Multi-site Best Practices

SolidWorks Enterprise PDM multi-site implementation

[SolidWorks Enterprise PDM 2010]

[May 2011]

[Revision 2]
Contents

Multi-site pre-requisites .......................................................... 5
Network connectivity .................................................................. 5
Firewall considerations ............................................................... 6
Network bandwidth and latency .................................................. 7

Installing SolidWorks Enterprise PDM in a replicated environment ................................................. 9
Servers installation..................................................................... 9
Clients installation..................................................................... 9
Mixed languages setup ............................................................... 10
Time zones ............................................................................... 10
Toolbox ................................................................................... 10

Using replication ....................................................................... 10
Replication schemas .................................................................. 11
Windows logins ......................................................................... 12
Test Settings ............................................................................ 13
Disk Space considerations .......................................................... 13

Site specific rules....................................................................... 13
Site specific workflows ............................................................... 14
Restricting access to files by site ............................................... 14
Notifications ............................................................................. 16

What if the system behaves slowly? ............................................. 17
Hardware solution for WAN optimization ..................................... 17
Network adapters: mismatched duplex settings ................................ 17
Network adapters: checksum offload .......................................... 17
Network bandwidth: advanced replication settings ....................... 18
Enterprise PDM administration settings ....................................... 19
Multi-site Best Practices

Explorer Get-Files policy ................................................................................................................. 21
SolidWorks add-in ............................................................................................................................ 23
Data card variables .......................................................................................................................... 25
Enterprise PDM templates .............................................................................................................. 25
Other alternatives ............................................................................................................................ 25
Post Sales and Support Considerations .......................................................................................... 27
Appendixes ....................................................................................................................................... 27
File Version Upgrade tool .................................................................................................................. 27
Removing already replicated archive files on a replicated server in a secure environment .......................... 27
Custom add-ins ............................................................................................................................... 28
Brief Overview: This document has been written to provide general guidelines to VARs to help them plan for, install and configure SolidWorks Enterprise PDM in a multi-site environment.

(i) This best practice was written as a guideline and should not be used without proper alignment to customer situation.

(ii) This document is only applicable to customers planning to use SolidWorks Enterprise PDM in a multi-site environment.
Multi-site pre-requisites

Network connectivity

SolidWorks Enterprise PDM uses TCP / IP protocol to communicate in between its clients and servers. By default, Enterprise PDM relies solely on system names to find server machines on the network.

Consequently, all PDM server / client machines must be able to ping one another using their respective system names. Note that running the ping test using fully qualified domain name or IP address does not constitute a valid test to verify the readiness of a network for Enterprise PDM unless Enterprise PDM has been configured to use pure IP address per the instructions found in the installation guide under the chapter “Configuring Enterprise PDM to Communicate Using IP Addresses”.

NOTE: In Windows networks, computer names should never exceed 15 characters in length (refer to Microsoft KB article 909264). It is therefore important to verify that all PDM clients and servers respect this simple rule.

In a multi-site environment, there will be two or more separate network domains. On one of them, you will find the Microsoft SQL server and one archive server, and on the other domain(s) you will have the remote archive server(s). In order for the servers to communicate with one another across the WAN it is required to have a working VPN connection in between all sites and each site should know how to resolve the distant servers’ system names to an IPv4 address. The name resolution to an IP address can be easily accomplished by editing the servers’ hosts files. SolidWorks recommends this simple approach whereby each server hosts file will have new lines with IPv4 addresses and system names of all “remote” servers the local server needs to communicate with. The hosts file can be found in C:\Windows\System32\drivers\etc\hosts. On Windows Vista, 7 or server 2008, you will have to start notepad with administrative privileges in order to modify and save the system protected hosts file.
NOTE: The benefit of using a VPN connection is mainly that the network traffic in between each site will be encrypted hence making your Enterprise PDM vault more secure.

Firewall considerations

Enterprise PDM uses two ports 1433 and 3030 to transfer metadata and data across its clients and servers. Using the telnet command will allow verifying this.

Below is a comprehensive list of what types of communication to expect when using Enterprise PDM:

- **Client ⇔ Microsoft SQL Server over TCP port 1433.** A client talks to SQL server constantly when performing operations in a vault: browsing, opening, viewing, etc.
- **Client ⇔ Archive Server over TCP port 3030.** Clients talks to an archive server when authenticating (logging in) and when sending / receiving files. An archive server also sends out broadcast refresh messages to logged in clients (e.g. to automatically refresh view listings when files are checked out, checked in, renamed, etc.)
- **Archive Server ⇔ Archive Server over TCP port 3030.** An archive server talks to another archive server when replicating a file. The target archive server requests files from source archive server. Archive files are always “pulled” from source not the other way around.
- Archive Server ↔ Microsoft SQL Server over TCP port 1433. At set times, depending on schemas defined in vault, archive servers contact SQL server to get a list of files to replicate, destroy, cold store, etc.

Consequently, the servers’ firewalls must be configured appropriately so that:

- TCP port 1433 is opened on Microsoft SQL server’s firewall
- TCP port 3030 is opened on all archive servers’ firewalls
- TCP port 80 (or 443 if using HTTPS / SSL) is opened on Microsoft IIS web server’s firewall

**NOTE:** because firewalls can be of two types, software or hardware, always ask your IT group for potential hardware firewalls that are in place and may be blocking traffic on TCP ports 1433 and 3030.

**NOTE:** there is no need to configure the clients’ firewalls to add TCP port exclusions unless the firewalls block outgoing traffic on TCP ports 1433, 3030 and 80.

**NOTE:** Microsoft SQL Server can be configured to use named instances. In which case, the default SQL TCP port may no longer be 1433 but another port, typically 1434.

**Network bandwidth and latency**

SolidWorks Enterprise PDM requires at a bare minimum a WAN bandwidth of 1 Mbit/sec. Concerning latency times, SolidWorks Enterprise PDM will become inoperable or unreliable if the latency time exceeds 250 milliseconds.

Measuring bandwidth can be achieved in many different ways. It is therefore best to ask your IT department for help. If your IT department has no tool to measure bandwidth, then they could start looking into two utilities freely available on the internet: **iperf** or **bwping**.

Measuring network latency time is much easier. Simply run in a DOS prompt the ping command with the following switches:

```
ping -4 -n 1000 <target server name>
```
The average value will be the average latency time in milliseconds for 1000 echo requests sent.
Installing SolidWorks Enterprise PDM in a replicated environment

Servers installation

It is recommended practice to have:

- Microsoft SQL Server installed on a server machine that is not the domain controller
- Separate servers for the archive server and the Microsoft SQL server
- Microsoft SQL Server installed locally to the engineering site that will have most users working in vault
- Microsoft SQL Server installed on server machine that has access to a lot of RAM. 64-bit server edition is preferred for Windows Server and Microsoft SQL Server.
- Archive servers installed on server machine with lots of available disk space and fast IO access to hard drives.

Clients installation

It is recommended practice to have:

- Administrative image for the client software available on each replicated site to easily deploy Enterprise PDM clients from central location. This can be done via simple batch scripting or using Active Directory group policy to deploy software. Please refer to the installation guide chapters “Creating an Enterprise PDM Client Administrative Image”, “Scripting a Silent Installation of Enterprise PDM” and “Deploying Clients Using Windows Active Directory” for detailed instructions.
- Review client machines for older installed version of SolidWorks eDrawings. If any, uninstall them via add/remove programs
- Determine which installer will install SolidWorks eDrawings Viewer: SolidWorks Installation Manager or Enterprise PDM client installer. Please refer to KB article S-049486 for details

NOTE: deploying Enterprise PDM client and vault views via ghost image technology is NOT supported because each vault view must be unique on each client machine. Using a ghost image will prevent the uniqueness of each vault view.
Mixed languages setup

SolidWorks Enterprise PDM has no restriction language-wise when it comes to the installer. It is therefore possible to install one archive server on an English Windows server and another archive server on a German Windows server. Same is true with Enterprise PDM clients; the language of the OS does not matter. Note that the date / time used by Enterprise PDM is UTC time, hence it will convert correctly to the local time using the regional settings.

**NOTE:** KB solution S-021298 (Is it possible to have an Enterprise PDM file data card show up in a different language depending on the logged in user or group) provides a nice example on how to configure data cards in a multi-language system setup.

Time zones

There is no problem having clients or servers in different time zones, or switching them to another local time zone after the initial installation. The archive servers do not use local server time to set dates on archives, instead it uses the date assigned by the file vault database. The database stores date using a “generic” UTC date format to handle vaults shared by clients and servers located in different time zones.

The only time the local archive server time is used is when triggering different schedules, such as replication, cold store and compression schedule. The specified schedule will start based on local server time.

Clients will also see the dates correctly according to the local time zone specified in Windows.

Toolbox

If planning to use the new or old Toolbox integration provided with Enterprise PDM, it will be required to create a replication schema for the Toolbox root folder in the vault. Complete documentation on how to configure Toolbox with Enterprise PDM can be found in the administration guide.

Using replication
Setting up replication is not always the right choice when working with remote offices. For instance, if you only have one remote user that needs access to the vault over WAN, it may be good enough to give him VPN access to the LAN network, and use the offline work mode in Enterprise PDM or setup the Enterprise PDM Web Server so that he can connect to vault using the web client.

Replication really makes sense when you have 5 or more users in remote site(s) or considerable amount of data that needs to flow back and forth on a regular basis.

**Replication schemas**

The example below should help clarify how to correctly setup Enterprise PDM for replication across WAN:

Let’s imagine an Enterprise PDM vault that is replicated in between Boston in the United States and Cambridge England. The time difference in between the two sites is 4 - 5 hours (depending on daylight saving). In our example, everything will be based on a 5 hours time difference.
The American engineers start working in vault from 9am to 6pm Monday to Friday local Boston time
- The UK engineers start working in vault from 8 am to 5 pm Monday to Friday local UK time

The first question that comes in mind is what the best time to start a scheduled replication on each replicated site is. The answer is quite simple. SolidWorks recommends that scheduled replications start when no user is working in vault so that no users are affected by a decrease in available bandwidth. Running scheduled replications off business hours does not mean users cannot replicate newer file versions from a remote archive server during regular business hours: on-demand replication is always available to users for that.

To go back to our example and answer the question we know that:

- UK engineers will leave work 5 hours before the US engineers do.
- UK engineers will work in vault from 3 am to noon US local time, then US engineers will work from 9 am to 6 pm.

When setting up replication schedules, the time entered is the local time of the target archive server.

If a new replication schedule is created where the source server is the UK archive server and the target server is the US archive server, setting the schedule to 7 pm will mean that replication will occur at 7 pm Boston time. This is a perfect time because no users are working in the vault hence all the bandwidth should be available for replication of files across WAN.

Another replication schedule can be created where the source server is the US archive server and the target server is the UK archive server, setting this schedule to midnight will mean that replication will occur at midnight UK time (7 pm US time). Again no users should be connected to vault at this time.

**Windows logins**

Because each replicated site will most likely have a different domain, the Windows domain users local to one site will not be visible to the other remote sites. Consequently, it is normal to have the “remote” Windows domain users show with a red plus sign next to their names in the administration tool users’ node when connecting to the local archive server.

If there is a need to have Windows users be visible across domains, then it is possible to create trust relationships in between the domains. Please refer to Microsoft articles for details on how to configure Microsoft Active Directory Servers:


Test Settings

Always use the Test button available in the replication settings dialog of your replicated vault. This provides an easy centralized location for testing replication connectivity settings.

**NOTE:** KB S-055138 “What are the most common errors received when testing replication connections in the SolidWorks Enterprise PDM administration tool?” can help diagnose errors encountered when testing the replication settings.

Disk Space considerations

Determining how quickly a vault grows and planning for disk upgrades can be a difficult task. SolidWorks KB solution S-046620 proposes a T-SQL query to help calculate vault growth knowing a date range by querying version metadata in database.

Site specific rules

Depending on your customer’s requirements, it may be required to have site specific rules in place. Site specific rules could be separate workflows, different access rules to files in vault, different CAD systems, and yet share projects and standard library parts across sites.
Site specific workflows

The easiest way to configure Enterprise PDM to use different workflows for each site is to use a condition on a folder structure or by using a site specific variable value condition.

Or using a variable value condition

You could automate the writing of the Workspace variable value by creating site specific Enterprise PDM templates. Then configure the templates to be only visible to a group or users that belong to the correct site.

Restricting access to files by site

This can be achieved by creating site specific groups and restricting folder permissions to a group.

For example, Site A group can read file contents, add or rename file, add or rename folder in Project 100 ...
... but has no folder permissions to Project 200.

Another alternative is to use file based permissions. File based permissions can be set by right-clicking Properties on a file.
Notifications

Similar to how you can restrict files access to site-specific groups, notifications can be assigned to site-specific groups.
What if the system behaves slowly?

Hardware solution for WAN optimization

Some SolidWorks customers have successfully used Riverbed Steelhead appliances to optimize WAN traffic. Please refer to http://www.riverbed.com/results/solutions/ for more information.

Network adapters: mismatched duplex settings

The most common network performance hit comes from mismatched duplex settings in between client to server, server to client, and server to server network adapters. SolidWorks recommends trying different duplex speed settings to determine which duplex speed is the best for transferring data across the network. Half duplex speed settings should never be used, instead trying different full duplex speeds and auto modes will be sufficient.

The simplest way to measure this is:

- Configure machine A network adapter duplex speed to 100 Mbps Full Duplex
- Configure machine B network adapter duplex speed to 100 Mbps Full Duplex
- Create a network share on computer B
- Copy a large SolidWorks file (e.g. 20 MB) from computer A to network share on computer B
- Record how long it takes to complete the copy
- Repeat above steps using a different duplex speed (e.g. auto-negotiate)

Once exact times have been recorded for each full and auto duplex speeds, it is very easy to compare the timings and determine which duplex speed setting must be used to have the best optimized data transfer in between two computers.

Network adapters: checksum offload

For most common network traffic, offloading checksum calculation to the network adapter hardware offers a significant performance advantage by reducing the number of CPU cycles required per byte. However, it has been brought to our attention that offloading checksum calculation to the network adapter can cause serious slowness when working with SolidWorks Enterprise PDM add-in.
Hence it may be worth disabling checksum offload to see if performance can return to a more normal state.

**Network bandwidth: advanced replication settings**

To minimize the number of files being replicated across WAN, Enterprise PDM has advanced replication settings available to help fine tune bandwidth usage:

- Only latest version of files will be considered for replication
- Only replicate files that have a revision
- Only replicate files that have a specific workflow state
The last advanced setting can be useful to force a scheduled replication to stop after a given amount of time. A typical scenario would be to stop scheduled replication an hour before users start their working day and connect to vault; hence ensuring maximum bandwidth is available to them.

**Enterprise PDM administration settings**

A few Enterprise PDM user settings can improve performance.

For check-in operations, turning off the setting “include drawings automatically when checking in the model” can reduce the time to display the check in dialog as drawings will not be included.
File Type Properties can also be configured to improve performance when previewing SolidWorks assembly or drawing files by selecting the option “Preview does not need referenced files” as it will tell Enterprise PDM not to cache reference files when previewing assembly or drawing files in eDrawings window.

Another setting can negatively impact performance when calling get version, change state, check in dialogs: “Show this file type as a sub-parent (drawing)”. This setting is turned on by default for SolidWorks drawings. Unselecting it will tell Enterprise PDM not to display parent drawings in reference tree display of the get version, change state and check-in dialogs.
If turned on, checking out a part file used by a drawing will display the parent drawing in blue in the reference tree.

**Explorer Get-Files policy**

If dealing with slow time caching large assembly or drawing structure in a vault view, it is possible to configure an Enterprise PDM group policy: Explorer Get-Files policy to use a lower number of threads.
Enabling and configuring this policy to only use one thread when retrieving files can noticeably reduce the time to cache large number of files in a vault view.

More information on how to setup this policy can be found in the installation guide under the chapter “Specifying SolidWorks Enterprise PDM Settings Group Policy Manually”.

**NOTE:** this group policy client setting can be applied to PDM clients in a replicated and non-replicated environment. If in a replicated environment, note that this setting does not affect on-demand replication which by design is a single threaded operation.
SolidWorks add-in

The Enterprise PDM add-in for SolidWorks can be reconfigured to help with poor performance in remote locations.

As a first step, remote users can configure their Enterprise PDM client options so that the add-in no longer update the tree in the extra tree pane after a component’s window has been activated, after a component has been added, deleted or renamed, after a component has been reloaded, after a component has been suppressed or un-suppressed and after the get, check out and check in operations.

![Options settings](image)

Although this will help with overall performance while working in SolidWorks, users will be losing access to valuable functionality.

If this is not sufficient, a more radical approach consists in hiding the extra tree pane altogether.
Hiding the task pane will not prevent users from calling basic Enterprise PDM commands from SolidWorks such as check out, check in, get latest version, file data card, etc. Those commands are still available from a right-click selection in SolidWorks FeatureManager tree.
Data card variables

The less card variables you use in your file data cards definition, the less SQL traffic is needed, the faster Enterprise PDM will behave. It is therefore always best to be considerate on how many card variables are really needed when setting up Enterprise PDM in a multi-site environment.

Enterprise PDM templates

The same principle that was explained above for data card variables can be applied to template input forms. Always keep number of used card variables in template input forms to a bare minimum when working in a multi-site vault.

Other alternatives

When dealing with a WAN with a latency time that is too high, it may be best not to use a central Microsoft SQL Server for all replicated sites. Instead it may make more sense to have one vault per site.
with its own Microsoft SQL Server so that all local clients and archive server connect to SQL database via LAN. Replication can then be set up for each vault so that archive files can be accessed via replication from remote site if needed. Users will consequently have more than one vault view: one being their production vault view that connects to a local Microsoft SQL database, and other vault views will point to a remote vault that has its own separate database but will allow caching locally files from the remote vaults.
Multi-site Best Practices

Post Sales and Support Considerations


Multi-site accounts require special considerations for planning of on-going support. It is important to have this conversation with the customer during implementation planning to set the proper expectations. For all customers that purchase PSL license, the responsibility of PDM support lies with the VAR that deploys and configures Enterprise PDM server. Customer may have support from local VAR for SolidWorks but they must contact proper VAR for Enterprise PDM support issues and questions. As stated in Support Guidelines, customer must assign a single point of contact called ‘Lead Administrator’ at the site where the server is hosted.

For any local projects where remote site has unique requirements e.g. need to migrate legacy data, it is recommended that the Lead Administrator should initiate such activity by engaging with VAR. If there is a local VAR involved at remote site and you have any concerns, please contact fieldservices@solidworks.com

Appendixes

File Version Upgrade tool

SolidWorks recommends upgrading files on site local to Microsoft SQL Server, then setup a replication schema to schedule replication of the converted SolidWorks files to the remote sites.

Removing already replicated archive files on a replicated server in a secure environment

A customer has a manufacturing division abroad and replication is in place for some of the projects between the two locations. After a project is finished and run its course, there is a need to stop replication on that specific project. Of course, this is no problem but can the physical archive files for that project be removed from the remote replicated archive server for security purposes?

A solution exists and is documented in KB S-055231 “Is it possible to remove already replicated archives from specific folders on a replicated server in a secure environment?” The KB provides a maintenance tool along with documentation to allow physically removing archive files from a replicated archive server belonging to a specific project folder. The maintenance tool is not downloadable from the VRC.
is therefore required to submit a new service request to request a copy of the tool.

**Custom add-ins**

Add-ins are replicated to all archive servers when first added to a vault, then loaded to all workstations that have a local view. This means that custom add-ins will be global to the replicated vault i.e. there is no way to restrict add-in usage to one replicated site.

If the add-in contains T-SQL queries, one must ensure that the SQL queries are optimized for WAN. Any add-ins planned for production should always be tested in a replicated environment to ensure they do not add any unnecessary overhead.