL login or a Windows account. The default is [WI] for Windows Integrated.

The account must be a member of the SQL server sysadmin fixed server role. The script checks for this.

The script connects to the database server and validates the server's TLS configuration. Then it prompts you for the name of the database that will be created.

14. Enter the name for your new blank Vantagepoint database. The default is [Vantagepoint]. The script prompts you for a SQL login and password.

15. Enter a SQL login and password.

These credentials will be associated with the Vantagepoint database and the report server databases and granted the db_owner role.

This account can be a SQL Server or Windows login.

- If you use a SQL Login, the default is [DeltekVantagepoint]. The script prompts you to enter and confirm a password and verifies that the password meets [Password Complexity Rules](#).

- If you use a Windows account, it must be the IIS Application Pool Identity and must be entered in the form domain\user. If you use a Windows account, the script automatically selects the **Windows Authentication** checkbox in Weblink for both Vantagepoint and report server database access.

The script does the following:

- a. Checks that the password entered is a secure password so that it will pass standard Domain Group Policy password tests.
- b. Checks for the existence of the report server databases. If the script does not find the default Report Server database name, **ReportServer**, it prompts you for the name of the report database server and the Report Server database name.

The script has all of the information that it needs to complete the setup and begins performing setup steps.

16. When the setup steps are completed, your Vantagepoint administrator can log into Vantagepoint and begin the activation and setup process.

Setup Steps Performed by the Script

After you enter all of the information needed to run **DeltekVantagepoint.ps1 -Setup**, the script completes the following steps:

1. The script verifies that the SQL Server version is supported and FileStream is enabled and reminds you to check the Platform Compatibility Matrix for the currently supported SQL Server Cumulative Update.
2. The script downloads and extracts the DeltekVantagepoint<Build#>.exe file, which contains the core Vantagepoint installation files, and the PHP.exe file, needed to set up Deltek mobile applications. This process takes several minutes.
3. The script sets up required IIS components:
 - Application Pool (DeltekVantagepointAppPool)
 - Applications:
 - **Vantagepoint**: Server side components
 - **Vantagepoint/App**: Web client
 - **VantagepointClient**: Smart client
 - **Vantagepoint/Reporting**: Reporting application (only for Vantagepoint 3.0.2 and higher)
4. The script makes the necessary configuration changes to IIS for PHP.
5. The script creates the blank Vantagepoint database and creates and configures a blank FileStream database (VantagepointFILES). Then it runs the database script to create the default Vantagepoint database schema.
6. The script creates new SQL logins or associates existing logins with their respective databases. This includes creating a local account on the database server if you are using a local account for the Application Pool Identity.
7. The script creates a backup device named Vantagepoint for use with the backup utility in the desktop client.
8. The script updates databases.enc with values that were provided during the setup, including the password that you provide for Weblink

9. The script installs the Process Server service and sets the service account to the account identified for the Application Pool Identity.
10. If you said **Yes** to the prompt about using a shared path to Databases.enc, the script creates a fileshare for databases.enc.
11. The script sets permissions for Reporting Services. This includes creating a local account if you are using a local account for the Application Pool Identity.
12. The script creates the web configuration file in the \Vantagepoint\Web directory.
13. The script updates the Vantagepoint Mobile configuration files.
14. The script writes information about the Vantagepoint configuration to the DeltekVantagepointSettings.xml file at the root of the installation directory.

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

15. The script obtains your current Vantagepoint license information and applies the licenses to your newly created database.
16. The script loads reports to the report server for all languages. The report loading process can take up to 10 minutes for each language. Depending on the number of processor cores in your report server, multiple languages may be loaded concurrently. If reports for a particular language fail to load, the script will attempt to reload that language.
17. The script clears the PowerShell console memory of all values used in the setup process.
18. The script launches the [VantagepointURL.htm file](#) from the root of the installation directory. This file lists URLs for all of your Vantagepoint applications.

Run the Script with the SetupAndMigrate Switch

If you are migrating to Vantagepoint from Deltek Vision, GovWin CM, or Ajera CRM, use the PowerShell script, DeltekVantagepoint.ps1, with the SetupAndMigrate switch to install Vantagepoint. If you are not migrating from Deltek Vision, GovWin CM, or Ajera CRM to Vantagepoint, use the [Setup switch](#) instead.

Note: You must migrate from Deltek Vision, GovWin CM, or Ajera CRM 7.6 (CU 9) or a later version.

You can use the SetupAndMigrate switch to perform a one, two, or three tier installation.

Procedure

Note: When you install on a server without an Internet connection, any acknowledgement and licensing prompts and file downloads occur only on the Download Server.

To run the script with the SetupAndMigrate switch:

1. From the installation directory Scripts folder, enter **.\DeltekVantagepoint.ps1 - SetupAndMigrate**.
2. Enter your Deltek Support username and password.
The script checks prerequisites, verifies your access to Deltek Vantagepoint, checks your IIS prerequisites, and then displays the message:

Installing Deltek Vantagepoint <version>

Deltek Vantagepoint requires resolvable FQDN using a valid SSL certificate being installed on both the Web Server (IIS) and the Report Server. TLS 1.1/1.2 are 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.

3. Select **Yes** if you have read the installation documentation.
A new browser window opens, containing Deltek's licensing terms.
4. Read the licensing terms and, if you agree with them, return to the PowerShell console and select **Yes**.
The script prompts you for the URL for your web server. It will display the fully qualified domain name of the server, in brackets, with the prefix HTTPS.
5. 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 script prompts you for the account to be used as the IIS Application Pool identity. The default value is a local account called [DeltekVantagepoint], which is a local Windows account. Deltek recommends that you use a domain account instead.
This account is used for the following service roles:
 - Application Pool Identity
 - Process Server service account
 - Report Server Content Manager account
 (Use the SetServiceAccounts switch if you need to change these settings at a later time.)
6. Either accept the default value of [DeltekVantagepoint] or use an existing domain account.
The script prompts you for a password for this account. If you use a local account, [Password Complexity Rules](#) apply.
7. Enter and confirm the password.
The script uses the account value to create a local user account and add that user to the local administrator account.
If you entered a local account, the script uses the account value to create a local user account. Regardless of whether you entered a local or domain account, the script adds the account to the local administrator group. The script checks that the password entered is a secure password so that it will pass standard Domain Group Policy password tests.
The script prompts you for a password for Weblink.
8. Enter and confirm the password.
The script checks that the password is a secure password.
The script asks if you are using a [shared path for databases.enc](#).
9. Enter **Yes** or **No**.
If you enter **Yes**, the script creates a shared directory to eliminate the need to synchronize changes made to databases.enc across your servers.

The script prompts you for the name of your report server.

10. Enter the hostname of your report server and press ENTER. This must be the machine name, not the FQDN or the IP address.

When you enter the hostname, the script uses it to build a URL to the report server, which is the default value you will see in brackets. Your actual FQDN will likely be different and must be tied to the SSL certificate. The server URL must be SSL secured.

If the script cannot connect to the server, it prompts you to confirm this information:

- Report server name (the default is [HostName])
- Report server URL, in the format [https://FQDN/ReportServer]

If you are using a named instance for your Reporting Services installation (for example, if you are performing a SQL Express installation), your virtual directory is probably in the format: ReportServer_<InstanceName>. Your report server databases is probably in the form ReportServer\$<InstanceName>. The script checks for your report server database names and prompts you if a connection cannot be made. Because you may have your Report Server databases on a different SQL Server instance, you will be prompted for the name of the report database server as well as the Report Server database name.

11. If the Report Server URL presented in brackets is correct, press ENTER. If not, change the value to the correct URL for your Report Server and press ENTER.

The script connects to the report server and validates the server's TLS configuration. Then it prompts you for the information needed to connect to your database server.

12. Identify your database server.

- Enter the name of your database server. If you are using a named SQL instance, identify the server in the form Server\Instance.
- The script attempts, via Windows Management Instrumentation, to obtain the port that your SQL Server instance is listening on and validate that a connection can be made. If a port cannot be determined, the connection attempt is made on TCP port 1433. If a connection still cannot be made, the script prompts you for the port on which your SQL Instance is listening. If a connection still cannot be made, the script prompts you to check that the server name is correct and that the necessary ports are open in the firewall.
- If you are using dynamic ports, see the [firewall information](#) in this document.

If the connection is successful, the script prompts you for your database username.

13. Enter your database username. This should be either a SQL login or a Windows account. The default is [WI] for Windows Integrated.

The account must be a member of the SQL server sysadmin fixed server role. The script checks for this.

The script connects to the database server, verifies that the SQL Server version is supported and that FileStream is enabled, and validates the server's TLS configuration.

The script prompts you for the name of the Deltek Vision, GovWin CM, or Ajera CRM database that you will migrate to Vantagepoint.

14. Enter the name of the Deltek Vision, GovWin CM, or Ajera CRM database that you will migrate to Vantagepoint.

The script warns you to remove any custom database objects (indexes, triggers, and so on) before you proceed with the migration.

15. Enter **Yes** to acknowledge the warning and proceed or enter **No** to exit the script.

The script checks that the database has been converted to Unicode. If not, it will convert it as part of the migration process,

The script asks you if you have a backup of the database.

16. Enter **YES** in capital letters if you have a backup.

Warning: Do not proceed unless you have a backup of your Deltek Vision, GovWin CM, or Ajera CRM database.

The script checks if you have a FileStream database (<database>FILES) and creates one if you do not. The script prompts you for a SQL login and password.

17. Enter a SQL login and password.

These credentials will be associated with the migrated Vantagepoint database and report server databases and granted the db_owner role.

- If you use a SQL Login, the default is [DeltekVantagepoint]. The script prompts you to enter and confirm a password and verifies that the password meets [Password Complexity Rules](#).
- If you use a Windows account, it must be the IIS Application Pool Identity and must be entered in the form domain\user.

If you use a Windows account, the script automatically selects the **Windows Authentication** checkbox in Weblink for both Vantagepoint and report server database access.

The script:

- a. Checks that the password entered is a secure password so that it will pass standard Domain Group Policy password tests.
- b. Checks for the existence of the report server databases. If the script does not find the default Report Server database name, **ReportServer**, it prompts you for the name of the report database server and the Report Server database name.

The script has all of the information that it needs to complete the setup and begins performing setup steps.

18. When the setup steps are completed, your Vantagepoint administrator can log in to Vantagepoint.

Setup Steps Performed by the Script

After you enter all of the information needed to run **DeltekVantagepoint.ps1 -SetupAndMigrate**, the script completes the following steps:

1. The script verifies that the SQL Server version is supported and FileStream is enabled and reminds you to check the Platform Compatibility Matrix for the currently supported SQL Server Cumulative Update.
2. The script downloads and extracts the DeltekVantagepoint<Build#>.exe file, which contains the core Vantagepoint installation files, and the PHP.exe file, needed to set up Deltek mobile applications. This process takes several minutes.
3. The script sets up required IIS components:
 - Application Pool (DeltekVantagepointAppPool)
 - Applications:
 - **Vantagepoint:** Server side components

- **Vantagepoint/App:** Web client
 - **VantagepointClient:** Smart client
 - **Vantagepoint/Reporting:** Reporting application (only for Vantagepoint 3.0.2 and higher)
4. The script makes the necessary configuration changes to IIS for PHP.
 5. The script converts your Deltek Vision, GovWin CM, or Ajera CRM database to Unicode (if necessary) and migrates the database to Vantagepoint.
 6. The script creates new SQL logins or associates existing logins with their respective databases. This includes creating a local account on the database server if you are using a local account for the Application Pool Identity.
 7. The script creates a backup device named Vantagepoint for use with the backup utility in the desktop client.
 8. The script updates databases.enc with values that were provided during the setup, including the password that you provided for Weblink.
 9. The script installs the Process Server service and sets the service account to the account identified for the Application Pool Identity.
 10. If you said **Yes** to the prompt about using a shared path to Databases.enc, the script creates a fileshare for databases.enc.
 11. The script sets permissions for Reporting Services. This includes creating a local account if you are using a local account for the Application Pool Identity.
 12. The script creates the web configuration file in the \Vantagepoint\Web directory.
 13. The script updates the Vantagepoint Mobile configuration files.
 14. The script writes information about the Vantagepoint configuration to the DeltekVantagepointSettings.xml file at the root of the installation directory.

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

15. The script obtains your current Vantagepoint license information and applies the licenses to your newly migrated database.
16. The script loads reports to the report server for all languages. The report loading process can take up to 10 minutes for each language. Depending on the number of processor cores in your report server, multiple languages may be loaded concurrently. If reports for a particular language fail to load, the script will attempt to reload that language.
17. The script clears the PowerShell console memory of all values used in the setup process.
18. The script launches the [VantagepointURL.htm file](#) from the root of the installation directory. This file lists URLs for all of your Vantagepoint applications.

Step 5: Rerun the Script Using Optional Switches

Re-run the script as many times as needed, using the [Optional Switches](#). Use only those switches that are relevant to your situation; skip those that are not.

Step 6: Verify That the Installation Was Successful

After you complete the installation process, verify that the installation was successful.

Note: If any errors occur during the installation process when reloading reports, these errors will be listed in the installation log. Resolve any errors and reload your reports manually through the application or by using the [LoadReports](#) switch.

First-Time Installation

To verify the success of an installation that was run using the Setup switch:

1. Open Internet Explorer and enter the URL to the Vantagepoint application.
For example, https://<Web Server URL>\Vantagepoint.
2. Launch both the web client and desktop applications.
3. On the Logon form, enter **SETUP** as your username and leave the password field blank.
4. Use the drop-down list to select the **Database**. (If you have only one database, you will not see a database drop-down list in the web client.)
5. Click **Login**.
If the Vantagepoint application opens and you see the initial activation prompts, your installation was successful.

Migration from Another Deltek Product

To verify the success of an installation that was run using either of the Setup switches:

1. Open Internet Explorer and enter the URL to the Vantagepoint application.
For example, https://<Web ServerURL>\Vantagepoint.
2. Launch both the Web Client and Smart Client applications.
3. On the Logon form, enter your **User ID**. If you are unsure of your user ID, enter **admin**.
4. Enter your **Password**. If you are unsure of your password, leave this field blank.
If you do not have a user ID and password, and a user ID of **admin** and a blank password do not work, contact Deltek Customer Care.
5. Use the drop-down list to select the **Database**. (If you have only one database, you will not see database drop-down in the Web Client.)
6. Click **Login**. If the Vantagepoint application opens, displaying the Welcome page, your installation is successful.

Step 7: Optimize Database

Deltek provides a script to optimize your database. The script does not take long to run and can be added to daily or weekly maintenance plan activities.

See [Database Maintenance Activities](#) for more information.

Optional Switches

In addition to the switches that you must use to install Vantagepoint, you may want to use some optional switches. These switch are listed in the following tables:

- **Primary Switches:** Use these switches to perform operations, such as installing additional servers, creating or migrating databases, or upgrading your Vantagepoint servers.

Add these switches directly after `.\DeltekVantagepoint.ps1`. For example:

`.\DeltekVantagepoint.ps1 -SetupWebApp`
- **Additional Setup Switches:** Use these switches to perform maintenance operations, such as loading reports, changing service accounts, and changing the Weblink password

Add these switches after the `-AdditionalSetupOption` switch. For example:

`.\DeltekVantagepoint.ps1 -AdditionalSetupOption <switch>`
- **Advanced Setup Switches:** Use these switches to perform advanced setup operations, such as configuring Windows Authentication and configuring the database session state.

Add these switches after the `-AdvancedSetupOption` switch. For example:

`.\DeltekVantagepoint.ps1 -AdvancedSetupOption <switch>`
- **Support Setup Switches:** Use these switches to perform support operations, such as configuring failed request tracing, obtaining various server logs, and monitoring Web/report server activity.

Add these switches after the `-SupportSetupOption` switch. For example:

`.\DeltekVantagepoint.ps1 -SupportSetupOption <switch>`
- **Intelligence Setup Switches:** Use these switches to download Vantagepoint Intelligence Server and Desktop installation files, deploy or uninstall the Analysis Cubes configuration, and deploy packages when upgrade errors occur.

Add these switches after the `-IntelligenceSetupOption` switch. For example:

`.\DeltekVantagepoint.ps1 -IntelligenceSetupOption <switch>`

Important: You can tab through the available switches rather than entering them manually. See [Running Scripts and Switches](#) for more information.

Primary Switches

Switch	Use this switch to...	Read this section...
SetupWebApp	Install a secondary web/application server for load balanced configurations.	Setup WebApp Switch
SetupProcessServer	Install a stand-alone dedicated process server.	Setup ProcessServer Switch
SetupCustom	Installs custom packages.	Setup Custom Switch

Switch	Use this switch to...	Read this section...
SetupDatabaseNew	Create a new blank database after you have already installed Vantagepoint.	Setup DatabaseNew Switch
MigrateDatabase	Migrate an existing Deltek Vision, GovWin CM, or Ajera CRM database after you install Vantagepoint. For more information, see Upgrade Scenarios for Vantagepoint 4.5 .	MigrateDatabase Switch
ValidateDatabases	Validate upgrade or migration requirements for all databases in databases.enc.	ValidateDatabases Switch
CreateDatabaseEntry	Add a migrated database to the databases.enc file.	CreateDatabaseEntry Switch
RemoveInvalidWeblinkEntries	Remove weblink entries where Vantagepoint cannot access the database or the database server by looping through databasesenc	RemoveInvalidWeblinkEntries Switch
SetVersion	<p>Set the version branch to upgrade to a new major version (for example, upgrading from 4.0 to 4.5).</p> <p>When upgrading to the next major version, use this switch before running Upgrade, UpgradeWebApp or UpgradeProcessServer switches.</p> <p>If you are upgrading from any point release (for example, 3.0, 3.5, 4.0, and so on) you must first run this switch before running the Upgrade switches.</p>	SetVersion Switch
Upgrade; UpgradeWebApp; UpgradeProcessServer; UpgradeDatabases;	Apply upgrades to your Vantagepoint implementation.	Upgrade, UpgradeWebApp, UpgradeProcessServer, and UpgradeDatabases Switches
RunSQLScriptOnSelectedDatabases	Run a .SQL script against specific databases defined in databases.enc	RunSQLScriptOnSelectedDatabases Switch

Switch	Use this switch to...	Read this section...
Uninstall	Remove Vantagepoint from the web/application server.	Uninstall Switch
Download; DownloadAndExtract; DownloadDatabases; DownloadSetupPrep	Download and extract installation files.	Download, DownloadAndExtract, DownloadDatabases, and DownloadSetupPrepSwitches
SilentInstall	Run the Vantagepoint installation without manual intervention.	Set Up Silent Installation

Additional Setup Switches

Use these switches with the **AdditionalSetupOption** switch, in the format:

.\DeltekVantagepoint.ps1 –AdditionalSetupOption <switch>

Switch	Use this switch to...	Read this section...
InstallProcessServerService; RemoveProcessServerService	Uninstall or reinstall the process server service.	InstallProcessServer and RemoveProcessServer Switches
EnableIISRequiredFeatures	Enable required IIS features that are currently disabled.	EnableIISRequiredFeatures Switch
SetServiceAccount	Change the default service account used for the IIS Application Pool Identity, the Process Server service account and for Reporting Services authentication.	SetServiceAccount Switch
Cleanup	Remove older files no longer needed in Smart Client and the Database Scripts folder.	Cleanup Switch
EnableWindows-ExplorerPowerShellIntegration	Enable Windows Explorer to open a PowerShell prompt from the folder selected.	EnableWindows-ExplorerPowerShellIntegration Switch
CreateDeltekVantagepointCMDFile	Create a batch file to run DeltekVantagepoint.ps1 and set the PowerShell Execution Policy for the process.	CreateDeltekVantagepointCMDFile Switch

Switch	Use this switch to...	Read this section...
LoadReports	Reload Vantagepoint reports to the report server.	LoadReports Switch
LoadReportsCustom	Reload Vantagepoint custom reports to the report server.	LoadReportsCustom Switch
GetLicenseFile	Generate the Vantagepoint license file as a .SQL script that can be applied to your databases.	GetLicenseFile Switch
UpdateLicenseFile	Generate the Vantagepoint license file as a .SQL script and apply it to all of the databases defined in your databases.enc file.	UpdateLicenseFile Switch
ChangeWeblinkPassword	Change the password for Weblink access. Requires knowledge of current password.	ChangeWeblinkPassword Switch

Advanced Setup Switches

Use these switches with the AdvancedSetupOption switch, in the format:

.\DeltekVantagepoint.ps1 -AdvancedSetupOption <switch>

Switch	Use this switch to...	Read this section...
ConfigureARR	Configure Application Request Routing (Reverse Proxy) for reporting. See Create a Reverse Proxy for SQL Reporting Using Application Request Routing (ARR) for more information.	ConfigureARR Switch
ConfigureDatabaseSessionState	Configure Database Session State. See Configure Database Session State for Vantagepoint for more information.	ConfigureDatabaseSessionState Switch

Switch	Use this switch to...	Read this section...
ConfigureIISCompression	Configure HTTP compression for IIS to improve application performance over latent connections. See Configure HTTP Compression for more information.	ConfigureIISCompression Switch
ConfigureWindowsAuthentication	Configure Windows Authentication for Vantagepoint. See Configure Integrated Security for Vantagepoint for more information.	ConfigureWindowsAuthentication Switch
EnableAuthenticationPersistence	Configure Authentication Persistence when using Windows Authentication. See Configure Authentication Persistence for more information.	ConfigureAuthenticationPersistence Switch

Support Setup Switches

Use these switches with the SupportSetupOption switch, in the format:

.\DeltekVantagepoint.ps1 –SupportSetupOption <switch>

Switch	Use this switch to...	Read this section...
EnableFailedRequestTracing	Enable and configure IIS Failed Request Tracing for Vantagepoint.	EnableFailedRequestTracing Switch
DisableFailedRequestTracing	Disable IIS Failed Request Tracing for Vantagepoint.	DisableFailedRequestTracing Switch
GetConfigFiles	Collect and email the configuration files for your Vantagepoint installation.	GetConfigFiles Switch
GetAllLogs	Collect and email the log files from all servers in your Vantagepoint installation.	GetAllLogs Switch
GetSetupLogs	Collect and email the setup logs from your Vantagepoint installation.	GetSetupLogs Switch

Switch	Use this switch to...	Read this section...
GetSSRSLogs	Collect and email the SQL Reporting Services logs from your Vantagepoint installation.	GetSSRSLogs Switch
GetIISLogs	Collect and email the IIS log files from your Vantagepoint installation, including IIS, HTTP.sys error, and Failed Request Tracing logs.	GetIISLogs Switch
GetEventLogs	Collect and email the application/system event logs from a specific server in your Vantagepoint installation.	GetEventLogs Switch
GetSQLErrorLogs	Collect and email the SQL Server error logs from your Vantagepoint database server.	GetSQLErrorLogs Switch
GetAppUserInQuery	Identify the owner of a query that has been running for a long time.	GetAppUserInQuery Switch
GetActiveRunningReports	Identify all actively running reports on the report server.	GetActiveRunningReports Switch
GetActiveWebRequests	Identify all actively running requests executing in IIS.	GetActiveWebRequests Switch
GenerateMachineKey	<p>Generate a <machinekey> element for the Vantagepoint web configuration file when you balance load across web servers.</p> <p>This switch is only available in Vantagepoint 3.0 and higher.</p>	GenerateMachineKey Switch

Intelligence Setup Switches

Use these switches with the IntelligenceSetupOption switch, in the following format:

.\DeltekVantagepoint.ps1 -IntelligenceSetupOption <switch>

Switch	Use this switch to...	Read this section...
DownloadVantagepointIntelligence	Download Vantagepoint Intelligence Server and Desktop installation files. You must have a Vantagepoint Intelligence license to download them.	DownloadVantagepointIntelligence
SetupCube	Deploy Vantagepoint Intelligence Analysis Cubes.	Analysis Cubes Switches For more information, refer to the <i>Vantagepoint Intelligence Installation and Configuration Guide</i> .
UninstallCube	Uninstall a currently deployed Analysis Cubes configuration.	
UpdateCubeDtsxPackages	Deploy updated packages if error occurs during the upgrade.	

SetupDatabaseNew Switch

Use the SetupDatabaseNew switch to create a new blank Vantagepoint database and an associated FileStream database after Vantagepoint is installed. The script adds the new database to the databases.enc file.

Procedure

To run the script with the SetupDatabaseNew switch:

- From the installation directory Scripts folder, enter **.\DeltekVantagepoint.ps1 - SetupDatabaseNew**.
- Enter your Deltek Support username and password.
- The script checks prerequisites, verifies your access to Deltek Vantagepoint, and checks your IIS prerequisites, and then prompts you for the information needed to connect to your database server.
- Identify your database server.
 - Enter the name of your database server. If you are using a named SQL instance, identify the server in the form Server\Instance.
 - The script attempts, via Windows Management Instrumentation (WMI), to obtain the port on which your SQL Server instance is listening and validate that a connection can be made. If the script cannot determine the port, the connection attempt is made on TCP port 1433. If a connection still cannot be made, the script prompts you for the port on which your SQL Instance is listening. If a connection still cannot be made, the script prompts you to check that the server name is correct and that the necessary ports are open in the firewall.
 - If you are using dynamic ports, see the [firewall information](#) in this document.

If the connection is successful, the script prompts you for your database username.

- Enter your database username. This should be either a SQL login or a Windows account. The default is [WI] for Windows Integrated.

The account must be a member of the SQL server sysadmin fixed server role. The script checks for this.

The script verifies that the SQL Server version is supported and that FileStream is enabled, and validates the server's TLS configuration.

6. Enter the name for your new blank Vantagepoint database. The default is [Vantagepoint].

If a database with that name already exists, the script prompts you to enter a new name.

The script prompts you for a SQL login and password.

Enter a SQL login and password.

If you use a local account, [Password Complexity Rules](#) apply.

7. These credentials will be associated with the Vantagepoint database and the report server databases and granted the db_owner role.

If you use a Windows account, it must be the IIS Application Pool Identity and must be entered in the form domain\user. If you use a Windows account, the script automatically selects the **Windows Authentication** checkbox in Weblink for both Vantagepoint and report server database access.

The script performs the following steps:

- If you are using a SQL login, the script checks that the password entered is a secure password so that it will pass standard Domain Group Policy password tests.
- The script checks for the existence of the report server databases. If the script does not find the default Report Server database name, **ReportServer**, it prompts you for the name of the report database server and the Report Server database name.

8. Enter the password for the Application Pool Identity account for access to the FileStream database.

The script now has all of the information that it needs to complete the setup of the new database and begins performing setup steps.

When the new database operations are completed, the script prompts you for a Weblink password.

9. Enter the Weblink password.

The script adds the new database connection information to databases.enc.

Setup Steps Performed by the Script

When you run **DeltekVantagepoint.ps1 -SetupDatabaseNew**, the script completes the following steps:

1. The script validates that a connection can be made to the database server.
2. The script validates that the database username is a member of the SQL server sysadmin fixed server role.
3. The script verifies that the SQL Server version is supported and that FileStream is enabled, and validates the server's TLS configuration.
4. The script prompts for the SQL login and password to be associated with the Vantagepoint database and verifies that the password meets [Password Complexity Rules](#).
5. The script checks for the existence of the report server databases.
6. The script creates the new databases and schema.
7. The script creates the necessary database associations.

8. The script updates databases.enc with the new database connection information.
9. The script obtains your current Vantagepoint license information and applies the licenses to your newly created database.
10. The script clears the PowerShell console memory of all values used in the setup process.

MigrateDatabase Switch

Use the MigrateDatabase switch to migrate a Deltek Vision, GovWin CM, or Ajera CRM database for use by Vantagepoint. Use this switch with a fully installed Vantagepoint system or use it with the DownloadAndExtract switch to perform test migrations prior to installing the Vantagepoint software.

Note: The database must be from Deltek Vision, GovWin CM, or Ajera CRM 7.6 (CU 9) or a later version.

Procedure

To run the script with the MigrateDatabase switch:

1. From the installation directory Scripts folder, enter **.\DeltekVantagepoint.ps1 -MigrateDatabase**.
2. Enter your Deltek Support username and password.
3. The script checks prerequisites, verifies your access to Deltek Vantagepoint, and then displays the message:

This switch will migrate an Ajera CRM/GovWin CM/Vision 7.6 database to Deltek Vantagepoint 1.x (including converting it to Unicode, if necessary). This switch will ONLY migrate the database to Vantagepoint. You can add this database to Weblink by running the -CreateDatabaseEntry switch.

The script prompts you for the information needed to connect to your database server.

4. Identify your database server.
 - Enter the name of your database server. If you are using a named SQL instance, identify the server in the form Server\Instance.
 - The script attempts, via Windows Management Instrumentation (WMI), to obtain the port on which your SQL Server instance is listening and validate that a connection can be made. If the script cannot determine the port, the connection attempt is made on TCP port 1433. If a connection still cannot be made, the script prompts you for the port on which your SQL Instance is listening. If a connection still cannot be made, the script prompts you to check that the server name is correct and that the necessary ports are open in the firewall.
 - If you are using dynamic ports, see the [firewall information](#) in this document.
5. If the connection is successful, the script prompts you for your database username.
6. Enter your database username. This will be either a SQL login or a Windows account. The default is [WI] for Windows Integrated.

The account must be a member of the SQL server sysadmin fixed server role. The script checks for this.

The script verifies that the SQL Server version is supported and that FileStream is enabled, and validates the server's TLS configuration.

Then it prompts you for the name of the Deltek Vision, GovWin CM, or Ajera CRM database that you will migrate to Vantagepoint.

7. Enter the name of the Deltek Vision, GovWin CM, or Ajera CRM database that you will migrate to Vantagepoint.

The script then warns you about custom database objects (indexes, triggers, etc.) that may need to be removed before proceeding with the migration.

8. Enter **YES** to acknowledge the warning and proceed or **No** to exit the script.

The script checks to see if the database is Unicode and, if not, displays a message that the database will be converted to Unicode.

The script prompts you to confirm that you have a backup of your database before continuing with the migration.

Warning: Do not proceed unless you have a backup of your Deltek Vision, GovWin CM, or Ajera CRM database. The database must be from version 7.6 (CU 9) or later.

9. Enter **YES** in capital letters if you have a backup.

The script checks if you have a FileStream database (<database>FILES) and creates one if you do not.

The script starts the database migration and, if necessary, the Unicode conversion process.

Setup Steps Performed by the Script

When you run **DeltekVantagepoint.ps1 -MigrateDatabase**, the script completes the following steps:

1. The script validates that a connection can be made to the database server.
2. The script validates that the database username is a member of the SQL server sysadmin fixed server role.
3. The script verifies that the SQL Server version is supported and that FileStream is enabled, and validates the server's TLS configuration.
4. The script checks if you have a FileStream database (<database>FILES) and creates one if you do not.
5. The script prompts for the Deltek Vision, GovWin CM, or Ajera CRM database to be migrated and checks to see if it has been converted to Unicode. If not, it will be converted.
6. If the Unicode conversion is successful, the database is migrated to Vantagepoint. If the Unicode conversion is not successful, the setup process ends. The Unicode conversion issues must be resolved before the database can be migrated to Vantagepoint.
7. The script obtains your current Vantagepoint license information and applies the licenses to your newly migrated database.
8. The script clears the PowerShell console memory of all values used in the setup process.

UpgradeDatabase Switch

Use the UpgradeDatabase switch to upgrade a Deltek Vantagepoint 2.x or 3.x database to Vantagepoint 4.0. Use this switch with a fully installed Vantagepoint system.

Note: To upgrade all databases in databases.enc that are at Vantagepoint 3.0.6 or higher to Vantagepoint 4.0, use the **-UpgradeDatabases** (plural) switch.

Procedure

To run the script with the UpgradeDatabase switch:

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

The script checks prerequisites and verifies your access to Deltek Vantagepoint.
3. When the confirmation message displays, enter information to connect to your database server.
 - a. Enter the name of your database server. If you are using a named SQL instance, identify the server in the form Server\Instance.

Through the Windows Management Instrumentation (WMI), the script attempts to obtain the port on which your SQL Server instance is listening and validates that a connection can be made. If the script cannot determine the port, the connection attempt is made on TCP port 1433. If a connection still cannot be made, the script prompts you for the port on which your SQL Instance is listening.

If the connection still fails, check that the server name is correct and that the necessary ports are open in the firewall.
 - b. Enter your database username, which is either your SQL login or Windows account. The default is [WI] for Windows Integrated.

The script checks for the following:

 - The account is a member of the SQL server sysadmin fixed server role.
 - The SQL server version is supported.
 - The FileStream is enabled.
 - The SQL server's TLS configuration is valid.

The script lists the current status and version of your databases in databases.enc. To upgrade a database that is not in databases.enc, proceed to step 5.
4. Enter your Weblink password.

The script returns information about databases in databases.enc.
5. In **Database Name to upgrade**, enter the databases that you want to upgrade.

You must remove custom database objects before proceeding with the migration.
6. Enter **YES** to proceed or **NO** to exit the script.

Warning: Do not proceed unless you have a backup of the database that you are upgrading.

7. If you chose to proceed, enter **YES** to confirm that you have a backup of your databases.

The database upgrade starts and the script notifies you when the upgrade is complete.

Setup Steps Performed by the Script

When you run **DeltekVantagepoint.ps1 -UpgradeDatabase**, the script completes the following steps:

1. The script validates that a connection can be made to the database server.
2. The script validates that the database username is a member of the SQL server sysadmin fixed server role.
3. The script verifies that the SQL Server version is supported and that FileStream is enabled, and validates the SQL server TLS configuration.
4. The script prompts for your Weblink password and provides information about the status and version of your existing databases in databases.enc.
5. The script prompts for the Deltek Vantagepoint database to upgrade. You can include databases that are not in databases.enc.
6. The script clears the PowerShell console memory of all values used in the setup process.

ValidateDatabases Switch

The **-ValidateDatabases** switch provides upgrade or migration details for each database in databases.enc. You can upgrade Vantagepoint 3.5.x databases and higher directly to Vantagepoint 4.0.

If you are upgrading or migrating Vantagepoint databases with a version earlier than 3.5.x (2.0.x through 3.0.x) to Vantagepoint 4.0, use the **-Upgrade** switch, and then use the **-UpgradeDatabase** switch.

Note: If the **-ValidateDatabases** switch is not available, do the following:

1. Use the **-SetVersion** switch and change the branch to 4.0.
2. Run **\\DeltekVantagepoint.ps1** with no switches for the new 4.0 deployment scripts.

The installer downloads the missing switch.

Procedure

To run the script with the ValidateDatabases switch:

1. From the installation directory Scripts folder, enter **\\DeltekVantagepoint.ps1 -ValidateDatabases**.
2. Enter your Deltek Support username and password.
The script checks prerequisites and verifies your access to Deltek Vantagepoint.
3. When the confirmation message displays, enter information to connect to your database server.
 - a. Enter the name of your database server. If you are using a named SQL instance, identify the server in the form **Server\\Instance**.

Through the Windows Management Instrumentation (WMI), the script attempts to obtain the port on which your SQL Server instance is listening and validates that a connection can be made. If the script cannot determine the port, the connection attempt is made on TCP port 1433. If a connection still cannot be made, the script prompts you for the port on which your SQL Instance is listening.

If connection still fails, check that the server name is correct and that the necessary ports are open in the firewall.

- b. Enter your database username, which is either your SQL login or Windows account. The default is [WI] for Windows Integrated. The script checks for the following:

- The account is a member of the SQL server sysadmin fixed server role.
- The SQL server version must be supported.
- The FileStream is enabled.
- The SQL server's TLS configuration is valid.

The script loops through the databases defined in databases.enc and guides you in upgrading or migrating your databases to Vantagepoint 4.0.

4. Depending on your upgrade scenario, use the appropriate switch to upgrade or migrate your databases:
 - If a database is at Vantagepoint 3.5.x or higher, use the –Upgrade switch to automatically upgrade to Vantagepoint 4.0.
 - If a database is at Vantagepoint 2.0.x to 3.0.x, run the –Upgrade switch, and then run the –UpgradeDatabase switch for each database.

For more information, see [Upgrade Scenarios for Vantagepoint 4.5](#).

Setup Steps Performed by the Script

When you run **DeltekVantagepoint.ps1 -ValidateDatabases**, the script completes the following steps:

1. The script prompts for the Weblink password.
2. The script validates that a connection can be made to the database server and verifies the TLS configuration.
3. The script validates that the database username is a member of the SQL server sysadmin fixed server role.
4. The script loops through databases.enc and provides information on the upgrade/migration path for each databases.

CreateDatabaseEntry Switch

Use the CreateDatabaseEntry switch to add a migrated database to the databases.enc file.

The MigrateDatabase switch performs the database operations needed to convert the database to Unicode (if necessary) and then migrate the database to Vantagepoint. It does not add the database entry to databases.enc. The reason that the MigrateDatabase switch does not add the database to databases.enc is that you can use the MigrateDatabase switch to perform a test migration before Vantagepoint is installed. (You can use the DownloadAndExtract switch followed by the MigrateDatabase switch to perform a test migration).

Procedure

To run the script with the CreateDatabaseEntry switch:

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

The script checks prerequisites, verifies your access to Deltek Vantagepoint, and checks your IIS prerequisites, and then displays this message:

This will add a database entry to WebLink.

The script prompts you for the information needed to connect to your database server.

3. Identify your database server.

- Enter the name of your database server. If you are using a named SQL instance, identify the server in the form Server\Instance.
- The script attempts, via Windows Management Instrumentation (WMI), to obtain the port on which your SQL Server instance is listening and validate that a connection can be made. If the script cannot determine the port, the connection attempt is made on TCP port 1433. If a connection still cannot be made, the script prompts you for the port on which your SQL Instance is listening. If a connection still cannot be made, the script prompts you to check that the server name is correct and that the necessary ports are open in the firewall.
- If you are using dynamic ports, see the [firewall information](#) in this document.

If the connection is successful, the script prompts you for your database username.

4. Enter your database username. This will be either a SQL login or a Windows account. The default is [WI] for Windows Integrated.

The account must be a member of the SQL server sysadmin fixed server role. The script checks for this.

The script verifies that the SQL Server version is supported and that FileStream is enabled, and validates the server's TLS configuration.

Then it prompts you for the name of the database to add to Weblink.

5. Enter the name of the database.

The script prompts you for a SQL login and password.

Enter a SQL login and password.

6. These credentials will be associated with the migrated Vantagepoint database and the report server databases and granted the db_owner role.

These credentials will be associated with the migrated Vantagepoint database and report server databases and granted the db_owner role.

- If you use a SQL Login, the default is [DeltekVantagepoint]. The script prompts you to enter and confirm a password and verifies that the password meets [Password Complexity Rules](#).
- If you use a Windows account, it must be the IIS Application Pool Identity and must be entered in the form domain\user. If you use a Windows account, the script automatically selects the **Windows Authentication** checkbox in Weblink for both Vantagepoint and report server database access.

The script:

- a. Checks that the password entered is a secure password so that it will pass standard Domain Group Policy password tests.
 - b. Checks for the existence of the report server databases. If the script does not find the default Report Server database name, **ReportServer**, it prompts you for the name of the report database server and the Report Server database name.
- Enter the password for the Application Pool Identity account for access to the FileStream database.

The script now has all of the information that it needs to complete the setup of the new database and begins performing setup steps.

When the database operations are completed, the script prompts you for a Weblink password.

7. Enter the Weblink password.

The script adds the new database connection information to databases.enc.

Setup Steps Performed by the Script

When you run **DeltekVantagepoint.ps1 -CreateDatabaseEntry**, the script completes the following steps:

1. The script validates that a connection can be made to the database server.
2. The script validates that the database username is a member of the SQL server sysadmin fixed server role.
3. The script prompts for the SQL Login and password to be associated with the Vantagepoint database and verifies that the password meets [Password Complexity Rules](#).
4. The script checks for the existence of the report server databases.
5. The script retrieves the Application Pool credentials and prompts for the password of the Application Pool Identity so that it can be associated with the FileStream database.
6. The script creates the necessary database associations.
7. The script updates databases.enc with the new database connection information.
8. The script clears the PowerShell console memory of all values used in the setup process.

RemoveInvalidWeblinkEntries Switch

Use the RemoveInvalidWeblinkEntries switch to remove database entries in your databases.enc file where Vantagepoint cannot access the database and/or database server.

Procedure

To run the script with the RemoveInvalidWeblinkEntries switch:

1. From the installation directory Scripts folder, enter **.\DeltekVantagepoint.ps1 -RemoveInvalidWeblinkEntries**.
2. Enter your Deltek Support username and password.
The script checks prerequisites, verifies your access to Deltek Vantagepoint, checks your IIS prerequisites, creates a backup of your databases.enc file, and then prompts for your Weblink password.
3. Enter the Weblink password.
If there are database entries where Vantagepoint cannot access the database and/or the server, the Server, Database, and Description are displayed. You are asked if you want remove the entries.
4. Enter **Yes** or **No**.
You are notified if there are no entries to remove.

Setup Steps Performed by the Script

When you run **DeltekVantagepoint.ps1 -RemoveInvalidWeblinkEntries**, the script completes the following steps:

1. The script prompts for the Weblink password.

2. The script validates that a connection can be made to the database server and the database for each entry in databases.enc.
3. If a connection cannot be made, the entry is flagged for removal and you are prompted to confirm the removal. You are notified if there are no invalid entries.
4. The script clears the PowerShell console memory of all values used in the setup process.

SetupWebApp Switch

Use the SetupWebApp switch to install additional web/application server(s) if you have a load balanced configuration. You must have an existing installation of Vantagepoint to use this switch. Deltek recommends that you use a shared path to databases.enc for this setup.

Attention: See [Configure a Shared Location for Databases.enc](#) for more information.

This process does not create or migrate databases or load reports.

Procedure

Note: When you install on a server without an Internet connection, any acknowledgement and licensing prompts and file downloads occur only on the Download Server.

To run the script with the SetupWebApp switch:

1. From the installation directory Scripts folder, enter **.\DeltekVantagepoint.ps1 -SetupWebApp**.
2. Enter your Deltek Support username and password.
The script checks prerequisites, verifies your access to Deltek Vantagepoint, checks your IIS prerequisites, and then opens a new browser window, containing Deltek's licensing terms.
3. Read the licensing terms and, if you agree with them, return to the PowerShell console and select **Yes**.
The script prompts you for the URL for your web server. It will display the fully qualified domain name of the server, with the prefix HTTPS.
4. 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.
5. The script prompts you for the account to be used as the IIS Application Pool identity. The default value is an account called [DeltekVantagepoint], which is a local Windows account. Deltek recommends that you use a domain account instead.
This account will need read access to the shared databases.enc path, if you are using one.
This account is used for the following service roles:
 - Application Pool Identity
 - Process Server service account
 (Use the [SetServiceAccount switch](#) if you need to change these settings at a later time.)
6. Either accept the default value of [DeltekVantagepoint] or use an existing domain account.
The script prompts you for a password for this account.

If you use a local account, [Password Complexity Rules](#) apply.

Enter and confirm the password.

The script asks you if you are using a shared path to databases.enc. See [Configure a Shared Location for Databases.enc](#) for more information.

7. Enter **Yes** or **No**.

- **Yes:** The script prompts you for the shared path on your primary web/application server and tests that the path is valid.
- **No:** The script tells you that you need to copy the databases.enc file from the primary web/application server to the new web/application server after the setup process is completed.

The script now has all of the information that it needs to complete the setup and begins performing setup steps.

8. When the setup steps are completed, your Vantagepoint administrator can log in to Vantagepoint.

Setup Steps Performed by the Script

After you enter all of the information needed to run **DeltekVantagepoint.ps1 -SetupWebApp**, the script completes the following steps:

- The script downloads and extracts the DeltekVantagepoint<Build#>.exe file, which contains the core Vantagepoint installation files, and the PHP.exe file, needed to set up the Deltek mobile applications. This process takes several minutes.
1. The script sets up required IIS components:
 - Application Pool (DeltekVantagepointAppPool)
 - Applications:
 - **Vantagepoint:** Server side components
 - **Vantagepoint/App:** Web client
 - **VantagepointClient:** Smart client
 - **Vantagepoint/Reporting:** Reporting application (only for Vantagepoint 3.0.2 and higher)
 2. The script configures IIS for PHP (the Vantagepoint Mobile applications).
 3. If you are using a shared databases.enc path, the script enters the path in the web.config file.
 4. The script installs the Process Server service and sets the service account to the account identified for the Application Pool Identity.
 5. The script creates the web configuration file in the \Vantagepoint\Web directory.
 6. The script updates the Vantagepoint Mobile configuration files.
 7. The script writes information about the Vantagepoint configuration to the DeltekVantagepointSettings.xml file at the root of the installation directory.

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

8. The script clears the PowerShell console memory of all values used in the setup process.
9. The script launches the [VantagepointURL.htm file](#) from the root of the installation directory. This file lists URLs for all of your Vantagepoint applications.

SetupProcessServer Switch

Use the SetupProcessServer switch to install a stand-alone dedicated process server. This server has application server components but does not require IIS. (In Deltek for Professional Services, this switch was called the InstallDedicatedProcessServer switch.)

You must have an existing installation of Vantagepoint to set up a dedicated process server. Deltek recommends that you use a shared path to databases.enc for this setup. See [Configure a Shared Location for Databases.enc](#) for more information.

This process will not create or migrate databases or load reports.

Procedure

Note: When you install on a server without an Internet connection, any acknowledgement and licensing prompts and file downloads occur only on the Download Server.

To run the script with the SetupProcessServer switch:

1. From the installation directory Scripts folder, enter **.\DeltekVantagepoint.ps1 -SetupProcessServer**.
2. Enter your Deltek Support username and password.
3. The script checks prerequisites and verifies your access to Deltek Vantagepoint, and then prompts you for the account to be used as the Process Server service account. The default value is an account called [DeltekVantagepoint], which is a local Windows account. Deltek recommends that you use a domain account instead.

This account will need read access to the shared databases.enc path, if you are using one.

(Use the [SetServiceAccounts switch](#) if you need to change these settings at a later time.)

4. Either accept the default value of [DeltekVantagepoint] or use an existing domain account.

The script prompts you for a password for this account.

If you use a local account, [Password Complexity Rules](#) apply.

5. Enter and confirm the password.

The script asks you if you are using a shared path to databases.enc. See [Configure a Shared Location for Databases.enc](#) for more information.

6. Enter **Yes** or **No**.

- **Yes:** The script prompts you for the shared path on your primary web/application server and tests that the path is valid.
- **No:** The script tells you that you need to copy the databases.enc file from the primary web/application server to the new web/application server after the setup process is completed.

The script now has all of the information that it needs to complete the setup and begins performing setup steps

Setup Steps Performed by the Script

After you enter all of the information needed to run **DeltekVantagepoint.ps1 -SetupProcessServer**, the script completes the following steps:

1. The script installs the Deltek Vantagepoint build and configures the Process Server Windows service.
2. If you are using a shared databases.enc path, the script enters the path in the web.config file.
3. The script sets the Process Server service account to the account that you entered.
4. The script grants the necessary service rights to the service account.
5. The script starts the service and updates the settings file.

When the process server installation is completed, perform these steps:

1. (Optional) The process server is installed by default on all web/application servers. Consider disabling or removing the process server from these servers. Use the RemoveProcessServer switch if you want to remove the service. However, you may want to keep the additional process servers so that you can have multiple process servers sharing the processing load during times of heavy use.
2. Go to the Process Server settings in Vantagepoint and add the new process server. If appropriate, set up process queues to use dedicated process servers. See the [Vantagepoint online help](#) for more information.

SetupCustom Switch

Use the SetupCustom switch to complete the initial installation of a custom package.

Procedure

To run the script with the SetupCustom switch:

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

The script checks prerequisites, verifies your access to Deltek Vantagepoint, and detects any custom installation packages in the Vantagepoint\Custom directory. If there are no custom packages installed, the script exits.

Setup Steps Performed by the Script

After you enter all of the information needed to run **DeltekVantagepoint.ps1 -SetupCustom**, the script completes the following steps:

1. If at least a custom installer package is found, the script extracts the custom installation files to the appropriate locations.
2. The script reloads both standard and custom reports to the report server.

Note: When you run the Upgrade, UpgradeWebApp and UpgradeProcessServer switches, all custom installation packages are automatically reapplied.

Download, DownloadAndExtract, DownloadDatabases, and DownloadSetupPrep Switches

Use the Download, DownloadAndExtract, DownloadDatabases, and DownloadSetupPrep switches to perform downloads of the installation files, databases and prerequisite software.

You can use the Download and DownloadAndExtract switches to download files, and then use the MigrateDatabase switch to run and test your database migration from Vantagepoint to Deltek Vision, GovWin CM, or Ajera CRM. This will not prevent you from setting up Vantagepoint in the future. However, if you do this, you will still need to run the script with the Setup or SetupAndMigrate switch at a later time.

Switch	Use this switch to...
Download	Download installation files.
DownloadAndExtract	Download installation files and extract them to the correct Vantagepoint installation path. You must run the Setup or SetupAndMigrate switch to use the extracted files for Vantagepoint. See the notes below.
DownloadDatabases	Download specialized databases (for example, language and demo) for use with Vantagepoint. The switch will prompt you to restore these databases.
DownloadSetupPrep	Download all setup files needed to install Vantagepoint on servers that are not connected to the Internet.

DownloadAndExtract

- Use the MigrateDatabase switch primarily with the DownloadAndExtract switch to test migrations from Ajera CRM, GovWin CM, or Vision 7.6 (CU 9 or later). Run the DownloadAndExtract switch, and then run the MigrateDatabase switch. After you validate your database migration, use the SetupAndMigrate switch on the same server to make your installation production-ready and perform your go-live migration at the same time.
- Alternatively, use the Setup switch (which will, by default, install a blank Vantagepoint database) to make the installation production-ready, and then use the MigrateDatabase switch to perform your go-live migration.

DownloadSetupPrep

- Use the DownloadSetupPrep switch if you are installing Vantagepoint on servers that do not have an Internet connection. Use it to download setup files to a Download Server, from which you can copy the files to your non-Internet-accessible servers.
- The Download Server cannot contain a build or installation of Vantagepoint.
- Once the files are copied to your non-Internet-accessible servers, run the regular Setup switches (Setup, SetupAndMigrate, SetupProcessServer or SetupWebApp).

- When a new build is available, run the DownloadSetupPrep switch again on the Download Server to download the updated build files. (Previous build files will be removed.) Then copy these files to your existing server(s), overwriting existing files as necessary, and run the appropriate upgrade switches (Upgrade, UpgradeProcessServer or UpgradeWebApp).
- Once the DownloadSetupPrep switch is run on the Download Server, no other switches can be run on this server.

Procedure

To run the script with the DownloadAndExtract, DownloadDatabases, or DownloadSetupPrep switches:

1. From the installation directory Scripts folder, enter **.\DeltekVantagepoint.ps1 -<Download Option>**.
2. Enter your Deltek Support username and password.
The script checks prerequisites and verifies your access to Deltek Vantagepoint, and then opens a new browser window, containing Deltek's licensing terms.
3. Read the licensing terms and, if you agree with them, return to the PowerShell console and select **Yes**.
The download starts.

Setup Steps Performed by the Script

After you enter the information needed to run DeltekVantagepoint.ps1 using one of the download switches, the script downloads the files to the server where the script was run.

If You Use the Download Switch

The script downloads the self-extracting file DeltekVantagepoint<Build>.exe to the root of the Vantagepoint installation directory.

If You Use the DownloadAndExtract Switch

The script downloads the self-extracting file DeltekVantagepoint<Build>.exe to the root of the Vantagepoint installation directory and extracts the build files. You must run the Setup or SetupAndMigrate switch to use the extracted files for Vantagepoint.

When you run the Setup or SetupAndMigrate switch after using DownloadAndExtract, at the point where the DeltekVantagepoint<Build#>.exe would normally start downloading, the script displays the message:

Detected –DownloadAndExtract switch used, not downloading build.

If You Use the DownloadDatabases Switch

1. The script downloads the self-extracting file DeltekVantagepointDatabases.exe to the \Databases folder and extracts the contents. The downloaded files include the DeltekVantagepointDatabasesVersion.txt file, which contains the Vantagepoint version number of the databases.

If no build of Vantagepoint is installed, the script notifies you that a restore of the database is the only option, as setup cannot add an entry to databases.enc.

A message indicates that the script will need to share the Vantagepoint directory (Windows share) and that the SQL Service account must be granted read access to the share. These steps

are necessary for the restore to happen over the network. The SQL Service account must be a domain account; if it is not, the script exits.

2. The script asks you if you want to restore a demo database.
3. If you enter **No**, the script ends. If you enter **Yes** to restore a demo database, these steps occur:
 - a. The script prompts you for the database server\instance to which the database will be restored.
 - b. The script prompts you for the SQL sysadmin account used to make the connection (the default is WI).
 - c. The script asks if you would like to restore the demo database. If you do, enter `Yes` as the prompt.
 - d. The script prompts you for a SQL login and password. Enter a SQL login and password. If you use a SQL account or local Windows account, [Password Complexity Rules](#) apply.

These credentials will be associated with the Vantagepoint database and the report server databases and will be granted the db_owner role.

This account can be a SQL Server or Windows login.

- If you use a SQL Login, the default is [DelttekVantagepoint]. The script prompts you to enter and confirm a password and verifies that the password meets Password Complexity Rules.
 - If you use a Windows account, it must be the IIS Application Pool Identity and must be entered in the form domain\user. If you use a Windows account, the script automatically selects the Windows Authentication checkbox in Weblink for both Vantagepoint and report server database access.
- e. The script prompts you for the password for the Application Pool Identity (for FileStream database access).
 - f. The script checks to see if the SQL Service account is a domain account. If it is not a domain account, you will receive a message indicating that the databases will need to be restored manually. If the SQL Service account is a domain account, the script prompts you for the password for the SQL Service account.
 - g. The script restores the Vantagepoint demo database and creates the corresponding FileStream database.
 - h. The script assigns the necessary rights to the SQL login account entered and adds a database entry to databases.enc.

If You Use the DownloadSetupPrep Switch

1. As with the regular Setup and SetupAndMigrate switches, the script prompts you to acknowledge that you have read the installation documentation and agree with the Delttek licensing terms. You are prompted on this server but will not be prompted on the servers where you have no Internet access.
2. The script displays a message indicating that it will be downloading 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.
3. The script downloads the following files to the installation directory:
 - DelttekVantagepointConfiguration.xml

- DeltekVantagepointSettings.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
 - Sample (demo) databases (optional installation)
 - Application Request Routing components (optional installation)
 - DeltekVantagepoint<Build>.exe
 - PHP.exe
 - Vantagepoint license file script
4. The script creates a new DeltekVantagepointSettingsInternet.xml file to track the build version and download date.
 5. 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 or process server and run the appropriate Setup switch for that server (Setup, SetupAndMigrate, SetupWebApp, or SetupProcessServer).
 6. When a new build is available, run the DownloadSetupPrep switch again on the Download Server to download the updated build files. (Previous build files will be removed.) Then copy these files to your existing server(s), overwriting existing files as necessary, and run the appropriate upgrade switches (Upgrade, UpgradeProcessServer or UpgradeWebApp).

DownloadVantagepointIntelligence Switch

Use the DownloadVantagepointIntelligence switch to download the Vantagepoint Intelligence (Tableau) server and desktop installation files. Once the download is completed, refer to the *Deltek Vantagepoint Intelligence Installation and Configuration Guide* for installation and configuration instructions.

To download the software, you must have a valid module code for Vantagepoint Intelligence.

Procedure

To run the script with the DownloadVantagepointIntelligence switch:

1. From the installation directory Scripts folder, enter **.\DeltekVantagepoint.ps1 – IntelligenceSetupOption DownloadVantagepointIntelligence**.
2. Enter your Deltek Support username and password.

The script checks prerequisites and verifies your access to Deltek Vantagepoint Intelligence.

The download of DeltekVantagepointIntelligence_<build>.zip starts. The download location of the zip file is <Vantagepoint_Installation_Directory>\Support\Intelligence.

Once this file download is complete the files are extracted to the same directory.

Setup Steps Performed by the Script

After you enter the information needed to run DeltekVantagepoint.ps1 using DownloadVantagepointIntelligence switch, the script downloads the files and then extracts them to the \Support\Intelligence directory.

SetVersion Switch

Use the SetVersion switch to prepare the deployment scripts for a major version upgrade (for example, from 3.0 or 3.5 to 4.0).

Procedure

To run the script with the SetVersion switch:

From the installation directory Scripts folder, enter `\DeltekVantagepoint.ps1 -SetVersion <version>` (for example, `\DeltekVantagepoint.ps1 -SetVersion 3.5`)

Setup Steps Performed by the Script

When you run the SetVersion script, the <branch> element in the DeltekVantagepointSettings.xml file is updated. The scripts pull the updated software from the correct product branch. After running the SetVersion script, you can run the Upgrade, UpgradeWebApp, or Upgrade/ProcessServer switches to complete upgrading Vantagepoint to the next major release.

Upgrade Switches

Important:

- If you are upgrading to a higher major version of Vantagepoint (for example, from Vantagepoint 3.5 to 4.0, or 4.0 to 4.5), then you must first run the SetVersion switch before running the Upgrade switches.
- If you are upgrading to the currently available maintenance release software version (for example, from Vantagepoint 4.0.5 to 4.0.6), you can run Upgrade switches right away.
- If you are directly upgrading to Vantagepoint 4.5, your database must be at Vantagepoint 4.0.x or higher. Before proceeding, see [Upgrade Scenarios for Vantagepoint 4.5](#).

Use the Upgrade switches to apply software updates to your Vantagepoint installation.

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

- New features are added only to the latest version.
- Except in critical situations, Deltek fixes 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.

Before upgrading, review the [Vantagepoint Release Notes](#) and perform a test conversion and test installation of the new version to ensure that your firm's business processes are working properly in the new version.

Deltek's Global Services team is available to support you as you plan for this upgrade. We offer both technical and custom services to ensure the best possible Deltek experience. Contact DeltekforPSConsulting@deltek.com.

Important: When you initially run the Setup or SetupAndMigrate switch to set up your Vantagepoint environment, the setup prompts you for a variety of information about your servers and validates that information. Once validated, the information is written to the DeltekVantagepointSettings.xml file at the root of the Vantagepoint 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. Make sure to make a backup of this file before you make any manual edits.

Upgrade Switch

Use the UpgradeWeb switch to upgrade the primary web/application server (the server that was installed using Setup or SetupAndMigrate) to the current Vantagepoint build.

Procedure

Note: When you install on a server without an Internet connection, any acknowledgement and licensing prompts and file downloads occur only on the Download Server.

To run the script with the Upgrade switch:

1. From the installation directory Scripts folder, enter **.\DeltekVantagepoint.ps1 -upgrade**.
The script prompts you for your Deltek Support username and password.
2. Enter your Deltek Support username and password.
The script checks prerequisites, verifies your access to Deltek Vantagepoint, checks your IIS prerequisites, and then opens a new browser window, containing Deltek's licensing terms.
3. Read the licensing terms and, if you agree with them, return to the PowerShell console and select **Yes**.
4. If you have Vantagepoint Intelligence Analysis Cubes deployed and the current maintenance release requires a rebuild of the Analysis Cubes, Vantagepoint displays a prompt instructing you to run the **-IntelligenceSetupOption SetupCube** switch and choose **Option 3**. You should do that now.
5. Enter **Yes** to proceed with the upgrade.
The script attempts to retrieve the report server hostname provided on the initial setup by reading the values in the DeltekVantagepointSettings.xml file.
6. Enter the hostname of your report server (if the value was not automatically retrieved) and press ENTER. This must be the machine name, not the FQDN or the IP address.
When you enter the hostname, the script uses it to build a URL to the report server, which is the default value you will see in brackets. (Note that your actual FQDN will likely be different and must be tied to the SSL certificate). The server URL must be SSL secured.

If the script cannot connect to the server, it prompts you to confirm this information:

- Report server name (the default is [HostName])
- Report server URL, in the format [https://FQDN/ReportServer]

If you are using a named instance for your Reporting Services installation (for example, if you are performing a SQL Express installation), your virtual directory is probably in the format: ReportServer_<InstanceName>. Your report server databases is probably in the form ReportServer\$<InstanceName>. The script checks for your report server database names and prompts you if a connection cannot be made.

The script attempts to retrieve the report server URL provided on the initial setup by reading the values in the DeltekVantagepointSettings.xml file.

If the Report Server URL was not automatically retrieved, you will be prompted for it.

If the Report Server URL presented in brackets is correct, press ENTER. If not, change the value to the correct URL for your Report Server and press ENTER.

The script connects to the report server and validates the server's TLS configuration.

The script attempts to retrieve the database server provided on the initial setup by reading the values in the DeltekVantagepointSettings.xml file. If it cannot retrieve the value, it prompts you for the information needed to connect to your database server.

7. Identify your database server.

- Enter the name of your database server (if the value was not automatically retrieved). If you are using a named SQL instance, identify the server in the form Server\Instance.
- The script attempts, via Windows Management Instrumentation, to obtain the port that your SQL Server instance is listening on and validate that a connection can be made. If a port cannot be determined, the connection attempt is made on TCP port 1433. If a connection still cannot be made, the script prompts you for the port on which your SQL Instance is listening. If a connection still cannot be made, the script prompts you to check that the server name is correct and that the necessary ports are open in the firewall.
- If you are using dynamic ports, see the [firewall information](#) in this document.

If the connection is successful, the script attempts to retrieve the database username provided on the initial setup by reading the values in the DeltekVantagepointSettings.xml file. If the value cannot be retrieved, the script prompts you for your database username.

8. Enter your database username (if the value was not automatically retrieved). This should be either a SQL login or a Windows account. The default is [WI] for Windows Integrated.

The account must be a member of the SQL server sysadmin fixed server role. The script checks for this.

The script connects to the database server and validates the server's TLS configuration.

9. The script prompts your for the Weblink password so that it can retrieve database information for upgrade. Enter the Weblink password.

It then prompts you start the upgrade and asks whether you have database backups.

10. Enter **Yes** if you have backups or **No** if you do not (if you enter **No**, the script exits). The default is **No**.

The script will now perform the upgrade process.

Setup Steps Performed by the Script

After you enter all of the information needed to run DeltekVantagepoint.ps1 using the Upgrade switch, the script completes the following steps:

1. The script stops the W3SVC (IIS) and Process Server services.
2. The script removes any older database upgrade scripts from the Databases\Scripts folder.
3. The script downloads and extracts the new Vantagepoint build and removes the prior build.
4. The script searches for custom installers to deploy. If there are no custom installers found, the files are extracted to the appropriate locations.
5. The script creates the Reporting web application.
6. The script updates the Vantagepoint Mobile configuration files.
7. The script updates the DeltekVantagepointSettings.xml file with the new build information.
8. The script upgrades all databases in databases.enc to the current build.
9. The script restarts the services stopped in Step 1 above.
10. The script creates a backup of your current web configuration file and checks for changes on specific configuration options. If there are changes, the script notifies you. You must manually make the changes to the new web configuration file. For more information, see [Important Note for Vantagepoint 4.0 Upgrades](#). If Windows Authentication is enabled, setup will automatically detect this and make the IIS and web.configuration changes necessary for third-party integrations that utilize the Vantagepoint API to function correctly. For more information, see [Important Configuration Changes for Vantagepoint API](#).
11. The script reports on the outcome of the upgrade.
12. The script loads reports to the report server for all languages. The report loading process can take up to 10 minutes for each language. Depending on the number of processor cores in your report server, multiple languages may be loaded concurrently. If reports for a particular language fail to load, the script will attempt to reload that language.
13. If the script extracted custom installation files, it loads custom reports for all languages.
14. If you deployed Vantagepoint Intelligence Analysis Cubes and Vantagepoint requires a cube rebuild for the upgrade, a reminder to rebuild the Analysis Cubes displays. If there are other Analysis Cube updates that do not require a rebuild, the upgrade process performs the necessary updates to all Analysis Cubes deployed.

UpgradeWebApp Switch

Use the UpgradeWebApp switch to upgrade a secondary web/application server to the current Vantagepoint build.

Procedure

Note: When you install on a server without an Internet connection, any acknowledgement and licensing prompts and file downloads occur only on the Download Server.

To run the script with the UpgradeWebApp switch:

1. From the installation directory Scripts folder, enter **.DeltekVantagepoint.ps1 -upgradewebapp**.
The script prompts you for your Deltek Support username and password.
2. Enter your Deltek Support username and password.
The script checks prerequisites, verifies your access to Deltek Vantagepoint, checks your IIS prerequisites, and then opens a new browser window, containing Deltek's licensing terms.
3. Read the licensing terms and, if you agree with them, return to the PowerShell console and select **Yes**.
The script prompts you to start the upgrade and asks whether you have database backups.
4. Enter **Yes** if you have backups or **No** if you do not (if you enter **No**, the script exits). The default is **No**.
The script performs the upgrade process.

Setup Steps Performed by the Script

After you enter all of the information needed to run DeltekVantagepoint.ps1 using the UpgradeWebApp switch, the script completes the following steps:

1. The script stops the W3SVC (IIS) and Process Server services
2. The script downloads and extracts the new Vantagepoint build and removes the prior build.
3. The script searches for custom installers to deploy. If no custom installers are found, the files are extracted to the appropriate locations.
4. The script updates the Vantagepoint Mobile configuration files.
5. The script updates the DeltekVantagepointSettings.xml file with the new build information.
6. The script restarts the services stopped in Step 1 above.
7. The script creates a backup of your current web configuration file and checks for changes on specific configuration options. If there are changes, the script notifies you. You must manually make the changes to the new web configuration file. For more information, see [Important Note for Vantagepoint 4.0 Upgrades](#). If Windows Authentication is enabled, setup automatically detects this and makes the IIS and web.configuration changes necessary for third-party integrations that utilize the Vantagepoint API to function correctly. For more information, see [Important Configuration Changes for Vantagepoint API](#).
8. The script reports on the outcome of the upgrade.

UpgradeProcessServer Switch

Use the UpgradeProcessServer switch to upgrade a dedicated process server installation to the current Vantagepoint version.

You do not need to run this switch if you have a process server installed as part of a web/application tier installation. In this scenario, the Upgrade and UpgradeWebApp switches will also upgrade the process server installation.

Procedure

Note: When you install on a server without an Internet connection, any acknowledgement and licensing prompts and file downloads occur only on the Download Server.

To run the script with the UpgradeProcessServer switch:

1. From the installation directory Scripts folder, enter **.\DeltekVantagepoint.ps1 - upgradeprocessserver**.
The script prompts you for your Deltek Support username and password.
2. Enter your Deltek Support username and password.
The script checks prerequisites, verifies your access to Deltek Vantagepoint, checks your IIS prerequisites, and then opens a new browser window, containing Deltek's licensing terms.
3. Read the licensing terms and, if you agree with them, return to the PowerShell console and select **Yes**.
The script prompts you to start the upgrade and asks whether you have database backups.
4. Enter **Yes** if you have backups or **No** if you do not (if you enter **No**, the script exits). The default is **No**.
The script performs the upgrade process.

Setup Steps Performed by the Script

After you enter all of the information needed to run DeltekVantagepoint.ps1 using the UpgradeProcessServer switch, the script completes the following steps:

1. The script stops the W3SVC (IIS) and Process Server services.
2. The script downloads and extracts the new Vantagepoint build and removes the prior build.
3. The script searches for custom installers to deploy. If no custom installers are found, the files are extracted to the appropriate locations.
4. The script updates the DeltekVantagepointSettings.xml file with the new build information.
5. The script restarts the W3SVC (IIS) and Process Server services.

UpgradeDatabases Switch

Use the UpgradeDatabases switch to upgrade all databases in Databases.enc to the current Vantagepoint build.

Procedure

To run the script with the UpgradeDatabases switch:

1. From the installation directory Scripts folder, enter **.\DeltekVantagepoint.ps1 - UpgradeDatabases**.

The script prompts you for your Deltek Support username and password.

2. Enter your Deltek Support username and password.

The script checks prerequisites and verifies your access to Deltek Vantagepoint, and then attempts to retrieve the database server value provided on the initial setup by reading the values in the DeltekVantagepointSettings.xml file. If it cannot retrieve the value, it prompts you for the information needed to connect to your database server.

3. Identify your database server.

- Enter the name of your database server (if the value was not automatically retrieved). If you are using a named SQL instance, identify the server in the form Server\Instance.
- The script attempts, via Windows Management Instrumentation, to obtain the port that your SQL Server instance is listening on and validate that a connection can be made. If a port cannot be determined, the connection attempt is made on TCP port 1433. If a connection still cannot be made, the script prompts you for the port on which your SQL Instance is listening. If a connection still cannot be made, the script prompts you to check that the server name is correct and that the necessary ports are open in the firewall.
- If you are using dynamic ports, see the [firewall information](#) in this document.

If the connection is successful, the script attempts to retrieve the database username provided on the initial setup by reading the values in the DeltekVantagepointSettings.xml file. If the value cannot be retrieved, the script prompts you for your database username.

4. Enter your database username (if the value was not automatically retrieved). This should be either a SQL login or a Windows account. The default is [WI] for Windows Integrated.

The account must be a member of the SQL server sysadmin fixed server role. The script checks for this.

The script connects to the database server and validates the server's TLS configuration. Then it prompts you start the upgrade.

5. Enter **Yes** to start the upgrade of all databases in Databases.enc or **No** if you do not (if you enter **No**, the script exits). The default is **No**.

The script prompts you for the Weblink password to obtain the list of databases to upgrade.

6. Enter the Weblink password.

The script performs the database upgrade process.

Setup Steps Performed by the Script

The UpgradeDatabases switch loops through all databases in Databases.enc and runs the current build upgrade script against each database in turn. The result of each database upgrade is displayed. The database upgrade logs can be found in the Logs\<date_timestamp\JobsSQL\ folder.

RunSQLScriptOnSelectedDatabases Switch

Use the RunSQLScriptOnSelectedDatabases switch to run .SQL scripts on specific databases in Databases.enc.

Procedure

To run the script with the RunSQLScriptOnSelectedDatabases switch:

1. From the installation directory Scripts folder, enter **.\DeltekVantagepoint.ps1 - RunSQLScriptOnSelectedDatabases**.

The script prompts you for your Deltek Support username and password.

2. Enter your Deltek Support username and password.

The script checks prerequisites and verifies your access to Deltek Vantagepoint.

Your Windows account must have db_owner rights to any selected database that is configured for Windows Integrated Authentication.

If the database is not configured for Windows Integrated Authentication, the script uses the SQL Login/Password when connecting to the database.

3. Select the .SQL script to run in Databases\Scripts directory in your Vantagepoint installation directory. Or, browse to a different location to select the script.
4. Enter your Weblink password.
Vantagepoint databases defined in the dtbases.enc file display.
5. Select the databases you want to have the .SQL script run against. To select more than one database, press the CTRL key and select the databases.
6. Click OK.

The databases you selected display. The .SQL script is executed on each database.

Setup Steps Performed by the Script

The RunSQLScriptOnSelectedDatabases switch loops through all selected databases in Databases.enc and runs the selected .SQL script against each database in turn. The result of the script is displayed.

A log of each script execution can be found in the Logs\<date_timestamp folder with the name of the script, the database and the timestamp.

Uninstall Switch

Use the Uninstall switch to remove Vantagepoint from your web/application server. This process removes the following components:

- IIS Application Pool (DeltekVantagepointAppPool)
- IIS Applications (Vantagepoint, Vantagepoint\App, VantagepointClient)

- Deltek Vantagepoint Process Server service
- All files and directories in the installation directory except those in \Scripts and \Logs

It will also prompt you to delete the local account (DeltekVantagepoint) if one exists.

Note: The Uninstall switch will not remove local accounts created by the Setup or SetupAndMigrate switches on the report or database servers. Nor will it remove databases, SQL Logins, or loaded reports on the report server.

Procedure

To run the script with the Uninstall switch:

1. From the installation directory Scripts folder, enter **.\DeltekVantagepoint.ps1 -Uninstall**.
After the [script prerequisite checks](#) have been performed and your access to Deltek Vantagepoint has been verified, the script asks you if you want to continue with the uninstall process.
2. Enter **Yes** to start the uninstall process.

Setup Steps Performed by the Script

The script completes the following steps:

- The script removes the Vantagepoint, Vantagepoint\App, and VantagepointClient IIS applications.
- The script removes the DeltekVantagepointApplicationPool IIS application pool.
- The script removes the Deltek Vantagepoint Process Server service.
- The script checks to see if the local DeltekVantagepoint account exists and, if it does, asks you if you want to delete the account.
- The script removes the installation files, except for the \Scripts and \Logs folders.

InstallProcessServerService and RemoveProcessServerService Switches

Use these switches to install and uninstall the Vantagepoint Process Server service:

Switch	Use this switch to...
InstallProcessServerService	If you experience an error installing the service using the Setup or SetupAndMigrate switch, use the InstallProcessServer switch to install the service.
RemoveProcessServerService	If you experience an error uninstalling the service using the Uninstall switch, use the RemoveProcessServer switch to uninstall the service.

Procedure

To run the script with the InstallProcessServerService or RemoveProcessServerService switch:

1. From the installation directory Scripts folder, enter **.\DeltekVantagepoint.ps1 – AdditionalSetupOption InstallProcessServerService** or **.\DeltekVantagepoint.ps1 – AdditionalSetupOption RemoveProcessServerService**.
2. Respond to the prompt:
 - If you are using the InstallProcessServerService switch, enter the service account name and password. The script validates the information that you enter and adds the user to the local administrator group (if applicable). The script installs the service, sets the identity, and grants the necessary service rights.
 - If you are using the RemoveProcessServerService switch, enter **Yes** to uninstall the service.

SetServiceAccounts Switch

When you run the DeltekVantagepoint.ps1 script using the Setup or SetupAndMigrate switch, all Vantagepoint service accounts are configured by default using the account identified as the Application Pool Identity account. These accounts include:

- IIS Application Pool Identity (DeltekVantagepointAppPool)
- Service account for the Vantagepoint Process Server service
- Account used for authentication to Reporting Services (the value entered in the Report Server Windows Username field on the Report Server tab in Weblink)

If you configured a local account (for example, DeltekVantagepoint), use the SetServiceAccount switch to configure the service accounts listed above to use a domain account. To use this switch, the new account must be a domain account.

If you want to configure local service accounts after installation, you will need to perform manual steps to configure the service account to use a domain account.

Procedure

To run the script with the SetServiceAccounts switch:

1. From the installation directory Scripts folder, enter **.\DeltekVantagepoint.ps1 – AdditionalSetupOption SetServiceAccounts**.

The script checks for prerequisites. The script also prompts you for the information needed to use this switch, including the name of the IIS Application Pool ([DeltekVantagepointAppPool]), the Weblink password and the name of the database entry from Databases.enc.

2. Enter this information.

The script displays the service accounts currently in use and asks which account you want to change:

- a. Change Service Account for the IIS Application Pool Identity.
- b. Change Service Account for the Deltek Vantagepoint Process Server service.
- c. Change Service Account for the Report Server user account.
- d. Exit.

3. Select an option.

The script prompts you for the name and password for the account that you want to change and performs these additional steps:

If you chose...	This happens...
Change Service Account for the IIS Application Pool Identity	The script prompts you for database server connection information so that it can update the FileStream database rights for the new account and the identity of the IIS Application Pool.
Change Service Account for the Deltek Vantagepoint Process Server service	The script updates the logon account for the Vantagepoint Process Server service and grants Service Local Security Policy rights to the logon account.
Change Service Account for the Report Server user account	The script grants System Administrator and Content Manager rights to Reporting Services and updates the database entry in databases.enc for the database that you identified in Step 1.

The script updates the service account that you chose and prompts you to change another service account.

4. Enter **4 (Exit)** when you are finished updating the service accounts.

If a shared databases.enc path is in use (see [Configure a Shared Location for Databases.enc](#)) and either the Application Pool Identity or the Process Server Identity are chosen to be updated, the script automatically adds the new account to the share permissions. The script does not remove the prior account. If needed, remove the prior account from the share permissions manually.

LoadReports Switch

Use the LoadReports switch to load reports if you experienced an error loading reports using the Setup or SetupAndMigrate switch.

Procedure

To run the script with the LoadReports switch:

1. From the installation directory Scripts folder, enter **.\DeltekVantagepoint.ps1 – AdditionalSetupOption LoadReports**.

The script checks for prerequisites. If necessary, the script prompts you for the information needed to connect to the report server.

2. Enter the information needed to connect to the report server.

The script prompts you for the report server root folder. You may have several report root folders if the report server is being shared between different environments.

3. Enter the name of the report server root folder (the default is Vantagepoint).

The script validates that the connection can be made, loads the reports for all languages, and displays the results of the loading process. The report loading process can take up to 10 minutes for each language. Depending on the number of processor cores in your report server, multiple

languages may be loaded concurrently. If reports for a particular language fail to load, the script will attempt to reload that language.

Setup Steps Performed by the Script

- If needed, the scripts prompts you for the Report Server service account.

Note: If you changed accounts, using the `SetServiceAccounts` switch or manually, enter the account that has the System Administrator and Content Manager rights to your reporting services instance.

- The script validates the account information.
- If needed, the script prompts you for information about your reporting services instance and validates that a successful connection can be made using the account information provided in the first bullet item.
- The script loads reports on the report server for all enabled languages.

LoadReportsCustom Switch

If you experienced an error using the `SetupCustom` switch, use the `LoadReportsCustom` switch to load custom reports.

Procedure

To run the script with the `LoadReportsCustom` switch:

1. From the installation directory Scripts folder, enter `.\DeltekVantagepoint.ps1 – AdditionalSetupOption LoadReportsCustom`.

The script checks for prerequisites. If the service account name is not saved in the `DeltekVantagepointSettings.xml` file, the script prompts you for it.

2. Enter the service account name; use the account already configured as the Report Server Windows Username in Weblink.

If necessary, the script prompts you for the information needed to connect to the report server.

3. Enter the information needed to connect to the report server.

The script validates that the connection can be made, loads the reports for all languages, and displays the results of the loading process. The report loading process can take up to 10 minutes for each language. Depending on the number of processor cores in your report server, multiple languages may be loaded concurrently. If reports for a particular language fail to load, the script will attempt to reload that language.

Setup Steps Performed by the Script

- If needed, the scripts prompts you for the Report Server service account.

Note: If you changed accounts, using the `SetServiceAccounts` switch or manually, enter the account that has the System Administrator and Content Manager rights to your reporting services instance.

- The script validates the account information.
- If needed, the script prompts you for information about your reporting services instance and validates that a successful connection can be made using the account information provided in the first bullet item.
- The script loads reports on the report server for all enabled languages.

EnableIISRequiredFeatures Switch

Use the `EnableIISRequiredFeatures` switch if the IIS prerequisite check indicates that you have not enabled all required IIS modules. This switch will use the `Enable-WindowsOptionalFeature` PowerShell cmdlet to enable required IIS modules that are currently disabled.

Procedure

To run the script with the `EnableIISRequiredFeatures` switch:

1. From the installation directory Scripts folder, enter **`.\DeltekVantagepoint.ps1 – AdditionalSetupOption EnableIISRequiredFeatures`**.

The script checks for prerequisites and checks to see if any required IIS modules are not installed. It displays the names of any missing modules and prompts you to enable them.

2. Enter **Yes** to enable all required modules.

This process takes several minutes

Setup Steps Performed by the Script

The script completes the following steps:

- The script checks each required IIS feature to see if it is enabled.
- The script provides a list of required features that are currently disabled and prompt you to enable them.
- If you enter **Yes**, the script enables the required features.

GetLicenseFile Switch

The `GetLicenseFile` switch generates the Vantagepoint module passwords for your database if they need to be generated as a separate step. The script generates the license file as a .SQL script and places it in the `\Databases\Scripts` folder with the name `DeltekVantagepointModulePasswords<ClientID>.sql`, in which `<clientID>` is your Deltek customer ID number.

You can run this .SQL script against your database using SQL Server Management Studio.

The `Setup`, `SetupAndMigrate`, `SetupDatabaseNew`, and `MigrateDatabase` switches also call this function and automatically apply the created .SQL script against the database.

Procedure

From the installation directory Scripts folder, enter **.\DeltekVantagepoint.ps1 – AdditionalSetupOption GetLicenseFile**.

The script generates the license file.

Setup Steps Performed by the Script

The script generates the license file as a .SQL script and places it in the \Databases\Scripts folder with the name DeltekVantagepointModulePasswords<ClientID>.sql.

UpdateLicenseFile Switch

The UpdateLicenseFile switch generates the Vantagepoint module passwords for your database when they need to be generated as a separate step. This happens when licensing information changes, such as when you add a module or add new licenses.

The script generates the license file as a .SQL script and places it in the \Databases\Scripts folder with the name DeltekVantagepointModulePasswords<ClientID>.sql, in which <clientID> is your Deltek customer ID number. The script automatically runs the generated SQL script against all databases in the databases.enc file. If needed, you can run this .SQL script against additional databases using SQL Server Management Studio.

Procedure

From the installation directory Scripts folder, enter **.\DeltekVantagepoint.ps1 – AdditionalSetupOption UpdateLicenseFile**.

The script generates the license file.

Setup Steps Performed by the Script

The script generates the license file as a .SQL script and places it in the \Databases\Scripts folder with the name DeltekVantagepointModulePasswords<ClientID>.sql.

The script automatically runs the generated SQL script against all databases in the databases.enc file.

EnableWindowsExplorerPowerShellIntegration Switch

Use the EnableWindowsExplorerPowerShellIntegration switch to enable the **Open Windows PowerShell Here as Administrator** menu option in Windows Explorer. This option displays in the right-click context menu in Windows Explorer.

Procedure

From the installation directory Scripts folder, enter **.\DeltekVantagepoint.ps1 – AdditionalSetupOption EnableWindowsExplorerPowerShellIntegration**.

Setup Steps Performed by the Script

The script makes the necessary registry changes to allow the right-click **Open Windows PowerShell Here as Administrator** menu option.

CreateDeltekVantagepointCMDFile Switch

Use this switch to create a Windows batch file (.cmd) that launches PowerShell using the RemoteSigned PowerShell execution policy. Use this switch if your organization has a more restrictive execution policy, such as Restricted, and you cannot change the policy.

The batch file will set the execution policy only for the batch file process, whereas using Set-ExecutionPolicy from the PowerShell console prompt will, by default, set the policy for the machine. See [PowerShell Execution Policy](#) for more information.

From the installation directory Scripts folder, enter **.\DeltekVantagepoint.ps1 – AdditionalSetupOption CreateDeltekVantagepointCMDFile**.

Setup Steps Performed by the Script

The script creates a batch file (DeltekVantagepoint.cmd) in the root of the Deltek Vantagepoint installation directory (<drive>:\Program Files\Deltek\Vantagepoint) that you can use to launch the PowerShell console with the execution policy set to RemoteSigned.

Procedure

To pass the switch parameter to the batch file, follow the steps below:

1. Open the PowerShell console (or a Windows command prompt) using **Run as Administrator**.
2. Enter the following:

DeltekVantagepointCMD -<switch parameter> (e.g. DeltekVantagepointCMD –Setup)

Cleanup Switch

Use this switch to remove older database upgrade scripts from the Databases\Scripts folder. Run this switch after upgrades to remove obsolete files.

Procedure

From the installation directory Scripts folder, enter **.\DeltekVantagepoint.ps1 – AdditionalSetupOption Cleanup**.

Setup Steps Performed by the Script

This switch removes the database upgrade scripts that are no longer applicable to the current installation.

ChangeWeblinkPassword Switch

Use this switch to change the Weblink password. You must know the current password to use this switch.

Procedure

From the installation directory Scripts folder, enter **.\DeltekVantagepoint.ps1 – AdditionalSetupOption ChangeWeblink**.

Setup Steps Performed by the Script

This switch prompts you for the current Weblink password and then prompts you for a new Weblink password.

ConfigureARR Switch

Use this switch to configure Application Request Routing (Reverse Proxy) for reporting. Reporting Services must be installed on a separate server from the web/application server. See [Create a Reverse Proxy for SQL Reporting Using Application Request Routing \(ARR\)](#) for more information.

Procedure

From the installation directory Scripts folder, enter **.\DeltekVantagepoint.ps1 –AdvancedSetupOption ConfigureARR**.

Setup Steps Performed by the Script

This switch downloads the Application Request Routing installation files, installs the Application Request Routing components, creates the reverse proxy application pool and application in IIS, configures the reverse proxy rules, and updates Weblink with the new report server URL.

ConfigureIISCompression Switch

Use this switch to configure HTTP Compression for IIS, which can improve application performance over latent network connections. See [Configure HTTP Compression](#) for more information.

Procedure

From the installation directory Scripts folder, enter **.\DeltekVantagepoint.ps1 –AdvancedSetupOption ConfigureIISCompression**.

Setup Steps Performed by the Script

This switch enables the necessary IIS HTTP Compression modules (if they are not already enabled) and configures HTTP static and dynamic compression rules.

ConfigureWindowsAuthentication Switch

Use this switch to configure Windows Authentication for Vantagepoint. See [Configure Integrated Security for Vantagepoint](#) for more information.

Procedure

From the installation directory Scripts folder, enter **.\DeltekVantagepoint.ps1 –AdvancedSetupOption ConfigureWindowsAuthentication**.

Setup Steps Performed by the Script

This switch enables the IIS Windows Authentication module (if it is not already enabled), configures Windows Authentication, and checks to see if a custom DNS value is being used for the web server URL and whether a BackConnectionHostNames registry entry is needed for your configuration.

This switch also enables Anonymous Authentication for the Touch folder (CRM/Time applications). The Touch applications handle Windows Authentication differently than Vantagepoint does.

ConfigureAuthenticationPersistence Switch

Use this switch to configure Authentication Persistence for Windows Authentication for Vantagepoint. See [Configure Authentication Persistence](#) for more information.

Procedure

From the installation directory Scripts folder, enter **.\DeltekVantagepoint.ps1 –AdvancedSetupOption ConfigureAuthenticationPersistence**.

Setup Steps Performed by the Script

This switch ensures that Windows Authentication is enabled, asks you if Vantagepoint is accessible over the Internet, configures Authentication Persistence, and updates Weblink with the appropriate Authentication Persistence configuration.

ConfigureDatabaseSessionState Switch

Use this switch to configure Database Session State for Vantagepoint. See [Configure Database Session State for Vantagepoint](#) for more information.

Procedure

From the installation directory Scripts folder, enter **.\DeltekVantagepoint.ps1 –AdvancedSetupOption ConfigureDatabaseSessionState**.

Setup Steps Performed by the Script

This switch connects to your Vantagepoint database server, creates and configures the session state database (Vantagepointsessions), and updates Weblink to use Database Session State.

EnableFailedRequestTracing Switch

Use this switch to enable IIS Failed Request Tracing for Vantagepoint and to configure the rule that controls when a trace runs.

Procedure

From the installation directory Scripts folder, enter **.\DeltekVantagepoint.ps1 –SupportSetupOption EnableFailedRequestTracing**.

Setup Steps Performed by the Script

The script completes the following steps:

- The script displays a warning that changes will be made to the Vantagepoint web.config file, causing all users to lose their sessions.

- The script prompts you to enter information about the conditions under which it should perform a trace: based on an HTTP status code, such as 500; based on the length of the request time, such as 10 seconds; or under both conditions.
- The script backs up the Vantagepoint web.config file.
- The script enables the IIS-HTTP Tracing module if it is not already enabled.
- The script configures the Failed Request Tracing rule.

DisableFailedRequestTracing Switch

Use this switch to disable IIS Failed Request Tracing for Vantagepoint.

Procedure

From the installation directory Scripts folder, enter **.\DeltekVantagepoint.ps1 –SupportSetupOption DisableFailedRequestTracing**.

Setup Steps Performed by the Script

The script completes the following steps:

- The script displays a warning that changes will be made to the Vantagepoint web.config file, causing all users to lose their sessions.
- The script backs up the Vantagepoint web.config file.
- The script removes existing Failed Request Tracing rules.

GetConfigFiles Switch

Use this switch to collect and, if desired, email the configuration files for your Vantagepoint installation.

Procedure

From the installation directory Scripts folder, enter **.\DeltekVantagepoint.ps1 –SupportSetupOption GetConfigFiles**.

Setup Steps Performed by the Script

The script completes the following steps:

- The script asks you whether you want to email the configuration files and, if so, asks for the email address and SMTP information needed to email them.
- The script collects the Vantagepoint and Vantagepoint\app web.config files.
- The script collects the Vantagepoint installation Configuration and Settings .xml files.
- The script collects the Vantagepoint Mobile .ini files.
- The script collects the Report Server configuration file (rsreportserver.config).
- The script collects the SQL Server configuration file (sp_configure).
- The script zips up the collected files.

- If you chose to email the files, the script emails the zipped files. If you did not choose to email them, the script displays the location of the zipped files.
- The script saves email addresses and SMTP information to the DeltekVantagepointSettings.xml file and uses them as default values in the future.

GetAllLogs Switch

Use this switch to collect and, if desired, email the log files from all servers in your Vantagepoint installation.

Procedure

From the installation directory Scripts folder, enter **.\DeltekVantagepoint.ps1 –SupportSetupOption GetAllLogs**.

Setup Steps Performed by the Script

The script completes the following steps:

- The script asks you whether you want to email the log files and, if so, asks for the email address and SMTP information needed to email them.
- The script collects the Vantagepoint setup logs.
- The script collects the SQL Reporting Services logs for the last 7 days.
- The script collects the IIS/HTTP.sys error logs and Failed Request Tracing logs for the last 7 days.
- The script collects the application/system event logs from the web/report and database servers.
- The script collects the SQL Server error logs for the last 30 days.
- The script zips up the collected files.
- If you chose to email the files, the script emails the zipped files. If you did not choose to email them, the script displays the location of the zipped files.
- The script saves email addresses and SMTP information to the DeltekVantagepointSettings.xml file and uses them as default values in the future.

GetSetupLogs Switch

Use this switch to collect and, if desired, email the setup logs from your Vantagepoint installation.

Procedure

From the installation directory Scripts folder, enter **.\DeltekVantagepoint.ps1 –SupportSetupOption GetSetupLogs**.

Setup Steps Performed by the Script

The script completes the following steps:

- The script asks you whether you want to email the log files and, if so, asks for the email address and SMTP information needed to email them.

- The script collects the Vantagepoint setup logs.
- The script zips up the collected log files.
- If you chose to email the files, the script emails the zipped files. If you did not choose to email them, the script displays the location of the zipped files.
- The script saves email addresses and SMTP information to the DeltekVantagepointSettings.xml file and uses them as default values in the future.

GetSSRSLogs Switch

Use this switch to collect and optionally email the SQL Reporting Services logs from your Vantagepoint installation.

Procedure

From the installation directory Scripts folder, enter **.\DeltekVantagepoint.ps1 –SupportSetupOption GetSSRSLogs**.

Setup Steps Performed by the Script

The script completes the following steps:

- The script asks you whether you want to email the log files and, if so, asks for the email address and SMTP information needed to email them.
- The script asks you how many days of logs to collect, with a maximum of 30 days.
- The script collects the SQL Reporting Services logs.
- The script zips up the collected log files.
- If you chose to email the files, the script emails the zipped files. If you did not choose to email them, the script displays the location of the zipped files.
- The script saves email addresses and SMTP information to the DeltekVantagepointSettings.xml file and uses them as default values in the future.

GetIISLogs Switch

Use this switch to collect and, if desired, email the IIS log files from your Vantagepoint installation. These logs include IIS, HTTP.sys error, and, if available, Failed Request Tracing logs.

Procedure

From the installation directory Scripts folder, enter **.\DeltekVantagepoint.ps1 –SupportSetupOption GetIISLogs**.

Setup Steps Performed by the Script

The script completes the following steps:

- The script asks you whether you want to email the log files and, if so, asks for the email address and SMTP information needed to email them.
- The script asks you how many days of logs to collect, with a maximum of 30 days.

- The script collects the IIS, HTTP.sys error, and, if available, Failed Request Tracing logs.
- The script zips up the collected log files.
- If you chose to email the files, the script emails the zipped files. If you did not choose to email them, the script displays the location of the zipped files.
- The script saves email addresses and SMTP information to the DeltekVantagepointSettings.xml file and uses them as default values in the future.

GetEventLogs Switch

Use this switch to collect and, if desired, email the application/system event logs from a specific server in your Vantagepoint installation.

Procedure

From the installation directory Scripts folder, enter **.\DeltekVantagepoint.ps1 –SupportSetupOption GetEventLogs**.

Setup Steps Performed by the Script

The script completes the following steps:

- The script asks you for the name of the server from which you want to collect log files.
- The script asks you whether you want to email the log files and, if so, asks for the email address and SMTP information needed to email them.
- The script collects the application/system event logs from the specified server.
- The script zips up the collected log files.
- If you chose to email the files, the script emails the zipped files. If you did not choose to email them, the script displays the location of the zipped files.
- The script saves email addresses and SMTP information to the DeltekVantagepointSettings.xml file and uses them as default values in the future.

GetSQLExceptions Switch

Use this switch to collect and, if desired, email the SQL Server error logs from your Vantagepoint database server.

Procedure

From the installation directory Scripts folder, enter **.\DeltekVantagepoint.ps1 –SupportSetupOption GetSQLExceptions**.

Setup Steps Performed by the Script

The script completes the following steps:

- The script asks you whether you want to email the log files and, if so, asks for the email address and SMTP information needed to email them.
- The script asks you how many days of logs to collect, with a maximum of 90 days.

- The script collects the SQL Server error logs from the database server.
- The script zips up the collected log files.
- If you chose to email the files, the script emails the zipped files. If you did not choose to email them, the script displays the location of the zipped files.
- The script saves email addresses and SMTP information to the DeltekVantagepointSettings.xml file and uses them as default values in the future.

GetAppUserInQuery Switch

Use this switch to find out who owns a query that has been running for a long time. This switch runs a query against your Vantagepoint database server and returns a list of all SQL Server query SPIDs and the Vantagepoint user who is executing each one. A SPID is a Server Process ID, synonymous with “connection” or “session.”

Procedure

From the installation directory Scripts folder, enter **.\DeltekVantagepoint.ps1 –SupportSetupOption GetAppUserInQuery**.

Setup Steps Performed by the Script

This switch executes the following query, which returns a list of SPIDs and their associated usernames. Press any key to refresh the list or CTRL/C to exit the script.

```
SELECT RTRIM(hostname) AS hostname
, spid
, status
, blocked
, login_time
, (select DATEDIFF(SECOND,login_time,SYSDATETIME())) AS ElapsedTimeSeconds
, RTRIM(program_name) AS program_name
, SUBSTRING(convert(nvarchar(80),context_info), 20, 20) AS Application_Username
FROM master.sys.sysprocesses
where program_name like '%(default)%'
order by ElapsedTimeSeconds desc
```

You can also run this query via SQL Management Studio. When you identify the SPID, run the following command to find out what SQL command is being executed:

```
dbcc inputbuffer(<SPID>)
```

GetActiveRunningReports Switch

Use this switch to execute a web service call to SQL Reporting Services to obtain a list of all actively running reports on the report server.

Procedure

From the installation directory Scripts folder, enter **.\DeltekVantagepoint.ps1 –SupportSetupOption GetActiveRunningReports**.

Setup Steps Performed by the Script

This switch executes a web service call to Reporting Services. The call returns the name of the report, the user executing the report, the database against which the report is running, and the start time of the report.

Press any key to refresh the list or CTRL/C to exit the script.

GetActiveWebRequests Switch

Use this switch to execute a request to IIS to obtain a list of all actively running requests executing in IIS.

Procedure

From the installation directory Scripts folder, enter **.\DeltekVantagepoint.ps1 –SupportSetupOption GetActiveWebRequests**.

Setup Steps Performed by the Script

The script completes the following steps:

- The switch enables the IIS-RequestMonitor if it is not already enabled.
- The switch executes a request to IIS to list the actively running web requests.
- The switch returns the verb, URL, local port, host name, client IP address and elapsed time (in milliseconds) of each request, and sorts requests so that the longest running request is listed last.
- The switch prompts you to press any key to refresh the list or CTRL/C to exit the script.

Analysis Cubes Switches

The IntelligenceSetupOption with sub-switches (SetupCube, UninstallCube, and UpdateCubeDtsxPackages) are specific to the Vantagepoint Intelligence module and are used to deploy or uninstall Vantagepoint Intelligence Analysis Cubes. For detailed information on these switches, refer to the *Vantagepoint Intelligence Installation and Configuration Guide*.

GenerateMachineKey Switch

Use this switch to generate a <machinekey> element that is required when you need to balance the load across web servers. The switch generates the <machinekey> element which you can copy and paste into the <system.web> element of the Vantagepoint web configuration file on each load balanced web server.

The same <machinekey> element is required on all load balanced web servers. This means that you should **not** re-run the switch to generate a new key for each web server. Copy and paste the exact <machinekey> element generated by the switch to the <system.web> element of the web.config file on each load balanced web server.

For more information, refer to the article on [Resolving view state MAC errors](#) in Microsoft Support.

Procedure

From the installation directory Scripts folder, enter **\DeltekVantagepoint.ps1 –SupportSetupOption GenerateMachineKey** .

Setup Steps Performed by the Script

The script completes the following steps:

- Prompts for the decryption algorithm to use. The choices are AES, DES, or 3DES.
- Prompts for the validation algorithm to use. The choices are MD5, SHA1, HMACSHA256, HMACSHA384, OR HMACSHA512.
- Generates a <machinekey> element as the output of the script based on the inputs provided. For example:

```
<machineKey decryption="AES"
decryptionKey="B09ED31D4160ED15E3E7BD656770DEC4F745D702915CD9C76C2D9CFB0274DFDA
" validation="HMACSHA256"
validationKey="248C1F781B3BC17662930E385B54BD564F78BCF3ABE2BFB0C6AF8DBA36F1D317
9B1A73C9DA6DCBD635053A7150E38F51A1F860CB561650A5685EAEC3AA5AECF1" />
```

The default algorithms are the same as that of Microsoft, which are “AES” for the decryption algorithm and “HMACSHA256” for the validation algorithm. To change the default algorithms, refer to the article on [Resolving view state MAC errors](#) in Microsoft Support.

- Detects if a <machinekey> element already exists in the web.config file.

If a <machinekey> element does not exist, the script prompts you to add the generated machine key to the web.config file on the current web server.

IMPORTANT: You must manually insert this exact machine key into the Vantagepoint web.config file on each additional load balanced web server. Refer to [Insert the <machinekey> element into web.config file](#).

Insert the <machinekey> element into web.config file

Insert the <machinekey> element into the Vantagepoint web.config file on each load balanced web server.

NOTE: Making changes to the web.config file causes all users to lose their session. Deltek recommends that you make these changes during a maintenance window.

1. Run the Notepad.exe as an Administrator.
2. Open the web.config file in <drive>:\Program Files\Deltek\Vantagepoint\Web.
3. Locate the <system.web> element under the <configuration> element. There may be additional <system.web> elements under several <location> tags. Do **not** place the <machinekey> element in the <locations> element.

The system.web elements look similar to the following:

```
<system.web>

    <httpRuntime targetFramework="4.5" executionTimeout="900"
maxRequestLength="128000" maxQueryStringLength="32768" maxUrlLength="65536"
requestPathInvalidCharacters="*,&,\,?" requestValidationMode="2.0"
enableVersionHeader="false" />
```

```

    <pages enableSessionState="true" enableViewState="true"
enableViewStateMac="true" />

    <compilation defaultLanguage="vb" debug="true" targetFramework="4.5" />

    <customErrors mode="Off" />

    <globalization requestEncoding="utf-8" responseEncoding="utf-8"
culture="en-US" uiCulture="en-US" />

</system.web>

```

4. Place the <machinekey> element just above the system.web end tag </system.web> as follows:

```

<system.web>

    <httpRuntime targetFramework="4.5" executionTimeout="900"
maxRequestLength="128000" maxQueryStringLength="32768" maxUrlLength="65536"
requestPathInvalidCharacters="*,&,\,?" requestValidationMode="2.0"
enableVersionHeader="false" />

    <pages enableSessionState="true" enableViewState="true"
enableViewStateMac="true" />

    <compilation defaultLanguage="vb" debug="true" targetFramework="4.5" />

    <customErrors mode="Off" />

    <globalization requestEncoding="utf-8" responseEncoding="utf-8"
culture="en-US" uiCulture="en-US" />

    <machineKey decryption="AES"
decryptionKey="B09ED31D4160ED15E3E7BD656770DEC4F745D702915CD9C76C2D9CFB0274DFDA
" validation="HMACSHA256"
validationKey="248C1F781B3BC17662930E385B54BD564F78BCF3ABE2BFB0C6AF8DBA36F1D317
9B1A73C9DA6DCBD635053A7150E38F51A1F860CB561650A5685EAEC3AA5AECF1" />

</system.web>

```

Optional Sub-Switches

Use these sub-switches if you are installing Vantagepoint for a specific configuration. For example, you may want to install an earlier build of Vantagepoint. Or, you may want to install Vantagepoint in a development environment but share resources via a production environment.

Sub-Switch	Use with Switches	Use this switch to...	Read this section...
-VersionToInstall <version>	Setup SetupAndMigrate SetupWebApp SetupProcessServer	Install a specific Vantagepoint build that is not the latest one	Sub-switches for Specific Configurations
-SkipLoadReports true	Setup SetupAndMigrate Upgrade	Install the latest build of Vantagepoint in a development environment, but share database and report tiers with the production environment	Sub-switches for Specific Configurations

Vantagepoint URLs

After installation, your Vantagepoint folder will contain a VantagepointURL.txt file listing your specific URLs. Your URLs for Vantagepoint will be in these formats:

Destination	URL Format
Launch Page	<a href="https://<FQDN>/Vantagepoint">https://<FQDN>/Vantagepoint
Web Client	<a href="https://<FQDN>/Vantagepoint/app">https://<FQDN>/Vantagepoint/app
Desktop Client ("Smart Client")	<a href="https://<FQDN>/VantagepointClient">https://<FQDN>/VantagepointClient To launch the desktop client, you must append /DeltekVision.application to the URL, like this: <a href="https://<FQDN>/VantagepointClient/DeltekVision.application">https://<FQDN>/VantagepointClient/DeltekVision.application . Alternatively, you can go to the launch page (<a href="https://<FQDN>/Vantagepoint">https://<FQDN>/Vantagepoint) and select the desktop client. The desktop client link appears on the launch page only if you run Vantagepoint from Internet Explorer or Edge.
Mobile Time and Expense*	<a href="https://<yourdomain>/vantagepoint/touch/crm/visionshared/backend/vantagepointcrmurl">https://<yourdomain>/vantagepoint/touch/crm/visionshared/backend/vantagepointcrmurl , where <yourdomain> refers to the user's company domain information
Mobile CRM*	<a href="https://<yourdomain>/vantagepoint/touch/time/visionshared/backend/vantagepointtimeurl">https://<yourdomain>/vantagepoint/touch/time/visionshared/backend/vantagepointtimeurl , where <yourdomain> refers to the user's company domain information
Weblink	You must run Weblink on the web/application server using the shortcut created in the Vantagepoint installation folder. Weblink is no longer a web application; you can only access it on the server.

Set Up Single Sign-On for Vantagepoint with Microsoft Azure Active Directory

Microsoft Azure Active Directory's single sign-on (SSO) feature enables users to log on to Vantagepoint using their Windows usernames and passwords, instead of using separate Vantagepoint usernames and passwords. Vantagepoint supports the single tenant and multi-tenant options for registering an application within the Azure portal. Refer to [Set Up Single Sign-On for Vantagepoint with Microsoft Azure Active Directory](#) for detailed steps.

The steps to configure Vantagepoint with SSO for on-premise deployments are the same as Vantagepoint hosted in the deltekfirst.com cloud with one difference; the Vantagepoint launch page URL from Vantagepoint URLs table shown in the above section (<https://<FQDN>/vantagepoint>) will be used in place of the customer URL that is specified in the reply URL settings (<https://abcengineers.deltekfirst.com/abcengineers>).

For example, if your Vantagepoint server is named **webserver1** in your applebartlett.com domain, then your customer URL per the instructions would be **<https://webserver1.applebartlett.com/vantagepoint>**.

Mobile Applications and Vantagepoint

If you are migrating from Deltek Vision, GovWin CM, or Ajera CRM and use the mobile applications, you must download the Vantagepoint Mobile CRM and/or Vantagepoint Mobile Time and Expense applications from your apps store.

Touch Server URL Setup in Email

Logging on for the first time no longer requires users to enter the complete Touch Server URL. You send them an email message containing a link that either directs them to the appropriate app store (if the mobile application is not yet installed) or populates the **Touch Server URL** field with their company URL.

Touch Server URL Format

For Vantagepoint applications installed locally, the SAASDEPLOY setting is set to **false** in the configuration.ini file. In this case, the Touch Server URL follows the format `https://<yourdomain>/vantagepoint/touch/<mobile application>/visionshared/backend/vantagepoint<mobileapplication>url.php`, where <yourdomain> refers to the user's company domain information and <mobileapplication> is replaced either by **crm** or **time**.

ProductApplication.php

This file performs the linking and passes the **Touch Server URL** value to the mobile application or redirects users to the appropriate app store.

Link for Customers

The link that you send to users is a hyperlink. When users click the hyperlink, the following scenarios occur:

1. If the mobile application is not installed, it takes them to the appropriate app store to download the application.
 - Users download the application from the app store.
 - They click the link again (and proceed to step 2).
2. If the application is installed, the **Touch Server URL** field is automatically populated with their company URL.
3. Users tap the **Connect** button to connect to the Touch Server.

Create the Link to Email Users

Each application may have specific steps required to create a hyperlink. This section describes the steps that apply to Microsoft Outlook. For other applications, see the documentation on creating a hyperlink.

1. Use the following format for the hyperlink:

`https://<yourdomain>/vantagepoint/touch/<mobileapplication>/visionshared/backend/vantagepoint<mobileapplication>url`

The domain must be externally accessible to devices on the Internet. The following part of the hyperlink, however, is fixed:

`vantagepoint/touch/<mobileapplication>/visionshared/backend/vantagepoint<mobileapplication>url`

2. Create the instructional text in the email message where you will embed the link.
3. Highlight the word “here,” right-click, and select **Hyperlink** from the menu (alternatively, click the Insert tab, and click the **Hyperlink** button).
4. Paste the hyperlink into the **Address** field of the dialog box, and click **OK**.

Example: You have been given access to the mobile application. Click this link from your device to start using it:

<https://<yourdomain>/vantagepoint/touch/crm/visionshared/backend/vantagepointcrmurl>

- If you have not yet installed the mobile application, you will need to click the link twice: once to install the app and once after installation to populate your company's URL. If you have already been using the mobile application on your device, there is no need to click the link.
- If you cannot click the link, you can also copy and paste it into the browser on your device.

When users receive the email and click the link as well as the mobile application is installed, the **Server URL** screen displays.

Configure Vantagepoint

Once the Vantagepoint software is installed, you can begin configuring Vantagepoint to meet your company's needs. Review the following documentation.

- [Online help](#)
- [What's new? / release notes](#)
- [How-to videos](#)
- [Settings and Configuration guide](#)

Back Up Your Vantagepoint Database

During installation of the database tier, the Vantagepoint backup device is created on the Database Server to allow you to perform ad hoc database backups before major data changes or processes take place.

To back up the database, click **Utilities » Backup Database** on the Vantagepoint desktop application Navigation menu.

Set Up Silent Installation

Use the SilentInstall switch with the DeltekVantagepoint.ps1 PowerShell script to run the Deltek Vantagepoint installer without manual intervention. Use it to perform multiple installation operations as one automated process.

The silent installation is designed to help you install into multiple environments quickly (Dev, Test, and Production) and is not intended for single-environment use.

To prepare for using the silent installation process, you create an xml-based “response file” that contains one or more installation steps. For example, the first step might run the installation script with the CheckPreReq switch, the second with the Setup switch, and the third with the DownloadDatabases switch.

When you use the SilentInstall switch, this response file is passed to the switch as a parameter and determines what steps the SilentInstall performs.

Basic Setup Steps

Follow these basic steps to set up silent installation:

1. Generate password files for the passwords needed to perform the installation.
2. Generate a response file that determines what steps the silent installation performs and “answers” the installer when the installer prompts you for information.
3. Run the DeltekVantagepoint.ps1 PowerShell script with the SilentInstall switch.

Note: As you follow the steps below, refer to the [flowcharts and samples](#) at the end of this section.

Generate Password Files

Note: If you use Windows Integrated Security, you do not need to generate password files.

To generate password files:

1. Open the Windows Powershell Console as an administrator.
2. Make sure your working directory is **C:\Program Files\Deltek\Vantagepoint\Scripts**.

Note: If your database and report servers are located on machines other than your web server and you are using local user accounts to access them, copy the CreatePwdFiles.ps1 script to those machines and generate the password files there. Then copy the password files to C:\Program Files\Deltek\Vantagepoint\Scripts>.

3. Run the CreatePwdFiles.ps1 script:

```
C:\Program Files\Deltek\Vantagepoint\Scripts> .\CreatePwdFiles.ps1
```

The script prompts you to enter and confirm password credentials.

4. Enter and confirm these passwords:
 - DSM User Download

- App Pool User
- **SQL Server “sa” System Administrator:** If you are not using **sa** as the SQL Server database system administrator user, enter **x** for this password.
- **SQL Server Service Domain Account:** This password is only needed for the DownloadDatabases and Restore switches.

The script uses these passwords to create the following .txt password files:

- sdownload.txt
 - appPool.txt
 - dbMSSsa.txt
 - sqlSvcDomainAcct.txt
5. Verify that the four generated password files are in the folder C:\Program Files\Deltek\Vantagepoint\Scripts.

Optional: Edit the Create Passwords Script

In some circumstances, you may need to generate additional password files – for example, if you use multiple domain accounts to access the database and report servers. In this case, you can edit the CreatePwdFiles.ps1 script.

To edit the CreatePwdFiles.ps1 script:

1. Copy the CreatePwdFiles.ps1 file to a temporary folder (for example, C:\Tmp).
2. Remove the read-only attribute of the file.
3. Open the file using a text editor such as Notepad or PowerShell ISE.
4. Add code to the file to generate the additional passwords that you need. For example, follow these steps if you need to generate a password for Domain Account 1:

Example:

- a. Search in the file for the string **\$sqlSvcDomainAcctFile**.
- b. Add the following code for your new password file after the line that you located:
\$domainAcctFile1 = -join(\$global:currentPath, "DomainAcct1.txt")
- c. Search in the file for the string **Generate-PasswordFile -sPrompt "Sql Service Domain Account Password"**
- d. Add the following code for your new password file after the line that you located:
Generate-PasswordFile -sPrompt "Domain Account1 Password" -sFilename \$domainAcctFile1

```
#region MAIN

Clear-Host
$global:currentPath = (Resolve-Path .\).Path + "\"
$downloadFile = -join($global:currentPath, "sdownload.txt" )
$appPoolFile = -join($global:currentPath, "appPool.txt" )
$dbSysAdminFile = -join($global:currentPath, "dbMSSsa.txt")
$sqlSvcDomainAcctFile = -join($global:currentPath, "sqlSvcDomainAcct.txt")
$domainAcctFile1 = -join($global:currentPath, "DomainAcct1.txt")

Generate-PasswordFile -sPrompt "DSM User Download Password" -sFilename $downloadFile
Generate-PasswordFile -sPrompt "App Pool User Password" -sFilename $appPoolFile
Generate-PasswordFile -sPrompt "MSS DB SysAdmin(sa) Password" -sFilename $dbSysAdminFile
Generate-PasswordFile -sPrompt "Sql Service Domain Account Password" -sFilename $sqlSvcDomainAcctFile
Generate-PasswordFile -sPrompt "Domain Account1 Password" -sFilename $domainAcctFile1

#endregion
```

5. Save your changes.
6. Open the Windows Powershell Console as an administrator.
7. Run the CreatePwdFiles.ps1 script.

The script should now include a prompt corresponding to the code that you entered.

```
Enter DSM User Download Password: *****
Confirm DSM User Download Password: *****
DSM User Download Password File generated: C:\Tmp\sdownload.txt
Enter App Pool User Password: *****
Confirm App Pool User Password: *****
App Pool User Password File generated: C:\Tmp\appPool.txt
Enter MSS DB SysAdmin(sa) Password: *****
Confirm MSS DB SysAdmin(sa) Password: *****
MSS DB SysAdmin(sa) Password File generated: C:\Tmp\dbMSSsa.txt
Enter Sql Service Domain Account Password: *****
Confirm Sql Service Domain Account Password: *****
Sql Service Domain Account Password File generated: C:\Tmp\sqlSvcDomainAcct.txt
Enter Domain Account1 Password: *****
Confirm Domain Account1 Password: *****
Domain Account1 Password File generated: C:\Tmp\DomainAcct1.txt
PS C:\Tmp> _
```

8. Copy the generated password file to C:\Program Files\Deltek\Vantagepoint\Scripts.

Generate the Response File

You can create the response file in two ways:

- **Create the file manually:** Find the DVPSilentInstall.xml file in C:\Program Files\Deltek\Vantagepoint\Scripts and use it as a guide to create the response file.
- **Use the ResponseGenerator.ps1 script to generate the file:** Follow the steps below.

Switches.json and Parameters.json Files

The ResponseGenerator.ps1 script uses two input files:

- **Switches.json:** This file contains the definition of the Vantagepoint installer switches and the parameters they need to run. Each parameter corresponds to a prompt that you would see if you were running the installer in interactive mode.

For example, the parameter **downloadUser** corresponds to the prompt **Enter your Deltek support username**.

- **Parameters.json:** This file contains a global list of all of the parameters used with all of the installer switches.

Both files are located in C:\Program Files\Deltek\Vantagepoint\Scripts.

You will never need to edit these files.

Refer to the [Flowcharts and Samples](#) section to see examples of these files.

Use the ResponseGenerator.ps1 Script

To generate the response file:

1. Open the Windows Powershell Console as an administrator.
2. Make sure your working directory is C:\Program Files\Deltek\Vantagepoint\Scripts.
3. Run the ResponseGenerator.ps1 script:

C:\Program Files\Deltek\Vantagepoint\Scripts> .\ ResponseGenerator.ps1

The script displays a form with a **Switches** drop-down list.

4. Follow these steps for each installation steps that you want the silent installation to perform:
 - a. Select the switch for which you want to generate a response file.

The script displays additional fields where you can enter prompts and parameters. For example, this is the screen you see if you select the **-CheckPreReq** switch:

- b. Enter the appropriate field values.

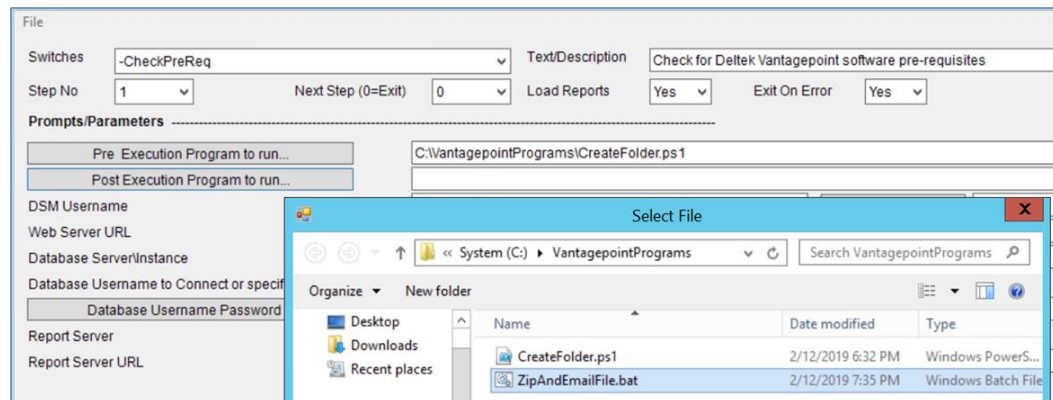
For the following fields, click the related command button to open Windows Explorer and browse to the file that you want to use:

Set Up Silent Installation

- Pre Execution Program to run:** Browse to the folder that contains the program or script that you want to run before you run the switch. In the following example, **CreateFolder.ps1** is selected for pre execution:

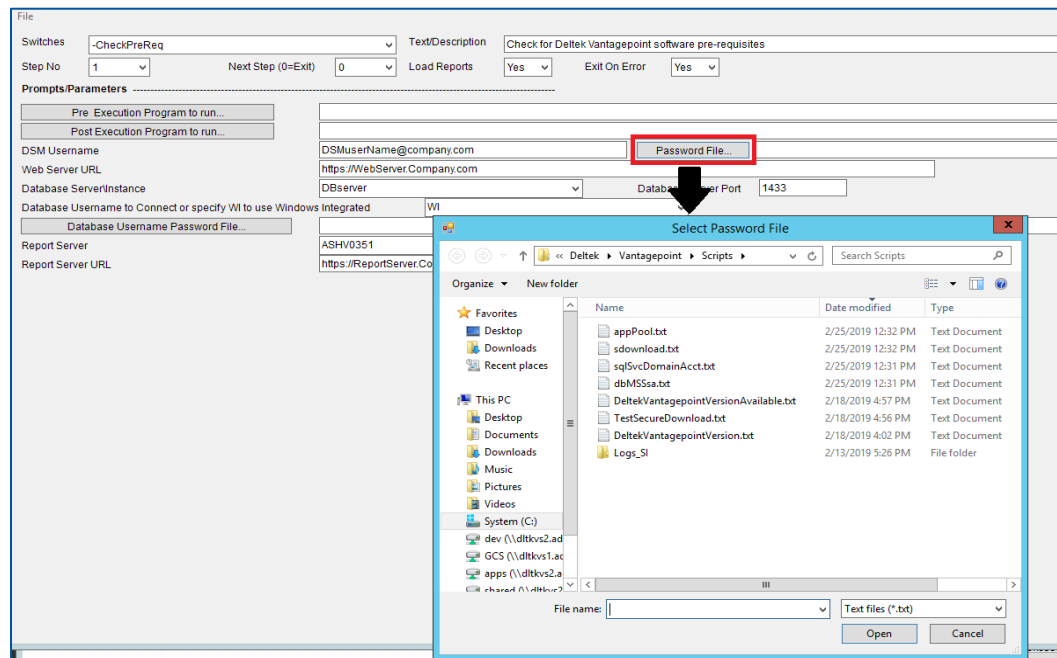
```
<Steps>
<Step no="1" nextStep="0" operation="-CheckPreReq" desc="Check for Deltek
Vantagepoint software pre-requisites" loadReports="N" exitOnError="Y">
  <preCmd TakeScrShotBefore="N" ExitBefore="N">powershell.exe | -ExecutionPolicy
  Bypass -File C:\VantagepointPrograms\CreateFolder.ps1 "C:\DEMO"</preCmd>
  <postCmd TakeScrShotBefore="N" ExitBefore="N"></postCmd>
  <downloadUser TakeScrShotBefore="N" ExitBefore="N">DSMuser@company.com
  </downloadUser>
  <downloadPwdFile TakeScrShotBefore="N" ExitBefore="N">C:\Program
  Files\Deltek\Vantagepoint\Scripts\download.txt</downloadPwdFile>
  <webServerUrl TakeScrShotBefore="N" ExitBefore="N" type="array">
    <value>localhost</value>
    <value>http://WebServer.company.com</value>
    <value>https:// WebServer.company.com</value>
  </webServerUrl>
  <dbServer TakeScrShotBefore="Y" ExitBefore="N">DBserver</dbServer>
  <dbServerPort TakeScrShotBefore="N" ExitBefore="N">1433</dbServerPort>
  <dbSysAdminUser TakeScrShotBefore="N" ExitBefore="N">sa</dbSysAdminUser>
  <dbSysAdminPwdFile TakeScrShotBefore="N" ExitBefore="N">C:\Program
  Files\Deltek\Vantagepoint\Scripts\dbMSSsa.txt</dbSysAdminPwdFile>
  <rptServer TakeScrShotBefore="N" ExitBefore="N">ReportServer</rptServer>
  <rptServerUrl TakeScrShotBefore="N" ExitBefore="N">
    https://ReportServer.company.com/ReportServer</rptServerUrl>
  </Step>
</Steps>
```

- Post Execution Program to run:** Browse to the folder that contains the program or script that you want to run after you run the switch. You can use any folder outside of the Installation script folder (C:\Program Files\Deltek\Vantagepoint\Scripts) as the location for your **CreateFolder.ps1** and **ZipAndEmail.bat** files. In this example, both files are located under the VantagepointPrograms folder.



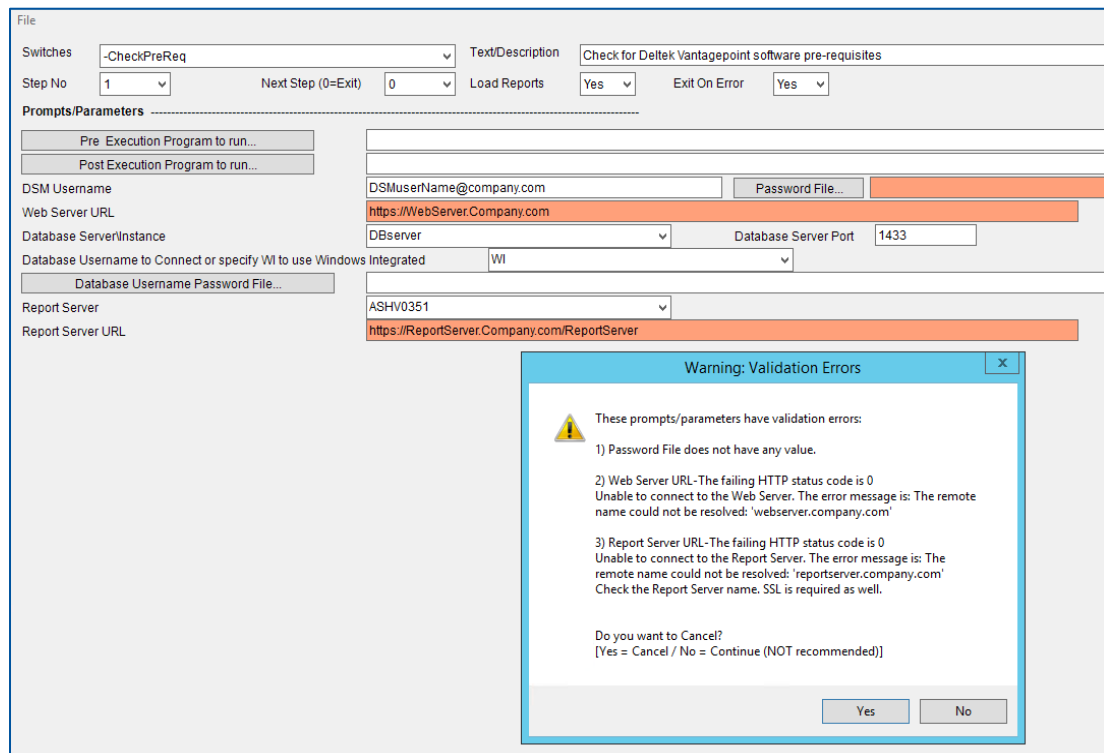
- Password File:** Browse to the password files that you generated earlier and select the appropriate file. By default, these files are in the <installation directory>\Scripts folder.

Set Up Silent Installation



- c. Save your changes.

The script validates your settings, looking for missing or incorrect values, and provides warnings if needed.



- d. Correct any settings that have warnings.
5. Repeat Step 4 for additional silent installation steps.

6. If you want to run the installer to test the current settings, click **File > Run** and then confirm that you want to run the installer.

The script saves the settings to a temporary file in C:\Program Files\Deltek\Vantagepoint\Scripts. The temp filename is in the format _switch.parm (for example, _CheckPreReq.parm).

7. Save the response file under an appropriate name (for example, DevWebServerSetup.xml) in C:\Program Files\Deltek\Vantagepoint\Scripts.

If a file already exists with that name, you can append new parameters to the file or overwrite the file.

ResponseGenerator.ps1 log files are located in the folder C:\Program Files\Deltek\Vantagepoint\Scripts\Logs_Sl.

Run DeltekVantagepoint.ps1 with the SilentInstall Switch

To run the DeltekVantagepoint.ps1 PowerShell script with the SilentInstall switch:

1. Open the Windows Powershell Console as an administrator.
2. Make sure your working directory is C:\Program Files\Deltek\Vantagepoint\Scripts.
3. Verify that your password files are stored in C:\Program Files\Deltek\Vantagepoint\Scripts.
4. Run the DeltekVantagepoint.ps1 PowerShell script with the SilentInstall switch:

```
C:\Program Files\Deltek\Vantagepoint\Scripts> .\DeltekVantagepoint.ps1 -SilentInstall
.\CheckPreReq.xml
```

The installer should run without asking for any prompts.

When the installer runs, it creates a log file, which is stored in C:\Program Files\Deltek\Vantagepoint\Logs.

Take Screenshots

- The script automatically takes a screenshot before and after executing the SilentInstall switch. These screenshots are stored in the folder C:\Program Files\Deltek\Vantagepoint\Logs\<date_time_stamp>, with the switch/operation name (for example, CheckPreReq) as a prefix.

Example filenames are:

Begin_CheckPreReq_20190225_165619_1727.png

End_CheckPreReq_20190225_165619_1727.png

- You can choose to take additional screenshots by adding commands to your response file. These screenshots will be stored in the same way as the “begin” and “end” screenshots.

You can take a screenshot for any parameter in the response file. Enter the **TakeScrShotBefore="Y"** command after the parameter.

For example, enter this command for the dbserver parameter:

<dbServer TakeScrShotBefore="Y"

Test the Silent Installation

While you are developing the response file, you may want to test part of the silent installation process without running all of the switches and parameters. For example, you might want to run downloadUser,

Set Up Silent Installation

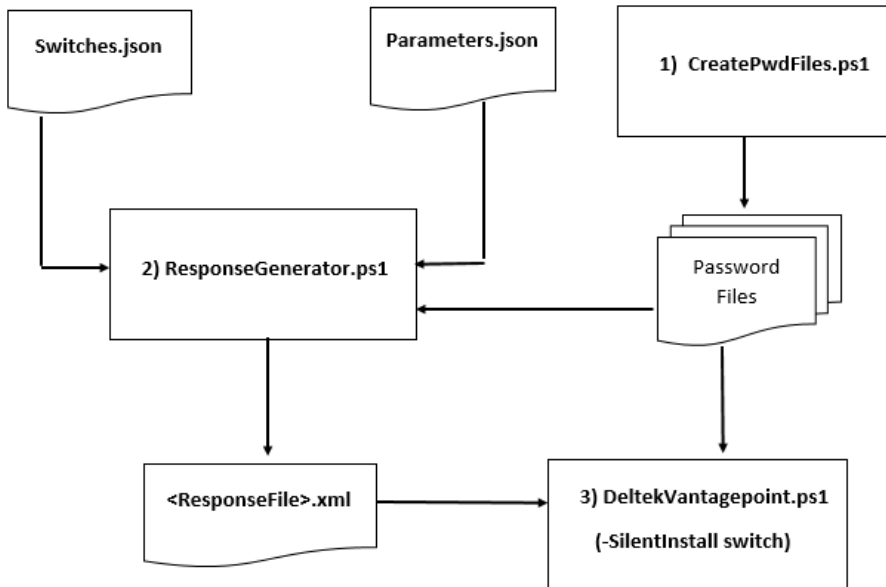
downloadPwdFile, understandInstallDoc, and licenseAgreement to make sure that those parts work, then stop at that point.

To stop the installer, insert the **ExitBefore=Y** command into the response file at the point where you want the process to stop. For example, to stop the process after the licenseAgreement parameter, include **ExitBefore=Y** for the next parameter, which is webServerUrl:

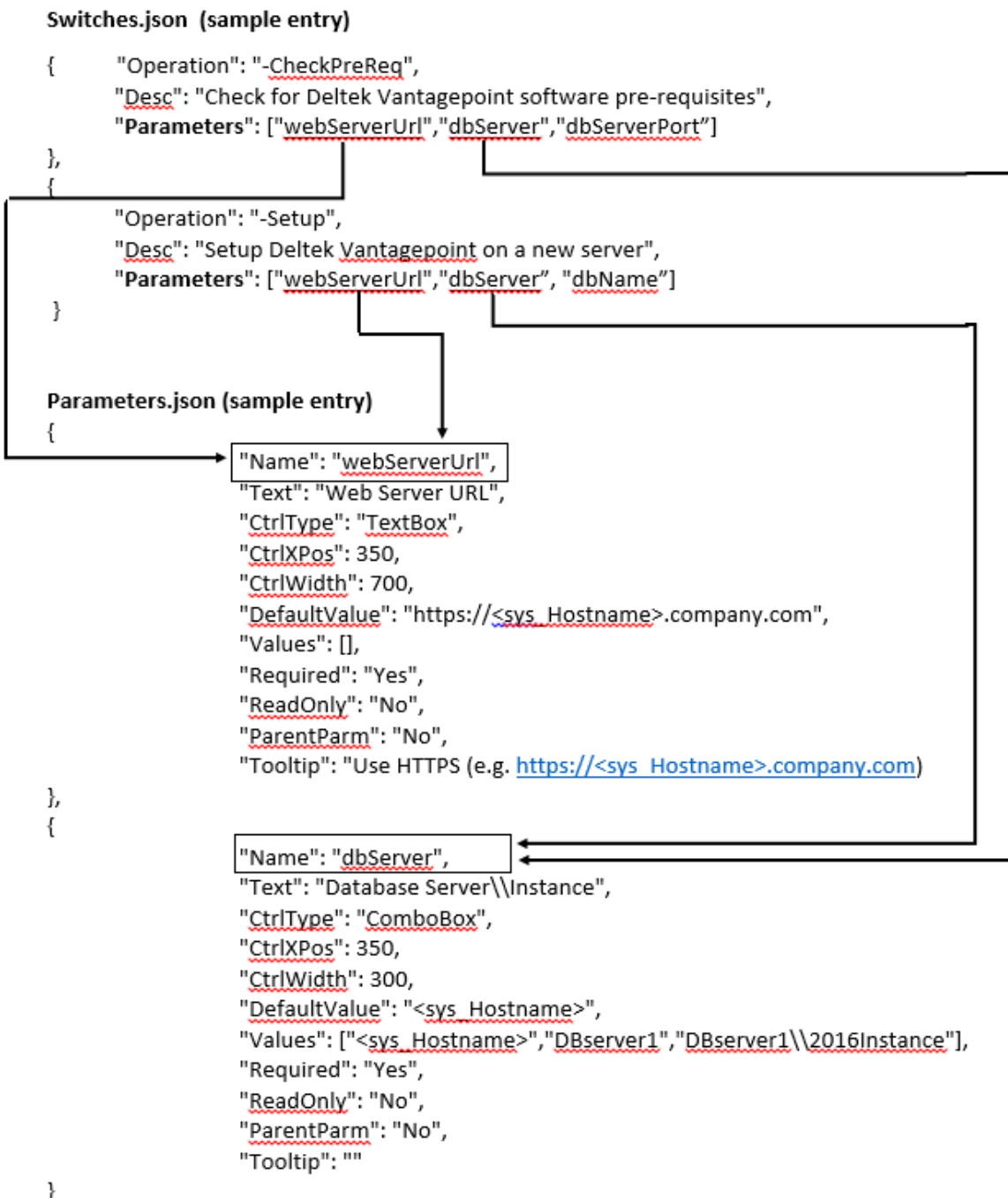
```
<?xml version="1.0" encoding="utf8"?>
<Steps>
    <Step no="1" nextStep="0" operation="-CheckPreReq" desc="Check for Deltek
Vantagepoint software "
                                loadReports="N" exitOnError="Y">
        <preCmd TakeScrShotBefore="N" ExitBefore="N"></preCmd>
        <postCmd TakeScrShotBefore="N" ExitBefore="N"></postCmd>
        <downloadUser TakeScrShotBefore="N"
ExitBefore="N">DSMuserName@company.com</downloadUser>
        <downloadPwdFile TakeScrShotBefore="N" ExitBefore="N">
                                C:\Program
Files\Deltek\Vantagepoint\Scripts\sdownload.txt</downloadPwdFile>
        <webServerUrl TakeScrShotBefore="N" ExitBefore="Y" type="array">
                                <value>https://WebServer.company..com</value>
        </webServerUrl>
        <dbServer TakeScrShotBefore="Y" ExitBefore="N"></dbServer>
        <dbServerPort TakeScrShotBefore="N" ExitBefore="N"></dbServerPort>
        <dbSysAdminUser TakeScrShotBefore="N" ExitBefore="N"></dbSysAdminUser>
        <dbSysAdminPwdFile TakeScrShotBefore="N"
ExitBefore="N"></dbSysAdminPwdFile>
        <rptServer TakeScrShotBefore="N" ExitBefore="N"> </rptServer>
        <rptServerUrl TakeScrShotBefore="N" ExitBefore="N"></rptServerUrl>
    </Step>
</Steps>
```

Flowcharts and Samples

Relationship of Files Used with the SilentInstall Switch



Relationship of Switches.json and Parameters.json Values



Sample Response File (for CheckPreReq.xml)

```
<?xml version="1.0" encoding="utf8"?>
<Steps>
```

Set Up Silent Installation

```
<Step no="1" nextStep="0" operation="-CheckPreReq" desc="Check for Deltek
Vantagepoint software pre-requisites" loadReports="N" exitOnError="Y">

  <preCmd TakeScrShotBefore="N" ExitBefore="N">powershell.exe | -
ExecutionPolicy Bypass -File .\CreateFolder.ps1 "C:\DEMO"</preCmd>

  <postCmd TakeScrShotBefore="N" ExitBefore="N"></postCmd>

  <downloadUser TakeScrShotBefore="N"
ExitBefore="N">DSMuserName@company.com</downloadUser>

  <downloadPwdFile TakeScrShotBefore="N" ExitBefore="N">C:\Program
Files\Deltek\Vantagepoint\Scripts\sdownload.txt</downloadPwdFile>

  <webServerUrl TakeScrShotBefore="N" ExitBefore="N" type="array">

    <value>localhost</value>

    <value>http://WebServer.company.com</value>

    <value>https:// WebServer.company..com</value>

  </webServerUrl>

  <dbServer TakeScrShotBefore="Y" ExitBefore="N">DBserver</dbServer>

  <dbServerPort TakeScrShotBefore="N" ExitBefore="N">1433</dbServerPort>

  <dbSysAdminUser TakeScrShotBefore="N" ExitBefore="N">sa</dbSysAdminUser>

  <dbSysAdminPwdFile TakeScrShotBefore="N" ExitBefore="N">C:\Program
Files\Deltek\Vantagepoint\Scripts\dbMSSsa.txt</dbSysAdminPwdFile>

  <rptServer TakeScrShotBefore="N" ExitBefore="N">ReportServer</rptServer>

  <rptServerUrl TakeScrShotBefore="N"
ExitBefore="N">https://ReportServer.company.com/ReportServer</rptServerUrl>

</Step>
</Steps>
```

Sample Elements/Prompts

In this section, review step elements, parameters for attributes, and parameters for elements/switches.

Steps

Here is an example of a step, followed by a walk-through of its elements:

```
(<Step no="1" nextStep="2" operation="-CheckPreReq" desc="Checking Pre-Requisites"
loadReports="N"> exitOnError="Y")
```

Step Element	Example	Description
no (String)	no="1"	Specify a step number from 1 to <nn>.
nextStep (String)	nextStep="2"	Specify the next step number from 1 to <nn>. Enter 0 (zero) to have the script exit. When you enter multiple steps in a response file, make sure that the last nextStep value is 0. If you do not, the script will run in an infinite loop.

Step Element	Example	Description
operation (String)	operation="-CheckPreReq"	Specify an operations correspond to Vantagepoint switches.
desc (String)	desc="Checking Pre-Requisites"	Enter a description of the operation.
loadReports (String)	loadReports="N"	Specify Y or N to tell SilentInstall whether or not the LoadReports operation will be performed on -Setup, -SetupAndMigrate, and other switches that call this feature.
exitOnError	exitOnError="Y"	Specify Y or N to tell SilentInstall whether or not to exit if it encounters an error while performing the switch/operation; for example, if a runtime error occurs.

Parameters: Attributes

In this section, we'll look at parameter attributes and walk through their elements:

```
(<preCmd TakeScrShotBefore="Y"
ExitBefore="N">.\StartSystem.bat|global:LogFilePath</preCmd>)
```

Attribute	Example	Description
TakeScreShotBefore (String)	TakeScreShotBefore="Y"	Specify Y or N to tell SilentInstall whether or not to take a screenshot before executing the prompt. Screenshot files are located under the C:\Program Files\Deltek\Vantagepoint\Logs\<runtime> folder.
ExitBefore	ExitBefore="N"	Specify Y or N to tell SilentInstall whether or not to exit the program before executing the prompt.

Parameters: Elements/Switches

This section discusses parameter elements/switches. Be sure to review the guidelines after the table.

Parameter	Example / Description
<preCmd>	<pre>(<preCmd TakeScrShotBefore="Y" ExitBefore="N">.\StartSystem.bat global:LogFilePath</preCmd>)</pre> <p>The parameter executes any program/script defined before the first prompt, such as "Enter your Deltek support username."</p>
<postCmd>	<p>The parameter executes any program/ script defined after all prompts are executed and before the script ends. This is a good place to execute error checking and to send log files.</p>

Parameter	Example / Description
<downloadUser>	This is the DSM/Deltek support password, in this format: userName@company.com
<downloadPwdFile>	This is the DSM/Deltek Support password file that is generated in Step 1 of the installation.
<webServerUrl type="array">	This element can contain an array of values. The last element should be the correct value, as in the bolded line in the following example: <pre><webServerUrl TakeScrShotBefore="N" ExitBefore="N" type="array"> <value>localhost</value> <value>http://WebServer.ads.company.com</value> <value>https://WebServer.ads.company.com</value> </webServerUrl></pre>
<understandInstallDoc>	Specify Y or N to indicate whether or not you understand the installation documentation.
<licenseAgreement>	Specify Y or N to indicate acceptance of the user license agreement.
Confirmation password files	<p>Create a confirmation password file, with values corresponding to the values in the primary password file.</p> <ol style="list-style-type: none"> confirmInitialWeblinkPwdFile = setInitialWeblinkPwdFile dbCreateUserConfPwdFile = dbCreateUserPwdFile rptDbCreateUserConfPwdFile = rptDbCreateUserPwdFile changeWeblinkConfirmNewPwdFile = changeWeblinkNewPwdFile <p>Example entry in a response file:</p> <pre><dbCreateUserPwdFile TakeScrShotBefore="N" ExitBefore="N"> C:\Program Files\Deltek\Vantagepoint\Scripts\appPool.txt </dbCreateUserPwdFile> <dbCreateUserConfPwdFile TakeScrShotBefore="N" ExitBefore="N"> C:\ProgramFiles\Deltek\Vantagepoint\Scripts\appPool.txt </dbCreateUserConfPwdFile></pre>

Guidelines:

- If your pre/post command to execute is a Powershell script (*.ps1), it should be located outside of the scripts folder: C:\Program Files\Deltek\Vantagepoint\Scripts. This is necessary because the installer validates *.ps1 and *.psm1 files to ensure that they were digitally signed by Deltek.
- Use the pipe symbol | to separate arguments for programs called in the <preCmd> and <postCmd> parameters. Example:

```
<postCmd TakeScrShotBefore="N"
ExitBefore="N">.\ZipAndEmailFile.bat|global:DeltekVPLogsDir|userName@abc.com</p
ostCmd>
```

In this example, the program ZipAndEmail.bat has two arguments in global: DeltekVPLogsDir and userName@abc.com

- You can use two system constants as arguments in <preCmd> and <postCmd> parameters:
 - **global:DeltekVPLogsDir** – Use this constant to specify the name of the logs folder for a particular switch/operation. Example:

```
C:\Program Files\Deltek\Vantagepoint\Logs\20190225_165558
```

- **global:LogFilePath** – Use this constant to specify the name of the log file for a particular switch/operation. Example:

```
C:\Program Files\Deltek\Vantagepoint\Logs\20190225_165558\
Vantagepoint_20190225_1655.txt
```

Sample Excerpt from the Switches.json File

The Switches.json file contains the definitions of the Vantagepoint installer switches and the parameters required to run the switches. Each parameter corresponds to a prompt that you would see if you were running the installer in interactive mode.

Here is an excerpt from the Switches.json file, describing the CheckPreReq switch.

```
{
  "switches": [
    {
      "Operation": "-CheckPreReq",
      "Desc": "Check for Deltek Vantagepoint software pre-requisites",
      "Parameters": [
        "webServerUrl", "dbServer", "dbServerPort", "dbSysAdminUser", "dbSysAdminPwdFile", "rptServer", "rptServerUrl"
      ]
    }
  ]
}
```

For each switch, the file includes:

Section	Purpose
Operation	This is the name of the switch.
Description	This is a description of the purpose of the switch.
Parameters	These are the parameters that you can use with the switch, which are defined in the Parameters.json file.

Sample Excerpt from the Parameters.json File

This Parameters.json file contains a global list of all of the parameters used with all of the installer switches.

Here is an excerpt from the Parameters.json file, describing the downloadUser parameter:

```
{
  "Name": "downloadUser",
```

```

        "Text": "DSM Username",
        "CtrlType": "TextBox",
        "CtrlXPos": 350,
        "CtrlWidth": 350,
        "DefaultValue": "<sys_UserName>@company.com",
        "Values": [],
        "Required": "Yes",
        "ReadOnly": "No",
        "ParentParm": "",
        "Tooltip": "Usually an email address. (e.g.
emailAddr@company.com)"
    }

```

For each parameter, the file includes:

Section	Purpose
Name	This is the name of the parameter.
Text	This is the label that displays on the form that you use to create the response file .
CtrlType	This is the type of control that displays on the form. Possible values are: <ul style="list-style-type: none"> ▪ FileDialogExe: Used for PreCmd and PostCmd parameters. ▪ TextBox: Used for most commands. ▪ FileDialogPwd: Used for parameters that need a password file to connect. ▪ ComboBox: Used for editable drop-down lists. ▪ Dropdownlist: Used for non-editable drop-down lists.
CtrlXPos	This is the position, in pixels, on the horizontal (x) axis, where the control appears on the form. Back up the Parameters.json file before changing this value.
CtrlWidth	This is the width, in pixels, of the control on the form. Back up the Parameters.json file before changing this value.
DefaultValue	This is the value of the parameter when it is first displayed on the form. It can be a system constant .
Values	These are valid values for the parameter. They can be system constants .
Required	This value is Yes or No , depending on whether the parameter is required for a specific switch.
ReadOnly	This value is Yes or No , depending on whether the parameter is read-only or can be changed.

Section	Purpose
ParentParm	This is the parent parameter of this parameter. The value of the parent parameter may determine how the child parameter works. For example, if the parent parameter rptDbSysAdminUser has a value of WI, for Windows Integrated Security, the child parameter rptDbSysAdminPwdFile does not need to prompt for a password.
Tooltip	This is the text that displays when you hover the cursor over the parameter on the form.

System Constants

When you create a response file, you can use system constants instead of actual values for parameters. For example, you can use the constant <sys_Username> instead of the actual username (for example, JoanDoe). When the script runs, it will translate <sys_Username> to be the username of the person who is currently logged in.

Here are the system constants that you can use:

Constant	Represents:	Example
<sys_DnsDomainName>	DNS domain name Corresponds to the PowerShell \$env:UserDnsDomain variable.	ads.company.com
<sys_DomainName>	Domain name Corresponds to the PowerShell \$env:UserDomain variable.	adscompanycom
<sys_Hostname>	Name of current server Corresponds to the PowerShell \$env:ComputerName variable.	DBServer1
<sys_UserName>	Name of the current logged-in user Corresponds to the PowerShell \$env:UserName variable.	JoanDoe
<sys_DomainAndUserName>	Domain name\user name	adscompanycom\JoanDoe

Advanced Administrator Topics

Microsoft Internet Information Server (IIS)

Installation on Windows Server

A prerequisite for installing Vantagepoint 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.

Run the setup script with the [EnableIISRequiredFeatures switch](#) if the IIS prerequisite check indicates that you have not enabled all required IIS modules. This switch uses the Enable-WindowsOptionalFeature Powershell cmdlet to enable required IIS modules that are currently disabled.

Required IIS Features

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

Area	Feature
Common HTTP Features	<ul style="list-style-type: none"> ▪ Default Document ▪ Directory Browsing ▪ HTTP Errors ▪ Static Content ▪ HTTP Redirection
Health and Diagnostics	<ul style="list-style-type: none"> ▪ HTTP Logging ▪ Request Monitor (recommended) ▪ Tracing (recommended)
Performance	<ul style="list-style-type: none"> ▪ Static Content Compression
Security	<ul style="list-style-type: none"> ▪ Windows Authentication (only necessary if you will be using it) ▪ Request Filtering
Application Development	<ul style="list-style-type: none"> ▪ .NET Extensibility 4.5 ▪ ASP.NET 4.5 (Add Roles and Features Wizard dialog box displays when you select this option. Click Add Features button.) ▪ CGI (Required if you will be using Deltek mobile products) ▪ ISAPI Extensions ▪ ISAPI Filters
Management Tools	<ul style="list-style-type: none"> ▪ IIS Management Console ▪ IIS Management Scripts and Tools

Microsoft SQL Server Edition and Version Information

Use the link below to access the Deltek Platform Compatibility Matrix to learn about currently supported SQL Server service packs and cumulative updates.

https://deltek.custhelp.com/app/answers/detail/a_id/38499

Microsoft SQL Server 2019 Express Edition with Advanced Services

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

<https://go.microsoft.com/fwlink/?linkid=866658>

- 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>

Microsoft SQL Server Reporting Tools

- Microsoft SQL Server Report Builder for Microsoft SQL Server 2014. You can use the Report Builder standalone version or the ClickOnce version of Report Builder installed with Reporting Services:
- Microsoft SQL Server Data Tools - Business Intelligence for Visual Studio. Installs Microsoft SQL Server Data Tools Business Intelligence project templates for Analysis Services, Integration Services, and Reporting Services that support Visual Studio and SQL Server:

<https://www.microsoft.com/en-us/download/details.aspx?id=42301>

<https://www.microsoft.com/en-us/download/details.aspx?id=42313>

Microsoft SQL Server Reporting Services

Vantagepoint uses Microsoft SQL Server Reporting Services as its report management and delivery platform. There are several things to consider when you migrate to Vantagepoint:

- SQL Server Reporting Services is not installed as part of the Vantagepoint installation. SQL Server Reporting Services must be installed and configured before Vantagepoint installation so that Vantagepoint can connect to the report server.
- The Vantagepoint reporting RDL (report definition language) schema supports the latest versions of SQL RS 2012 and 2014. Vantagepoint does not support SQL Server RS 2008 and 2005 Business Intelligence Development Studio (BIDS).

Overview of SQL Server Reporting Services

Microsoft SQL Server Reporting Services is a server-based reporting platform that you can use to create and manage reports that contain data from relational and multidimensional data sources. The reports that you create can be viewed and managed over an Internet connection. Reporting Services includes the following core components:

- A complete set of tools that you can use to create, manage, and view reports.
- A Report Server component that hosts and processes reports in a variety of formats. Output formats include HTML, PDF, TIFF, Excel, CSV, and more.
- An API that allows developers to integrate or extend data and report processing in custom applications, or create custom tools to build and manage reports.

The reports that you build can be based on relational or multidimensional data from SQL Server, Analysis Services, Oracle, or any Microsoft .NET data provider such as ODBC or OLE DB. You can create tabular, matrix, and free-form reports. You can also create ad hoc reports that use predefined models and data sources.

Reporting Services uses URLs to access the Report Server web service and Report Manager. Before you can use either application, you must configure at least one URL each for the web service and Report Manager. Reporting Services provides default values for both application URLs that work well in most deployment scenarios, including side-by-side deployments with other web services and applications.

Reporting Services uses a SQL Server database for internal storage. The database is a required component used to store reports, session data, resources, and server metadata.

The benefits of Reporting Services include:

- **Ease of Deployment and Management:** SSRS is embedded in the SQL Server that database clients already use. This streamlines deployment and updates, and provides a platform for delivery of new functionality for years to come.
- **Industry Leading Platform:** SSRS is fast becoming one of the leading Business Intelligence (BI) platforms on the market.
- **Better Technology Alignment with Vantagepoint:** SSRS aligns with the Microsoft-centric technology strategy for Vantagepoint.

Note: Scale-out configuration of SSRS is supported and provides a load balanced configuration for scalability. This configuration requires the Enterprise Edition of SQL Server.

More Information about Reporting Services

The best way to learn about Reporting Services is through the documentation included with your SQL Server (Books Online, Microsoft Labs, and so on).

These articles describe how to configure the latest versions of Reporting Services:

- [Getting Started \(SQL Server 2012\)](#)
- [Configuring Reporting Services](#)

These articles provide additional information about Reporting Services:

- [What is SQL Server Reporting Services \(SSRS\)?](#)
- [SQL Server Documentation](#)

Report Server Licensing Requirements

The method that you use to deploy your Report Server depends on the edition and licenses you own for your Microsoft SQL Server database. If you plan to host your Reporting Services web service on a machine separate from the Reporting Services report server database, you must determine whether your SQL Server edition and licenses can support this deployment.

The following Microsoft page describes the licensing options available with SQL Server and Reporting Services:

https://www.microsoft.com/en-US/sql-server/sql-server-2017?&OCID=AID631226_SEM_9gSDPzSr

Features Supported by Different SQL Server Editions

This table shows the features that come with the commonly used editions of Microsoft SQL Server available on the market today and supported by Vantagepoint.

Feature	Express with Advanced Services	Standard	Enterprise
Custom Reporting			
Report Builder	✓	✓	✓
Report Models for Report Builder	-	✓	✓
Report Designer (SSDT-BI)	✓	✓	✓
Standard Reporting			
Access to All Standard Reports		✓	✓
Report History (Previously Run)	-	✓	✓
Email Reports	-	✓	✓
Email Report Links	-	✓	✓

Feature	Express with Advanced Services	Standard	Enterprise
Schedule Reports	-	✓	✓
Schedule and Report History	-	✓	✓
Search and Download in Preview	-	✓	✓

You can also refer to the [Edition and supported feature of SQL Server 2016](#) article. Click the corresponding links in the article for the version that you use.

Custom Reports and Custom Invoices

Supported Report Writing Tools

Vantagepoint supports the following Microsoft SQL Server Reporting Services report-writing tools for creating custom reports and custom invoices:

- Report Builder 3.0
- SQL Server Data Tools - Business Intelligence Report Writer for Visual Studio 2013 (referred to as SSDT-BI 2013 Report Designer)

These report-writing tools produce a report file with the RDL 2010 schema that Vantagepoint requires.

Note: For help downloading and installing the supported report-writing tools and creating custom reports, see the [Deltek Vantagepoint Custom Reports and Microsoft SQL Server Reporting Services Guide](#).

Upgrade Custom Reports and Custom Invoices

If you are upgrading from an earlier Vantagepoint version, see the [Deltek Vantagepoint Custom Reports and Microsoft SQL Server Reporting Services Guide](#) for upgrade instructions.

Summary of Upgrading Custom Reports and Invoices

Vantagepoint Version Upgrading From...	Upgrade Action Required	Vantagepoint Custom Reports and Microsoft SQL Server Reporting Services Guide
An earlier 7.x version (your custom reports and/or custom invoices have an RDL 2005 or RDL 2008 schema)	Upgrade your reports to the RDL 2010 schema.	See Appendix A: Custom Reports and Migrating from Vision to Vantagepoint On-Premise.

Vantagepoint Version Upgrading From...	Upgrade Action Required	Vantagepoint Custom Reports and Microsoft SQL Server Reporting Services Guide
A 6.x version (Your custom reports and/or custom invoices have an RDL 2005 schema.)	Complete both of the following: <ul style="list-style-type: none"> Upgrade your reports to the RDL 2010 schema. Perform additional steps for changes to some Vantagepoint database table names. 	See the following sections: <ul style="list-style-type: none"> Appendix A: Custom Reports and Migrating from Vision to Vantagepoint On-Premise "Vision 7.0 Database Table Name Changes that Affect Custom Reports" section in Appendix A: Custom Reports and Migrating from Vision to Vantagepoint On-Premise.

Extra Space in Invoice Header

If you are using Vantagepoint with SQL Server Reporting Services, your invoices will print with extra space in the header when the top margins are expanded. This is a known issue with SQL Server Reporting Services.

Deltek recommends that you carefully review your invoice templates, and wherever possible, reduce the top margins in the Vantagepoint Invoice Template Editor to prevent the extra space issue from occurring.

Configure Microsoft SQL Server Reporting Services

Important Information about Configuring Reporting Services

- For more information about configuring Report Services, see [Important Information about Configuring Report Services](#) and [Reporting Services Configuration Manager \(Native Mode\)](#).
- If you have configured the Report Server service account to be a domain account, Reporting Services will use Kerberos Authentication by default. You must ensure that you have created an SPN for the account. To configure an SPN, see the article [Register a Service Principal Name \(SPN\) for a Report Server](#).
- For more information about Kerberos authentication, see the article [Configure Windows Authentication on the Report Server](#).
- Alternatively, you can configure the **RSReportServer.config** file with the following XML structure, which specifies NTLM only. This configuration is for deployments that do not support Kerberos or to work around Kerberos authentication errors (HTTP 401 errors) :

```
<AuthenticationTypes>
  <RSWindowsNTLM/>
</AuthenticationTypes>
```

Initial Setup Steps

Use these steps to configure your initial SQL Server Reporting Services setup. These steps are required for Vantagepoint to verify that SQL Server Reporting Services exists. Vantagepoint will use the accounts specified on the Report Server tab of Weblink to make connections to Reporting Services.

Note: Do not configure an Execution Account as part of Report Server configuration. If you do, the Execution Account will be used instead of the credentials listed in Weblink. This may result in reporting errors in Vantagepoint.

To configure your initial setup:

1. Click **Start » All Programs » Microsoft SQL Server <Select Your Version> » Configuration Tools » Reporting Services Configuration Manager** to launch the Reporting Services Configuration Wizard.
2. On the Reporting Services Configuration Connection dialog box, select your SQL Reporting Services Instance Name, and then click **Connect**.

If you have multiple installations of Reporting Services, you may see more than one instance. MSSQLServer is the default instance.
3. On the Report Server Status pane of the Reporting Services Configuration Manager dialog box, click **Start** to start the Reporting Services instance. If it is already running, click **Service Account** in the left pane.
4. On the Service Account pane of the Reporting Services Configuration Manager dialog box, choose the appropriate account and click **Apply**. Microsoft recommends using the Network Service account.

For additional information on choosing a service account, see [Service Account - Reporting Services Native Mode \(Configuration Manager\)](#).

If you have configured the Report Server Service Account to be a domain account, Reporting Services will use Kerberos Authentication by default.
5. The Service Account pane of the Reporting Services Configuration Manager dialog box displays again, showing the results in the bottom pane. Click **Web Service URL** in the left pane.
6. On the Web Service URL pane, accept the default values.

The default value for **Virtual Directory** is **ReportServer**. If you installed Report Server as an instance, the virtual directory is usually **ReportServer** and the instance name, separated by a character, such as an underscore or dollar sign.
7. Take note of the Report Server web service URL shown in the Web Service URL dialog box, in case Vantagepoint is unable to connect to the Report Server during the installation and prompts you for the correct path.
8. Click **Apply** to accept your settings. If the settings are correct, the Results pane displays the status.
9. Click **Database** in the left pane.

Vantagepoint uses the Report Server web service URL at the bottom of the dialog box as part of its test connection URL when it tries to connect to the Report Server.

SQL Server Reporting Services does not require IIS to be enabled.
10. In the Report Server Database pane, click **Change Database**.

11. On the Change Database screen, choose whether to create a new Report Server database or use an existing one. For a new installation, select **Create a new report server database**. Click **Next**.
12. Enter the database **Server Name** and a user account that has privileges to create or select the database and assign the required rights.
 - a. Click **Test Connection** to test your credentials. Make any needed corrections.
 - b. Click **OK** when you have connected successfully to the database. The Change Database screen displays.
 - c. Click **Next**.
13. Accept the default values. Click **Next**.

Note: Only **Native Mode** is supported. Select **Native Mode** if it is not selected by default.

14. In the Credentials pane of the Change Database screen, specify the type of credentials and accounts that Reporting Services will use to connect the database. Click **Next**.
15. Review the summary of the changes that you made. Click **Next**.
You can watch as the Report Server databases are created.
16. Click **Finish** when all steps are marked as successfully completed.
17. In the left pane of the Report Services Configuration Manager dialog box, click **Report Manager URL**.
18. In the Report Manager URL pane, accept the default values. Click **Apply**.
19. Click **Encryption Keys** in the left pane and back up the encryption keys to a safe location. Click **Apply**.
20. Click **Exit**. You are now ready to begin the Vantagepoint installation.

Connect to the Report Server Web Service

SQL Server Reporting Services provides access to the full functionality of the Report Server through the Report Server web service, **ReportingService2005.asmx**, an XML web service with a SOAP API.

The web service uses SOAP over HTTP and acts as a communication interface between client programs and the Report Server. It provides the interface for enumerating the reports and report folders and a host of other capabilities for report execution, rendering, and management.

The web service provides two endpoints: one for report execution and one for report management. The Vantagepoint setup script connects to the report execution endpoint.

Specify the Report Server Host Name and URL

When you run the setup script, the setup attempts to connect to the Reporting Service web service screen. If it cannot, it returns an error message and displays the Specify Report Server and Report Server URL Information screen.

Complete one of the following actions:

- Verify that the information on the screen is correct. Click Enter.
- If the information is incorrect, update the fields with the correct values:

- **Report Server:** The Report Server name is the host name (machine name) of your Report Server machine.
- **Report Server URL:** This is the URL used to connect to the Reporting Services web service on the Report Server. It should be in the format:

`https://<Report Server Fully Qualified Domain Name>/Virtual Directory/`

For example: <https://reportserver.company.com/reportserver>

The setup script automatically appends **reportservice2005.asmx** to the URL.

Elements in the Report Server URL

URL Element	Description
Fully Qualified Domain Name	The full DNS name of the server, which must match the assigned SSL certificate.
Virtual Directory	<p>This is the name of the folder that contains the XML web service for report execution. This folder is configured during setup or when you run the Microsoft SQL Server Reporting Services Configuration tool. The default name is reportserver.</p> <p>If you are unsure of the name, follow the steps in Identify Virtual Directory Name.</p> <p>If you installed Reporting Services as an instance, the name of the virtual directory may also include the instance name. For example, <code>reportserver_INSTANCENAME</code>.</p>
<endpointname>.asmx	<p>The setup script automatically appends reportservice2005.asmx to the URL.</p> <p>This is the name of the web service endpoint. The 2005 in the name does not refer to any version of SQL Server.</p>

Identify Virtual Directory Name

To identify the virtual directory name:

1. Click **Start » All Programs » Microsoft SQL Server <Select Your Version> » Configuration Tools » Reporting Services Configuration Manager**.
2. Connect to the Report Server Web Service URL in the left pane.
3. Check the **Virtual Directory** field in the right pane.

Note: Make sure that the entry in the **Virtual Directory** field matches the virtual directory listed on the Specify Report Server and Report Server URL screen.

If you have not configured SQL Reporting Services, click the Help icon in the lower left corner of the Reporting Services Configuration Manager dialog box to access Microsoft documentation for configuring Reporting Services.

SQL Report Server Database Prompt During Setup

If the Vantagepoint setup script is unable to connect to the ReportServer database server or to identify the Reporting Services databases, it will prompt you for the database server\Instance hosting the report server databases as well as the name of the Report Server database. You will be prompted to provide sysadmin credentials to authenticate to the database server and prompted for the SQL login credentials (SQL Server or Windows account) that will be granted db_owner rights to the ReportServer and ReportServerTempDB databases.

Enter the following information:

- **Report Database Server:** Enter the name of the database server that contains the Report Server databases. If the database server is using a specific instance name, enter the name in the format Server\Instance.
- Accept the **WI (Windows Integrated)** option if you use Windows integrated security. If you do not, enter the SQL login and password. If you do not use Windows integrated security, make sure that your server is configured to support Mixed Mode Security.
 - **SQL Login:** The default SYSADMIN account for SQL Server is **sa**.
 - **SQL Password:** Enter the password associated with this SQL Login.
- **ReportServer Database:** Enter the name of your ReportServer database. Typically, the default name for this database is **ReportServer**. If you have an instance, then the name is **ReportServer\$InstanceName**. If you are unsure of the name, follow the steps in [Identify ReportServer Database Names](#).
- **ReportServerTempDB Database:** Enter the name of your ReportServerTempDB database. Typically, the default name for this database is **ReportServerTempDB**. If you have an instance, then it is **ReportServer\$InstanceNameTempDB**. If you are unsure of the name, follow the steps in [Identify ReportServer Database Names](#).

Note: If the SQL Login does not have db_owner membership of the Report Server and ReportServerTempDB databases, setup grants these rights.

Identify ReportServer Database Names

To identify the ReportServer and ReportServer TempDB databases names, complete the following steps on your Report Server:

1. Click **Start » All Programs » Microsoft SQL Server <Select your Version> » Configuration Tools » Reporting Services Configuration Manager**.
2. On the Reporting Services Configuration Manager dialog box, click **Database** in the left pane, and then click **Change Database** in the right pane.
3. On the Change Database screen, select the **Choose an existing report server database** option. Click **Next**. The Change Database/Database Server screen displays.
4. If you are:
 - Logged in as an Administrator, accept the default values to make a connection using Integrated Authentication.
 - Not logged in as an Administrator, select **SQL Server Account** from the **Authentication Type** drop-down list. Enter the System Administrator (SA) credentials in the **Username** and **Password** fields.

5. Click **Next**.
6. Use the **Report Server Database** drop-down list to see the names of the **ReportServer** and **ReportServerTempDB** databases. Click **Cancel**.

Give Your Account Proper Rights and Privileges in Reporting Services Web Services

Two types of credentials are required for the Report Server installation to complete successfully:

- You must have a Windows account (local or domain) with proper rights and privileges to the Report Server web services component. This account must have Content Manager and System Administrator privileges in the Reporting Services Report Manager Tool. These privileges prevent 401 (unauthorized access) errors from occurring when the installation tests the connection to the Reporting Services web service and when you test and run reports.
- The Local Windows Administrator Group on the report server will appear to already have the Content Manager and System Administrator roles in Reporting Services. However, the Windows account must still be granted these rights explicitly so that the installation can connect to Reporting Services and assign the proper privileges to the local Vantagepoint Windows account that the installer creates.
- You must have a Report Server SQL Server database login that is a member of the db_owner role for the ReportServer and ReportSeverTempDB databases.

To configure/verify rights and privileges to the Report Server web services component:

1. Log on locally to the report server desktop console with a Windows account that is a member of the local administrator group.
2. Launch the Report Manager URL (<http://localhost/reports>):

You must be on the server and browse to the Report Manager URL using localhost as the server name (<http://localhost/reports>) to see the Report Manager configuration options.

If you do not see the configuration options, launch Internet Explorer using the **Run as administrator** option to run Internet Explorer with elevated privileges.
3. Click **Folder Settings** at the top of the SQL Server Reporting Services screen.
4. Click **New Role Assignment**.
5. In the Content Manager role, add the account that you will be logged into when you perform the Vantagepoint setup.

The account appears in the listing with the Content Manager rights.

During setup, this account is used to connect to the report server and install Vantagepoint reports into Reporting Services. (This is also the account listed in Weblink to run Vantagepoint reports).

If you do not enter a different account, the setup process creates an account named **DeltakVantagepoint** that is assigned Content Manager and System Administrator rights to load and run Vantagepoint reports on behalf of Vantagepoint users.
6. Click **Site Settings » Security » New Role Assignment**.
7. Enter your Windows account and select the **System Administrator** role.

Prerequisite Report Server and SQL Server Database Credentials

During Vantagepoint setup, when the script is testing for proper rights to the report server, a SQL Server account is required for connecting to the SQL Server database that hosts the report server databases used for managing the report server and Vantagepoint reports. This account must be configured on the SQL Server that hosts the report server. (Most installations have the SQL Server report server database on the same machine as the report server web server component.)

To avoid errors during the report server installation, or when testing Weblink entries or running reports, you must configure a report server SQL Server database login and give it membership to the db_owner role on the SQL Server that hosts the ReportServer and ReportServerTempDB databases and your Vantagepoint database.

Note: The steps below should also be performed on your database.

To configure/verify rights and privileges to the Report Server database server component:

1. Launch Microsoft SQL Server Management Studio.
2. Click the plus sign before the server name to expand the server, and then expand the Security folder.
3. Right-click the **Logins** folder and select **New Login**.
4. Select the Windows account, enter an existing SQL Server login, or create a new SQL Server login and assign it a password. The example below creates an account named **DeltakVantagepoint**.
5. Click **User Mapping** to display the User Mapping screen.
6. Select the **ReportServer** database option in the **Users mapped to this login** section.
The Database role membership for the server becomes enabled in the bottom section.
7. Select the **db_owner** option to add the login to the db_owner role for the database.
8. Repeat the same steps for the ReportServerTempDB database.
9. Repeat the same steps to map the login to the Vantagepoint database and give it **db_owner** role membership to the database.

Configure Transaction Document Management

Vantagepoint Transaction Document Management (TDM) uses Microsoft SQL Server FileStream technology to store and retrieve documents in a SQL Server database. Deltek has chosen to configure FileStream functionality and to store these documents in a separate database rather than in your Vantagepoint transactional database. These documents include transaction-related supporting documents as well as Adobe InDesign templates.

FileStream is a prerequisite to installing Vantagepoint and the various setup scripts will check to ensure that it is correctly installed and configured. If it is not, then you will need to install and configure it before you can install Vantagepoint. The setup scripts will also create the FileStream database (<databaseName>FILES) for you automatically with the Setup and SetupDatabaseNew switches and will check to ensure the FileStream database exists with SetupAndMigrate and MigrateDatabase and if it does not the setup will automatically create it.

This section will help you configure FileStream and Vantagepoint TDM.

Warning: Your separate Vantagepoint and FILESTREAM (TDM) databases must be backed up on the same schedule so that they will be in sync if a restore is needed.

Prerequisites

Install or upgrade to the current version of Vantagepoint.

FileStream Best Practices

Read the [FileStream Best Practices](#) article before you start.

Some examples of FileStream best practices are:

- Disable short file names on FileStream computer systems because they take significantly longer to create. To disable short file names, use the Windows fsutil utility.
- Regularly defragment FileStream computer systems.
- Use 64-KB NTFS clusters. Compressed volumes must be set to 4-KB NTFS clusters.
- Disable indexing on FileStream volumes and use the Windows fsutil utility to set **disablelastaccess**.
- Disable antivirus scanning of FileStream volumes, if possible. If antivirus scanning is necessary, avoid setting policies that automatically delete offending files.
- Ensure that your nightly backup routine (and any other backup processes) back up the FileStream database at the same time as your Vantagepoint transaction database. Metadata for uploaded files is stored in the Vantagepoint database, while the actual uploaded file data is stored in the FileStream database. If you restore one or both databases and the database backups are out of sync, data issues may occur. See "Databases Out of Sync" Issue for more information.

Note: The Vantagepoint Backup Utility application, on the Utilities menu, automatically backs up both the Vantagepoint transaction database and the FILESTREAM database.

Identify the SQL Server to Host the FileStream Database

In many Vantagepoint configurations, the SQL Server that hosts the Vantagepoint transaction database also hosts the FileStream database. However, Vantagepoint TDM has been developed to allow the FileStream database to exist on a separate SQL Server instance.

Enable FileStream on SQL Server

You must enable FileStream on the SQL Server instance intended to host the FileStream database before you can create the database. Because FileStream is not enabled by default, you must enable FileStream during the SQL Server installation or after SQL Server is installed. See the appropriate section for your installation.

Enable FileStream during SQL Server Installation

To enable FileStream during SQL Server installation:

1. Open the Database Engine Configuration.
2. Click the FileStream tab and ensure that the following options are selected:
 - Enable FILESTREAM for Transact-SQL access
 - Enable FILESTREAM for file I/O streaming access
 - Allow remote clients to have streaming access to FILESTREAM data

Note: By default, the Windows share name created for FILESTREAM access will be the SQL Server instance name (default SQL instances are named MSSQLSERVER). Deltak recommends that you use the default selections.

3. Click **Next** to continue.

Enable FileStream after SQL Server is installed

To enable FileStream after installing SQL Server:

1. On the database server, open the SQL Server Configuration Manager.
2. Right-click your SQL Server service, and click **Properties** on the shortcut menu.
3. Click the FileStream tab, ensure that all three options are selected, and click **OK**.

Note: By default, the Windows share name created for FileStream access will be the SQL Server instance name (default SQL instances are named MSSQLSERVER). Deltak recommends that you use the default selections.

In addition, complete the following configuration settings in SQL Server properties:

1. Open SQL Server Management Studio.
2. Right-click the server, and click **Properties**.
3. Select the **Advanced** page.

4. Check to ensure that the **Running Values** are displaying that the **Filestream Access level** is set to **Full access enabled**.
5. Click **OK**, and restart the SQL Server service.

Configure and Validate the FileStream Database with Weblink

After the FileStream database has been created and the IIS Application Pool identity has been granted db_owner rights to the FileStream database, use the Weblink Utility to create the FileStream database schema.

To configure the database schema and verify the configuration:

1. Launch and log in to the Weblink utility on the Vantagepoint web/application server, using the shortcut created in the Vantagepoint installation folder.
2. From the **Current Database** drop-down list, select the Vantagepoint database that will be used with Vantagepoint TDM.
3. Select the **Enable FileStream** check box.

You will receive a message asking if you would like to verify that the FileStream database is configured correctly.

By default, Weblink prefills:

- The name of the SQL Server being used for the Vantagepoint database
- The name of the FileStream database (required and grayed out)

If you are hosting the FileStream database on a different instance of SQL Server, click **No** and modify the name of the FileStream SQL Server. After you make the necessary changes, click **Test Connection** on the Weblink menu to re-test and create the FileStream database schema.

Note: Your FILESTREAM database can exist on a different SQL Server instance.

4. Click **Yes** to validate the configuration.
A message displays indicating that the FileStream database is not configured for use and asking if you would like to configure it.
5. Click **Yes** to create the FileStream database objects (tables, indexes, and so on).
When the objects are created, a message displays saying that the configuration is complete.

Files Administration Utility in Vantagepoint

Use the Vantagepoint Files Administration utility to search for and view files that were uploaded into Vantagepoint. These include supporting documents that were uploaded for Vantagepoint transactions, as well as InDesign templates that were imported or created using the Vantagepoint Merge Templates application.

To view the documents that have been uploaded using the Files Administration utility:

1. Open the Vantagepoint application.
2. On the Vantagepoint Utilities menu, click **Files Administration**.

3. On the Files Administration dialog box, use the **Date Range** fields to select the start and end dates to define the date range to search.
Vantagepoint defaults to use the past three days.
4. Click **Refresh Files List** to populate the Files grid.
Records that match the start and end date criteria display.
5. To further refine your results set, complete one or more of the following actions:
 - Enter specific text that you want to find. Vantagepoint searches the **File Name** and **Description** fields to locate the matching text.
 - Open the lookup and select a **User ID**.
 - Use the drop-down list to select a Vantagepoint application. This drop-down list displays the applications that allow supporting documents.
6. Click **Refresh Files List** to activate the search.
The Files grid lists all of the documents that match your criteria.
7. Click the **File Name** link to open the associated PDF.

“Databases Out of Sync” Issue

The Databases Out of Sync dialog box displays when the files in the Vantagepoint and FileStream databases are not synchronized. This file mismatch can occur when there is a database backup or restore on one database, but not the other. In this situation, the **File Name** link cannot open the selected file. Click **OK** to return to the Files Administration utility. Then contact your system administrator for details.

Troubleshooting FileStream

This section lists potential problems, causes, and solutions for issues with FileStream.

Weblink Cannot Create FileStream Database Objects

You test the database connection for the first time in Weblink, and Weblink cannot create the FileStream database objects.

Possible Cause	The FileStream filegroup name is not in the required format: [VantagepointFILESTREAMDBName]_FS .
Solution	Reformat the FileStream filegroup name.

Error: “FILESTREAM data cannot be placed on empty filegroup”

You receive a “FILESTREAM data cannot be placed on empty filegroup” error.

Possible Cause	The FileStream filegroup is not configured.
Solution	Configure the FileStream filegroup, and confirm that the FileStream filegroup name is in the required format: [VantagepointFILESTREAMDBName]_FS .

Not Configured to Upload Supporting Documents

When a user attempts to upload a document, Vantagepoint displays a message that it has not been configured to upload supporting documents.

Possible Cause	The Enable FILESTREAM option is not selected in Weblink and/or FILESTREAM is not configured properly (Weblink is unable to connect to the FILESTREAM database or the FW_Files table was not created.)
Solution	Confirm that the Enable FILESTREAM option is selected in Weblink and that FILESTREAM is configured properly.

FILESTREAM Database Cannot be Opened

When you test the FileStream configuration in Weblink, a message displays saying that the FileStream database cannot be opened and that the login failed for the user account running the IIS Application Pool Identity.

Possible Cause	The FileStream database has not been created or has not been created with the required naming format, or the identity of the DeltekVantagepointAppPool in IIS has not been granted db_owner rights to the FileStream database.
Solution	Confirm that the FileStream database exists and has been properly named and that the IIS Application Pool Identity has the required database rights.

Using FileStream with Other SQL Server Features

Refer to this table for information about how FileStream works with other SQL Server features.

Feature	Use with FileStream
All features	See Using FileStream with Other SQL Server Features .
SQL Server Availability Groups	See FileStream and FileTable with Always On Availability Groups (SQL Server) .
Transparent Data Encryption (TDE)	FileStream can be used with TDE although the FileStream data is not encrypted.
Log Shipping	Log shipping supports FileStream. Both the primary and secondary servers must be running SQL Server 2012 or later and have FileStream enabled.
Database Mirroring	Database mirroring does not support FileStream. A FileStream filegroup cannot be created on the principal server. Database mirroring cannot be configured for a database that contains FileStream filegroups.
Failover Clustering	For failover clustering, FileStream filegroups must be put on a shared disk. FileStream must be enabled on each node in the cluster that will host the FileStream instance.

Feature	Use with FileStream
SQL Server Express	SQL Server Express supports FileStream. The 4 GB database size limit does not include the FileStream data container.

How to Use FileStream in a Firewall-Protected Environment

To use FileStream in a firewall-protected environment, both the client and server must be able to resolve DNS names to the server that contains the FileStream files. FileStream requires that the Windows file-sharing ports 139 and 445 be open.

The “client” in your Vantagepoint TDM deployment is the web/application server, so if your Vantagepoint deployment has a firewall between the web/application server and the FileStream database server, then the ports referenced above must be open between the servers.

Queries to Join the Vantagepoint Transaction DB and FILES DB

The following query will obtain the file sizes in the FILES database by joining two [Vantagepoint] and [Vantagepoint]Files databases. This will work if the databases are on the same SQL Server.

```
SELECT DATALENGTH(a.FileData) as FileSize, b.FileName, b.ContentType FROM
[VantagepointDBName]FILES.dbo.FW_Files a inner join [VantagepointDBName].dbo.FW_Files b ON
a.FileID=b.FileID
```

The following query will obtain the file sizes in the FILES database by joining two [Vantagepoint] & [Vantagepoint]Files databases. This will work if the databases are on Linked SQL Servers.

```
SELECT DATALENGTH(a.FileData) as FileSize, b.FileName, b.ContentType FROM
[FILESTREAMDBServer].[ VantagepointDBName]FILES.dbo.FW_Files a inner join
[VantagepointDBName].dbo.FW_Files b ON a.FileID=b.FileID
```

Note: You must create the link between the servers first. See [SQL Server Books Online](#) for information on how to create Linked SQL Servers.

Configure a Shared Location for Databases.enc

If your Vantagepoint deployment includes multiple web/application servers, or a dedicated process server, you should create the shared directory as indicated below to eliminate the need to synchronize changes made to databases.enc across your servers. Although not required, Deltek recommends this configuration for the SetupWebApp and SetupProcessServer switches.

To configure a shared path for databases.enc:

1. Ensure that the databases.enc file is synchronized across all servers.
2. Identify a server that can host the file share.
This can be any server as long as it is located in the same data center as your Vantagepoint deployment.
3. Create a Windows file share on that server (for example, [\\server\share](#)).
4. Grant the service account(s) running the IIS Application Pool Identity and the Process Server service a minimum of modify rights to the share you created.
5. Modify the Vantagepoint web.config file (..\Vantagepoint\Web\web.config) on all web/application and process servers:
 - Under <appSettings>, locate the DatabasesEncDirectory entry and uncomment it out. (It will be commented out by default.)
 - For the value of this setting, enter the share path, not including the databases.enc file name. It should look like this, where [\\server\share](#) is the actual UNC path to your file share:

```
<add key="DatabasesEncDirectory" value="\\server\share" />
```
6. Copy the databases.enc file to the share.
7. Rename the databases.enc file on all web/application and process servers to **databases.old**.
8. Restart IIS and the Process Server service on all applicable servers and run tests to ensure that Vantagepoint and Weblink can be accessed on all web/application servers and that the Process Server service is processing jobs correctly.
9. Make sure to check the Application Event Logs on all servers for any errors or warnings.

Alternative to a Shared Databases.enc File

As an alternative to having a shared path for your databases.enc file, complete the following steps to synchronize changes made to databases.enc across your servers.

You must do this **every time** that you make changes to databases.enc.

1. Launch and log into the Weblink utility on one web/application server, using the shortcut created in the Vantagepoint installation folder. Configure your connection and application settings.
The settings are saved to a local encrypted databases.enc file on the server.
2. Copy the databases.enc file from your web/application server to all other web/application and process servers.
3. Restart the Deltek Vantagepoint Process Server Windows service and IIS on each machine.
4. Repeat this process whenever any update is made in Weblink.

Configure Secure Sockets Layer (SSL)

Important Information on SSL Configurations

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

Read this section to better understand:

- How the Vantagepoint reporting framework handles SSL requests.
- How the use of non-standard ports impacts functionality.
- What configurations are and are not possible using non-standard ports.

How the Reporting Framework Handles SSL

Each request to run a report in Vantagepoint includes several calls to the report server web service URL. Some of these calls are server-side (made from the Vantagepoint web/application server) and some of these calls are client-side (made from the Vantagepoint application on the user's workstation).

When Vantagepoint is configured for SSL, the SQL Reporting Services server must also be configured for SSL. When you use a reverse proxy, Vantagepoint does not support the use of SSL Offloading so an SSL certificate must be installed and configured on the report server.

The default behavior for server-side calls is that they are always made using only HTTP, which requires that the report server have an HTTP binding configured. An alternative approach is to use HTTPS for server-side calls. This approach works only if SSL is configured for use by both Vantagepoint and Reporting Services. Select the **Use HTTPS for Reporting Services server-side calls** option on the Report Server tab in Weblink to use HTTPS for server-side calls.

Client-side calls are always made using the protocol prefix used to access Vantagepoint, which requires SSL. When you use SSL, the communication between the client and the server is always encrypted, whether or not a reverse proxy is used. The SQL Reporting Services server must have an HTTPS binding in addition to the HTTP binding, or the **Use HTTPS for Reporting Services server-side calls** option must be selected to use HTTPS for server-side calls.

Non-Standard SSL Ports

While it is possible to use non-standard SSL ports with Vantagepoint, the default reporting framework behavior is that all server-side calls to the report server URL are made using HTTP. For this reason, if you are using a non-standard SSL port for your SQL Reporting Services URL (for example, `http://<ReportServer>:4443/reportserver`) in Weblink, you need to use a reverse proxy, such as ARR, and enable SSL Offloading. Alternatively, if you select the **Use HTTPS for Reporting Services server-side calls** option, you do not need to configure an HTTP binding for SSRS or use a reverse proxy.

In addition, you need to configure an HTTP port on SSRS with the same port value (for example, HTTPS web server port 4443 and SSRS HTTP port 4443). This will ensure that client requests to the ARR reporting virtual directories work properly and that server-side calls from the web server to the report server also work properly.

Similar changes are required if you use a hardware- or software-based reverse proxy solution other than ARR. ARR is the only reverse proxy solution tested by Deltek.

You can successfully use a non-standard SSL port for your Vantagepoint URL, but to use non-standard ports with SSRS, you must do one of the following:

- Use a reverse proxy.
- Select the **Use HTTPS for Reporting Services server-side calls** option.
- Reconfigure your system to use standard HTTP/HTTPS ports 80/443.

In a two- or three-tier Vantagepoint deployment where SSRS is on a different server than Vantagepoint, a configuration without a reverse proxy and SSL Offloading enabled would require that the same non-standard port be enabled on SSRS for both SSL and non-SSL bindings under the default reporting framework behavior. This is not possible due to the resulting port conflict. To resolve this issue, select the **Use HTTPS for Reporting Services server-side calls** option.

Likewise, using the default reporting framework behavior, you cannot configure a single server installation with non-standard ports for both Vantagepoint and SSRS, with or without ARR, because the same port would be required for both HTTP and HTTPS, resulting in a port conflict. However, you can have a single server installation of Vantagepoint and SSRS using standard HTTP/ HTTPS ports 443/80, with or without ARR. To resolve this issue, select the **Use HTTPS for Reporting Services server-side calls** option.

Secure the Vantagepoint Web Server

To configure Vantagepoint 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 at left, 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 web site.
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 web site using **https://** as the URL prefix and make sure that everything is working correctly.

Secure SQL Server Reporting Services

The Reporting Services Configuration Manager does not directly support requesting and importing the SSL certificate, as IIS does. To request and import the SSL certificate on your Reporting Services server, you must use the Certificates MMC (Microsoft Management Console) snap-in, described below.

If you are using SSL for Vantagepoint (required), you **must** use SSL for Reporting Services. You cannot run SSL for Vantagepoint without an SSL binding configured for Reporting Services.

- You cannot run Vantagepoint without SSL and still use SSL for Reporting Services.
- The Reporting Services web service URL in Weblink must reference the fully qualified domain name of the report server. This is specified in the SSL certificate. If the report server previously referenced a local netbios name, you must change it to the fully qualified domain name. The fully qualified domain name must be in the format:

<https://Vantagepoint.companyname.com/reportserver>

Note: If SQL Reporting Services and IIS are being used on the same server and you have already configured an SSL certificate for IIS, you do not need to use the Certificate MMC imported in steps 1 through 9 below. Start with Step 10.

To secure SQL Server Reporting Services for Vantagepoint:

1. Click **Start » Run**.
2. In the **Open** field on the Run dialog box, enter **mmc** and click **OK** to launch the MMC console.
3. Click **File » Add/Remove Snap-in**.
4. On the Add or Remove Snap-ins dialog box, select **Certificates** and click **Add**.
5. Select **Computer account**, and click **Next**.
6. Select **Local Computer**.

7. Click **Finish**, and then click **OK**. You should now see the certificate store.
Now you need to request a new certificate or import an existing certificate.
8. Right-click the Personal folder, and point to **All Tasks**.
9. Select one of the following actions:
 - If you have a domain Certificate Authority (CA), click **Request New Certificate**.
 - If you need to request a certificate from a stand-alone CA or an online CA, click **Advanced Operations » Create Custom Request**.
10. After you have your SSL certificate, import it using the following steps:
 - a. Right-click the Personal folder.
 - b. Click **All Tasks » Import** to launch the Certificate Import Wizard.
 - c. Browse to the location of your SSL certificate and complete the import process.

At this point, the certificate is registered with the server. The next step is to register the certificate with SQL Reporting Services.
11. Click **Start » All Programs » Microsoft SQL Server » Configuration Tools** to open the Reporting Services Configuration Manager on the Report Server.
Next you must create the SSL bindings for the Web Service URL and the Report Manager URL.
12. Under **Connect**, click **Web Service URL**. The Web Service URL window displays.
13. On the Web Service URL window, click **Advanced**.
14. On the Advanced Multiple Web Site Configuration dialog box, under **Multiple SSL Identities for the Report Server Web Service**, click **Add**.
15. On the Add a Report Server SSL Binding dialog box, select a specific **IP Address** (if appropriate).
16. Click the drop-down list for the **Certificate** option. The certificate you imported in the previous steps should display.
17. Select the certificate.
18. Click **OK** to add this URL to the system.

Note: If all communication to the report server will be done via SSL, you should also remove the HTTP binding from the configuration.

19. Repeat these steps for the Report Manager URL.
20. On the Web Server, launch Weblink, log in, and select the database.
21. On the ReportServer tab, verify that the URL contains a reference to the fully qualified domain name of the report server.

This is specified in the SSL certificate. If the report server previously referenced a local machine name, you must change it to the fully qualified domain name. The fully qualified domain name must be in the form: <https://vantagepoint.companyname.com/reportserver>

Test the SSL Configuration

Test Vantagepoint using SSL URLs to ensure that the product is functioning correctly. To do this, trace a Vantagepoint SSL session using [Telerik Fiddler](#) or another HTTP tracing tool.

Reload Reports into Vantagepoint

During the web server/tier installation process, Vantagepoint installs a standard set of reports for each supported language. Vantagepoint uses the following internal steps to complete this process:

1. Vantagepoint installs the report folders and files into the Vantagepoint\Reports folder (default location: \Program Files\Deltek\Vantagepoint\Reports).
2. Vantagepoint imports the Vantagepoint Report files into Microsoft SQL Server Reporting Services (SSRS), which makes the reports available in Reporting Services.

Connection Errors

If there are problems with the connection between Vantagepoint and the report server, the reports will not install correctly onto the report server.

Identify the Error

If the Vantagepoint installation displays a message stating that reports were not successfully imported during the installation process, you must complete the appropriate procedure for your installation type.

Test the Report Server Settings in Weblink

1. Launch the Vantagepoint Weblink application.
2. For each database in the drop-down list, click the Report Server tab.
3. Click the **Test Report Server** button to verify that no errors occur during the connection.
4. Save your changes and exit Weblink.
5. Reload your reports into Vantagepoint.

Reload Reports into Vantagepoint

You have two options for reloading reports into Vantagepoint:

To reload reports using the LoadReports switch:

See [LoadReports Switch](#).

To reload reports using the Smart Client application:

1. Launch the Vantagepoint Smart Client application.
2. In the Vantagepoint Navigation menu, click **Utilities » Report Administration** to display the Reporting Administration form.
3. Select the Load Reports tab to load reports on the report server.
4. In the **Location of reports on application server** field, enter the file path location of the reports (RDL files) on the report server.
5. From the **Type** option drop-down list, select **Standard**.
6. If you want to load a single report, enter the name of the report in the **Report Name** field. (You do not need to supply the .RDL extension.)

You can also use this field as a wild card search. For example, if you enter Project, Vantagepoint finds and loads all files that contain the word Project, such as Project List, Project Summary, and Project Audit.

Sub reports do not load for main reports; you must load them manually by name. If you leave the **Report Name** field blank, all reports load.

7. Click **Load Report Files**. A loading reports warning message displays.
8. Click **OK** to continue the reload report process.
9. To install custom reports, return to step 5.

This time, select **Custom** from the **Type** option drop-down list. Then complete the remaining steps of the procedure.

Attention: For additional information on reloading reports, click the **Help** button on the Load Reports Tab.

Create a Reverse Proxy for SQL Reporting Using Application Request Routing (ARR)

Do I Need a Reverse Proxy?

Vantagepoint uses the Microsoft SQL Reporting Services WinForms/Web report viewer control to render reports. This control requires a direct connection to the server running the SQL Reporting Services web service. Due to the nature of the Vantagepoint and SQL Reporting Services logical tier architectures and the available editions and licensing requirements of SQL Reporting Services, it is likely that the SQL Reporting Services web service will not be installed on the web/application server in your deployment of Vantagepoint.

Typically, this is not a problem when Vantagepoint is deployed inside the intranet. However, when Vantagepoint is deployed where it is accessible directly via the Internet, the infrastructure requirements needed to support the configuration become complex because it is necessary to have:

- Multiple points of entry (one each for the web server and SQL Reporting web service)
- Multiple firewall configurations
- Potentially, multiple public DNS records with your Internet Service Provider (ISP)

To complicate matters, if you have a two-tier deployment of Vantagepoint, this deployment may require that the server hosting your database is accessible to the Internet, posing additional security risks.

A reverse proxy using Microsoft's Application Request Routing (ARR) extension for IIS allows the direct forwarding of requests through the Vantagepoint web server to the reporting services web service, with responses back to your Internet clients. This configuration resolves all of the issues described above. The primary intent of a reverse proxy is to shield the SQL server from access via the Internet. Specifically, this applies in two-tier deployments where the SQL database and report server are on the same physical machine. Deltek does **not** generally recommend using a reverse proxy because it can have an adverse effect on the performance of the web/application server.

Deltek supports the use of Application Request Routing 3.0. Follow the steps below to install ARR. These installation instructions are specific to version 3.0 of ARR.

Attention: For additional information, see [Application Request Routing](#).

Important Information on the Use of Non-standard Ports

Before installing and configuring ARR, see [Configuring Secure Sockets Layer \(SSL\)](#) for information on how the reporting framework handles SSL requests and potential issues with the use of non-standard ports.

Prerequisites

The following prerequisites must be met before installation:

- The Vantagepoint web/application server must be running one of the following:
 - Windows Server 2016 / IIS 10.0
 - Windows Server 2012 R2 / IIS 8.5

- Vantagepoint must be installed.
- The IIS configuration must include the IIS role service **Management Service**.

Install Application Request Routing (ARR)

To download and install Application Request Routing on your Vantagepoint web/application server:

1. Go to the following URL to install ARR 3.0 via the Microsoft Web Platform installer:
<http://www.iis.net/downloads/microsoft/application-request-routing>
2. Click **Install this Extension**.
3. On the Microsoft Web Platform Installer page, click **Install Now**.
4. On the File Download dialog box, click **Run** to run the ARRv3_0.exe file.
5. When the Web Platform Installer launches, choose to install Application Request Routing 3.0.
The Web Platform Installer will ensure that all prerequisites required for the installation are also downloaded and installed.
6. Accept the license agreements.
7. When the Web Platform Installer has finished downloading and installing all components, click **Finish** and then click **Exit** on the Web Platform Installer main page.

Configure Application Request Routing (ARR)

To configure Application Request Routing:

1. Open Windows Explorer and create two folders under <drive>:\Program Files\Deltek\Vantagepoint\Web\, named:
 - **ReportServer**: For example, enter: c:\Program Files\Deltek\Vantagepoint\Web\Reportserver.
 - **Reports (optional)**: This folder is needed only if you want external access to Report Manager. Vantagepoint does not need this folder.
2. Create a new Application Pool called **DeltekVantagepointReportingProxy**:
 - a. In IIS Manager, expand the server name.
 - b. Right-click **Application Pools**, and select **Add Application Pool**.
 - c. Enter the name, and click **OK** to create the Application Pool.
3. Modify the Application Pool settings:
 - a. Right-click the DeltekVantagepointReportingProxy Application Pool, and select **Advanced Settings**.
 - b. Set **Enable 32 bit applications** to false.
 - c. Configure the **Identity** to be the same account as your DeltekVantagepointAppPool.
 - d. Set **Idle Time-out** to **0** (the default is 20).
 - e. Scroll down to see more Advanced Settings.
 - f. Set **Regular Time Interval (minutes)** to 0 (the default is 1740).

- g. Set **Specific Times** to **00:15:00** (the default is 00:00:00).
4. Create IIS Applications to act as the proxy for the Reports (SQL RS Report Manager) and ReportServer (SQL RS web service):
 - a. In IIS Manager, expand **Sites**.
 - b. Right-click **Default Web Site**, and select **Add Application**.
 - c. (Optional) In the **Alias** field, enter **Reports**, configure it to use the DeltekVantagepointReportingProxy, and enter (or browse to) the physical path that you created in step 1.
 - d. Click **OK** to create the Reports application.
5. (Required) Set up the ReportServer Application:
 - a. Right-click **Default Web Site**, and select **Add Application**.
 - b. In the **Alias** field, enter **ReportServer**, configure it to use the DeltekVantagepointReportingProxy, and enter (or browse to) the physical path you created in step 1.
 - c. Click **OK** to create the ReportServer Application.
6. Add **Rewrite Rules** for each reporting application.
 - a. Under **Default Web Site**, click **Reports Application**.
 - b. Double-click **URL Rewrite**.

Note: If you do not see the URL Rewrite module, it's possible that Internet Services Manager was open when ARR was installed. Close and re-open Internet Services Manager.

- c. Click **Actions » Add Rules**.
- d. Select **Reverse Proxy**, and click **OK**.
- e. Click **OK** when you see the prompt: **Are you sure you want to enable proxy functionality?**
- f. On the Add Reverse Proxy Rules dialog box, enter the name of your SQL Reporting Services server in the **Inbound Rules** text box.

Since your Vantagepoint server is configured for SSL and your Report Server is also required to be SSL enabled, the option **Enable SSL Offloading** (default) is not necessary, so clear this option so that this feature is not enabled. This ensures that all communication remains encrypted.

- g. Click **OK** to create the reverse proxy rule.
- h. Select the rule that was created and click the **Edit** link on the right, under **Inbound Rules**.
- i. By default, the rewrite rule only includes the base URL for the server name entered. Edit the URL under **Rewrite URL** to have the correct Reporting Services application. The correct URL is:

http://<reportserver>/Reports/{R:1}

Note: Make sure that there is a slash between Reports and {R:1}.

7. Repeat steps 6a through 6g for the ReportServer virtual directory.
 - a. Under **Default Web Site**, click **ReportServer Application**.
 - b. Double-click **URL Rewrite**.
 - c. Click **Actions » Add Rules**.
 - d. Select **Reverse Proxy** and click **OK**.
 - e. When prompted about enabling proxy functionality, click **OK**.
 - f. On the Reverse Proxy Rules dialog box, enter the name of your SQL Reporting Services server in the **Inbound Rules** text box.
 - g. Click **OK** to create the reverse proxy rule.
8. Select the rule that was created and click the **Edit** link on the right under **Inbound Rules**. By default, the rewrite rule only includes the base URL for the server name entered.
9. Edit the URL under **Rewrite URL** to have the correct Reporting Services application. The correct URL will be:
`http://<reportserver>/ReportServer/{R:1}`

Test the Proxy Server

To test the proxy server:

1. Open Internet Explorer.
2. Browse to the following URLs.

If ARR has been configured properly, your request will be proxied to the SQL Reporting Services server.

- `https://<VantagepointWebServer>/Reports`
 where <VantagepointWebServer> is the Fully Qualified Domain Name of the web/application server.
- `https://<VantagepointWebServer>/ReportServer`
 where <VantagepointWebServer> is the Fully Qualified Domain Name of the web/application server.

Configure Vantagepoint to Use the Reverse Proxy

To modify Weblink to use the reverse proxy:

1. On the web/application server, open and log into the Weblink utility, using the Weblink shortcut in the Vantagepoint installation directory.
2. Enter the password to access Weblink.
3. Click the Report Server tab, and modify the Server URL to be the URL to access the new ReportServer virtual directory that you created on the Vantagepoint Web Server.
4. Typically, the Server URL is in the form `https://<ReportServer>/ReportServer`. Change this to `https://<VantagepointWebServer>/ReportServer`.

No additional changes are necessary for the Weblink configuration. Be sure to change all databases that will use the reverse proxy.

5. To test the Report Server configuration, click **Test » Report Server Configuration**.
6. After the configuration tests successfully, save your changes.

Troubleshooting

If you need help, contact the Deltek Global Services consulting group, DeltekforPSConsulting@deltek.com. The consulting group will provide an estimate of the cost for the help that you need.

Configure HTTP Compression

Configuring HTTP Compression for Vantagepoint 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. Deltak 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. See the blog post [IIS 7 Compression. Good? Bad? How much?](#) for information and recommendations on setting compression levels. 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.

However, you must configure specific content types to compress the ClickOnce content types. Use these commands:

```
C:\Windows\system32\inetsrv\appcmd set config /section:httpCompression
/+dynamicTypes.[mimeType='application/octet-stream',enabled='true']
/commit:apphost

C:\Windows\system32\inetsrv\appcmd set config /section:httpCompression
/+dynamicTypes.[mimeType='application/x-ms-application',enabled='true']
/commit:apphost

C:\Windows\system32\inetsrv\appcmd set config /section:httpCompression
/+dynamicTypes.[mimeType='application/x-ms-manifest',enabled='true']
/commit:apphost
```

Note: ClickOnce content types are considered dynamic. If you add them under the `<staticTypes>` section, ClickOnce files are not compressed. See the following Microsoft support article for additional guidance on setting content types: [How to add content types for HTTP compression in IIS 7.0](#).

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" />`

Pre-Deploy Vantagepoint Smart Client to User Workstations

Vantagepoint uses two technologies in the client tier:

- The primary technology is a web-based interface (web client).
- The secondary technology is a smart client that uses the ClickOnce deployment technology for delivering Windows-based applications to the user. The smart client application checks for new updates on the web/application server each time the application is launched and automatically installs them into the local user's profile (%USERPROFILE%\Local Settings\Apps\2.0\...).

The smart client technology will be phased out prior to the release of Vantagepoint 3.0.

To reduce the size of the initial client-side download when a user launches the Vantagepoint smart client, you can pre-deploy the smart client files to user workstations. This "Hybrid Deployment Model" (HDM) installs the application by first looking in a specific folder on the workstation and, if no file is found there, downloading the file from the application/web server.

When you use HDM, ClickOnce delivers about 15 files (enough to display the login page). After that, HDM takes over to deliver core application assemblies, software updates, language-specific satellite assemblies, and custom items.

ClickOnce Deployment Features

- Applications are installed per-user, not per-computer.
- Administrator privileges are not required.
- Applications do not have to be installed through Add/Remove Programs.
- Nothing is registered to the GAC (Global Assembly Cache).
- No ActiveX objects, plug-ins, or Java applets are used.
- The ClickOnce cache is located here: c:\Users\USERPROFILE_Name\AppData\Local\Apps\2.0

Files to be Deployed

You must repeat the process below each time that you upgrade your Vantagepoint application/web servers to a new release.

The files that are pre-deployed to the user workstations are located on the application/web server in the **\Program Files\Deltek\Vantagepoint\SmartClient** folder (where Vantagepoint is installed):

- DeploymentManifest.xml
- One or more zip files (as listed in the DeploymentManifest.xml)

You must copy all of the zip files, plus the DeploymentManifest.xml, to the workstation.

The date and time on the time stamp for each zip file must match the date and time shown in the **DeploymentManifest.xml**.

Deploy Files to a Workstation

Use the procedure below to deploy files to a workstation. The workstation must be running Windows 7 or higher.

To deploy files:

1. Locate the \ProgramData\ directory, and create the Deltek directory.
By default, the \ProgramData folder on Windows 7 and higher is hidden. You may need to select the **Show Hidden Files** option in Windows Explorer.
2. Copy the DeploymentManifest.xml file and **all** zip files from the application/web server into the Deltek directory.
3. Repeat this process each time that you upgrade your Vantagepoint application/web servers to a new release.

Configure Integrated Security for Vantagepoint

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

To do this, you configure Windows Integrated Security for each user's Vantagepoint account, using the Windows Domain network login as the username for that user. This allows the user to be automatically logged in to Vantagepoint 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 Vantagepoint. 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 Vantagepoint.

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.

Alternative Approach: As an alternative to using Windows Integrated Security, you can use the Microsoft Azure Active Directory single sign-on (SSO) feature. Like Windows Integrated Security, it lets users log on to Vantagepoint using their Windows usernames and passwords instead of using separate Vantagepoint usernames and passwords.

This approach is more commonly used with the cloud version of Vantagepoint and is described in the [Cloud Administrator's Help System](#).

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 Vantagepoint:

- You must configure a domain user account as the IIS Application Pool identity for the DeltekVantagepointAppPool in IIS. The domain account does not require domain administrative rights. Optionally, the Vantagepoint installation creates a local Windows account, DeltekVantagepoint, 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 Vantagepoint web/application server:
 - The account must be a member of the following local groups:
 - Administrators group
 - IIS_IUSERS 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 Vantagepoint IIS Application (virtual directory) from using Anonymous Access to using Windows Integrated Security.

Important: If your web server URL uses a custom DNS name that does not match the FQDN of the machine (for example, Vantagepoint.company.com vs. server01.company.com), you probably need to enable the BackConnectionHostNames registry entry.

Refer to this Microsoft article for help creating the entry: <https://support.microsoft.com/en-us/help/926642/error-message-when-you-try-to-access-a-server-locally-by-using-its-fqd>

Important if you use Deltek Touch applications: When you use Windows Integrated Authentication with Vantagepoint, after you enable Windows Authentication for the Vantagepoint application, you must also disable Windows Authentication for the Touch folder in IIS and re-enable Anonymous Authentication. If you do not do this, the Touch applications will no longer authenticate successfully.

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.

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 **DeltekVantagepointAppPool**, 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 Vantagepoint 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

Do **not** make any modifications to the security settings for the VantagepointClient IIS Application. The application represents the ClickOnce deployment and must continue using Anonymous Access.

To configure IIS to use Windows Integrated Authentication:

1. From within Internet Information Services, expand the web site where the Vantagepoint application is installed.
2. Select the Vantagepoint 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, which is documented later in this section.

7. Select the Vantagepoint Mobile folder.
8. Double-click the **Authentication** icon under IIS.
9. Select **Anonymous Authentication** and click **Enable** on the Actions pane.
10. Select **Windows Authentication** and click **Disable** on the Actions pane.
11. Launch the Vantagepoint application.

You should test both the Smart Client and Web Client as well as the Touch applications to ensure authentication is working correctly. You may see the **Windows Authentication** option on the login page. This option displays if you have multiple databases configured in Weblink. If there is only one database, the user is automatically logged into Vantagepoint, and this screen does not display.

Configure Vantagepoint for Windows Integrated Authentication

After the servers are configured to support Windows Integrated Authentication, you must configure Vantagepoint application domain users with their domain logins.

Weblink has options on the System Settings Tab that may alleviate performance issues when using Windows Integrated Authentication. See the Weblink help for details. Test changes to these settings thoroughly before you implement the changes in a production environment.

To configure a domain login for Vantagepoint:

1. Launch the Vantagepoint Web application, and log in as a user with the appropriate security rights.
2. Click **Configuration » Security » Users**, and create a new user.
3. Enter the domain username for the user you want to create (for example, the login ID used to log in to the Windows domain).
4. Complete the additional information required for the user.
5. Select the **Windows Authentication** option.
6. From the **Domain** drop-down list, select the domain for this user. If the domain is not listed, you can manually enter the netbios name of the domain.
7. Save your changes.

When the user launches Vantagepoint, the login screen displays with the **User ID** and password blank and the **Windows Authentication** check box cleared unless the Weblink option **Automatically check Windows Authentication check box in Weblink** is selected.

- After a user logs in with **Windows Authentication** selected, this setting is remembered for subsequent logins.
- If there is only one database defined in Weblink and the application is configured for Windows Integrated Authentication, the user is automatically logged in to the application on all subsequent logins after the initial login.

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 Vantagepoint application.

The Internet Explorer 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, Internet Explorer.

Configure Windows Integrated Authentication for the Vantagepoint Database Connection

The first step in using Windows Integrated Authentication for the Vantagepoint database connection is to grant the domain user account running the IIS Application Pool Identity the appropriate rights to the Vantagepoint database (and the report server and session state databases, as needed).

To establish rights for SQL Server:

1. Identify the domain user account that is being used as the Application Pool Identity in IIS. See step 3 in the [Configure the Application Pool Identity](#) section.
2. In SQL Server Enterprise Manager, create a SQL login for this domain user account.
3. Click **User Mapping** and grant db_owner rights to the Vantagepoint database (and the report server and session state databases).
4. Modify Weblink to use Windows Integrated Authentication for the various database connections. Complete steps 5 through 10 to enable these settings.

5. Launch Weblink and enter the Weblink password when prompted.
6. Click **OK**.
7. From the **Current Database** drop-down list on the Weblink screen, select the database to which you want to connect.
8. Select the **Windows Authentication** option to use the domain Application Pool Identity user account to connect to the database.
9. If necessary, you can also enable Windows Integrated Authentication for the report server database connection. In this situation, the account requiring access may differ from the one used for the IIS Application Pool Identity.

The account that will be used to make this connection is shown on this page as the **Windows Username** under the report server URL. If this is a different account than the IIS Application Pool Identity, you must grant db_owner rights to the report server databases and then select the Windows Integrated option for the report server database authentication.

Optionally, if you are using SQL Server session state, you can also enable Windows Integrated Authentication for that connection. This will use the IIS Application Pool Identity to make the database connection.

Weblink has options on the System Settings Tab that may alleviate performance issues when using Windows Integrated Authentication. See the Weblink help for details. Test changes to these settings thoroughly before you implement the changes in a production environment.

10. On each of the tabs in Weblink, select the test button to test the connection.

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 Vantagepoint 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 Vantagepoint is installed).
4. Select the Vantagepoint 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. The Advanced Settings dialog box displays.

7. If the **Kernel Mode Authentication** check box is selected, Kernel Mode Authentication is enabled.

Kernel Mode Authentication Implementation

The default configuration works for the Vantagepoint 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 Vantagepoint 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 DeltekVantagepointAppPool.

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)

Note: 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 /Vantagepoint/MethodCall.aspx - 80 - 10.5.4.5 - - 401 2 5 484
2016-01-05 16:24:51 10.5.12.16 POST /Vantagepoint/MethodCall.aspx - 80 - 10.5.4.5 - - 401 1 2148074254 15
2016-01-05 16:24:51 10.5.12.16 POST /Vantagepoint/MethodCall.aspx - 80 DOMAIN\user 10.5.4.5 - - 200 0 0 501
2016-01-05 16:24:51 10.5.12.16 POST /Vantagepoint/MethodCall.aspx - 80 - 10.5.4.5 - - 401 2 5 15
2016-01-05 16:24:51 10.5.12.16 POST /Vantagepoint/MethodCall.aspx - 80 - 10.5.4.5 - - 401 1 2148074254 0
2016-01-05 16:24:51 10.5.12.16 POST /Vantagepoint/MethodCall.aspx - 80 DOMAIN\user 10.5.4.5 - - 200 0 0 15
2016-01-05 16:24:51 10.5.12.16 POST /Vantagepoint/MethodCall.aspx - 80 - 10.5.4.5 - - 401 2 5 0
2016-01-05 16:24:51 10.5.12.16 POST /Vantagepoint/MethodCall.aspx - 80 - 10.5.4.5 - - 401 1 2148074254 0
2016-01-05 16:24:51 10.5.12.16 POST /Vantagepoint/MethodCall.aspx - 80 DOMAIN\user 10.5.4.5 - - 200 0 0 15
2016-01-05 16:24:54 10.5.12.16 POST /Vantagepoint/MethodCall.aspx - 80 - 10.5.4.5 - - 401 2 5 15
2016-01-05 16:24:54 10.5.12.16 POST /Vantagepoint/MethodCall.aspx - 80 - 10.5.4.5 - - 401 1 2148074254 0
2016-01-05 16:24:54 10.5.12.16 POST /Vantagepoint/MethodCall.aspx - 80 DOMAIN\user 10.5.4.5 - - 200 0 0 140
```

Kerberos:

```
2016-01-05 17:37:46 10.5.12.16 POST /Vantagepoint/MethodCall.aspx - 80 - 10.5.4.5 - - 401 2 5 0
2016-01-05 17:37:47 10.5.12.16 POST /Vantagepoint/MethodCall.aspx - 80 DOMAIN\user 10.5.4.5 - - 200 0 0 93
2016-01-05 17:37:47 10.5.12.16 POST /Vantagepoint/MethodCall.aspx - 80 - 10.5.4.5 - - 401 2 5 0
2016-01-05 17:37:47 10.5.12.16 POST /Vantagepoint/MethodCall.aspx - 80 DOMAIN\user 10.5.4.5 - - 200 0 0 15
2016-01-05 17:37:47 10.5.12.16 POST /Vantagepoint/MethodCall.aspx - 80 - 10.5.4.5 - - 401 2 5 0
2016-01-05 17:37:47 10.5.12.16 POST /Vantagepoint/MethodCall.aspx - 80 DOMAIN\user 10.5.4.5 - - 200 0 0 15
2016-01-05 17:37:50 10.5.12.16 POST /Vantagepoint/MethodCall.aspx - 80 - 10.5.4.5 - - 401 2 5 0
2016-01-05 17:37:50 10.5.12.16 POST /Vantagepoint/MethodCall.aspx - 80 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.

Configuration Options for Authentication Persistence

If performance is a concern, you can enable Authentication Persistence via the Advanced Server Connection Settings on the System Settings tab of the Weblink utility.

Select one of the following configuration options.

Option	Description
Share a single HTTP connection for all HTTP requests and establish authentication persistence when using Windows Integrated Authentication (supports Kerberos only)	<p>Select this option if you are sure that all connections are authenticating via Kerberos (for example, if you have an Active Directory domain to which all users authenticate and you do not have Vantagepoint open to the Internet).</p> <p>Be sure that Negotiate is at the top of the list in the Providers link under the Windows Authentication configuration for the Vantagepoint application in IIS. You can further validate if Kerberos is in use by reviewing the IIS logs and comparing them to the examples above.</p>
Share a single HTTP connection for all HTTP requests when using Windows Authentication (supports Kerberos and NTLM) *requires additional configuration – see help documentation for more details*	<p>Select this option to support both Kerberos and NTLM authentication if Vantagepoint is open to the Internet.</p> <p>You must also change the IIS configuration to add the authPersistNonNTLM setting, which involves modifying the web.config file. Use the following references to learn more:</p> <ul style="list-style-type: none"> ▪ Article on Windows Authentication from Microsoft Support ▪ Article on how to troubleshoot Kerberos failures in IE from Microsoft Support ▪ Article comparing request-based and session-based Kerberos authentication from Microsoft Tech Community <p>The settings discussed above must be implemented on all Web/application servers.</p>
None Selected (default)	The default behavior of IIS does not change.

If the client is not going through a proxy to access the web server, select the related **Disable automatic proxy detection on HTTP requests (can improve performance over high latency connections)** check box to disable automatic proxy detection. This approach only has an impact on highly latent connections (100ms or higher).

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.

Important Configuration Changes for Vantagepoint API

If you are using Windows Authentication and third party integrations such as Vantagepoint Connect and GovWin IQ that make calls into the Vantagepoint API, the following configuration changes are needed. Note that the deployment scripts for Vantagepoint will detect if Windows Authentication is enabled and automatically make the necessary IIS and web.config changes.

Modify IIS Feature Delegation

The Anonymous and Windows Authentication features must be changed from Read Only to Read/Write in IIS Feature Delegation. Follow the steps below make this change:

1. On the Vantagepoint web server open Internet Information Services Manager (IIS).
2. On the connections pane, click on the server name.
3. On the <Server> Home pane (middle), double click on Feature Delegation under Management.
4. Locate and select **Authentication – Anonymous**. If the Delegation column shows Read Only, click on Read/Write in the Actions pane to change it.

5. Locate and select **Authentication – Windows**. If the Delegation column shows Read Only, click on Read/Write in the Actions pane to change it.
6. Close IIS.

Modify Vantagepoint Web.config File

IMPORTANT: The following steps involve modifying the Vantagepoint web.config file. Incorrect modification can cause the Vantagepoint application to stop functioning. If you have any questions or concerns about the steps below, contact Deltek Support for assistance.

Changes are required to the Vantagepoint web.config file as follows.

1. On the Vantagepoint web server, make a backup of the Vantagepoint web.config file in <drive>:\Program Files\Vantagepoint\Web.
2. Open Notepad using 'Run as Administrator' and open the web.config file.
3. Locate the <location path="api"> tag. Place your cursor at the end of that tag hit enter.
4. Add the following on the new line:

```
<system.web>
    <authorization>
        <!-- All anonymous users access to the virtual path api -->
        <allow users="*" />
    </authorization>
</system.web>
```

5. Still in the <location path="api"> tag, locate the <system.webServer> section and then locate the end tag for </handlers>. Place your cursor at the end of that tag hit enter.
6. Add the following which should be located between the </handlers> end tag and the </system.webServer> end tag:

```
<security>
    <authentication>
        <!-- Need to enable anonymous access and turn off Windows
authentication for the virtual path -->
        <anonymousAuthentication enabled="true"/>
        <windowsAuthentication enabled="false"/>
    </authentication>
</security>
```

7. Save the web.config file.

The original and modified <location path="api"> tags are shown below:

FROM (original):

```
<location path="api">
  <system.web>
    <!-- Need to include the security overrides else it will inherit from the root of
the application -->
    <system.webServer>
      <handlers>
        <remove name="ExtensionlessUrlHandler-ISAPI-4.0_32bit" />
        <remove name="ExtensionlessUrlHandler-ISAPI-4.0_64bit" />
        <remove name="ExtensionlessUrlHandler-Integrated-4.0" />
        <add name="ExtensionlessUrlHandler-ISAPI-4.0_32bit" path="*" verb="*"
modules="IsapiModule"
scriptProcessor="%windir%\Microsoft.NET\Framework\v4.0.30319\aspnet_isapi.dll"
preCondition="classicMode, runtimeVersionv4.0, bitness32" responseBufferLimit="0" />
        <add name="ExtensionlessUrlHandler-ISAPI-4.0_64bit" path="*" verb="*"
modules="IsapiModule"
scriptProcessor="%windir%\Microsoft.NET\Framework64\v4.0.30319\aspnet_isapi.dll"
preCondition="classicMode, runtimeVersionv4.0, bitness64" responseBufferLimit="0" />
        <add name="ExtensionlessUrlHandler-Integrated-4.0" path="*" verb="*"
type="System.Web.Handlers.TransferRequestHandler"
preCondition="integratedMode, runtimeVersionv4.0" />
      </handlers>
    </system.webServer>
  </location>
```

TO:

```
<location path="api">
  <system.web>
    <authorization>
      <!-- All anonymous users access to the virtual path api -->
      <allow users="*" />
    </authorization>
  </system.web>
  <!-- Need to include the security overrides else it will inherit from the root of
the application -->
  <system.webServer>
    <handlers>
      <remove name="ExtensionlessUrlHandler-ISAPI-4.0_32bit" />
      <remove name="ExtensionlessUrlHandler-ISAPI-4.0_64bit" />
      <remove name="ExtensionlessUrlHandler-Integrated-4.0" />
```

Configure Integrated Security for Vantagepoint

```

        <add name="ExtensionlessUrlHandler-ISAPI-4.0_32bit" path="*" verb="*"
modules="IsapiModule"
scriptProcessor="%windir%\Microsoft.NET\Framework\v4.0.30319\aspnet_isapi.dll"
preCondition="classicMode, runtimeVersionv4.0, bitness32" responseBufferLimit="0" />

        <add name="ExtensionlessUrlHandler-ISAPI-4.0_64bit" path="*" verb="*"
modules="IsapiModule"
scriptProcessor="%windir%\Microsoft.NET\Framework64\v4.0.30319\aspnet_isapi.dll"
preCondition="classicMode, runtimeVersionv4.0, bitness64" responseBufferLimit="0" />

        <add name="ExtensionlessUrlHandler-Integrated-4.0" path="*" verb="*"
type="System.Web.Handlers.TransferRequestHandler"
preCondition="integratedMode, runtimeVersionv4.0" />
    </handlers>

    <security>

        <authentication>

            <!-- Need to enable anonymous access and turn off Windows
authentication for the virtual path -->

            <anonymousAuthentication enabled="true"/>

            <windowsAuthentication enabled="false"/>

        </authentication>

    </security>
</system.webServer>
</location>

```

Configure Database Session State for Vantagepoint

Session state information is typically stored in memory on the web server in the IIS Application Pool process serving the application (w3wp.exe). Database session state is normally not a consideration unless you will be load balancing multiple front-end Vantagepoint web/application servers and you would like to isolate your user's session information from a failure or error on one web server where their session information may be lost.

Use the Weblink utility to configure Vantagepoint to store session state information in a database. Be aware that Deltek has written our own session state model and does not rely on the ASP.NET session state.

Create the Session State Database (Optional)

If you want to store session state information in the Vantagepoint database, Weblink automatically configures the database table where session state information is stored. However, if you want to store the database table in a database other than your Vantagepoint database, you must create a separate database and login for this purpose.

Configure Vantagepoint for Database Session State

Before you make this change, make sure that you are making it during a maintenance window when no one is logged into Vantagepoint. Changing the session state invalidates all active user sessions.

To configure Vantagepoint for database session state, complete the following steps on the web/application server:

1. On the web/application server, open and log into the Weblink utility, using the Weblink shortcut in the Vantagepoint installation directory.
2. Click the System Settings tab.
3. In the drop-down field, change **Store Session State in Memory** to **Store Session State in SQL Server**.

You will receive a message that switching session state modes will force a restart of ASP.NET and all users will lose their sessions.

4. Click **Yes**.
5. In the **SQL Server** field, enter the name of the database server where the session state database exists.
6. In the **Database Name** field, enter the name of the session state database.
7. If you plan to use Windows Integrated Authentication for the database connection, select the **Windows Authentication** option.

This disables the **SQL Username** and **SQL Password** fields.

Attention: See [Configure Integrated Security for Vantagepoint](#) for details on Windows Integrated Authentication.

8. In the **SQL username** field, enter the SQL Login ID with rights to that database.

9. In the **SQL password** field, enter the password for the SQL Login ID that you entered in the previous step.
10. Click **Test Database Connection** to validate the connection information that you entered.
11. Click **Apply** to save your changes.

A message displays that prompts you to configure this database to store session state information.

12. Click **Yes** to create a table in the database called **FW_SessionState**.

A message displays to tell you that Weblink has successfully configured the server (database) to store the Vantagepoint session state.

To verify that the session state is being stored correctly:

1. Access your database server via a query utility.
2. Log in to Vantagepoint.
3. Run the following query in Query Analyzer to verify that a row has been added to the table. There will be one row for every user logged in.

```
Use <Session State Database>
Go
Select * from FW_SessionState
Go
```

Note: If Vantagepoint is not closed properly, user sessions can be orphaned. A process server job named "Delete Old Sessions" runs every night to remove orphaned user sessions.

Securing Your Vantagepoint Deployment

When you install Vantagepoint, the installation script creates a number of user accounts on the Vantagepoint physical tiers (database, web/application, report, and process server). These user accounts include local Microsoft Windows user accounts and SQL Server Login IDs (for both Windows and Mixed Mode authentication). You also have the option of using domain accounts for all of these service accounts.

To secure your Vantagepoint deployment, you must change these accounts so that they are unique to your firm and do 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 DeltekVantagepoint local account because you will subsequently delete or disable this account on all Vantagepoint servers.

Another option for changing the user account is to run the Vantagepoint installation script with the [SetServiceAccounts](#) switch.

If You Have Multiple Servers

If you have multiple web/application, report, or process 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 DeltekVantagepoint local Windows account is used as all of the following:

- Application Pool Identity
- Reporting Services access account
- Process Server service account
- A 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 **DeltekVantagepoint**. (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 DeltekVantagepointAppPool.

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 Vantagepoint 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 **DeltekVantagepointAppPool**, 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 Vantagepoint database(s).

Attention: See [Database Tier](#) for more information.

11. Change the Process Server service account.

By default, the Process Server service is installed on every web/application server, as well as on any server installed as a Dedicated Process Server.

Attention: See [Process Server Tier](#) for more information.

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

Database Tier

By default, the Database tier installation creates a local Windows user account on the SQL Server named **DeltekVantagepoint**, as well as a SQL Server Login ID, also named **DeltekVantagepoint**. (You can opt to use domain accounts instead.)

SQL Server has two modes of authentication:

- Windows Integrated
- Mixed Mode

If you are unsure which mode of authentication you are using:

1. Launch and log in to the Weblink utility on the Vantagepoint web/application server, using the shortcut created in the Vantagepoint installation folder.
2. If you have not set a password for Weblink, click **Change Password**, and enter a unique password. The password for Weblink is prompted for during setup.

3. Log in to Weblink, and select your database from the **Current Database** drop-down list.
4. Review the information on the General tab to identify your method of SQL authentication.
 - If the **Windows Authentication** check box is selected, then you are using Windows Integrated Authentication.
 - If the **Windows Authentication** check box is cleared and a SQL username and password are entered, then you are using SQL Server or Mixed Mode authentication.

Windows Integrated Authentication

If you are using Windows Integrated Authentication for the SQL Server connection, the local Windows user account is created on the database tier. You need to update the database tier with the new user account that you created for the Vantagepoint Application Pool Identity in the Web/Application Tier section.

Note: See [Configure Integrated Security for Vantagepoint](#) for detailed information on configuring Windows Integrated Security for web/application and database connections.

To update the database tier with the new user account:

1. Select one of the following options:
 - If you are using a domain user account for the IIS Application Pool Identity, add this Domain user to the Local Users (not Administrators) group on the SQL Server.
 - If you are using a local user account as the IIS Application Pool Identity, use the Computer Management utility from Administrative Tools to create a local user on the database server with the same username and password as you used on the web/application server.

Administrative rights to your database server are not necessary for the domain or local user account described above.

2. Create a new Windows login in SQL Server for the domain or local user account that is being used for the IIS Application Pool Identity.
Create the new SQL Login using SQL Server Management Studio from the Security - Logins folder.
3. Grant this new Windows login dbo (database owner) rights to your Vantagepoint database(s).
4. On the web/application server, launch the Weblink utility.
5. Log in to Weblink, and select your database from the **Current Database** drop-down list.
6. If it is not already selected, select the **Windows Authentication** check box.
7. To ensure that the database connection information was updated correctly, click **Test » Database Connection** to validate the connection.
8. Use the **Computer Management** utility under Administrative Tools to delete or disable the local DeltekVantagepoint Windows user account on the database server.
9. Use SQL Server Management Studio to delete or disable the DeltekVantagepoint Windows Login ID from within SQL Server.
Deleting the Windows User Account does not remove it from SQL Server.

Mixed Mode Authentication

If you are using Mixed Mode Authentication for the SQL Server database connection, you must create a unique SQL Server login.

To create the SQL Server login:

1. If you have not already done so, secure the **sa** account with a unique password using SQL Server Management Studio from the Security - Logins folder.
2. Create a unique SQL Server login ID and password using SQL Server Management Studio.
3. Grant the new login **dbo** (database owner) rights to your Vantagepoint database(s) and, if appropriate, the reporting services databases (ReportServer and ReportServerTempDB).
4. If you want to use a different account for report server database access, create a second SQL login in SQL Server Management Studio and manually update the Report Server tab in Weblink with the new connection information.

Be sure to test the connection before saving your changes.

5. Log in to Weblink, and select your database from the **Current Database** drop-down list.
6. On the General tab, enter the new SQL Server login username and password.
7. To ensure that the database connection information was updated correctly, click **Test » Database Connection** to validate the connection.
8. Update the Report Server tab with the new connection information for the report server databases.
9. Use SQL Server Management Studio to delete or disable the DeltekVantagepoint SQL login ID that the installation created on the Database server.

Report Tier

By default, the Report tier installation creates a local Windows user account named DeltekVantagepoint on the report server (SQL Reporting Services server). This Windows user account is also granted System Administrator and Content Manager Rights in SQL Reporting Services. (You can opt to use a domain accounts instead.)

Note: When you created the database tier account, access rights to the report server databases were automatically given to the new user account.

To secure the report tier and customize the report tier account:

1. Select one of the following actions:
 - If you have a Windows Domain, create or have a domain user account created, and use the Computer Management utility under Administrative Tools to add this user to the Local Administrators group on the report server. Click **Computer Management » Local Users and Groups » Administrators**, and add the new Windows account.
 - If you are not using a Windows Domain, you must create a new local Windows user account and add that user to the Local Administrators group.

The next step is to use Report Manager to grant this new account the necessary rights in Reporting Services.

2. Use `http://<report_server>/reports` to open Report Manager, replacing `<report_server>` with the name of your report server.
To access Report Manager, you must have rights to the report server. You may also need to launch Internet Explorer using the **Run as Administrator** option.
3. Click the **Site Settings** link in the upper right corner and add the new account to the Administrators role.
4. Delete the DeltekVantagepoint account from this role.
5. Click the Properties tab or the **Folder Settings** button (depending on your version of SQL Server).
6. Add your new account to the Content Manager role.
7. Delete the DeltekVantagepoint account from that role.
8. Use the Computer Management utility from Administrative Tools to delete or disable the local DeltekVantagepoint Windows user account on the report server.

Process Server Tier

By default, the Process Server tier installation creates a local Windows user account named DeltekVantagepoint on the process server. (You can opt to use a domain accounts instead.) By default, the process server service is installed on every web/application server, as well as on any server installed as a dedicated process server. Therefore, you should perform the following steps on every web/application server as well as on every dedicated process server.

In this procedure, you change the Process Server Service Account (a Windows account on the process server tier).

To secure the Process Server tier and customize the Process Server service:

1. Select one of the following actions:
 - If you have a Windows Domain, create or have a domain user account created. Use the Computer Management utility under Administrative Tools to add this user to the Local Administrators group on the Report server. Click **Computer Management » Local Users and Groups » Administrators**, and add the new Windows account.
 - If you are not using a Windows Domain, you need to create a new local Windows user account and add that user to the Local Administrators group.
2. To change the service to run your new account, click **Start » Control Panel » Administrative Tools » Services**, and locate the Deltek Vantagepoint process server service.
3. Update the **Log On As** column to reflect the new user information that you created above.
4. Use the Computer Management utility from Administrative Tools to delete or disable the local DeltekVantagepoint Windows user account on the process server.

Configure Reporting Services Logging

You can debug Reporting Services issues using two different kinds of Reporting Services logging:

- Trace logging, which provides detailed logging of errors or warnings seen in the Reporting Services logs.
- HTTP logging, which helps identify HTTP- and authentication- related issues in Report Manager or the Report Server web service.

Consider enabling and configuring this logging.

Attention: For more information, see the article [Reporting Services Log Files and Sources](#).

Enable Reporting Services Trace Logging

To configure trace logging:

1. Stop the Reporting Services service.
2. Modify the ReportServer\bin\ReportServerService.exe.config file.
See the details in the [Changes to the ReportServer\bin\ReportServerService.exe.config File](#) section.
3. Restart the Reporting Services service.

Attention: For more information, see the article: [Report Server Service Trace Log](#).

Rules for Tracing

You can enable tracing for the components listed below. These are the trace level rules, as defined in the ReportServerService.exe.config file:

- If a trace level is defined for the specific component in RSTrace/Components, then that setting takes precedence.
- If a trace level is defined for all components (for example, **all:3**) then that level is used.
- If neither level is defined, the default trace level (labeled DefaultTraceSwitch) defined in system.diagnostics/switches is used.

Components that Can Be Traced Library

- | | | |
|---------------------|--------------------|-------------------|
| ▪ ConfigManager | ▪ WebServer | ▪ NtService |
| ▪ Session | ▪ BufferedResponse | ▪ RunningRequests |
| ▪ DbPolling | ▪ Notification | ▪ Provider |
| ▪ Schedule | ▪ Subscription | ▪ Security |
| ▪ ServiceController | ▪ DbCleanup | ▪ Cache |

- | | | |
|--------------------------|-----------------------|---------------------|
| ▪ Chunks | ▪ ExtensionFactory | ▪ RunningJobs |
| ▪ Processing | ▪ ReportRendering | ▪ HtmlViewer |
| ▪ DataExtension | ▪ EmailExtension | ▪ ImageRenderer |
| ▪ ExcelRenderrer | ▪ PreviewServer | ▪ ResourceUtilities |
| ▪ ReportPreview | ▪ UI | ▪ Crypto |
| ▪ SemanticModelGenerator | ▪ SemanticQueryEngine | ▪ AppDomainManager |
| ▪ HttpRuntime | | |

Changes to the ReportServer\bin\ReportServerService.exe.config File

Make the highlighted modifications to the ReportServer\bin\ReportServerService.exe.config file:

```
<configuration>
  <configSections>
    <section name="RSTrace"
type="Microsoft.ReportingServices.Diagnostics.RSTraceSectionHandler,Microsoft.Reportin
gServices.Diagnostics" />
  </configSections>
  <system.diagnostics>
    <switches>
      <add name="DefaultTraceSwitch" value="3" />
    </switches>
  </system.diagnostics>
  <RSTrace>
    <add name="FileName" value="ReportServerService_" />
    <add name="FileSizeLimitMb" value="32" />
    <add name="KeepFilesForDays" value="14" />
    <add name="Prefix" value="tid, time" />
    <add name="TraceListeners" value="debugwindow, file" />
    <add name="TraceFileMode" value="unique" />
    <add name="HttpTraceFileName" value="ReportServerService_HTTP_" />
    <add name="HttpTraceSwitches" value="date,time,
clientip,username,serverip,serverport,host,method,uristem,uriquery,protocolstatus,byte
sreceived,timetaken,protocolversion,useragent,cookiereceived,cookiesent,referrer" />
    <add name="Components"
value="all:3,http:3,Library:4,EmailExtension:4,Subscription:4,Schedule:4,Notification:
4,DbPolling:4,NtService:4" />
  </RSTrace>
```

Errors in the Reporting Services Log File

Errors appear in the reporting services log file as shown below:

```
session!ReportServer_0-1!e10!09/11/2011-13:14:51:: i INFO: LoadSnapshot: Item with session:
pvon0l55nrycom3uczjnho45, reportPath: , userName: KL\deltekadmin not found in the database

library!ReportServer_0-1!e10!09/11/2011-13:14:51:: e ERROR: Throwing
Microsoft.ReportingServices.Diagnostics.Utilities.ExecutionNotFoundException: Execution
'pvon0l55nrycom3uczjnho45' cannot be found, ;

Info: Microsoft.ReportingServices.Diagnostics.Utilities.ExecutionNotFoundException: Execution
'pvon0l55nrycom3uczjnho45' cannot be found
```

Each log entry begins with the sections (or components) that can be traced, followed by an exclamation point. For example, if you want verbose logging for the errors shown above, enable library and session verbose logging as follows:

```
<add name="Components" value="all:3,Library:4,Session:4" />
```

Enable Reporting Services HTTP Logging

The Reporting Services service runs its own http.sys listener to accept standard HTTP/HTTPS requests on standard HTTP ports (80/443). Unlike Internet Information Services, HTTP logging is not enabled by default, but can be enabled following the steps in the article [Report Server HTTP Log](#).

You can also use [Telerik Fiddler](#) to trace the HTTP requests from client to report server for help troubleshooting HTTP and authentication issues.

Configure an Alternate Database for Vantagepoint Reporting

When you use Vantagepoint reporting, your SQL Server database engine must handle two different workloads: transactional and reporting. These workloads demand tremendous resources from your SQL Server. One remedy is to offload the reporting workload to a different SQL Server, where you have a copy of your Vantagepoint database.

These reports use the alternate database:

- Dashboard reports
- Reports in the Reporting menu applications (excepting the Purchasing reports)

They use the alternate database whether they are previewed, directly printed, emailed, run via the process server, or processed in another way.

All other reports, including posting logs, billing (interactive and batch) reports, and timesheet and expense reports continue to run their queries against the Vantagepoint transaction database.

Note: Visualization reports do not use SQL Reporting Services and are not affected by this feature.

Alternate Database for Reporting

To set up an alternate database, configure a copy of your Vantagepoint database for access. Then configure the connection string information in Weblink on the Report Server tab in the Alternate Database for Reporting section. The primary benefit of using the Alternate Database for Reporting configuration in Weblink is that it can be used with any version or edition of SQL Server.

Note: With SQL Express, the Alternate Database for Reporting must be located on the same SQL Express instance as the transaction database. This is a limitation of SQL Express because Reporting Services for SQL Express can only use local databases.

Consider the following:

- Find an appropriate method to create a copy of the database on the second SQL Server (for example, transactional replication, log shipping, database backup/restore, or third party tools that support SQL Server snapshot backup).

Note: Deltek has not completed testing and does not provide support for the underlying database copy/synchronization methodology that you choose.

- Ensure that the database copy used for reporting is kept in sync with the transaction database. Not keeping the databases in sync will result in stale data for reporting purposes.
- Ensure that the SQL login used for authentication has read-only access to the database.

Configure an Alternate Database for Vantagepoint Reporting

This Microsoft documentation will help you choose an appropriate database replication/synchronization methodology:

- Transactional replication:

[SQL Server Replication](#)

Note: Vantagepoint uses the SET CONTEXT_INFO stored procedure, which is known to cause issues during the replication of objects that require schema changes on the replicated database (See the article [Make Schema Changes on Publication Databases.](#)) Fortunately, in Vantagepoint, this issue appears limited to the replication of custom user defined fields. To work around this issue, you can set up an internal process to identify and manually replicate these objects before they are put into production use.

- Log shipping:

[About Log Shipping \(SQL Server\)](#)

- Backup/restore:

[Back Up and Restore of SQL Server Databases](#)

- Third party tools that support snapshot backups:

[Snapshot Backups](#)

Note: SQL Server Database Mirroring is not supported for the Alternate Database for Reporting functionality because the mirrored database is not accessible for read-only queries.

Also, Database Mirroring does not support SQL Server FILESTREAM, which is required for Vantagepoint Transaction Document Management (TDM).

Configure the Alternate Database for Reporting in WebLink

To configure an alternate database for reporting:

1. Create a copy of your Vantagepoint transaction database on a second SQL Server.
For testing purposes, perform a backup/restore.
2. Identify and implement a methodology to ensure that data is synchronized between the databases within a timeframe differential suitable to your business needs.
3. Create a login that has read-only rights to the alternate database.
This can be accomplished by granting db_datareader rights, rather than db_owner rights, to the SQL Server login that is used for the alternate database.
4. Launch the Vantagepoint Weblink utility and select the Vantagepoint transaction database entry that you will configure as an alternate reporting database.
5. Click the Report Server tab.
6. Select the **Use Alternate Database for Reporting** option and click **OK**.
Vantagepoint displays a reminder message.
7. Click **OK** to continue.

8. Enter the connection string information for the alternate database:


Field	Description
Server Name	Enter the name of the SQL Server hosting the alternate database.
Database name	Enter the name of the alternate database.
Windows Authentication	Select this check box if you are using Windows Integrated Authentication for the database connection. The identity of the DeltekVantagepointAppPool will need read-only rights to the alternate database.
Database Username/Password	If you are not using Windows Integrated Authentication, enter the SQL server login with read-only rights to the alternate database.

9. From the Weblink menu, click **Test » Alternate Database for Reporting** to validate the connection.

Identify the Connection String Used in a Report

After configuring the Alternate Database for Reporting option, validate that reports are running against the correct database.

To acquire the connection string by previewing the report:

1. Click the construction hat icon  on the Reporting toolbar. If you don't see the icon, maximize the report.
2. From the **View Report Information** drop-down list, select **Report Data Source**.
3. Click the **View** button.
You will be prompted to **Open** or **Save** the XML file.
4. Click **Open**, and the file will open using the application configured to open XML files. On most computers, that will be your default browser.
5. Review the `ConnectionString` element for the following attributes:
 - **Data Source:** This is either the database server specified in the Alternate Database for Reporting configuration or, if you use Availability Groups, the Availability Group Listener.
 - **Initial Catalog:** This is either the database name specified for the Alternate Database for Reporting configuration or, if you use Availability Groups, the Vantagepoint database name.
 - **ApplicationIntent=ReadOnly:** This only displays when you use Availability Groups and if the report was run against the Read Only reporting database.
 - **MultiSubnetFailover:** This only displays when you use Availability Groups.

Configure Basic Availability Groups Using Microsoft SQL Server Standard Edition

Vantagepoint supports the use of Microsoft SQL Server AlwaysOn Basic Availability Groups if you have SQL Server 2016 or a later version.

- A SQL Server Basic Availability Group provides a high availability solution for databases hosted on SQL Server Standard Edition.
- Basic Availability Groups support failover for a single database.
- Multiple Basic Availability Groups are supported in the same server configuration, which provides failover support for multiple databases on the same server.

Differences in SQL Server Standard and Enterprise Features

You can use Availability Groups with SQL Server Standard Edition or Enterprise Edition, but features will vary:

SQL Server Edition	Features	See installation steps here:
SQL Server Standard Edition	<ul style="list-style-type: none"> ▪ Basic Availability Groups ▪ Multi-subnet Failover 	This section
SQL Server Enterprise Edition	<ul style="list-style-type: none"> ▪ Availability Groups ▪ Readable Secondary Replicas ▪ Read Only Routing ▪ Multi-subnet Failover 	Configure Availability Groups Using Microsoft SQL Server Enterprise Edition

Attention: This section focuses specifically on the SQL Server Basic Availability Group features supported by Vantagepoint. For more information on the limitations of Basic Availability Groups, see these articles:

- [Basic Availability Groups \(Always On Availability Groups\)](#)
- [Editions and supported features of SQL Server 2016](#)

Attention: Deltek Vantagepoint utilizes SQL Server Change Data Capture (CDC) as the method for auditing. See SQL Server Availability Groups for important information to ensure that database auditing continues in the event of a failover of the Availability Group to a read-only replica.

Prerequisites

See the MSDN documentation for prerequisites, restrictions, and recommendations for AlwaysOn Availability Groups:

[Prereqs, Restrictions, Recommendations - Always On Availability Groups](#)

Specific prerequisites for Basic Availability Groups with Vantagepoint are:

- Standard Edition of SQL Server 2016
- A maximum of two SQL Server Standard Edition nodes
- Standard Edition of Windows Server 2012 or later. (The specific operating system feature that is required to support Availability Groups is Windows Server Failover Clustering.)

Note: If you are using Transaction Document Management (which uses SQL Server FILESTREAM) and Windows Server 2012 Failover Clustering, you may need to install the following Microsoft hotfix:

[Can't access VNN FILESTREAM share when you use the FILESTREAM and FileTable features on a Windows Server 2012-based failover cluster](#)

- A Windows file share on a server other than the SQL Servers to which the SQL service accounts have write access. This is required to configure Availability Groups.
- Windows Server Failover Cluster feature, installed and configured

Multi-subnet Failover

The Multi-subnet Clustering feature provides failover support when the primary and secondary replicas of the Availability Groups are on different network subnets.

If your WSFC (and SQL Server Availability Group Listener) are configured so that your WSFC nodes are on different network subnets, multi-subnet failover support is automatically enabled.

The **MultisubnetFailover=True** option is automatically added to the connection string.

Attention: For more information, see the following articles:

- [Listeners, Client Connectivity, Application Failover](#)
- [Create or Configure an Availability Group Listener \(SQL Server\)](#)

Install and Configure Windows Server Failover Cluster (WSFC)

The WSFC will cluster applications and services. Your specific configuration depends on your intended use of SQL Server Availability Groups. For example, you may want to use a SQL Server Failover Cluster Instance (FCI) in addition to using Availability Groups. One of the primary differences in the cluster configuration of an FCI versus an Availability Group is the need to provide shared storage.

Attention: See the Microsoft documentation for in-depth details about configuring Windows Server Failover Clustering for your intended use.

When you configure Windows Server Failover Cluster:

- A cluster virtual network is created. You will need an IP address and DNS name for the cluster and server names for the nodes that will be members of the cluster.
- No shared storage is needed, so you can deselect the option to add available storage.
- A static IP or DHCP can be used for the cluster network. A static IP should be used for production environments.

- A DNS name is created automatically, or you can create a DNS entry before configuring the cluster.
- You will need domain rights because the process creates a computer account in the domain for the cluster virtual network.
- Two virtual networks are created, one for the Windows Server Failover Cluster and one for the Availability Group listener. Use a unique name for the cluster, one which is not SQL-specific but will be easily identifiable as the Windows cluster.
- When Vantagepoint connects to the SQL Server, it will not connect to the WSFC name but will connect to the Availability Group Listener (created later). The WSFC is enabled for the failover functionality of Availability Groups.

Use the following procedures to install and configure Windows Server Failover Clustering.

Note: Depending on your operating system, the steps in these procedures may vary slightly. The procedures in this section are based on Windows Server 2012 Standard Edition. See this article: [Windows Server Failover Clustering with SQL Server](#).

Install the Failover Clustering Feature

To install the failover clustering feature:

1. Open the Server Manager utility.
2. Access the **Local Server** and scroll down to **Roles and Features**.
3. From the **Tasks** drop-down list, select **Add Roles and Features**.
4. In the Add Roles and Features wizard, click **Next** until you get to the Select Features page.
5. Select the **Failover Clustering** option.
6. If prompted, click **OK** to install any dependent features.
7. Complete the wizard to perform the installation.
8. If prompted, reboot the server.

Configure Failover Clustering using Failover Cluster Manager

To configure the Failover Clustering feature:

1. From Administrative Tools, open the Failover Cluster Manager.
2. Under **Management**, click **Create Cluster**. The Create Cluster Wizard will guide you through the process.
3. On the Select Servers page of the wizard, browse to or enter the names of the servers that will be part of the cluster.
4. On the Validation Warning page, select **Yes** to run the Cluster Validation tests, and then click **Next**.

This process creates a report that identifies any problems that need to be addressed before you create the cluster.
5. When the validation is completed, provide a name for the cluster in the **Cluster Name** field.
6. Click **Next** to create the cluster.

7. If you are configuring a WSFC that does not require shared storage, clear the **Add all eligible storage to the cluster** option.

Install SQL Server on Each Cluster Node

After configuring the WSFC, you must perform the SQL Server installation on each node in the cluster.

After installing SQL Server on all nodes in the cluster, restore your Vantagepoint transaction and FileStream databases and configure the SQL Reporting Services databases (ReportServer and ReportServerTempDB) on the Primary node in the cluster.

Installation Requirements and Notes

- If you are only configuring Availability Groups (not a Failover Cluster Instance), you must perform a New SQL Server stand-alone installation, not a New SQL Server failover cluster installation, on each node.
- Shared storage is a requirement of Availability Groups only if they are installed in a SQL Cluster. The prerequisite check will fail if you choose a SQL Server Cluster installation and do not provide shared storage.
- Only the SQL database engine can use Basic Availability Groups. Even though the Availability Groups use a WSFC, this does not constitute a true cluster and will not provide fault tolerance for other SQL Server services (Analysis Services or Reporting Services).
- To be fault tolerant, Analysis Services must be part of an actual Failover Cluster Instance (FCI) where SQL is installed using a new SQL Server failover cluster installation.
- You can use an FCI with an Availability Group to enhance the availability of an availability replica. However, to prevent potential race conditions in the WSFC cluster, automatic failover of the Availability Group is not supported to or from an availability replica that is hosted on an FCI.
- Reporting Services use a scale-out deployment, which is not a cluster.
- You can use the same or different service accounts on each node, but all accounts must have rights to the file share described in the Prerequisites section above.
- FileStream functionality can be used with Availability Groups and will require that FileStream be enabled on both failover nodes.

Attention: For more information, see [FILESTREAM and FileTable with Always On Availability Groups \(SQL Server\)](#).

You may also need this Microsoft hotfix:

[Can't access VNN FILESTREAM share when you use the FILESTREAM and FileTable features on a Windows Server 2012-based failover cluster](#)

- Although this is not a requirement, you should consider performing the exact same SQL Server installation on each node, including the same installation, configuration, and instance name.
 - For proper failover support, the failover nodes should have comparable hardware resources.
- See the MSDN documentation for prerequisites, restrictions, and recommendations for AlwaysOn Availability Groups:

[Prereqs, Restrictions, Recommendations - Always On Availability Groups](#)

Configure Database Login

For the Vantagepoint and Reporting Services databases that are part of an Availability Group to be immediately available in the event of an Availability Group failover, you must complete these steps on **both** failover nodes. The following rights must be granted to the login used to access the Vantagepoint and Reporting Services databases that are part of the Availability Group:

Permission	Required for:
Dbo = Database Owner rights to all databases in the Availability Group	All databases in the Availability Group
View Any Definition	Availability Groups
View Server State	Availability Groups

When you back up and restore a database to another server, the login on the first server has a different SID (Security Identifier) than the same login on the second server. This issue is typically resolved using the `sp_change_users_login` stored procedure. However, since the database on the secondary replica will be in read-only mode, you cannot fix the login.

You can resolve this issue by using the `sp_help_revlogin` stored procedure, described in this article:

[How to transfer logins and passwords between instances of SQL Server](#)

Once the procedure is created in the master database, execute it to get:

- The list of SQL Logins with their associated SIDs.
- The CREATE statement needed to create the login on the Secondary replicas.

Here is an example:

```
CREATE LOGIN [DeltekVantagepoint] WITH PASSWORD =
0x0200E0E05D60876CCE39BD9209515FB63C5589D6C939F3AB56A6CE9DBFBF49A9410F66F098408
27135F800725E25A77714FDFA31FB6C18BCB46561217947C3749F0380A18AF5 HASHED, SID =
0x0124F12258D9BD49BE649C2D7A6DA838, DEFAULT_DATABASE = [master], CHECK_POLICY =
OFF, CHECK_EXPIRATION = OFF
```

Prior to configuring the Availability Groups, run the CREATE statement(s) created from executing the `sp_help_revlogin` on your server on all secondary replicas.

Create Availability Groups

You must enable Availability Groups and create an Availability Group on the primary node.

To enable Availability Groups:

1. Open the SQL Server Configuration Manager.
2. Right-click the SQL Server service and click **Properties**.
3. On the AlwaysOn High Availability tab, select the option to enable the Availability Groups for each node.
4. Restart the SQL Server service.
5. Repeat steps 1-4 on all nodes that will be part of the Availability Group.

To create an Availability Group:

1. For each database that requires failover support, put the database in FULL recovery mode and make a FULL database backup.

A Basic Availability Group can only handle failover for a single database, so you will need to create an Availability Group for each database that requires failover support.

In a typical Vantagepoint deployment you will have at least three databases: Vantagepoint, ReportServer, and ReportServerTempDB. Other possible databases include the Transaction Document Management (FileStream) database.

Attention: For more information on performing backups and restores of databases in FULL recovery mode, see the article:

[Back Up and Restore of SQL Server Databases](#)

2. In SQL Server Management Studio, start the Availability Group Wizard.
3. Expand **AlwaysOn High Availability**, right-click **Availability Groups**, and click **New Availability Group Wizard** on the shortcut menu.
4. Select a name for the Availability Group.

Because each database will be in its own Availability Group, you will need a separate Availability Group for each database. The name should describe the database that the Availability Group includes (for example, DeltekVantagepointAG).

5. Select the **Database Level Health Detection** option.

This undocumented option controls whether the entire Availability Group fails over if one database becomes suspect. Because Basic Availability Groups contain only one database, this setting is not directly applicable, but Deltek recommends selecting it anyway. This feature is only available in SQL Server 2016.

6. Select the database to be included in the Availability Group, and click **Next**.

The wizard will tell you whether or not the database meets requirements (for example, the database is in FULL recovery mode and you have made a FULL database backup).

7. On the Replicas tab, specify the Availability Group configuration (nodes, failover mode, and synchronization mode).

Attention: See this article for more information on failover and failover modes:
[Failover and Failover Modes \(Always On Availability Groups\)](#).

8. For Basic Availability Groups, use the **Add Replica** button on this tab to add the second node.
9. Select settings, referring to this table, and click **Next**.

Setting	Description
Server Instance	A maximum of two servers is allowed.
Initial Role	Select the role of the server (Primary or Secondary).
Automatic Failover	Check this option for failover to occur automatically. Otherwise, failover will be a manual process.
Synchronous Commit / Asynchronous Commit	<p>This option controls how transactions are committed, which has an impact on the performance of the synchronization and how much data may be lost in the event of a failure. Select one of these options:</p> <ul style="list-style-type: none"> ▪ Synchronous Commit: Each transaction must be committed to both Node 1 and Node 2 before the transaction is considered complete. This option reduces the possibility of data loss, but at the expense of performance. ▪ Asynchronous Commit: Each transaction is committed to Node 1. The transaction is also sent to Node 2 but there is no verification if it is or is not committed. This option performs better, but with the chance of data loss.
Readable Secondary	Select No because this setting does not apply to Basic Availability Groups, which do not allow connections to secondary replicas.

10. Check the information on the Endpoints tab.
 The Endpoint for each instance is created automatically.
11. Check the information on the Backup Preferences tab.
 Backup Preferences determine whether or not backups can be made from replicas other than the primary replica. This tab is grayed out because this feature is not available in Basic Availability Groups.
12. Click the Listener tab, where you create the Availability Group Listener.
 Only one listener is required, regardless of the number of Basic Availability Groups configured, unless your replicas are on different subnets.
13. Create a listener for the first Availability Group created, but not for subsequent Availability Groups.

14. From the **Network Mode** drop-down list, select the type of listener: **Static IP** or **DHCP**.

The port will be the same as the one used by the SQL Server port (the default is 1433).

Note: If you are using multiple subnets, click the **Add** button to add the IP address for the listener on all subnets. This option is available only if you are using Static IP addresses. See this article for more information:

[Add IP Address Dialog Box \(SQL Server Management Studio\)](#)

15. Click **Next**.
16. On the Data Synchronization Preference tab, enter the shared path or use the **Browse** button to select the location that all nodes/SQL service accounts can access.

This action determines how the databases synchronize to the replica.

17. Repeat these steps (except step 12) for all applicable databases in your Vantagepoint deployment.

For example, if your SQL Server will host the Vantagepoint transactional database, a FileStream (TDM) database, and the report server and ReportServerTempDB databases, you will have four Availability Groups, one for each database.

Configure Vantagepoint and Reporting Services to Use Availability Group Listener

Next, configure Vantagepoint and Reporting Services to use the Availability Group Listener that you configured above:

- Use the Weblink utility to configure your Vantagepoint database, Report Server database, and FileStream database to use the Availability Group Listener.
- Use the Report Server Configuration Tool to configure Reporting Services to use the Availability Group Listener.

Note: If you do not configure the applications to use the Availability Group Listener, your users will experience connection errors in the event of a server or database level failure.

Configure Vantagepoint to Use the Availability Group Listener

To configure Vantagepoint to use the Availability Group Listener:

1. Launch the Weblink utility and select or add the Vantagepoint transaction database that is part of the Availability Group.
2. On the General tab, enter (or change) the Availability Group Listener name in the **SQL Server** field.
3. In the **Database Name** field, enter the name of the Vantagepoint transaction database.
4. Enter the SQL Server Login ID and password for the login that has been granted the necessary SQL Server rights to the Availability Group database.

Attention: See the [Configure Database Login](#) section for more information.

If you see the **Use Availability Groups** check box, but it is not enabled, see if the **Use Alternate Database for Reporting** option is selected on the Report Server tab. You cannot use both the **Use Availability Groups** and **Use Alternate Database for Reporting** features because they provide the same functionality but are designed for different versions of SQL Server.

Note: Although you are modifying the server connection information for the Vantagepoint database, the Vantagepoint FILESTREAM database (if applicable), and the Reporting Services database to use the Availability Group listener, this action only ensures that these databases can still connect to the new primary node in the event of a failover.

5. Select the **Use Availability Groups** check box.

At this point a query is issued to identify the edition of SQL Server in use and the name of the Availability Group for the database. If this check returns **Standard**, the label of the check box will change to **Use Basic Availability Groups**. Selecting this option does not impact the failover functionality; it is just a visual identifier that Availability Groups are in use.

6. If you are using FileStream and the FileStream database is part of an Availability Group on the same server (which it should be if the database is on the same SQL Server as Vantagepoint), confirm that the FileStream SQL Server is using the Availability Group Listener name.

If it is not, change the listener name to the Availability Group Listener name.

7. On the Report Server tab, confirm that the **Server Name** specified in the Report Server Database Access section is using the Availability Group Listener name.

If it is not, change the listener name to the Availability Group Listener name.

Configure Reporting Services to Use the Availability Group Listener

If Reporting Services has not yet been configured, follow the steps in the [Microsoft SQL Server Reporting Services](#) section to configure Reporting Services. Remember to create and add Availability Groups for both the ReportServer and ReportServerTempDB databases. When you enter the database server name to use for the report server databases, use the Availability Group Listener.

If Reporting Services is already configured to use the primary node server name, follow these steps to configure Reporting Services to use the Availability Group Listener:

1. Open the Reporting Services Configuration Manager.
2. Select the Database menu.
3. Click the **Change Database** button.
4. Select the **Choose an existing report server database** option and click **Next**.
5. On the Connect to the Database Server screen, change the **Server Name** to be the Availability Group Listener and click **Next**.
6. Select the existing ReportServer database from the drop-down list and click **Next** to complete the configuration.

Flexible Failover Policy

The Failover Policy controls the Failover feature of Availability Groups. For more information on this feature, see this article:

[Flexible Failover Policy for Automatic Failover of an Availability Group \(SQL Server\)](#)

Failover Condition Level and Health Check Timeout

Transact-SQL Value	Level	Automatic Failover Initiated On...
1	One	Server down. The SQL Server service stops because of a failover or restart.
2	Two	Server unresponsive. Any condition of lower value is satisfied, the SQL Server service is connected to the cluster and the health check timeout threshold is exceeded, or the current primary replica is in a failed state.
3	Three	Critical server error. Any condition of lower value is satisfied or an internal critical server error occurs. This is the default level.
4	Four	Moderate server error. Any condition of lower value is satisfied or a moderate server error occurs.
5	Five	Any qualified failure conditions. Any condition of lower value is satisfied or a qualifying failure condition occurs.

The failover condition is determined by WSFC executing sp_server_diagnostics at regular intervals.

The following query identifies the existing Failover Policy:

```
select name,failure_condition_level,health_check_timeout from sys.availability_groups
```

Query Result:

name	failure_condition_level	health_check_timeout
<AG_NAME>	3	30000

The following statements configure the Failover Policy for this configuration:

```
ALTER AVAILABILITY GROUP <AG_NAME> SET (FAILURE_CONDITION_LEVEL = 1); //default is 3
ALTER AVAILABILITY GROUP <AG_NAME> SET (HEALTH_CHECK_TIMEOUT = 60000); //default is 30000
```

Monitoring Availability Groups

The following tools are available for monitoring the status of an Availability Group:

- Availability Group Dashboard
- System and Dynamic Management Views (DMVs)
- System Monitor (PerfMon)
- Windows PowerShell

Availability Group Dashboard

To display the Availability Group Dashboard:

1. Launch SQL Server Management Studio and connect to the primary replica.
2. Right-click the **Availability Group** folder and click **Show Dashboard** on the shortcut menu.

System and Dynamic Management Views (DMVs)

The following MSDN article provides a variety of System Views and DMVs that can be used to monitor the health and status of WSFC and Availability Groups:

[Monitor Availability Groups \(Transact-SQL\)](#)

System Monitor (PerfMon)

A variety of System Monitor counters can be used to monitor the performance of Availability Groups. See this article for more information on the available counters and how to use them:

[Monitoring of Availability Groups \(SQL Server\)](#)

Windows PowerShell

These links are to a four-part MSDN series on using PowerShell to monitor Availability Groups:

- [Part 1 – Basic Cmdlet Overview](#)
- [Part 2 – Advanced Usage of AlwaysOn Health Cmdlets](#)
- [Part 3 – A Simple Monitoring Application for AlwaysOn](#)
- [Part 4 – Scheduling and Notification with SQL Agent](#)

Troubleshooting

Use Availability Groups Check Box Does Not Display

If the **Use Availability Groups** check box does not display for your Vantagepoint database when selected in Weblink, execute the following query to see if it returns anything:

```
SELECT e.name, s.database_name
FROM sys.availability_groups_cluster AS e
INNER JOIN sys.availability_databases_cluster AS s
ON e.group_id = s.group_id
```

The query should return a result set showing the name of the Availability Group and each database included in the Availability Group.

System Health Check

When you use Availability Groups, a system health check query is run to determine the health of the Availability Group. If the result of this query returns 0 or 1, the system will fall back to running all reports against the primary replica and Read Only Routing will be effectively disabled. The health check query is:

```
select synchronization_health from sys.dm_hadr_availability_group_states
```

Synchronization Health Values

Value	Description
0	Not healthy. None of the availability replicas have a healthy synchronization_health (2 = HEALTHY).
1	Partially healthy. The synchronization health of some, but not all, availability replicas is healthy.
2	Healthy. The synchronization health of every availability replica is healthy.

Framework Exception: The User Does Not Have Permission to Perform this Action

The following error displays if the SQL login used for the Vantagepoint database does not have View Definition or View Server State permissions.

FrameworkException:

The user does not have permission to perform this action.

Call Stack:

```
{\b Query: }
select synchronization_health from sys.dm_hadr_availability_group_states
```

Attention: For more information, see the [Configure Database Login](#) section.

Solution:

Grant View Definition and View Server State permissions to the SQL Login.

Configure Availability Groups Using Microsoft SQL Server Enterprise Edition

Vantagepoint supports the use of Microsoft SQL Server AlwaysOn Availability Groups. The Enterprise Edition of SQL Server Availability Groups provides an all-inclusive high availability and disaster recovery solution for SQL Server databases.

Differences in SQL Server Standard and Enterprise Features

You can use Availability Groups with SQL Server Standard Edition or Enterprise Edition, but features will vary:

SQL Server Edition	Features	See installation steps here:
SQL Server Standard Edition	<ul style="list-style-type: none"> Basic Availability Groups Multi-subnet Failover 	Configure Basic Availability Groups Using Microsoft SQL Server Standard Edition
SQL Server Enterprise Edition	<ul style="list-style-type: none"> Availability Groups Readable Secondary Replicas Read Only Routing Multi-subnet Failover 	This section

Attention: Deltek Vantagepoint utilizes SQL Server Change Data Capture (CDC) as the method for auditing. See [SQL Server Availability Groups](#) for important information to ensure that database auditing continues in the event of a failover of the Availability Group to a read-only replica.

More Information

This section focuses specifically on the SQL Server Availability Group features supported by Vantagepoint. For information about other SQL Server Availability Group features, see these articles:

- [Overview of Always On Availability Groups \(SQL Server\)](#)
- [Editions and supported features of SQL Server 2016](#)

These guides provide valuable information about solution design:

- [AlwaysOn Architecture Guides](#)

SQL Server 2016 introduced a number of significant enhancements to the Enterprise Edition of Availability Groups (in addition to the Basic Availability Group feature added to Standard Edition). See the following article:

- [Enhanced Always On Availability Groups in SQL Server 2016](#)

Prerequisites

See the MSDN documentation for prerequisites, restrictions, and recommendations for AlwaysOn Availability Groups:

- [Prereqs, Restrictions, Recommendations - Always On Availability Groups](#)

Specific prerequisites for Vantagepoint are:

- Enterprise Edition of SQL Server 2012 or higher
- At least two SQL Server server nodes
- Standard Edition of Windows Server 2012 or later. The specific operating system feature that is required to support Availability Groups is Windows Server Failover Clustering.

Note: If you are using Transaction Document Management (which uses SQL Server FILESTREAM) and Windows Server 2012 Failover Clustering, you may need to install the following Microsoft hotfix:

[Can't access VNN FILESTREAM share when you use the FILESTREAM and FileTable features on a Windows Server 2012-based failover cluster](#)

- A Windows file share on a server other than the SQL Servers to which the SQL service accounts have write access. This is required to configure Availability Groups.

Installation Overview

These are the primary installation steps, described in more detail in the sections that follow:

1. Use Server Manager to install the following features on all nodes:
 - Failover Clustering
 - Failover Clustering Tools (part of Remote Administration Tools)
 - .NET Framework 4.5.2
2. Create a file share on a different server that the SQL Server service account(s) will have full control rights to.

Create the Windows Server Failover Cluster (WSFC)

The WSFC clusters applications and services. Your specific configuration depends on your intended use of SQL Server Availability Groups. For example, you may want to use a SQL Server Failover Cluster Instance (FCI) in addition to using Availability Groups. One of the primary differences in the cluster configuration of an FCI versus an Availability Group is the need to provide shared storage.

Attention: See Microsoft documentation for in-depth details about configuring Windows Server Failover Clustering.

When you configure Windows Server Failover Cluster:

- A cluster virtual network is created. You will need an IP address and DNS name for the cluster and server names for the nodes that will be members of the cluster.
- No shared storage is needed, so you can clear the check box to add available storage.

- A static IP or DHCP can be used for the cluster network. Use a static IP for production environments.
- A DNS name is created automatically, or you can create a DNS entry before configuring the cluster.
- You will need domain rights because the process creates a computer account in the domain for the cluster virtual network.
- Two virtual networks are created, one for the Windows Server Failover Cluster and one for the Availability Group listener. Use a unique name for the cluster, one which is not SQL-specific but which will be easily identifiable as the Windows cluster.
- When Vantagepoint connects to the SQL Server, it will not connect to the WSFC name. It will connect to the Availability Group Listener (created later). The WSFC is enabled for the failover functionality of Availability Groups.

Multi-subnet Clustering

The Multi-subnet Clustering feature provides failover support when the Primary and Secondary replicas of the Availability Groups are on different network subnets.

If your WSFC (and SQL Server Availability Group Listener) are configured so that your WSFC nodes are on different network subnets, Multi-subnet Failover support is automatically turned on.

The **MultisubnetFailover=True** option is automatically added to the connection string.

Attention: See the following articles for more information:

- [Availability Group Listeners, Client Connectivity, and Application Failover \(SQL Server\)](#)
- [Create or Configure an Availability Group Listener \(SQL Server\)](#)

Install and Configure WSFC

Use the following procedures to install and configure Windows Server Failover Clustering.

Depending on your operating system, the steps in these procedures may vary slightly. The procedures in this section are based on Windows Server 2012 Standard Edition.

Install the Failover Clustering Feature

To install the failover clustering feature:

1. Open the Server Manager utility.
2. Access the **Local Server**, and scroll down to **Roles and Features**.
3. From the **Tasks** drop-down list, select **Add Roles and Features**.
4. In the Add Roles and Features wizard, click **Next** until you get to the Select Features page.
5. Select the **Failover Clustering** option.
6. If prompted, click **OK** to install any dependent features.
7. Complete the wizard to perform the installation.
8. If prompted, reboot the server.

Configure Failover Clustering using Failover Cluster Manager

To configure the failover clustering feature:

1. From Administrative Tools, open the Failover Cluster Manager.
2. Under **Management**, click **Create Cluster**.
The Create Cluster Wizard will guide you through the process.
3. On the Select Servers page of the wizard, browse to or enter the names of the servers that will be part of the cluster.
4. On the Validation Warning page, select **Yes** to run the Cluster Validation tests, and click **Next**.
This process creates a report that identifies any problems that need to be addressed before creating the cluster.
5. When the validation is completed, provide a name for the cluster in the **Cluster Name** field.
6. Click **Next** to create the cluster.

If you are configuring a WSFC that does not require shared storage, clear the **Add all eligible storage to the cluster** option.

Install SQL Server on Each Node

After configuring the WSFC, you must perform the SQL Server installation on each node in the cluster.

Installation Requirements and Notes

- SQL Server 2012 or later Enterprise Edition is required for Availability Groups.
- If you are only configuring Availability Groups (not a Failover Cluster Instance), you must perform a new SQL Server stand-alone installation, not a new SQL Server failover cluster installation, on each node.
- Shared storage is a requirement of Availability Groups only if they are installed in a SQL cluster. The prerequisite check will fail if you choose a SQL Server cluster installation and do not provide shared storage.
- Only the SQL database engine can use Basic Availability Groups. Even though the Availability Groups use a WSFC, this relationship does not constitute a true cluster and will not provide fault tolerance for other SQL Server services (Analysis Services or Reporting Services).
- To be fault tolerant, Analysis Services must be part of an actual Failover Cluster Instance (FCI) where SQL is installed using a new SQL Server failover cluster installation.
- An FCI may be used together with an Availability Group to enhance the availability of an availability replica. However, to prevent potential race conditions in the WSFC cluster, automatic failover of the Availability Group is not supported to or from an availability replica that is hosted on an FCI.
- Reporting Services use a Scale-out Deployment, which is not a cluster.
- You can use the same or different service accounts on each node, but all accounts must have rights to the file share described in the Prerequisites section above.

- FileStream functionality can be used with Availability Groups and will require that FileStream be enabled on all failover nodes.

Attention: For more information, see:

- [FILESTREAM and FileTable with Always On Availability Groups \(SQL Server\) | Microsoft Docs](#)

You may also need the following Microsoft hotfix:

- [Can't access VNN FILESTREAM share when you use the FILESTREAM and FileTable features on a Windows Server 2012-based failover cluster](#)

- Although this is not a specific requirement, you should consider performing the exact same SQL Server installation on each node, including the same installation and data paths and instance name.
- For proper failover support, the failover nodes should have comparable hardware resources.
- See the MSDN documentation for prerequisites, restrictions, and recommendations for AlwaysOn Availability Groups:

[Prereqs, Restrictions, Recommendations - Always On Availability Groups](#)

After installing SQL Server on all nodes in the cluster, restore your Vantagepoint transaction and FileStream databases and configure the SQL Reporting Services databases (ReportServer and ReportServerTempDB) on the primary node in the cluster.

Configure Database Login

For the Vantagepoint and Reporting Services databases that are part of an Availability Group to be immediately available in the event of an Availability Group failover, you must complete these steps on all failover nodes. The following rights need to be granted to the login used to access the databases (Vantagepoint and Reporting Services databases) that are part of the Availability Group:

Permission	Required for
Dbo = Database Owner rights to all databases in the Availability Group	All databases in the Availability Group
View Any Definition	Availability Groups
View Server State	Availability Groups

When you back up and restore a database to another server, the login on Server A has a different SID (Security Identifier) than the same login on Server B. This issue is typically resolved using the `sp_change_users_login` stored procedure. However, because the database on the secondary replica will be in read-only mode, you cannot fix the login.

You can resolve this issue by using the `sp_help_revlogin` stored procedure, found in the following article:

[How to transfer logins and passwords between instances of SQL Server](#)

Once the procedure is created in the master database, execute it to get the list of SQL logins with their associated SIDs and the CREATE statement to create the login on the secondary replicas.

Here is an example.

```
CREATE LOGIN [DeltekVantagepoint] WITH PASSWORD =
0x0200E0E05D60876CCE39BD9209515FB63C5589D6C939F3AB56A6CE9DBFBF49A9410F66F09840827135F8
00725E25A77714FDFA31FB6C18BCB46561217947C3749F0380A18AF5 HASHED, SID =
0x0124F12258D9BD49BE649C2D7A6DA838, DEFAULT_DATABASE = [master], CHECK_POLICY = OFF,
CHECK_EXPIRATION = OFF
```

Prior to configuring the Availability Groups, run the CREATE statement(s) created from executing the sp_help_revlogin on your server on all secondary replicas.

Create Availability Groups

You must enable Availability Groups and create an Availability Group on the primary node.

To enable Availability Groups:

1. Open the SQL Server Configuration Manager.
2. Right-click the SQL Server service, and click **Properties**.
3. On the AlwaysOn High Availability tab, select the check box to enable the Availability Groups for each node.
4. Restart the SQL Server service.
5. Repeat steps 1-4 on all nodes that will be part of the Availability Group.

To create an Availability Group:

1. Select the databases to be included in the Availability Group (all of these databases will fail over together if there is a failover).

At a minimum, include the Vantagepoint and Reporting Services databases (ReportServer and ReportServerTempDB).

The database must be in FULL recovery mode and a FULL database backup must have been taken of the database prior to starting the Availability Group wizard.

Attention: For more information on performing backups and restores of databases in FULL recovery model, see the following MSDN documentation:

[Back Up and Restore of SQL Server Databases](#)

2. In SQL Server Management Studio, start the Availability Group Wizard.
3. Expand **AlwaysOn High Availability**, right-click **Availability Groups**, and click **New Availability Group Wizard** on the shortcut menu.
4. Select a name for the Availability Group.

This is not the virtual name of the Availability Group listener, but it can be the same. The name should describe the databases the Availability Group includes (for example, DeltekVantagepointAG) because multiple Availability Groups can exist on the same servers.

5. Select the **Database Level Health Detection** option.

This undocumented option controls whether the entire Availability Group fails over if one database becomes suspect.

6. Select the databases that you want to include in the Availability Group.
The wizard will tell you whether or not they meet the requirements (for example, FULL recovery and FULL backup taken).
7. Specify the Availability Group configuration (nodes, failover mode, and synchronization mode).

Attention: See this article for more information on failover and failover modes:
[Failover and Failover Modes \(Always On Availability Groups\)](#)

See the following settings to complete the fields on this form:

Setting	Description
Server Instance	A maximum of four servers is allowed (eight with SQL Server 2016)
Initial Role	Select the role of the server (Primary or Secondary).
Automatic Failover	Check this option for failover to occur automatically. Otherwise, failover will be a manual process.
Synchronous Commit / Asynchronous Commit	<p>This option controls how transactions are committed, which has an impact on the performance of the synchronization and how much data may be lost in the event of a failure. Select one of these options:</p> <ul style="list-style-type: none"> ▪ Synchronous Commit: Each transaction must be committed to both Node 1 and Node 2 before the transaction is considered complete. This option reduces the possibility of data loss, but at the expense of performance. ▪ Asynchronous Commit: Each transaction is committed to Node 1. The transaction is also sent to Node 2 but there is no verification if it is or is not committed. This option performs better, but with the chance of data loss.
Readable Secondary	<p>Select one of these options:</p> <ul style="list-style-type: none"> ▪ No: Connections are not allowed to secondary replicas. ▪ Yes: Connections are allowed in read-only mode. ▪ Read-intent only: Connections using the ApplicationIntent=ReadOnly keyword are used for Read Only Routing.

8. Click the Endpoints tab.
The Endpoint for each instance is created automatically.
9. Click **Backup Preferences** to select whether or not backups can be taken from replicas other than the primary replica (another feature of Availability Groups).
10. Click the Listener tab. You use this tab to create the Availability Group Listener.

11. From the **Network Mode** drop-down list, select the type of listener: **Static IP** or **DHCP**.

The port will be the same as the one used by the SQL Server port (the default is 1433).

Note: If you are using multiple subnets, use the **Add** button to add the IP address for the listener on all subnets. This option is available only if you are using Static IP addresses. See the following article for more information:

[Add IP Address Dialog Box \(SQL Server Management Studio\)](#)

12. Click **Next**.
13. On the Data Synchronization Preference tab, enter the shared path or use the **Browse** button to select the location that all nodes/SQL Service accounts can access. This determines how the databases synchronize to the replicas.

Read Only Routing Configuration

Vantagepoint architecture changes have been made to support the Read Only Routing feature. This feature lets certain report queries to run against a read-only copy of the Vantagepoint transaction database on a secondary replica of the Availability Group. The benefit of this feature is that it allows much of the Vantagepoint reporting workload to be offloaded from the database on the primary replica to the secondary replica, which frees resources for the transaction workload.

- Only the following reports use Read Only Routing:
 - Dashboard reports
 - Reports that you run from the Reporting menu (except Purchasing reports)

Reports that use the replica database will do so regardless of how they are generated: when they are previewed, directly printed, emailed, run via the process server, or generated in another way.

- Read Only Routing requires that the connection string uses the **ApplicationIntent=ReadOnly** keyword. The Vantagepoint Reporting architecture has been modified to allow for this change in the connection string when the database configuration specified in Weblink is configured to use Availability Groups.
- With this keyword and the proper configuration (queries below), the Availability Group will automatically route connections with this keyword to the read-only secondary replicas configured for **Read-intent only**.
- Even though you have configured the Availability Group for read-intent only secondary replicas, manual queries are required to configure the Read Only Routing part of the configuration.

Attention: For more information about Read Only Routing, read the following article:

[Configure Read-Only Routing for an Availability Group \(SQL Server\)](#)

Read Only Routing Queries

Two queries are required to modify the Availability Group configuration to support Read Only Routing:

- Configure the Read Only Routing URL
- Configure Read Only Routing Lists

Configure the Read Only Routing URL

Read Only Routing URLs are different from Availability Group endpoints, which were automatically configured earlier. In the Availability Group configuration above, there are two nodes, each configured to allow read-intent only connections when the node is in secondary mode. (A node in secondary mode is promoted to primary when a failover occurs.)

- The following query identifies existing read-only routing URLs:

```
select read_only_routing_url from sys.availability_replicas
```

Query Result (if present; otherwise the query will return NULL):

```
read_only_routing_url
tcp://CAMDEVSQL12AG1:1433
tcp://CAMDEVSQL12AG2:1433
```

- This blog post identifies a script that can be run against each replica to calculate the read-only routing URL:

[Calculating read only routing url for AlwaysOn](#)

Here is sample output from the script:

```
Read-only-routing url script v.2012.1.24.1
This SQL Server instance version is [11.0.2100.60]
This SQL Server instance is a standard (not clustered) SQL Server instance.
This SQL Server instance is enabled for AlwaysOn.
This SQL Server instance is NOT a Sql Azure instance.
This SQL Server instance DAC (dedicated admin) port is 1434
This SQL Server instance is listening to all IP addresses (default mode).
This SQL Server instance is listening on fixed tcp port(s) (it is not
configured for dynamic ports), this is a recommended configuration when using
read-only routing.
This SQL Server instance resides in domain 'dev.ads.deltek.com'
This SQL Server instance FQDN (Fully Qualified Domain Name) is
'CAMDEVSQL12AG1.dev.ads.deltek.com'
This SQL Server instance port is 1433
*****

The read_only_routing_url for this SQL Server instance is
'tcp://CAMDEVSQL12AG1.dev.ads.deltek.com:1433'
*****
```

- The following statements configure the read-only routing URL for each node:

```
ALTER AVAILABILITY GROUP [SQL12AG1]

MODIFY REPLICA ON N'CAMDEVSQL12AG1' WITH
(SECONDARY_ROLE (READ_ONLY_ROUTING_URL=N'tcp://CAMDEVSQL12AG1.dev.ads.deltek.com:1433'))

ALTER AVAILABILITY GROUP [SQL12AG1]

MODIFY REPLICA ON N'CAMDEVSQL12AG2' WITH
(SECONDARY_ROLE (READ_ONLY_ROUTING_URL=N'tcp://CAMDEVSQL12AG2.dev.ads.deltek.com:1433'))
```

Where:

- [SQL12AG1] is the name of the Availability Group (not the listener).
- CAMDEVSQL12AG1 is node 1 and CAMDEVSQL12AG2 is node 2.
- tcp://CAMDEVSQL12AG1.dev.ads.deltek.com:1433 is the read-only routing URL for node 1 and tcp://CAMDEVSQL12AG1.dev.ads.deltek.com:1433 is the read-only routing URL for node 2.

Configure Read Only Routing Lists

Read Only Routing Lists provide a priority order for the routing of read-intent only connections among nodes in an Availability Group configured for Read Only Routing.

- The following query identifies existing Read Only Routing Lists and shows that when CAMDEVSQL12AG1 is the primary, the priority order will be the replica (CAMDEVSQL12AG2) and then itself if the replica is not available (and vice versa if CAMDEVSQL12AG2 is the primary):

```
select g.name, r1.replica_server_name, l.routing_priority,
r2.replica_server_name, r2.read_only_routing_url
from sys.availability_read_only_routing_lists as l
join sys.availability_replicas as r1 on l.replica_id = r1.replica_id
join sys.availability_replicas as r2 on l.read_only_replica_id = r2.replica_id
join sys.availability_groups as g on r1.group_id = g.group_id
```

Query Result:

name	replica_server_name	routing_priority	replica_server_name	read_only_routing_url
SQL12AG1	CAMDEVSQL12AG1	2	CAMDEVSQL12AG1	tcp://CAMDEVSQL12AG1:1433
SQL12AG1	CAMDEVSQL12AG2	1	CAMDEVSQL12AG1	tcp://CAMDEVSQL12AG1:1433
SQL12AG1	CAMDEVSQL12AG1	1	CAMDEVSQL12AG2	tcp://CAMDEVSQL12AG2:1433
SQL12AG1	CAMDEVSQL12AG2	2	CAMDEVSQL12AG2	tcp://CAMDEVSQL12AG2:1433

- The following statements configure the Read Only Routing Lists for this configuration:

```
ALTER AVAILABILITY GROUP [SQL12AG1]

MODIFY REPLICA ON N'CAMDEVSQL12AG1' WITH (PRIMARY_ROLE (READ_ONLY_ROUTING_LIST
= (N'CAMDEVSQL12AG2',N'CAMDEVSQL12AG1')) )

ALTER AVAILABILITY GROUP [SQL12AG1]

MODIFY REPLICA ON N'CAMDEVSQL12AG2' WITH (PRIMARY_ROLE (READ_ONLY_ROUTING_LIST
= (N'CAMDEVSQL12AG1',N'CAMDEVSQL12AG2')) )
```

Where:

- [SQL12AG1] is the name of the Availability Group (not the listener).
- CAMDEVSQL12AG1 is node 1 and CAMDEVSQL12AG2 is node 2.

Configure Vantagepoint and Reporting Services to Use Availability Group Listener

Next, configure Vantagepoint and Reporting Services to use the Availability Group Listener that you configured above:

- Use the Weblink utility to configure your Vantagepoint transaction database, report server database, and FileStream database to use the Availability Group Listener.
- Use the Report Server Configuration Tool to configure Reporting Services to use the Availability Group Listener.

Configure Vantagepoint to Use the Availability Group Listener

To configure Vantagepoint to use the Availability Group Listener:

1. Launch the Weblink utility, and select or add the Vantagepoint transaction database that is part of the Availability Group.
2. On the General tab, enter (or change) the Availability Group Listener name in the **SQL Server** field.
3. In the **Database Name** field, enter the name of the Vantagepoint transaction database.

Enter the SQL Server login ID and password for the login that has been granted the necessary SQL Server rights to the Availability Group database. See the Configure Database Login section for more information.

If you see the **Use Availability Groups** check box, but it is not enabled, check to see if the **Use Alternate Database for Reporting** check box is selected on the Report Server tab. You cannot use both the Availability Groups and Alternate Database for Reporting features because they provide the same functionality but are designed for different versions of SQL Server.

Note: Although you are modifying the server connection information for the Vantagepoint database, the Vantagepoint FILESTREAM database (if applicable), and the Reporting Services database to use the Availability Group Listener, this action only ensures that these databases can still connect to the new primary node in the event of a failover.

The only features that use the Vantagepoint database on the secondary (Read Only) replica are the database queries for the specific reports described earlier in this document. This includes reports on the Reporting Applications menu (excepting Purchasing reports) and Dashboard reports.

4. Select the **Use Availability Groups** check box.

At this point a query is issued to identify the edition of SQL Server and the name of the Availability Group for the database. If the check returns **Standard**, the label of the check box changes to **Use Basic Availability Groups**. Selecting this option does not impact the failover functionality; it is just a visual identifier that Availability Groups are in use.

5. If you are using FileStream and the FileStream database is part of the Availability Group (which it should be if the database is on the same SQL Server as Vantagepoint), confirm that the FileStream SQL Server is using the Availability Group Listener name.

If it is not, change the listener name to the Availability Group Listener name.

6. On the Report Server tab, confirm that the **Server Name** specified in the Report Server Database Access section is using the Availability Group Listener name.

If it is not, change the listener name to the Availability Group Listener name.

Configure Reporting Services to Use the Availability Group Listener

If Reporting Services has not yet been configured, follow the steps in [Microsoft SQL Reporting Services](#) to configure Reporting Services. Remember to add the report server databases to the Availability Group. When you enter the Database Server name to use for the report server databases, use the Availability Group Listener.

If Reporting Services is already configured to use the primary node server name:

1. Open the Reporting Services Configuration Manager.
2. Select the Database menu.
3. Click the **Change Database** button.
4. Select the **Choose an existing report server database** option and click **Next**.
5. On the **Connect to the Database Server** screen, change the **Server Name** to be the Availability Group Listener, and click **Next**.
6. Select the existing ReportServer database from the drop-down list and click **Next** to complete the re-configuration.

Flexible Failover Policy

The Failover Policy controls the Failover feature of Availability Groups. For more Information on this feature, see this article:

[Flexible Failover Policy for Automatic Failover of an Availability Group \(SQL Server\)](#)

Failover Condition Level and Health Check Timeout

Transact-SQL Value	Level	Automatic Failover Initiated On...
1	One	Server down: The SQL Server service stops because of a failover or restart.
2	Two	Server unresponsive: Any condition of a lower value is satisfied, the SQL Server service is connected to the cluster and the health check timeout threshold is exceeded, or the current primary replica is in a failed state. This is the default level.
3	Three	Critical server error: Any condition of a lower value is satisfied or an internal critical server error occurs.
4	Four	Moderate server error: Any condition of a lower value is satisfied or a moderate server error occurs.
5	Five	Any qualified failure conditions: Any condition of a lower value is satisfied or a qualifying failure condition occurs.

The failover condition is determined by WSFC executing sp_server_diagnostics at regular intervals.

The following query identifies the existing Failover Policy:

```
select name,failure_condition_level,health_check_timeout from sys.availability_groups
```

Query Result:

name	failure_condition_level	health_check_timeout
SQL12AG1	3	30000

The following statements configure the Failover Policy for this configuration:

```
ALTER AVAILABILITY GROUP AG1 SET (FAILURE_CONDITION_LEVEL = 1); //default is 3
ALTER AVAILABILITY GROUP AG1 SET (HEALTH_CHECK_TIMEOUT = 60000); //default is 30000
```

Monitoring Availability Groups

The following tools are available for monitoring the status of an Availability Group:

- Availability Group Dashboard
- System and Dynamic Management Views (DMVs)
- System Monitor (PerfMon)
- Windows PowerShell

Availability Group Dashboard

To display the Availability Group Dashboard:

1. Launch SQL Server Management Studio and connect to the primary replica.

2. Right-click the **Availability Group** folder and click **Show Dashboard** on the shortcut menu.

System and Dynamic Management Views (DMVs)

This article provides a variety of System Views and DMVs that you can use to monitor the health and status of the WSFC and Availability Groups:

[Monitor Availability Groups \(Transact-SQL\)](#)

System Monitor (PerfMon)

A variety of System Monitor counters can be used to monitor the performance of Availability Groups. This article provides more information on the available counters and how to use them:

[Monitoring of Availability Groups \(SQL Server\)](#)

Windows PowerShell

These links are to a four-part MSDN series on using PowerShell to monitor Availability Groups:

- [Part 1 – Basic Cmdlet Overview](#)
- [Part 2 – Advanced Usage of AlwaysOn Health Cmdlets](#)
- [Part 3 – A Simple Monitoring Application for AlwaysOn](#)
- [Part 4 – Scheduling and Notification with SQL Agent](#)

Troubleshooting

Use Availability Groups Check Box Does Not Display

If the **Use Availability Groups** check box does not display for your Vantagepoint database when selected in Weblink, execute the following query to see if it returns anything:

```
SELECT e.name, s.database_name
FROM sys.availability_groups_cluster AS e
INNER JOIN sys.availability_databases_cluster AS s
ON e.group_id = s.group_id
```

The query should return a result set showing the name of the Availability Group and each database included in the Availability Group.

System Health Check

When you use Availability Groups, a system health check query is run to determine the health of the Availability Group. If the result of this query returns 0 or 1, the system falls back to running all reports against the Primary replica and effectively disables Read Only Routing. The health check query is:

```
select synchronization_health from sys.dm_hadr_availability_group_states
```

Synchronization Health Values

Value	Description
0	Not healthy: None of the availability replicas have a healthy synchronization_health (2 = HEALTHY).
1	Partially healthy: The synchronization health of some, but not all, availability replicas is healthy.
2	Healthy: The synchronization health of every availability replica is healthy.

Framework Exception: The user does not have permission to perform this action

The following error displays if the SQL login used for the Vantagepoint database does not have View Definition or View Server State permissions.

FrameworkException:

The user does not have permission to perform this action.

Call Stack:

```
{\b Query: }
```

```
select synchronization_health from sys.dm_hadr_availability_group_states
```

Attention: For more information, see the [Configure Database Login_section](#).

Solution:

Grant View Definition and View Server State permissions to the SQL Login.

Identify the Connection String Used by the Application or Process Server

To validate that the **MultiSubnetFailover=True** keyword is being added to the connection string for your Availability Group configuration, add the following setting to the web.config file under the <ApplicationSettings> tag:

```
<add key="LogConnectionString" value="Y"/>
```

When this option is set to **Y**:


- The application connection string (created at login) is logged in the ConnectionString.txt file named in the application Logs directory.
- The process server connection string is logged in the ProcessServerConnectionString.txt file in the same location.

Review these logs to ensure that the **MultiSubnetFailover=True** keyword is added to the connection string. After you have validated that the correct connection string is being issued, change the value of the **LogConnectionString** setting to **N**.

Identify the Connection String Used in a Report

After you configure the **Alternate Database for Reporting** or **Availability Group** option, you must validate that reports are running against the correct database. Preview the report to check the connection string.

To review the connection string by previewing the report:

1. Display any report.
2. Click the construction hat icon  on the Reporting toolbar.
If you don't see the icon, maximize the report.
3. From the **View Report Information** drop-down list, select **Report Data Source**.
4. Click the **View** button. You will be prompted to **Open** or **Save** the XML file.
5. Click **Open** to open the file using the application configured to open XML files (usually the default browser).
6. Review the `ConnectionString` element for the following attributes:
 - **Data Source:** This is either the database server specified in the Alternate Database for Reporting configuration or, if you use Availability Groups, the Availability Group Listener.
 - **Initial Catalog:** This is either the database name specified in the Alternate Database for Reporting configuration or, if you use Availability Groups, the Vantagepoint database name.
 - **ApplicationIntent=ReadOnly:** This only displays when you use Availability Groups and if the report was run against the Read Only Reporting database.
 - **MultiSubnetFailover:** This only displays when you use Availability Groups.



About Deltek

Better software means better projects. Deltek delivers software and information solutions that enable superior levels of project intelligence, management and collaboration. Our industry-focused expertise makes your projects successful and helps you achieve performance that maximizes productivity and revenue. www.deltek.com