# InfoPath Forms Services Best Practices

|  |  |
| --- | --- |
|  | Note: |
|  | This content is preliminary content for a preliminary software release. It might be incomplete and is subject to change. |

We recommend that you follow these best practices when managing your InfoPath Forms Services environment.

## Document limit of 2,000 in WSS document libraries

If a form template will be filled out and submitted more than 2,000 times in total, you should either develop the form template to submit to a database through the use of a Web service, or create a custom submit function that places forms into multiple libraries. This is due to a limitation in the capacity of Microsoft Office SharePoint Server 2007 document libraries, which may experience serious performance degradation if more than 2,000 documents exist in the library.

If you think a form template may be submitted more than 2,000 times, it is easier to begin by developing the form to use an alternative submit method than to correct this issue once it becomes a problem, particularly if the form template is available to a publicly accessible Web site. For more information on developing a form template to submit data to a Web service, see *About submitting data to a server or Web service*.

## Use Form View when configuring Forms Services session state

You can configure InfoPath Forms Services to use the Session State Service (the default option) or Form View to control how user sessions are managed. When you configure InfoPath Forms Services to use the Session State Service, all browser sessions are maintained on the SQL Server database corresponding with the Shared Service Provider (SSP) associated with the Web application on which the form template is hosted. This scenario uses little network bandwidth, but has a cumulative performance impact on the computer running SQL Server. When you are using Form View, sessions are maintained on the client browser, and all session data is included in each postback to the server, up to 40 kilobytes of session data. This uses more bandwidth than using session state, but does not affect the computer running SQL Server. Once session data reaches 40 KB in size, the session automatically transitions to session-state management.

We recommend the use of Form View in environments that have smaller groups of users, because it reduces the impact on SQL Server. If your InfoPath Forms Services deployment will have many users, particularly if session data is below 40 KB for many high-usage form templates, session state is likely a better choice. If Form View is used, the bandwidth used by browser sessions of 40 KB or fewer can be monitored if there is a concern that network performance might be adversely affected.

## Running SQL Server on a front-end Web server not recommended

If you run SQL Server on an Office SharePoint Server front-end Web server (for example, in a single-server evaluation deployment), the ASP.NET cache will release system memory at a lower threshold than SQL Server, which could result in InfoPath Forms Services memory starvation.

ASP.NET employs a strategy of targeting maximum Internet Information Server (IIS) memory use of the lessor of either 800 megabytes or 60% of available physical RAM. These settings are configurable in IIS manager. ASP.NET also monitors physical RAM use, not just for the w3wp service, but for the entire system. When 80% of the physical memory on the server is committed, ASP.NET begins periodically dropping the oldest and lowest priority 5% of the cache. When 85% of physical memory is committed, ASP.NET will drop 50% of the cache periodically. At 90% or more, ASP.NET aggressively trims the cache and sets low limits on the maximum number of entries, which remains in effect until ASP.NET reassesses memory pressure on the server and raises the threshold.

The memory usage threshold for SQL Server is higher by default than the ASP.NET cache. In this scenario, SQL Server will never release memory because the ASP.NET cache will already have released memory before the SQL Server threshold is reached. This can lead to a condition in which the throughput of InfoPath Forms Services is reduced with a subsequent impact on performance.

To mitigate this issue, you should configure SQL Server memory limits manually when SQL Server is installed on the same server as Office SharePoint Server . For more information on adjusting SQL Server memory settings, see the article [Server Memory Options](http://msdn.microsoft.com/library/default.asp?url=/library/en-us/adminsql/ad_config_9zfy.asp) on the Microsoft Web site.

## Best practices for anonymously accessible forms

When you deploy a form to a location where it is exposed to anonymous users, such as a public SharePoint document library or an imbedded form in a Web page on the Internet, there are a number of additional steps you should take to mitigate the risk of improper form usage, Denial of Service (DoS) exploits, and potential performance issues.

|  |  |
| --- | --- |
| • | Ensure that form templates cannot be accessed by scripts or other automated or non-human processes. One way to achieve this is to force users who are submitting a form template to enter an identification code such as a short alphanumeric string displayed in an image, which cannot be "read" by a script or automated process. |
| • | Form templates that contain sensitive information such as authentication information, server or database names, or proprietary code should never be exposed to anonymous users. |
| • | Form templates that contain an e-mail submit data connection should not be deployed to servers that are anonymously accessible, as e-mails generated when the form is submitted will show "sent by anonymous user" in the subject line. |
| • | Form templates that contain code or functionality that can invoke processes on a server should be carefully evaluated and tested to ensure that security cannot be compromised by making the form template accessible to anonymous users. |
| • | In order to prevent users from submitting multiple copies of a form, you might consider including code that tracks the IP address of each user who submits a form and prevents duplicate submissions from the same IP address. |
| • | Protect the integrity of form templates by enabling protection to prevent the form template from being changed. |