WTB/04/017

Document type: Reference

Filtered Warnings Application infrastructure

(V2.0) August 2006

Keywords

[Filtered warnings application, infrastructure, software]

Version control

This document may be made available in more than one electronic version or in print. In a case of existing or perceived difference in contents between such versions, the reference version is the version available for download from the WARP Toolbox site http://www.warp.gov.uk

If you find errors in the current document, please send your comment to editor@warp.gov.uk

Disclaimer

Copyright notification

Contents

1 Scope

The Filtered Warnings Application supplied by NISCC to assist in the operation of the Filtered Warnings Service has some infrastructure requirements that must be addressed in order to successfully operate.

Consideration of the items described in this document during the service provision phase of a WARP deployment will ensure that the Filtered Warnings Application is deployed in a manner that will ensure smooth operation.

It should be noted that it is not necessary to run the Filtered Warnings Application in order to provide a filtered warnings service.

2 Definitions and abbreviations

2.1 Definitions

For the purposes of this document, the following terms and definitions apply:

Internet: The public Internet – as apposed to a private network to which the general public have no access.

2.2 Abbreviations

For the purposes of this document, the following abbreviations apply:

NISCC:	National Infrastructure Security Co-ordination Centre
WARP:	Warning, Advice and Reporting Point

3 Server Provision Models

The Filtered Warnings Application is a Web based system that operates on a Microsoft Windows platform. The hardware and software required to operate the Filtered Warnings Application can be purchased out-right or leased. It is important that it be hosted on a network that will provide connectivity to the WARP community, in many cases this will mean the hardware on which the Filtered Warnings Application is run will require connection to the Internet, and care must be taken to define a suitable security policy. The two main models of provision will be local ownership and hosted services. The capacity of the server(s) required to operate FWA will depend on the deployment option chosen.

3.1 Local Provision

Where the WARP operation is run from within an organisation that has access to their own IT services (or IT services managed on their behalf under an existing contract arrangement), it may be cost effective to add the server(s) that will run FWA to the existing facilities. Given the nature of the information that may be shared amongst WARP

members, it is not recommended that WARP services be hosted on an existing server that also supports other functions, as guaranteeing the segregation of data may be hard to achieve. When using existing facilities it is important to ensure that all the potential members of the WARP will be able to get network connectivity to it - some liaising with IT support staff on this issue is likely to be required.

3.2 Hosted Services

An alternative model is one where the FWA server(s) can be leased from a hosting company. Usually this will mean the server will be accessed via the Internet, which is likely to make it easy for WARP members to access the services provided, but careful consideration of the security policy is required. Generally speaking hosting companies will offer the kind of server(s) that would be suitable for running a secure FWA system described as "dedicated and managed".

4 Technical Requirements

4.1 Deployment Options

The Filtered Warnings Application can be deployed either entirely on a single server, or with a separate database server. The separate database server approach, whilst costlier, has two distinct advantages over the single server method:

1. All the data used to drive the application can be securely separated from the Internet facing web server, thus providing a better security model;
2. It may be possible to us an existing SQL Server installation for data storage, thus saving on licensing costs (although additional components would have to be installed on the SQL server system, see the next section).

4.2 Software

The Filtered Warnings Application is built on a Microsoft Windows platform. The following table lists the Microsoft software products that are required in order to install the application.

Standalone server or web server font-end		
Item	Version	Licensable
Windows 2003 Server	R1 or R2	Yes
SQL Server 2000 Standard Edition (*)	SP3a or higher	Yes
SQLXML	V3.0 SP2 or higher	No
Notification Services	V2.0 SP1 or higher	No

(*) If a separate SQL server database is being used, only the client access components are required on the web server.

Database server back-end (for separate database server installations)		
Item	Version	Licensable
Windows 2003 Server	R1 or R2	Yes
SQL Server 2000 Standard Edition	SP3a or higher	Yes
SQLXML	V3.0 SP2 or higher	No
Notification Services (+)	V2.0 SP1 or higher	No

(+) Only the database components required.

Minimum software versions are shown, it is always recommended that any security patches that become available also be applied.

4.3 Hardware

The following table shows the MINIMUM hardware requirements for operating the Filtered Warnings Application. The actual specification used should take into account a WARP's requirements for on-line storage, backups and redundancy.

CPU	Intel Pentium IV 3.2 GHz
Memory	1GB
Storage	15MB for the FWA Product, plus database storage. The amount of database storage required is entirely dependant upon the number of notifications sent, and the length of time they are retained.

History

Version	Date	Description
V1.0	June 2004	First issue for WARP Toolbox
V2.0	August 2006	Updated for FWAV4.1.