



Best Practices & Deployment
SurfControl Mobile Filter v 5.0.2.60
rev2.1, January 2006

Enterprise Threat Protection

Notice

© 2006 SurfControl. All rights reserved. SurfControl, SurfControl E-mail Filter, SurfControl Web Filter, SurfControl RiskFilter, SurfControl Mobile Filter, SurfControl Enterprise Threat Shield, SurfControl Report Central, Single Management Console, Virtual Control Agent, Anti-Spam Agent, Anti-Virus Agent, Virtual Learning Agent, Virtual Image Agent, and the LexiMatch logos are registered trademarks and trademarks of SurfControl plc. All other trademarks are properties of their respective owners.

No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, photocopying, recording, or otherwise, without the prior permission of the copyright owner.

.

.

.

ABOUT SURFCONTROL MOBILE FILTER

SurfControl Mobile Filter extends your Internet Acceptable Use Policy to remote users and branch offices -- no matter how they connect to the Internet (including wireless hot-spots, local ISPs or hotel dial-ups). SurfControl Mobile Filter provides all the protection of Web Filter (including the Internet Threat Database and the Real-time Threat Technology of the Virtual Control Agent) with the ability to manage and share rules, and monitor and report from a central location.

How to Use This Guide

The purpose of this document is to help facilitate your Mobile Filter installation by outlining the options for deployment and configuration. This document covers:

- Network topology.
- Deployment recommendations.
- Installation recommendations for Mobile Filter Server and Mobile Filter Client.
- Sizing guidance.
- Best practice guidelines, including recommendations on how to help facilitate Mobile Filter's security settings.

For details on installing Mobile Filter, refer to the [Mobile Filter Installation Guide](#). For details on administering Mobile Filter Server, consult the [Mobile Filter Administrator's Guide](#).

NETWORK TOPOLOGY

Mobile Filter leverages the server-client relationship between Mobile Filter Server (a Windows 2000 or 2003 server used only for Mobile Filter), and Mobile Filter Client, which you install on all laptops and other remote PCs that are not connected to your corporate network.

Mobile Filter uses pass-through technology to apply your filtering rules. When a mobile user (a device with Mobile Filter Client installed, such as a laptop or remote desktop), attempts to connect to the Internet, Mobile Filter Client sends the Internet request to Mobile Filter Server, which checks it against your enabled rules. Mobile Filter Server then passes the Block or Allow decision back to Mobile Filter Client.

Allowed Requests

When a mobile user attempts to connect to the Internet, the client installed on the laptop or remote PC checks the request against the rules you configured within Mobile Filter Server. If the request is allowed, the user can proceed with connecting to the site.

Figure 1 illustrates this flow.

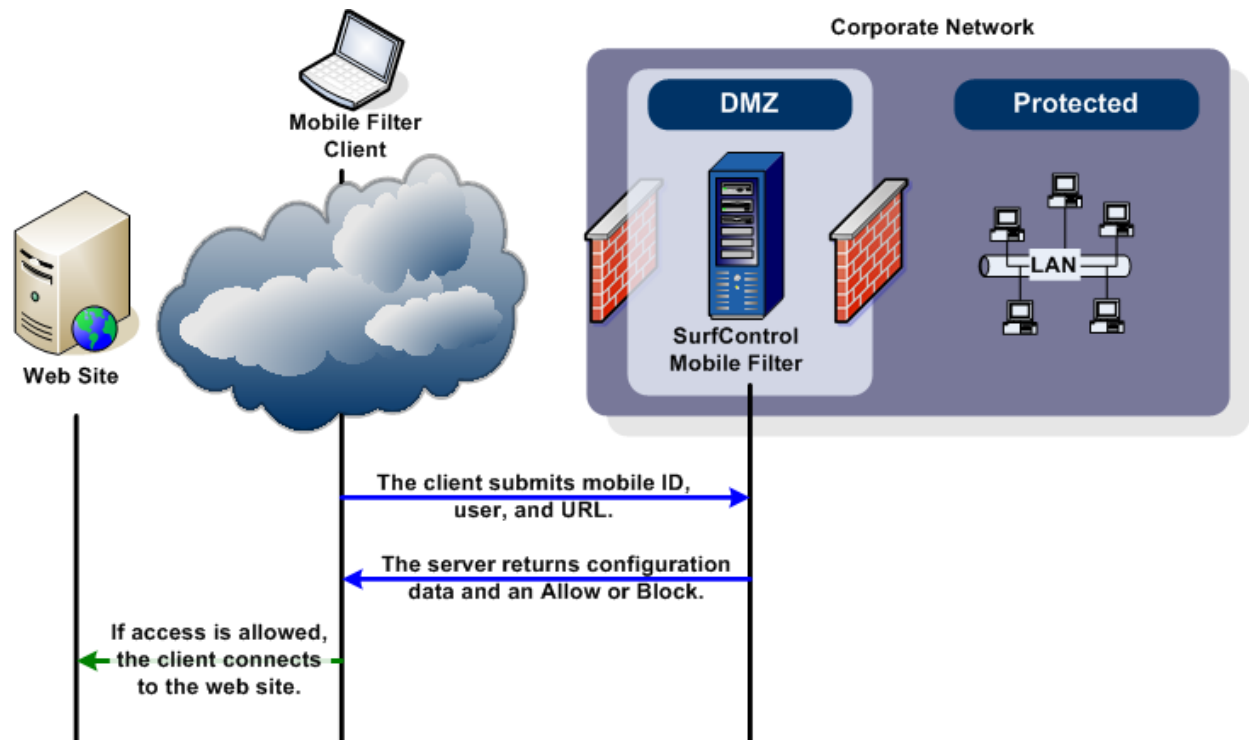


Figure 1 User's request is allowed

Blocked Requests

If the request is not allowed, Mobile Filter Server returns the Block decision to the client installed on the remote PC or laptop, which presents the Access Denied page to the user.

Figure 2 depicts this scenario.

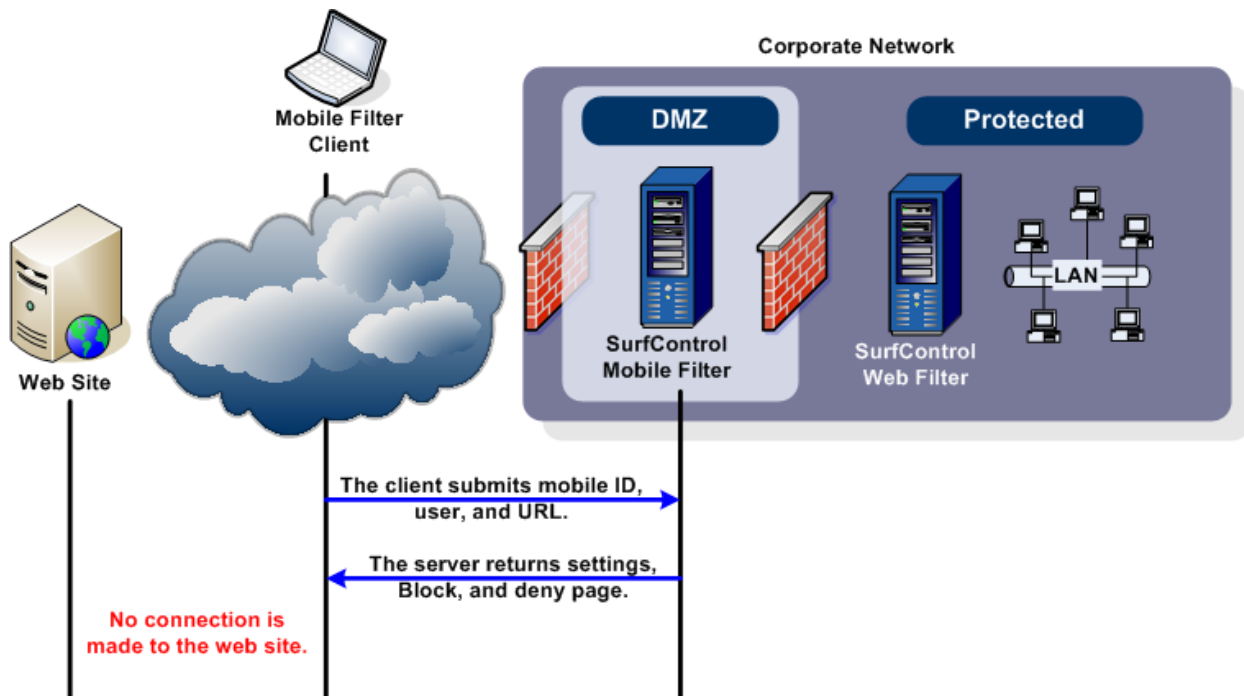


Figure 2 User's request is blocked

DEPLOYMENT

While it is possible to deploy Mobile Filter Server and the Mobile Filter database within the DMZ or within the protected network, **SurfControl recommends that you deploy Mobile Filter Server in the DMZ.**

In the DMZ

When you deploy Mobile Filter Server and the Mobile Filter database in the DMZ (as shown in Figure 3), this ensures that the traffic between Mobile Filter Client and Mobile Filter Server does not cross your internal firewall. Additionally, because Mobile Filter Server requires IIS, you may want to install Mobile Filter Server on your IIS server, which already resides in the DMZ.

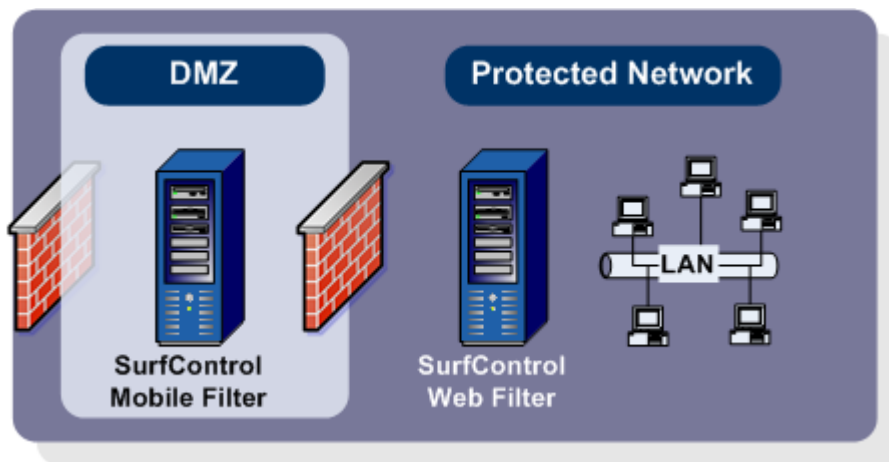


Figure 3 Mobile Filter deployed in the DMZ

If you have an instance of Web Filter that filters users within your protected network, you can write Mobile Filter data to the same SQL database -- sharing the same rule set and using a single database for running reports.

If you do not want to write Mobile Filter data to the database within your protected network, you can also create a database in the DMZ exclusively for your mobile users.

More detailed database recommendations appear on page 10.

Within the Protected Network

Mobile Filter is designed to be deployed in the DMZ, and this is the only deployment SurfControl recommends. Mobile Filter uses IIS, which is a web server and should reside in the DMZ.

Configuring Mobile Filter for Failover

When you configure Mobile Filter for failover, if one of the Mobile Filter servers becomes unavailable, clients automatically communicate with an alternate server.

- .
- .
- . **Installation**

One way to configure failover is with DNS round robin. In this configuration, each Mobile Filter server shares the same fully qualified domain name; when a client makes a request, DNS returns the list of IP addresses associated with the fully qualified domain name. The client machine then attempts to communicate with the first IP address in the list. If the first IP address in the list is also unavailable, the client tries to contact the second, and so on, until the client establishes a connection.

For more information on configuring Mobile Filter for failover, refer to Knowledge Base article 1741: [“How to Configure Failover for Mobile Filter.”](#)

INSTALLATION

Mobile Filter’s installation includes four parts:

- Mobile Filter Server.
- Mobile Filter Client.
- Service Pack 2 (applied to the server).
- For upgrades only, Service Pack 2 (applied to all clients).

Note: If you downloaded Mobile Filter after January 17th, 2006, you do not need to apply the service pack to the clients.

- CNDS (installed on your internal Web Filter server).

MOBILE FILTER SERVER

The Mobile Filter Server installation includes the following components:

- SurfControl Mobile Filter Server.
- SurfControl Report Central (SRC).
- MSDE.
- Service Pack 2 (applied after the installation).

You must install Mobile Filter Server on a server with IIS. Make sure IIS is running before performing the Mobile Filter Server installation. Refer to page 8 for details on installing and configuring IIS.

When you install Mobile Filter Server, you install all administrative components, including the Monitor, Rules Administrator, Mobile Filter Administrator, and SRC.

During the installation, you may install MSDE, which you can install locally or in another location. Likewise, if you have a fully licensed version of SQL, you may choose to not install MSDE and instead use your existing instance of SQL.

Service Pack 2 includes important security enhancements and fixes. Service Pack 2 is available as a separate download on SurfControl’s web site, and must be applied to Mobile Filter Server after you install Mobile Filter in order to communicate with Mobile Filter Client.

MOBILE FILTER CLIENT

Mobile Filter Client is a separate download from SurfControl's web site. Install Mobile Filter Client on every laptop or remote PC you want to monitor and filter.

For easiest deployment, SurfControl recommends that you install the client to all workstations simultaneously using Active Directory and Group Policy. For details on installing the client using this method, refer to page 7 of the [Service Pack 2 for Mobile Filter Installation Guide](#).

If you are already running an older version of Mobile Filter Client (anything prior to 5.0.2.60), you must apply Service Pack 2 to all instances of Mobile Filter Client. (You do not need to apply the service pack to the clients if this is your first installation of Mobile Filter.)

CORPORATE NETWORK DETECTION SERVICE (CNDS)

If your network uses Network Address Translation (NAT) and has a version of Web Filter for filtering users within your protected network, SurfControl recommends that you install CNDS on the Web Filter server.

CNDS is an optional component (downloadable from SurfControl's web site) that detects whether Mobile Filter Client is connecting to your corporate network. If CNDS detects the presence of Mobile Filter Client, CNDS sends a signal to the client, putting it to "sleep."

This defers all filtering to your internal Web Filter server while the Mobile Filter Client is connected to your network -- preventing redundant monitoring or any rule conflicts between Mobile Filter and Web Filter.

After you install and configure CNDS on your internal Web Filter server, enter the details of the Web Filter server within Mobile Filter.

To perform this configuration on the Mobile Filter server:

- 1 From the **Start** menu, select **Programs, SurfControl Web Filter, Mobile Administrator**.
- 2 Click **Configure** and select **Corporate Web Filters**.
- 3 Click **Add** and enter the details of the Web Filter server.
- 4 Click **Accept, OK**.

For details on configuring CNDS on the Web Filter server, refer to the [SurfControl Mobile Filter Installation Guide](#).

RECOMMENDED INSTALLATION ORDER

To ensure that you have optimally prepared each installation component for the others, SurfControl recommends that you install the Mobile Filter components in the following order:

- 1 Install and configure IIS on the server to be used for Mobile Filter Server.
- 2 Install Mobile Filter Server. This installation includes the optional install of MSDE, and the cascading install of SRC.
- 3 On each laptop or remote PC, install Mobile Filter Client.
- 4 If you have corporate Web Filter servers, install CNDS on the Web Filter servers.

For details on installing all components of Mobile Filter, refer to the [SurfControl Mobile Filter Installation Guide](#).

MOBILE FILTER SIZING

Mobile Filter Server and each laptop or remote PC must meet the specifications outlined below.

MOBILE FILTER SERVER SIZE

SurfControl recommends that each Mobile Filter Server manage no more than 2,000 mobile users.

Mobile Filter Server must meet the minimum specifications listed in Table 1*.

Table 1 Mobile Filter Managing 2,000 users

Component	Recommendation
Supported Operating Systems	Windows 2000 Server SP4 Windows Server 2003 SP1
Required Applications	Microsoft IIS
Processor	Pentium IV or higher
Memory	1 GB
Disk Space	5 GB free

*These sizing recommendations include the presence of SRC and MSDE on Mobile Filter Server.

MOBILE FILTER CLIENT SIZE

A laptop or remote PC must meet the following minimum specifications in order to install Mobile Filter Client.

Table 2 Mobile Workstations: Requirements to Install Mobile Filter Client

Supported Operating Systems	Windows XP Windows 2000/2003
Processor	Pentium III or higher
Memory	48 MB
Disk Space	10 MB free

BEST PRACTICES

When configuring Mobile Filter Server, SurfControl recommends that you follow the guidelines suggested below.

INSTALL, CONFIGURE, AND SECURE IIS

Mobile Filter Server requires IIS. Before you install Mobile Filter Server, make sure that IIS is running on the server. To locate IIS on your Windows server, click **Start** and select **All Programs, Administrative Tools**.

Installing IIS

IIS is a Windows component. If you need to add IIS to your server, you can add it through the Add or Remove Programs utility. SurfControl recommends that you do this prior to the Mobile Filter installation.

To add IIS on a Windows 2000 server:

- 1 From the **Start** menu, select **Settings, Control Panel, Add or Remove Programs, Add or Remove Windows Components**.
- 2 Select **Internet Information Services (IIS)**, and click **Next** to begin the installation process.

To add IIS on a Windows 2003 server:

- 1 From the **Start** menu, select **Control Panel, Add or Remove Programs, Add or Remove Windows Components**.
- 2 Highlight **Application Server** and click **Details**.
- 3 Select **Internet Information Services (IIS)**, and click **Next** to begin the installation process.
- 4 From the **Start** menu, select **Administrative Tools**.
- 5 Double-click **Internet Information Services (IIS) Manager**.

- 6 Expand the IIS tree to **Web Service Extensions**.
- 7 Highlight **Web Service Extensions, All Unknown ISAPI Extensions**.
- 8 Click **Allow**.

Configuring IIS for HTTPS

To use HTTPS on the server either on port 443 (the default port for HTTPS) or any other port, you must configure IIS to listen for connections on a secure port.

For details on performing this configuration, refer to [Microsoft Knowledge Base Article 324069](#).

Securing IIS

IIS is a web server. When a user requests a web site, Mobile Filter Server checks the request against the rules database, using IIS. SurfControl recommends that you take measures to secure IIS before you install Mobile Filter Server.

For details on locking down IIS, refer to [Microsoft Knowledge Base Article 325864](#).

SECURE MOBILE FILTER CLIENT FROM USER TAMPERING

To prevent users from tampering with Mobile Filter Client, SurfControl recommends that you make sure users do not have local administrative privileges, or that you prevent them from having “write” access to the registry.

For more information on securing the Windows registry, refer to http://www.windowsecurity.com/articles/Securing_the_Windows_2000_Registry.html.

SECURE THE LDAP CONNECTION BETWEEN MOBILE FILTER AND THE DOMAIN CONTROLLER

A DMZ is not connected to the directory services within a protected network. Therefore, by default, you are unable to use the network group objects in the Rules Administrator. However, you can configure Mobile Filter to access your directory services by opening Port 389 on your internal firewall.

Note: Make sure this firewall configuration is in accordance with your network security policies before you make any changes.

When performing this configuration, **SurfControl recommends that you secure the LDAP connection between Mobile Filter and the domain controller**. For details on performing this configuration, refer to Knowledge Base Article 1739: [“How to Secure Mobile Filter’s LDAP Connection.”](#)

SECURE THE CONNECTION BETWEEN THE CLIENT AND THE SERVER

SurfControl recommends that you ensure a secure connection between Mobile Filter Client and Mobile Filter Server. You can configure the security of the server and the client during the installation of Service Pack 2 or on the server itself by configuring port 443 to use HTTPS.

SECURE THE CONNECTION BETWEEN MOBILE FILTER AND THE SQL SERVER

If your SQL server is not already running in a fully secure environment, SurfControl recommends that you configure a secure connection to the SQL server after you create the Mobile Filter's database.

Note: Be sure to secure the connection *after* you create Mobile Filter's database.

For details on performing this procedure, refer to Knowledge Base Article 1738: [“How to Secure Mobile Filter's Connection to SQL.”](#)

EXCLUDE THE WEB FILTER DIRECTORY FROM REAL-TIME SCANNING

If your anti-virus software uses real-time virus scanning, SurfControl recommends that you configure your anti-virus software to exclude the following directories on Mobile Filter Server:

- The directory on Mobile Filter Server that stores flat files (by default, C:\Program Files\SurfControl\Web Filter). For information on how to store flat files in a different directory, refer to Knowledge Base Article 1301: [“How to Change Flat File Locations.”](#)
- If SQL/MSDE is installed on Mobile Filter Server, the SQL directory (by default, C:\Program Files\Microsoft SQL Server\Data).

CONFIGURE THE WEB FILTER SERVICE

In Services (from the Windows Control Panel), make sure Mobile Filter's Web Filter service:

- Runs as a Windows user with proper permissions on the SQL database.
- Re-starts on failure.
- Starts automatically.

CONFIGURE DATABASE SETTINGS

Follow SurfControl's recommendations for database configuration and sizing as listed below, taking into consideration the size and needs of your unique organization.

SQL vs. MSDE

MSDE, included with the Mobile Filter Server download, is based on Microsoft SQL server technology. An MSDE database has a 2 GB size limitation and does not include management tools, but is an effective database for environments with fewer than 500 mobile users. For environments with more than 500 users, SurfControl recommends using a fully licensed version of SQL, which allows more flexibility and the ability to fine-tune database performance.

SurfControl also recommends a fully licensed version of SQL in environments with multiple Web Filter and/or Mobile Filter servers writing to a shared database; MSDE is designed for a single server connection only.

Authentication to the Database

To ensure a solid connection to the database, SurfControl recommends that you authenticate to the database using SQL authentication, not Windows (trusted) authentication.

Running Reports on a Database Residing in the DMZ

If you have deployed Mobile Filter's database in the DMZ and you want to run reports from within your protected network on mobile users, you can connect to Report Central using a secure (HTTPS) connection.

Refer to the [SurfControl Report Central Administrator's Guide](#) for details on using a secure connection to run reports.

Database Sizing

SurfControl estimates that 5,000 users generate approximately 1 GB of data per month.

However, the size of your database correlates to:

- The amount of traffic your employees generate.
- The amount of traffic Mobile Filter is monitoring.
- The number of users Mobile Filter is monitoring.

The amount of data your database can handle depends on:

- Whether the database is installed on Mobile Filter Server or a dedicated server.
- The amount of available RAM on the database server.
- The type of processor used by the database server.
- How much disk space is available on the database server.

Database Maintenance

In order to maintain Mobile Filter at its optimum level of performance (and to prevent your system from crashing or hanging), SurfControl recommends that you execute the tasks listed in Table 3 on a regular basis.

If you are using an MSDE database, be sure that your database maintenance plan keeps your database at under 2 GB.

Table 3 Maintenance Plan

Action	Servers	Frequency
Update Category List	Web Filter servers	Daily
Export Rules (from the Rules Administrator)	SQL Server	Monthly
Archive Web Filter Database	SQL Server	Monthly
Purge Web Filter Database	SQL Server	Monthly
Compact Web Filter Database	SQL Server	Monthly (to occur after the purge)

Before you purge the Monitor database:

- Make an archive copy of the database.
- Make sure that the flat file import process (dbupdate.exe) is not running.

Note: When you perform a purge, be sure you have enough disk space for the purge to be successful. The available disk space on your server should be twice the size of the database.

- .
- .
- . *Best Practices*