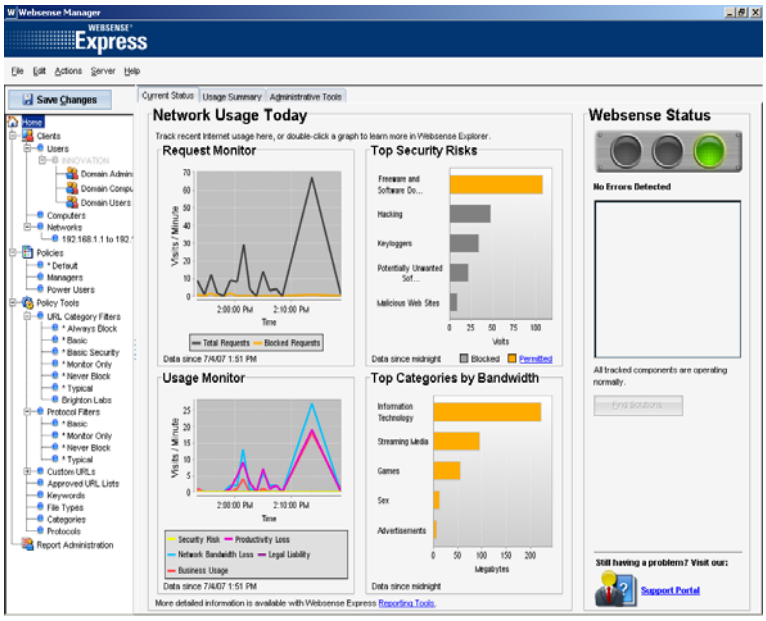
Websense Express 1.0

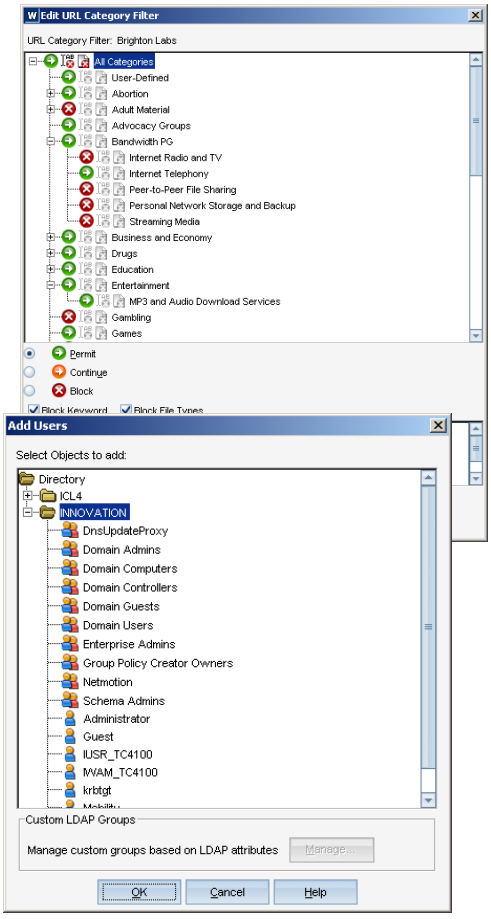


Small to mid-sized businesses need the same tough security measures on their network as enterprises but few have the resources to manage them effectively. In many cases SMBs have to make do with 'cut-down' solutions that have had their feature set restricted in the drive to reduce costs and complexity. Web content security is a prime example as many SMB solutions have limited filtering capabilities making it difficult to enforce a flexible business AUP (acceptable use policy).

With the launch of its Express product, Websense has taken all the best features of its flagship Enterprise software and packaged it into a solution that is designed to be simple to install, deploy and manage. Along with industrial strength web filtering it delivers protection against malicious web site content which can often circumvent traditional security solutions. Furthermore, it includes protocol filtering capabilities which function at the network and transport layers allowing it to monitor and block applications such as IM, P2P and Skype.

Whereas Enterprise has a distributed architecture, Express is designed to run on a single Windows server where all functions and reporting facilities are accessed and managed from one console. You have two options as Websense Express (WSX) can be delivered on a preconfigured HP ProLiant pedestal or rack server (North America only) or you can load the software yourself. For this review we opted for the latter approach and used a Supermicro dual Xeon server loaded with Windows Server 2003 R2 as our base system.

WSX is completely transparent to network clients so deployment is particularly easy as workstations and client browsers do not need to be reconfigured. However, unlike the majority of appliances that function as transparent gateways, Websense Express has a different modus operandi. Transparent gateways generally need to be placed in between LAN and WAN links which can cause a small amount of downtime. Obviously, the WSX server needs to see all web traffic to be able to filter it but it sits to one side rather than mid-stream. The server uses two NICs (network interface cards) with one dedicated to monitoring traffic and the other providing blocking and notification functions. Two scenarios are supported as you can connect the monitoring NIC to an Ethernet hub which also has the Internet feed passing through it or link it to a switch and mirror, or span, traffic from the WAN port.

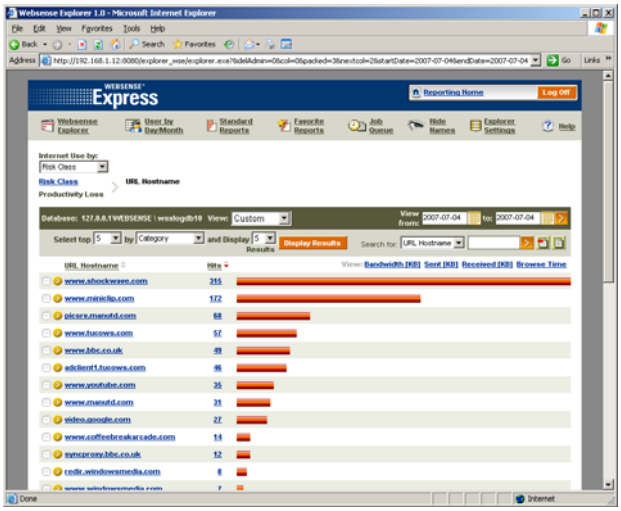


For testing we chose the latter method and had no problems configuring an HP ProCurve Switch 2848 to span traffic from our WAN ports to the WSX filtering connection. The blocking NIC just needs to see all of the LAN systems so setup for this is simple enough. We would recommend taking some time out to make sure you have your connections in the right place as it is possible for some systems to slip through the net if the blocking NIC can't see them. Usefully, Websense includes a network monitoring tool that shows all LAN systems detected by the NIC and also those that are generating HTTP traffic

Software installation is smoothly handled by a single routine that detects your NICs and asks which roles they should play. You just need to provide a Windows domain account for the server to use and that's all there is to it. We found initial installation could be completed in less than thirty minutes. First contact is via the Websense Manager which opens with a tidy home page providing a complete rundown of network usage and server status. More on this later as your first task is to license the software and once a registration code has been entered the Websense master database will be automatically downloaded.

Websense uses a database currently comprising 24.5 million web sites organised into more than ninety categories. At the time of review this was over 300MB in size and took us ninety minutes to retrieve but the download is a one-time process as WSX subsequently carries out automatic incremental database updates. Protection against critical threats is provided during the initial download as a sub-segment of the database is loaded during installation.

WSX enforces basic filtering immediately as its default policy is to block access for all LAN systems to malicious web sites and the majority of messaging applications. From here you can create your own policies which contain separate filters for URL categories, protocols and approved web sites. These are then applied to your client systems and each policy runs to a schedule that determines when it is active. This makes WSX more flexible as it allows you to, for example, apply an AUP for normal working hours and different ones outside these hours where you may wish to relax filtering restrictions.



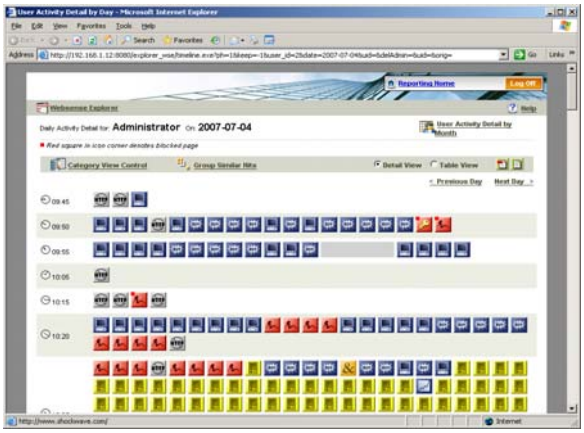
WSX integrates with Windows directory services and we had no problems with it working happily with our Windows Server 2003 AD services allowing us to import users, groups, domains and organizational units. Businesses without directory services can still use WSX as it also allows you to define networks by address ranges or individual computers by their IP addresses.

WSX offers the most extensive URL filtering capabilities we've seen at this level of the market as its database is organized into over ninety categories – most competing products only offer between forty and fifty categories at most. During testing we found policy creation simple enough as we defined our URL and protocol filtering categories and could use existing ones as templates and then edit them. We could add lists of approved URLs, implement blocking by URL keyword and stop specific file types from being downloaded. For very precise filtering it is possible to deploy policies that only contain approved URLs which will block everything else.

Along with blocking or permitting access to web sites WSX offers a Continue option. This could prove very useful as you can allow access to certain sites but only for a specific period of time and once the countdown has expired users will be blocked from further access. We had no problems using the protocol filters to stop our test clients accessing services such as FTP and Windows Messenger. For the latter, once a blocking policy was in action all our test clients found that they were unable to sign in to their accounts.

Policy based filtering has other advantages as modifying a URL or protocol category automatically propagates the changes to any policy that is using it. We found that as soon as we had saved changes to our categories they were enforced immediately on our client systems. WSX impressed during testing as its URL category filtering was particularly accurate. Normally, with SMB web filtering products we expect a few sites to slip through the net but WSX never failed to correctly identify all the sites our clients visited during the test period.

Reporting is often a big casualty with SMB security products but not so with WSX as these are very detailed. Furthermore, the report functions are very accessible as double clicking on any of the graphs in the home page takes you straight to the Websense Explorer which loads a web based report on the relevant data. You can drill down through each category for more in-depth detail on specific users, URLs and domains. Favourite reports can be stored and scheduled to run regularly with the output emailed to selected users and exported as PDFs and Excel spreadsheets. We particularly liked the web usage reports as these provide a blow by blow account of the selected user's every move. Each web site visited is represented by a different icon showing what category it has been classed as and whether access was permitted or denied and each icon contains a hotlink to the URL it represents.



Websense already has an enviable reputation in the enterprise web content filtering market and Websense Express takes a well established product as its foundation and delivers a wealth of features to smaller businesses. It does require a dedicated server but installation has been neatly streamlined and its transparency means it won't require any extra client configuration during implementation.

The use of policies makes it simple to deploy allowing company-wide AUPs and protection against malicious web sites to be easily enforced and the extensive protocol filtering capabilities are not normally seen in security products at this price point. The sophisticated reporting tools also make it stand out as these are far superior to the majority of competing SMB web filtering products.

Testing conducted and report compiled by

Binary Testing Ltd Newhaven Enterprise Centre Denton Island Newhaven BN9 9BA
Tel: 01273 615270 E info@binarytesting.com